aws

Panduan Pengguna

Amazon Detective

Amazon Detective: Panduan Pengguna

Table of Contents

Apa itu Detektif Amazon?

Amazon Detective membantu Anda menganalisis, menyelidiki, dan mengidentifikasi akar penyebab temuan keamanan atau aktivitas mencurigakan dengan cepat. Detective secara otomatis mengumpulkan data log dari sumber daya Anda. AWS Kemudian menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk menghasilkan visualisasi yang membantu Anda melakukan penyelidikan keamanan yang lebih cepat dan lebih efisien. Agregasi data Detective prebuilt, ringkasan, dan konteks membantu Anda menganalisis dan menentukan sifat dan tingkat kemungkinan masalah keamanan dengan cepat.

Dengan Detective, Anda dapat mengakses data peristiwa historis hingga satu tahun. Data ini tersedia melalui serangkaian visualisasi yang menunjukkan perubahan jenis dan volume aktivitas pada jendela waktu yang dipilih. Detektif menghubungkan perubahan ini dengan temuan. GuardDuty Untuk informasi lebih lanjut tentang sumber data di Detektif, lihat. the section called “Sumber data yang digunakan dalam grafik perilaku”

Dengan menggabungkan data secara otomatis dan menyediakan alat visual, Amazon Detective memungkinkan Anda melakukan investigasi keamanan yang lebih cepat dan efisien. Anda dapat dengan cepat menganalisis potensi masalah dan menentukan ruang lingkup ancaman keamanan.

Topik

Fitur Detektif Amazon

Berikut adalah beberapa cara utama Detektif Amazon membantu untuk menyelidiki aktivitas mencurigakan di AWS lingkungan Anda dan menganalisis sumber daya untuk mengidentifikasi akar penyebab masalah keamanan.

Kelompok pencari Detektif

Grup pencarian Detektif memungkinkan Anda memeriksa beberapa aktivitas yang terkait dengan peristiwa keamanan potensial. Anda dapat menganalisis akar penyebab GuardDuty temuan tingkat keparahan tinggi menggunakan kelompok temuan. Jika pelaku ancaman mencoba untuk membahayakan AWS lingkungan Anda, mereka biasanya melakukan serangkaian tindakan yang menghasilkan beberapa temuan keamanan dan perilaku yang tidak biasa.

Halaman grup temuan di Detective menampilkan semua grup temuan terkait yang diekstrak dari grafik perilaku Anda di halaman grup pencarian. Anda dapat mengamati bukti untuk berbagai jenis utama (seperti pengguna IAM atau peran IAM). Untuk beberapa jenis bukti, Anda dapat mengamati bukti untuk semua akun.

Detective menyediakan visualisasi interaktif dari setiap kelompok pencari untuk membantu Anda menyelidiki masalah keamanan lebih cepat dan lebih menyeluruh. Visualisasi dirancang untuk menampilkan entitas dan temuan yang terlibat dalam insiden keamanan, sehingga lebih mudah untuk memahami koneksi dan akar penyebab. membantu Anda menyelidiki masalah lebih cepat dan lebih menyeluruh dengan sedikit usaha. Panel Visualisasi grup temuan menampilkan temuan dan entitas yang terlibat dalam kelompok temuan.

Investigasi Detektif untuk temuan triase

Dengan Detective Investigation Anda dapat menyelidiki pengguna IAM dan peran IAM menggunakan indikator kompromi, yang dapat membantu Anda menentukan apakah sumber daya terlibat dalam insiden keamanan. Indikator penyusupan (IOC) adalah artefak yang diamati di dalam atau pada jaringan, sistem, atau lingkungan yang dapat (dengan tingkat kepercayaan tinggi) mengidentifikasi aktivitas berbahaya atau insiden keamanan. Dengan investigasi Detektif, Anda dapat memaksimalkan efisiensi, fokus pada ancaman keamanan, dan memperkuat kemampuan respons insiden.

Detective Investigation menggunakan model pembelajaran mesin dan kecerdasan benang untuk memunculkan hanya masalah yang paling kritis dan mencurigakan, yang memungkinkan Anda untuk fokus pada investigasi tingkat tinggi. Ini secara otomatis menganalisis sumber daya di AWS lingkungan Anda untuk mengidentifikasi indikator potensial kompromi atau aktivitas yang mencurigakan. Ini memungkinkan Anda mengidentifikasi pola dan memahami sumber daya mana yang dipengaruhi oleh peristiwa keamanan, menawarkan pendekatan proaktif untuk identifikasi dan mitigasi ancaman.

Anda dapat menggunakan memulai Investigasi Detektif dari konsol Detektif dengan Menjalankan Investigasi Detektif. Untuk menjalankan investigasi secara terprogram, gunakan

StartInvestigationpengoperasian Detective API. Jika Anda menggunakan AWS Command Line Interface (AWS CLI) jalankan perintah start-investigation.

Integrasi Detektif dengan Amazon Security Lake

Detective terintegrasi dengan Amazon Security Lake, yang berarti Anda dapat melakukan kueri dan mengambil data log mentah yang disimpan oleh Security Lake. Dengan integrasi ini, Anda dapat mengumpulkan log dan peristiwa dari sumber berikut yang didukung oleh Security Lake secara native.

- AWS CloudTrail acara manajemen
- Log Aliran Amazon Virtual Private Cloud (Amazon VPC)

Setelah Anda mengintegrasikan Detective dengan Security Lake, Detective mulai menarik log mentah dari Security Lake yang terkait dengan AWS CloudTrail peristiwa manajemen dan Amazon VPC Flow Logs. Anda dapat meminta log mentah untuk melihat log dan peristiwa di Detective.

Selidiki volume aliran VPC

Dengan Detective, Anda dapat secara interaktif memeriksa detail aktivitas alur jaringan virtual private cloud (VPC) dari instans Amazon Elastic Compute Cloud (Amazon EC2) dan pod Kubernetes. Detective secara otomatis mengumpulkan log aliran VPC dari akun yang dipantau, menggabungkannya dengan instans EC2, dan menyajikan ringkasan visual dan analitik tentang alur jaringan ini.

Untuk instans EC2, detail aktivitas untuk Volume aliran VPC Keseluruhan menunjukkan interaksi antara instans EC2 dan alamat IP selama rentang waktu yang dipilih.

Untuk pod Kubernetes, Volume aliran VPC secara keseluruhan menampilkan keseluruhan volume byte masuk dan keluar dari alamat IP yang ditetapkan pod Kubernetes untuk semua alamat IP tujuan.

Mengakses Detektif Amazon

Amazon Detective tersedia di sebagian besar. Wilayah AWS Untuk daftar Wilayah di mana Detektif saat ini tersedia, lihat titik akhir Detektif Amazon dan kuota di. Referensi Umum AWS Untuk informasi tentang mengelola Wilayah AWS akun Anda Akun AWS, lihat Menentukan Wilayah AWS akun mana yang dapat digunakan dalam Panduan AWS Account Management Referensi.

Di setiap Wilayah, Anda dapat bekerja dengan Detektif dengan salah satu cara berikut.

AWS Management Console

AWS Management Console Ini adalah antarmuka berbasis browser yang dapat Anda gunakan untuk membuat dan mengelola AWS sumber daya. Sebagai bagian dari konsol itu, konsol Detektif Amazon menyediakan akses ke akun Detektif, data, dan sumber daya Anda. Anda dapat melakukan tugas Detektif apa pun dengan menggunakan konsol Detektif — meninjau potensi ancaman keamanan dan menganalisis, menyelidiki, dan mengidentifikasi akar penyebab temuan keamanan.

AWS alat baris perintah

Dengan alat baris AWS perintah, Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk melakukan tugas dan AWS tugas Detektif. Menggunakan baris perintah dapat lebih cepat dan lebih nyaman dibandingkan konsol. Alat baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan tugas.

AWS menyediakan dua set alat baris perintah: AWS Command Line Interface (AWS CLI) dan AWS Tools for PowerShell. Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat Panduan AWS Command Line Interface Pengguna. Untuk informasi tentang menginstal dan menggunakan Alat untuk PowerShell, lihat Panduan AWS Tools for PowerShell Pengguna.

AWS SDK

AWS menyediakan SDK yang terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman — misalnya, Java, Go, Python, C ++, dan .NET. SDK menyediakan akses terprogram yang nyaman ke Detective dan lainnya. Layanan AWS SDK menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi tentang menginstal dan menggunakan AWS SDK, lihat Alat untuk Dibangun AWS.

API REST Detektif Amazon

Amazon Detective REST API memberi Anda akses terprogram yang komprehensif ke akun Detektif, data, dan sumber daya Anda. Dengan API ini, Anda dapat mengirim permintaan HTTPS langsung ke Detective. Namun, tidak seperti alat baris AWS perintah dan SDK, penggunaan API ini mengharuskan aplikasi Anda untuk menangani detail tingkat rendah seperti membuat hash untuk menandatangani permintaan. Untuk informasi tentang API ini, lihat Referensi API Detective.

Harga untuk Amazon Detective

Seperti AWS produk lainnya, tidak ada kontrak atau komitmen minimum untuk menggunakan Amazon Detective.

Detective pricing didasarkan pada beberapa dimensi — dan membebankan tarif flat berjenjang per GB untuk semua data terlepas dari sumbernya. Untuk informasi selengkapnya, lihat harga Detektif Amazon.

Untuk membantu Anda memahami dan memperkirakan biaya penggunaan Detective, Detective memberikan perkiraan biaya penggunaan untuk akun Anda. Anda dapat meninjau perkiraan ini di konsol Detektif Amazon dan mengaksesnya dengan Amazon Detective API. Bergantung pada cara Anda menggunakan layanan, Anda mungkin dikenakan biaya tambahan untuk menggunakan yang lain Layanan AWS dalam kombinasi dengan fitur Detektif tertentu, seperti integrasi Security Lake dan Detective Investigations.

Saat Anda mengaktifkan Detektif untuk pertama kalinya, Anda Akun AWS secara otomatis terdaftar dalam uji coba gratis Detektif 30 hari. Ini termasuk akun individu yang diaktifkan sebagai bagian dari organisasi di AWS Organizations. Selama uji coba gratis, tidak ada biaya untuk menggunakan Detektif dalam hal yang berlaku. Wilayah AWS

Untuk membantu Anda memahami dan memperkirakan biaya penggunaan Detective setelah uji coba gratis berakhir, Detective memberi Anda perkiraan biaya penggunaan berdasarkan penggunaan Detective selama uji coba. Data penggunaan Anda juga menunjukkan jumlah waktu yang tersisa sebelum uji coba gratis berakhir. Anda dapat meninjau data ini di konsol Detektif Amazon dan mengaksesnya dengan Amazon Detective API.

Bagaimana cara kerja Detektif?

Detective secara otomatis mengekstrak peristiwa berbasis waktu seperti upaya login, panggilan API, dan lalu lintas jaringan dari dan log aliran VPC AWS CloudTrail Amazon. Ini juga menelan temuan yang terdeteksi oleh GuardDuty.

Dari peristiwa tersebut, Detective menggunakan pembelajaran mesin dan visualisasi untuk menciptakan pandangan interaktif yang terpadu tentang perilaku sumber daya Anda dan interaksi di antara mereka dari waktu ke waktu. Anda dapat menjelajahi grafik perilaku ini untuk memeriksa tindakan yang berbeda seperti upaya masuk yang gagal atau panggilan API yang mencurigakan. Anda juga dapat melihat bagaimana tindakan ini memengaruhi sumber daya seperti AWS akun dan

instans Amazon EC2. Anda dapat menyesuaikan cakupan dan garis waktu grafik perilaku untuk berbagai tugas:

- Selidiki dengan cepat setiap aktivitas yang berada di luar norma.
- Identifikasi pola yang mungkin mengindikasikan masalah keamanan.
- Memahami semua sumber daya yang dipengaruhi oleh temuan.

Visualisasi yang disesuaikan dengan Detektif memberikan dasar untuk dan meringkas informasi akun. Temuan ini dapat membantu menjawab pertanyaan seperti “Apakah ini panggilan API yang tidak biasa untuk peran ini?” Atau “Apakah lonjakan lalu lintas dari contoh ini diharapkan?”

Dengan Detective, Anda tidak perlu mengatur data apa pun atau mengembangkan, mengonfigurasi, atau menyetel kueri dan algoritme Anda sendiri. Tidak ada biaya di muka dan Anda hanya membayar untuk acara yang dianalisis, tanpa perangkat lunak tambahan untuk digunakan atau umpan lain untuk berlangganan.

Siapa yang menggunakan Detektif?

Ketika sebuah akun mengaktifkan Detektif, itu menjadi akun administrator untuk grafik perilaku. Grafik perilaku adalah kumpulan data yang diekstraksi dan dianalisis dari satu atau lebih AWS akun. Akun administrator mengundang akun anggota untuk menyumbangkan datanya ke grafik perilaku akun administrator.

Detective juga terintegrasi dengan. AWS Organizations Akun manajemen organisasi Anda menunjuk akun administrator Detektif untuk organisasi. Akun administrator Detektif memungkinkan akun organisasi sebagai akun anggota dalam grafik perilaku organisasi.

Untuk informasi tentang cara Detektif menggunakan data sumber dari akun grafik perilaku, lihat. the section called “Sumber data yang digunakan dalam grafik perilaku”

Untuk informasi tentang cara akun administrator mengelola grafik perilaku, lihatMengelola akun. Untuk informasi tentang cara akun anggota mengelola undangan grafik perilaku dan keanggotaan mereka, lihat. the section called “Untuk akun anggota: Mengelola undangan dan keanggotaan”

Akun administrator menggunakan analisis dan visualisasi yang dihasilkan dari grafik perilaku untuk menyelidiki AWS sumber daya dan GuardDuty temuan. Menggunakan integrasi Detective dengan GuardDuty dan AWS Security Hub, Anda dapat berputar dari GuardDuty temuan di layanan ini langsung ke konsol Detective.

Investigasi Detektif berfokus pada aktivitas yang terhubung dengan sumber daya yang terlibat AWS . Untuk ikhtisar proses investigasi di Detektif, lihat Bagaimana Detektif Amazon digunakan untuk penyelidikan di Panduan Pengguna Detektif.

Layanan terkait

Untuk lebih mengamankan data, beban kerja, dan aplikasi Anda AWS, pertimbangkan untuk menggunakan yang berikut ini Layanan AWS dalam kombinasi dengan Amazon Detective.

AWS Security Hub

AWS Security Hub memberi Anda pandangan komprehensif tentang keadaan keamanan AWS sumber daya Anda dan membantu Anda memeriksa AWS lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Hal ini dilakukan sebagian dengan mengkonsumsi, menggabungkan, mengatur, dan memprioritaskan temuan keamanan Anda dari beberapa (Layanan AWS termasuk Detective) dan produk Partner Network (APN) yang didukung AWS . Security Hub membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi di AWS lingkungan Anda.

Untuk mempelajari selengkapnya tentang Security Hub, lihat Panduan Pengguna AWS Security Hub.

Amazon GuardDuty

Amazon GuardDuty adalah layanan pemantauan keamanan yang menganalisis dan memproses jenis AWS log tertentu, seperti log peristiwa AWS CloudTrail data untuk Amazon S3 CloudTrail dan log peristiwa manajemen. Ini menggunakan umpan intelijen ancaman, seperti daftar alamat IP dan domain berbahaya, dan pembelajaran mesin untuk mengidentifikasi aktivitas yang tidak terduga dan berpotensi tidak sah dan berbahaya di lingkungan Anda. AWS

Untuk mempelajari selengkapnya GuardDuty, lihat Panduan GuardDuty Pengguna Amazon.

Danau Keamanan Amazon

Amazon Security Lake adalah layanan danau data keamanan yang dikelola sepenuhnya. Anda dapat menggunakan Security Lake untuk secara otomatis memusatkan data keamanan dari AWS lingkungan, penyedia SaaS, sumber lokal, sumber cloud, dan sumber pihak ketiga ke dalam data lake yang dibuat khusus yang disimpan di akun Anda. AWS Security Lake membantu Anda menganalisis data keamanan, sehingga Anda bisa mendapatkan pemahaman yang lebih lengkap

tentang postur keamanan Anda di seluruh organisasi Anda. Dengan Security Lake, Anda juga dapat meningkatkan perlindungan beban kerja, aplikasi, dan data Anda.

Untuk mempelajari selengkapnya tentang Security Lake, lihat Panduan Pengguna Amazon Security Lake. Untuk mempelajari lebih lanjut tentang menggunakan Detective and Security Lake bersama-sama, lihat. Integrasi dengan Amazon Security Lake

Untuk mempelajari tentang layanan AWS keamanan tambahan, lihat Keamanan, Identitas, dan Kepatuhan di AWS.

Memulai dengan Amazon Detective

Tutorial ini memberikan pengantar untuk Amazon Detective. Anda akan belajar cara mengaktifkan Detektif untuk akun Anda AWS . Anda juga akan belajar cara memverifikasi bahwa Detektif telah mulai menelan dan mengekstrak data dari AWS akun Anda ke dalam grafik perilaku Anda.

Saat Anda mengaktifkan Detektif Amazon, Detektif membuat grafik perilaku khusus Wilayah yang memiliki akun Anda sebagai akun administratornya. Ini awalnya satu-satunya akun dalam grafik perilaku. Akun administrator kemudian dapat mengundang AWS akun lain untuk menyumbangkan data mereka ke grafik perilaku. Lihat Mengelola akun.

Mengaktifkan Detective in a Region untuk pertama kalinya juga memulai uji coba gratis 30 hari untuk grafik perilaku. Jika akun menonaktifkan Detective dan kemudian mengaktifkannya lagi, tidak ada uji coba gratis yang tersedia. Lihat the section called “Tentang uji coba gratis untuk grafik perilaku”.

Setelah uji coba gratis, setiap akun dalam grafik perilaku ditagih untuk data yang mereka kontribusikan. Akun administrator dapat melacak penggunaan dan melihat total biaya yang diproyeksikan untuk periode 30 hari tipikal untuk seluruh grafik perilaku mereka. Untuk informasi selengkapnya, lihat the section called “Penggunaan dan biaya akun administrator”. Akun anggota dapat melacak penggunaan dan biaya yang diproyeksikan untuk grafik perilaku yang mereka miliki. Untuk informasi selengkapnya, lihat the section called “Pelacakan penggunaan akun anggota”.

Topik

Sebelum kamu memulai

Sebelum Anda dapat mengaktifkan Amazon Detective, Anda harus memiliki file. Akun AWS

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk secara online.

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya dalam akun. Sebagai praktik terbaik keamanan, tetapkan akses administratif ke pengguna administratif dan hanya gunakan pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun kapan pun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.

   Untuk bantuan masuk menggunakan pengguna root, lihat Masuk sebagai pengguna root dalam Panduan Pengguna AWS Sign-In .
2. Aktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Membuat pengguna administratif

1. Aktifkan Pusat Identitas IAM.

Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke sebuah pengguna administratif.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email Anda saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Prasyarat

Pastikan persyaratan berikut terpenuhi.

Memberikan izin Detektif yang diperlukan

Sebelum Anda dapat mengaktifkan Detektif, Anda harus memastikan bahwa kepala IAM Anda memiliki izin Detektif yang diperlukan. Prinsipal dapat berupa pengguna atau peran yang sudah Anda gunakan, atau Anda dapat membuat pengguna atau peran baru yang akan digunakan untuk Detektif.

Saat Anda mendaftar ke Amazon Web Services (AWS), akun Anda secara otomatis mendaftar untuk semua Layanan AWS, termasuk Amazon Detective. Namun, untuk mengaktifkan dan menggunakan Detektif, pertama-tama Anda harus menyiapkan izin yang memungkinkan Anda mengakses konsol Detektif Amazon dan operasi API. Anda atau administrator Anda dapat melakukan ini dengan menggunakan AWS Identity and Access Management (IAM) untuk melampirkan kebijakan `AmazonDetectiveFullAccess` terkelola ke kepala IAM Anda, yang memberikan akses ke semua tindakan Detektif.

Volume data akun harus dalam kuota Detektif

Volume data yang mengalir ke grafik perilaku harus kurang dari maksimum yang diizinkan oleh Detective.

Ketika Anda mencoba mengaktifkan Detective, jika volume data untuk akun Anda terlalu besar, Anda tidak dapat mengaktifkan Detective. Konsol Detective menampilkan notifikasi untuk menunjukkan bahwa volume data terlalu besar.

AWS Command Line Interface Versi yang didukung

Untuk menggunakan AWS CLI to melakukan tugas Detective, versi minimum yang diperlukan adalah 1.16.303.

Rekomendasi

Direkomendasikan penyelarasan dengan GuardDuty dan AWS Security Hub

Jika Anda terdaftar GuardDuty dan AWS Security Hub, kami menyarankan agar akun Anda menjadi akun administrator untuk layanan tersebut. Jika akun administrator sama untuk ketiga layanan, maka poin integrasi berikut bekerja dengan mulus.

- Di GuardDuty atau Security Hub, saat melihat detail untuk GuardDuty temuan, Anda dapat beralih dari detail temuan ke profil pencarian Detektif.
- Di Detektif, saat menyelidiki GuardDuty temuan, Anda dapat memilih opsi untuk mengarsipkan temuan itu.

Jika Anda memiliki akun administrator GuardDuty dan Security Hub yang berbeda, sebaiknya Anda menyelaraskan akun administrator berdasarkan layanan yang lebih sering Anda gunakan.

- Jika Anda menggunakan GuardDuty lebih sering, maka aktifkan Detective menggunakan akun GuardDuty administrator.

  Jika Anda menggunakan AWS Organizations untuk mengelola akun, tetapkan akun GuardDuty administrator sebagai akun administrator Detektif untuk organisasi.
- Jika Anda lebih sering menggunakan Security Hub, aktifkan Detective menggunakan akun administrator Security Hub.

  Jika Anda menggunakan Organizations untuk mengelola akun, tetapkan akun administrator Security Hub sebagai akun administrator Detektif untuk organisasi.

Jika Anda tidak dapat menggunakan akun administrator yang sama di semua layanan, maka setelah Anda mengaktifkan Detective, Anda dapat membuat peran lintas akun secara opsional. Peran ini memberikan akses akun administrator ke akun lain.

Untuk informasi tentang cara IAM mendukung jenis peran ini, lihat Menyediakan akses ke pengguna IAM di AWS akun lain yang Anda miliki di Panduan Pengguna IAM.

Pembaruan yang disarankan untuk frekuensi GuardDuty CloudWatch notifikasi

Di GuardDuty, detektor dikonfigurasi dengan frekuensi CloudWatch notifikasi Amazon untuk melaporkan kejadian temuan berikutnya. Ini termasuk mengirim notifikasi ke Detektif.

Secara default, frekuensinya enam jam. Ini berarti bahwa bahkan jika temuan berulang berkali-kali, kejadian baru tidak tercermin dalam Detektif sampai enam jam kemudian.

Untuk mengurangi jumlah waktu yang dibutuhkan Detektif untuk menerima pembaruan ini, kami menyarankan agar akun GuardDuty administrator mengubah pengaturan pada detektor mereka menjadi 15 menit. Perhatikan bahwa mengubah konfigurasi tidak berpengaruh pada biaya penggunaan GuardDuty.

Untuk informasi tentang menyetel frekuensi notifikasi, lihat Memantau GuardDuty Temuan dengan CloudWatch Acara Amazon di Panduan GuardDuty Pengguna Amazon.

Mengaktifkan Detektif Amazon

Anda dapat mengaktifkan Detective dari konsol Detective, Detective API, atau. AWS Command Line Interface

Anda hanya dapat mengaktifkan Detektif sekali di setiap Wilayah. Jika Anda sudah menjadi akun administrator untuk grafik perilaku di Wilayah, maka Anda tidak dapat mengaktifkan Detektif lagi di Wilayah tersebut.

Mengaktifkan Detektif (Konsol)

Anda dapat mengaktifkan Amazon Detective dari file. AWS Management Console

Untuk mengaktifkan Detective (konsol)

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.

2. Pilih Mulai.
3. Pada halaman Aktifkan Detektif Amazon, Align akun administrator (disarankan) menjelaskan rekomendasi untuk menyelaraskan akun administrator antara Detektif dan Amazon dan. GuardDuty AWS Security Hub Lihat the section called “Direkomendasikan penyelarasan dengan GuardDuty dan AWS Security Hub”.
4. Tombol Lampirkan kebijakan IAM membawa Anda langsung ke konsol IAM dan membuka kebijakan yang disarankan, Anda memiliki opsi untuk melampirkan kebijakan yang disarankan ke kepala sekolah yang Anda gunakan untuk Detektif. Jika Anda tidak memiliki izin untuk beroperasi di konsol IAM, dalam izin yang diperlukan, Anda dapat menyalin kebijakan Nama Sumber Daya Amazon (ARN) untuk memberikannya kepada administrator IAM Anda. Mereka dapat melampirkan kebijakan atas nama Anda.

   Konfirmasikan bahwa kebijakan IAM yang diperlukan sudah ada.
5. Bagian Tambahkan tag memungkinkan Anda menambahkan tag ke grafik perilaku.

   Untuk menambahkan tanda, lakukan hal berikut:

   a. Pilih Tambahkan tag baru.
   b. Untuk Kunci, masukkan nama tag.
   c. Untuk Nilai, masukkan nilai tag.

   Untuk menghapus tag, pilih opsi Hapus untuk tag itu.
6. Pilih Aktifkan Detektif Amazon.
7. Setelah mengaktifkan Detektif, Anda dapat mengundang akun anggota ke grafik perilaku Anda.

   Untuk menavigasi ke halaman Manajemen akun, pilih Tambahkan anggota sekarang. Untuk informasi tentang mengundang akun anggota, lihatthe section called “Mengundang akun anggota ke grafik perilaku”.

Mengaktifkan Detektif (Detective API,) AWS CLI

Anda dapat mengaktifkan Amazon Detective dari Detective API atau file. AWS Command Line Interface

Untuk mengaktifkan Detective (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `CreateGraph`

- AWS CLI: Pada baris perintah, jalankan `create-graph`perintah.

```
aws detective create-graph --tags '{"tagName": "tagValue"}'
```

Perintah berikut memungkinkan Detektif dan menetapkan nilai `Department` tag ke. `Security`

```
aws detective create-graph --tags '{"Department": "Security"}'
```

Mengaktifkan Detektif di Seluruh Wilayah (skrip Python aktif) GitHub

Detective menyediakan skrip open-source GitHub yang melakukan hal berikut:

- Mengaktifkan Detektif untuk akun administrator dalam daftar Wilayah yang ditentukan
- Menambahkan daftar akun anggota yang disediakan ke setiap grafik perilaku yang dihasilkan
- Mengirim email undangan ke akun anggota
- Secara otomatis menerima undangan untuk akun anggota

Untuk informasi tentang cara mengkonfigurasi dan menggunakan GitHub skrip, lihatthe section called “Skrip Python Detektif Amazon”.

Memeriksa bahwa data sedang diekstraksi

Setelah Anda mengaktifkan Detective, Detective mulai menyerap dan mengekstrak data dari AWS akun Anda ke dalam grafik perilaku Anda.

Untuk ekstraksi awal, data biasanya tersedia dalam grafik perilaku dalam waktu 24 jam.

Salah satu cara untuk memeriksa bahwa Detective mengekstraksi data adalah dengan mencari contoh nilai pada halaman Detective Search.

Untuk memeriksa nilai contoh pada halaman Pencarian

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi, pilih Cari.
3. Dari menu Pilih jenis, pilih jenis item.

Contoh dari data Anda berisi kumpulan sampel pengenal dari jenis yang dipilih yang ada dalam data grafik perilaku Anda.

Jika Anda dapat melihat nilai contoh, maka Anda tahu bahwa data sedang dicerna dan diekstraksi ke dalam grafik perilaku Anda.

Konsep dan terminologi Detektif Amazon

Istilah dan konsep berikut ini penting untuk memahami Detektif Amazon dan cara kerjanya.

Akun administrator

Akun AWS Yang memiliki grafik perilaku dan yang menggunakan grafik perilaku untuk penyelidikan.

Akun administrator mengundang akun anggota untuk menyumbangkan data mereka ke grafik perilaku. Untuk informasi selengkapnya, lihat the section called “Mengundang akun anggota ke grafik perilaku”.

Untuk grafik perilaku organisasi, akun administrator adalah akun administrator Detektif yang ditetapkan oleh akun manajemen organisasi. Untuk informasi selengkapnya, lihat the section called “Menunjuk akun administrator Detektif”. Akun administrator Detektif dapat mengaktifkan akun organisasi apa pun sebagai akun anggota dalam grafik perilaku organisasi. Untuk informasi selengkapnya, lihat the section called “Mengelola akun anggota organisasi”.

Akun administrator juga dapat melihat penggunaan data untuk grafik perilaku, dan menghapus akun anggota dari grafik perilaku.

Organisasi Sistem Otonom (ASO)

Organisasi berjudul yang ditugaskan sistem otonom. Sistem otonom ini adalah jaringan heterogen atau seperangkat jaringan yang menggunakan logika dan kebijakan routing yang serupa.

Grafik perilaku

Kumpulan data terkait yang dihasilkan dari data sumber masuk yang dikaitkan dengan satu atau lebih Akun AWS.

Setiap grafik perilaku menggunakan struktur temuan, entitas, dan hubungan yang sama.

Akun administrator yang didelegasikan ()AWS Organizations

Dalam Organizations, akun administrator yang didelegasikan untuk suatu layanan dapat mengelola penggunaan layanan untuk organisasi.

Dalam Detektif, akun administrator Detektif juga merupakan akun administrator yang didelegasikan, kecuali akun administrator Detektif adalah akun manajemen organisasi. Akun manajemen organisasi tidak dapat berupa akun administrator yang didelegasikan.

Dalam Detektif, delegasi diri diperbolehkan. Akun manajemen organisasi dapat mendelegasikan akun mereka sendiri untuk menjadi administrator Detektif yang didelegasikan tetapi ini akan didaftarkan atau diingat hanya dalam lingkup Detektif dan bukan organisasi.

Akun administrator Detektif

Akun yang ditunjuk oleh akun manajemen organisasi menjadi akun administrator untuk grafik perilaku organisasi di Wilayah. Untuk informasi selengkapnya, lihat the section called “Menunjuk akun administrator Detektif”.

Detective merekomendasikan agar akun manajemen organisasi memilih akun selain akun mereka.

Jika akun tersebut bukan akun manajemen organisasi, maka akun administrator Detektif juga merupakan akun administrator yang didelegasikan untuk Detective in Organizations.

Data sumber detektif

Versi informasi yang diproses dan terstruktur dari jenis umpan berikut:

- Log dari AWS layanan, seperti AWS CloudTrail log dan Amazon VPC Flow Logs
- GuardDuty temuan

Detective menggunakan data sumber Detective untuk mengisi grafik perilaku. Detective juga menyimpan salinan data sumber Detective untuk mendukung analitiknya.

Entitas

Item yang diekstraksi dari data yang dicerna.

Setiap entitas memiliki tipe, yang mengidentifikasi jenis objek yang diwakilinya. Contoh tipe entitas termasuk alamat IP, instans Amazon EC2, dan pengguna. AWS

Entitas dapat berupa AWS sumber daya yang Anda kelola, atau alamat IP eksternal yang telah berinteraksi dengan sumber daya Anda.

Untuk setiap entitas, data sumber juga digunakan untuk mengisi properti entitas. Nilai properti dapat diekstraksi langsung dari catatan sumber atau dikumpulkan di beberapa catatan.

Menemukan

Masalah keamanan yang terdeteksi oleh Amazon GuardDuty.

Menemukan grup

Kumpulan temuan, entitas, dan bukti terkait yang mungkin terkait dengan peristiwa atau masalah keamanan yang sama. Detective menghasilkan kelompok pencarian berdasarkan model pembelajaran mesin bawaan.

Bukti Detektif

Detective mengidentifikasi bukti tambahan yang terkait dengan kelompok temuan berdasarkan data dalam grafik perilaku Anda yang dikumpulkan dalam 45 hari terakhir. Bukti ini disajikan sebagai temuan dengan nilai keparahan Informasi. Bukti memberikan informasi pendukung yang menyoroti aktivitas yang tidak biasa atau perilaku yang tidak diketahui yang berpotensi mencurigakan ketika dilihat dalam kelompok temuan. Contohnya mungkin geolokasi yang baru diamati atau panggilan API yang diamati dalam lingkup waktu penemuan. Saat ini, temuan ini hanya dapat dilihat di Detektif dan tidak dikirim ke Security Hub.

Menemukan ikhtisar

Satu halaman yang memberikan ringkasan informasi tentang temuan.

Ikhtisar temuan berisi daftar entitas yang terlibat untuk temuan tersebut. Dari daftar, Anda dapat berputar ke profil untuk entitas.

Ikhtisar temuan juga berisi panel detail yang berisi atribut temuan.

Entitas volume tinggi

Entitas yang memiliki koneksi ke atau dari sejumlah besar entitas lain selama interval waktu. Misalnya, instans EC2 mungkin memiliki koneksi dari jutaan alamat IP. Jumlah koneksi melebihi ambang batas yang dapat ditampung Detektif.

Ketika waktu lingkup saat ini berisi interval waktu volume tinggi, Detective memberi tahu pengguna.

Untuk informasi selengkapnya, lihat Melihat detail untuk entitas bervolume tinggi di Panduan Pengguna Detektif Amazon.

Investigasi

Proses memprioritaskan aktivitas yang mencurigakan atau menarik, menentukan ruang lingkupnya, sampai ke sumber atau penyebabnya yang mendasarinya, dan kemudian menentukan bagaimana melanjutkannya.

Akun anggota

Sebuah akun administrator Akun AWS yang diundang untuk menyumbangkan data ke grafik perilaku. Dalam grafik perilaku organisasi, akun anggota dapat berupa akun organisasi yang mengaktifkan akun administrator Detektif sebagai akun anggota.

Akun anggota yang diundang dapat menanggapi undangan grafik perilaku dan menghapus akun mereka dari grafik perilaku. Untuk informasi selengkapnya, lihat the section called “Untuk akun anggota: Mengelola undangan dan keanggotaan”.

Akun organisasi tidak dapat mengubah keanggotaannya dalam grafik perilaku organisasi.

Semua akun anggota juga dapat melihat informasi penggunaan untuk akun mereka di seluruh grafik perilaku tempat mereka menyumbangkan data.

Mereka tidak memiliki akses lain ke grafik perilaku.

Grafik perilaku organisasi

Grafik perilaku yang dimiliki oleh akun administrator Detective. Akun manajemen organisasi menunjuk akun administrator Detektif. Untuk informasi selengkapnya, lihat the section called “Menunjuk akun administrator Detektif”.

Dalam grafik perilaku organisasi, akun administrator Detektif mengontrol apakah akun organisasi adalah akun anggota. Akun organisasi tidak dapat menghapus dirinya sendiri dari grafik perilaku organisasi.

Akun administrator Detektif juga dapat mengundang akun lain ke grafik perilaku organisasi.

Profil

Satu halaman yang menyediakan kumpulan visualisasi data yang terkait dengan aktivitas untuk suatu entitas.

Untuk temuan, profil membantu analis untuk menentukan apakah temuan itu benar-benar menjadi perhatian atau positif palsu.

Profil memberikan informasi untuk mendukung penyelidikan terhadap temuan atau untuk perburuan umum untuk kegiatan yang mencurigakan.

Panel profil

Visualisasi tunggal pada profil. Setiap panel profil dimaksudkan untuk membantu menjawab pertanyaan atau pertanyaan spesifik untuk membantu analis dalam penyelidikan.

Panel profil dapat berisi pasangan nilai kunci, tabel, garis waktu, diagram batang, atau bagan geolokasi.

Hubungan

Aktivitas yang terjadi antara entitas individu. Hubungan juga diekstraksi dari data sumber yang masuk.

Mirip dengan entitas, hubungan memiliki tipe, yang mengidentifikasi jenis entitas yang terlibat dan arah koneksi. Contoh tipe hubungan adalah alamat IP yang menghubungkan ke instans Amazon EC2.

Lingkup waktu

Jendela waktu yang digunakan untuk cakupan data yang ditampilkan pada profil.

Waktu lingkup default untuk temuan mencerminkan waktu pertama dan terakhir ketika aktivitas mencurigakan diamati.

Waktu cakupan default untuk profil entitas adalah 24 jam sebelumnya.

Data dalam grafik perilaku

Di Amazon Detective, Anda melakukan investigasi menggunakan data dari grafik perilaku Detektif.

Grafik perilaku adalah kumpulan data tertaut yang dihasilkan dari data sumber Detektif yang dicerna dari satu atau beberapa akun Amazon Web Services ()AWS.

Grafik perilaku menggunakan data sumber untuk melakukan hal berikut:

- Hasilkan gambaran keseluruhan sistem Anda, pengguna, dan interaksi di antara mereka dari waktu ke waktu
- Lakukan analisis yang lebih rinci tentang aktivitas spesifik untuk membantu Anda menjawab pertanyaan yang muncul saat Anda melakukan investigasi
- Mengkorelasikan koleksi temuan, entitas, dan bukti yang mungkin terkait dengan peristiwa atau masalah keamanan yang sama.

Perhatikan bahwa semua ekstraksi, pemodelan, dan analitik data grafik perilaku terjadi dalam konteks setiap grafik perilaku individu.

Untuk informasi tentang cara akun administrator mengelola akun anggota dalam grafik perilaku, lihat Mengelola akun.

Daftar Isi

Bagaimana Amazon Detective menggunakan data sumber untuk mengisi grafik perilaku

Untuk menyediakan data mentah untuk investigasi, Detective menyatukan data dari seluruh lingkungan AWS Anda dan sekitarnya, termasuk yang berikut:

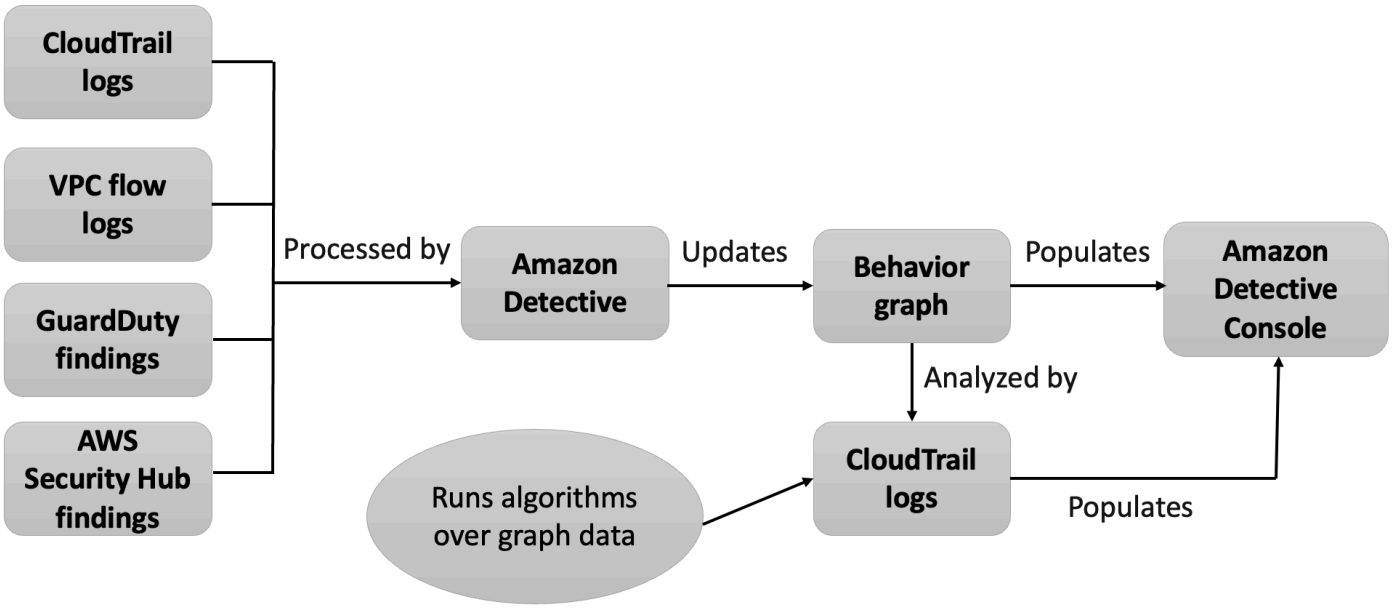
- Log data, termasuk Amazon Virtual Private Cloud (Amazon VPC) dan AWS CloudTrail
- Temuan dari Amazon GuardDuty

- Temuan dari AWS Security Hub

Untuk mempelajari lebih lanjut tentang sumber data yang digunakan dalam grafik perilaku, lihat Sumber data yang digunakan dalam grafik perilaku.

Bagaimana Detective memproses data sumber

Saat data baru masuk, Detective menggunakan kombinasi ekstraksi dan analitik untuk mengisi grafik perilaku.



Ekstraksi Detektif

Ekstraksi didasarkan pada aturan pemetaan yang dikonfigurasi. Aturan pemetaan pada dasarnya mengatakan, “Setiap kali Anda melihat potongan data ini, gunakan dengan cara khusus ini untuk memperbarui data grafik perilaku.”

Misalnya, catatan data sumber Detektif yang masuk mungkin menyertakan alamat IP. Jika ya, Detective menggunakan informasi dalam catatan itu untuk membuat entitas alamat IP baru atau memperbarui entitas alamat IP yang ada.

Analitik Detektif

Analytics adalah algoritma yang lebih kompleks yang menganalisis data untuk memberikan wawasan tentang aktivitas yang terkait dengan entitas.

Misalnya, salah satu jenis analitik Detektif menganalisis seberapa sering aktivitas terjadi dengan menjalankan algoritma. Untuk entitas yang melakukan panggilan API, algoritme mencari panggilan API yang biasanya tidak digunakan entitas. Algoritma ini juga mencari lonjakan besar dalam jumlah panggilan API.

Wawasan analitik mendukung investigasi dengan memberikan jawaban atas pertanyaan analis kunci dan sering digunakan untuk mengisi panel temuan dan profil entitas.

Periode pelatihan untuk grafik perilaku baru

Salah satu jalan investigasi untuk sebuah temuan adalah dengan membandingkan aktivitas selama waktu lingkup temuan dengan aktivitas yang terjadi sebelum temuan terdeteksi. Aktivitas yang belum pernah terlihat sebelumnya mungkin lebih mencurigakan.

Beberapa panel profil Detektif Amazon menyoroti aktivitas yang tidak diamati selama periode waktu sebelum temuan. Beberapa panel profil juga menampilkan nilai dasar untuk menunjukkan aktivitas rata-rata selama 45 hari sebelum waktu lingkup. Waktu lingkup adalah ringkasan aktivitas suatu entitas dari waktu ke waktu.

Karena semakin banyak data yang diekstraksi ke dalam grafik perilaku Anda, Detective mengembangkan gambaran yang lebih akurat tentang aktivitas apa yang normal di organisasi Anda dan aktivitas apa yang tidak biasa.

Namun, untuk membuat gambar ini, Detektif membutuhkan akses ke setidaknya dua minggu data. Kematangan analisis Detektif juga meningkat dengan jumlah akun dalam grafik perilaku.

Dua minggu pertama setelah Anda mengaktifkan Detektif dianggap sebagai periode pelatihan. Selama periode ini, panel profil yang membandingkan aktivitas waktu lingkup dengan aktivitas sebelumnya menampilkan pesan bahwa Detektif berada dalam periode pelatihan.

Selama masa percobaan, Detective merekomendasikan agar Anda menambahkan sebanyak mungkin akun anggota ke grafik perilaku. Ini memberi Detective kumpulan data yang lebih besar, yang memungkinkannya menghasilkan gambaran yang lebih akurat tentang aktivitas normal untuk organisasi Anda.

Ikhtisar struktur data grafik perilaku

Struktur data grafik perilaku mendefinisikan struktur data yang diekstraksi dan dianalisis. Ini juga mendefinisikan bagaimana data sumber dipetakan ke grafik perilaku.

Jenis elemen dalam struktur data grafik perilaku

Struktur data grafik perilaku terdiri dari elemen informasi berikut.

Entitas

Entitas mewakili item yang diekstrak dari data sumber Detektif.

Setiap entitas memiliki tipe, yang mengidentifikasi jenis objek yang diwakilinya. Contoh tipe entitas termasuk alamat IP, instans Amazon EC2, dan pengguna. AWS

Untuk setiap entitas, data sumber juga digunakan untuk mengisi properti entitas. Nilai properti dapat diekstraksi langsung dari catatan sumber atau dikumpulkan di beberapa catatan.

Beberapa properti terdiri dari satu skalar atau nilai agregat. Misalnya, untuk instans EC2, Detective melacak jenis instance dan jumlah total byte yang diproses.

Properti deret waktu melacak aktivitas dari waktu ke waktu. Misalnya, untuk instans EC2, Detective melacak dari waktu ke waktu port unik yang digunakannya.

Hubungan

Suatu hubungan mewakili aktivitas yang terjadi antara entitas individu. Hubungan juga diekstraksi dari data sumber Detektif.

Mirip dengan entitas, hubungan memiliki tipe, yang mengidentifikasi jenis entitas yang terlibat dan arah koneksi. Contoh tipe hubungan adalah alamat IP yang menghubungkan ke instans EC2.

Untuk setiap hubungan individu, seperti alamat IP tertentu yang menghubungkan ke instance tertentu, Detective melacak kejadian dari waktu ke waktu.

Jenis entitas dalam struktur data grafik perilaku

Struktur data grafik perilaku terdiri dari jenis entitas dan hubungan yang melakukan hal berikut:

- Lacak server, alamat IP, dan agen pengguna yang digunakan
- Lacak AWS pengguna, peran, dan akun yang digunakan
- Lacak koneksi jaringan dan otorisasi yang terjadi di lingkungan Anda AWS

Struktur data grafik perilaku berisi jenis entitas berikut.

AWS akun

AWS akun yang ada di data sumber Detektif.

Untuk setiap akun, Detektif menjawab beberapa pertanyaan:

- Panggilan API apa yang digunakan akun?
- Agen pengguna apa yang menggunakan akun tersebut?
- Organisasi sistem otonom (ASOs) apa yang digunakan akun?
- Di lokasi geografis apa akun tersebut aktif?

AWS peran

AWS peran yang ada dalam data sumber Detektif.

Untuk setiap peran, Detektif menjawab beberapa pertanyaan:

- Panggilan API apa yang memiliki peran yang digunakan?
- Agen pengguna apa yang memiliki peran yang digunakan?
- ASO apa yang memiliki peran yang digunakan?
- Di lokasi geografis apa peran tersebut aktif?
- Sumber daya apa yang telah mengambil peran ini?
- Peran apa yang diasumsikan peran ini?
- Sesi peran apa yang melibatkan peran ini?

AWS pengguna

AWS pengguna yang hadir dalam data sumber Detektif.

Untuk setiap pengguna, Detective menjawab beberapa pertanyaan:

- Panggilan API apa yang digunakan pengguna?
- Agen pengguna apa yang digunakan pengguna?
- Di lokasi geografis apa pengguna aktif?
- Peran apa yang diasumsikan pengguna ini?
- Sesi peran apa yang melibatkan pengguna ini?

Pengguna federasi

Contoh pengguna federasi. Contoh pengguna federasi meliputi:

- Identitas yang masuk menggunakan Security Assertion Markup Language (SAMB)
- Identitas yang masuk menggunakan federasi identitas web

Untuk setiap pengguna federasi, Detective menjawab pertanyaan-pertanyaan ini:

- Penyedia identitas apa yang diautentikasi oleh pengguna federasi?
- Apa audiens pengguna federasi? Audiens mengidentifikasi aplikasi yang meminta token identitas web dari pengguna federasi.
- Di lokasi geografis apa pengguna federasi telah aktif?
- Agen pengguna apa yang digunakan pengguna federasi?
- ASO apa yang digunakan pengguna federasi?
- Peran apa yang diasumsikan oleh pengguna federasi ini?
- Sesi peran apa yang melibatkan pengguna federasi ini?

Instans EC2

Instans EC2 yang ada dalam data sumber Detektif.

Untuk instans EC2, Detective menjawab beberapa pertanyaan:

- Alamat IP apa yang telah dikomunikasikan dengan instans?
- Port apa yang telah digunakan untuk berkomunikasi dengan instance?
- Berapa volume data yang telah dikirim ke dan dari instance?
- VPC apa yang berisi instance?
- Panggilan API apa yang digunakan instans EC2?
- Agen pengguna apa yang menggunakan instans EC2?
- ASO apa yang menggunakan instans EC2?
- Di lokasi geografis apa instans EC2 telah aktif?
- Peran apa yang diasumsikan oleh instans EC2?

Sesi peran

Contoh sumber daya yang mengasumsikan peran. Setiap sesi peran diidentifikasi oleh pengidentifikasi peran dan nama sesi.

Untuk setiap peran, Detektif menjawab beberapa pertanyaan:

- Sumber daya apa yang terlibat dalam sesi peran ini? Dengan kata lain, peran apa yang diasumsikan, dan sumber daya apa yang mengambil peran itu?

Perhatikan bahwa untuk asumsi peran lintas akun, Detektif tidak dapat mengidentifikasi sumber daya yang mengambil peran tersebut.

- Panggilan API apa yang digunakan sesi peran?
- Agen pengguna apa yang memiliki sesi peran yang digunakan?
- ASO apa yang memiliki sesi peran yang digunakan?
- Di lokasi geografis apa sesi peran aktif?
- Pengguna atau peran apa yang memulai sesi peran ini?
- Sesi peran apa yang dimulai dari sesi peran ini?

Temuan

Temuan yang ditemukan oleh Amazon GuardDuty yang dimasukkan ke dalam data sumber Detektif.

Untuk setiap temuan, Detective melacak jenis temuan, asal, dan jendela waktu untuk aktivitas pencarian.

Ini juga menyimpan informasi khusus untuk temuan, seperti peran atau alamat IP yang terlibat dalam aktivitas yang terdeteksi.

Alamat IP

Alamat IP yang ada dalam data sumber Detektif.

Untuk setiap alamat IP, Detective menjawab beberapa pertanyaan:

- Panggilan API apa yang memiliki alamat yang digunakan?
- Port apa yang memiliki alamat yang digunakan?
- Pengguna dan agen pengguna apa yang telah menggunakan alamat IP?
- Di lokasi geografis apa alamat IP telah aktif?
- Instans EC2 apa yang telah ditetapkan dan dikomunikasikan dengan alamat IP ini?

Bucket S3

Bucket S3 yang ada di data sumber Detektif.

Untuk setiap bucket S3, Detective menjawab pertanyaan-pertanyaan ini:

- Prinsipal apa yang berinteraksi dengan bucket S3?
- Panggilan API apa yang dilakukan ke bucket S3?

- Dari lokasi geografis apa kepala sekolah melakukan panggilan API ke bucket S3?
- Agen pengguna apa yang digunakan untuk berinteraksi dengan bucket S3?
- ASO apa yang digunakan untuk berinteraksi dengan bucket S3?

Anda dapat menghapus bucket S3 dan kemudian membuat bucket baru dengan nama yang sama. Karena Detective menggunakan nama bucket S3 untuk mengidentifikasi bucket S3, ia memperlakukan ini sebagai entitas bucket S3 tunggal. Pada profil entitas, waktu pembuatan adalah waktu pembuatan pertama. Waktu penghapusan adalah waktu penghapusan terbaru.

Untuk melihat semua peristiwa pembuatan dan penghapusan, atur waktu lingkup untuk memulai dengan waktu pembuatan dan akhiri dengan waktu penghapusan. Pada panel profil volume panggilan API Keseluruhan, tampilkan detail aktivitas untuk waktu cakupan. Filter metode API untuk ditampilkan `Create` dan `Delete` metode. Lihat the section called “Volume panggilan API keseluruhan”.

Agen pengguna

Agen pengguna yang hadir dalam data sumber Detektif.

Untuk setiap agen pengguna, Detective menjawab pertanyaan seperti berikut:

- Panggilan API apa yang digunakan agen pengguna?
- Pengguna dan peran apa yang telah menggunakan agen pengguna?
- Alamat IP apa yang telah menggunakan agen pengguna?

Klaster EKS

Kluster EKS yang ada di data sumber Detektif.

> **Note**
>
> Untuk melihat detail lengkap untuk jenis entitas ini, sumber data log audit EKS opsional harus diaktifkan. Untuk info selengkapnya lihat Sumber data opsional

Untuk setiap cluster EKS, Detective menjawab pertanyaan-pertanyaan seperti berikut:

- Panggilan API Kubernetes apa yang telah dijalankan di cluster ini?
- Pengguna Kubernetes dan akun layanan (subjek) apa yang aktif di klaster ini?
- Wadah apa yang telah diluncurkan di cluster ini?

- Gambar apa yang digunakan untuk meluncurkan wadah di cluster ini?

Kubernetes Pod

Pod Kubernetes yang ada di data sumber Detective.

> **Note**
>
> Untuk melihat detail lengkap untuk jenis entitas ini, sumber data log audit EKS opsional harus diaktifkan. Untuk info selengkapnya lihat Sumber data opsional

Untuk setiap pod, Detective menjawab pertanyaan-pertanyaan seperti berikut:

- Gambar kontainer apa di pod ini yang umum di akun saya?
- Aktivitas apa yang telah diarahkan pada pod ini?
- Wadah apa yang berjalan di pod ini?
- Apakah pendaftar dari kontainer di pod ini umum di akun saya?
- Wadah apa lagi yang berjalan di pod lain dari beban kerja?
- Apakah ada wadah anomali di pod ini yang tidak ada di pod lain dari beban kerja?

Gambar Kontainer

Gambar kontainer yang ada di data sumber Detektif.

> **Note**
>
> Untuk melihat detail lengkap untuk jenis entitas ini, sumber data log audit EKS opsional harus diaktifkan. Untuk info selengkapnya lihat Sumber data opsional

Untuk setiap gambar kontainer, Detektif menjawab pertanyaan seperti berikut:

- Gambar apa lagi di lingkungan saya yang berbagi repositori atau registri yang sama dengan gambar ini?
- Berapa banyak salinan gambar ini yang berjalan di lingkungan saya?

Subjek Kubernetes

Subjek Kubernetes yang hadir dalam data sumber Detektif. Subjek Kubernetes adalah akun pengguna atau layanan.

> **Note**
>
> Untuk melihat detail lengkap untuk jenis entitas ini, sumber data log audit EKS opsional harus diaktifkan. Untuk info selengkapnya lihat Sumber data opsional

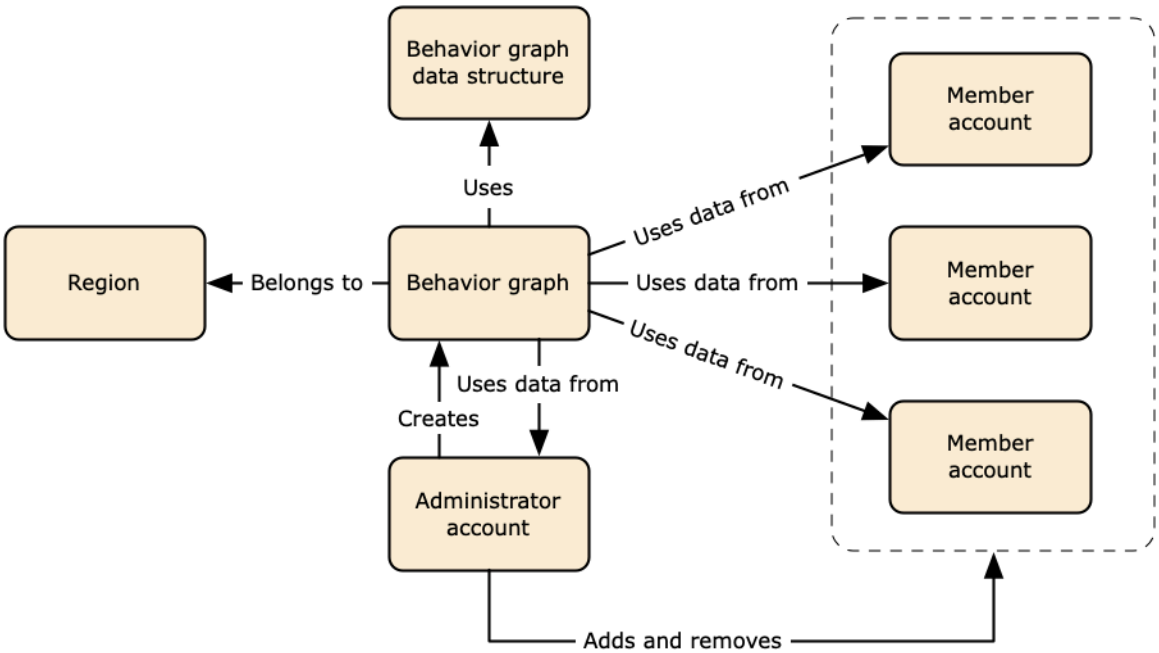
Untuk setiap subjek, Detektif menjawab pertanyaan-pertanyaan seperti berikut:

- Prinsipal IAM apa yang telah diautentikasi sebagai subjek ini?
- Temuan apa yang terkait dengan subjek ini?
- Alamat IP apa yang digunakan subjek?

Sumber data yang digunakan dalam grafik perilaku

Untuk mengisi grafik perilaku, Amazon Detective menggunakan data sumber dari akun administrator grafik perilaku dan akun anggota.

Dengan Detective, Anda dapat mengakses data peristiwa historis hingga satu tahun. Data ini tersedia melalui serangkaian visualisasi yang menunjukkan perubahan jenis dan volume aktivitas pada jendela waktu yang dipilih. Detektif menghubungkan perubahan ini dengan temuan. GuardDuty



Untuk detail tentang struktur data grafik perilaku, lihat Ikhtisar struktur data grafik perilaku di Panduan Pengguna Detektif.

Jenis sumber data inti di Detective

Detective menyerap data dari jenis log ini: AWS

- AWS CloudTrail log
- Log aliran Amazon Virtual Private Cloud (Amazon VPC)
  - Mencerna catatan IPv4 dan IPv6, tetapi bukan catatan MAC yang diproduksi oleh Elastic Fabric Adapters.
  - Menyerap catatan log saat nilai `log-status` bidang dalam `OK` status. Untuk informasi selengkapnya, lihat Catatan log alur di Panduan Pengguna Amazon VPC.
  - Menyerap log aliran yang dihasilkan oleh instans Amazon Elastic Compute Cloud yang hanya berjalan di VPC tersebut. Tidak ada sumber daya lain, seperti gateway NAT, instans RDS, atau cluster Fargate yang digunakan.
  - Menyerap lalu lintas yang diterima dan ditolak.
- Untuk akun yang terdaftar GuardDuty, Detektif juga GuardDuty mencerna temuan.

Detective mengkonsumsi dan peristiwa log aliran CloudTrail VPC menggunakan aliran independen dan duplikatif dari dan log aliran VPC. CloudTrail Proses ini tidak memengaruhi atau menggunakan konfigurasi log aliran VPC CloudTrail dan yang ada. Mereka juga tidak mempengaruhi kinerja atau meningkatkan biaya Anda untuk layanan ini.

Jenis sumber data opsional di Detective

Detective menawarkan paket sumber opsional selain tiga sumber data yang ditawarkan dalam paket inti Detektif (paket inti termasuk log AWS CloudTrail , log Aliran VPC, dan temuan). GuardDuty Paket sumber data opsional dapat dimulai atau dihentikan untuk grafik perilaku kapan saja.

Detective menyediakan uji coba gratis 30 hari untuk semua paket sumber inti dan opsional per Wilayah.

> **Note**
>
> Detective menyimpan semua data yang diterima dari setiap paket sumber data hingga 1 tahun.

Saat ini paket sumber opsional berikut tersedia:

- Log audit EKS

  Paket sumber data opsional ini memungkinkan Detective untuk menyerap informasi terperinci tentang kluster EKS di lingkungan Anda dan menambahkan data tersebut ke grafik perilaku Anda. Detective menghubungkan aktivitas pengguna dengan peristiwa AWS CloudTrail Management dan aktivitas jaringan dengan Amazon VPC Flow Logs tanpa perlu mengaktifkan atau menyimpan log ini secara manual. Lihat Log audit Amazon EKS untuk Detektif untuk detail.
- AWS temuan keamanan

  Paket sumber data opsional ini memungkinkan Detective untuk menyerap data dari Security Hub dan menambahkan data tersebut ke grafik perilaku Anda. Lihat AWS temuan keamanan untuk detail.

Memulai atau menghentikan sumber data opsional:

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Dari panel navigasi di bawah Pengaturan, pilih Umum.
3. Di bawah Paket sumber opsional, pilih Perbarui. Kemudian pilih sumber data yang ingin Anda aktifkan atau batalkan pilihan kotak untuk sumber data yang sudah diaktifkan dan pilih Perbarui untuk mengubah paket sumber data mana yang diaktifkan.

> **Note**
>
> Jika Anda berhenti dan kemudian memulai ulang sumber data opsional, Anda akan melihat celah dalam data yang ditampilkan pada beberapa profil entitas. Kesenjangan ini akan dicatat di tampilan konsol dan mewakili periode waktu ketika sumber data dihentikan. Ketika sumber data dimulai ulang Detektif tidak secara surut menelan data.

Log audit Amazon EKS untuk Detektif

Log audit Amazon EKS adalah paket sumber data opsional yang dapat ditambahkan ke grafik perilaku Detektif Anda. Anda dapat melihat paket sumber opsional yang tersedia, dan statusnya di akun Anda, dari halaman Pengaturan di konsol atau melalui Detective API.

Uji coba gratis 30 hari disediakan untuk sumber data ini. Untuk mempelajari lebih lanjut lihatUji coba gratis untuk sumber data opsional.

Mengaktifkan log audit Amazon EKS memungkinkan Detektif menambahkan informasi mendalam tentang sumber daya yang dibuat dengan Amazon EKS ke grafik perilaku Anda. Sumber data ini meningkatkan informasi yang diberikan tentang jenis entitas berikut: EKS Cluster, Kubernetes Pod, Container Image, dan subjek Kubernetes.

Selain itu, jika Anda telah mengaktifkan log audit EKS sebagai sumber data di Amazon, GuardDuty Anda akan dapat melihat detail untuk temuan Kubernetes. GuardDuty Untuk info selengkapnya tentang mengaktifkan sumber data ini di GuardDuty lihat Perlindungan Kubernetes di Amazon. GuardDuty

> **Note**
>
> Sumber data ini diaktifkan secara default untuk grafik perilaku baru yang dibuat setelah 26 Juli 2022. Untuk grafik perilaku yang dibuat sebelum 26 Juli 2022 harus diaktifkan secara manual.

Menambahkan atau menghapus log audit Amazon EKS sebagai sumber data opsional:

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Dari panel navigasi di bawah Pengaturan, pilih Umum.
3. Di bawah paket Sumber, pilih log audit EKS untuk mengaktifkan sumber data ini. Jika sudah diaktifkan, pilih lagi untuk berhenti menelan log audit EKS ke dalam grafik perilaku Anda.

AWS temuan keamanan

AWS temuan keamanan adalah paket sumber data opsional yang dapat ditambahkan ke grafik perilaku Detektif Anda.

Anda dapat melihat paket sumber opsional yang tersedia, dan statusnya di akun Anda, dari halaman Pengaturan di konsol atau melalui Detective API.

Uji coba gratis 30 hari disediakan untuk sumber data ini. Untuk mempelajari lebih lanjut lihatUji coba gratis untuk sumber data opsional.

Mengaktifkan temuan AWS keamanan memungkinkan Detective untuk menggunakan temuan dari Security Hub yang dikumpulkan oleh Security Hub dari layanan hulu dalam format temuan standar yang disebut AWS Security Format (ASFF), yang menghilangkan kebutuhan akan upaya konversi

data yang memakan waktu. Kemudian menghubungkan temuan yang dicerna di seluruh produk untuk memprioritaskan yang paling penting.

Menambahkan atau menghapus temuan AWS keamanan sebagai sumber data opsional:

> **Note**
>
> Sumber data temuan AWS keamanan diaktifkan secara default untuk grafik perilaku baru yang dibuat setelah 16 Mei 2023. Untuk grafik perilaku yang dibuat sebelum 16 Mei 2023, grafik tersebut harus diaktifkan secara manual.

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Dari panel navigasi di bawah Pengaturan, pilih Umum.
3. Di bawah paket Sumber, pilih temuan AWS keamanan untuk mengaktifkan sumber data ini. Jika sudah diaktifkan, pilih lagi untuk berhenti memasukkan temuan AWS Security Finding Format (ASFF) ke dalam grafik perilaku Anda.

Temuan yang saat ini didukung

Detective menyerap semua temuan ASFF di Security Hub dari layanan yang dimiliki oleh Amazon atau. AWS

- Untuk melihat daftar integrasi layanan yang didukung, lihat Integrasi layanan AWS yang tersedia di AWS Security Hub Panduan Pengguna.
- Untuk daftar sumber daya yang didukung, lihat Sumber daya di Panduan AWS Security Hub Pengguna.
- AWS Temuan Layanan dengan status Kepatuhan tidak ditetapkan `FAILED` dan temuan agregat lintas wilayah tidak dicerna.

Bagaimana Detective mencerna dan menyimpan data sumber

Ketika Detektif diaktifkan, Detektif mulai menelan data sumber dari akun administrator grafik perilaku. Saat akun anggota ditambahkan ke grafik perilaku, Detektif juga mulai menggunakan data dari akun anggota tersebut.

Data sumber Detektif terdiri dari versi terstruktur dan diproses dari umpan asli. Untuk mendukung analitik Detective, Detective menyimpan salinan data sumber Detective.

Proses penyerapan Detektif memasukkan data ke dalam bucket Amazon Simple Storage Service (Amazon S3) di penyimpanan data sumber Detective. Saat data sumber baru tiba, komponen Detektif lainnya mengambil data dan memulai proses ekstraksi dan analitik. Untuk informasi selengkapnya, lihat Bagaimana Detektif menggunakan data sumber untuk mengisi grafik perilaku di Panduan Pengguna Detektif.

Bagaimana Detective memberlakukan kuota volume data untuk grafik perilaku

Detective memiliki kuota ketat pada volume data yang memungkinkan dalam setiap grafik perilaku. Volume data adalah jumlah data per hari yang mengalir ke grafik perilaku Detektif.

Detektif memberlakukan kuota ini ketika akun administrator mengaktifkan Detektif, dan ketika akun anggota menerima undangan untuk berkontribusi pada grafik perilaku.

- Jika volume data untuk akun administrator melebihi 10 TB per hari, maka akun administrator tidak dapat mengaktifkan Detektif.
- Jika volume data yang ditambahkan dari akun anggota akan menyebabkan grafik perilaku melebihi 10 TB per hari, akun anggota tidak dapat diaktifkan.

Volume data untuk grafik perilaku juga dapat tumbuh secara alami dari waktu ke waktu. Detective memeriksa volume data grafik perilaku setiap hari untuk memastikan tidak melebihi kuota.

Jika volume data grafik perilaku mendekati kuota, Detective menampilkan pesan peringatan di konsol. Untuk menghindari melebihi kuota, Anda dapat menghapus akun anggota.

Jika volume data grafik perilaku melebihi 10 TB per hari, maka Anda tidak dapat menambahkan akun anggota baru ke grafik perilaku.

Jika volume data grafik perilaku melebihi 15 TB per hari, maka Detective berhenti menelan data ke dalam grafik perilaku. Kuota 15 TB per hari mencerminkan volume data normal dan lonjakan volume data. Ketika kuota ini tercapai, tidak ada data baru yang dicerna ke dalam grafik perilaku, tetapi data yang ada tidak dihapus. Anda masih dapat menggunakan data historis itu untuk penyelidikan. Konsol menampilkan pesan untuk menunjukkan bahwa penyerapan data ditangguhkan untuk grafik perilaku.

Jika konsumsi data ditangguhkan, Anda harus bekerja sama AWS Support untuk mengaktifkannya kembali. Jika memungkinkan, sebelum Anda menghubungi AWS Support, cobalah untuk menghapus akun anggota untuk mendapatkan volume data di bawah kuota. Ini membuatnya lebih mudah untuk mengaktifkan kembali data ingest untuk grafik perilaku.

Bagaimana Amazon Detective digunakan untuk penyelidikan

Amazon Detective memudahkan untuk menganalisis, menyelidiki, dan dengan cepat mengidentifikasi akar penyebab temuan keamanan atau aktivitas yang mencurigakan. Jika Anda baru mengenal Detektif, lihat Apa itu Detektif Amazon? dan konsep dan terminologi Detektif Amazon.

Topik

Investigasi Detektif

Anda dapat menggunakan fitur Investigasi Detektif Amazon untuk menyelidiki pengguna IAM dan peran IAM menggunakan indikator kompromi, yang dapat membantu Anda menentukan apakah sumber daya terlibat dalam insiden keamanan. Indikator penyusupan (IOC) adalah artefak yang diamati di dalam atau pada jaringan, sistem, atau lingkungan yang dapat (dengan tingkat kepercayaan tinggi) mengidentifikasi aktivitas berbahaya atau insiden keamanan. Dengan Detective Investigations, Anda dapat memaksimalkan efisiensi, fokus pada ancaman keamanan, dan memperkuat kemampuan respons insiden.

Detective Investigations menggunakan model pembelajaran mesin dan intelijen ancaman untuk secara otomatis menganalisis sumber daya di AWS lingkungan Anda untuk mengidentifikasi potensi insiden keamanan. Ini memungkinkan Anda secara proaktif, efektif, dan efisien menggunakan otomatisasi yang dibangun di atas grafik perilaku Detektif untuk meningkatkan operasi keamanan. Dengan menggunakan Detective Investigations, Anda dapat menyelidiki taktik serangan, perjalanan yang tidak mungkin, alamat IP yang menyebar, dan menemukan kelompok. Ini melakukan langkah-langkah investigasi keamanan awal dan menghasilkan laporan yang menyoroti risiko yang diidentifikasi oleh Detektif, untuk membantu Anda memahami peristiwa keamanan dan menanggapi potensi insiden.

Menjalankan Investigasi Detektif

Gunakan investigasi Jalankan untuk menganalisis sumber daya seperti pengguna IAM dan peran IAM dan untuk menghasilkan laporan investigasi. Laporan yang dihasilkan merinci perilaku anomali yang menunjukkan potensi kompromi.

Console

Ikuti langkah-langkah berikut untuk menjalankan Investigasi Detektif dari halaman Investigasi menggunakan konsol Detektif Amazon.

1. Masuk ke Konsol AWS Manajemen. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Investigasi.
3. Di halaman Investigasi, pilih Jalankan investigasi di pojok kanan atas.
4. Di bagian Pilih sumber daya, Anda memiliki tiga cara untuk menjalankan penyelidikan. Anda dapat memilih untuk menjalankan penyelidikan untuk sumber daya yang direkomendasikan oleh Detektif. Anda dapat menjalankan penyelidikan untuk sumber daya tertentu. Anda juga dapat menyelidiki sumber daya dari halaman Pencarian Detektif.

    1. `Choose a recommended resource`Detective merekomendasikan sumber daya berdasarkan aktivitasnya dalam temuan dan menemukan kelompok. Untuk menjalankan investigasi sumber daya yang direkomendasikan oleh Detektif, dalam tabel Sumber daya yang direkomendasikan, pilih sumber daya untuk diselidiki.

        Tabel sumber daya yang direkomendasikan memberikan rincian berikut:

        - Sumber daya ARN — Nama Sumber Daya Amazon (ARN) dari sumber daya. AWS
        - Alasan untuk menyelidiki - Menampilkan alasan utama untuk menyelidiki sumber daya. Alasan Detective merekomendasikan untuk menyelidiki sumber daya adalah sebagai berikut:
            - Jika sumber daya terlibat dalam temuan Keparahan Tinggi dalam 24 jam terakhir.
            - Jika sumber daya terlibat dalam kelompok temuan yang diamati dalam 7 hari terakhir. Kelompok pencari Detektif memungkinkan Anda memeriksa beberapa aktivitas yang terkait dengan peristiwa keamanan potensial. Untuk detail selengkapnya, lihat the section called “Menemukan grup”.
            - Jika sumber daya terlibat dalam temuan dalam 7 hari terakhir.
        - Temuan terbaru — Temuan terbaru diprioritaskan di atas daftar.
        - Jenis sumber daya - Mengidentifikasi jenis sumber daya. Misalnya, AWS pengguna atau AWS peran.
    2. `Specify an AWS role or user with an ARN`— Anda dapat memilih AWS peran atau AWS pengguna dan menjalankan penyelidikan untuk sumber daya tertentu.

Ikuti langkah-langkah ini untuk menyelidiki jenis sumber daya tertentu.

a. Dari daftar drop-down Pilih jenis sumber daya, pilih AWS peran atau AWS pengguna.

b. Masukkan ARN Sumber Daya dari sumber daya IAM. Untuk detail selengkapnya tentang ARN Sumber Daya, lihat Nama Sumber Daya Amazon (ARN) di Panduan Pengguna IAM.

3. `Find a resource to investigate from the Search page`— Anda dapat mencari semua sumber daya IAM Anda dari halaman Pencarian Detektif.

   Ikuti langkah-langkah ini untuk menyelidiki sumber daya dari halaman Penelusuran.

   a. Di panel navigasi, pilih Cari.

   b. Di halaman Pencarian, cari sumber daya IAM.

   c. Arahkan ke halaman profil sumber daya dan jalankan penyelidikan dari sana.

5. Di bagian Waktu lingkup investigasi, pilih Waktu lingkup investigasi untuk menilai aktivitas sumber daya yang dipilih. Anda dapat memilih Tanggal mulai dan waktu mulai; dan Tanggal akhir dan Waktu akhir dalam format UTC. Jendela waktu lingkup yang dipilih dapat antara minimal 3 jam dan maksimal 30 hari.
6. Pilih Jalankan investigasi.

API

Untuk menjalankan investigasi secara terprogram, gunakan StartInvestigationpengoperasian Detective API. Jika Anda menggunakan AWS Command Line Interface (AWS CLI) jalankan perintah start-investigation.

Dalam permintaan Anda, gunakan parameter ini untuk menjalankan investigasi di Detective:

- `GraphArn`— Tentukan Nama Sumber Daya Amazon (ARN) dari grafik perilaku.
- `EntityArn`— Tentukan Nama Sumber Daya Amazon (ARN) unik dari pengguna IAM dan peran IAM.
- `ScopeStartTime`— Secara opsional, tentukan data dan waktu dari mana penyelidikan harus dimulai. Nilainya adalah string berformat UTC ISO8601. Misalnya, `2021-08-18T16:35:56.284Z`.
- `ScopeEndTime`— Secara opsional, tentukan data dan waktu kapan investigasi harus berakhir. Nilainya adalah string berformat UTC ISO8601. Misalnya, `2021-08-18T16:35:56.284Z`.

Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
aws detective start-investigation \
--graph-arn arn:aws:detective:us-
east-1:123456789123:graph:fdac8011456e4e6182facb26dfceade0
 --entity-arn arn:aws:iam::123456789123:role/rolename --scope-start-
time 2023-09-27T20:00:00.00Z
--scope-end-time 2023-09-28T22:00:00.00Z
```

Anda juga dapat menjalankan investigasi dari halaman-halaman berikut di Detective:

- Halaman profil peran pengguna IAM atau IAM di Detective.
- Panel visualisasi grafik dari grup pencari.
- Kolom tindakan dari sumber daya yang terlibat.
- Pengguna IAM atau peran IAM pada halaman pencarian.

Setelah Detective menjalankan penyelidikan untuk sumber daya, laporan investigasi dihasilkan. Untuk mengakses laporan, buka Investigasi dari panel navigasi.

Meninjau laporan investigasi

Laporan investigasi memungkinkan Anda meninjau Laporan yang dihasilkan untuk investigasi yang telah Anda jalankan sebelumnya di Detective.

Untuk meninjau laporan investigasi

1. Masuk ke Konsol AWS Manajemen. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Investigasi.

Perhatikan atribut berikut dari laporan investigasi.

- ID — Pengenal yang dihasilkan dari laporan investigasi. Anda dapat memilih ID ini untuk membaca ringkasan laporan investigasi, yang memiliki rincian investigasi.
- Status — Setiap investigasi dikaitkan dengan Status berdasarkan status penyelesaian investigasi. Nilai status bisa Dalam proses, Berhasil, atau Gagal.

- Keparahan — Setiap investigasi diberi Keparahan. Detektif secara otomatis memberikan tingkat keparahan pada temuan tersebut.

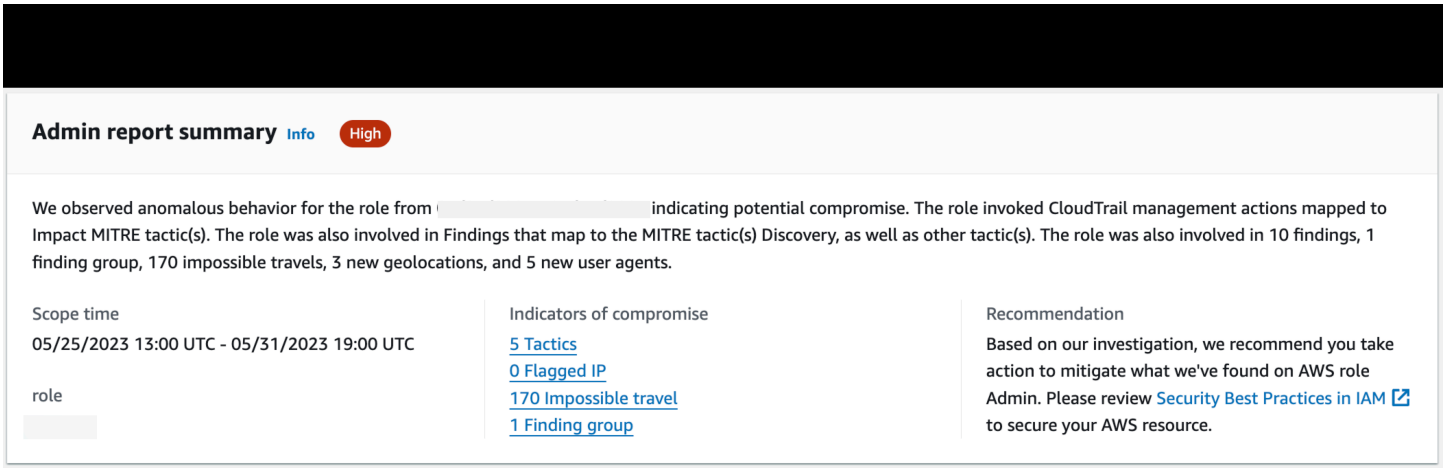
  Tingkat keparahan mewakili disposisi sebagaimana dianalisis oleh penyelidikan sumber daya tunggal pada waktu lingkup tertentu. Tingkat keparahan yang dilaporkan oleh investigasi tidak menyiratkan atau menunjukkan kekritisan atau pentingnya sumber daya yang terkena dampak bagi organisasi Anda.

  Nilai tingkat keparahan investigasi dapat Kritis, Tinggi, Sedang, Rendah, atau Informasi dari yang paling parah hingga yang paling tidak parah.

  Investigasi yang diberi nilai tingkat keparahan kritis atau tinggi harus diprioritaskan untuk pemeriksaan lebih lanjut, karena lebih cenderung mewakili masalah keamanan berdampak tinggi yang diidentifikasi oleh Detektif.
- Entitas - Kolom Entitas berisi rincian tentang entitas spesifik yang terdeteksi dalam penyelidikan. Beberapa entitas adalah AWS akun, seperti pengguna dan peran.
- Status - Kolom Tanggal Pembuatan berisi rincian tentang tanggal dan waktu laporan investigasi pertama kali dibuat.

Memahami laporan Investigasi Detektif

Laporan Detective Investigations mencantumkan ringkasan perilaku yang tidak biasa atau aktivitas jahat yang menunjukkan kompromi. Ini juga mencantumkan rekomendasi yang disarankan Detective untuk mengurangi risiko keamanan.



Untuk melihat laporan investigasi untuk ID investigasi tertentu.

1. Masuk ke Konsol AWS Manajemen. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Investigasi.
3. Pada tabel Laporan, pilih ID investigasi.

Detective menghasilkan laporan untuk waktu Lingkup dan Pengguna yang dipilih. Laporan ini berisi bagian Indikator Kompromi yang mencakup rincian mengenai satu atau lebih indikator kompromi yang tercantum di bawah ini. Saat Anda meninjau setiap indikator kompromi, secara opsional pilih item untuk ditelusuri dan tinjau detailnya.

- Taktik. Teknik, dan Prosedur — Mengidentifikasi taktik, teknik, dan prosedur (TTP) yang digunakan dalam peristiwa keamanan potensial. Kerangka MITRE ATT&CK digunakan untuk memahami TTP. Taktik didasarkan pada matriks MITRE ATT&CK untuk Enterprise.
- Alamat IP Bertanda Kecerdasan Ancaman — Alamat IP yang mencurigakan ditandai dan diidentifikasi sebagai ancaman kritis atau berat berdasarkan intelijen ancaman Detektif.
- Impossible Travel — Mendeteksi dan mengidentifikasi aktivitas pengguna yang tidak biasa dan tidak mungkin untuk sebuah akun. Misalnya, indikator ini mencantumkan perubahan drastis antara sumber ke lokasi tujuan pengguna dalam rentang waktu yang singkat.
- Related Finding Group — Menampilkan beberapa aktivitas yang berhubungan dengan peristiwa keamanan potensial. Detective menggunakan teknik analisis grafik yang menyimpulkan hubungan antara temuan dan entitas, dan mengelompokkannya bersama-sama sebagai kelompok pencari.
- Temuan Terkait — Kegiatan terkait yang terkait dengan peristiwa keamanan potensial. Daftar semua kategori bukti yang berbeda yang terhubung ke sumber daya atau kelompok temuan.
- Geolokasi Baru - Mengidentifikasi geolokasi baru yang digunakan baik di tingkat sumber daya atau akun. Misalnya, indikator ini mencantumkan geolokasi yang diamati yang merupakan lokasi yang jarang atau tidak digunakan berdasarkan aktivitas pengguna sebelumnya.
- Agen Pengguna Baru — Mengidentifikasi agen pengguna baru yang digunakan baik di tingkat sumber daya atau akun.
- New ASOS — Mengidentifikasi Autonomous System Organizations (ASO) baru yang digunakan baik di tingkat sumber daya atau akun. Misalnya, indikator ini mencantumkan organisasi baru yang ditetapkan sebagai ASO.

Ringkasan laporan investigasi

Ringkasan investigasi menyoroti indikator anomali yang memerlukan perhatian, untuk waktu lingkup yang dipilih. Dengan menggunakan ringkasan, Anda dapat lebih cepat mengidentifikasi akar penyebab masalah keamanan potensial, mengidentifikasi pola, dan memahami sumber daya yang terkena dampak peristiwa keamanan.

Dalam ringkasan laporan investigasi terperinci, Anda dapat melihat detail berikut.

Ikhtisar investigasi

Di panel Ikhtisar, Anda dapat melihat visualisasi IP dengan aktivitas tingkat keparahan tinggi, yang dapat memberikan lebih banyak konteks pada jalur penyerang.

Detektif menyoroti Aktivitas yang tidak biasa dalam penyelidikan, misalnya perjalanan yang tidak mungkin dari sumber ke tujuan yang jauh oleh pengguna IAM.

Detective memetakan investigasi ke taktik, teknik, dan prosedur (TTP) yang digunakan dalam peristiwa keamanan potensial. Kerangka MITRE ATT&CK digunakan untuk memahami TTP. Taktik didasarkan pada matriks MITRE ATT&CK untuk Enterprise.

Indikator investigasi

Anda dapat menggunakan informasi di panel Indikator, untuk menentukan apakah AWS sumber daya terlibat dalam aktivitas tidak biasa yang dapat menunjukkan perilaku jahat dan dampaknya. Indikator penyusupan (IOC) adalah artefak yang diamati di dalam atau pada jaringan, sistem, atau lingkungan yang dapat (dengan tingkat kepercayaan tinggi) mengidentifikasi aktivitas berbahaya atau insiden keamanan.

Mengunduh laporan investigasi

Anda dapat mengunduh laporan Detective Investigations dalam format JSON, untuk menganalisisnya lebih lanjut atau menyimpannya ke solusi penyimpanan pilihan Anda seperti bucket Amazon S3.

Untuk mengunduh laporan investigasi dari tabel Laporan.

1. Masuk ke Konsol AWS Manajemen. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Investigasi.
3. Pilih investigasi, dari tabel Laporan, dan pilih Unduh.

Untuk mengunduh laporan investigasi dari halaman ringkasan.

1. Masuk ke Konsol AWS Manajemen. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Investigasi.
3. Pilih investigasi, dari tabel Laporan.
4. Di halaman ringkasan investigasi, pilih Unduh.

Mengarsipkan laporan investigasi

Ketika Anda menyelesaikan penyelidikan Anda di Detektif Amazon, Anda dapat Mengarsipkan laporan investigasi. Investigasi yang diarsipkan menunjukkan bahwa Anda telah menyelesaikan peninjauan investigasi.

Anda dapat mengarsipkan atau membatalkan arsip penyelidikan hanya jika Anda seorang Administrator Detektif. Detective akan menyimpan investigasi arsip Anda selama 90 hari.

Untuk mengarsipkan laporan investigasi dari tabel Laporan.

1. Masuk ke Konsol AWS Manajemen. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Investigasi.
3. Pilih investigasi, dari tabel Laporan, dan pilih Arsip.

Untuk mengarsipkan laporan investigasi dari halaman ringkasan.

1. Masuk ke Konsol AWS Manajemen. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Investigasi.
3. Pilih investigasi, dari tabel Laporan.
4. Di halaman ringkasan investigasi, pilih Arsip.

Fase investigasi dan titik awal

Amazon Detective menyediakan alat untuk mendukung proses investigasi secara keseluruhan. Investigasi di Detektif dapat dimulai dari temuan, kelompok pencari, atau entitas.

Fase investigasi

Setiap proses investigasi melibatkan fase-fase berikut:

Triase

Proses investigasi dimulai ketika Anda diberi tahu tentang dugaan kejadian berbahaya atau berisiko tinggi. Misalnya, Anda ditugaskan untuk melihat temuan atau peringatan yang ditemukan oleh layanan seperti Amazon GuardDuty dan Amazon Inspector.

Pada fase triase, Anda menentukan apakah Anda yakin aktivitas tersebut benar-benar positif (aktivitas jahat asli) atau positif palsu (bukan aktivitas berbahaya atau berisiko tinggi). Profil Detektif mendukung proses triase dengan memberikan wawasan tentang aktivitas untuk entitas yang terlibat.

Untuk contoh positif sejati, Anda melanjutkan ke fase berikutnya.

Pelingkupan

Selama fase pelingkupan, analis menentukan sejauh mana aktivitas berbahaya atau berisiko tinggi dan penyebab yang mendasarinya.

Pelingkupan menjawab jenis pertanyaan berikut:

- Sistem dan pengguna apa yang dikompromikan?
- Dari mana serangan itu berasal?
- Sudah berapa lama serangan itu terjadi?
- Apakah ada kegiatan terkait lainnya untuk diungkap? Misalnya, jika penyerang mengekstraksi data dari sistem Anda, bagaimana mereka mendapatkannya?

Visualisasi detektif dapat membantu Anda mengidentifikasi entitas lain yang terlibat atau terpengaruh.

Respons

Langkah terakhir adalah menanggapi serangan untuk menghentikan serangan, meminimalkan kerusakan, dan mencegah serangan serupa terjadi lagi.

Titik awal untuk Investigasi Detektif

Setiap investigasi di Detective memiliki titik awal yang penting. Misalnya, Anda mungkin diberi Amazon GuardDuty atau AWS Security Hub temuan untuk diselidiki. Atau Anda mungkin memiliki kekhawatiran tentang aktivitas yang tidak biasa untuk alamat IP tertentu.

Titik awal yang khas untuk penyelidikan termasuk temuan yang terdeteksi oleh GuardDuty dan entitas yang diekstraksi dari data sumber Detektif.

Temuan yang terdeteksi oleh GuardDuty

GuardDuty menggunakan data log Anda untuk mengungkap dugaan kejadian berbahaya atau berisiko tinggi. Detective menyediakan sumber daya yang membantu Anda menyelidiki temuan ini.

Untuk setiap temuan, Detective memberikan rincian temuan terkait. Detective juga menunjukkan entitas, seperti alamat IP dan AWS akun, yang terhubung ke temuan.

Anda kemudian dapat menjelajahi aktivitas untuk entitas yang terlibat untuk menentukan apakah aktivitas yang terdeteksi dari temuan tersebut merupakan penyebab asli yang perlu dikhawatirkan.

Untuk informasi selengkapnya, lihat the section called “Menemukan ikhtisar”.

AWS Temuan keamanan dikumpulkan oleh Security Hub

AWS Security Hub mengumpulkan temuan keamanan dari berbagai penyedia temuan di satu tempat, dan memberi Anda pandangan komprehensif tentang status keamanan Anda di AWS. Security Hub menghilangkan kompleksitas dalam menangani sejumlah besar temuan dari beberapa penyedia. Ini mengurangi upaya yang diperlukan untuk mengelola dan meningkatkan keamanan semua AWS akun, sumber daya, dan beban kerja Anda. Detective menyediakan sumber daya yang membantu Anda menyelidiki temuan ini.

Untuk setiap temuan, Detective memberikan rincian temuan terkait. Detective juga menunjukkan entitas, seperti alamat IP dan AWS akun, yang terhubung ke temuan.

Untuk informasi selengkapnya, lihat the section called “Menemukan ikhtisar”.

Entitas yang diambil dari data sumber Detektif

Dari data sumber Detective yang dicerna, Detective mengekstrak entitas seperti alamat IP dan pengguna. AWS Anda dapat menggunakan salah satunya sebagai titik awal investigasi.

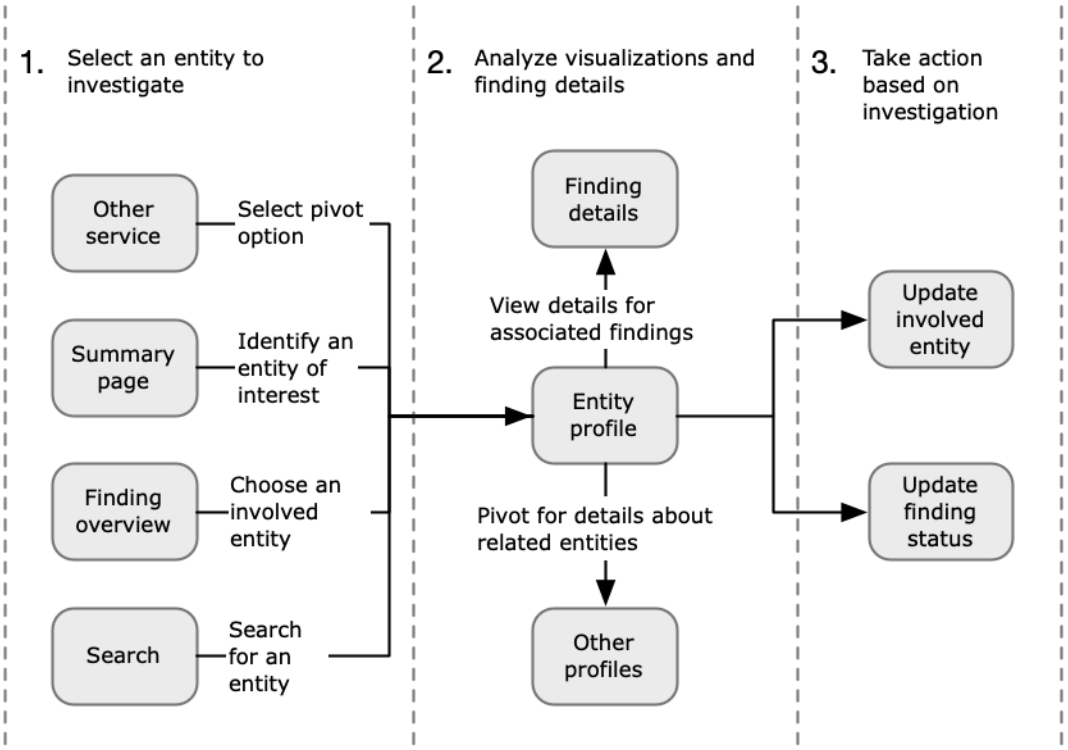
Detective memberikan rincian umum tentang entitas, seperti alamat IP atau nama pengguna. Ini juga memberikan rincian tentang riwayat aktivitas. Misalnya, Detektif dapat melaporkan alamat IP lain yang telah terhubung, terhubung, atau digunakan oleh entitas.

Untuk informasi selengkapnya, lihat Menganalisis entitas.

Alur Investigasi Detektif Amazon

Anda dapat menggunakan Amazon Detective untuk menyelidiki entitas seperti instans EC2 atau pengguna. AWS Anda juga dapat menyelidiki temuan keamanan.

Pada tingkat tinggi, gambar berikut menunjukkan proses untuk Investigasi Detektif.



Langkah 1: Pilih entitas yang akan diselidiki

Ketika melihat temuan di GuardDuty, analis dapat memilih untuk menyelidiki entitas terkait di Detective. Lihat the section called “Berputar dari konsol lain”.

Memilih entitas akan membawa Anda ke profil entitas di Detektif.

Langkah 2: Analisis visualisasi pada profil

Setiap profil entitas berisi serangkaian visualisasi yang dihasilkan dari grafik perilaku. Grafik perilaku dibuat dari file log dan data lain yang dimasukkan ke Detective.

Visualisasi menunjukkan aktivitas yang terkait dengan suatu entitas. Anda menggunakan visualisasi ini untuk menjawab pertanyaan guna menentukan apakah aktivitas entitas tidak biasa. Lihat Menganalisis entitas.

Untuk membantu memandu penyelidikan, Anda dapat menggunakan panduan Detektif yang disediakan untuk setiap visualisasi. Panduan menguraikan informasi yang ditampilkan, menyarankan pertanyaan untuk Anda tanyakan, dan mengusulkan langkah selanjutnya berdasarkan jawaban. Lihat the section called “Menggunakan panduan panel profil”.

Setiap profil berisi daftar temuan terkait. Anda dapat melihat detail untuk temuan, dan melihat ikhtisar temuan. Lihat the section called “Melihat temuan untuk suatu entitas”.

Dari profil entitas, Anda dapat beralih ke entitas lain dan menemukan profil, untuk menyelidiki lebih lanjut aktivitas aset terkait.

Langkah 3: Ambil tindakan

Berdasarkan hasil investigasi Anda, ambil tindakan yang sesuai.

Untuk temuan yang positif palsu, Anda dapat mengarsipkan temuan tersebut. Dari Detektif, Anda dapat mengarsipkan GuardDuty temuan. Lihat the section called “Mengarsipkan temuan GuardDuty ”.

Jika tidak, Anda mengambil tindakan yang tepat untuk mengatasi kerentanan dan mengurangi kerusakan. Misalnya, Anda mungkin perlu memperbarui konfigurasi sumber daya.

Menganalisis temuan di Amazon Detective

Temuan adalah contoh aktivitas yang berpotensi berbahaya atau risiko lain yang terdeteksi. Amazon GuardDuty dan temuan AWS keamanan dimuat ke Detektif Amazon sehingga Anda dapat menggunakan Detektif untuk menyelidiki aktivitas yang terkait dengan entitas yang terlibat. GuardDuty Temuan adalah bagian dari paket inti Detektif dan dicerna secara default. Semua temuan AWS keamanan lainnya yang dikumpulkan oleh Security Hub dicerna sebagai sumber data opsional. Lihat Sumber data yang digunakan dalam grafik perilaku untuk detail selengkapnya.

Ikhtisar temuan Detektif memberikan informasi rinci tentang temuan tersebut. Ini juga menampilkan ringkasan entitas yang terlibat, dengan tautan ke profil entitas terkait.

Jika temuan berkorelasi dengan aktivitas yang lebih besar, Detektif memberi tahu Anda untuk Pergi ke grup pencarian. Sebaiknya gunakan grup pencarian untuk melanjutkan penyelidikan Anda, karena grup pencarian memungkinkan Anda memeriksa beberapa aktivitas yang terkait dengan peristiwa keamanan potensial. Lihat the section called “Menemukan grup”.

Konten

Menganalisis ikhtisar temuan

Ikhtisar temuan Detektif memberikan informasi rinci tentang temuan tersebut. Ini juga menampilkan ringkasan entitas yang terlibat, dengan tautan ke profil entitas terkait.

Lingkup waktu yang digunakan untuk ikhtisar temuan

Waktu lingkup untuk ikhtisar temuan diatur ke jendela waktu pencarian. Jendela waktu penemuan mencerminkan pertama dan terakhir kali aktivitas temuan diamati.

Detail temuan

Panel di sebelah kanan berisi detail untuk temuan tersebut. Ini adalah detail yang diberikan oleh penyedia temuan.

Dari detail temuan, Anda juga dapat mengarsipkan temuan. Lihat the section called “Mengarsipkan temuan GuardDuty ”.

Entitas terkait

Ikhtisar temuan berisi daftar entitas yang terlibat dalam temuan. Untuk setiap entitas, daftar memberikan informasi ikhtisar tentang entitas. Informasi ini mencerminkan informasi pada panel profil detail entitas pada profil entitas terkait.

Anda dapat memfilter daftar berdasarkan jenis entitas. Anda juga dapat memfilter daftar berdasarkan teks di pengenal entitas.

Untuk berputar ke profil entitas, pilih Lihat profil. Saat Anda berpivot ke profil entitas, hal berikut terjadi:

- Waktu lingkup diatur ke jendela waktu pencarian.
- Pada panel temuan terkait untuk entitas, temuan dipilih. Detail temuan tetap ditampilkan di sebelah kanan profil entitas.

Pemecahan Masalah 'Halaman tidak ditemukan'

Saat Anda menavigasi ke entitas atau temuan di Detektif, Anda mungkin melihat pesan galat Halaman tidak ditemukan.

Untuk mengatasinya, lakukan salah satu hal berikut:

- Pastikan bahwa entitas atau temuan milik salah satu akun anggota Anda. Untuk informasi tentang cara meninjau akun anggota, lihat Melihat daftar akun.
- Pastikan akun administrator Anda selaras dengan GuardDuty dan/atau Security Hub untuk berpivot ke Detective dari layanan ini. Untuk rekomendasinya, lihat Penyelarasan yang disarankan dengan GuardDuty dan Security Hub.
- Verifikasi bahwa temuan terjadi setelah akun anggota menerima undangan Anda.
- Verifikasi grafik perilaku Detektif menelan data dari paket sumber data opsional. Untuk informasi selengkapnya tentang data sumber yang digunakan dalam grafik perilaku Detektif, lihat Data sumber yang digunakan dalam grafik perilaku.

- Untuk memungkinkan Detective menyerap data dari Security Hub dan menambahkan data tersebut ke grafik perilaku Anda, Anda harus mengaktifkan Detective for AWS security finding sebagai paket sumber data. Untuk informasi lebih lanjut, lihat temuan AWS keamanan.

- Jika Anda menavigasi ke profil entitas atau menemukan ikhtisar di Detective, pastikan URL dalam format yang benar. Untuk detail tentang pembentukan URL profil, lihat Menavigasi ke profil entitas atau menemukan ikhtisar menggunakan URL.

Menganalisis kelompok temuan

Grup pencari Detektif Amazon memungkinkan Anda memeriksa beberapa aktivitas yang terkait dengan peristiwa keamanan potensial. Anda dapat menganalisis akar penyebab GuardDuty temuan tingkat keparahan tinggi menggunakan kelompok temuan. Jika pelaku ancaman mencoba membahayakan AWS lingkungan Anda, mereka biasanya melakukan serangkaian tindakan yang mengarah pada beberapa temuan keamanan dan perilaku yang tidak biasa. Tindakan ini sering tersebar di seluruh waktu dan entitas. Ketika temuan keamanan diselidiki secara terpisah, itu dapat menyebabkan salah tafsir signifikansi mereka, dan kesulitan dalam menemukan akar penyebabnya. Amazon Detective mengatasi masalah ini dengan menerapkan teknik analisis grafik yang menyimpulkan hubungan antara temuan dan entitas, dan mengelompokkannya bersama-sama. Kami merekomendasikan memperlakukan kelompok pencari sebagai titik awal untuk menyelidiki entitas dan temuan yang terlibat.

Detective menganalisis data dari temuan dan mengelompokkannya dengan temuan lain yang mungkin terkait berdasarkan sumber daya yang mereka bagikan. Misalnya, temuan yang terkait dengan tindakan yang diambil oleh sesi peran IAM yang sama atau berasal dari alamat IP yang sama sangat mungkin menjadi bagian dari aktivitas dasar yang sama. Sangat berharga untuk menyelidiki temuan dan bukti sebagai sebuah kelompok, bahkan jika asosiasi yang dibuat oleh Detektif tidak terkait.

Selain temuan, setiap kelompok mencakup entitas yang terlibat dalam temuan. Entitas dapat menyertakan sumber daya di luar AWS seperti Alamat IP atau agen pengguna.

> **Note**
>
> Setelah GuardDuty temuan awal terjadi yang terkait dengan temuan lain, kelompok temuan dengan semua temuan terkait dan semua entitas yang terlibat dibuat dalam waktu 48 jam.

Memahami halaman grup temuan

Halaman grup temuan mencantumkan semua grup temuan yang dikumpulkan oleh Amazon Detective dari grafik perilaku Anda. perhatikan atribut berikut dari grup pencarian:

Tingkat keparahan suatu kelompok

Setiap kelompok temuan diberi tingkat keparahan berdasarkan tingkat keparahan AWS Security Finding Format (ASFF) dari temuan terkait. Nilai keparahan temuan ASFF adalah Kritis, Tinggi, Sedang, Rendah, atau Informasi dari yang paling parah hingga yang paling tidak parah. Tingkat keparahan pengelompokan sama dengan temuan tingkat keparahan tertinggi di antara temuan dalam pengelompokan itu.

Kelompok yang terdiri dari temuan kritis atau tingkat keparahan tinggi yang berdampak pada sejumlah besar entitas harus diprioritaskan untuk penyelidikan, karena mereka lebih cenderung mewakili masalah keamanan berdampak tinggi.

Judul grup

Di kolom Judul, setiap grup memiliki ID unik dan judul yang tidak unik. Ini didasarkan pada namespace tipe ASFF untuk grup dan jumlah temuan dalam namespace tersebut di cluster. Misalnya, jika pengelompokan memiliki judul: Kelompokkan dengan: TTP (2), Efek (1), dan Perilaku yang tidak biasa (2) itu mencakup lima temuan total yang terdiri dari dua temuan di namespace TTP, satu temuan di Namespace Efek, dan dua temuan di namespace Perilaku Tidak Biasa. Untuk daftar lengkap ruang nama, lihat Jenis taksonomi untuk ASFF.

Taktik dalam kelompok

Kolom Taktik dalam kelompok merinci kategori taktik mana yang termasuk dalam aktivitas tersebut. Kategori taktik, teknik, dan prosedur dalam daftar berikut selaras dengan matriks MITRE ATT&CK.

Anda dapat memilih taktik pada rantai untuk melihat deskripsi taktik dan temuan mana dalam kelompok yang termasuk dalam kategori itu. Mengikuti rantai adalah daftar taktik yang terdeteksi dalam kelompok. Kategori-kategori ini dan kegiatan yang biasanya mereka wakili adalah sebagai berikut:

- Akses Awal — Musuh mencoba masuk ke jaringan orang lain.
- Eksekusi — Musuh mencoba masuk ke jaringan orang lain.
- Kegigihan — Musuh berusaha mempertahankan pijakan mereka.
- Eskalasi Hak Istimewa — Musuh mencoba mendapatkan izin tingkat yang lebih tinggi.

- Penghindaran Pertahanan — Musuh berusaha menghindari terdeteksi.
- Akses Kredenal — Musuh mencoba mencuri nama akun dan kata sandi.
- Penemuan — Musuh sedang mencoba memahami dan belajar tentang suatu lingkungan.
- Gerakan Lateral — Musuh sedang mencoba untuk bergerak melalui lingkungan.
- Koleksi — Musuh mencoba mengumpulkan data yang menarik untuk tujuan mereka.
- Command and Control — Musuh sedang mencoba masuk ke jaringan orang lain.
- Eksfiltrasi — Musuh mencoba mencuri data.
- Dampak — Musuh mencoba memanipulasi, mengganggu, atau menghancurkan sistem dan data Anda.
- Lainnya — Menunjukkan aktivitas dari temuan yang tidak selaras dengan taktik yang tercantum dalam matriks.

Entitas dalam grup

Kolom Entitas berisi rincian tentang entitas tertentu yang terdeteksi dalam pengelompokan ini. Pilih nilai ini untuk rincian entitas berdasarkan kategori: Identity, Network, Storage, dan Compute. Contoh entitas dalam setiap kategori adalah:

- Identitas — Prinsipal IAM dan Akun AWS, seperti pengguna dan peran
- Jaringan — Alamat IP atau entitas jaringan dan VPC lainnya
- Penyimpanan - Ember Amazon S3 atau DDB
- Hitung instans Amazon EC2 atau container Kubernetes

Akun dalam grup

Kolom Akun memberi tahu Anda entitas AWS akun apa yang terlibat dengan temuan dalam grup. AWS Akun dicantumkan berdasarkan nama dan AWS ID sehingga Anda dapat memprioritaskan investigasi aktivitas yang melibatkan akun penting.

Temuan dalam kelompok

Kolom Temuan memiliki daftar entitas dalam grup berdasarkan tingkat keparahan. Temuan ini meliputi GuardDuty temuan Amazon, temuan Amazon Inspector, temuan AWS keamanan, dan bukti dari Detective. Anda dapat memilih grafik untuk melihat jumlah temuan yang tepat berdasarkan tingkat keparahan.

GuardDuty Temuan adalah bagian dari paket inti Detektif dan dicerna secara default. Semua temuan AWS keamanan lainnya yang dikumpulkan oleh Security Hub dicerna sebagai

sumber data opsional. Lihat Sumber data yang digunakan dalam grafik perilaku untuk detail selengkapnya.

Temuan informasi dalam menemukan kelompok

Amazon Detective mengidentifikasi informasi tambahan yang terkait dengan grup pencari berdasarkan data dalam grafik perilaku Anda yang dikumpulkan dalam 45 hari terakhir. Detektif menyajikan informasi ini sebagai temuan dengan tingkat keparahan informasi. Bukti memberikan informasi pendukung yang menyoroti aktivitas yang tidak biasa atau perilaku yang tidak diketahui yang berpotensi mencurigakan ketika dilihat dalam kelompok temuan. Ini mungkin termasuk geolokasi yang baru diamati atau panggilan API yang diamati dalam lingkup waktu temuan. Temuan bukti hanya dapat dilihat di Detektif dan tidak dikirim ke. AWS Security Hub

Detektif menentukan lokasi permintaan menggunakan database GeoIP MaxMind . MaxMind melaporkan akurasi data mereka yang sangat tinggi di tingkat negara, meskipun akurasi bervariasi sesuai dengan faktor-faktor seperti negara dan jenis IP. Untuk informasi selengkapnya MaxMind, lihat Geolokasi MaxMind IP. Jika menurut Anda salah satu data GeoIP salah, Anda dapat mengirimkan permintaan koreksi ke Maxmind di Data GeoIP2 MaxMind yang Benar.

Anda dapat mengamati bukti untuk jenis utama yang berbeda (seperti pengguna IAM atau peran IAM). Untuk beberapa jenis bukti, Anda dapat mengamati bukti untuk semua akun. Ini berarti bukti memengaruhi seluruh grafik perilaku Anda. Jika temuan bukti diamati untuk semua akun, Anda juga akan melihat setidaknya satu temuan bukti informasi tambahan dari jenis yang sama untuk peran IAM individu. Misalnya, jika Anda melihat geolokasi baru diamati untuk semua temuan akun, Anda akan melihat yang lain untuk Geolokasi baru yang diamati untuk prinsipal.

Jenis bukti dalam menemukan kelompok

- Geolokasi baru diamati
- Organisasi Sistem Otonomi Baru (ASO) diamati
- Agen pengguna baru diamati
- Panggilan API baru dikeluarkan
- Geolokasi baru diamati untuk semua akun
- Prinsipal IAM baru diamati untuk semua akun

Menemukan profil grup

Saat Anda memilih judul grup, profil grup pencarian akan terbuka dengan detail tambahan tentang grup tersebut. Panel detail di halaman profil grup pencarian mendukung tampilan hingga 1000 entitas dan temuan untuk menemukan kelompok orang tua dan anak.

Halaman profil grup menampilkan waktu Lingkup yang ditetapkan grup. Ini adalah tanggal dan waktu dari temuan atau bukti paling awal yang termasuk dalam kelompok hingga temuan atau bukti terbaru dalam suatu kelompok. Anda juga dapat melihat tingkat keparahan kelompok Finding, yang sama dengan kategori tingkat keparahan tertinggi di antara temuan dalam kelompok. Rincian lain dalam panel profil ini meliputi:

- Rantai taktik Terlibat menunjukkan kepada Anda taktik mana, yang dikaitkan dengan temuan dalam kelompok. Taktik didasarkan pada MITRE ATT&CK Matrix for Enterprise. Taktik ditampilkan sebagai rantai titik-titik berwarna yang mewakili perkembangan khas serangan dari tahap awal hingga tahap terbaru. Ini berarti lingkaran paling kiri pada rantai biasanya mewakili aktivitas yang tidak terlalu parah di mana musuh mencoba untuk mendapatkan atau mempertahankan akses lingkungan Anda. Sebaliknya, kegiatan ke arah kanan adalah yang paling parah dan dapat mencakup gangguan atau penghancuran data.
- Hubungan yang dimiliki kelompok ini dengan kelompok lain. Kadang-kadang, satu atau lebih kelompok temuan yang sebelumnya tidak terhubung dapat digabungkan ke dalam kelompok baru berdasarkan tautan yang baru ditemukan, misalnya, temuan yang melibatkan entitas dari kelompok yang ada. Dalam hal ini, Amazon Detective menonaktifkan grup induk dan membuat grup anak. Anda dapat melacak garis keturunan untuk grup apa pun kembali ke grup induknya. Grup dapat memiliki hubungan berikut:
  - Kelompok pencari anak — Kelompok pencari yang dibuat ketika sebuah temuan yang terlibat dalam dua kelompok temuan lain terlibat dalam temuan baru. Kelompok induk dari temuan ini terdaftar untuk kelompok anak mana pun.
  - Grup pencarian orang tua — Grup pencari adalah orang tua ketika grup anak telah dibuat darinya. Jika kelompok pencari adalah orang tua, anak-anak terkait terdaftar dengannya. Status grup induk menjadi Tidak Aktif saat digabungkan menjadi grup anak Aktif.

Ada dua tab informasi yang membuka panel profil. Dengan menggunakan tab Entitas yang terlibat dan temuan Terlibat, Anda dapat melihat detail lebih lanjut tentang grup.

Gunakan investigasi Jalankan untuk menghasilkan laporan investigasi. Laporan yang dihasilkan merinci perilaku anomali yang menunjukkan kompromi.

Panel profil dalam kelompok

Entitas yang terlibat

Berfokus pada entitas dalam kelompok pencari, termasuk temuan apa dalam kelompok yang terkait dengan setiap entitas. Tag yang dilampirkan ke setiap entitas juga ditampilkan sehingga Anda dapat dengan cepat mengidentifikasi entitas penting berdasarkan penandaan. Pilih entitas untuk melihat profil entitasnya.

Temuan yang terlibat

Memiliki rincian tentang setiap temuan, termasuk menemukan tingkat keparahan, setiap entitas yang terlibat, dan kapan temuan itu pertama dan terakhir terlihat. Pilih jenis temuan dalam daftar untuk membuka panel rincian temuan dengan informasi tambahan tentang temuan itu. Sebagai bagian dari panel temuan Terlibat, Anda mungkin melihat temuan Informasi berdasarkan bukti Detektif dari grafik perilaku Anda.

Menemukan visualisasi grup

Amazon Detective menyediakan visualisasi interaktif untuk menemukan kelompok. Visualisasi ini dirancang untuk membantu Anda menyelidiki masalah lebih cepat dan lebih menyeluruh dengan sedikit usaha. Panel Visualisasi grup temuan menampilkan temuan dan entitas yang terlibat dalam kelompok temuan. Anda dapat menggunakan visualisasi interaktif ini untuk menganalisis, memahami, dan melakukan triase dampak dari kelompok pencari. Panel ini membantu memvisualisasikan informasi yang disajikan dalam entitas Terlibat dan tabel temuan Terlibat. Dari presentasi visual, Anda dapat memilih temuan atau entitas untuk analisis lebih lanjut.

Kelompok temuan Detektif dengan temuan agregat adalah sekelompok temuan yang terhubung ke jenis sumber daya yang sama. Dengan temuan agregat, Anda dapat dengan cepat menilai susunan kelompok pencari dan menafsirkan masalah keamanan lebih cepat. Dalam panel rincian kelompok temuan, temuan serupa digabungkan dan Anda dapat memperluas temuan untuk melihat temuan yang relatif mirip bersama-sama. Misalnya, simpul bukti, yang memiliki temuan informasi dan temuan media dari jenis yang sama dikumpulkan. Saat ini, Anda dapat melihat judul, sumber, jenis, dan tingkat keparahan grup pencarian dengan temuan agregat.

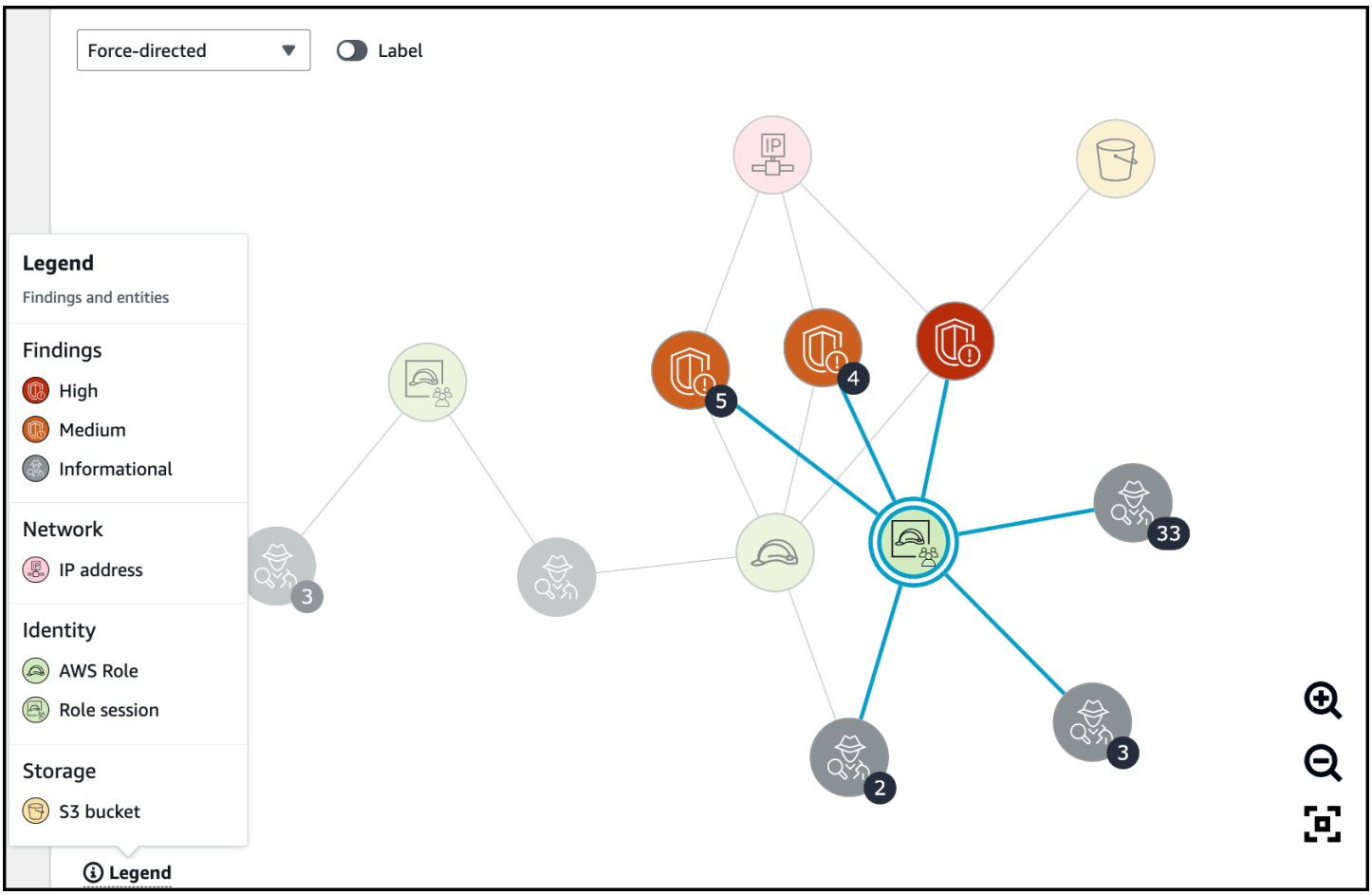
Dari panel interaktif ini, Anda dapat:

- Gunakan investigasi Jalankan untuk menghasilkan laporan investigasi. Laporan yang dihasilkan merinci perilaku anomali yang menunjukkan kompromi.

- Lihat detail lebih lanjut tentang menemukan kelompok dengan temuan agregat untuk menganalisis bukti, entitas, dan temuan yang terlibat.
- Lihat label untuk entitas dan temuan untuk mengidentifikasi entitas yang terkena dampak dengan potensi masalah keamanan. Anda dapat mematikan Label.
- Atur ulang entitas dan temuan untuk lebih memahami keterkaitan mereka. Isolasi entitas dan temuan dari grup dengan memindahkan item yang dipilih dalam grup temuan.
- Pilih bukti, entitas, dan temuan untuk melihat detail lebih lanjut tentang mereka. Untuk memilih beberapa item, pilih **`command/control`** dan pilih item, atau seret dan jatuhkan menggunakan penunjuk Anda.
- Sesuaikan tata letak agar sesuai dengan semua entitas dan temuan ke dalam jendela grup pencarian. Lihat jenis entitas apa yang lazim dalam grup temuan.

> **Note**
>
> Panel Visualisasi grup temuan mendukung tampilan kelompok pencarian dengan hingga 100 entitas dan temuan.

Anda dapat memilih Pilih tata letak untuk melihat temuan dan entitas dalam tata letak Circle, Force-directed, atau Grid. Tata letak yang diarahkan pada gaya memposisikan entitas dan temuan sehingga tautan memiliki panjang yang konsisten antara item dan tautan didistribusikan secara merata. Ini membantu mengurangi tumpang tindih. Tata letak yang Anda pilih menentukan penempatan temuan di panel Visualisasi.



Legenda dinamis berubah berdasarkan entitas dan temuan dalam grafik Anda saat ini. Ini membantu Anda mengidentifikasi apa yang diwakili oleh setiap elemen visual.

Menemukan ringkasan grup yang didukung oleh AI generatif

Secara default, Amazon Detective secara otomatis memberikan ringkasan grup pencarian individu. Ringkasan ini didukung oleh model kecerdasan buatan generatif (AI generatif) yang dihosting di Amazon Bedrock.

Dengan menggunakan grup pencarian, Anda dapat memeriksa beberapa temuan keamanan, karena terkait dengan peristiwa keamanan potensial, dan mengidentifikasi pelaku ancaman potensial. Menemukan ringkasan kelompok untuk menemukan kelompok dibangun di atas kemampuan ini. Menemukan ringkasan kelompok mengkonsumsi data untuk kelompok temuan, dengan cepat menganalisis hubungan antara temuan dan sumber daya yang terpengaruh, dan kemudian merangkum potensi ancaman dalam bahasa alami. Anda dapat memanfaatkan ringkasan ini untuk mengidentifikasi ancaman keamanan yang lebih besar, meningkatkan efisiensi investigasi, dan mempersingkat jadwal respons.

> **Note**
>
> Menemukan ringkasan grup yang didukung oleh AI generatif mungkin dan tidak selalu memberikan informasi yang sepenuhnya akurat. Lihat Kebijakan AI yang Bertanggung AWS Jawab untuk informasi lebih lanjut.

Meninjau ringkasan grup temuan

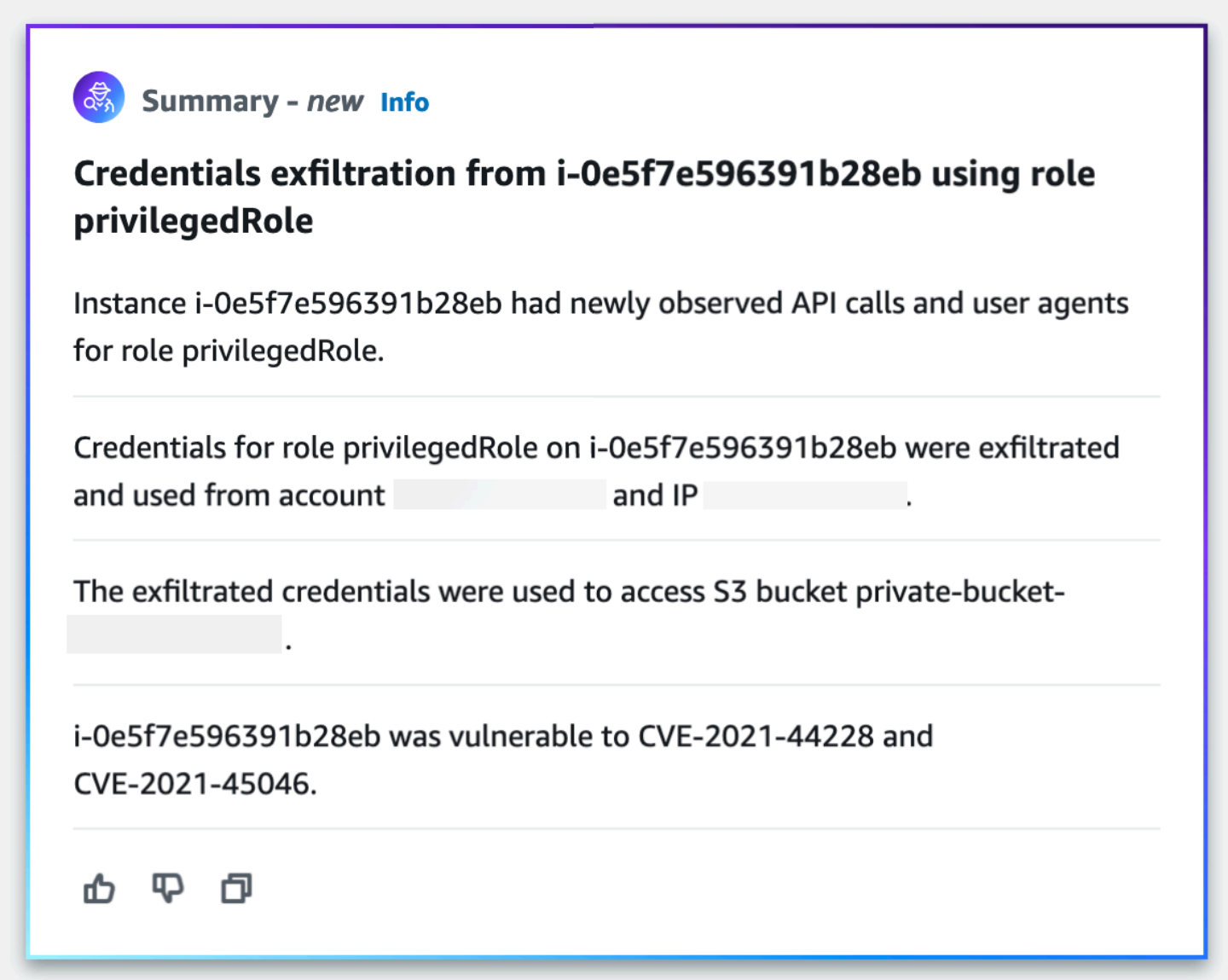
Ringkasan grup temuan untuk grup pencari memberi Anda penjelasan yang jelas dan terperinci tentang peristiwa keamanan. Dalam bahasa alami, penjelasannya mencakup judul yang ringkas, ringkasan sumber daya yang terlibat, dan informasi yang dikuratori tentang sumber daya tersebut.

Untuk meninjau ringkasan grup temuan

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Menemukan grup.
3. Dalam tabel Menemukan grup, pilih grup pencarian yang ingin Anda tampilkan ringkasannya. Halaman detail muncul.

Pada halaman detail, Anda dapat menggunakan panel Ringkasan untuk meninjau ringkasan deskriptif yang dihasilkan dari temuan teratas dalam grup temuan. Anda juga dapat meninjau analisis peristiwa ancaman teratas dalam kelompok pencari, yang kemudian dapat Anda selidiki lebih lanjut. Untuk menambahkan ringkasan yang dihasilkan ke catatan Anda atau sistem tiket, pilih ikon salin di panel. Ini menyalin ringkasan ke clipboard Anda. Anda juga dapat membagikan umpan balik Anda tentang keluaran ringkasan grup temuan dalam ringkasan, yang dapat memberikan pengalaman yang lebih baik di masa depan. Untuk membagikan umpan balik Anda, pilih ikon jempol ke atas atau jempol ke bawah, tergantung pada sifat umpan balik Anda.

> **Note**
>
> Jika Anda memberikan umpan balik tentang ringkasan grup temuan, umpan balik Anda tidak digunakan untuk penyetelan model. Kami menggunakannya hanya untuk membantu memfasilitasi bahwa petunjuk di Detektif dibuat secara efektif.



Menonaktifkan ringkasan grup pencarian

Secara default, menemukan ringkasan grup diaktifkan untuk menemukan grup. Anda dapat menonaktifkan menemukan ringkasan grup kapan saja. Jika Anda menonaktifkan, Anda dapat mengaktifkannya lagi nanti.

Untuk menonaktifkan ringkasan grup pencarian

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Preferensi.
3. Di bawah Menemukan ringkasan grup, pilih Edit.
4. Matikan Diaktifkan.

5. Pilih Simpan.

Mengaktifkan ringkasan grup pencarian

Jika sebelumnya Anda menonaktifkan mencari ringkasan grup untuk menemukan grup, Anda dapat mengaktifkannya lagi kapan saja.

Untuk mengaktifkan menemukan ringkasan grup

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Preferensi.
3. Di bawah Menemukan ringkasan grup, pilih Edit.
4. Aktifkan Diaktifkan.
5. Pilih Simpan.

Wilayah yang Didukung

Menemukan ringkasan grup tersedia di AWS Wilayah berikut.

- AS Timur (Virginia Utara)
- AS Barat (Oregon)
- Asia Pasifik (Tokyo)
- Eropa (Frankfurt)

Menganalisis entitas di Amazon Detective

Entitas adalah objek tunggal yang diekstraksi dari data sumber. Contohnya termasuk alamat IP tertentu, instans Amazon EC2, atau AWS akun. Untuk daftar tipe entitas, lihatthe section called “Jenis entitas dalam struktur data grafik perilaku”.

Profil entitas Detektif Amazon adalah satu halaman yang memberikan informasi terperinci tentang entitas dan aktivitasnya. Anda dapat menggunakan profil entitas untuk mendapatkan detail pendukung untuk penyelidikan temuan atau sebagai bagian dari pencarian umum untuk aktivitas mencurigakan.

Konten

Menggunakan halaman Ringkasan untuk mengidentifikasi entitas yang diminati

Gunakan halaman Ringkasan di Detektif Amazon untuk mengidentifikasi entitas guna menyelidiki asal aktivitas selama 24 jam sebelumnya. Halaman Ringkasan Detektif Amazon membantu Anda mengidentifikasi entitas yang terkait dengan jenis aktivitas tidak biasa tertentu. Ini adalah salah satu dari beberapa titik awal yang mungkin untuk penyelidikan.

Untuk menampilkan halaman Ringkasan, di panel navigasi Detektif, pilih Ringkasan. Halaman Ringkasan juga ditampilkan secara default saat Anda pertama kali membuka konsol Detektif.

Dari halaman Ringkasan, Anda dapat mengidentifikasi entitas yang memenuhi kriteria berikut:

- Investigasi yang menunjukkan potensi peristiwa keamanan yang diidentifikasi oleh Detektif

- Entitas yang terlibat dalam aktivitas yang terjadi di geolokasi yang baru diamati
- Entitas yang membuat jumlah panggilan API terbesar
- Instans EC2 yang memiliki volume lalu lintas terbesar
- Cluster kontainer yang memiliki jumlah kontainer terbesar

Dari setiap panel halaman Ringkasan, Anda dapat berputar ke profil untuk entitas yang dipilih.

Saat Anda meninjau halaman Ringkasan, Anda dapat menyesuaikan waktu Cakupan untuk melihat aktivitas untuk kerangka waktu 24 jam apa pun dalam 365 hari sebelumnya. Saat Anda mengubah tanggal dan waktu Mulai, tanggal dan waktu Berakhir secara otomatis diperbarui menjadi 24 jam setelah waktu mulai yang Anda pilih.

Dengan Detective, Anda dapat mengakses data peristiwa historis hingga satu tahun. Data ini tersedia melalui serangkaian visualisasi yang menunjukkan perubahan jenis dan volume aktivitas pada jendela waktu yang dipilih. Detektif menghubungkan perubahan ini dengan temuan. GuardDuty

Untuk informasi selengkapnya tentang sumber data di Detektif, lihat Sumber data yang digunakan dalam grafik perilaku.

Investigasi

Investigasi menunjukkan kepada Anda peristiwa keamanan potensial yang diidentifikasi oleh Detektif. Pada panel Investigasi, Anda dapat melihat Investigasi kritis dan AWS peran serta pengguna terkait yang terkena dampak peristiwa keamanan selama periode waktu tertentu. Investigasi mengelompokkan indikator kompromi untuk membantu menentukan apakah AWS sumber daya terlibat dalam aktivitas yang tidak biasa yang dapat menunjukkan perilaku jahat dan dampaknya.

Pilih Lihat semua investigasi untuk meninjau temuan, grup pencarian triase, dan detail sumber daya untuk mempercepat penyelidikan keamanan Anda. Investigasi ditampilkan tergantung pada waktu Lingkup yang dipilih. Anda dapat menyesuaikan waktu lingkup untuk melihat investigasi dalam kerangka waktu 24 jam dalam 365 hari sebelumnya. Anda dapat beralih langsung ke investigasi Kritis untuk melihat laporan investigasi terperinci.

Jika Anda mengidentifikasi AWS peran atau pengguna yang tampaknya memiliki aktivitas mencurigakan, Anda dapat beralih langsung dari panel Investigasi ke peran atau pengguna untuk melanjutkan penyelidikan Anda. Pivot ke peran atau pengguna dan klik Jalankan investigasi untuk menghasilkan laporan investigasi. Setelah Anda menjalankan investigasi terhadap peran atau pengguna, peran atau pengguna akan dipindahkan ke tab Investigasi.

Geolokasi yang baru diamati

Geolokasi yang baru diamati menyoroti lokasi geografis yang merupakan asal aktivitas selama 24 jam sebelumnya, tetapi itu tidak terlihat selama periode waktu awal sebelum itu.

Panel mencakup hingga 100 geolokasi. Lokasi ditandai pada peta dan tercantum dalam tabel di bawah peta.

Untuk setiap geolokasi, tabel menampilkan jumlah panggilan API yang gagal dan berhasil dilakukan dari geolokasi tersebut selama 24 jam sebelumnya.

Anda dapat memperluas setiap geolokasi untuk menampilkan daftar pengguna dan peran yang membuat panggilan API dari geolokasi tersebut. Untuk setiap prinsipal, tabel mencantumkan jenis dan yang terkait Akun AWS.

Jika Anda mengidentifikasi pengguna atau peran yang tampaknya mencurigakan, maka Anda dapat berputar langsung dari panel ke pengguna atau profil peran untuk melanjutkan penyelidikan Anda. Untuk berputar ke profil, pilih pengguna atau pengenal peran.

Detektif menentukan lokasi permintaan menggunakan database GeoIP MaxMind . MaxMind melaporkan akurasi data mereka yang sangat tinggi di tingkat negara, meskipun akurasi bervariasi sesuai dengan faktor-faktor seperti negara dan jenis IP. Untuk informasi selengkapnya MaxMind, lihat Geolokasi MaxMind IP. Jika menurut Anda salah satu data GeoIP salah, Anda dapat mengirimkan permintaan koreksi ke Maxmind di Data GeoIP2 MaxMind yang Benar.

Kelompok pencarian aktif dalam 7 hari terakhir

Kelompok temuan aktif dalam 7 hari terakhir menunjukkan kepada Anda pengelompokan berkorelasi temuan Detektif, entitas, dan bukti di lingkungan Anda yang terjadi selama periode waktu tertentu. Pengelompokan ini mengkorelasikan aktivitas yang tidak biasa yang dapat menunjukkan perilaku jahat. Halaman ringkasan menampilkan hingga lima kelompok yang diurutkan berdasarkan kelompok yang berisi temuan paling kritis yang telah aktif dalam seminggu terakhir.

Anda dapat memilih nilai dalam konten Taktik, Akun, Sumber Daya, dan Temuan untuk melihat detail selengkapnya.

Kelompok temuan dihasilkan setiap hari. Jika Anda mengidentifikasi kelompok yang menarik, Anda dapat memilih judul untuk dipindahkan ke tampilan detail profil grup untuk melanjutkan penyelidikan Anda.

Peran dan pengguna dengan volume panggilan API terbanyak

Peran dan pengguna dengan volume panggilan API terbanyak mengidentifikasi pengguna dan peran yang telah membuat jumlah panggilan API terbesar selama 24 jam sebelumnya.

Panel dapat mencakup hingga 100 pengguna dan peran. Untuk setiap pengguna atau peran, Anda dapat melihat jenis (pengguna atau peran) dan akun terkait. Anda juga dapat melihat jumlah panggilan API yang dikeluarkan oleh pengguna atau peran tersebut selama 24 jam sebelumnya.

Secara default, peran terkait layanan ditampilkan. Peran terkait layanan dapat menghasilkan volume AWS CloudTrail aktivitas yang besar, yang menggantikan prinsip-prinsip yang ingin Anda selidiki lebih lanjut. Anda dapat memilih untuk menonaktifkan Tampilkan peran terkait layanan, untuk memfilter peran terkait layanan dari tampilan halaman ringkasan.

Anda dapat mengekspor file nilai dipisahkan koma (.csv) yang berisi data di panel ini.

Ada juga timeline volume panggilan API selama 7 hari sebelumnya. Garis waktu dapat membantu Anda menentukan apakah volume panggilan API tidak biasa untuk prinsipal tersebut.

Jika Anda mengidentifikasi pengguna atau peran yang volume panggilan API tampak mencurigakan, maka Anda dapat berputar langsung dari panel ke pengguna atau profil peran untuk melanjutkan penyelidikan Anda. Anda juga dapat melihat profil akun yang terkait dengan pengguna atau peran. Untuk melihat profil, pilih pengguna, peran, atau pengenal akun.

Instans EC2 dengan volume lalu lintas terbanyak

Instans EC2 dengan volume lalu lintas terbanyak mengidentifikasi instans EC2 yang memiliki total volume lalu lintas terbesar selama 24 jam sebelumnya.

Panel dapat mencakup hingga 100 instans EC2. Untuk setiap instans EC2, Anda dapat melihat akun terkait dan jumlah byte masuk, byte keluar, dan total byte dari 24 jam sebelumnya.

Anda dapat mengekspor file nilai dipisahkan koma (.csv) yang berisi data di panel ini.

Anda juga dapat melihat garis waktu yang menunjukkan lalu lintas masuk dan keluar selama 7 hari sebelumnya. Garis waktu dapat membantu menentukan apakah volume lalu lintas tidak biasa untuk instans EC2 tersebut.

Jika Anda mengidentifikasi instans EC2 yang memiliki volume lalu lintas mencurigakan, maka Anda dapat langsung pergi dari panel ke profil instans EC2 untuk melanjutkan penyelidikan Anda. Anda

juga dapat melihat profil akun yang memiliki instans EC2. Untuk melihat profil, pilih instans EC2 atau pengenal akun.

Cluster kontainer dengan pod Kubernetes terbanyak

Cluster kontainer dengan pod Kubernetes terbanyak yang dibuat mengidentifikasi cluster yang memiliki kontainer paling banyak berjalan selama 24 jam sebelumnya.

Panel ini mencakup hingga 100 cluster yang diatur oleh cluster mana memiliki temuan paling banyak yang terkait dengannya. Untuk setiap cluster, Anda dapat melihat akun terkait, jumlah kontainer saat ini di cluster tersebut, dan jumlah temuan yang terkait dengan cluster tersebut selama 24 jam terakhir. Anda dapat mengekspor file nilai dipisahkan koma (.csv) yang berisi data di panel ini.

Jika Anda mengidentifikasi klaster dengan temuan terbaru, Anda dapat berputar langsung dari panel ke profil klaster untuk melanjutkan penyelidikan Anda. Anda juga dapat berputar ke profil akun yang memiliki cluster. Untuk berputar ke profil, pilih nama cluster atau pengenal akun.

Perkiraan pemberitahuan nilai

Pada Peran dan pengguna dengan volume panggilan API terbanyak dan instans EC2 dengan volume lalu lintas terbanyak, jika nilai diikuti oleh tanda bintang (*), itu berarti nilainya adalah perkiraan. Nilai sebenarnya sama dengan atau lebih besar dari nilai yang ditampilkan.

Hal ini terjadi karena metode yang digunakan Detective untuk menghitung volume untuk setiap interval waktu. Pada halaman Ringkasan, interval waktu adalah satu jam.

Untuk setiap jam, Detective menghitung total volume untuk 1.000 pengguna, peran, atau instans EC2 dengan volume terbesar. Ini mengecualikan data untuk pengguna, peran, atau instans EC2 yang tersisa.

Jika sumber daya terkadang berada di 1.000 teratas dan terkadang tidak, maka volume yang dihitung untuk sumber daya itu mungkin tidak mencakup semua data. Data untuk interval waktu di mana tidak berada di 1.000 teratas dikecualikan.

Perhatikan bahwa ini hanya berlaku untuk halaman Ringkasan. Profil untuk pengguna, peran, atau instans EC2 memberikan detail yang tepat.

Menggunakan profil entitas

Profil entitas muncul saat Anda melakukan salah satu tindakan berikut:

- Dari GuardDuty konsol Amazon, pilih opsi untuk menyelidiki entitas yang terkait dengan temuan yang dipilih.

  Lihat the section called “Berputar dari konsol lain”.
- Buka URL Detektif untuk profil entitas.

  Lihat the section called “Menavigasi menggunakan URL”.
- Gunakan pencarian Detektif di konsol Detektif untuk mencari entitas.
- Pilih tautan ke profil entitas dari profil entitas lain atau dari ikhtisar temuan.

Cakupan waktu untuk profil entitas

Saat Anda menavigasi langsung ke profil entitas tanpa memberikan waktu lingkup, waktu cakupan diatur ke 24 jam sebelumnya.

Saat Anda menavigasi ke profil entitas dari profil entitas lain, waktu lingkup yang dipilih saat ini tetap ada.

Saat Anda menavigasi ke profil entitas dari ikhtisar temuan, waktu cakupan diatur ke jendela waktu pencarian.

Untuk informasi tentang menyesuaikan waktu lingkup untuk membatasi data yang ditampilkan pada profil entitas, lihat Mengelola waktu cakupan.

Pengidentifikasi dan tipe entitas

Di bagian atas profil adalah pengenal entitas dan tipe entitas. Setiap jenis entitas memiliki ikon yang sesuai, untuk memberikan indikator visual dari jenis profil.

Temuan yang terlibat

Setiap profil berisi daftar temuan yang melibatkan entitas selama waktu lingkup.

Anda dapat melihat detail untuk setiap temuan, mengubah waktu lingkup untuk mencerminkan jendela waktu pencarian, dan pergi ke ikhtisar temuan untuk mencari sumber daya lain yang terlibat.

Lihat the section called “Melihat temuan untuk suatu entitas”.

Menemukan kelompok yang melibatkan entitas ini

Setiap profil berisi daftar grup pencarian tempat entitas disertakan.

Kelompok temuan terdiri dari temuan, entitas, dan bukti yang dikumpulkan Detektif ke dalam kelompok untuk memberikan lebih banyak konteks tentang kemungkinan masalah keamanan.

Untuk informasi lebih lanjut tentang menemukan grup, lihatthe section called “Menemukan grup”.

Panel profil yang berisi detail entitas dan hasil analitik

Setiap profil entitas berisi satu set tab atau lebih. Setiap tab berisi satu atau lebih panel profil. Setiap panel profil berisi teks dan visualisasi yang dihasilkan dari data grafik perilaku. Tab dan panel profil tertentu disesuaikan dengan jenis entitas.

Untuk sebagian besar entitas, panel di bagian atas tab pertama memberikan informasi ringkasan tingkat tinggi tentang entitas.

Panel profil lainnya menyoroti berbagai jenis aktivitas. Untuk entitas yang terlibat dengan temuan, informasi pada panel profil entitas dapat memberikan bukti pendukung tambahan untuk membantu menyelesaikan penyelidikan. Setiap panel profil menyediakan akses ke panduan tentang cara menggunakan informasi. Untuk informasi selengkapnya, lihat the section called “Menggunakan panduan panel profil”.

Untuk detail selengkapnya tentang panel profil, jenis data yang dikandungnya, dan opsi yang tersedia untuk berinteraksi dengannya, lihatthe section called “Melihat dan berinteraksi dengan panel profil”.

Melihat dan berinteraksi dengan panel profil

Setiap profil entitas di konsol Detektif Amazon terdiri dari satu set panel profil. Panel profil adalah visualisasi yang memberikan rincian umum atau menyoroti aktivitas spesifik yang terkait dengan entitas. Panel profil menggunakan berbagai jenis visualisasi untuk menyajikan berbagai jenis informasi. Mereka juga dapat memberikan tautan ke detail tambahan atau ke profil lain.

Setiap panel profil dimaksudkan untuk membantu analis menemukan jawaban atas pertanyaan spesifik tentang entitas dan aktivitas terkait mereka. Jawaban atas pertanyaan-pertanyaan itu membantu mengarah pada kesimpulan tentang apakah aktivitas tersebut merupakan ancaman asli.

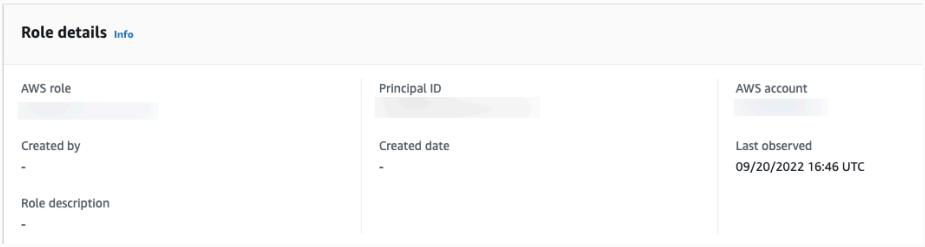
Daftar Isi

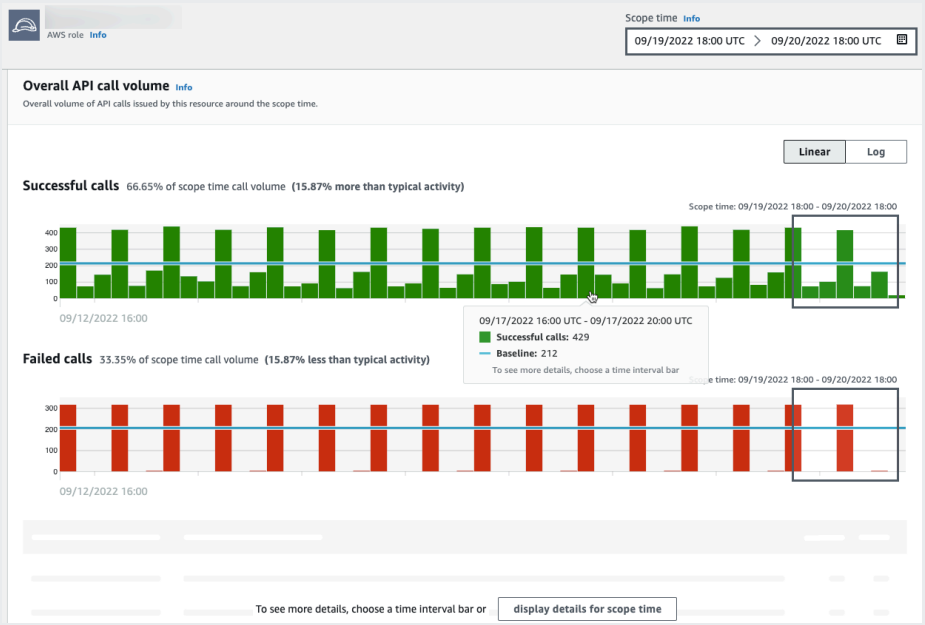
Konten panel profil

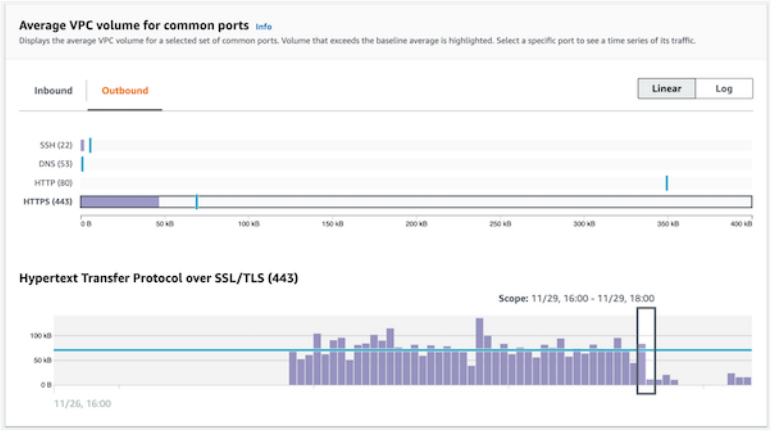
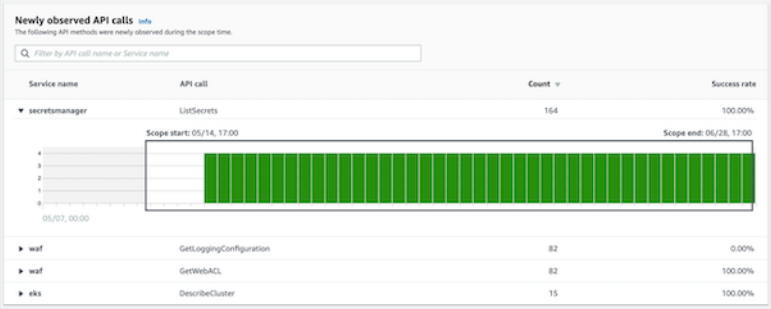
Panel profil menggunakan berbagai jenis visualisasi untuk menyajikan berbagai jenis informasi.

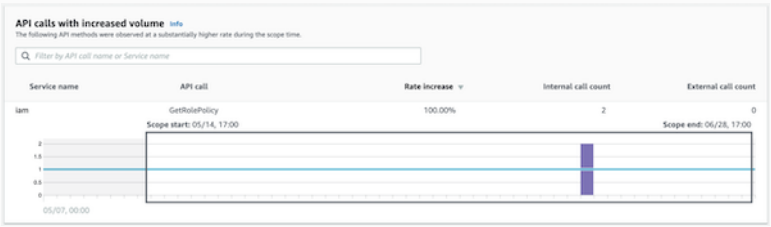
Jenis informasi pada panel profil

Panel profil biasanya menyediakan jenis data berikut.

Tipe data panel	Deskripsi
Informasi tingkat tinggi tentang temuan atau entitas	Jenis panel yang paling sederhana memberikan beberapa informasi dasar tentang suatu entitas. Contoh informasi yang disertakan pada panel informasi termasuk pengenal, nama, jenis, dan tanggal pembuatan.  Sebagian besar profil entitas berisi panel informasi untuk entitas tersebut.
Ringkasan umum kegiatan dari waktu ke waktu	Menampilkan ringkasan aktivitas untuk entitas dari waktu ke waktu. Jenis panel ini memberikan pandangan keseluruhan tentang bagaimana entitas berperilaku selama waktu lingkup.

Tipe data panel	Deskripsi
	 Berikut adalah beberapa contoh data ringkasan yang disediakan pada panel profil Detektif: • Panggilan API yang gagal dan berhasil • Volume VPC masuk dan keluar

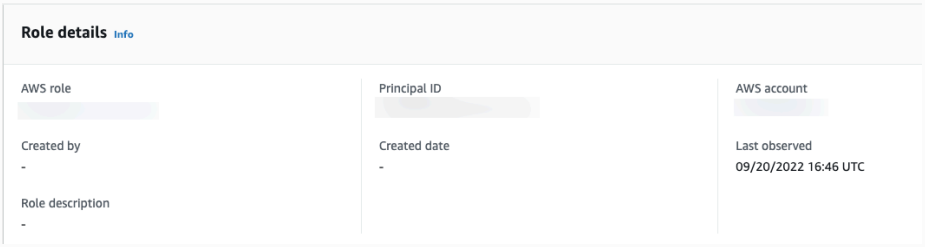
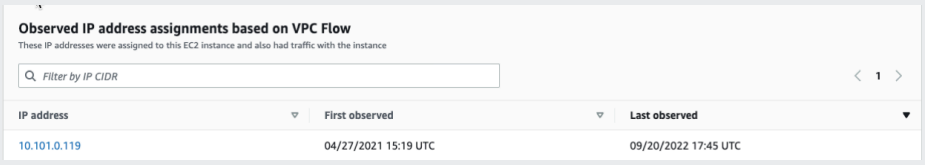
Tipe data panel	Deskripsi
Ringkasan aktivitas dikelompokkan berdasarkan nilai	Menampilkan ringkasan aktivitas untuk entitas, dikelompokkan berdasarkan nilai tertentu. Anda dapat melihat jenis panel profil ini di profil untuk instans EC2. Panel profil menunjukkan volume rata-rata data log aliran VPC ke dan dari instans EC2 untuk port umum yang terkait dengan jenis layanan tertentu. 
Aktivitas yang hanya dimulai selama waktu lingkup	Selama penyelidikan, penting untuk melihat aktivitas apa yang baru mulai terjadi selama jangka waktu tertentu. Misalnya, apakah ada panggilan API, lokasi geografis, atau agen pengguna yang tidak terlihat sebelumnya?  Jika grafik perilaku masih dalam mode pelatihan, panel profil akan menampilkan pesan notifikasi. Pesan dihapus ketika grafik perilaku telah mengumpulkan setidaknya dua minggu data. Untuk informasi selengkapnya tentang mode pelatihan, lihatthe section called “Periode pelatihan untuk grafik perilaku baru”.

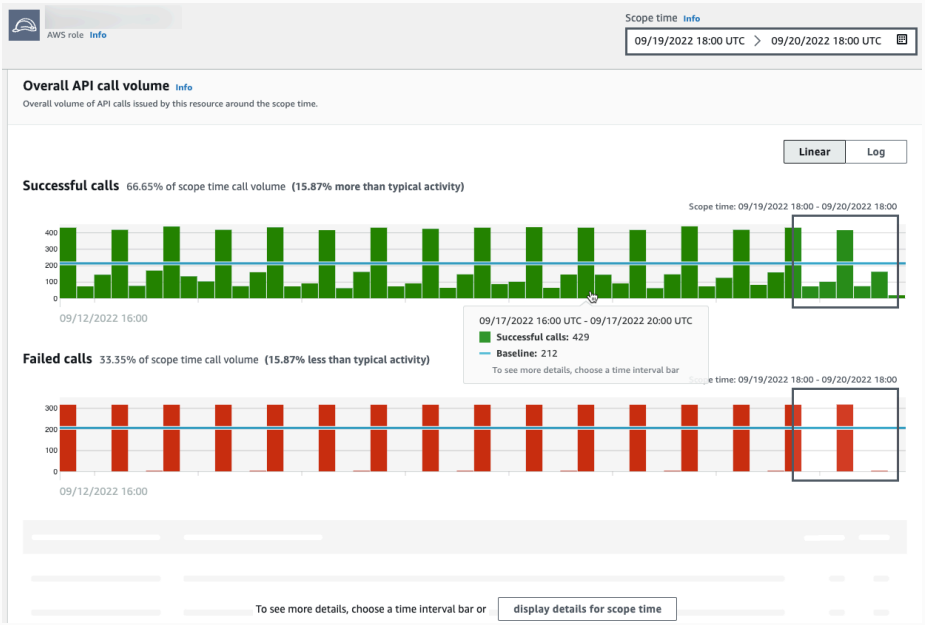
Tipe data panel	Deskripsi
Aktivitas yang berubah secara signifikan selama waktu lingkup	Mirip dengan panel aktivitas baru, panel profil juga dapat menampilkan aktivitas yang berubah secara signifikan selama waktu lingkup. Misalnya, pengguna mungkin secara teratur mengeluarkan panggilan API tertentu beberapa kali seminggu. Jika pengguna yang sama tiba-tiba mengeluarkan panggilan yang sama beberapa kali dalam satu hari, itu mungkin bukti aktivitas jahat.  Jika grafik perilaku masih dalam mode pelatihan, panel profil akan menampilkan pesan notifikasi. Pesan dihapus ketika grafik perilaku telah mengumpulkan setidaknya dua minggu data. Untuk informasi selengkapnya tentang mode pelatihan, lihatthe section called “Periode pelatihan untuk grafik perilaku baru”.

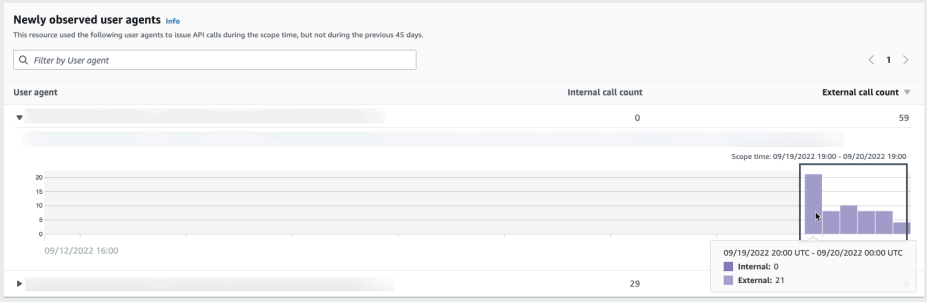
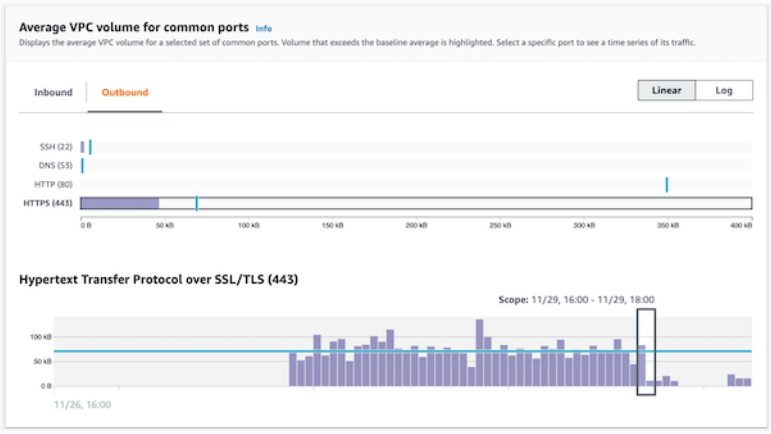
Jenis visualisasi panel profil

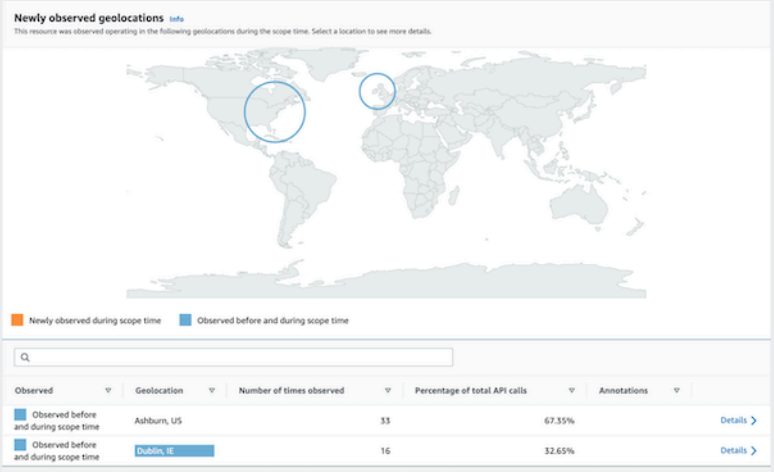
Konten panel profil dapat mengambil salah satu formulir berikut.

Jenis visualisasi	Deskripsi
Pasangan kunci/nilai	Jenis visualisasi yang paling sederhana adalah satu set pasangan kunci-nilai. Panel informasi temuan atau entitas adalah contoh paling umum dari panel pasangan kunci-nilai.

Jenis visualisasi	Deskripsi
	 Pasangan nilai kunci juga dapat digunakan untuk menambahkan informasi tambahan ke jenis panel lainnya. Dari panel pasangan kunci-nilai, jika nilai adalah pengidentifikasi entitas, maka Anda dapat berputar ke profilnya.
Tabel	Tabel adalah daftar item multi-kolom sederhana.  Anda dapat mengurutkan, memfilter, dan halaman melalui tabel. Anda dapat mengubah jumlah entri yang akan ditampilkan di setiap halaman. Lihat the section called “Preferensi untuk panel profil”. Jika nilai dalam tabel adalah pengidentifikasi entitas, maka Anda dapat berputar ke profilnya.

Jenis visualisasi	Deskripsi
Garis Waktu	Visualisasi garis waktu menunjukkan nilai agregat untuk interval yang ditentukan dari waktu ke waktu.  Garis waktu menyoroti waktu lingkup saat ini, dan mencakup waktu periferal tambahan sebelum dan sesudah waktu lingkup. Waktu periferal memberikan konteks untuk aktivitas dalam waktu lingkup. Arahkan kursor ke interval waktu untuk menampilkan ringkasan data untuk interval waktu tersebut.

Jenis visualisasi	Deskripsi
Tabel yang dapat diperluas	Tabel yang dapat diperluas menggabungkan tabel dan garis waktu.  Visualisasi dimulai sebagai tabel. Anda dapat mengurutkan, memfilter, dan halaman melalui tabel. Anda dapat mengubah jumlah entri yang akan ditampilkan di setiap halaman. Lihat the section called “Preferensi untuk panel profil”. Anda kemudian dapat memperluas setiap baris untuk menampilkan visualisasi garis waktu khusus untuk baris itu.
Bagan batang	Bagan batang menunjukkan nilai berdasarkan pengelompokan. Bergantung pada bagan, Anda mungkin dapat memilih bilah untuk menampilkan garis waktu aktivitas terkait. 

Jenis visualisasi	Deskripsi
Bagan geolokasi	Bagan geolokasi menampilkan peta yang ditandai untuk menyorot data berdasarkan lokasi geografis. Ini dapat diikuti oleh tabel yang berisi rincian tentang geolokasi individu.  Perhatikan bahwa saat memproses data geografis yang masuk, Detective membulatkan nilai lintang dan bujur ke satu titik desimal.

Catatan lain pada konten panel profil

Saat melihat konten panel profil, perhatikan item berikut:

Perkiraan hitungan peringatan data

Peringatan ini menunjukkan bahwa item dengan jumlah yang sangat rendah tidak muncul karena volume data yang berlaku.

Untuk memastikan penghitungan yang benar-benar akurat, kurangi jumlah data. Cara termudah untuk melakukannya adalah dengan mengurangi lamanya waktu lingkup. Lihat the section called “Mengelola ruang lingkup waktu”.

Pembulatan untuk lokasi geografis

Detective membulatkan semua nilai lintang dan bujur ke titik desimal tunggal.

Perubahan cara Detective merepresentasikan panggilan API

Mulai 14 Juli 2021, Detective melacak layanan yang melakukan setiap panggilan API. Setiap kali Detective menampilkan metode API, itu juga menampilkan layanan terkait. Pada panel profil yang menampilkan informasi tentang panggilan API, panggilan selalu dikelompokkan berdasarkan layanan. Untuk data yang dicerna Detektif sebelum tanggal tersebut, nama layanan terdaftar sebagai layanan Tidak Dikenal.

Juga dimulai pada 14 Juli 2021, untuk akun dan peran, detail aktivitas untuk panel profil volume panggilan API Keseluruhan tidak lagi menampilkan AKID sumber daya yang mengeluarkan panggilan. Untuk akun, Detective menampilkan pengenal kepala sekolah (pengguna atau peran) yang mengeluarkan panggilan. Untuk peran, Detective menampilkan pengenal sesi peran. Untuk data yang dicerna Detektif sebelum 14 Juli 2021, pengenal terdaftar sebagai sumber daya Tidak Dikenal.

Untuk panel profil yang menampilkan daftar panggilan API, timeline terkait menyoroti periode waktu selama transisi ini terjadi. Sorotan dimulai pada 14 Juli 2021, dan berakhir ketika pembaruan sepenuhnya disebarkan di Detective.

Mengatur preferensi untuk panel profil

Di konsol Detective, Anda dapat mengatur panjang Tabel dan tampilan Timestamp pada halaman Preferensi.

Mengatur panjang meja

Untuk panel profil yang berisi tabel atau tabel yang dapat diperluas, Anda dapat mengonfigurasi jumlah baris yang akan ditampilkan di setiap halaman.

Tetapkan preferensi Anda untuk jumlah entri di setiap halaman.

1. Buka konsol Amazon Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, di bawah Pengaturan, pilih Preferensi.
3. Pada halaman Preferensi, di bawah Panjang tabel, klik Edit.
4. Pilih jumlah baris tabel yang ingin Anda tampilkan di setiap halaman.
5. Pilih Simpan.

Mengatur format stempel waktu

Untuk panel profil, Anda dapat mengonfigurasi preferensi format stempel waktu yang akan diterapkan ke semua stempel waktu untuk setiap pengguna IAM atau peran IAM di Detective.

> **Note**
>
> Preferensi format stempel waktu tidak diterapkan di seluruh AWS akun.

Atur preferensi untuk stempel waktu.

1. Buka konsol Amazon Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, di bawah Pengaturan, pilih Preferensi.
3. Pada halaman Preferensi, di bawah preferensi stempel waktu, lihat dan ubah tampilan yang disukai untuk semua stempel waktu.
4. Secara default, format stempel waktu diatur ke UTC. Klik Edit untuk memilih zona waktu lokal Anda.

   Contoh:

   Example

   UTC - 09/20/22 16:39 UTC

   Lokal - 09/20/2022 9:39 (UTC- 07:00)
5. Pilih Simpan.

Berputar dari panel profil ke konsol lain

Untuk instans EC2, pengguna IAM, dan peran IAM, Anda dapat menavigasi langsung dari panel profil detail ke konsol yang sesuai. Informasi yang tersedia dari konsol dapat memberikan masukan tambahan untuk penyelidikan Anda.

Pada panel profil detail instans EC2, pengenal instans EC2 ditautkan ke konsol Amazon EC2.

Pada panel profil Detail pengguna, nama pengguna ditautkan ke konsol IAM.

Pada panel profil Rincian peran, nama peran ditautkan ke konsol IAM.

Berputar dari panel profil ke profil entitas lain

Ketika panel profil berisi pengenal entitas yang berbeda, biasanya tautan ke profil entitas tersebut. Pengecualiannya adalah tautan ke konsol Amazon EC2 dan IAM pada instans EC2, pengguna IAM, dan profil peran IAM. Lihat the section called “Beralih ke konsol lain”.

Misalnya, dari daftar alamat IP, Anda mungkin dapat menampilkan profil untuk alamat IP tertentu. Dengan begitu Anda dapat melihat apakah ada informasi lain yang tersedia untuk membantu Anda menyelesaikan penyelidikan Anda.

Menjelajahi detail aktivitas di panel profil

Selama investigasi, Anda mungkin ingin menyelidiki lebih lanjut tentang pola aktivitas untuk suatu entitas.

Pada panel profil berikut, Anda dapat menampilkan ringkasan detail aktivitas:

- Volume panggilan API secara keseluruhan, kecuali untuk panel profil pada profil agen pengguna
- Geolokasi yang baru diamati
- Volume aliran VPC keseluruhan
- Volume aliran VPC ke dan dari alamat IP pencarian, untuk temuan yang terkait dengan satu alamat IP
- Detail kontainer
- Volume aliran VPC untuk cluster
- Keseluruhan aktivitas API Kubernetes

Detail aktivitas dapat menjawab jenis pertanyaan ini:

- Alamat IP mana yang digunakan?
- Di mana alamat IP tersebut berada?
- Panggilan API mana yang dilakukan setiap alamat IP, dan dari layanan mana mereka melakukan panggilan itu?
- Prinsipal atau pengidentifikasi kunci akses (AKID) mana yang digunakan untuk melakukan panggilan?
- Sumber daya apa yang digunakan untuk melakukan panggilan itu?

- Berapa banyak panggilan yang dilakukan? Berapa banyak yang berhasil dan gagal?
- Berapa volume data log aliran VPC yang dikirim ke atau dari setiap alamat IP?
- Wadah apa yang aktif untuk cluster, image, atau pod tertentu?

Topik

Detail aktivitas untuk Volume panggilan API Keseluruhan

Detail aktivitas untuk Volume panggilan API Keseluruhan menunjukkan panggilan API yang dikeluarkan selama rentang waktu yang dipilih.

Untuk menampilkan detail aktivitas untuk interval waktu tunggal, pilih interval waktu pada bagan.

Untuk menampilkan detail aktivitas untuk waktu lingkup saat ini, pilih Menampilkan detail untuk waktu lingkup.

Perhatikan bahwa Detective mulai menyimpan dan menampilkan nama layanan untuk panggilan API per 14 Juli 2021. Tanggal itu disorot pada timeline panel profil. Untuk aktivitas yang terjadi sebelum tanggal tersebut, nama layanan adalah layanan Tidak Dikenal.

Konten detail aktivitas (pengguna, peran, akun, sesi peran, instans EC2, bucket S3)

Untuk pengguna IAM, peran IAM, akun, sesi peran, instans EC2, dan bucket S3, detail aktivitas berisi informasi berikut:

- Setiap tab memberikan informasi tentang kumpulan panggilan API yang dikeluarkan selama rentang waktu yang dipilih.

  Untuk bucket S3, informasi tersebut mencerminkan panggilan API yang dilakukan ke bucket S3.

  Panggilan API dikelompokkan berdasarkan layanan yang memanggilnya. Untuk bucket S3, layanan ini selalu Amazon S3. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.

- Untuk setiap entri, detail aktivitas menunjukkan jumlah panggilan yang berhasil dan gagal. Tab Alamat IP yang Diamati juga menunjukkan lokasi setiap alamat IP.
- Setiap entri menunjukkan informasi tentang siapa yang melakukan panggilan. Untuk akun, detail aktivitas mengidentifikasi pengguna atau peran. Untuk peran, detail aktivitas mengidentifikasi sesi peran. Untuk pengguna dan sesi peran, detail aktivitas mengidentifikasi pengenal kunci akses (AKID).

  Perhatikan bahwa per 14 Juli 2021, untuk profil akun, detail aktivitas menampilkan pengguna atau peran, bukan AKID. Untuk profil peran, detail aktivitas menampilkan sesi peran, bukan AKID. Untuk aktivitas yang terjadi sebelum 14 Juli 2021, penelepon terdaftar sebagai Sumber daya tidak dikenal.

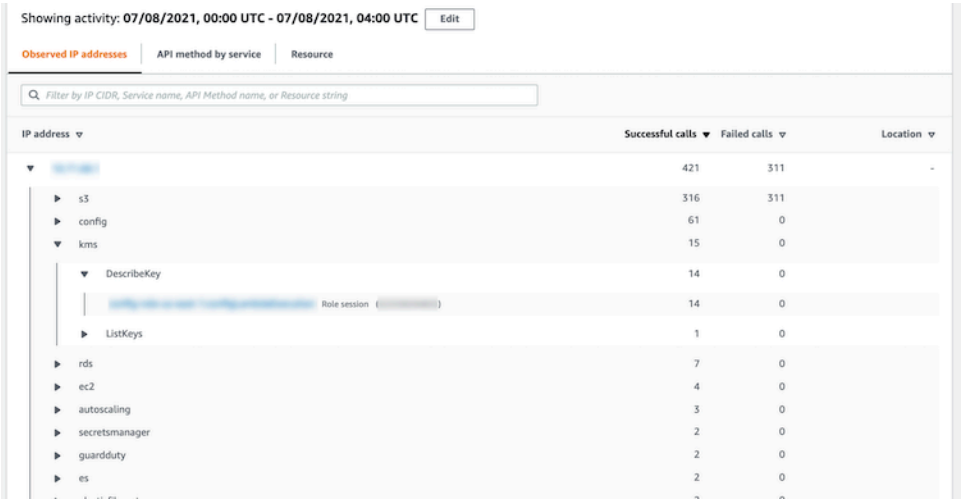
Detail aktivitas berisi tab berikut:

Alamat IP yang diamati

Awalnya menampilkan daftar alamat IP yang digunakan untuk mengeluarkan panggilan API.

Anda dapat memperluas setiap alamat IP untuk menampilkan daftar panggilan API yang dikeluarkan dari alamat IP tersebut. Panggilan API dikelompokkan berdasarkan layanan yang memanggilnya. Untuk bucket S3, layanan ini selalu Amazon S3. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.

Anda kemudian dapat memperluas setiap panggilan API untuk menampilkan daftar penelepon dari alamat IP tersebut. Bergantung pada profilnya, penelepon mungkin pengguna, peran, sesi peran, atau AKID.

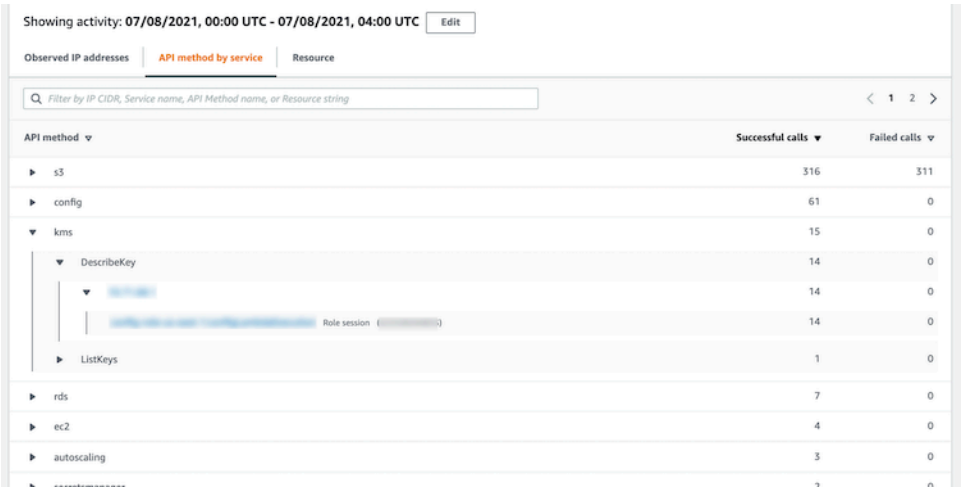


Metode API berdasarkan layanan

Awalnya menampilkan daftar panggilan API yang dikeluarkan. Panggilan API dikelompokkan berdasarkan layanan yang mengeluarkan panggilan. Untuk bucket S3, layanan ini selalu Amazon S3. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.

Anda dapat memperluas setiap metode API untuk menampilkan daftar alamat IP dari mana panggilan dikeluarkan.

Anda kemudian dapat memperluas setiap alamat IP untuk menampilkan daftar AKID yang mengeluarkan panggilan API dari alamat IP tersebut.

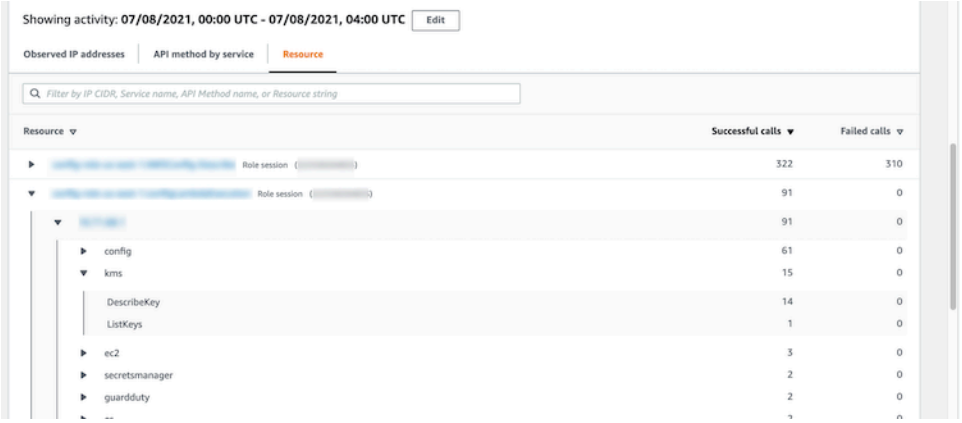


Sumber Daya atau ID Kunci Akses

Awalnya menampilkan daftar pengguna, peran, sesi peran, atau AKID yang digunakan untuk mengeluarkan panggilan API.

Anda dapat memperluas setiap pemanggil untuk menampilkan daftar alamat IP dari mana pemanggil mengeluarkan panggilan API.

Anda kemudian dapat memperluas setiap alamat IP untuk menampilkan daftar panggilan API yang dikeluarkan dari alamat IP tersebut oleh penelepon tersebut. Panggilan API dikelompokkan berdasarkan layanan yang mengeluarkan panggilan. Untuk bucket S3, layanan ini selalu Amazon S3. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.



Isi detail aktivitas (alamat IP)

Untuk alamat IP, detail aktivitas berisi informasi berikut:

- Setiap tab memberikan informasi tentang kumpulan panggilan API yang dikeluarkan selama rentang waktu yang dipilih. Panggilan API dikelompokkan berdasarkan layanan yang mengeluarkan panggilan. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.
- Untuk setiap entri, detail aktivitas menunjukkan jumlah panggilan yang berhasil dan gagal.

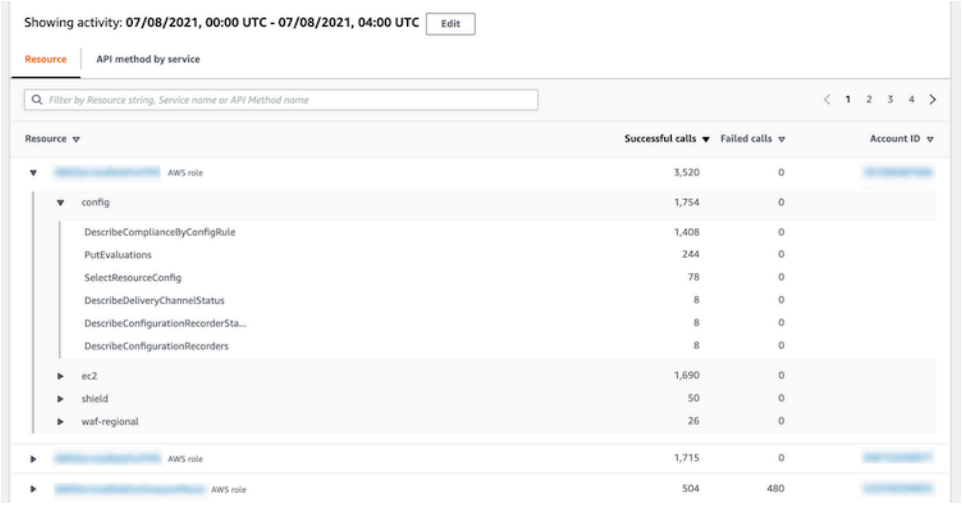
Detail aktivitas berisi tab berikut:

Sumber daya

Awalnya menampilkan daftar sumber daya yang mengeluarkan panggilan API dari alamat IP.

Untuk setiap sumber daya, daftar mencakup nama sumber daya, jenis, dan AWS akun.

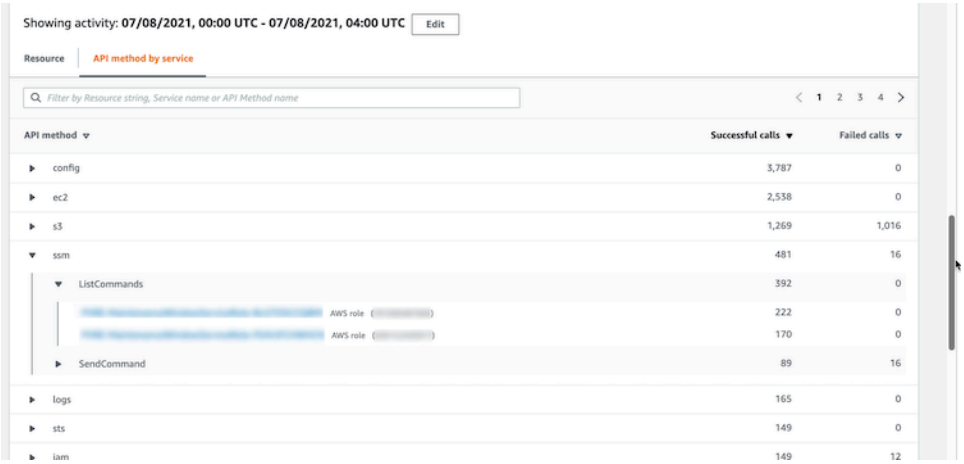
Anda dapat memperluas setiap sumber daya untuk menampilkan daftar panggilan API yang sumber daya dikeluarkan dari alamat IP. Panggilan API dikelompokkan berdasarkan layanan yang mengeluarkan panggilan. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.



Metode API berdasarkan layanan

Awalnya menampilkan daftar panggilan API yang dikeluarkan. Panggilan API dikelompokkan berdasarkan layanan yang mengeluarkan panggilan. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.

Anda dapat memperluas setiap panggilan API untuk menampilkan daftar sumber daya yang mengeluarkan panggilan API dari alamat IP selama periode waktu yang dipilih.



Menyortir detail aktivitas

Anda dapat mengurutkan detail aktivitas berdasarkan kolom daftar mana pun.

Saat Anda mengurutkan menggunakan kolom pertama, hanya daftar tingkat atas yang diurutkan. Daftar tingkat yang lebih rendah selalu diurutkan berdasarkan jumlah panggilan API yang berhasil.

Memfilter detail aktivitas

Anda dapat menggunakan opsi pemfilteran untuk fokus pada himpunan bagian atau aspek tertentu dari aktivitas yang direpresentasikan dalam detail aktivitas.

Pada semua tab, Anda dapat memfilter daftar dengan salah satu nilai di kolom pertama.

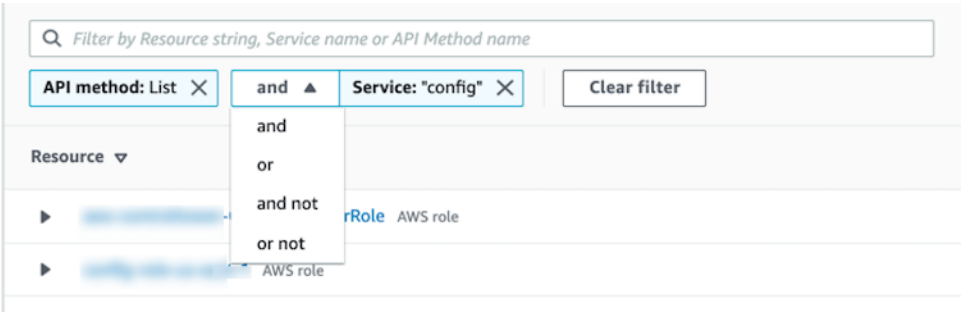
Untuk menambahkan filter

1. Pilih kotak filter.
2. Dari Properties, pilih properti yang akan digunakan untuk penyaringan.
3. Berikan nilai yang akan digunakan untuk penyaringan. Filter mendukung nilai paral. Misalnya, ketika Anda memfilter berdasarkan metode API, jika Anda memfilter menurut**`Instance`**, hasilnya menyertakan operasi API apa pun `Instance` yang memiliki namanya. Jadi keduanya `ListInstanceAssociations` dan `UpdateInstanceInformation` akan cocok.

   Untuk nama layanan, metode API, dan alamat IP, Anda dapat menentukan nilai atau memilih filter bawaan.

   Untuk substring Common API, pilih substring yang mewakili jenis operasi, seperti, `ListCreate`, atau. `Delete` Setiap nama metode API dimulai dengan jenis operasi.

   Untuk pola CIDR, Anda dapat memilih untuk menyertakan hanya alamat IP publik, alamat IP pribadi, atau alamat IP yang cocok dengan pola CIDR tertentu.
4. Jika Anda memiliki beberapa filter, pilih opsi Boolean untuk mengatur bagaimana filter tersebut terhubung.



5. Untuk menghapus filter, pilih ikon x di sudut kanan atas.
6. Untuk menghapus semua filter, pilih Hapus filter.

Memilih rentang waktu untuk detail aktivitas

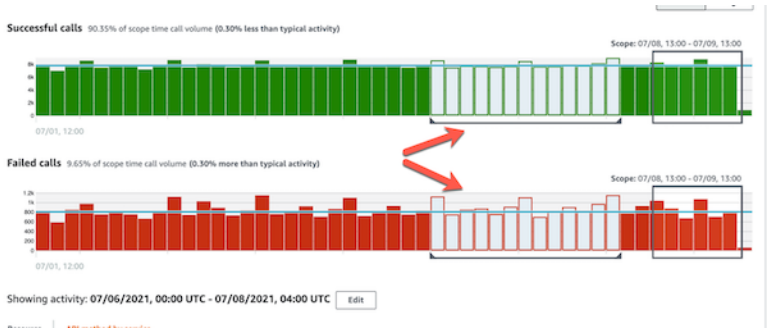
Saat pertama kali menampilkan detail aktivitas, rentang waktu adalah waktu lingkup atau interval waktu yang dipilih. Anda dapat mengubah rentang waktu untuk detail aktivitas.

Untuk mengubah rentang waktu untuk detail aktivitas

1. Pilih Edit.
2. Pada jendela Edit waktu, pilih waktu mulai dan akhir untuk digunakan.

   Untuk mengatur jendela waktu ke waktu cakupan default untuk profil, pilih Setel ke waktu cakupan default.
3. Pilih jendela Perbarui waktu.

Rentang waktu untuk detail aktivitas disorot pada bagan panel profil.



Menanyakan log mentah

Amazon Detective terintegrasi dengan Amazon Security Lake, yang berarti Anda dapat menanyakan dan mengambil data log mentah yang disimpan oleh Security Lake. Untuk detail selengkapnya tentang integrasi ini, lihatIntegrasi dengan Amazon Security Lake.

Dengan menggunakan integrasi ini, Anda dapat mengumpulkan dan menanyakan log dan peristiwa dari sumber berikut yang didukung oleh Security Lake secara native.

- AWS CloudTrail acara manajemen
- Log Aliran Amazon Virtual Private Cloud (Amazon VPC)

> **Note**
>
> Tidak ada biaya tambahan untuk menanyakan log data mentah di Detective. Biaya penggunaan untuk AWS Layanan lain, termasuk Amazon Athena, masih berlaku dengan tarif yang dipublikasikan.

Untuk menanyakan log mentah

1. Pilih detail tampilan untuk waktu lingkup.
2. Dari sini, Anda dapat mulai Query log mentah.
3. Dalam tabel pratinjau log mentah, Anda dapat melihat log dan peristiwa yang diambil dengan menanyakan data dari Security Lake. Untuk detail selengkapnya tentang log peristiwa mentah, Anda dapat melihat data yang ditampilkan di Amazon Athena.

   Dari tabel log mentah kueri, Anda dapat Membatalkan permintaan kueri, Melihat hasil di Amazon Athena, dan Unduh hasil sebagai file nilai yang dipisahkan koma (.csv).

Jika Anda melihat log di Detective, tetapi kueri tidak mengembalikan hasil, itu bisa terjadi karena alasan berikut.

- Log mentah mungkin tersedia di Detective sebelum muncul di tabel log Security Lake. Coba lagi nanti.
- Log mungkin hilang dari Security Lake. Jika Anda menunggu untuk jangka waktu yang lama, ini menunjukkan bahwa log hilang dari Security Lake. Hubungi administrator Security Lake Anda untuk mengatasi masalah ini.

Detail aktivitas untuk geolokasi

Detail aktivitas untuk geolokasi yang baru diamati menunjukkan panggilan API yang dikeluarkan dari geolokasi selama waktu lingkup. Panggilan API mencakup semua panggilan yang dikeluarkan dari geolokasi. Mereka tidak terbatas pada panggilan yang menggunakan entitas temuan atau profil. Untuk bucket S3, panggilan aktivitas adalah panggilan API yang dilakukan ke bucket S3.

Detektif menentukan lokasi permintaan menggunakan database GeoIP MaxMind . MaxMind melaporkan akurasi data mereka yang sangat tinggi di tingkat negara, meskipun akurasi bervariasi sesuai dengan faktor-faktor seperti negara dan jenis IP. Untuk informasi selengkapnya MaxMind, lihat

Geolokasi MaxMind IP. Jika menurut Anda salah satu data GeoIP salah, Anda dapat mengirimkan permintaan koreksi ke Maxmind di Data GeoIP2 MaxMind yang Benar.

Panggilan API dikelompokkan berdasarkan layanan yang mengeluarkan panggilan. Untuk bucket S3, layanan ini selalu Amazon S3. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.

Untuk menampilkan detail aktivitas, lakukan salah satu hal berikut:

- Di peta, pilih geolokasi.
- Dalam daftar, pilih Detail untuk geolokasi.

Detail aktivitas menggantikan daftar geolokasi. Untuk kembali ke daftar geolokasi, pilih Kembali ke semua hasil.

Perhatikan bahwa Detective mulai menyimpan dan menampilkan nama layanan untuk panggilan API per 14 Juli 2021. Untuk aktivitas yang terjadi sebelum tanggal tersebut, nama layanan adalah layanan Tidak Dikenal.

Isi detail aktivitas

Setiap tab memberikan informasi tentang semua panggilan API yang dikeluarkan dari geolokasi selama waktu lingkup.

Untuk setiap alamat IP, sumber daya, dan metode API, daftar menunjukkan jumlah panggilan API yang berhasil dan gagal.

Detail aktivitas berisi tab berikut:

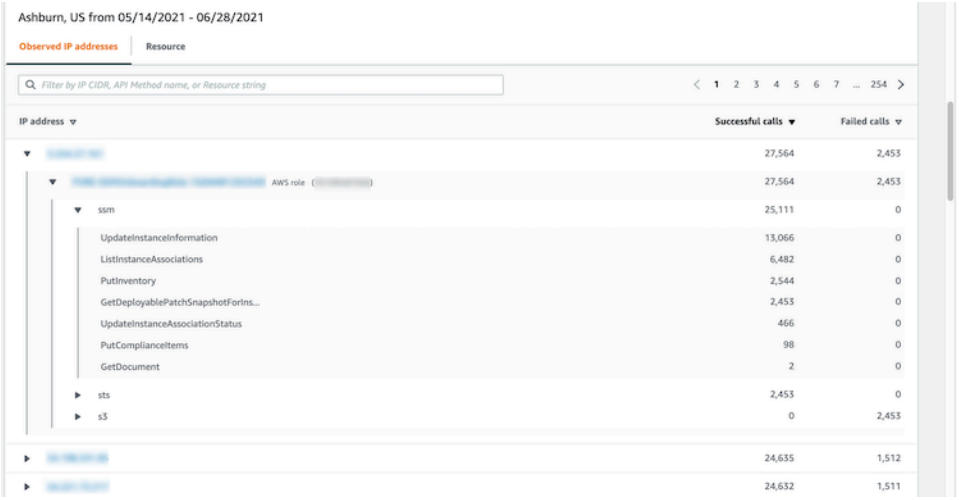
Alamat IP yang diamati

Awalnya menampilkan daftar alamat IP yang digunakan untuk mengeluarkan panggilan API dari geolokasi yang dipilih.

Anda dapat memperluas setiap alamat IP untuk menampilkan sumber daya yang mengeluarkan panggilan API dari alamat IP tersebut. Daftar menampilkan nama sumber daya. Untuk melihat ID utama, arahkan kursor ke nama.

Anda kemudian dapat memperluas setiap sumber daya untuk menampilkan panggilan API tertentu yang dikeluarkan dari alamat IP tersebut oleh sumber daya tersebut. Panggilan API dikelompokkan berdasarkan layanan yang mengeluarkan panggilan. Untuk bucket S3, layanan ini

selalu Amazon S3. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.

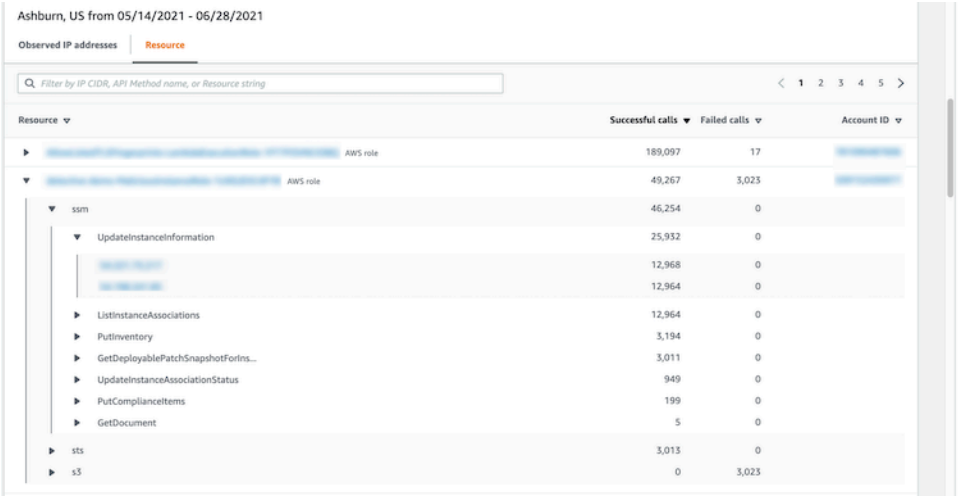


Sumber

Awalnya menampilkan daftar sumber daya yang mengeluarkan panggilan API dari geolokasi yang dipilih. Daftar menampilkan nama sumber daya. Untuk melihat ID utama, jeda pada nama. Untuk setiap sumber daya, tab Sumber Daya juga menampilkan yang terkait Akun AWS.

Anda dapat memperluas setiap pengguna atau peran untuk menampilkan daftar panggilan API yang dikeluarkan oleh sumber daya tersebut. Panggilan API dikelompokkan berdasarkan layanan yang mengeluarkan panggilan. Untuk bucket S3, layanan ini selalu Amazon S3. Jika Detektif tidak dapat menentukan layanan yang mengeluarkan panggilan, panggilan tersebut terdaftar di bawah layanan Tidak Dikenal.

Anda kemudian dapat memperluas setiap panggilan API untuk menampilkan daftar alamat IP dari mana sumber daya mengeluarkan panggilan API.



Menyortir detail aktivitas

Anda dapat mengurutkan detail aktivitas berdasarkan kolom daftar mana pun.

Saat Anda mengurutkan menggunakan kolom pertama, hanya daftar tingkat atas yang diurutkan. Daftar tingkat yang lebih rendah selalu diurutkan berdasarkan jumlah panggilan API yang berhasil.

Memfilter detail aktivitas

Anda dapat menggunakan opsi pemfilteran untuk fokus pada himpunan bagian atau aspek tertentu dari aktivitas yang direpresentasikan dalam detail aktivitas.

Pada semua tab, Anda dapat memfilter daftar dengan salah satu nilai di kolom pertama.

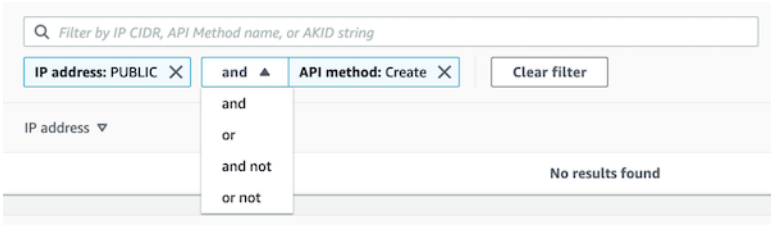
Untuk menambahkan filter

1. Pilih kotak filter.
2. Dari Properties, pilih properti yang akan digunakan untuk penyaringan.
3. Berikan nilai yang akan digunakan untuk penyaringan. Filter mendukung nilai paral. Misalnya, ketika Anda memfilter berdasarkan metode API, jika Anda memfilter menurut**`Instance`**, hasilnya menyertakan operasi API apa pun `Instance` yang memiliki namanya. Jadi keduanya `ListInstanceAssociations` dan `UpdateInstanceInformation` akan cocok.

   Untuk nama layanan, metode API, dan alamat IP, Anda dapat menentukan nilai atau memilih filter bawaan.

   Untuk substring Common API, pilih substring yang mewakili jenis operasi, seperti, `ListCreate`, atau. `Delete` Setiap nama metode API dimulai dengan jenis operasi.

   Untuk pola CIDR, Anda dapat memilih untuk menyertakan hanya alamat IP publik, alamat IP pribadi, atau alamat IP yang cocok dengan pola CIDR tertentu.
4. Jika Anda memiliki beberapa filter, pilih opsi Boolean untuk mengatur bagaimana filter tersebut terhubung.



5. Untuk menghapus filter, pilih ikon x di sudut kanan atas.

6. Untuk menghapus semua filter, pilih Hapus filter.

Detail aktivitas untuk volume aliran VPC secara keseluruhan

Untuk instans EC2, detail aktivitas untuk Volume aliran VPC Keseluruhan menunjukkan interaksi antara instans EC2 dan alamat IP selama rentang waktu yang dipilih.

Untuk pod Kubernetes, Volume aliran VPC secara keseluruhan menampilkan keseluruhan volume byte masuk dan keluar dari alamat IP yang ditetapkan pod Kubernetes untuk semua alamat IP tujuan. Alamat IP pod Kubernetes tidak unik saat. `hostNetwork:true` Dalam hal ini, panel menunjukkan lalu lintas ke pod lain dengan konfigurasi yang sama dan node hosting mereka.

Untuk alamat IP, detail aktivitas untuk Volume aliran VPC Keseluruhan menunjukkan interaksi antara alamat IP dan instans EC2 selama rentang waktu yang dipilih.

Untuk menampilkan detail aktivitas untuk interval waktu tunggal, pilih interval waktu pada bagan.

Untuk menampilkan detail aktivitas untuk waktu lingkup saat ini, pilih detail tampilan untuk waktu lingkup.

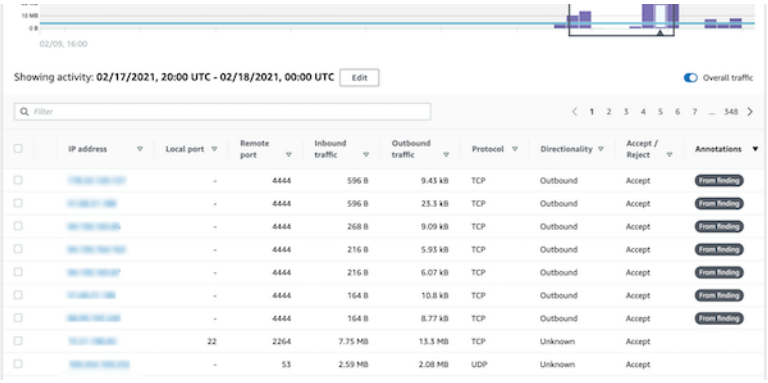
Isi detail aktivitas

Konten mencerminkan aktivitas selama rentang waktu yang dipilih.

Untuk instans EC2, detail aktivitas berisi entri untuk setiap kombinasi unik alamat IP, port lokal, port jarak jauh, protokol, dan arah.

Untuk alamat IP, detail aktivitas berisi entri untuk setiap kombinasi unik instans EC2, port lokal, port jarak jauh, protokol, dan arah.

Setiap entri menampilkan volume lalu lintas masuk, volume lalu lintas keluar, dan apakah permintaan akses diterima atau ditolak. Saat menemukan profil, kolom Anotasi menunjukkan kapan alamat IP terkait dengan temuan saat ini.



Menyortir detail aktivitas

Anda dapat mengurutkan detail aktivitas menurut salah satu kolom dalam tabel.

Secara default, detail aktivitas diurutkan terlebih dahulu berdasarkan anotasi, kemudian oleh lalu lintas masuk.

Memfilter detail aktivitas

Untuk fokus pada aktivitas tertentu, Anda dapat memfilter detail aktivitas dengan nilai berikut:

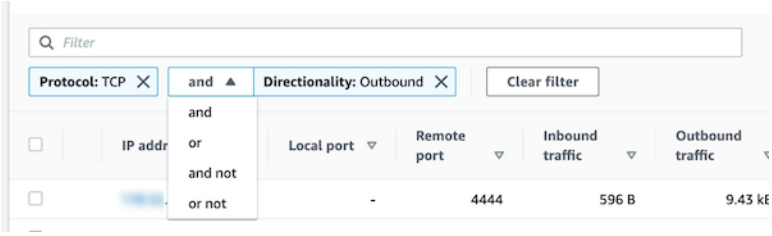
- Alamat IP atau instans EC2
- Port lokal atau jarak jauh
- Arahan
- Protokol
- Apakah permintaan diterima atau ditolak

Untuk menambah dan menghapus filter

1. Pilih kotak filter.
2. Dari Properties, pilih properti yang akan digunakan untuk penyaringan.
3. Berikan nilai yang akan digunakan untuk penyaringan. Filter mendukung nilai paral.

   Untuk memfilter berdasarkan alamat IP, Anda dapat menentukan nilai atau memilih filter bawaan.

   Untuk pola CIDR, Anda dapat memilih untuk menyertakan hanya alamat IP publik, alamat IP pribadi, atau alamat IP yang cocok dengan pola CIDR tertentu.
4. Jika Anda memiliki beberapa filter, pilih opsi Boolean untuk mengatur bagaimana filter tersebut terhubung.



5. Untuk menghapus filter, pilih ikon x di sudut kanan atas.
6. Untuk menghapus semua filter, pilih Hapus filter.

Memilih rentang waktu untuk detail aktivitas

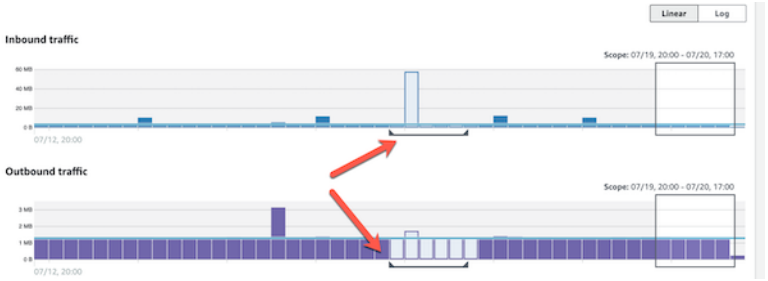
Saat pertama kali menampilkan detail aktivitas, rentang waktu adalah waktu lingkup atau interval waktu yang dipilih. Anda dapat mengubah rentang waktu untuk detail aktivitas.

Untuk mengubah rentang waktu untuk detail aktivitas

1. Pilih Edit.
2. Pada jendela Edit waktu, pilih waktu mulai dan akhir untuk digunakan.

   Untuk mengatur jendela waktu ke waktu cakupan default untuk profil, pilih Setel ke waktu cakupan default.
3. Pilih jendela Perbarui waktu.

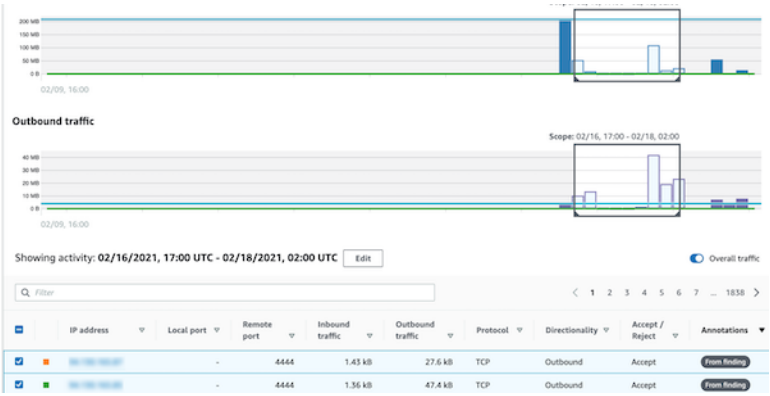
Rentang waktu untuk detail aktivitas disorot pada bagan panel profil.



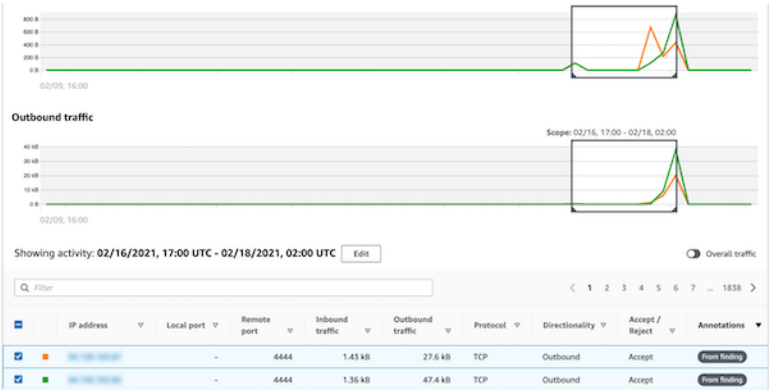
Menampilkan volume lalu lintas untuk baris yang dipilih

Ketika Anda mengidentifikasi baris yang menarik, Anda dapat menampilkan pada grafik utama volume lalu lintas dari waktu ke waktu untuk baris tersebut.

Untuk setiap baris untuk ditambahkan ke grafik, pilih kotak centang. Untuk setiap baris yang dipilih, volume ditampilkan sebagai garis pada grafik masuk atau keluar.



Untuk fokus pada volume lalu lintas untuk entri yang dipilih, Anda dapat menyembunyikan volume keseluruhan. Untuk menampilkan atau menyembunyikan volume lalu lintas keseluruhan, alihkan Lalu lintas keseluruhan.



Menampilkan lalu lintas arus VPC untuk kluster EKS

Detective memiliki visibilitas ke log aliran Amazon Virtual Private Cloud (Amazon VPC) Anda, yang mewakili lalu lintas yang melintasi kluster Amazon Elastic Kubernetes Service (Amazon EKS) Anda. Untuk sumber daya Kubernetes, konten log aliran VPC bergantung pada Container Network Interface (CNI) yang digunakan di cluster EKS.

Kluster EKS dengan konfigurasi default menggunakan plugin Amazon VPC CNI. Untuk detail selengkapnya, lihat Mengelola VPC CNI di Panduan Pengguna Amazon EKS. Plugin Amazon VPC CNI mengirimkan lalu lintas internal dengan alamat IP pod dan menerjemahkan alamat IP sumber ke alamat IP node untuk komunikasi eksternal. Detective dapat menangkap dan menghubungkan lalu lintas internal ke pod yang benar tetapi tidak dapat melakukan hal yang sama untuk lalu lintas eksternal.

Jika Anda ingin Detective memiliki visibilitas ke lalu lintas eksternal pod Anda, aktifkan Terjemahan Alamat Jaringan Sumber Eksternal (SNAT). Mengaktifkan SNAT hadir dengan keterbatasan dan kekurangan. Untuk detail selengkapnya, lihat SNAT untuk pod di Panduan Pengguna Amazon EKS.

Jika Anda menggunakan plugin CNI yang berbeda, Detective memiliki visibilitas terbatas ke pod dengan. `hostNetwork:true` Untuk pod ini, panel VPC Flow menampilkan semua lalu lintas ke alamat IP pod. Ini termasuk lalu lintas ke node host dan pod apa pun pada node dengan `hostNetwork:true` konfigurasi.

Detective menampilkan lalu lintas di panel aliran VPC pod EKS untuk konfigurasi cluster EKS berikut:

- Dalam cluster dengan plugin Amazon VPC CNI, pod apa pun dengan konfigurasi `hostNetwork:false` mengirimkan lalu lintas di dalam VPC cluster.
- Dalam cluster dengan plugin Amazon VPC CNI dan konfigurasi`AWS_VPC_K8S_CNI_EXTERNALSNAT=`**`true`**, pod apa pun dengan `hostNetwork:false` mengirimkan lalu lintas di luar VPC cluster.
- Pod apa pun dengan konfigurasi`hostNetwork:true`. Lalu lintas dari node dicampur dengan lalu lintas dari pod lain yang memiliki konfigurasi`hostNetwork:true`.

Detektif tidak menampilkan lalu lintas di panel aliran VPC untuk:

- Dalam cluster dengan plugin Amazon VPC CNI dan konfigurasi`AWS_VPC_K8S_CNI_EXTERNALSNAT=false`, pod apa pun dengan konfigurasi `hostNetwork:false` mengirimkan lalu lintas di luar VPC cluster.
- Di cluster tanpa plugin Amazon VPC CNI untuk Kubernetes, pod apa pun dengan konfigurasi. `hostNetwork:false`
- Pod apa pun yang mengirimkan lalu lintas ke pod lain yang di-host di node yang sama.

Menampilkan lalu lintas arus VPC untuk VPC Amazon bersama

Detective memiliki visibilitas ke log aliran Amazon Virtual Private Cloud (Amazon VPC) Anda untuk VPC bersama:

- Jika akun anggota Detektif memiliki VPC Amazon bersama dan ada akun Non-Detektif lainnya yang menggunakan VPC bersama, Detective memantau semua lalu lintas dari VPC tersebut, dan memberikan visualisasi pada semua arus lalu lintas dalam VPC.
- Jika Anda memiliki instans Amazon EC2 di dalam VPC Amazon bersama dan pemilik VPC bersama bukan anggota Detektif, Detektif tidak akan memantau lalu lintas apa pun dari VPC. Jika Anda ingin melihat arus lalu lintas dalam VPC, Anda harus menambahkan pemilik Amazon VPC sebagai anggota grafik Detektif Anda.

Keseluruhan aktivitas API Kubernetes yang melibatkan kluster EKS

Detail aktivitas untuk Keseluruhan aktivitas API Kubernetes yang melibatkan kluster EKS menunjukkan jumlah panggilan API Kubernetes yang berhasil dan gagal yang dikeluarkan selama rentang waktu yang dipilih.

Untuk menampilkan detail aktivitas untuk interval waktu tunggal, pilih interval waktu pada bagan.

Untuk menampilkan detail aktivitas untuk waktu lingkup saat ini, pilih Menampilkan detail untuk waktu lingkup.

Isi detail aktivitas (Cluster, pod, pengguna, peran, sesi peran)

Untuk sesi klaster, pod, pengguna, peran, atau peran, detail aktivitas berisi informasi berikut:

- Setiap tab memberikan informasi tentang kumpulan panggilan API yang dikeluarkan selama rentang waktu yang dipilih.

  Untuk cluster, panggilan API terjadi di dalam cluster.

  Untuk pod, panggilan API menargetkan pod.

  Untuk pengguna, peran, dan sesi peran, panggilan API dikeluarkan oleh pengguna Kubernetes yang diautentikasi sebagai pengguna, peran, atau sesi peran tersebut.
- Untuk setiap entri, detail aktivitas menunjukkan jumlah panggilan yang berhasil, gagal, tidak sah, dan terlarang.
- Informasi tersebut mencakup alamat IP, jenis panggilan Kubernetes, entitas yang terpengaruh oleh panggilan, dan subjek (akun layanan atau pengguna) yang melakukan panggilan. Dari detail aktivitas, Anda dapat berputar ke profil untuk alamat IP, subjek, dan entitas yang terpengaruh.

Detail aktivitas berisi tab berikut:

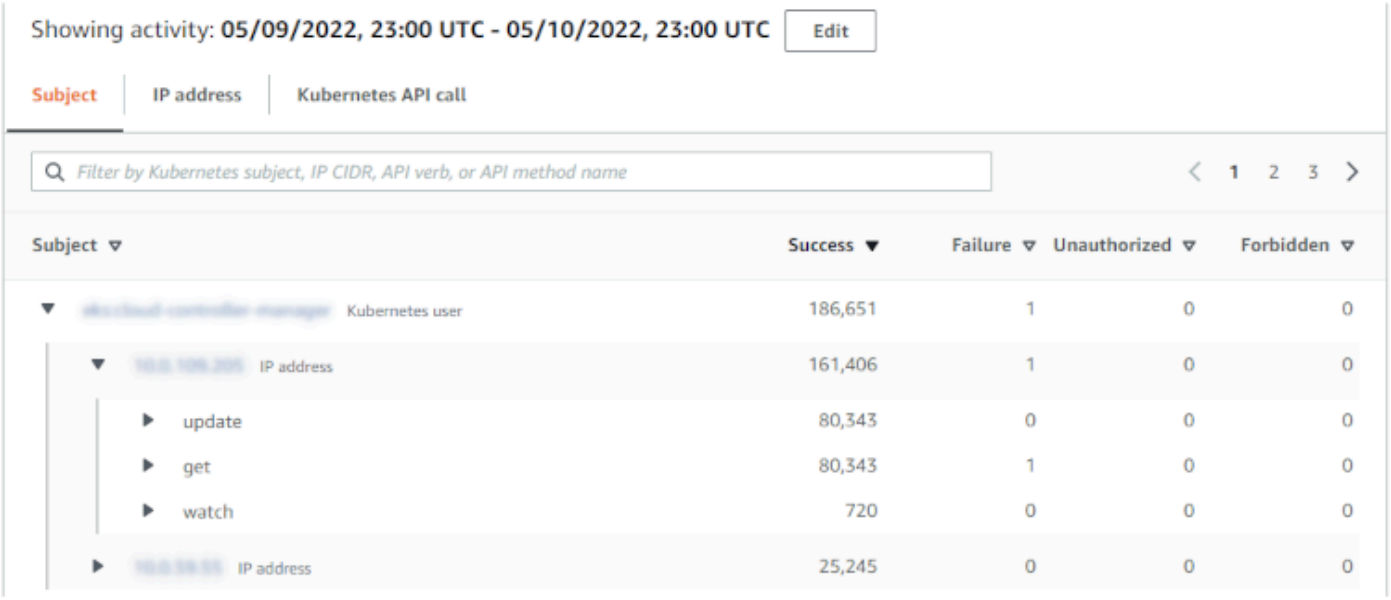
Subjek

Awalnya menampilkan daftar akun layanan dan pengguna yang digunakan untuk melakukan panggilan API.

Anda dapat memperluas setiap akun layanan dan pengguna untuk menampilkan daftar alamat IP dari mana akun atau pengguna melakukan panggilan API.

Anda kemudian dapat memperluas setiap alamat IP untuk menampilkan panggilan API Kubernetes yang dibuat oleh akun tersebut atau pengguna dari alamat IP tersebut.

Perluas panggilan API Kubernetes untuk melihat `requestURI` untuk mengidentifikasi tindakan yang telah dilakukan.



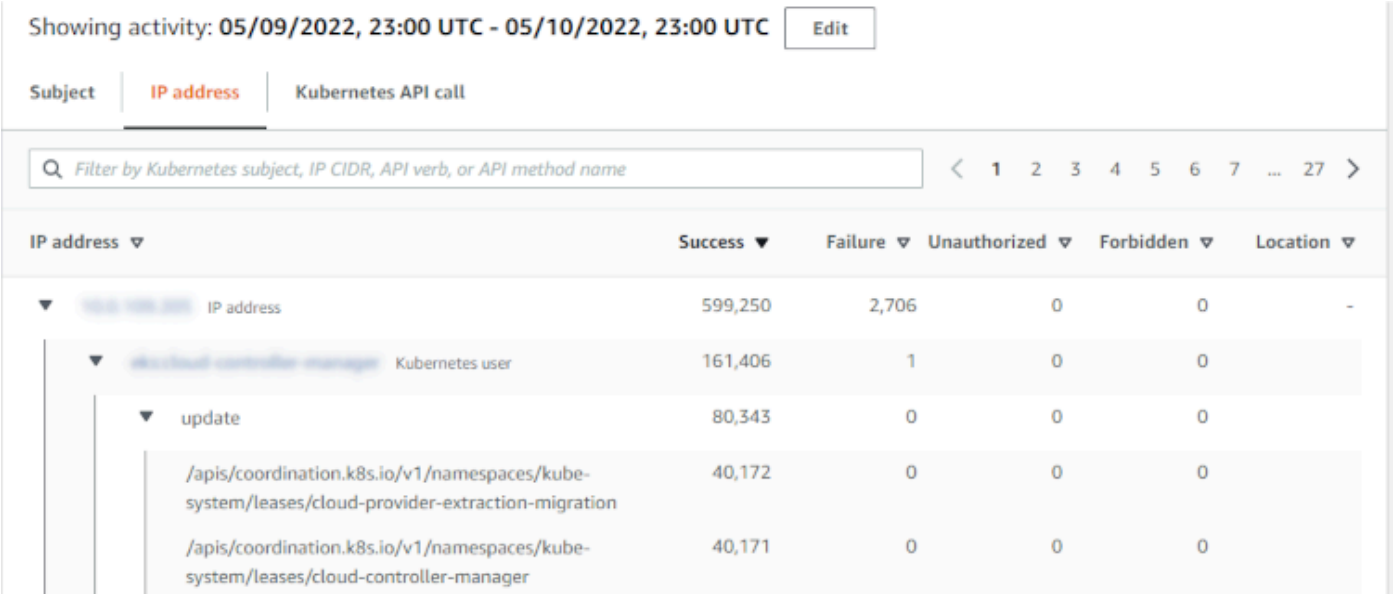
Alamat IP

Awalnya menampilkan daftar alamat IP dari mana panggilan API dibuat.

Anda dapat memperluas setiap panggilan untuk menampilkan daftar subjek Kubernetes (akun layanan dan pengguna) yang melakukan panggilan.

Anda kemudian dapat memperluas setiap subjek ke daftar jenis panggilan API yang dibuat oleh subjek selama waktu cakupan.

Perluas jenis panggilan API untuk melihat requestURI guna mengidentifikasi tindakan yang telah dilakukan.



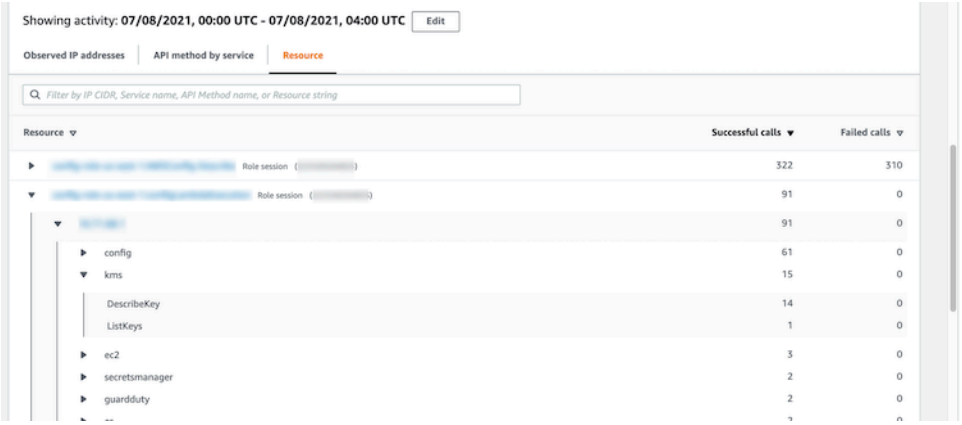
Panggilan API Kubernetes

Awalnya menampilkan daftar kata kerja panggilan API Kubernetes.

Anda dapat memperluas setiap kata kerja API untuk menampilkan requesturis yang terkait dengan tindakan tersebut.

Anda kemudian dapat memperluas setiap requestURI untuk melihat subjek Kubernetes (akun layanan dan pengguna) yang melakukan panggilan API.

Perluas subjek untuk melihat IP mana yang digunakan subjek untuk melakukan panggilan API.



Menyortir detail aktivitas

Anda dapat mengurutkan detail aktivitas berdasarkan kolom daftar mana pun.

Saat Anda mengurutkan menggunakan kolom pertama, hanya daftar tingkat atas yang diurutkan. Daftar tingkat yang lebih rendah selalu diurutkan berdasarkan jumlah panggilan API yang berhasil.

Memfilter detail aktivitas

Anda dapat menggunakan opsi pemfilteran untuk fokus pada himpunan bagian atau aspek tertentu dari aktivitas yang direpresentasikan dalam detail aktivitas.

Pada semua tab, Anda dapat memfilter daftar dengan salah satu nilai di kolom pertama.

Memilih rentang waktu untuk detail aktivitas

Saat pertama kali menampilkan detail aktivitas, rentang waktu adalah waktu lingkup atau interval waktu yang dipilih. Anda dapat mengubah rentang waktu untuk detail aktivitas.

Untuk mengubah rentang waktu untuk detail aktivitas

1. Pilih Edit.
2. Pada jendela Edit waktu, pilih waktu mulai dan akhir untuk digunakan.

   Untuk mengatur jendela waktu ke waktu cakupan default untuk profil, pilih Setel ke waktu cakupan default.
3. Pilih jendela Perbarui waktu.

Rentang waktu untuk detail aktivitas disorot pada bagan panel profil.

Menggunakan panduan panel profil selama investigasi

Setiap panel profil dirancang untuk memberikan jawaban atas pertanyaan spesifik yang muncul saat Anda melakukan penyelidikan dan menganalisis aktivitas untuk entitas terkait.

Panduan yang diberikan untuk setiap panel profil membantu Anda menemukan jawaban ini.

Panduan panel profil dimulai dengan satu kalimat pada panel itu sendiri. Panduan ini memberikan penjelasan singkat tentang data yang disajikan di panel.

Untuk menampilkan panduan yang lebih rinci untuk panel, pilih Info lebih lanjut dari judul panel. Panduan tambahan ini muncul di panel bantuan.

Panduan ini dapat memberikan jenis informasi ini:

- Ikhtisar konten panel
- Cara menggunakan panel untuk menjawab pertanyaan yang relevan
- Langkah selanjutnya yang disarankan berdasarkan jawaban

Menavigasi langsung ke profil entitas atau menemukan ikhtisar

Untuk menavigasi langsung ke profil entitas atau menemukan ikhtisar di Amazon Detective, Anda dapat menggunakan salah satu opsi ini.

- Dari Amazon GuardDuty atau AWS Security Hub, Anda dapat beralih dari GuardDuty temuan ke profil pencarian Detektif yang sesuai.
- Anda dapat merakit URL Detektif yang mengidentifikasi temuan atau entitas dan menetapkan waktu lingkup untuk digunakan.

Berputar ke profil entitas atau menemukan ikhtisar dari Amazon atau GuardDuty AWS Security Hub

Dari GuardDuty konsol Amazon, Anda dapat menavigasi ke profil entitas untuk entitas yang terkait dengan temuan.

Dari AWS Security Hub konsol GuardDuty dan, Anda juga dapat menavigasi ke ikhtisar temuan. Ini juga menyediakan tautan ke profil entitas untuk entitas yang terlibat.

Tautan ini dapat membantu merampingkan proses investigasi. Anda dapat dengan cepat menggunakan Detective untuk melihat aktivitas entitas terkait dan menentukan langkah selanjutnya. Anda kemudian dapat mengarsipkan temuan jika itu positif palsu atau mengeksplorasi lebih lanjut untuk menentukan ruang lingkup masalah.

Cara berputar ke konsol Detektif Amazon

Tautan investigasi tersedia untuk semua GuardDuty temuan. GuardDuty juga memungkinkan Anda untuk memilih apakah akan menavigasi ke profil entitas atau ke ikhtisar temuan.

Untuk beralih ke Detective dari konsol GuardDuty

1. Buka GuardDuty konsol di https://console.aws.amazon.com/guardduty/.
2. Jika perlu, pilih Temuan di panel navigasi kiri.
3. Pada halaman GuardDuty Temuan, pilih temuan.

   Panel rincian temuan ditampilkan di sebelah kanan daftar temuan.
4. Pada panel Finding Details, pilih Investigate in Detective.

   GuardDuty menampilkan daftar item yang tersedia untuk diselidiki di Detective.

   Daftar ini berisi entitas terkait, seperti alamat IP atau instans EC2, dan temuan.
5. Pilih entitas atau temuan.

   Konsol Detektif terbuka di tab baru. Konsol terbuka ke entitas atau menemukan profil.

   Jika Anda belum mengaktifkan Detective, maka konsol terbuka ke halaman arahan yang memberikan ikhtisar Detective. Dari sana, Anda dapat memilih untuk mengaktifkan Detektif.

Untuk beralih ke Detective dari konsol Security Hub

1. Buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Jika perlu, pilih Temuan di panel navigasi kiri.
3. Pada halaman Temuan Security Hub, pilih GuardDuty temuan.
4. Di panel detail, pilih Selidiki di Detektif dan kemudian pilih Selidiki temuan.

   Saat Anda memilih Selidiki temuan, konsol Detektif akan terbuka di tab baru. Konsol terbuka untuk ikhtisar temuan.

   Konsol Detektif selalu terbuka ke Wilayah tempat temuan itu berasal, bahkan jika Anda berputar dari Wilayah agregasi Anda. Untuk informasi selengkapnya tentang menemukan agregasi, lihat Mengagregasi temuan di seluruh Wilayah di Panduan Pengguna.AWS Security Hub

Jika Anda belum mengaktifkan Detektif, konsol terbuka ke halaman arahan Detektif. Dari sana, Anda dapat mengaktifkan Detektif.

Memecahkan masalah pivot

Untuk menggunakan pivot, salah satu dari berikut ini harus benar:

- Akun Anda harus merupakan akun administrator untuk Detektif dan layanan tempat Anda berputar.
- Anda telah mengambil peran lintas akun yang memberi Anda akses akun administrator ke grafik perilaku.

Untuk informasi selengkapnya tentang rekomendasi untuk menyelaraskan akun administrator, lihat Penyelarasan yang disarankan dengan Amazon GuardDuty dan. AWS Security Hub

Jika pivot tidak berfungsi, periksa yang berikut ini.

- Apakah temuan tersebut milik akun anggota yang diaktifkan dalam grafik perilaku Anda? Jika akun terkait tidak diundang ke grafik perilaku sebagai akun anggota, maka grafik perilaku tidak berisi data untuk akun tersebut.

  Jika akun anggota yang diundang tidak menerima undangan, maka grafik perilaku tidak berisi data untuk akun tersebut.
- Apakah temuan itu diarsipkan? Detektif tidak menerima temuan yang diarsipkan dari. GuardDuty
- Apakah temuan itu terjadi sebelum Detektif mulai menyerap data ke dalam grafik perilaku Anda? Jika temuan tidak ada dalam data yang dicerna Detective, maka grafik perilaku tidak berisi data untuk itu.
- Apakah temuan dari Wilayah yang benar? Setiap grafik perilaku khusus untuk Wilayah. Grafik perilaku tidak berisi data dari Wilayah lain.

Menavigasi ke profil entitas atau menemukan ikhtisar menggunakan URL

Untuk menavigasi ke profil entitas atau menemukan ikhtisar di Amazon Detective, Anda dapat menggunakan URL yang menyediakan tautan langsung ke sana. URL mengidentifikasi temuan atau entitas. Itu juga dapat menentukan ruang lingkup waktu untuk digunakan pada profil. Detective mempertahankan data peristiwa historis hingga satu tahun.

Format URL profil

> **Note**
>
> Jika Anda menggunakan format URL lama, Detective akan secara otomatis mengalihkan ke URL baru. Format URL yang lama adalah: *https://console.aws.amazon.com/detective/home?region = Wilayah # ketik/namespace/instanceId? parameter*

Format baru URL profil adalah sebagai berikut:

- *Untuk entitas - https://console.aws.amazon.com/detective/home?region = Wilayah # entitas/namespace/instanceId? parameter*
- Untuk temuan - https://console.aws.amazon.com/detective/home?region = *Region* # *temuan/InstanceId*? *parameter*

URL membutuhkan nilai-nilai berikut.

Wilayah

Wilayah yang ingin Anda gunakan.

jenis

Jenis item untuk profil yang Anda navigasikan.

- `entities`- Menunjukkan bahwa Anda sedang menavigasi ke profil entitas
- `findings`- Menunjukkan bahwa Anda sedang menavigasi ke ikhtisar temuan

namespace

Untuk entitas, namespace adalah nama dari tipe entitas.

- `AwsAccount`
- `AwsRole`
- `AwsRoleSession`
- `AwsUser`
- `Ec2Instance`

- `FederatedUser`
- `IpAddress`
- `S3Bucket`
- `UserAgent`
- `FindingGroup`
- `KubernetesSubject`
- `ContainerPod`
- `ContainerCluster`
- `ContainerImage`

`InstanceID`

Instance identifier dari temuan atau entitas.

- Untuk GuardDuty temuan, pengidentifikasi GuardDuty temuan.
- Untuk AWS akun, ID akun.
- Untuk AWS peran dan pengguna, ID utama peran atau pengguna.
- Untuk pengguna federasi, ID utama pengguna federasi. ID utama adalah salah satu *<identityProvider>*:*<username>* atau*<identityProvider>*:*<audience>*:*<username>*.
- Untuk alamat IP, alamat IP.
- Untuk agen pengguna, nama agen pengguna.
- Untuk instans EC2, ID instance.
- Untuk sesi peran, pengidentifikasi sesi. Pengidentifikasi sesi menggunakan format *<rolePrincipalID>*:*<sessionName>*.
- Untuk ember S3, nama bucket.
- Untuk FindingGroups, UUID. misalnya, `ca6104bc-a315-4b15-bf88-1c1e60998f83`
- Untuk sumber daya EKS, gunakan format berikut:
  - Kluster EKS: *~ ~EKS* <clusterName><accountId>
  - *Kubernetes Pod: ~ ~EKS* <podUid><clusterName><accountId>
  - *Subjek Kubernetes: ~ ~* <subjectName><clusterName><accountId>
  - Gambar kontainer:*/: @* <registry><repository><tag><digest>

Temuan atau entitas harus dikaitkan dengan akun yang diaktifkan dalam grafik perilaku Anda.

URL juga dapat menyertakan parameter opsional berikut, yang digunakan untuk mengatur waktu lingkup. Untuk informasi selengkapnya tentang waktu lingkup dan cara penggunaannya pada profil, lihatthe section called “Mengelola ruang lingkup waktu”.

`scopeStart`

Waktu mulai untuk ruang lingkup waktu untuk digunakan pada profil. Waktu mulai harus dalam 365 hari terakhir.

Nilainya adalah stempel waktu zaman.

Jika Anda memberikan waktu mulai tetapi tidak ada waktu akhir, maka waktu lingkup berakhir pada waktu saat ini.

`scopeEnd`

Waktu akhir untuk ruang lingkup waktu untuk digunakan pada profil.

Nilainya adalah stempel waktu zaman.

Jika Anda memberikan waktu akhir, tetapi tidak ada waktu mulai, maka waktu lingkup mencakup semua waktu sebelum waktu akhir.

Jika Anda tidak menentukan waktu lingkup, maka waktu lingkup default digunakan.

- Untuk temuan, waktu lingkup default menggunakan waktu pertama dan terakhir bahwa aktivitas temuan diamati.
- Untuk entitas, waktu lingkup default adalah 24 jam sebelumnya.

Berikut adalah contoh URL Detektif:

```
https://console.aws.amazon.com/detective/home?region=us-east-1#entities/
IpAddress/192.168.1.1?scopeStart=1552867200&scopeEnd=1552910400
```

URL contoh ini memberikan instruksi berikut.

- Tampilkan profil entitas untuk alamat IP 192.168.1.
- Gunakan lingkup waktu yang dimulai Senin, 18 Maret 2019 12:00:00 GMT dan yang berakhir Senin, 18 Maret 2019 12:00:00 GMT.

Memecahkan masalah URL

Jika URL tidak menampilkan profil yang diharapkan, periksa dulu apakah URL menggunakan format yang benar dan Anda telah memberikan nilai yang benar.

- Apakah Anda memulai dengan URL yang benar (`findingsataueentities`)?
- Apakah Anda menentukan namespace yang benar?
- Apakah Anda memberikan pengenal yang benar?

Jika nilainya benar, maka Anda juga dapat memeriksa yang berikut ini.

- Apakah temuan atau entitas milik akun anggota yang diaktifkan dalam grafik perilaku Anda? Jika akun terkait tidak diundang ke grafik perilaku sebagai akun anggota, maka grafik perilaku tidak berisi data untuk akun tersebut.

  Jika akun anggota yang diundang tidak menerima undangan, maka grafik perilaku tidak berisi data untuk akun tersebut.
- Untuk temuan, apakah temuan itu diarsipkan? Detektif tidak menerima temuan yang diarsipkan dari Amazon. GuardDuty
- Apakah temuan atau entitas terjadi sebelum Detektif mulai menyerap data ke dalam grafik perilaku Anda? Jika temuan atau entitas tidak ada dalam data yang dicerna Detective, maka grafik perilaku tidak berisi data untuk itu.
- Apakah temuan atau entitas dari Wilayah yang benar? Setiap grafik perilaku khusus untuk Wilayah. Grafik perilaku tidak berisi data dari Wilayah lain.

Menambahkan URL Detektif untuk temuan ke Splunk

Proyek Splunk Trumpet memungkinkan Anda mengirim data dari AWS layanan ke Splunk.

Anda dapat mengonfigurasi proyek Trumpet untuk menghasilkan URL Detektif untuk temuan Amazon. GuardDuty Anda kemudian dapat menggunakan URL ini untuk berputar langsung dari Splunk ke profil pencarian Detektif yang sesuai.

Proyek Trumpet tersedia dari https://github.com/splunk/ GitHub . splunk-aws-project-trumpet

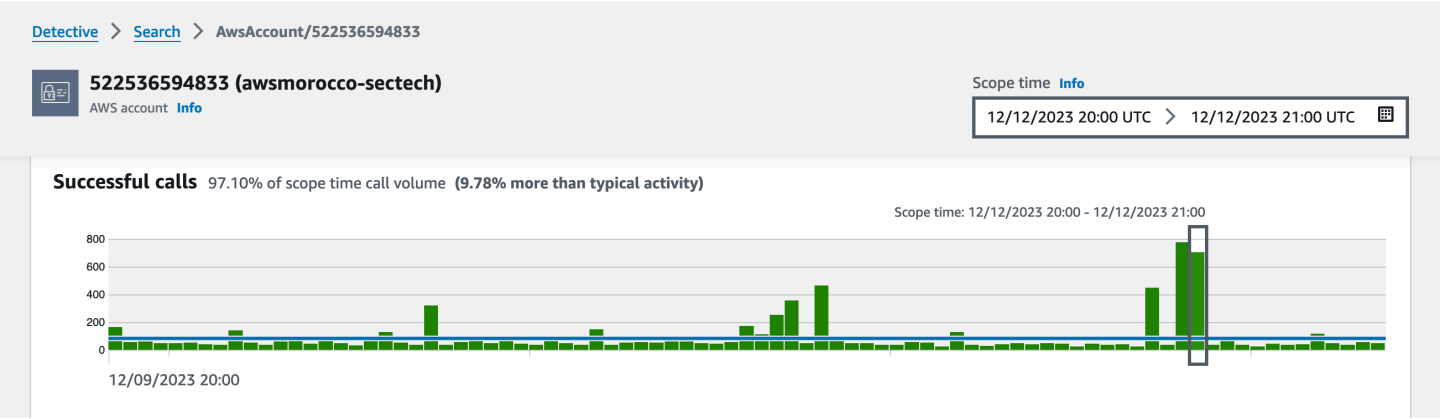
Pada halaman konfigurasi untuk proyek Trumpet, dari AWS CloudWatch Acara, pilih URL Detektif. GuardDuty

Menavigasi dalam profil

Profil entitas berisi satu set tab atau lebih. Setiap tab berisi satu atau lebih panel profil. Setiap panel profil berisi teks dan visualisasi yang dihasilkan dari data grafik perilaku.

Saat Anda menggulir ke bawah melalui tab profil, informasi berikut tetap terlihat di bagian atas profil:

- Jenis entitas
- Pengidentifikasi entitas
- Lingkup waktu



Mengelola ruang lingkup waktu

Sesuaikan waktu lingkup yang digunakan untuk membatasi data yang ditampilkan pada profil entitas.

Bagan, garis waktu, dan data lain yang ditampilkan pada profil entitas semuanya didasarkan pada waktu lingkup saat ini. Waktu lingkup adalah ringkasan aktivitas untuk suatu entitas dari waktu ke waktu. Ini muncul di kanan atas setiap profil di konsol Detektif Amazon. Data yang ditampilkan pada bagan, garis waktu, dan visualisasi lainnya didasarkan pada waktu lingkup. Untuk beberapa panel profil, waktu tambahan ditambahkan sebelum dan sesudah waktu lingkup untuk memberikan konteks. Di Detective, semua stempel waktu ditampilkan di UTC secara default. Anda dapat memilih zona waktu lokal Anda dengan mengubah preferensi Timestamp. Untuk memperbarui preferensi Timestamp, lihat. the section called “Mengatur format stempel waktu”

Detective analytics menggunakan scope time saat memeriksa aktivitas yang tidak biasa. Proses analitik mendapatkan aktivitas selama waktu lingkup, kemudian membandingkannya dengan

aktivitas selama 45 hari sebelum waktu lingkup. Ini juga menggunakan kerangka waktu 45 hari untuk menghasilkan garis dasar aktivitas.

Pada ikhtisar temuan, waktu lingkup mencerminkan pertama dan terakhir kali temuan diamati. Untuk informasi selengkapnya tentang menemukan ikhtisar, lihatthe section called “Menemukan ikhtisar”.

Saat Anda mengerjakan investigasi, Anda dapat menyesuaikan waktu lingkup. Misalnya, jika analisis asli didasarkan pada aktivitas dari satu hari, Anda mungkin ingin mengembangkannya menjadi satu minggu atau sebulan. Periode yang diperluas dapat membantu Anda mendapatkan pemahaman yang lebih baik apakah aktivitas tersebut sesuai dengan pola normal atau tidak biasa.

Anda juga dapat mengatur waktu cakupan agar sesuai dengan temuan terkait untuk entitas saat ini.

Saat Anda mengubah waktu lingkup, Detective mengulangi analisisnya dan memperbarui data yang ditampilkan berdasarkan waktu lingkup baru.

Waktu lingkup tidak boleh lebih pendek dari satu jam dan tidak lebih dari satu tahun. Waktu mulai dan berakhir harus pada satu jam.

Menetapkan tanggal dan waktu mulai dan berakhir tertentu

Anda dapat mengatur tanggal mulai dan berakhir waktu lingkup dari konsol Detektif.

Untuk mengatur waktu mulai dan akhir tertentu untuk waktu lingkup baru

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Pada profil entitas, pilih waktu lingkup.
3. Pada panel Edit ruang lingkup waktu, di bawah Mulai, pilih tanggal dan waktu mulai baru untuk waktu lingkup. Untuk waktu mulai yang baru, Anda memilih jam saja.
4. Di bawah Akhir, pilih tanggal dan waktu akhir yang baru untuk waktu lingkup. Untuk akhir waktu yang baru, Anda hanya memilih jam. Waktu akhir harus setidaknya satu jam lebih lambat dari waktu mulai.
5. Setelah selesai mengedit, untuk menyimpan perubahan dan memperbarui data yang ditampilkan, pilih Perbarui waktu lingkup.

Edit lamanya waktu untuk ruang lingkup waktu

Saat Anda menetapkan panjang waktu lingkup, Detective menetapkan waktu lingkup ke jumlah waktu tersebut dari waktu saat ini.

Untuk mengedit panjang waktu untuk ruang lingkup waktu

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Pada profil entitas, pilih waktu lingkup.
3. Pada panel Edit ruang lingkup waktu, di sebelah Historis, pilih lamanya waktu untuk ruang lingkup waktu.

   Menentukan rentang waktu memperbarui pengaturan Mulai dan Akhir.
4. Setelah selesai mengedit, untuk menyimpan perubahan dan memperbarui data yang ditampilkan, pilih Perbarui waktu lingkup.

Mengatur waktu lingkup ke jendela waktu pencarian

Setiap temuan memiliki jendela waktu terkait, yang mencerminkan kali pertama dan terakhir temuan itu diamati. Saat Anda melihat ikhtisar temuan, waktu lingkup berubah ke jendela waktu pencarian.

Dari profil entitas, Anda dapat menyelaraskan waktu lingkup ke jendela waktu untuk temuan terkait. Ini memungkinkan Anda untuk menyelidiki aktivitas yang terjadi selama waktu itu.

Untuk menyelaraskan waktu lingkup ke jendela waktu pencarian, pada panel temuan terkait, pilih temuan yang ingin Anda gunakan.

Detective mengisi rincian temuan dan menetapkan waktu lingkup ke jendela waktu pencarian.

Mengatur waktu lingkup pada halaman ringkasan

Saat Anda meninjau halaman Ringkasan, Anda dapat menyesuaikan waktu Cakupan untuk melihat aktivitas untuk kerangka waktu 24 jam dalam 365 hari sebelumnya.

Untuk mengatur waktu lingkup pada halaman Ringkasan

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Ringkasan.
3. Pada panel Waktu lingkup, di samping Ringkasan, Anda dapat mengubah tanggal dan waktu mulai. Waktu mulai harus dalam 365 hari terakhir.

   Saat Anda mengubah tanggal dan waktu Mulai, tanggal dan waktu Berakhir secara otomatis diperbarui menjadi 24 jam setelah waktu mulai yang Anda pilih.

> **Note**
>
> Dengan Detective, Anda dapat mengakses data peristiwa historis hingga satu tahun. Untuk informasi selengkapnya tentang data sumber di Detektif, lihat Sumber data yang digunakan dalam grafik perilaku.

4. Setelah selesai mengedit, untuk menyimpan perubahan dan memperbarui data yang ditampilkan, pilih Perbarui waktu lingkup.

Melihat detail untuk temuan terkait

Setiap profil entitas berisi panel temuan terkait yang mencantumkan temuan yang melibatkan entitas selama waktu lingkup saat ini. Salah satu indikasi bahwa suatu entitas telah dikompromikan adalah keterlibatannya dalam berbagai temuan. Jenis-jenis temuan juga dapat memberikan wawasan tentang jenis kegiatan yang harus diperhatikan.

Panel temuan terkait ditampilkan tepat di bawah panel profil detail entitas.

Untuk setiap temuan, tabel mencakup informasi berikut:

- Judul temuan, yang juga merupakan tautan ke ikhtisar temuan.
- AWS Akun yang terkait dengan temuan, yang juga merupakan tautan ke profil akun
- Jenis temuan
- Waktu paling awal temuan itu diamati
- Waktu terbaru bahwa temuan itu diamati
- Keparahan temuan

Untuk menampilkan detail temuan untuk temuan, pilih tombol radio untuk temuan tersebut. Detective mengisi panel rincian temuan di sebelah kanan halaman. Detective juga mengubah ruang lingkup waktu menjadi jendela waktu pencarian. Ini memungkinkan Anda untuk fokus pada aktivitas yang terjadi selama waktu itu.

Jika Anda menavigasi ke profil entitas dari ikhtisar temuan, maka temuan itu dipilih secara otomatis dan detail untuk temuan ditampilkan.

Dari detail temuan, untuk menavigasi kembali ke ikhtisar temuan, pilih Lihat semua entitas terkait.

Anda juga dapat mengarsipkan temuan. Lihat the section called “Mengarsipkan temuan GuardDuty ”.

Melihat detail untuk entitas volume tinggi

Dalam grafik perilaku, Amazon Detective melacak hubungan antar entitas. Misalnya, setiap grafik perilaku melacak saat AWS pengguna membuat AWS peran dan ketika instans EC2 terhubung ke alamat IP.

Ketika suatu entitas memiliki terlalu banyak hubungan selama periode waktu tertentu, Detektif tidak dapat menyimpan semua hubungan. Ketika ini terjadi selama waktu lingkup saat ini, Detektif memberi tahu Anda. Detective juga menyediakan daftar kemunculan entitas volume tinggi.

Apa itu entitas volume tinggi?

Selama interval waktu tertentu, entitas mungkin merupakan asal atau tujuan dari sejumlah besar koneksi. Misalnya, instans EC2 mungkin memiliki koneksi dari jutaan alamat IP.

Detective mempertahankan batas jumlah koneksi yang dapat ditampung selama setiap interval waktu. Jika entitas melebihi batas itu, maka Detective membuang koneksi untuk interval waktu tersebut.

Misalnya, asumsikan bahwa batasnya adalah 100.000.000 koneksi per interval waktu. Jika instans EC2 terhubung dengan lebih dari 100.000.000 alamat IP selama interval waktu, maka Detective membuang koneksi dari interval waktu tersebut.

Namun, Anda mungkin dapat menganalisis aktivitas tersebut berdasarkan entitas di ujung lain hubungan. Untuk melanjutkan contoh, sementara instans EC2 mungkin terhubung dari jutaan alamat IP, satu alamat IP terhubung ke instans EC2 yang jauh lebih sedikit. Setiap profil alamat IP memberikan rincian tentang instans EC2 yang terhubung dengan alamat IP.

Melihat notifikasi entitas volume tinggi di profil

Detective menampilkan pemberitahuan di bagian atas temuan atau profil entitas jika waktu lingkup mencakup interval waktu di mana entitas bervolume tinggi. Untuk menemukan profil, pemberitahuan adalah untuk entitas yang terlibat.

Pemberitahuan tersebut mencakup daftar hubungan yang memiliki interval waktu volume tinggi. Setiap entri daftar berisi deskripsi hubungan dan awal interval waktu volume tinggi.

Interval waktu volume tinggi mungkin merupakan indikator aktivitas yang mencurigakan. Untuk memahami aktivitas lain apa yang terjadi pada saat yang sama, Anda dapat memfokuskan

penyelidikan Anda pada interval waktu volume tinggi. Pemberitahuan entitas volume tinggi mencakup opsi untuk mengatur waktu lingkup ke interval waktu tersebut.

Untuk mengatur waktu lingkup ke interval waktu volume tinggi

1. Dalam pemberitahuan entitas volume tinggi, pilih interval waktu.
2. Pada menu pop-up, pilih Terapkan waktu lingkup.

Melihat daftar entitas volume tinggi untuk waktu lingkup saat ini

Halaman entitas bervolume tinggi berisi daftar interval waktu volume tinggi dan entitas selama waktu lingkup saat ini.

Untuk menampilkan halaman entitas Volume tinggi

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Entitas volume tinggi.

Setiap entri dalam daftar berisi informasi berikut:

- Awal interval waktu volume tinggi
- Pengidentifikasi dan jenis entitas
- Deskripsi hubungan, seperti “instans EC2 terhubung dari alamat IP”

Anda dapat memfilter dan mengurutkan daftar berdasarkan kolom mana pun. Anda juga dapat menavigasi ke profil entitas untuk entitas yang terlibat.

Untuk menavigasi ke profil untuk entitas

1. Dalam daftar Entitas volume tinggi, pilih baris yang akan dinavigasi.
2. Pilih Lihat profil dengan waktu lingkup volume tinggi.

Saat Anda menggunakan opsi ini untuk menavigasi ke profil entitas, waktu cakupan ditetapkan sebagai berikut:

- Waktu lingkup dimulai 30 hari sebelum interval waktu volume tinggi.
- Waktu lingkup berakhir pada akhir interval waktu volume tinggi.

Mengelola temuan dan entitas

Amazon Detective menawarkan beberapa fitur penting untuk membantu Anda mencari, mengekspor, dan mengelola temuan Anda. Fitur-fitur ini akan membantu Anda menyesuaikan temuan dengan lingkungan spesifik Anda, mengurangi kebisingan dari temuan bernilai rendah, dan membantu Anda fokus pada ancaman terhadap AWS lingkungan unik Anda. Tinjau topik di halaman ini untuk memahami bagaimana Anda dapat menggunakan fitur ini untuk meningkatkan nilai temuan Detektif.

Konten

Mencari temuan atau entitas

Dengan fungsi pencarian Detektif Amazon, Anda dapat mencari temuan atau entitas. Dari hasil penelusuran, Anda dapat menavigasi ke profil entitas atau ikhtisar temuan. Jika pencarian Anda menghasilkan lebih dari 10.000 hasil, hanya 10.000 hasil teratas yang ditampilkan. Mengubah urutan penyortiran mengubah hasil yang dikembalikan.

Anda dapat mengekspor hasil pencarian Anda ke file nilai yang dipisahkan koma (.csv). File ini berisi data yang dikembalikan di halaman pencarian. Untuk informasi selengkapnya, lihat the section called “Mengekspor data dari Detective”.

Menyelesaikan pencarian

Untuk menyelesaikan pencarian, pilih jenis entitas yang akan dicari. Kemudian berikan pengenal atau pengidentifikasi yang tepat dengan karakter wildcard atau. * ? Untuk mencari berbagai alamat IP, Anda juga dapat menggunakan CIDR atau notasi titik. Lihat contoh string pencarian berikut.

Untuk alamat IP:

- `1.0.*.*`
- `1.0.133.*`
- `1.0.0.0/16`
- `0.239.48.198/31`

Untuk semua jenis entitas lainnya:

- `Admin`
- `ad*`
- `ad*n`
- `ad*n*`
- `adm?n`
- `a?m*`
- `*min`

Untuk setiap jenis entitas, pengidentifikasi berikut didukung:

- Untuk Temuan, pengidentifikasi temuan atau menemukan Amazon Resource Name (ARN).
- Untuk AWS akun, ID akun.
- Untuk AWS peran dan AWS pengguna, baik ID utama, nama, atau ARN.
- Untuk cluster Container, nama cluster atau ARN.
- Untuk gambar Container, repositori atau intisari penuh dari gambar kontainer.
- Untuk Container Pod atau Tasks, nama pod atau UID pod.
- Untuk instans EC2, pengidentifikasi instans atau ARN.
- Untuk Menemukan grup, pengidentifikasi grup pencarian.
- Untuk alamat IP, alamat dalam CIDR atau notasi titik.
- Untuk subjek Kubernetes (akun layanan atau pengguna), namanya.
- Untuk sesi peran, Anda dapat menggunakan salah satu nilai berikut untuk mencari:
  - Pengidentifikasi sesi peran.

    Pengidentifikasi sesi peran menggunakan format*<rolePrincipalID>*`:`*<sessionName>*.

    Ini contohnya: `AROA12345678910111213:MySession` .
  - Sesi peran ARN
  - Nama sesi
  - ID Utama dari peran yang diasumsikan
  - Nama peran yang diasumsikan

- Untuk ember S3, nama bucket atau bucket ARN.
- Untuk pengguna federasi, ID utama atau nama pengguna. ID utama adalah salah satu *<identityProvider>*:*<username>* atau*<identityProvider>*:*<audience>*:*<username>*.
- Untuk agen pengguna, nama agen pengguna.

Untuk mencari temuan atau entitas

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Cari.
3. Dari menu Pilih jenis, pilih jenis item yang Anda cari.

   Perhatikan bahwa ketika Anda memilih Pengguna, Anda dapat mencari AWS pengguna atau pengguna gabungan.

   Contoh dari data Anda berisi kumpulan sampel pengenal dari jenis yang dipilih yang ada dalam data grafik perilaku Anda. Untuk menampilkan profil untuk salah satu contoh, pilih pengenalnya.
4. Masukkan pengenal yang tepat atau pengenal dengan karakter wildcard untuk dicari.

   Pencarian tidak peka huruf besar/kecil.
5. Pilih Cari atau tekan Enter.

Menggunakan hasil pencarian

Saat Anda menyelesaikan pencarian, Detective menampilkan daftar hingga 10.000 hasil yang cocok. Untuk pencarian yang menggunakan pengenal unik, hanya ada satu hasil yang cocok.

Dari hasil, untuk menavigasi ke profil entitas atau menemukan ikhtisar, pilih pengenal.

Untuk temuan, peran, pengguna, dan instans EC2, hasil pencarian menyertakan akun terkait. Untuk menavigasi ke profil akun, pilih pengenal akun.

Memecahkan masalah pencarian

Jika Detektif tidak menemukan temuan atau entitas, periksa terlebih dahulu apakah Anda memasukkan pengenal yang benar. Jika pengenal benar, Anda juga dapat memeriksa yang berikut ini.

- Apakah temuan atau entitas milik akun anggota yang diaktifkan dalam grafik perilaku Anda? Jika akun terkait tidak diundang ke grafik perilaku sebagai akun anggota, maka grafik perilaku tidak berisi data untuk akun tersebut.

  Jika akun anggota yang diundang tidak menerima undangan, maka grafik perilaku tidak berisi data untuk akun tersebut.
- Untuk temuan, apakah temuan itu diarsipkan? Detektif tidak menerima temuan yang diarsipkan dari Amazon. GuardDuty
- Apakah temuan atau entitas terjadi sebelum Detektif mulai menyerap data ke dalam grafik perilaku Anda? Jika temuan atau entitas tidak ada dalam data yang dicerna Detective, maka grafik perilaku tidak berisi data untuk itu.
- Apakah temuan atau entitas dari Wilayah yang benar? Setiap grafik perilaku khusus untuk Wilayah AWS. Grafik perilaku tidak berisi data dari Wilayah lain.

Mengekspor data dari Detective

Anda dapat mengekspor data dari halaman Ringkasan Detektif Amazon dan halaman hasil pencarian. Data diekspor dalam format nilai dipisahkan koma (CSV). Nama file dari data yang diekspor mengikuti `detective-page-panel-yyyy-mm-dd.csv` format pola. Anda dapat memperkaya investigasi keamanan Anda dengan memanipulasi data menggunakan layanan AWS lain, aplikasi pihak ketiga, atau program spreadsheet yang mendukung impor CSV.

> **Note**
>
> Jika ekspor sedang berlangsung, tunggu hingga ekspor selesai sebelum Anda mencoba mengekspor data tambahan.

Anda dapat mengekspor file nilai yang dipisahkan koma (.csv) yang berisi data dari panel dan halaman berikut di Detective:

- Halaman ringkasan
  - Peran dan pengguna dengan panel volume panggilan API terbanyak
  - Instans EC2 dengan panel volume lalu lintas terbanyak
  - Kluster EKS dengan panel yang paling banyak dibuat pod Kubernetes

- Halaman pencarian - Jika pencarian Anda menghasilkan lebih dari 10.000 hasil, hanya 10.000 hasil teratas yang diekspor. Mengubah urutan penyortiran mengubah hasil yang dikembalikan.

Mengarsipkan temuan Amazon GuardDuty

Ketika Anda menyelesaikan penyelidikan Anda tentang GuardDuty temuan Amazon, Anda dapat mengarsipkan temuan dari Amazon Detective. Ini menghemat kesulitan karena harus kembali GuardDuty untuk melakukan pembaruan. Mengarsipkan temuan menunjukkan bahwa Anda telah menyelesaikan penyelidikan Anda.

Anda hanya dapat mengarsipkan GuardDuty temuan dari dalam Detektif jika Anda juga merupakan akun GuardDuty administrator untuk akun yang terkait dengan temuan tersebut. Jika Anda bukan akun GuardDuty administrator dan Anda mencoba mengarsipkan temuan, GuardDuty menampilkan kesalahan.

Untuk mengarsipkan GuardDuty temuan

1. Di konsol Detektif, di panel rincian pencarian, pilih Menemukan arsip.
2. Saat diminta untuk mengonfirmasi, pilih Arsip.

Anda dapat melihat GuardDuty temuan yang diarsipkan di GuardDuty konsol. Untuk mempelajari selengkapnya, lihat Aturan Penindasan di Panduan GuardDuty Pengguna Amazon.

Mengelola akun

Setiap grafik perilaku berisi data dari satu atau beberapa akun. Ketika sebuah akun mengaktifkan Detektif, akun tersebut menjadi akun administrator untuk grafik perilaku, dan akun anggota akan memilih akun anggota untuk grafik perilaku. Grafik perilaku dapat memiliki hingga 1.200 akun anggota.

Jika Anda terintegrasi dengan AWS Organizations, maka akun manajemen organisasi menunjuk akun administrator Detektif untuk organisasi. Akun administrator Detektif itu kemudian menjadi akun administrator untuk grafik perilaku organisasi. Akun administrator Detektif dapat mengaktifkan akun organisasi apa pun sebagai akun anggota dalam grafik perilaku organisasi. Akun organisasi tidak dapat menghapus dirinya sendiri dari grafik perilaku organisasi.

Akun administrator juga dapat mengundang akun untuk bergabung dengan grafik perilaku. Ketika akun menerima undangan, Detektif mengaktifkan akun sebagai akun anggota. Akun anggota yang ditambahkan melalui undangan dapat menghapus dirinya sendiri dari grafik perilaku.

Ketika akun diaktifkan sebagai akun anggota, Detektif mulai menelan dan mengekstrak data akun anggota ke dalam grafik perilaku tersebut.

Detective membebankan biaya setiap akun untuk data yang dikontribusikannya pada setiap grafik perilaku. Untuk informasi tentang melacak volume data untuk setiap akun dalam grafik perilaku, lihat Peramalan dan pemantauan biaya Detektif Amazon.

Konten

Pembatasan akun dan rekomendasi di Detective

Saat mengelola akun di Amazon Detective, perhatikan batasan dan rekomendasi berikut.

Jumlah maksimum akun anggota

Detective memungkinkan hingga 1.200 akun anggota di setiap grafik perilaku.

Akun dan Wilayah

Jika Anda menggunakan AWS Organizations untuk mengelola akun, akun manajemen organisasi menunjuk akun administrator Detektif untuk organisasi. Akun administrator Detektif menjadi akun administrator untuk grafik perilaku organisasi.

Akun administrator Detektif harus sama di semua Wilayah. Akun manajemen organisasi menunjuk akun administrator Detektif secara terpisah di setiap Wilayah. Akun administrator Detektif juga mengelola grafik perilaku organisasi dan akun anggota secara terpisah di setiap Wilayah.

Untuk akun anggota yang dibuat berdasarkan undangan, asosiasi administrator-anggota dibuat hanya di Wilayah tempat undangan dikirim. Akun administrator harus mengaktifkan Detektif di setiap Wilayah, dan memiliki grafik perilaku terpisah di setiap Wilayah. Akun administrator kemudian mengundang setiap akun untuk diasosiasikan sebagai akun anggota di Wilayah tersebut.

Akun dapat berupa akun anggota dari beberapa grafik perilaku di Wilayah yang sama. Akun hanya dapat menjadi akun administrator dari satu grafik perilaku per Wilayah. Akun dapat berupa akun administrator di Wilayah yang berbeda.

Penyelarasan akun administrator dengan Security Hub dan GuardDuty

Untuk memastikan bahwa integrasi dengan AWS Security Hub dan Amazon GuardDuty berfungsi dengan lancar, kami menyarankan agar akun yang sama adalah akun administrator di semua layanan ini.

Lihat the section called “Direkomendasikan penyelarasan dengan GuardDuty dan AWS Security Hub”.

Memberikan izin yang diperlukan untuk akun administrator

Untuk memastikan bahwa akun administrator memiliki izin yang diperlukan untuk mengelola grafik perilakunya, lampirkan kebijakan `AmazonDetectiveFullAccess` terkelola ke prinsipal IAM.

Mencerminkan pembaruan organisasi di Detective

Perubahan pada organisasi tidak segera tercermin dalam Detektif.

Untuk sebagian besar perubahan, seperti akun organisasi baru dan yang dihapus, Detective dapat memakan waktu hingga satu jam untuk diberitahu.

Perubahan ke akun administrator Detective yang ditunjuk di Organizations membutuhkan waktu lebih sedikit untuk disebarkan.

Melakukan transisi untuk menggunakan Organizations untuk mengelola akun grafik perilaku

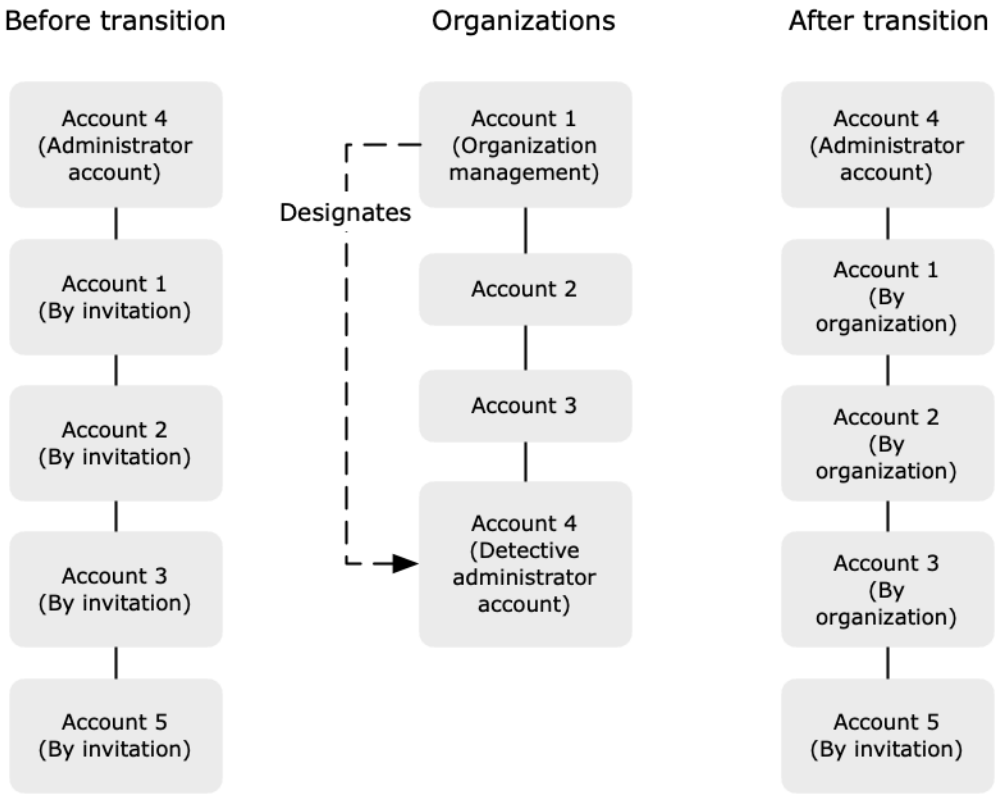
Anda mungkin memiliki grafik perilaku yang ada dengan akun anggota yang menerima undangan manual. Jika Anda terdaftar AWS Organizations, gunakan langkah-langkah berikut untuk menggunakan Organizations guna mengaktifkan dan mengelola akun anggota alih-alih menggunakan proses undangan manual:

1. Tentukan akun administrator Detektif untuk organisasi Anda. Ini menciptakan grafik perilaku organisasi.

   Jika akun administrator Detektif sudah memiliki grafik perilaku, maka grafik perilaku tersebut menjadi grafik perilaku organisasi.
2. Aktifkan akun organisasi sebagai akun anggota dalam grafik perilaku organisasi.

   Jika grafik perilaku organisasi memiliki akun anggota yang sudah ada yang merupakan akun organisasi, akun tersebut akan diaktifkan secara otomatis.

Diagram berikut menunjukkan ikhtisar struktur grafik perilaku sebelum transisi, konfigurasi dalam Organizations, dan struktur akun grafik perilaku setelah transisi.



Tentukan akun administrator Detektif untuk organisasi Anda

Akun manajemen organisasi Anda menunjuk akun administrator Detektif dari organisasi Anda. Lihat the section called “Menunjuk akun administrator Detektif”.

Untuk mempermudah transisi, Detective merekomendasikan agar Anda memilih akun administrator saat ini sebagai akun administrator Detektif untuk organisasi.

Jika ada akun administrator yang didelegasikan untuk Detective in Organizations, maka Anda harus menggunakan akun tersebut atau akun manajemen organisasi sebagai akun administrator Detective.

Jika tidak, saat pertama kali Anda menunjuk akun administrator Detektif yang bukan akun manajemen organisasi, Detective memanggil Organizations untuk menjadikan akun tersebut sebagai akun administrator yang didelegasikan untuk Detektif.

Aktifkan akun organisasi sebagai akun anggota

Akun administrator Detektif adalah akun administrator untuk grafik perilaku organisasi. Akun administrator Detektif memilih akun organisasi untuk diaktifkan sebagai akun anggota dalam grafik perilaku organisasi. Lihat the section called “Mengelola akun anggota organisasi”.

Pada halaman Akun, akun administrator Detektif melihat semua akun di organisasi.

Jika akun administrator Detektif sudah menjadi akun administrator untuk grafik perilaku, maka grafik perilaku tersebut menjadi grafik perilaku organisasi. Akun organisasi yang sudah menjadi akun anggota dalam grafik perilaku tersebut diaktifkan sebagai akun anggota secara otomatis. Akun organisasi lain memiliki status Bukan anggota.

Akun organisasi memiliki jenis Berdasarkan organisasi, bahkan jika mereka sebelumnya adalah akun anggota berdasarkan undangan.

Akun anggota yang bukan milik organisasi memiliki jenis Undangan Dengan.

Halaman Manajemen akun juga menyediakan opsi, Aktifkan akun organisasi baru secara otomatis, untuk mengaktifkan akun baru secara otomatis saat ditambahkan ke organisasi. Lihat the section called “Mengaktifkan akun organisasi baru secara otomatis”. Opsi ini awalnya dimatikan.

Ketika akun administrator Detektif pertama kali menampilkan halaman Manajemen akun, itu akan menampilkan pesan yang berisi tombol Aktifkan semua akun organisasi. Saat Anda memilih Aktifkan semua akun organisasi, Detektif melakukan tindakan berikut:

- Mengaktifkan semua akun organisasi saat ini sebagai akun anggota.
- Mengaktifkan opsi untuk mengaktifkan akun organisasi baru secara otomatis.

Ada juga opsi Aktifkan semua akun organisasi di daftar akun anggota.

Menunjuk akun administrator Detektif untuk suatu organisasi

Dalam grafik perilaku organisasi, akun administrator Detektif mengelola keanggotaan grafik perilaku untuk semua akun organisasi.

Bagaimana akun administrator Detektif dikelola

Akun manajemen organisasi menunjuk akun administrator Detektif untuk organisasi di masing-masing. Wilayah AWS

Mengatur akun administrator Detektif sebagai akun administrator yang didelegasikan

Akun administrator Detective juga menjadi akun administrator yang didelegasikan untuk Detective in. AWS Organizations Pengecualiannya adalah jika akun manajemen organisasi menunjuk dirinya

sebagai akun administrator Detektif. Akun manajemen organisasi tidak dapat menjadi administrator yang didelegasikan di Organizations.

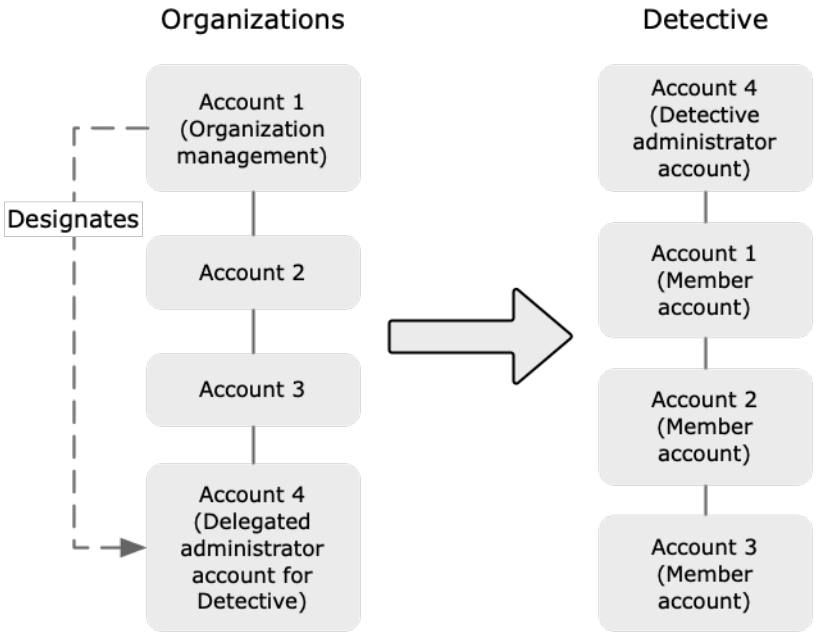
Setelah akun administrator yang didelegasikan diatur dalam Organizations, akun manajemen organisasi hanya dapat memilih akun administrator yang didelegasikan atau akun mereka sendiri sebagai akun administrator Detektif. Kami menyarankan Anda memilih akun administrator yang didelegasikan di semua Wilayah.

Membuat dan mengelola grafik perilaku organisasi

Saat akun manajemen organisasi memilih akun administrator Detektif, Detektif membuat grafik perilaku baru untuk akun tersebut. Grafik perilaku itu adalah grafik perilaku organisasi.

Jika akun administrator Detektif adalah akun administrator untuk grafik perilaku yang ada, maka grafik perilaku tersebut menjadi grafik perilaku organisasi.

Akun administrator Detektif memilih akun organisasi untuk diaktifkan sebagai akun anggota dalam grafik perilaku organisasi.



Akun administrator Detektif juga dapat mengirim undangan ke akun yang bukan milik organisasi. Lihat informasi yang lebih lengkap di the section called “Mengelola akun anggota organisasi” dan the section called “Mengelola akun yang diundang”.

Menghapus akun administrator Detektif

Akun manajemen organisasi dapat menghapus akun administrator Detektif saat ini di Wilayah. Saat Anda menghapus akun administrator Detektif, Detektif hanya menghapusnya dari Wilayah saat ini. Itu tidak mengubah akun administrator yang didelegasikan di Organizations.

Saat akun manajemen organisasi menghapus akun administrator Detektif di Wilayah, Detektif menghapus grafik perilaku organisasi. Detektif dinonaktifkan untuk akun administrator Detektif yang dihapus.

Untuk menghapus akun administrator yang didelegasikan saat ini untuk Detective, Anda menggunakan Organizations API. Saat Anda menghapus akun administrator yang didelegasikan untuk Detective in Organizations, Detective menghapus semua grafik perilaku organisasi di mana akun administrator yang didelegasikan adalah akun administrator Detektif. Grafik perilaku organisasi yang memiliki akun manajemen organisasi sebagai akun administrator Detektif tidak terpengaruh.

Izin yang diperlukan untuk mengonfigurasi akun administrator Detektif

Untuk memastikan bahwa akun manajemen organisasi dapat mengonfigurasi akun administrator Detektif, Anda dapat melampirkan kebijakan `AmazonDetectiveOrganizationsAccess` terkelola ke entitas AWS Identity and Access Management (IAM) Anda.

Menunjuk akun administrator Detektif (konsol)

Akun manajemen organisasi dapat menggunakan konsol Detektif untuk menunjuk akun administrator Detektif.

Anda tidak perlu mengaktifkan Detektif untuk mengelola akun administrator Detektif. Anda dapat mengelola akun administrator Detektif dari halaman Enable Detective.

Untuk menunjuk akun administrator Detektif (Aktifkan halaman Detektif)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Pilih Mulai.
3. Di panel Izin yang diperlukan untuk akun administrator, berikan izin yang diperlukan ke akun yang Anda pilih sehingga mereka dapat beroperasi sebagai administrator Detektif dengan akses penuh ke semua tindakan di Detektif. Untuk beroperasi sebagai administrator, Kami merekomendasikan melampirkan `AmazonDetectiveFullAccess` kebijakan ke kepala sekolah.

4. Pilih Lampirkan kebijakan dari IAM untuk melihat kebijakan yang direkomendasikan secara langsung di konsol IAM.
5. Bergantung pada apakah Anda memiliki izin di konsol IAM, lanjutkan sebagai berikut:

   - Jika Anda memiliki izin untuk beroperasi di konsol IAM, lampirkan kebijakan yang disarankan ke prinsipal yang Anda gunakan untuk Detektif.
   - Jika Anda tidak memiliki izin untuk beroperasi di konsol IAM, salin Kebijakan Nama Sumber Daya Amazon (ARN) dan berikan ke administrator IAM Anda. Mereka kemudian dapat melampirkan kebijakan atas nama Anda.
6. Di bawah Administrator yang didelegasikan, pilih akun administrator Detektif.

   Opsi yang tersedia tergantung pada apakah Anda memiliki akun administrator yang didelegasikan untuk Detective in Organizations.

   - Jika Anda tidak memiliki akun administrator yang didelegasikan untuk Detective in Organizations, maka masukkan pengenal akun akun untuk menunjuknya sebagai akun administrator Detektif.

     Anda mungkin memiliki akun administrator dan grafik perilaku yang ada dari proses undangan manual. Jika demikian, kami sarankan Anda menetapkan akun itu sebagai akun administrator Detektif.

     Jika Anda memiliki akun administrator yang didelegasikan di Organizations for Amazon GuardDuty AWS Security Hub, atau Amazon Macie, Detective meminta Anda untuk memilih salah satu akun tersebut. Anda juga dapat memasukkan akun yang berbeda.
   - Jika Anda memiliki akun administrator yang didelegasikan untuk Detective in Organizations, maka Anda diminta untuk memilih akun tersebut atau akun Anda. Kami menyarankan Anda memilih akun administrator yang didelegasikan di semua Wilayah.
7. Pilih Delegasikan.

Jika Detektif diaktifkan, atau merupakan akun anggota dalam grafik perilaku yang ada, maka Anda dapat menunjuk akun administrator Detektif dari halaman Umum.

Untuk menunjuk akun administrator Detektif (Halaman umum)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, di bawah Pengaturan, pilih Umum.

3. Di panel Kebijakan terkelola, Anda dapat mempelajari lebih lanjut tentang semua kebijakan terkelola yang didukung Detektif. Anda dapat memberikan izin yang diperlukan ke akun tergantung pada tindakan yang Anda ingin pengguna lakukan di Detective. Untuk beroperasi sebagai administrator, Kami merekomendasikan melampirkan `AmazonDetectiveFullAccess` kebijakan ke kepala sekolah.
4. Bergantung pada apakah Anda memiliki izin di konsol IAM, lanjutkan sebagai berikut:

   - Jika Anda memiliki izin untuk beroperasi di konsol IAM, lampirkan kebijakan yang disarankan ke prinsipal yang Anda gunakan untuk Detektif.
   - Jika Anda tidak memiliki izin untuk beroperasi di konsol IAM, salin Kebijakan Nama Sumber Daya Amazon (ARN) dan berikan ke administrator IAM Anda. Mereka kemudian dapat melampirkan kebijakan atas nama Anda.

   Opsi yang tersedia tergantung pada apakah Anda memiliki akun administrator yang didelegasikan untuk Detective in Organizations.

   - Jika Anda tidak memiliki akun administrator yang didelegasikan untuk Detective in Organizations, maka masukkan pengenal akun akun untuk menunjuknya sebagai akun administrator Detektif.

     Anda mungkin memiliki akun administrator dan grafik perilaku yang ada dari proses undangan manual. Jika demikian, maka kami sarankan Anda menunjuk akun itu sebagai akun administrator Detektif.

     Jika Anda memiliki akun administrator yang didelegasikan di Organizations for Amazon GuardDuty AWS Security Hub, atau Amazon Macie, Detective meminta Anda untuk memilih salah satu akun tersebut. Anda juga dapat memasukkan akun yang berbeda.
   - Jika Anda memiliki akun administrator yang didelegasikan untuk Detective in Organizations, maka Anda diminta untuk memilih akun tersebut atau akun Anda. Kami menyarankan Anda memilih akun administrator yang didelegasikan di semua Wilayah.
5. Pilih Delegasikan.

Menunjuk akun administrator Detektif (Detective API, AWS CLI)

Untuk menunjuk akun administrator Detektif, Anda dapat menggunakan panggilan API atau file. AWS Command Line Interface Anda harus menggunakan kredenal akun manajemen organisasi.

Jika Anda sudah memiliki akun administrator yang didelegasikan untuk Detektif dalam organisasi, maka Anda harus memilih akun itu atau akun Anda, kami sarankan Anda memilih akun administrator yang didelegasikan.

Untuk menunjuk akun administrator Detektif (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `EnableOrganizationAdminAccount` Anda harus memberikan pengenal AWS akun akun administrator Detektif. Untuk mendapatkan pengenal akun, gunakan `ListOrganizationAdminAccounts`operasi.
- AWS CLI: Pada baris perintah, jalankan `enable-organization-admin-account`perintah.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

Contoh

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Menghapus akun administrator Detektif (konsol)

Dari konsol Detektif, Anda dapat menghapus akun administrator Detektif.

Saat Anda menghapus akun administrator Detektif, Detektif dinonaktifkan untuk akun tersebut, dan grafik perilaku organisasi akan dihapus. Akun administrator Detektif hanya dihapus di Wilayah saat ini.

> **Important**
>
> Menghapus akun administrator Detective tidak memengaruhi akun administrator yang didelegasikan di Organizations.

Untuk menghapus akun administrator Detektif (Aktifkan halaman Detektif)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Pilih Mulai.
3. Di bawah Administrator Delegasi, pilih Nonaktifkan Detektif Amazon.
4. Pada kotak dialog konfirmasi, masukkan**`disable`**, lalu pilih Nonaktifkan Detektif Amazon.

Untuk menghapus akun administrator Detektif (Halaman umum)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, di bawah Pengaturan, pilih Umum.
3. Di bawah Administrator Delegasi, pilih Nonaktifkan Detektif Amazon.
4. Pada kotak dialog konfirmasi, masukkan**`disable`**, lalu pilih Nonaktifkan Detektif Amazon.

Menghapus akun administrator Detektif (Detective API,) AWS CLI

Untuk menghapus akun administrator Detektif, Anda dapat menggunakan panggilan API atau file. AWS CLI Anda harus menggunakan kredenal akun manajemen organisasi.

Saat Anda menghapus akun administrator Detektif, Detektif dinonaktifkan untuk akun tersebut, dan grafik perilaku organisasi akan dihapus.

> **Important**
>
> Menghapus akun administrator Detective tidak memengaruhi akun administrator yang didelegasikan di Organizations.

Untuk menghapus akun administrator Detektif (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `DisableOrganizationAdminAccount`

  Saat Anda menggunakan API Detektif untuk menghapus akun administrator Detektif, akun tersebut hanya akan dihapus di Wilayah tempat panggilan atau perintah API dikeluarkan.
- AWS CLI: Pada baris perintah, jalankan `disable-organization-admin-account`perintah.

```
aws detective disable-organization-admin-account
```

Menghapus akun administrator yang didelegasikan (Organizations API, AWS CLI)

Menghapus akun administrator Detective tidak secara otomatis menghapus akun administrator yang didelegasikan di Organizations. Untuk menghapus akun administrator yang didelegasikan untuk Detective, Anda dapat menggunakan Organizations API.

Saat Anda menghapus akun administrator yang didelegasikan, ini akan menghapus semua grafik perilaku organisasi di mana akun administrator yang didelegasikan adalah akun administrator Detektif. Ini juga menonaktifkan Detektif untuk akun di Wilayah tersebut.

Untuk menghapus akun administrator yang didelegasikan (Organizations API, AWS CLI)

- Organizations API: Gunakan `DeregisterDelegatedAdministrator`operasi. Anda harus memberikan pengenal akun dari akun administrator Detektif, dan kepala layanan untuk Detektif, yaitu. `detective.amazonaws.com`
- AWS CLI: Pada baris perintah, jalankan `deregister-delegated-administrator`perintah.

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

Contoh

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --
service-principal detective.amazonaws.com
```

Tindakan yang tersedia untuk akun

Akun administrator dan anggota memiliki akses ke tindakan Detektif berikut. Dalam tabel, nilai-nilai memiliki arti sebagai berikut:

- Setiap — Akun dapat melakukan tindakan untuk semua akun di bawah akun administrator Detective yang sama.
- Self — Akun hanya dapat melakukan tindakan di akun mereka sendiri.
- Dash (—) — Akun tidak dapat melakukan tindakan.

Dalam grafik perilaku organisasi, akun administrator Detektif menentukan akun organisasi mana yang akan diaktifkan sebagai akun anggota. Mereka dapat mengonfigurasi Detektif untuk mengaktifkan akun organisasi baru sebagai akun anggota secara otomatis, atau mereka dapat mengaktifkan akun organisasi secara manual.

Akun administrator dapat mengundang akun untuk menjadi akun anggota dalam grafik perilaku. Ketika akun anggota menerima undangan dan diaktifkan, Detektif Amazon mulai menelan dan mengekstrak data akun anggota ke dalam grafik perilaku tersebut.

Untuk grafik perilaku selain grafik perilaku organisasi, semua akun anggota adalah akun yang diundang.

Tabel berikut mencerminkan izin default untuk akun administrator dan anggota. Anda dapat menggunakan kebijakan IAM khusus untuk membatasi akses lebih lanjut ke fitur dan fungsi Detektif.

Tindakan	Akun administrator (Organisasi)	Akun administrator (Undangan)	Anggota (Organisasi)	Anggota (Undangan)
Lihat akun	Setiap	Setiap	Mandiri (Lihat akun administrator)	Mandiri (Lihat akun administrator)
Hapus akun anggota	Setiap Akun yang diundang dihapus Akun organisasi dipisahkan	Setiap	–	Mandiri
Menambahkan atau menghapus paket sumber data opsional	Setiap (Pengaturan berlaku untuk semua akun anggota)	Setiap (Pengaturan berlaku untuk semua akun anggota)	–	–
Nonaktifkan Detektif	Mandiri	Mandiri	–	–
Lihat data grafik perilaku	Setiap	Setiap	–	–
Mengaktifkan atau menonaktifkan paket sumber data opsional	Semua	Semua	–	–

Melihat daftar akun

Akun administrator dapat menggunakan konsol Detektif atau API untuk melihat daftar akun. Daftar ini dapat mencakup:

- Akun yang diundang oleh akun administrator untuk bergabung dengan grafik perilaku. Akun-akun ini memiliki jenis Undangan.
- Untuk grafik perilaku organisasi, semua akun dalam organisasi. Akun-akun ini memiliki jenis Berdasarkan organisasi.

Hasilnya tidak termasuk akun anggota yang diundang yang menolak undangan atau akun administrator dihapus dari grafik perilaku. Ini hanya mencakup akun dengan status berikut.

Verifikasi sedang berlangsung

Untuk akun yang diundang, Detektif memverifikasi alamat email akun sebelum mengirim undangan.

Untuk akun organisasi, Detective memverifikasi bahwa akun tersebut milik organisasi. Detective juga memverifikasi bahwa itu adalah akun administrator Detective yang mengaktifkan akun tersebut.

Verifikasi gagal

Verifikasi gagal. Undangan tidak dikirim, atau akun organisasi tidak diaktifkan sebagai anggota.

Diundang

Untuk akun yang diundang. Undangan telah dikirim, tetapi akun anggota belum merespons.

Bukan anggota

Untuk akun organisasi dalam grafik perilaku organisasi. Akun organisasi saat ini bukan akun anggota. Itu tidak menyumbangkan data ke grafik perilaku organisasi.

Diaktifkan

Untuk akun yang diundang, akun anggota menerima undangan dan menyumbangkan data ke grafik perilaku.

Untuk akun organisasi dalam grafik perilaku organisasi, akun administrator Detektif mengaktifkan akun sebagai akun anggota. Akun menyumbangkan data ke grafik perilaku organisasi.

Tidak diaktifkan

Untuk akun yang diundang, akun anggota menerima undangan, tetapi tidak dapat diaktifkan.

Untuk akun organisasi dalam grafik perilaku organisasi, akun administrator Detektif mencoba mengaktifkan akun, tetapi akun tidak dapat diaktifkan.

Status ini terjadi karena salah satu alasan berikut.

- Akun anggota belum menjadi GuardDuty pelanggan Amazon setidaknya selama 48 jam.
- Data akun anggota akan menyebabkan volume data grafik perilaku melebihi kuota Detektif.

Daftar akun (Konsol)

Anda dapat menggunakan AWS Management Console untuk melihat dan memfilter daftar akun Anda.

Untuk menampilkan daftar akun (konsol)

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, pilih Manajemen akun.

   Daftar akun anggota berisi akun berikut:

   - Akun Anda
   - Akun yang Anda undang untuk menyumbangkan data ke grafik perilaku
   - Dalam grafik perilaku organisasi, semua akun organisasi

   Untuk setiap akun, daftar menampilkan informasi berikut:

   - Pengidentifikasi AWS akun.
   - Untuk akun organisasi, nama akun.
   - Jenis akun (Dengan undangan atau Berdasarkan organisasi).
   - Untuk akun yang diundang, alamat email pengguna root akun.
   - Status akun.
   - Volume data harian untuk akun. Detektif tidak dapat mengambil volume data untuk akun yang tidak diaktifkan sebagai akun anggota.

- Tanggal ketika status akun terakhir diperbarui.

Anda dapat menggunakan tab di bagian atas tabel untuk memfilter daftar berdasarkan status akun anggota. Setiap tab menunjukkan jumlah akun anggota yang cocok.

- Pilih Semua untuk melihat semua akun anggota.
- Pilih Diaktifkan untuk melihat akun yang berstatus Diaktifkan.
- Pilih Tidak diaktifkan untuk melihat akun yang memiliki status selain Diaktifkan.

Anda juga dapat menambahkan filter lain ke daftar akun anggota.

Untuk menambahkan filter ke daftar akun dalam grafik perilaku (konsol)

1. Pilih kotak filter.
2. Pilih kolom yang ingin Anda gunakan untuk memfilter daftar.
3. Untuk kolom yang ditentukan, pilih nilai yang akan digunakan untuk filter.
4. Untuk menghapus filter, pilih ikon x di kanan atas.
5. Untuk memperbarui daftar dengan informasi status terbaru, pilih ikon penyegaran di kanan atas.

Daftar akun anggota Anda (Detective API,) AWS CLI

Anda dapat menggunakan panggilan API atau AWS Command Line Interface untuk melihat daftar akun anggota dalam grafik perilaku Anda.

Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk mengambil daftar akun anggota (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `ListMembers` Untuk mengidentifikasi grafik perilaku yang dimaksud, tentukan grafik perilaku ARN.

  Perhatikan bahwa untuk grafik perilaku organisasi, `ListMembers`tidak menampilkan akun organisasi yang tidak Anda aktifkan sebagai akun anggota atau yang Anda lepaskan dari grafik perilaku.
- AWS CLI: Pada baris perintah, jalankan `list-members`perintah.

```
aws detective list-members --graph-arn <behavior graph ARN>
```

Contoh:

```
aws detective list-members --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Untuk mengambil detail tentang akun anggota tertentu dalam grafik perilaku Anda (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `GetMembers` Tentukan grafik perilaku ARN dan daftar pengidentifikasi akun untuk akun anggota.
- AWS CLI: Pada baris perintah, jalankan `get-members`perintah.

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior
 graph ARN>
```

Contoh:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Mengelola akun organisasi sebagai akun anggota

Dalam grafik perilaku organisasi, akun administrator Detektif menentukan akun organisasi mana yang akan diaktifkan sebagai akun anggota.

Mereka dapat mengonfigurasi Detektif untuk mengaktifkan akun organisasi baru sebagai akun anggota secara otomatis, atau mereka dapat mengaktifkan akun organisasi secara manual.

Akun administrator Detektif juga dapat memisahkan akun organisasi dari grafik perilaku organisasi.

Daftar Isi

- Memutuskan akun organisasi sebagai akun anggota

Mengaktifkan akun organisasi baru sebagai akun anggota secara otomatis

Akun administrator Detektif dapat mengonfigurasi Detektif untuk mengaktifkan akun organisasi baru secara otomatis sebagai akun anggota dalam grafik perilaku organisasi.

Ketika akun baru ditambahkan ke organisasi Anda, akun tersebut ditambahkan ke daftar di halaman Manajemen akun. Untuk akun organisasi, Type is By Organization.

Secara default, akun organisasi baru tidak diaktifkan sebagai akun anggota. Status mereka bukan anggota.

Ketika Anda memilih untuk mengaktifkan akun organisasi secara otomatis, Detektif mulai mengaktifkan akun baru sebagai akun anggota saat ditambahkan ke organisasi. Detective tidak mengaktifkan akun organisasi yang ada yang belum diaktifkan.

Apakah Detektif dapat mengaktifkan akun organisasi sebagai akun anggota bergantung pada hal berikut:

- Jumlah maksimum akun anggota untuk grafik perilaku adalah 1.200. Jika grafik perilaku Anda sudah berisi 1.200 akun anggota, maka akun baru tidak dapat diaktifkan.
- Detektif tidak dapat mengaktifkan akun yang belum GuardDuty mengaktifkan Amazon setidaknya selama 48 jam.
- Detektif tidak dapat mengaktifkan akun jika itu akan menyebabkan volume data grafik perilaku melebihi maksimum yang diizinkan.

Mengaktifkan akun organisasi baru secara otomatis (konsol)

Pada halaman Pengelolaan akun, pengaturan Aktifkan akun organisasi baru secara otomatis menentukan apakah akan mengaktifkan akun secara otomatis saat ditambahkan ke organisasi.

Untuk secara otomatis mengaktifkan akun organisasi baru sebagai akun anggota

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Alihkan Aktifkan akun organisasi baru secara otomatis ke posisi aktif.

Mengaktifkan akun organisasi baru secara otomatis (Detective API,) AWS CLI

Untuk menentukan apakah akan mengaktifkan akun organisasi baru secara otomatis sebagai akun anggota, akun administrator dapat menggunakan Detective API atau file. AWS Command Line Interface

Untuk melihat dan mengelola konfigurasi, Anda harus memberikan grafik perilaku ARN. Untuk mendapatkan ARN, gunakan operasi. `ListGraphs`

Untuk melihat konfigurasi saat ini untuk mengaktifkan akun organisasi secara otomatis

- Detective API: Gunakan operasi. `DescribeOrganizationConfiguration`

  Sebagai tanggapan, jika akun organisasi baru diaktifkan secara otomatis, maka `AutoEnable` adalah`true`.
- AWS CLI: Pada baris perintah, jalankan `describe-organization-configuration`perintah.

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

  Contoh

```
aws detective describe-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Untuk mengaktifkan akun organisasi baru secara otomatis

- Detective API: Gunakan operasi. `UpdateOrganizationConfiguration` Untuk mengaktifkan akun organisasi baru secara otomatis, setel `AutoEnable` ke`true`.
- AWS CLI: Pada baris perintah, jalankan `update-organization-configuration`perintah.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN> --
auto-enable | --no-auto-enable
```

  Contoh

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --auto-enable
```

Mengaktifkan akun organisasi sebagai akun anggota

Jika Anda tidak secara otomatis mengaktifkan akun organisasi baru, maka Anda dapat mengaktifkan akun tersebut secara manual. Anda juga harus mengaktifkan akun yang Anda putuskan secara manual.

Menentukan apakah akun dapat diaktifkan

Anda tidak dapat mengaktifkan akun organisasi sebagai akun anggota jika grafik perilaku organisasi sudah memiliki maksimum 1.200 akun yang diaktifkan. Dalam hal ini, status akun organisasi tetap Bukan anggota.

Saat Anda mengaktifkan akun organisasi, Detektif memeriksa apakah akun tersebut telah menjadi GuardDuty pelanggan Amazon setidaknya selama 48 jam. Jika sudah, maka Detektif memeriksa apakah data akun akan menyebabkan laju data untuk grafik perilaku melebihi kuota. Pemeriksaan ini bisa memakan waktu 24 hingga 48 jam.

Sementara Detective memverifikasi kecepatan data, status akun anggota tidak diaktifkan.

Jika akun anggota melewati kedua cek tersebut, maka status akun anggota diperbarui ke Diaktifkan. Detektif mulai menyerap data dari akun anggota ke dalam grafik perilaku.

Jika akun gagal salah satu dari pemeriksaan tersebut, maka status akun anggota tetap Tidak diaktifkan. Akun tidak menyumbangkan data ke grafik perilaku.

Segera setelah akun anggota dapat diaktifkan, Detektif secara otomatis mengubah status akun anggota menjadi Diaktifkan.

Mengaktifkan akun organisasi sebagai akun anggota (konsol)

Dari halaman Manajemen akun, Anda dapat mengaktifkan akun organisasi sebagai akun anggota.

Untuk mengaktifkan akun organisasi sebagai akun anggota

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Untuk melihat daftar akun yang saat ini tidak diaktifkan, pilih Tidak diaktifkan.
4. Anda dapat memilih akun organisasi tertentu, atau mengaktifkan semua akun organisasi.

   Untuk mengaktifkan akun organisasi yang dipilih:

a. Pilih setiap akun organisasi yang ingin Anda aktifkan.

b. Pilih Aktifkan akun.

Untuk mengaktifkan semua akun organisasi, pilih Aktifkan semua akun organisasi.

Mengaktifkan akun organisasi sebagai akun anggota (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS Command Line Interface untuk mengaktifkan akun organisasi sebagai akun anggota dalam grafik perilaku organisasi. Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk mengaktifkan akun organisasi sebagai akun anggota (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `CreateMembers` Anda harus memberikan grafik ARN.

  Untuk setiap akun, tentukan pengenal akun. Akun organisasi dalam grafik perilaku organisasi tidak menerima undangan. Anda tidak perlu memberikan alamat email atau informasi undangan lainnya.
- AWS CLI: Pada baris perintah, jalankan `create-members`perintah.

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-
arn <behavior graph ARN>
```

Contoh

```
aws detective create-members --accounts AccountId=444455556666 AccountId=123456789012
 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Memutuskan akun organisasi sebagai akun anggota

Untuk menghentikan pengambilan data dari akun organisasi dalam grafik perilaku organisasi, Anda dapat memisahkan akun. Data yang ada untuk akun itu tetap ada dalam grafik perilaku.

Saat Anda memisahkan akun organisasi, status berubah menjadi Bukan anggota. Detektif berhenti menelan data dari akun itu, tetapi akun tetap dalam daftar.

Memutuskan akun organisasi (konsol)

Dari halaman Manajemen akun, Anda dapat memisahkan akun organisasi sebagai akun anggota.

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Untuk menampilkan daftar akun yang diaktifkan, pilih Diaktifkan.
4. Pilih kotak centang untuk setiap akun untuk dipisahkan.
5. Pilih Tindakan. Kemudian pilih Nonaktifkan akun.

   Status akun untuk akun yang terputus berubah menjadi Bukan anggota.

Memutuskan akun organisasi (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS Command Line Interface untuk memisahkan akun organisasi sebagai akun anggota dalam grafik perilaku Anda.

Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk memisahkan akun organisasi dari grafik perilaku organisasi (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `DeleteMembers` Tentukan grafik ARN dan daftar pengidentifikasi akun untuk memisahkan akun anggota.
- AWS CLI: Pada baris perintah, jalankan `delete-members`perintah.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Contoh

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Mengelola akun anggota yang diundang

Akun administrator dapat mengundang akun untuk menjadi akun anggota dalam grafik perilaku. Ketika akun anggota menerima undangan dan diaktifkan, Detektif Amazon mulai menyerap dan mengekstrak data akun anggota ke dalam grafik perilaku tersebut.

Untuk grafik perilaku selain grafik perilaku organisasi, semua akun anggota adalah akun yang diundang.

Akun administrator Detektif juga dapat mengundang akun yang bukan akun organisasi ke grafik perilaku organisasi.

Akun administrator dapat menghapus akun anggota yang diundang dari grafik perilaku.

Daftar Isi

Mengundang akun anggota ke grafik perilaku

Akun administrator dapat mengundang akun untuk berkontribusi pada grafik perilaku. Grafik perilaku dapat berisi hingga 1.200 akun anggota.

Pada tingkat tinggi, proses mengundang akun untuk berkontribusi pada grafik perilaku adalah sebagai berikut.

1. Untuk setiap akun anggota untuk ditambahkan, akun administrator menyediakan pengenal AWS akun dan alamat email pengguna root.
2. Detektif memvalidasi bahwa alamat email adalah alamat email pengguna root untuk akun tersebut.

   Detektif tidak melakukan validasi ini di Wilayah AWS GovCloud (AS-Timur) atau AWS GovCloud (AS-Barat).
3. Jika informasi akun valid, Detektif mengirimkan undangan ke akun anggota.

   Detektif tidak pernah mengirim undangan email ke akun anggota di Wilayah AWS GovCloud (AS-Timur) atau AWS GovCloud (AS-Barat).

Untuk Wilayah lain, Detective API menyertakan opsi untuk tidak mengirim undangan ke akun anggota.

Opsi ini berguna untuk akun yang dikelola secara terpusat.

4. Akun anggota menerima atau menolak undangan.

   Bahkan jika akun administrator tidak mengirim email undangan, akun anggota tetap harus menanggapi undangan.

5. Jika akun anggota menerima undangan, Detektif memeriksa apakah akun anggota telah menjadi pelanggan GuardDuty Amazon setidaknya selama 48 jam.

   Jika sudah, maka Detektif memeriksa apakah data akun anggota akan menyebabkan laju data untuk grafik perilaku melebihi kuota.

   Pemeriksaan ini dapat memakan waktu antara 24 hingga 48 jam.

   Sementara Detective memverifikasi kecepatan data, status akun anggota tidak diaktifkan.

6. Jika akun anggota melewati kedua pemeriksaan tersebut, maka status akun anggota secara otomatis diperbarui ke Diaktifkan. Detektif mulai menelan data dari akun anggota ke dalam grafik perilaku.

   Jika gagal salah satu dari pemeriksaan tersebut, maka status akun anggota tetap Tidak diaktifkan. Akun anggota tidak menyumbangkan data ke grafik perilaku.

7. Segera setelah akun anggota memenuhi syarat untuk diaktifkan, Detektif secara otomatis mengubah status akun anggota menjadi Diaktifkan.

   Misalnya, status akun anggota berubah menjadi Diaktifkan jika akun anggota diaktifkan GuardDuty dan Detektif memverifikasi bahwa volume datanya tidak terlalu besar, atau jika akun administrator menghapus akun anggota lain untuk memberi ruang bagi akun.

   Jika lebih dari satu akun tidak diaktifkan, maka Detektif mengaktifkan akun dalam urutan di mana mereka diundang. Proses untuk memeriksa apakah akan mengaktifkan akun Not enabled berjalan setiap jam.

   Akun administrator juga dapat mengaktifkan akun secara manual, alih-alih menunggu proses otomatis. Misalnya, akun administrator mungkin ingin memilih akun yang akan diaktifkan. Lihat the section called “Mengaktifkan akun anggota yang tidak diaktifkan”.

Perhatikan bahwa Detektif mulai secara otomatis mengaktifkan akun yang Tidak diaktifkan pada 12 Mei 2021. Akun yang tidak diaktifkan sebelumnya tidak diaktifkan secara otomatis. Akun administrator harus mengaktifkannya secara manual.

Mengundang akun individual ke grafik perilaku (Konsol)

Anda dapat secara manual menentukan akun anggota yang akan diundang untuk menyumbangkan data mereka ke grafik perilaku.

Untuk secara manual memilih akun anggota yang akan diundang (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Pilih Tindakan. Kemudian pilih Undang akun.
4. Di bawah Tambah akun, pilih Tambahkan akun individual.
5. Untuk menambahkan akun anggota ke daftar undangan, lakukan langkah-langkah berikut.

   a. Pilih Tambah akun.

   b. Untuk ID AWS Akun, masukkan ID AWS akun.

   c. Untuk alamat Email, masukkan alamat email pengguna root untuk akun tersebut.
6. Untuk menghapus akun dari daftar, pilih Hapus untuk akun itu.
7. Di bawah Personalisasi email undangan, tambahkan konten yang disesuaikan untuk disertakan dalam email undangan.

   Misalnya, Anda dapat menggunakan area ini untuk memberikan informasi kontak. Atau gunakan untuk mengingatkan akun anggota bahwa mereka perlu melampirkan kebijakan IAM yang diperlukan kepada pengguna atau peran mereka sebelum mereka dapat menerima undangan.
8. Kebijakan IAM akun anggota berisi teks kebijakan IAM yang diperlukan untuk akun anggota. Undangan email mencakup teks kebijakan ini. Untuk menyalin teks kebijakan, pilih Salin.
9. Pilih Undang.

Mengundang daftar akun anggota ke grafik perilaku (Konsol)

Dari konsol Detektif, Anda dapat menyediakan `.csv` file yang berisi daftar akun anggota untuk diundang ke grafik perilaku Anda.

Baris pertama dalam file adalah baris header. Setiap akun kemudian terdaftar pada baris terpisah. Setiap entri akun anggota berisi ID AWS akun dan alamat email pengguna root akun.

Contoh:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Ketika Detective memproses file, ia mengabaikan akun yang sudah diundang, kecuali status akun Verifikasi gagal. Status tersebut menunjukkan bahwa alamat email yang diberikan untuk akun tidak cocok dengan alamat email pengguna root akun. Dalam hal ini, Detective menghapus undangan asli dan mencoba lagi untuk memverifikasi alamat email dan mengirim undangan.

Opsi ini juga menyediakan template yang dapat Anda gunakan untuk membuat daftar akun.

Untuk mengundang akun anggota dari daftar.csv (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Pilih Tindakan. Kemudian pilih Undang akun.
4. Di bawah Tambah akun, pilih Tambah dari.csv.
5. Untuk mengunduh file templat agar berfungsi, pilih Unduh template.csv.
6. Untuk memilih file yang berisi daftar akun, pilih Pilih file.csv.
7. Di bawah Tinjau akun anggota, verifikasi daftar akun anggota yang ditemukan Detektif dalam file.
8. Di bawah Personalisasi email undangan, tambahkan konten yang disesuaikan untuk disertakan dalam email undangan.

   Misalnya, Anda dapat memberikan informasi kontak, atau mengingatkan akun anggota tentang kebijakan IAM yang diperlukan.
9. Kebijakan IAM akun anggota berisi teks kebijakan IAM yang diperlukan untuk akun anggota. Undangan email mencakup teks kebijakan ini. Untuk menyalin teks kebijakan, pilih Salin.
10. Pilih Undang.

Mengundang akun anggota ke grafik perilaku (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau akun AWS Command Line Interface untuk mengundang anggota untuk menyumbangkan data mereka ke grafik perilaku. Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk mengundang akun anggota ke grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `CreateMembers` Anda harus memberikan grafik ARN. Untuk setiap akun, tentukan pengenal akun dan alamat email pengguna root.

  Untuk tidak mengirim email undangan ke akun anggota, atur `DisableEmailNotification` ke true. Secara default, `DisableEmailNotification` adalah false.

  Jika Anda mengirim email undangan, Anda dapat secara opsional memberikan teks khusus untuk ditambahkan ke email undangan.
- AWS CLI: Pada baris perintah, jalankan `create-members` perintah.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --message "<Custom message
 text>"
```

Contoh

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This is Paul
 Santos. I need to add your account to the data we use for security investigation in
 Amazon Detective. If you have any questions, contact me at psantos@example.com."
```

Untuk menunjukkan tidak mengirim email undangan ke akun anggota, sertakan`--disable-email-notification`.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --disable-email-notification
```

Contoh

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-
notification
```

Menambahkan daftar akun anggota di seluruh Wilayah (skrip Python aktif) GitHub

Detective menyediakan skrip open-source GitHub yang memungkinkan Anda melakukan hal berikut:

- Tambahkan daftar akun anggota tertentu ke grafik perilaku akun administrator di seluruh daftar Wilayah yang ditentukan.
- Jika akun administrator tidak memiliki grafik perilaku di Wilayah, maka skrip juga mengaktifkan Detektif dan membuat grafik perilaku di Wilayah tersebut.
- Kirim email undangan ke akun anggota.
- Secara otomatis menerima undangan untuk akun anggota.

Untuk informasi tentang cara mengkonfigurasi dan menggunakan GitHub skrip, lihatthe section called “Skrip Python Detektif Amazon”.

Mengaktifkan akun anggota yang tidak diaktifkan

Setelah akun anggota menerima undangan, Amazon Detective memeriksa apakah akun tersebut dapat mengaktifkan akun anggota. Jika Detektif tidak dapat mengaktifkan akun anggota, maka ia menetapkan status akun anggota ke Tidak diaktifkan. Hal ini dapat terjadi karena salah satu alasan berikut:

- Akun anggota belum menjadi GuardDuty pelanggan Amazon setidaknya selama 48 jam.
- Detektif memverifikasi volume data untuk akun anggota.
- Data akun anggota akan menyebabkan laju data grafik perilaku melebihi kuota.

Akun anggota yang Tidak diaktifkan tidak menyumbangkan data ke grafik perilaku.

Detective secara otomatis mengaktifkan akun karena grafik perilaku dapat mengakomodasi mereka.

Anda juga dapat mencoba mengaktifkan akun anggota secara manual yang tidak diaktifkan akun anggota. Misalnya, Anda dapat menghapus akun anggota yang ada untuk mengurangi volume data. Alih-alih menunggu proses otomatis untuk mengaktifkan akun, Anda dapat mencoba mengaktifkan Akun anggota yang tidak diaktifkan.

Mengaktifkan akun anggota yang Tidak diaktifkan (Konsol)

Daftar akun anggota mencakup opsi untuk mengaktifkan akun anggota terpilih yang Tidak diaktifkan.

Untuk mengaktifkan akun anggota yang tidak diaktifkan

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Di bawah Akun anggota saya, pilih kotak centang untuk mengaktifkan setiap akun anggota.

   Anda hanya dapat mengaktifkan akun anggota yang memiliki status Tidak diaktifkan.
4. Pilih Aktifkan akun.

Detektif menentukan apakah akun anggota dapat diaktifkan. Jika akun anggota dapat diaktifkan, status akan berubah menjadi Diaktifkan.

Mengaktifkan akun anggota yang Tidak diaktifkan (Detective API,) AWS CLI

Anda dapat menggunakan panggilan API atau AWS Command Line Interface untuk mengaktifkan satu akun anggota yang tidak diaktifkan. Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk mengaktifkan akun anggota yang tidak diaktifkan

- Detective API: Gunakan operasi `StartMonitoringMember`API. Anda harus memberikan grafik perilaku ARN. Untuk mengidentifikasi akun anggota, gunakan pengenal AWS akun.
- AWS CLI: Pada baris perintah, jalankan `start-monitoring-member`perintah:

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account
 ID>
```

  Misalnya:

```
start-monitoring-member --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --account-id 444455556666
```

Menghapus akun anggota yang diundang dari grafik perilaku

Akun administrator dapat menghapus akun anggota dari grafik perilaku kapan saja.

Detektif secara otomatis menghapus akun anggota yang dihentikan di AWS, kecuali di Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).

Ketika akun anggota yang diundang dihapus dari grafik perilaku, hal berikut akan terjadi.

- Akun anggota dihapus dari akun anggota Saya.
- Amazon Detective berhenti menelan data dari akun yang dihapus.

Detective tidak menghapus data yang ada dari grafik perilaku, yang mengumpulkan data di seluruh akun anggota.

Menghapus akun anggota yang diundang dari grafik perilaku (konsol)

Anda dapat menggunakan AWS Management Console untuk menghapus akun anggota yang diundang dari grafik perilaku Anda.

Untuk menghapus akun anggota (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Dalam daftar akun, pilih kotak centang untuk menghapus setiap akun anggota.

   Anda tidak dapat menghapus akun Anda sendiri dari daftar.
4. Pilih Tindakan. Kemudian pilih Nonaktifkan akun.

Menghapus akun anggota yang diundang dari grafik perilaku (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS Command Line Interface untuk menghapus akun anggota yang diundang dari grafik perilaku Anda. Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk menghapus akun anggota yang diundang dari grafik perilaku Anda (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `DeleteMembers` Tentukan grafik ARN dan daftar pengidentifikasi akun untuk dihapus akun anggota.
- AWS CLI: Pada baris perintah, jalankan `delete-members`perintah.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Contoh:

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Menghapus daftar akun anggota yang diundang di seluruh Wilayah (skrip Python aktif) GitHub

Detective menyediakan skrip sumber terbuka di. GitHub Anda dapat menggunakan skrip ini untuk menghapus daftar akun anggota tertentu dari grafik perilaku akun administrator di seluruh daftar Wilayah yang ditentukan.

Untuk informasi tentang cara mengkonfigurasi dan menggunakan GitHub skrip, lihatthe section called “Skrip Python Detektif Amazon”.

Untuk akun anggota: Mengelola undangan grafik perilaku dan keanggotaan

Amazon Detective menagih setiap akun anggota untuk data yang dicerna untuk setiap grafik perilaku yang dikontribusikannya.

Halaman Manajemen akun memungkinkan akun anggota untuk melihat akun administrator untuk grafik perilaku yang menjadi anggotanya.

Akun anggota yang diundang ke grafik perilaku dapat melihat dan menanggapi undangan mereka. Mereka juga dapat menghapus akun mereka dari grafik perilaku.

Untuk grafik perilaku organisasi, akun organisasi tidak mengontrol apakah akun mereka adalah akun anggota. Akun administrator Detektif memilih akun organisasi untuk mengaktifkan atau menonaktifkan sebagai akun anggota.

Daftar Isi

Kebijakan IAM yang diperlukan untuk akun anggota

Sebelum akun anggota dapat melihat dan mengelola undangan, kebijakan IAM yang diperlukan harus dilampirkan pada prinsipal mereka. Prinsipal dapat berupa pengguna atau peran yang sudah ada, atau Anda dapat membuat pengguna atau peran baru yang akan digunakan untuk Detektif.

Idealnya, akun administrator meminta administrator IAM mereka melampirkan kebijakan yang diperlukan.

Kebijakan IAM akun anggota memberikan akses ke tindakan akun anggota di Amazon Detective. Undangan email untuk berkontribusi pada grafik perilaku mencakup teks kebijakan IAM tersebut.

Untuk menggunakan kebijakan ini, ganti *<behavior graph ARN>* dengan grafik ARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
   {
    "Effect":"Allow",
    "Action":[
```

```
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

Perhatikan bahwa akun organisasi dalam grafik perilaku organisasi tidak menerima undangan dan tidak dapat memisahkan akun mereka dari grafik perilaku organisasi. Jika mereka tidak termasuk dalam grafik perilaku lain, maka mereka hanya memerlukan `ListInvitations` izin. `ListInvitations`memungkinkan mereka untuk melihat akun administrator untuk grafik perilaku. Izin untuk mengelola undangan dan memisahkan keanggotaan hanya berlaku untuk keanggotaan berdasarkan undangan.

Melihat daftar undangan grafik perilaku

Dari konsol Amazon Detective, Detective API, atau AWS Command Line Interface, akun anggota dapat melihat undangan grafik perilaku mereka.

Melihat undangan grafik perilaku (konsol)

Anda dapat melihat undangan grafik perilaku dari. AWS Management Console

Untuk melihat undangan grafik perilaku (konsol)

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, pilih Manajemen akun.

Pada halaman Pengelolaan akun, Akun administrator saya berisi undangan grafik perilaku terbuka dan diterima di Wilayah saat ini. Untuk akun organisasi, Akun administrator saya juga berisi grafik perilaku organisasi.

Jika akun Anda saat ini dalam masa uji coba gratis, halaman tersebut juga menampilkan jumlah hari yang tersisa dalam uji coba gratis Anda.

Daftar tidak berisi undangan yang Anda tolak, keanggotaan yang Anda pasrahkan, atau keanggotaan yang dihapus oleh akun administrator.

Setiap undangan menunjukkan nomor akun administrator, tanggal undangan diterima, dan status undangan saat ini.

- Untuk undangan yang belum Anda tanggapi, statusnya adalah Diundang.
- Untuk undangan yang Anda terima, status Diaktifkan atau Tidak diaktifkan.

  Jika status Diaktifkan, akun Anda akan menyumbangkan data ke grafik perilaku.

  Jika status tidak diaktifkan, akun Anda tidak akan menyumbangkan data ke grafik perilaku.

  Status akun Anda awalnya disetel ke Tidak diaktifkan sementara Detektif memeriksa apakah Anda telah GuardDuty mengaktifkan, dan jika demikian, apakah akun Anda akan menyebabkan volume data untuk grafik perilaku melebihi kuota Detektif.

  Jika akun Anda tidak menyebabkan grafik perilaku melebihi kuota, Detektif memperbarui status akun Anda ke Diaktifkan. Jika tidak, statusnya tetap Tidak diaktifkan.

  Ketika grafik perilaku dapat mengakomodasi volume data untuk akun Anda, Detective secara otomatis memperbaruinya ke Diaktifkan. Misalnya, akun administrator mungkin menghapus akun anggota lain sehingga akun Anda dapat diaktifkan. Akun administrator juga dapat mengaktifkan akun Anda secara manual.

Melihat undangan grafik perilaku (Detective API,) AWS CLI

Anda dapat mencantumkan undangan grafik perilaku dari Detective API atau file. AWS Command Line Interface

Untuk mengambil daftar undangan yang terbuka dan diterima ke grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `ListInvitations`
- AWS CLI: Pada baris perintah, jalankan `list-invitations`perintah.

```
aws detective list-invitations
```

Menanggapi undangan grafik perilaku

Ketika Anda menerima undangan, status akun Anda awalnya disetel ke Tidak diaktifkan sementara Detektif memeriksa apakah akun Anda akan menyebabkan volume data untuk grafik perilaku melebihi kuota Detektif. Agar Detektif melakukan pemeriksaan ini, akun Anda harus GuardDuty mengaktifkan Amazon setidaknya selama 48 jam.

Jika akun Anda tidak menyebabkan grafik perilaku melebihi kuota, Detektif memperbarui status akun Anda ke Diaktifkan. Detektif mulai menelan dan mengekstrak data dari log dan temuan ke dalam grafik perilaku pada saat itu. Akun Anda dikenakan biaya untuk data.

Jika penambahan akun Anda akan menyebabkan volume data untuk grafik perilaku melebihi kuota Detektif, atau jika Anda belum GuardDuty mengaktifkan, status tetap Tidak diaktifkan. Dalam hal ini, kecuali Anda menghapus akun Anda, Detective secara otomatis mengaktifkan akun Anda segera setelah grafik perilaku dapat mengakomodasi akun tersebut. Akun administrator juga dapat mengaktifkan akun Anda secara manual.

Jika Anda menolak undangan, maka itu dihapus dari daftar undangan Anda, dan Detektif tidak menggunakan data akun Anda dalam grafik perilaku.

Menanggapi undangan grafik perilaku (konsol)

Anda dapat menggunakan AWS Management Console untuk menanggapi undangan email, yang mencakup tautan ke konsol Detektif. Anda hanya dapat menanggapi undangan yang berstatus Diundang.

Untuk menanggapi undangan grafik perilaku (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Di bawah Akun administrator saya, untuk menerima undangan dan mulai menyumbangkan data ke grafik perilaku, pilih Terima undangan.

   Untuk menolak undangan dan menghapusnya dari daftar, pilih Tolak.

Menanggapi undangan grafik perilaku (Detective API,) AWS CLI

Anda dapat menanggapi undangan grafik perilaku dari Detective API atau file. AWS Command Line Interface

Untuk menerima undangan grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `AcceptInvitation` Anda harus menentukan grafik ARN.
- AWS CLI: Pada baris perintah, jalankan `accept-invitation`perintah.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

Contoh:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Untuk menolak undangan grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `RejectInvitation` Anda harus menentukan grafik ARN.
- AWS CLI: Pada baris perintah, jalankan `reject-invitation`perintah.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

Contoh:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Menghapus akun Anda dari grafik perilaku

Setelah menerima undangan, Anda dapat menghapus akun dari grafik perilaku kapan saja. Saat Anda menghapus akun dari grafik perilaku, Detektif Amazon berhenti memasukkan data dari akun Anda ke dalam grafik perilaku. Data yang ada tetap dalam grafik perilaku.

Hanya akun yang diundang yang dapat menghapus akun mereka dari grafik perilaku. Akun organisasi tidak dapat menghapus akun mereka dari grafik perilaku organisasi.

Menghapus akun Anda dari grafik perilaku (Konsol)

Anda dapat menggunakan AWS Management Console untuk menghapus akun Anda dari grafik perilaku.

Untuk menghapus akun Anda dari grafik perilaku (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Di bawah Akun administrator saya, untuk grafik perilaku tempat Anda ingin mengundurkan diri, pilih Mengundurkan diri.

Menghapus akun Anda dari grafik perilaku (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS Command Line Interface untuk menghapus akun Anda dari grafik perilaku.

Untuk menghapus akun Anda dari grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `DisassociateMembership` Anda harus menentukan grafik ARN.
- AWS CLI: Pada baris perintah, jalankan `disassociate-membership`perintah.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

Contoh:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Pengaruh tindakan akun pada grafik perilaku

Tindakan ini memiliki efek berikut pada data dan akses Detektif Amazon.

Detektif dinonaktifkan

Ketika akun administrator menonaktifkan Detektif, hal berikut terjadi:

- Grafik perilaku dihapus.
- Detective berhenti menelan data dari akun administrator dan akun anggota untuk grafik perilaku tersebut.

Akun anggota dihapus dari grafik perilaku

Ketika akun anggota dihapus dari grafik perilaku, Detektif berhenti menelan data dari akun tersebut.

Data yang ada dalam grafik perilaku tidak terpengaruh.

Untuk akun yang diundang, akun dihapus dari daftar akun anggota saya.

Untuk akun organisasi dalam grafik perilaku organisasi, status akun berubah menjadi Bukan anggota.

Akun anggota meninggalkan organisasi

Ketika akun anggota meninggalkan organisasi, hal berikut terjadi:

- Akun dihapus dari daftar Akun anggota saya untuk grafik perilaku organisasi.
- Detective berhenti menelan data dari akun itu.

Data yang ada dalam grafik perilaku tidak terpengaruh.

AWS akun ditangguhkan

Ketika akun administrator ditangguhkan AWS, akun kehilangan izin untuk melihat grafik perilaku di Detektif. Detective berhenti menelan data ke dalam grafik perilaku.

Ketika akun anggota ditangguhkan AWS, Detektif berhenti menelan data untuk akun itu.

Setelah 90 hari, akun dihentikan atau diaktifkan kembali. Ketika akun administrator diaktifkan kembali, izin Detektif-nya dipulihkan. Detektif melanjutkan pengambilan data dari akun. Ketika akun anggota diaktifkan kembali, Detektif melanjutkan pengambilan data dari akun tersebut.

AWS akun ditutup

Ketika AWS akun ditutup, Detektif menanggapi penutupan sebagai berikut.

- Untuk akun administrator, Detective menghapus grafik perilaku.
- Untuk akun anggota, Detektif menghapus akun dari grafik perilaku.

AWS menyimpan data kebijakan untuk akun selama 90 hari sejak tanggal efektif penutupan akun administrator. Pada akhir periode 90 hari, AWS secara permanen menghapus semua data kebijakan untuk akun.

- Untuk mempertahankan temuan selama lebih dari 90 hari, Anda dapat mengarsipkan kebijakan. Anda juga dapat menggunakan tindakan kustom dengan EventBridge aturan untuk menyimpan temuan dalam bucket S3.
- Selama AWS mempertahankan data kebijakan, ketika Anda membuka kembali akun yang ditutup, AWS menetapkan kembali akun sebagai administrator layanan dan memulihkan data kebijakan layanan untuk akun tersebut.
- Untuk informasi selengkapnya, lihat Menutup akun.

> **Important**
>
> Untuk pelanggan di AWS GovCloud (US) Wilayah:
>
> - Sebelum menutup akun Anda, buat cadangan lalu hapus sumber daya akun. Anda tidak akan lagi memiliki akses ke mereka setelah Anda menutup akun.

Menggunakan skrip Amazon Detective Python untuk mengelola akun

Amazon Detective menyediakan satu set skrip Python open-source di repositori. GitHub amazon-detective-multiaccount-scripts Skrip membutuhkan Python 3.

Anda dapat menggunakan ini untuk melakukan tugas-tugas berikut:

- Aktifkan Detektif untuk akun administrator di seluruh Wilayah.

  Saat mengaktifkan Detektif, Anda dapat menetapkan nilai tag ke grafik perilaku.
- Tambahkan akun anggota ke grafik perilaku akun administrator di seluruh Wilayah.
- Secara opsional mengirim email undangan ke akun anggota. Anda juga dapat mengonfigurasi permintaan untuk tidak mengirim email undangan.
- Hapus akun anggota dari grafik perilaku akun administrator di seluruh Wilayah.
- Nonaktifkan Detektif untuk akun administrator di seluruh Wilayah. Ketika akun administrator menonaktifkan Detektif, grafik perilaku akun administrator di setiap Wilayah akan dinonaktifkan.

Ikhtisar **`enableDetective.py`** skrip

`enableDetective.py`Script melakukan hal berikut:

1. Mengaktifkan Detektif masuk untuk akun administrator di setiap Wilayah tertentu, jika akun administrator belum mengaktifkan Detektif di Wilayah tersebut.

   Saat Anda menggunakan skrip untuk mengaktifkan Detektif, Anda dapat menetapkan nilai tag ke grafik perilaku.
2. Secara opsional mengirim undangan dari akun administrator ke akun anggota yang ditentukan untuk setiap grafik perilaku.

   Pesan email undangan menggunakan konten pesan default dan tidak dapat disesuaikan.

   Anda juga dapat mengonfigurasi permintaan untuk tidak mengirim email undangan.
3. Secara otomatis menerima undangan untuk akun anggota.

   Karena skrip secara otomatis menerima undangan, akun anggota dapat mengabaikan pesan-pesan ini.

   Kami merekomendasikan untuk menghubungi akun anggota secara langsung untuk memberi tahu mereka bahwa undangan diterima secara otomatis.

Ikhtisar **`disableDetective.py`** skrip

`disableDetective.py`Skrip menghapus akun anggota yang ditentukan dari grafik perilaku akun administrator di seluruh Wilayah yang ditentukan.

Ini juga menyediakan opsi untuk menonaktifkan Detektif untuk akun administrator di seluruh Wilayah yang ditentukan.

Izin yang diperlukan untuk skrip

Skrip memerlukan AWS peran yang sudah ada sebelumnya di akun administrator dan di semua akun anggota yang Anda tambahkan atau hapus.

> **Note**
>
> Nama peran harus sama di semua akun.

Praktik terbaik yang direkomendasikan oleh kebijakan IAM adalah menggunakan peran yang paling sedikit cakupan. Untuk menjalankan alur kerja skrip untuk membuat grafik, membuat anggota, dan menambahkan anggota ke grafik, izin yang diperlukan adalah:

- detektif: CreateGraph
- detektif: CreateMembers
- detektif: DeleteGraph
- detektif: DeleteMembers
- detektif: ListGraphs
- detektif: ListMembers
- detektif: AcceptInvitation

Hubungan kepercayaan peran

Hubungan kepercayaan peran harus memungkinkan instans atau kredensil lokal Anda untuk mengambil peran tersebut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Jika Anda tidak memiliki peran umum yang menyertakan izin yang diperlukan, Anda harus membuat peran dengan setidaknya izin tersebut di setiap akun anggota. Anda juga harus membuat peran di akun administrator.

Saat Anda membuat peran, pastikan Anda melakukan hal berikut:

- Gunakan nama peran yang sama di setiap akun.

- Tambahkan izin yang diperlukan di atas (disarankan) atau pilih kebijakan AmazonDetectiveFullAccessterkelola.
- Tambahkan blok hubungan kepercayaan peran seperti yang dibahas di atas.

Untuk mengotomatiskan proses ini, Anda dapat menggunakan `EnableDetective.yaml` AWS CloudFormation template. Karena template hanya membuat sumber daya global, template dapat dijalankan di Wilayah mana pun.

Menyiapkan lingkungan run untuk skrip Python

Anda dapat menjalankan skrip dari instans EC2 atau dari mesin lokal.

Meluncurkan dan mengonfigurasi instans EC2

Salah satu opsi untuk menjalankan skrip adalah menjalankannya dari instance EC2.

Untuk meluncurkan dan mengkonfigurasi instans EC2

1. Luncurkan instans EC2 di akun administrator Anda. Untuk detail tentang cara meluncurkan instans EC2, lihat Memulai Instans Linux Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Linux.
2. Lampirkan ke instance peran IAM yang memiliki izin untuk memungkinkan instance memanggil `AssumeRole` dalam akun administrator.

   Jika Anda menggunakan `EnableDetective.yaml` AWS CloudFormation template, maka peran instance dengan profil bernama `EnableDetective` telah dibuat.

   Jika tidak, untuk informasi tentang membuat peran instans, lihat posting blog Mudah Ganti atau Lampirkan Peran IAM ke Instans EC2 yang Ada dengan Menggunakan Konsol EC2.
3. Instal perangkat lunak yang diperlukan:
   - TEPAT: `sudo apt-get -y install python3-pip python3 git`
   - RPM: `sudo yum -y install python3-pip python3 git`
   - Boto (versi minimum 1.15): `sudo pip install boto3`
4. Kloning repositori ke instans EC2.

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

Mengkonfigurasi mesin lokal untuk menjalankan skrip

Anda juga dapat menjalankan skrip dari mesin lokal Anda.

Untuk mengkonfigurasi mesin lokal untuk menjalankan skrip

1. Pastikan Anda telah menyiapkan kredensi mesin lokal untuk akun administrator Anda yang memiliki izin untuk menelepon. `AssumeRole`
2. Instal perangkat lunak yang diperlukan:
   - Python 3
   - Boto (versi minimum 1.15)
   - GitHub skrip

Platform	Instruksi pengaturan
Windows	1. Instal Python 3 (https://www.python.org/downloads/windows/). 2. Buka prompt perintah. 3. Untuk menginstal Boto, jalankan: `pip install boto3` 4. Unduh kode sumber skrip dari GitHub (https://github.com/aws-samples/ amazon-detective-multiaccount-scripts).
Mac	1. Instal Python 3 (https://www.python.org/downloads/mac-osx/). 2. Buka prompt perintah. 3. Untuk menginstal Boto, jalankan: `pip install boto3` 4. Unduh kode sumber skrip dari GitHub (https://github.com/aws-samples/ amazon-detective-multiaccount-scripts).
Linux	1. Untuk menginstal Python 3, jalankan salah satu dari berikut ini: • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python`

Platform	Instruksi pengaturan
	2. Untuk menginstal Boto, jalankan: `sudo pip install boto3` 3. Kloning kode sumber skrip dari https://github.com/aws-samples/. amazon-detective-multiaccount-scripts

Membuat `.csv` daftar akun anggota untuk menambah atau menghapus

Untuk mengidentifikasi akun anggota yang akan ditambahkan atau dihapus dari grafik perilaku, Anda menyediakan `.csv` file yang berisi daftar akun.

Buat daftar setiap akun pada baris terpisah. Setiap entri akun anggota berisi ID AWS akun dan alamat email pengguna root akun.

Lihat contoh berikut ini:

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Berlari `enableDetective.py`

Anda dapat menjalankan `enableDetective.py` skrip dari instans EC2 atau mesin lokal Anda.

Untuk menjalankan **`enableDetective.py`**

1. Salin `.csv` file ke `amazon-detective-multiaccount-scripts` direktori pada instans EC2 atau mesin lokal Anda.
2. Ubah ke direktori `amazon-detective-multiaccount-scripts`.
3. Jalankan `enableDetective.py` skrip.

```
enableDetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
disable_email
```

Saat Anda menjalankan skrip, ganti nilai berikut:

administratorAccountID

ID AWS akun untuk akun administrator.

roleName

Nama AWS peran yang akan diambil di akun administrator dan setiap akun anggota.

inputFileName

Nama `.csv` file yang berisi daftar akun anggota untuk ditambahkan ke grafik perilaku akun administrator.

tagValueList

(Opsional) Daftar nilai tag yang dipisahkan koma untuk ditetapkan ke grafik perilaku baru.

Untuk setiap nilai tag, formatnya adalah*key*=*value*. Misalnya:

```
--tags Department=Finance,Geo=Americas
```

regionList

(Opsional) Daftar Wilayah yang dipisahkan koma untuk menambahkan akun anggota ke grafik perilaku akun administrator. Misalnya:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

Akun administrator mungkin belum mengaktifkan Detektif di Wilayah. Dalam hal ini, skrip mengaktifkan Detektif dan membuat grafik perilaku baru untuk akun administrator.

Jika Anda tidak memberikan daftar Wilayah, maka skrip bertindak di semua Wilayah yang didukung Detektif.

`--disable_email`

(Opsional) Jika disertakan, Detektif tidak mengirim email undangan ke akun anggota.

Berlari **`disableDetective.py`**

Anda dapat menjalankan `disableDetective.py` skrip dari instans EC2 atau mesin lokal Anda.

Untuk menjalankan **`disableDetective.py`**

1. Salin `.csv` file ke `amazon-detective-multiaccount-scripts` direktori.
2. Untuk menggunakan `.csv` file untuk menghapus akun anggota yang terdaftar dari grafik perilaku akun administrator di seluruh daftar Wilayah yang ditentukan, jalankan `disableDetective.py` skrip sebagai berikut:

   ```
   disabledetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --disabled_regions regionList
   ```

3. Untuk menonaktifkan Detektif untuk akun administrator di semua Wilayah, jalankan `disableDetective.py` skrip dengan bendera. `--delete-master`

   ```
   disabledetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --disabled_regions regionList --delete_master
   ```

Saat Anda menjalankan skrip, ganti nilai berikut:

`administratorAccountID`

ID AWS akun untuk akun administrator.

`roleName`

Nama AWS peran yang akan diambil di akun administrator dan setiap akun anggota.

`inputFileName`

Nama `.csv` file yang berisi daftar akun anggota untuk dihapus dari grafik perilaku akun administrator.

Anda harus memberikan `.csv` file bahkan jika Anda menonaktifkan Detektif.

`regionList`

(Opsional) Daftar Wilayah yang dipisahkan koma untuk melakukan salah satu hal berikut:

- Hapus akun anggota dari grafik perilaku akun administrator.
- Jika `--delete-master` bendera disertakan, nonaktifkan Detektif.

Misalnya:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

Jika Anda tidak memberikan daftar Wilayah, maka skrip bertindak di semua Wilayah yang didukung Detektif.

Integrasi dengan Amazon Security Lake

Amazon Security Lake adalah layanan danau data keamanan yang dikelola sepenuhnya. Anda dapat menggunakan Security Lake untuk secara otomatis memusatkan data keamanan dari AWS lingkungan, penyedia SaaS, sumber lokal, sumber cloud, dan sumber pihak ketiga ke dalam data lake yang dibuat khusus yang disimpan di akun Anda. AWS Security Lake membantu Anda menganalisis data keamanan, sehingga Anda bisa mendapatkan pemahaman yang lebih lengkap tentang postur keamanan Anda di seluruh organisasi Anda. Dengan Security Lake, Anda juga dapat meningkatkan perlindungan beban kerja, aplikasi, dan data Anda.

Amazon Detective terintegrasi dengan Amazon Security Lake, yang berarti Anda dapat menanyakan dan mengambil data log mentah yang disimpan oleh Security Lake.

Dengan menggunakan integrasi ini, Anda dapat mengumpulkan log dan peristiwa dari sumber berikut yang didukung oleh Security Lake secara native.

- AWS CloudTrail acara manajemen versi 1.0
- Log Aliran Amazon Virtual Private Cloud (Amazon VPC) versi 1.0

Untuk detail tentang cara Security Lake secara otomatis mengonversi log dan peristiwa yang berasal dari AWS layanan yang didukung secara asli ke skema OCSF, lihat Panduan Pengguna Amazon Security Lake.

Setelah Anda mengintegrasikan Detective dengan Security Lake, Detective mulai menarik log mentah dari Security Lake yang terkait dengan AWS CloudTrail peristiwa manajemen dan Amazon VPC Flow Logs. Untuk detail selengkapnya, lihat Menanyakan log mentah.

Untuk mengintegrasikan Detective dengan Security Lake, selesaikan langkah-langkah berikut:

1. Sebelum Anda memulai

   Gunakan akun manajemen Organizations untuk menunjuk administrator Security Lake yang didelegasikan untuk organisasi Anda. Pastikan Security Lake diaktifkan dan verifikasi bahwa Security Lake mengumpulkan log dan peristiwa dari peristiwa AWS CloudTrail manajemen dan Log Aliran Amazon Virtual Private Cloud (Amazon VPC).

   Sejalan dengan Arsitektur Referensi Keamanan, Detective merekomendasikan penggunaan akun Log Archive dan menunda penggunaan akun Security Tooling untuk penyebaran Security Lake.

2. Buat pelanggan Security Lake

   Untuk menggunakan log dan acara dari Amazon Security Lake, Anda harus menjadi pelanggan Security Lake. Ikuti langkah-langkah berikut untuk memberikan akses kueri ke administrator akun Detektif.

3. Tambahkan izin yang diperlukan AWS Identity and Access Management (IAM) ke identitas IAM Anda.
   - Tambahkan izin ini untuk membuat integrasi Detektif dengan Security Lake:
     - Lampirkan izin AWS Identity and Access Management (IAM) ini ke identitas IAM Anda. Untuk detailnya, lihat bagian Tambahkan izin IAM yang diperlukan ke akun Anda.
     - Tambahkan kebijakan IAM ini ke prinsipal IAM yang Anda rencanakan untuk digunakan untuk lulus peran AWS CloudFormation layanan. Untuk detail selengkapnya, lihat bagian Tambahkan izin ke prinsipal IAM Anda.
   - Jika Anda telah mengintegrasikan Detective dengan Security Lake, gunakan integrasi melampirkan izin ini (IAM) ke identitas IAM Anda. Untuk detailnya, lihat bagian Tambahkan izin IAM yang diperlukan ke akun Anda.
4. Terima undangan ARN Berbagi Sumber Daya dan aktifkan integrasi

Gunakan AWS CloudFormation template untuk mengatur parameter yang diperlukan untuk membuat dan mengelola akses kueri untuk pelanggan Security Lake. Untuk langkah-langkah rinci untuk membuat tumpukan, lihat Membuat tumpukan menggunakan AWS CloudFormation template. Setelah Anda selesai membuat tumpukan, aktifkan integrasi.

Untuk demonstrasi cara mengintegrasikan Detektif Amazon dengan Amazon Security Lake menggunakan konsol Detektif, tonton video berikut: Integrasi Detektif Amazon dengan Amazon Security Lake- Cara Pengaturan ->

Sebelum Anda memulai

Security Lake terintegrasi dengan AWS Organizations mengelola pengumpulan log di beberapa akun dalam suatu organisasi. Untuk menggunakan Security Lake untuk organisasi, akun AWS Organizations manajemen Anda harus terlebih dahulu menunjuk administrator Security Lake yang didelegasikan untuk organisasi Anda. Administrator Security Lake yang didelegasikan kemudian harus mengaktifkan Security Lake, dan mengaktifkan log dan pengumpulan acara untuk akun anggota di organisasi.

Sebelum Anda mengintegrasikan Security Lake, dengan Detective, pastikan Security Lake diaktifkan untuk akun administrator Security Lake. Untuk langkah-langkah mendetail tentang cara mengaktifkan Security Lake, lihat Memulai di Panduan Pengguna Amazon Security Lake.

Selain itu, verifikasi bahwa Security Lake mengumpulkan log dan peristiwa dari peristiwa AWS CloudTrail manajemen dan Log Aliran Amazon Virtual Private Cloud (Amazon VPC). Untuk detail selengkapnya tentang pengumpulan log di Security Lake, lihat Mengumpulkan data dari AWS layanan di Panduan Pengguna Amazon Security Lake.

Langkah 1: Buat pelanggan Security Lake

Untuk menggunakan log dan acara dari Amazon Security Lake, Anda harus menjadi pelanggan Security Lake. Pelanggan dapat menanyakan dan mengakses data yang dikumpulkan Security Lake. Pelanggan dengan akses kueri dapat melakukan kueri AWS Lake Formation tabel secara langsung di bucket Amazon Simple Storage Service (Amazon S3) dengan menggunakan layanan seperti Amazon Athena. Untuk menjadi pelanggan, administrator Security Lake harus memberi Anda akses pelanggan yang memungkinkan Anda menanyakan data lake. Untuk informasi tentang cara administrator melakukan hal ini, lihat Membuat pelanggan dengan akses kueri di Panduan Pengguna Amazon Security Lake.

Ikuti langkah-langkah berikut untuk memberikan akses kueri ke administrator akun Detektif.

Untuk membuat pelanggan Detektif di Security Lake

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Integrasi.
3. Di panel pelanggan Security Lake, perhatikan nilai ID Akun dan ID Eksternal.

   Minta administrator Security Lake untuk menggunakan ID ini untuk:

   - Untuk membuat pelanggan Detektif untukmu di Security Lake.
   - Untuk mengkonfigurasi pelanggan agar memiliki akses kueri.
   - Untuk memastikan bahwa pelanggan kueri Security Lake dibuat dengan izin Lake Formation, pilih Lake Formation sebagai Metode Akses Data di konsol Security Lake.

   Saat administrator Security Lake membuat pelanggan untuk Anda, Security Lake menghasilkan ARN Berbagi Sumber Daya Amazon untuk Anda. Minta administrator untuk mengirimkan ARN ini kepada Anda.

4. Masukkan ARN Berbagi Sumber Daya yang disediakan oleh administrator Security Lake di panel pelanggan Security Lake.
5. Setelah Anda menerima ARN Berbagi Sumber Daya dari Administrator Danau Keamanan, masukkan ARN di kotak ARN Berbagi Sumber Daya di panel pelanggan Security Lake.

Langkah 2: Tambahkan izin IAM yang diperlukan ke akun Anda

Untuk mengaktifkan integrasi Detektif dengan Security Lake, Anda harus melampirkan kebijakan izin AWS Identity and Access Management (IAM) berikut ke identitas IAM Anda.

Lampirkan kebijakan inline berikut ke peran. Ganti `athena-results-bucket` dengan nama bucket Amazon S3 Anda jika Anda ingin menggunakan bucket Amazon S3 Anda sendiri untuk menyimpan hasil kueri Athena. Jika Anda ingin Detektif membuat bucket Amazon S3 secara otomatis untuk menyimpan hasil kueri Athena, hapus keseluruhan dari kebijakan IAM. `S3ObjectPermissions`

Jika Anda tidak memiliki izin yang diperlukan untuk melampirkan kebijakan ini ke identitas IAM Anda, hubungi administrator Anda AWS . Jika Anda memiliki izin yang diperlukan tetapi terjadi masalah, lihat Memecahkan masalah IAM umum di Panduan Pengguna IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ObjectPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::<athena-results-bucket>",
        "arn:aws:s3:::<athena-results-bucket>/*"
      ]
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:aws:glue:*:<ACCOUNT ID>:database/amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:table/amazon_security_lake*/
amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "lakeformation:GetDataAccess"
      ],
      "Resource": "*"
    },
    {
       "Effect": "Allow",
        "Action": [
          "ssm:GetParametersByPath"
        ],
        "Resource": [
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/ResourceShareArn",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/S3Bucket",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/TableNames",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/DatabaseName",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/StackId"
        ]
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetTemplateSummary",
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "securitylake.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Langkah 3: Terima undangan ARN Berbagi Sumber Daya dan aktifkan integrasi

Untuk mengakses log data mentah dari Security Lake, Anda harus menerima undangan Berbagi Sumber Daya dari akun Security Lake yang dibuat oleh administrator Security Lake. Anda juga memerlukan AWS Lake Formation izin untuk mengatur berbagi tabel lintas akun. Selain itu, Anda harus membuat bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) yang dapat menerima log kueri mentah.

Pada langkah berikutnya, Anda akan menggunakan AWS CloudFormation templat untuk membuat tumpukan untuk: menerima undangan ARN Berbagi Sumber Daya, membuat sumber daya yang Perayap AWS Glue diperlukan, dan AWS Lake Formation memberikan izin administrator.

Untuk membuat AWS CloudFormation tumpukan

1. Buat CloudFormation tumpukan baru menggunakan CloudFormation template. Untuk detail selengkapnya, lihat Membuat tumpukan menggunakan AWS CloudFormation template.
2. Setelah Anda selesai membuat tumpukan, pilih Aktifkan integrasi.

Membuat tumpukan menggunakan AWS CloudFormation template

Detective menyediakan AWS CloudFormation template, yang dapat Anda gunakan untuk mengatur parameter yang diperlukan untuk membuat dan mengelola akses kueri untuk pelanggan Security Lake.

Langkah 1: Buat peran AWS CloudFormation layanan

Anda harus membuat peran AWS CloudFormation layanan untuk membuat tumpukan menggunakan AWS CloudFormation template. Jika Anda tidak memiliki izin yang diperlukan untuk membuat peran layanan, hubungi administrator akun administrator Detektif. Untuk informasi selengkapnya tentang peran AWS CloudFormation layanan, lihat peran AWS CloudFormation layanan.

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, pilih Peran, dan lalu pilih Buat peran.
3. Untuk Pilih entitas tepercaya, pilih AWS layanan.
4. Pilih AWS CloudFormation. Lalu, pilih Selanjutnya.
5. Masukkan nama untuk peran. Misalnya, `CFN-DetectiveSecurityLakeIntegration`.
6. Lampirkan kebijakan inline berikut ke peran. Ganti `<Account ID>` dengan ID AWS Akun Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudFormationPermission",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateChangeSet"
            ],
            "Resource": [
```

```
                "arn:aws:cloudformation:*:aws:transform/*"
            ]
        },
        {
            "Sid": "IamPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:CreatePolicy",
                "iam:DeletePolicy",
                "iam:PassRole",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::<ACCOUNT ID>:role/*",
                "arn:aws:iam::<ACCOUNT ID>:policy/*"
            ]
        },
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket*",
                "s3:PutBucket*",
                "s3:GetBucket*",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "LambdaPermissions",
            "Effect": "Allow",
```

```
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:TagResource",
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:*:<ACCOUNT ID>:function:*"
            ]
        },
        {
            "Sid": "CloudwatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        },
        {
            "Sid": "KmsPermission",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:<ACCOUNT ID>:key/*"
        }
    ]
}
```

Langkah 2: Tambahkan izin ke kepala IAM Anda.

Anda memerlukan izin berikut untuk membuat tumpukan menggunakan peran CloudFormation layanan yang Anda buat pada langkah sebelumnya. Tambahkan kebijakan IAM berikut ke prinsipal IAM yang Anda rencanakan untuk digunakan untuk lulus peran CloudFormation layanan. Anda akan menganggap prinsip IAM ini untuk membuat tumpukan. Jika Anda tidak memiliki izin yang diperlukan untuk menambahkan kebijakan IAM, hubungi administrator akun administrator Detektif.

> **Note**
>
> Dalam kebijakan berikut, yang `CFN-DetectiveSecurityLakeIntegration` digunakan dalam kebijakan ini mengacu pada peran yang Anda buat di langkah peran `Creating an AWS CloudFormation` layanan sebelumnya. Ubah ke nama peran yang Anda masukkan pada langkah sebelumnya jika berbeda.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
            "Sid": "PassRole",
            "Effect": "Allow",
            "Action":
            [
               "iam:GetRole",
               "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
       },
       {
           "Sid": "RestrictCloudFormationAccess",
           "Effect": "Allow",
           "Action": [
               "cloudformation:CreateStack",
               "cloudformation:DeleteStack",
               "cloudformation:UpdateStack"
           ],
           "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*",
           "Condition": {
               "StringEquals": {
                   "cloudformation:RoleArn": [
                       "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
                   ]
               }
           }
       },
       {
           "Sid": "CloudformationDescribeStack",
```

```
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:GetStackPolicy"
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*"
        },
        {
            "Sid": "CloudformationListStacks",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        }
    ]
}
```

Langkah 3: Tentukan nilai kustom di AWS CloudFormation konsol

1. Pergi ke AWS CloudFormation konsol dari Detektif.
2. (Opsional) Masukkan nama Stack. Nama tumpukan diisi secara otomatis. Anda dapat mengubah nama tumpukan menjadi nama yang tidak bertentangan dengan nama tumpukan yang ada.
3. Masukkan Parameter berikut.

    - AthenaResultsBucket— Jika Anda tidak memasukkan nilai, template ini menghasilkan bucket Amazon S3. Jika Anda ingin menggunakan bucket Anda sendiri, masukkan nama bucket untuk menyimpan hasil kueri Athena. Jika Anda menggunakan bucket sendiri, pastikan bucket berada di Region yang sama dengan ARN Resource Share. Jika Anda menggunakan bucket sendiri, pastikan yang `LakeFormationPrincipals` Anda pilih memiliki izin untuk menulis objek dan membaca objek dari bucket. Untuk detail selengkapnya tentang izin bucket, lihat Hasil kueri dan kueri terbaru di Panduan Pengguna Amazon Athena.

- dtRegion - Bidang ini sudah diisi sebelumnya. Jangan mengubah nilai di bidang ini.
- LakeFormationPrincipals— Masukkan ARN dari prinsipal IAM (misalnya, ARN peran IAM) yang ingin Anda berikan akses untuk menggunakan integrasi Security Lake, dipisahkan dengan koma. Ini bisa jadi analis keamanan dan insinyur keamanan Anda yang menggunakan Detektif.

  Anda hanya dapat menggunakan prinsip IAM yang sebelumnya Anda lampirkan izin IAM di langkah [. `Step 2: Add the required IAM permissions to your account]`
- ResourceShareARN - Bidang ini sudah diisi sebelumnya. Jangan mengubah nilai di bidang ini.

4. Izin

   Peran IAM - Pilih peran yang Anda buat di `Creating an AWS CloudFormation Service Role` langkah. Secara opsional, Anda dapat mengosongkannya jika peran IAM Anda saat ini memiliki semua izin yang diperlukan di langkah tersebut. `Creating an AWS CloudFormation Service Role`
5. Tinjau dan centang semua kotak I Acknowledge dan kemudian klik tombol Create stack. Untuk lebih jelasnya, tinjau sumber daya IAM berikut yang akan dibuat.

```
* ResourceShareAcceptorCustomResourceFunction
    - ResourceShareAcceptorLambdaRole
    - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
    - SsmParametersLambdaRole
    - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
    - GlueDatabaseLambdaRole
    - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
    - GlueTablesLambdaRole
    - GlueTablesLogsAccessPolicy
```

Langkah 4: Tambahkan kebijakan bucket Amazon S3 ke prinsipal IAM di **`LakeFormationPrincipals`**

(Opsional) Jika Anda membiarkan template ini menghasilkan `AthenaResultsBucket` untuk Anda, Anda harus melampirkan kebijakan berikut ke prinsipal IAM di. `LakeFormationPrincipals`

```
{
```

```
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}
```

Ganti `athena-results-bucket` dengan `AthenaResultsBucket` nama. `AthenaResultsBucket`Dapat ditemukan di AWS CloudFormation konsol:

1. Buka AWS CloudFormation konsol di https://console.aws.amazon.com/cloudformation.
2. Klik pada Stack Anda.
3. Klik tab Sumber Daya.
4. Cari ID logis `AthenaResultsBucket` dan salin ID fisiknya.

Menghapus tumpukan CloudFormation

Jika Anda tidak menghapus tumpukan yang ada, pembuatan tumpukan baru di Wilayah yang sama akan gagal. Anda dapat menghapus CloudFormation tumpukan dengan menggunakan CloudFormation konsol atau menggunakan AWS CLI.

Untuk menghapus AWS CloudFormation tumpukan (Konsol)

1. Buka AWS CloudFormation konsol di https://console.aws.amazon.com/cloudformation.
2. Pada halaman Stacks di CloudFormation konsol, pilih tumpukan yang ingin Anda hapus. Tumpukan pasti sedang berjalan.
3. Di panel detail tumpukan, pilih Hapus.
4. Pilih Hapus tumpukan saat diminta.

> **Note**
>
> Operasi penghapusan tumpukan tidak dapat dihentikan setelah penghapusan tumpukan dimulai. Tumpukan diproses ke `DELETE_IN_PROGRESS` status.

Setelah penghapusan tumpukan selesai, tumpukan akan berada di `DELETE_COMPLETE` status.

Memecahkan masalah kesalahan penghapusan tumpukan

Jika Anda melihat kesalahan izin dengan pesan `Failed to delete stack` setelah mengklik `Delete` tombol, peran IAM Anda tidak memiliki CloudFormation izin untuk menghapus tumpukan. Hubungi administrator akun Anda untuk menghapus tumpukan.

Untuk menghapus CloudFormation tumpukan (AWS CLI)

Masukkan perintah berikut di antarmuka AWS CLI:

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
      arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

`CFN-DetectiveSecurityLakeIntegration`adalah peran layanan yang Anda buat di `Creating an AWS CloudFormation Service Role` langkah.

Mengubah konfigurasi integrasi

Jika Anda ingin mengubah salah satu parameter yang Anda gunakan untuk mengintegrasikan Detective dengan Security Lake, Anda dapat mengeditnya, dan kemudian mengaktifkan integrasi lagi. Anda dapat mengedit AWS CloudFormation template untuk mengaktifkan kembali integrasi ini untuk skenario berikut:

- Untuk memperbarui langganan Security Lake, Anda dapat membuat pelanggan baru, atau administrator Security Lake dapat memperbarui sumber data untuk langganan yang ada.
- Untuk menentukan bucket Amazon S3 yang berbeda untuk menyimpan log kueri mentah.
- Untuk menentukan prinsip Lake Formation yang berbeda.

Saat mengaktifkan kembali integrasi Detective dengan Security Lake, Anda dapat mengedit ARN Resource Share, dan melihat izin IAM. Untuk mengedit izin IAM, Anda dapat pergi ke konsol IAM

dari Detective. Anda juga dapat mengedit nilai yang sebelumnya Anda masukkan dalam AWS CloudFormation template. Anda harus menghapus CloudFormation tumpukan yang ada dan membuatnya kembali untuk mengaktifkan kembali integrasi.

Untuk mengaktifkan kembali integrasi Detektif dengan Security Lake

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Integrasi.
3. Anda dapat mengedit integrasi menggunakan salah satu dari langkah-langkah ini:
   - Di panel Security Lake, pilih Edit.
   - Di panel Security Lake, pilih View. Di halaman tampilan, pilih Edit.
4. Masukkan ARN Berbagi Sumber Daya baru, untuk mengakses sumber data di Wilayah.
5. Lihat izin IAM saat ini, dan buka konsol IAM, jika Anda ingin mengedit izin IAM.
6. Edit nilai dalam CloudFormation template.
   1. Hapus tumpukan yang ada terlebih dahulu, sebelum membuat tumpukan baru. Jika Anda tidak menghapus tumpukan yang ada dan Anda mencoba membuat tumpukan baru di Wilayah yang sama, permintaan Anda gagal. Untuk detail selengkapnya, lihat Menghapus tumpukan CloudFormation .
   1. Buat CloudFormation tumpukan baru. Untuk detail selengkapnya, lihat Membuat tumpukan menggunakan AWS CloudFormation template.
7. Pilih Aktifkan integrasi.

Menonaktifkan integrasi

Jika Anda menonaktifkan integrasi Detektif dengan Security Lake, Anda tidak dapat lagi meminta data log dan peristiwa dari Security Lake.

Untuk menonaktifkan integrasi Detektif dengan Security Lake

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Integrasi.
3. Hapus tumpukan yang ada. Untuk detail selengkapnya, lihat Menghapus tumpukan CloudFormation .

4. Di panel Nonaktifkan Integrasi Danau Keamanan, pilih Nonaktifkan.

AWS Wilayah yang Didukung

Anda dapat mengintegrasikan Detektif dengan Security Lake di Wilayah berikut AWS .

Nama Wilayah	Wilayah	Titik Akhir	Protokol;
Timur AS (Ohio)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
US West (N. California)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
Asia Pasifik (Sydney)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS
Asia Pasifik (Tokyo)	ap-northeast-1	securitylake.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	securitylake.ca-central-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol;
Europe (Frankfurt)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

Menanyakan log mentah di Detective

Setelah Anda mengintegrasikan Detective dengan Security Lake, Detective mulai menarik log mentah dari Security Lake yang terkait dengan peristiwa AWS CloudTrail manajemen dan Amazon Virtual Private Cloud (Amazon VPC) Flow Logs.

> **Note**
>
> Tidak ada biaya tambahan untuk menanyakan log mentah di Detective. Biaya penggunaan untuk AWS Layanan lain, termasuk Amazon Athena, masih berlaku dengan tarif yang dipublikasikan.

AWS CloudTrail acara manajemen tersedia untuk profil berikut:

- AWS akun
- AWS pengguna
- AWS peran

- AWS peran Sesi
- Instans Amazon EC2
- Bucket Amazon S3
- Alamat IP

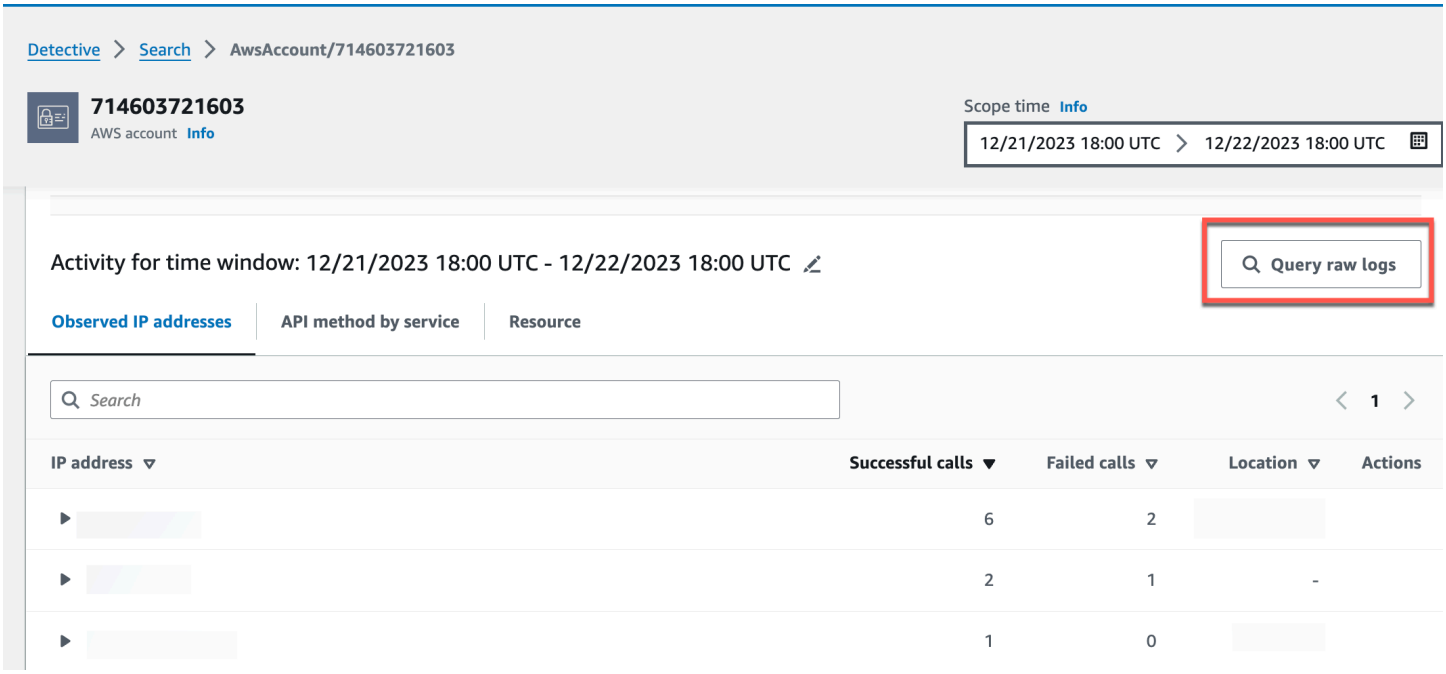
Amazon VPC Flow Logs tersedia untuk profil berikut:

- Instans Amazon EC2
- Pod Kubernetes

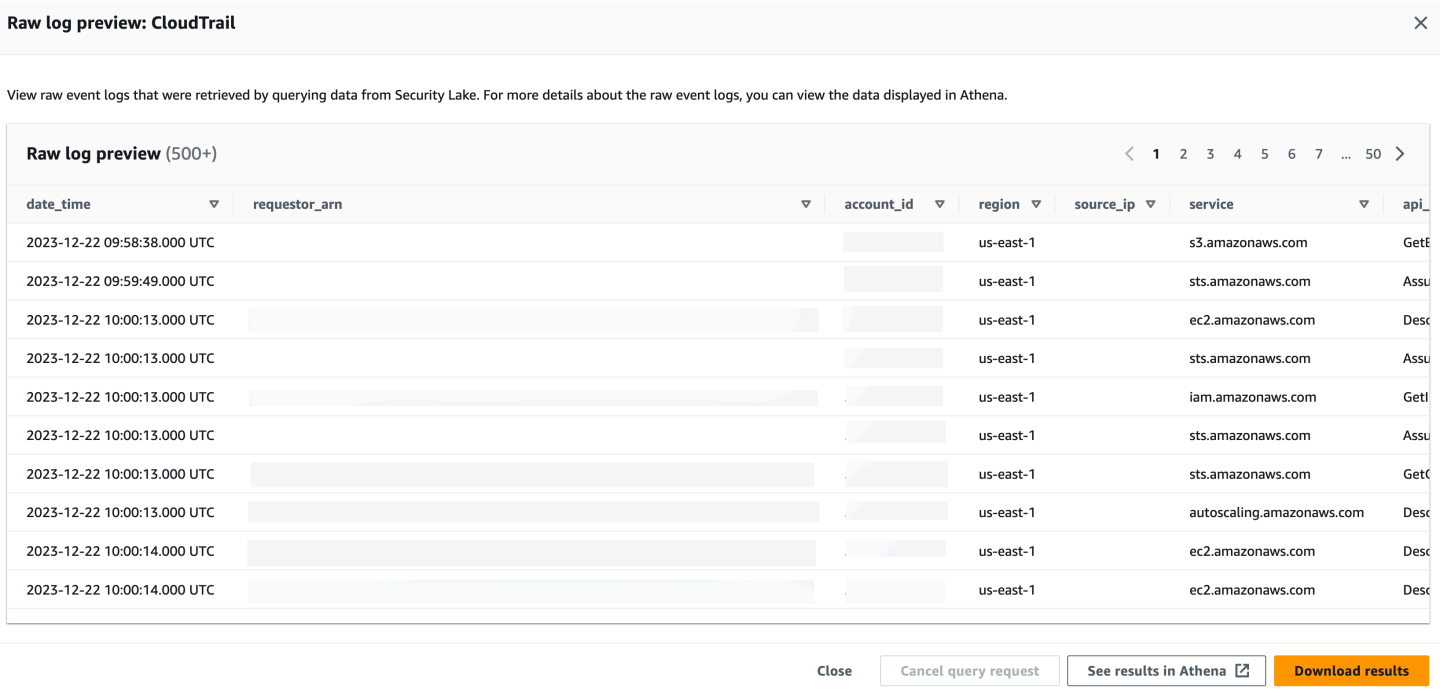
Untuk demonstrasi cara mengintegrasikan Detektif Amazon dengan Amazon Security Lake menggunakan konsol Detektif, tonton video berikut: Integrasi Detektif Amazon dengan Amazon Security Lake- Cara Menggunakan ->

Untuk menanyakan log mentah untuk akun AWS

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Cari dan cari. `AWS account`
3. Di bagian Volume panggilan API Keseluruhan, pilih detail tampilan untuk waktu lingkup.
4. Dari sini, Anda dapat mulai Query log mentah.



Dalam tabel pratinjau log mentah, Anda dapat melihat log dan peristiwa yang diambil dengan menanyakan data dari Security Lake. Untuk detail selengkapnya tentang log peristiwa mentah, Anda dapat melihat data yang ditampilkan di Amazon Athena.



Dari tabel log mentah kueri, Anda dapat Membatalkan permintaan kueri, Melihat hasil di Amazon Athena, dan Unduh hasil sebagai file nilai yang dipisahkan koma (.csv).

Jika Anda melihat log di Detective, tetapi kueri tidak mengembalikan hasil, itu bisa terjadi karena alasan berikut.

- Log mentah mungkin tersedia di Detective sebelum muncul di tabel log Security Lake. Coba lagi nanti.
- Log mungkin hilang dari Security Lake. Jika Anda menunggu untuk jangka waktu yang lama, ini menunjukkan bahwa log hilang dari Security Lake. Hubungi administrator Security Lake Anda untuk mengatasi masalah ini.

Contoh-contoh

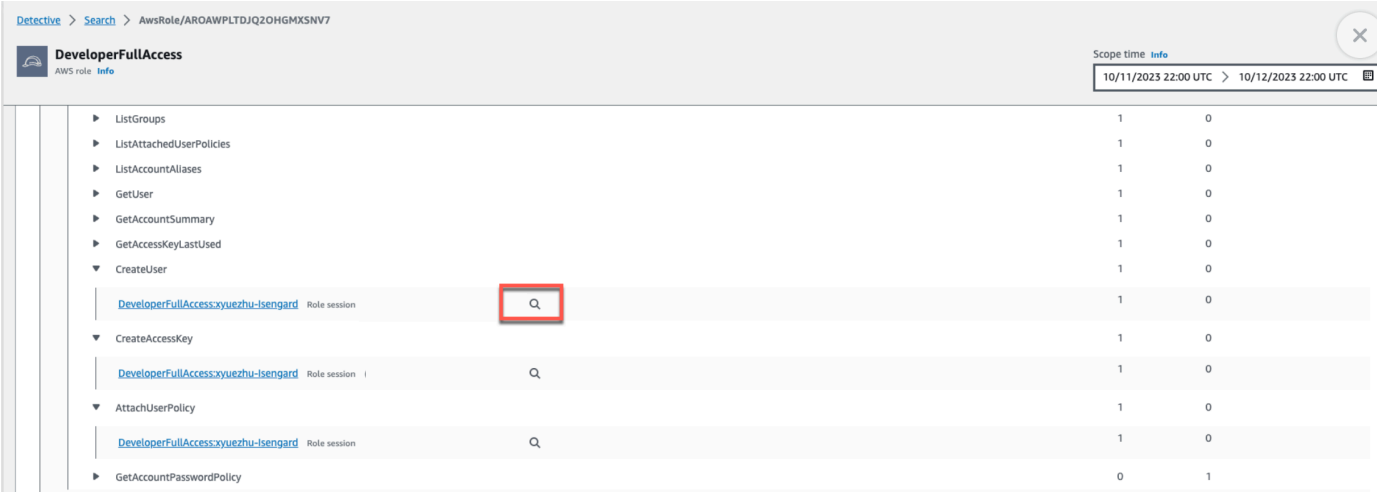
- Kueri log mentah untuk AWS peran
- Kueri log mentah untuk instans Amazon EC2

Kueri log mentah untuk AWS peran

Jika Anda ingin memahami aktivitas AWS peran dalam geolokasi baru, Anda dapat melakukannya di dalam konsol Detektif.

Untuk menanyakan log mentah untuk peran AWS

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Dari halaman Ringkasan Detektif Bagian geolokasi yang baru diamati, catat perannya. AWS
3. Di panel navigasi, pilih Cari dan cari. `AWS role`
4. Untuk AWS peran tersebut, perluas sumber daya untuk menampilkan panggilan API tertentu yang dikeluarkan dari alamat IP tersebut oleh sumber daya tersebut.
5. Pilih ikon kaca pembesar di sebelah panggilan API yang ingin Anda selidiki untuk membuka tabel pratinjau log mentah.

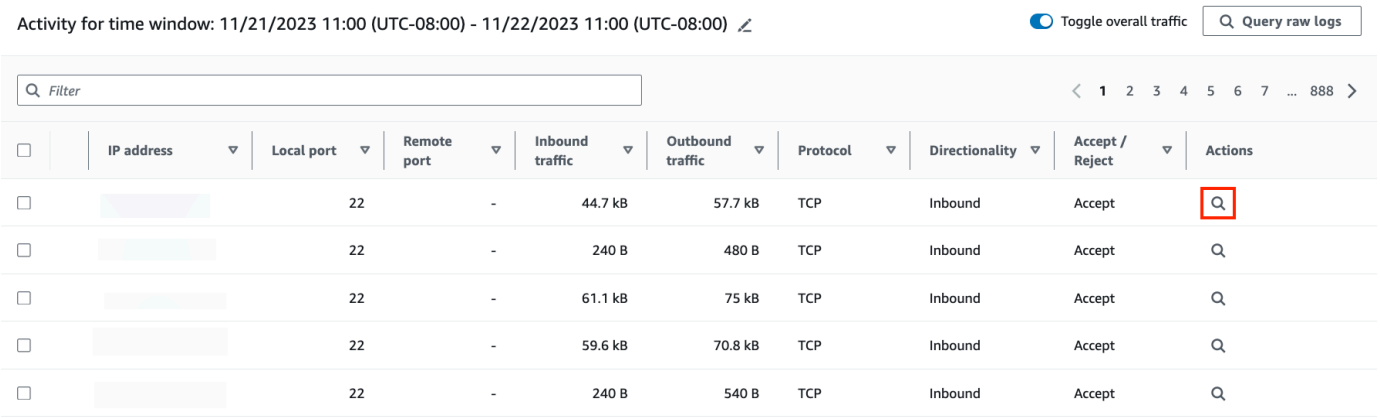


Dalam tabel pratinjau log mentah, Anda dapat melihat log dan peristiwa yang diambil dengan menanyakan data dari Security Lake. Untuk detail selengkapnya tentang log peristiwa mentah, Anda dapat melihat data yang ditampilkan di Amazon Athena.

Dari tabel log mentah kueri, Anda dapat Membatalkan permintaan kueri, Melihat hasil di Amazon Athena, dan Unduh hasil sebagai file nilai yang dipisahkan koma (.csv).

Kueri log mentah untuk instans Amazon EC2

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi, pilih Cari dan cari. `Amazon EC2 instance`
3. Di bagian Volume Aliran VPC Keseluruhan, pilih ikon kaca pembesar di sebelah panggilan API yang ingin Anda selidiki untuk membuka tabel pratinjau log mentah.
4. Dari sini, Anda dapat mulai Query log mentah.



Dalam tabel pratinjau log mentah, Anda dapat melihat log dan peristiwa yang diambil dengan menanyakan data dari Security Lake. Untuk detail selengkapnya tentang log peristiwa mentah, Anda dapat melihat data yang ditampilkan di Amazon Athena.

Dari tabel log mentah kueri, Anda dapat Membatalkan permintaan kueri, Melihat hasil di Amazon Athena, dan Unduh hasil sebagai file nilai yang dipisahkan koma (.csv).

Keamanan di Amazon Detective

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menggambarkan hal ini sebagai dari keamanan cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman.

  Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari AWS program kepatuhan.

  Untuk mempelajari tentang program kepatuhan yang berlaku untuk Detektif Amazon, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Detective. Topik berikut menunjukkan cara mengonfigurasi Detektif untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Detektif Anda.

Konten

Perlindungan data di Amazon Detective

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon Detective. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Detective atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan

supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Detective mengenkripsi semua data yang diproses dan disimpan saat istirahat dan dalam perjalanan.

Konten

Manajemen kunci untuk Amazon Detective

Karena Detective tidak menyimpan data pelanggan yang dapat diidentifikasi secara pribadi, ia menggunakannya. Kunci yang dikelola AWS

Jenis kunci KMS ini dapat digunakan di beberapa akun. Lihat deskripsi kunci yang AWS dimiliki di Panduan AWS Key Management Service Pengembang.

Jenis tombol KMS ini berputar secara otomatis setiap satu tahun (sekitar 365 hari). Lihat deskripsi rotasi kunci di Panduan AWS Key Management Service Pengembang.

Manajemen identitas dan akses untuk Amazon Detective

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Detektif. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Daftar Isi

Audiens

Bagaimana Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Detective.

Pengguna layanan — Jika Anda menggunakan layanan Detektif untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Detektif untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Detective, lihat. Memecahkan masalah identitas dan akses Detektif Amazon

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Detektif di perusahaan Anda, Anda mungkin memiliki akses penuh ke Detektif. Tugas Anda adalah menentukan fitur dan sumber daya Detektif mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Detective, lihat. Bagaimana Amazon Detective bekerja dengan IAM

Administrator IAM — Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Detektif. Untuk melihat contoh kebijakan berbasis identitas Detektif yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas Detektif Amazon

Mengautentikasi Menggunakan Identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas gabungan, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, silakan lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat bagian Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Pengguna dan Grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Apabila memungkinkan, kami merekomendasikan untuk mengandalkan pada kredensial sementara alih-alih membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, silakan lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah pengelolaan izin untuk sejumlah besar pengguna sekaligus. Sebagai contoh, Anda dapat memiliki grup yang diberi nama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, silakan lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas gabungan mengautentikasi, identitas tersebut terhubung dengan peran dan memperoleh izin yang ditentukan oleh peran. Untuk informasi tentang peran-peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi serangkain izin. Untuk mengontrol apa yang dapat diakses oleh identitas Anda setelah diautentikasi, Pusat Identitas IAM menghubungkan izin yang ditetapkan dengan peran di IAM. Untuk informasi tentang rangkaian izin, lihat Rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya

(alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Layanan dapat melakukan hal tersebut menggunakan izin pengguna utama, menggunakan peran layanan, atau menggunakan peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Saat menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan Pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan pada instans EC2 untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola Akses Menggunakan Kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan dapat menentukan permintaan yang diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan Berbasis Identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol tindakan apa yang dapat dilakukan oleh pengguna dan peran, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang

dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, lihat Memilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan Berbasis Sumber Daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan tepercaya peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh pengguna utama tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar Kontrol Akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Pengembang Amazon Simple Storage Service.

Tipe Kebijakan Lainnya

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai Tipe Kebijakan

Jika beberapa jenis kebijakan diterapkan pada suatu permintaan, izin yang dihasilkan akan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Amazon Detective bekerja dengan IAM

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Detektif Amazon. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. Administrator Detektif harus memiliki kebijakan AWS Identity and Access Management (IAM) yang memberikan izin kepada pengguna dan peran IAM untuk melakukan operasi API tertentu pada sumber daya tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke kepala sekolah yang memerlukan izin tersebut.

Detective menggunakan kebijakan berbasis identitas IAM untuk memberikan izin untuk jenis pengguna dan tindakan berikut:

- Akun administrator — Akun administrator adalah pemilik grafik perilaku, yang menggunakan data dari akun mereka. Akun administrator dapat mengundang akun anggota untuk menyumbangkan data mereka ke grafik perilaku. Akun administrator juga dapat menggunakan grafik perilaku untuk triase dan investigasi temuan dan sumber daya yang terkait dengan akun tersebut.

Anda dapat menyiapkan kebijakan agar pengguna selain akun administrator dapat melakukan berbagai jenis tugas. Misalnya, pengguna dari akun administrator mungkin hanya memiliki izin untuk mengelola akun anggota. Pengguna lain mungkin hanya memiliki izin untuk menggunakan grafik perilaku untuk penyelidikan.

- Akun anggota — Akun anggota adalah akun yang diundang untuk menyumbangkan data ke grafik perilaku. Akun anggota menanggapi undangan. Setelah menerima undangan, akun anggota dapat menghapus akun mereka dari grafik perilaku.

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Detektif dan Layanan AWS lainnya dengan IAM, lihat Membuat kebijakan pada tab JSON di Panduan Pengguna IAM.

Kebijakan berbasis identitas Detektif

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta kondisi di mana tindakan diizinkan atau ditolak. Detective mendukung tindakan, sumber daya, dan kunci kondisi tertentu.

Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi Elemen Kebijakan JSON IAM dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan-tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Pernyataan kebijakan harus mencakup `Action` elemen atau `NotAction` elemen. `Action`Elemen mencantumkan tindakan yang diizinkan oleh kebijakan. `NotAction`Elemen mencantumkan tindakan yang tidak diizinkan.

Tindakan yang didefinisikan untuk Detective mencerminkan tugas yang dapat Anda lakukan menggunakan Detective. Tindakan kebijakan di Detektif memiliki awalan berikut:. `detective:`

Misalnya, untuk memberikan izin menggunakan operasi `CreateMembers` API guna mengundang akun anggota ke grafik perilaku, Anda menyertakan `detective:CreateMembers` tindakan tersebut dalam kebijakan mereka.

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut dengan koma. Misalnya, untuk akun anggota, kebijakan mencakup serangkaian tindakan yang terkait dengan pengelolaan undangan:

```
"Action": [
      "detective:ListInvitations",
      "detective:AcceptInvitation",
      "detective:RejectInvitation",
      "detective:DisassociateMembership
]
```

Anda juga dapat menggunakan wildcard (*) untuk menentukan beberapa tindakan. Misalnya, untuk mengelola data yang digunakan dalam grafik perilaku mereka, akun administrator di Detective harus dapat melakukan tugas-tugas berikut:

- Lihat daftar akun anggota mereka (`ListMembers`).
- Dapatkan informasi tentang akun anggota yang dipilih (`GetMembers`).
- Undang akun anggota ke grafik perilaku mereka (`CreateMembers`).
- Hapus anggota dari grafik perilaku mereka (`DeleteMembers`).

Alih-alih mencantumkan tindakan ini secara terpisah, Anda dapat memberikan akses ke semua tindakan yang diakhiri dengan kata tersebut`Members`. Kebijakan untuk itu dapat mencakup tindakan berikut:

```
"Action": "detective:*Members"
```

Untuk melihat daftar tindakan Detektif, lihat Tindakan yang ditentukan oleh Detektif Amazon di Referensi Otorisasi Layanan.

Sumber daya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan entah elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk informasi selengkapnya tentang format ARN, lihat Nama Sumber Daya Amazon (ARN) dan Ruang Nama AWS Layanan.

Untuk Detective, satu-satunya jenis sumber daya adalah grafik perilaku. Sumber daya grafik perilaku di Detective memiliki ARN berikut:

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

Misalnya, grafik perilaku memiliki nilai-nilai berikut:

- Wilayah untuk grafik perilaku adalah`us-east-1`.
- ID akun untuk ID akun administrator adalah`111122223333`.
- ID grafik dari grafik perilaku adalah`027c7c4610ea4aacaf0b883093cab899`.

Untuk mengidentifikasi grafik perilaku ini dalam sebuah `Resource` pernyataan, Anda akan menggunakan ARN berikut:

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

Untuk menentukan beberapa sumber daya dalam `Resource` pernyataan, gunakan koma untuk memisahkannya.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Misalnya, AWS akun yang sama dapat diundang untuk menjadi akun anggota di lebih dari satu grafik perilaku. Dalam kebijakan untuk akun anggota tersebut, `Resource` pernyataan tersebut akan mencantumkan grafik perilaku yang mereka undang.

```
"Resource": [
      "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

Beberapa tindakan Detektif, seperti membuat grafik perilaku, mencantumkan grafik perilaku, dan daftar undangan grafik perilaku, tidak dilakukan pada grafik perilaku tertentu. Untuk tindakan tersebut, `Resource` pernyataan harus menggunakan wildcard (*).

```
"Resource": "*"
```

Untuk tindakan akun administrator, Detektif selalu memverifikasi bahwa pengguna yang membuat permintaan milik akun administrator untuk grafik perilaku yang terpengaruh. Untuk tindakan akun anggota, Detektif selalu memverifikasi bahwa pengguna yang membuat permintaan milik akun anggota. Bahkan jika kebijakan IAM memberikan akses ke grafik perilaku, jika pengguna bukan milik akun yang benar, pengguna tidak dapat melakukan tindakan tersebut.

Untuk semua tindakan yang dilakukan pada grafik perilaku tertentu, kebijakan IAM harus menyertakan grafik ARN. Grafik ARN dapat ditambahkan nanti. Misalnya, ketika akun pertama kali mengaktifkan Detektif, kebijakan IAM awal menyediakan akses ke semua tindakan Detektif, menggunakan wildcard untuk grafik ARN. Hal ini memungkinkan pengguna untuk segera mulai mengelola akun anggota dan melakukan investigasi dalam grafik perilaku mereka. Setelah grafik perilaku dibuat, Anda dapat memperbarui kebijakan untuk menambahkan grafik ARN.

Kunci syarat

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, AWS akan mengevaluasinya dengan menggunakan operasi `AND` yang logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tanda dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Detective tidak mendefinisikan set sendiri dari kunci kondisi. Itu mendukung penggunaan kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat Kunci Konteks Kondisi AWS Global di Panduan Pengguna IAM.

Untuk mempelajari tindakan dan sumber daya yang memungkinkan Anda menggunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Detektif Amazon.

Contoh-contoh

Untuk melihat contoh kebijakan berbasis identitas Detektif, lihat. Contoh kebijakan berbasis identitas Detektif Amazon

Kebijakan berbasis sumber daya Detektif (Tidak didukung)

Detective tidak mendukung kebijakan berbasis sumber daya.

Otorisasi berdasarkan tag grafik perilaku Detektif

Setiap grafik perilaku dapat diberi nilai tag. Anda dapat menggunakan nilai tag tersebut dalam pernyataan kondisi untuk mengelola akses ke grafik perilaku.

Pernyataan kondisi untuk nilai tag menggunakan format berikut.

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

Misalnya, gunakan kode berikut untuk mengizinkan atau menolak tindakan ketika nilai `Department` tag tersebut`Finance`.

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

Untuk contoh kebijakan yang menggunakan nilai tag sumber daya, lihatthe section called “Akun administrator: Membatasi akses berdasarkan nilai tag”.

Peran Detektif IAM

Peran IAM adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensil sementara dengan Detective

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensil keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau. GetFederationToken

Detective mendukung menggunakan kredensil sementara.

Peran terkait layanan

Peran terkait AWS layanan memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan Detektif, lihat. the section called “Menggunakan peran terkait layanan”

Peran layanan (Tidak didukung)

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

Detektif tidak mendukung peran layanan.

Contoh kebijakan berbasis identitas Detektif Amazon

Secara default, pengguna dan peran IAM tidak memiliki izin untuk membuat atau memodifikasi sumber daya Detektif. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API.

Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat Kebijakan pada Tab JSON dalam Panduan Pengguna IAM.

Topik

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Detektif di akun Anda. Tindakan ini mengenakan biaya kepada Akun AWS Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan terkelola AWS atau kebijakan terkelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan pengguna IAM untuk mengajukan izin, lihat Kebijakan dan izin di IAM dalam Panduan Pengguna IAM.
- Menggunakan syarat dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu syarat ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat dalam Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang diproteksi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan konsol Detective

Untuk menggunakan konsol Detektif Amazon, pengguna atau peran harus memiliki akses ke tindakan yang relevan, yang cocok dengan tindakan terkait di API.

Untuk mengaktifkan Detektif dan menjadi akun administrator untuk grafik perilaku, pengguna atau peran harus diberikan izin untuk tindakan tersebut`CreateGraph`.

Untuk menggunakan konsol Detektif untuk melakukan tindakan akun administrator, pengguna atau peran harus diberikan izin untuk tindakan tersebut`ListGraphs`. Ini memberikan izin untuk mengambil grafik perilaku akun mereka sebagai akun administrator. Mereka juga harus diberikan izin untuk melakukan tindakan akun administrator tertentu.

Tindakan akun administrator yang paling dasar adalah melihat daftar akun anggota dalam grafik perilaku, dan menggunakan grafik perilaku untuk penyelidikan.

- Untuk melihat daftar akun anggota dalam grafik perilaku, kepala sekolah harus diberikan izin untuk `ListMembers` tindakan tersebut.
- Untuk melakukan investigasi dalam grafik perilaku, kepala sekolah harus diberikan izin untuk `SearchGraph` tindakan tersebut.

Untuk menggunakan konsol Detektif untuk melakukan tindakan akun anggota, pengguna atau peran harus diberikan izin untuk tindakan tersebut`ListInvitations`. Ini memberikan izin untuk melihat undangan grafik perilaku. Mereka kemudian dapat diberikan izin untuk tindakan akun anggota tertentu.

Memungkinkan pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Akun administrator: Mengelola akun anggota dalam grafik perilaku

Kebijakan contoh ini ditujukan untuk pengguna akun administrator yang hanya bertanggung jawab untuk mengelola akun anggota yang digunakan dalam grafik perilaku. Kebijakan ini juga memungkinkan pengguna untuk melihat informasi penggunaan dan menonaktifkan Detektif. Kebijakan tidak memberikan izin untuk menggunakan grafik perilaku untuk penyelidikan.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
  },
  {
```

```
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Akun administrator: Menggunakan grafik perilaku untuk penyelidikan

Kebijakan contoh ini ditujukan untuk pengguna akun administrator yang menggunakan grafik perilaku hanya untuk penyelidikan. Mereka tidak dapat melihat atau mengedit daftar akun anggota dalam grafik perilaku.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":["detective:SearchGraph"],
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
   },
   {
    "Effect":"Allow",
    "Action":["detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Akun anggota: Mengelola undangan grafik perilaku dan keanggotaan

Kebijakan contoh ini ditujukan untuk pengguna yang termasuk dalam akun anggota. Dalam contoh, akun anggota termasuk dalam dua grafik perilaku. Kebijakan memberikan izin untuk menanggapi undangan dan menghapus akun anggota dari grafik perilaku.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembership"],
   "Resource":[
```

```
       "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
       "arn:aws:detective:us-
east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
    "Effect":"Allow",
    "Action":["detective:ListInvitations"],
    "Resource":"*"
  }
 ]
}
```

Akun administrator: Membatasi akses berdasarkan nilai tag

Kebijakan berikut memungkinkan pengguna menggunakan grafik perilaku untuk penyelidikan jika `SecurityDomain` tag grafik perilaku cocok dengan `SecurityDomain` tag pengguna.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Allow",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals"{
                "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":["detective:ListGraphs"],
        "Resource":"*"
    } ]
}
```

Kebijakan berikut mencegah pengguna menggunakan grafik perilaku untuk penyelidikan jika nilai `SecurityDomain` tag untuk grafik perilaku adalah`Finance`.

```
{
```

```
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

AWS kebijakan terkelola untuk Amazon Detective

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AmazonDetectiveFullAccess

Anda dapat melampirkan kebijakan `AmazonDetectiveFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke semua tindakan Detektif Amazon. Anda dapat melampirkan kebijakan ini ke kepala sekolah sebelum mereka mengaktifkan Detektif untuk akun mereka. Itu juga harus dilampirkan pada peran yang digunakan untuk menjalankan skrip Detective Python untuk membuat dan mengelola grafik perilaku.

Prinsipal dengan izin ini dapat mengelola akun anggota, menambahkan tag ke grafik perilaku mereka, dan menggunakan Detektif untuk penyelidikan. Mereka juga dapat mengarsipkan GuardDuty temuan. Kebijakan ini memberikan izin yang dibutuhkan konsol Detektif untuk menampilkan nama akun untuk akun yang ada di dalamnya. AWS Organizations

Detail izin

Kebijakan ini mencakup izin berikut:

- `detective`— Memungkinkan kepala sekolah akses penuh ke semua tindakan Detektif.
- `organizations`— Memungkinkan kepala sekolah untuk mengambil dari AWS Organizations informasi tentang akun dalam suatu organisasi. Jika akun milik organisasi, izin ini memungkinkan konsol Detektif menampilkan nama akun selain nomor akun.
- `guardduty`— Memungkinkan kepala sekolah untuk mendapatkan dan mengarsipkan GuardDuty temuan dari dalam Detektif.
- `securityhub`— Memungkinkan kepala sekolah untuk mendapatkan temuan Security Hub dari dalam Detektif.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "detective:*",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ArchiveFindings"
            ],
            "Resource": "arn:aws:guardduty:*:*:detector/*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "guardduty:GetFindings",
                "guardduty:ListDetectors"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "securityHub:GetFindings"
            ],
            "Resource": "*"
         }
    ]
}
```

AWS kebijakan terkelola: AmazonDetectiveMemberAccess

Anda dapat melampirkan `AmazonDetectiveMemberAccess` kebijakan ke entitas IAM Anda.

Kebijakan ini memberikan akses anggota ke Detektif Amazon dan akses cakupan ke konsol.

Dengan kebijakan ini, Anda dapat:

- Lihat undangan ke keanggotaan grafik Detektif dan terima atau tolak undangan tersebut.
- Lihat bagaimana aktivitas Anda di Detective berkontribusi terhadap biaya penggunaan layanan ini di halaman Penggunaan.
- Mengundurkan diri dari keanggotaan Anda dalam grafik.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan akses cakupan ke Detektif konsol.

Detail izin

Kebijakan ini mencakup izin berikut:

- `detective`— Memungkinkan akses anggota ke Detektif.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan terkelola AWS : AmazonDetectiveInvestigatorAccess

Anda dapat melampirkan `AmazonDetectiveInvestigatorAccess` kebijakan ke entitas IAM Anda.

Kebijakan ini menyediakan akses penyidik ke layanan Detektif dan akses cakupan ke dependensi UI konsol Detektif. Kebijakan ini memberikan izin untuk mengaktifkan investigasi Detektif di Detektif untuk pengguna IAM dan peran IAM. Anda dapat menyelidiki untuk mengidentifikasi indikator kompromi seperti temuan menggunakan laporan investigasi, yang memberikan analisis dan wawasan tentang indikator keamanan. Laporan ini diberi peringkat berdasarkan tingkat keparahan, yang ditentukan menggunakan analisis perilaku Detektif dan pembelajaran mesin. Anda dapat menggunakan laporan untuk memprioritaskan remediasi sumber daya.

Detail izin

Kebijakan ini mencakup izin berikut:

- `detective`— Memungkinkan penyidik kepala sekolah mengakses tindakan Detektif, untuk mengaktifkan investigasi Detektif, dan untuk memungkinkan menemukan ringkasan kelompok.
- `guardduty`— Memungkinkan kepala sekolah untuk mendapatkan dan mengarsipkan GuardDuty temuan dari dalam Detektif.
- `securityhub`— Memungkinkan kepala sekolah untuk mendapatkan temuan Security Hub dari dalam Detektif.
- `organizations`— Memungkinkan kepala sekolah untuk mengambil informasi tentang akun dalam suatu organisasi dari. AWS Organizations Jika akun milik organisasi, maka izin ini memungkinkan konsol Detektif untuk menampilkan nama akun selain nomor akun.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPermissions",
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
        "securityHub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS kebijakan terkelola: AmazonDetectiveOrganizationsAccess

Anda dapat melampirkan `AmazonDetectiveOrganizationsAccess` kebijakan ke entitas IAM Anda.

Kebijakan ini memberikan izin untuk mengaktifkan dan mengelola Detektif Amazon dalam suatu organisasi. Anda dapat mengaktifkan Detektif di seluruh organisasi dan menentukan akun administrator yang didelegasikan untuk Detektif.

Detail izin

Kebijakan ini mencakup izin berikut:

- `detective`— Memungkinkan kepala sekolah mengakses tindakan Detektif.
- `iam`— Menentukan bahwa peran layanan terkait dibuat ketika `EnableOrganizationAdminAccount` Detective memanggil.
- `organizations`— Memungkinkan kepala sekolah untuk mengambil informasi tentang akun dalam suatu organisasi dari. AWS Organizations Jika akun milik organisasi, maka izin ini memungkinkan konsol Detektif untuk menampilkan nama akun selain nomor akun. Mengaktifkan integrasi AWS layanan, memungkinkan register dan deregister akun anggota yang ditentukan sebagai administrator Delegasi, dan memungkinkan prinsipal untuk mengambil akun administrator Delegasi di layanan keamanan lain seperti Amazon Detective, Amazon, Amazon Macie, dan. GuardDuty AWS Security Hub

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Kebijakan terkelola AWS : AmazonDetectiveServiceLinkedRole

Anda tidak dapat melampirkan kebijakan `AmazonDetectiveServiceLinkedRole` ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Detektif melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat the section called “Menggunakan peran terkait layanan”.

Kebijakan ini memberikan izin administratif yang memungkinkan peran terkait layanan untuk mengambil informasi akun untuk organisasi.

Detail izin

Kebijakan ini mencakup izin berikut:

- `organizations`— Mengambil informasi akun untuk suatu organisasi.

```
{
  "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "organizations:DescribeAccount",
              "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

Detective update untuk AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Detektif sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat dokumen.

Perubahan	Deskripsi	Tanggal
AmazonDetectiveInvestigatorAccess— Pembaruan kebijakan yang ada	Menambahkan investigasi Detektif dan menemukan tindakan ringkasan kelompok ke kebijakan. `AmazonDetectiveInvestigatorAccess` Tindakan ini memungkinkan memulai, mengambil, dan memperbarui investigasi Detektif; dan mendapatkan ringkasan menemukan kelompok dari dalam Detektif.	26 November 2023
AmazonDetectiveFullAccessdan AmazonDetectiveInvestigatorAccess— Pembaruan kebijakan yang ada	Detective menambahkan `GetFindings` tindakan Security Hub ke `AmazonDetectiveFullAccess` dan `AmazonDetectiveInvestigatorAccess` kebijakan. Tindakan ini memungkinkan mendapatkan temuan Security Hub dari dalam Detektif.	16 Mei 2023
AmazonDetectiveOrganizationsAccess – Kebijakan baru	Detektif menambahkan `AmazonDetectiveOrganizationsAccess` kebijakan. Kebijakan ini memberikan izin untuk mengaktifkan dan mengelola Detektif dalam suatu organisasi	Maret 02, 2023
AmazonDetectiveMemberAccess – Kebijakan baru	Detektif menambahkan kebijakan . `AmazonDetectiveMemberAccess`	Januari 17, 2023

Perubahan	Deskripsi	Tanggal
	Kebijakan ini memberikan akses anggota ke Detektif dan akses cakupan ke dependensi UI konsol.	
AmazonDetectiveFullAccess— Pembaruan untuk kebijakan yang ada	Detektif menambahkan GuardDuty `GetFindings` tindakan ke kebijakan. `AmazonDetectiveFullAccess` Tindakan ini memungkinkan mendapatkan GuardDuty temuan dari dalam Detektif.	Januari 17, 2023
AmazonDetectiveInvestigatorAccess – Kebijakan baru	Detektif menambahkan kebijakan . `AmazonDetectiveInvestigatorAccess` Kebijakan ini memungkinkan kepala sekolah untuk melakukan investigasi di Detektif.	Januari 17, 2023
AmazonDetectiveServiceLinkedRole – Kebijakan baru	Detective menambahkan kebijakan baru untuk peran terkait layanannya. Kebijakan ini memungkinkan peran terkait layanan untuk mengambil informasi tentang akun dalam organisasi.	Desember 16, 2021
Detektif mulai melacak perubahan	Detective mulai melacak perubahan untuk kebijakan yang AWS dikelola.	10 Mei 2021

Menggunakan peran terkait layanan untuk Detektif

Amazon Detective menggunakan peran terkait layanan AWS Identity and Access Management (IAM). Peran terkait layanan adalah jenis unik peran IAM yang terkait langsung dengan Detektif. Peran terkait layanan telah ditentukan sebelumnya oleh Detektif dan mencakup semua izin yang diperlukan layanan untuk memanggil layanan lain atas nama Anda. AWS

Peran terkait layanan membuat pengaturan Detektif lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Detective mendefinisikan izin dari peran terkait layanan, dan kecuali ditentukan lain, hanya Detective yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Detektif Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang support peran yang terkait dengan layanan, lihat Layanan AWS yang Bekerja dengan IAM dan mencari layanan yang memiliki Ya dalam kolom Peran Tertaut Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Detektif

Detektif menggunakan peran terkait layanan bernama — AWSServiceRoleForDetectiveMemungkinkan Detektif mengakses informasi atas nama Anda. AWS Organizations

Peran AWSServiceRoleForDetective terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `detective.amazonaws.com`

AWSServiceRoleForDetective Peran terkait layanan menggunakan kebijakan terkelola. `AmazonDetectiveServiceLinkedRolePolicy`

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Detektif

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda menetapkan akun administrator Detektif untuk organisasi di AWS Management Console, API, atau API, AWS CLI Detektif AWS akan membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda menunjuk akun administrator Detektif untuk suatu organisasi, Detektif membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Detektif

Detektif tidak mengizinkan Anda mengedit peran terkait AWSServiceRoleForDetective layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Detektif

Jika tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran tertaut layanan, sebaiknya Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Detektif menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika itu terjadi, tunggu beberapa menit dan kemudian coba operasi lagi.

Untuk menghapus sumber daya Detektif yang digunakan oleh AWSServiceRoleForDetective

1. Hapus akun administrator Detektif. Lihat the section called “Menunjuk akun administrator Detektif”.
2. Ulangi proses di setiap Wilayah tempat Anda menunjuk akun administrator Detektif.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForDetective terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk peran terkait layanan Detektif

Detective mendukung penggunaan peran terkait layanan di semua Wilayah di mana layanan tersedia. Untuk informasi lebih lanjut, lihat Wilayah dan Titik Akhir AWS.

Memecahkan masalah identitas dan akses Detektif Amazon

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Detective dan IAM. Jika Anda mengalami masalah akses yang ditolak atau kesulitan serupa saat bekerja dengan AWS Identity and Access Management(IAM), lihat topik Pemecahan Masalah IAM di Panduan Pengguna IAM.

Saya tidak berwenang untuk melakukan tindakan di Detective

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator adalah orang yang memberikan nama pengguna dan kata sandi kepada Anda.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan konsol untuk menerima undangan untuk menjadi akun anggota untuk grafik perilaku, tetapi tidak memiliki `detective:AcceptInvitation` izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakan miliknya agar dia dapat mengakses sumber daya `arn:aws:detective:us-east-1:444455556666:graph:567856785678` dengan menggunakan tindakan `detective:AcceptInvitation`.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Detektif.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Detective. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang-orang di luar AWS akun saya untuk mengakses sumber daya Detektif saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah Detective mendukung fitur-fitur ini, lihat. Bagaimana Amazon Detective bekerja dengan IAM
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) dalam Panduan Pengguna IAM.

- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Pencatatan dan pemantauan di Amazon Detective

Amazon Detective terintegrasi. AWS CloudTrail CloudTrail menangkap semua panggilan API untuk Detective sebagai event.

Untuk detail tentang penggunaan CloudTrail logging untuk Detective, lihat. the section called "Mencatat panggilan Detective API dengan CloudTrail"

Validasi kepatuhan untuk Amazon Detective

Amazon Detective berada dalam Lingkup program AWS jaminan. Untuk informasi lebih lanjut, lihat Health Information Trust Alliance Common Security Framework (HITRUST) CSF Health Information Trust) CSF.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWS Services in Scope by Compliance Program . Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Pengunduhan Laporan dalam AWS Artifact.

AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah–langkah untuk melakukan deployment terhadap lingkungan dasar di AWS yang menjadi fokus keamanan dan kepatuhan.
- Mengevaluasi sumber daya dengan aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di Detektif Amazon

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Detective memanfaatkan ketahanan yang dibangun ke dalam Amazon DynamoDB dan Amazon Simple Storage Service (Amazon S3).

Arsitektur Detective juga tahan terhadap kegagalan Availability Zone tunggal. Ketahanan ini dibangun ke dalam Detektif, dan tidak memerlukan konfigurasi apa pun.

Keamanan infrastruktur di Amazon Detective

Sebagai layanan terkelola, Amazon Detective; dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Detective; melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda bisa menggunakan AWS Security

Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Praktik terbaik keamanan untuk Detektif Amazon

Detective menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

Untuk Detektif, praktik terbaik keamanan dikaitkan dengan mengelola akun dalam grafik perilaku.

Praktik terbaik untuk akun administrator

Saat mengundang akun anggota ke grafik perilaku Anda, hanya undang akun yang Anda awasi.

Batasi akses ke grafik perilaku. Ketika pengguna memiliki akses ke grafik perilaku, mereka dapat melihat semua temuan untuk akun anggota. Temuan semacam itu mungkin mengekspos informasi keamanan yang sensitif.

Praktik terbaik untuk akun anggota

Saat Anda menerima undangan ke grafik perilaku, pastikan untuk memvalidasi sumber undangan.

Periksa pengenal AWS akun akun administrator yang mengirim undangan. Verifikasi bahwa Anda tahu milik siapa akun tersebut, dan bahwa akun yang mengundang memiliki alasan yang sah untuk memantau data keamanan Anda.

Peramalan dan pemantauan biaya Detektif Amazon

Untuk membantu Anda melacak aktivitas Detektif Anda, halaman Penggunaan menunjukkan jumlah data yang tertelan dan biaya yang diproyeksikan.

- Untuk akun administrator, halaman Penggunaan menunjukkan volume data dan biaya yang diproyeksikan di seluruh grafik perilaku.
- Untuk akun anggota, halaman Penggunaan menunjukkan volume data dan biaya yang diproyeksikan untuk akun mereka di seluruh grafik perilaku yang mereka sumbangkan.

Detective juga mendukung AWS CloudTrail logging.

Konten

Tentang uji coba gratis untuk grafik perilaku

Amazon Detective menyediakan uji coba gratis 30 hari untuk setiap akun di setiap Wilayah. Uji coba gratis untuk akun dimulai saat pertama kali salah satu tindakan berikut terjadi.

- Akun memungkinkan Detektif secara manual dan menjadi akun administrator untuk grafik perilaku.
- Akun ditetapkan sebagai akun administrator Detektif untuk organisasi di AWS Organizations, dan Detektif diaktifkan untuk pertama kalinya.
- Jika akun administrator Detektif sudah mengaktifkan Detektif sebelum mereka ditunjuk, maka akun tersebut tidak memulai uji coba gratis 30 hari yang baru.
- Akun menerima undangan untuk menjadi akun anggota dalam grafik perilaku dan diaktifkan sebagai akun anggota.
- Akun organisasi diaktifkan sebagai akun anggota oleh akun administrator Detektif.

Uji coba gratis berlangsung selama 30 hari sejak saat itu. Akun tidak ditagih untuk data apa pun yang diproses selama periode tersebut. Ketika masa percobaan berakhir, Detektif mulai menagih akun untuk data yang dikontribusikannya pada grafik perilaku. Untuk informasi selengkapnya tentang cara melacak aktivitas Detektif, pantau penggunaan, dan lihat biaya yang diproyeksikan, lihat. Peramalan dan pemantauan biaya Detektif Amazon Untuk informasi lebih lanjut tentang harga, lihat Harga Detektif

Periode 30 hari yang sama digunakan untuk semua grafik perilaku di Wilayah. Misalnya, akun diaktifkan sebagai akun anggota untuk grafik perilaku. Ini memulai uji coba gratis 30 hari. Setelah 10 hari, akun diaktifkan untuk grafik perilaku kedua di Wilayah yang sama. Untuk grafik perilaku kedua, akun menerima 20 hari data gratis.

Uji coba gratis memberikan banyak manfaat:

- Akun administrator dapat menjelajahi fitur dan fungsionalitas Detektif untuk memverifikasi nilainya.
- Akun administrator dan anggota dapat memantau jumlah data dan perkiraan biaya sebelum Detective mulai menagih mereka untuk itu. Lihat the section called “Penggunaan dan biaya akun administrator” dan the section called “Pelacakan penggunaan akun anggota”.

Uji coba gratis untuk sumber data opsional

Detective juga menyediakan uji coba 30 hari gratis untuk sumber data opsional. Uji coba gratis ini terpisah dari uji coba gratis yang disediakan untuk sumber data Detektif inti saat Detektif pertama kali diaktifkan.

> **Note**
>
> Jika pelanggan menonaktifkan paket sumber data opsional dalam waktu 7 hari setelah mengaktifkannya, Detective melakukan reset otomatis satu kali uji coba gratis untuk paket sumber data tersebut jika diaktifkan lagi.

Untuk mengaktifkan atau menonaktifkan sumber data opsional, lihatJenis sumber data opsional di Detective.

Memantau penggunaan dan biaya untuk grafik perilaku (akun administrator)

Amazon Detective menagih setiap akun untuk data yang digunakan dalam setiap grafik perilaku yang dimiliki akun tersebut. Detective mengenakan tarif flat berjenjang per GB untuk semua data terlepas dari sumbernya.

Untuk akun administrator, halaman Penggunaan konsol Detektif memungkinkan Anda untuk melihat volume data yang dicerna oleh sumber data atau Berdasarkan akun selama 30 hari sebelumnya. Akun administrator juga melihat biaya yang diproyeksikan untuk periode 30 hari tipikal untuk akun mereka dan untuk seluruh grafik perilaku.

Untuk melihat informasi penggunaan Detektif

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, di bawah Pengaturan, pilih Penggunaan.
3. Pilih tab untuk memilih antara penggunaan tampilan Berdasarkan sumber data atau Berdasarkan akun.

Volume data yang dicerna untuk setiap akun

Volume yang dicerna oleh akun anggota mencantumkan akun aktif dalam grafik perilaku. Itu tidak mencantumkan akun anggota yang telah dihapus.

Untuk setiap akun, daftar volume yang dicerna memberikan informasi berikut.

- Pengenal AWS akun dan alamat email pengguna root.
- Tanggal ketika akun mulai menyumbangkan data ke grafik perilaku.

  Untuk akun administrator, ini adalah tanggal ketika akun diaktifkan Detektif.

  Untuk akun anggota, ini adalah tanggal ketika akun diaktifkan sebagai akun anggota setelah menerima undangan.
- Volume data yang tertelan dari akun selama 30 hari sebelumnya. Total mencakup semua jenis sumber.

- Apakah akun saat ini dalam masa uji coba gratis. Untuk akun yang saat ini dalam masa uji coba gratis, daftar menampilkan jumlah hari yang tersisa.

  Jika tidak ada akun yang berada dalam periode uji coba gratis, maka kolom status uji coba gratis tidak ditampilkan.

Biaya yang diproyeksikan untuk grafik perilaku

Biaya yang diproyeksikan akun ini menunjukkan biaya yang diproyeksikan selama 30 hari data untuk akun administrator. Biaya yang diproyeksikan didasarkan pada volume rata-rata harian untuk akun administrator.

> **Important**
>
> Jumlah ini hanya biaya yang diproyeksikan. Ini memproyeksikan total biaya untuk data akun administrator untuk periode waktu 30 hari yang khas. Ini didasarkan pada penggunaan dari 30 hari sebelumnya. Lihat the section called “Bagaimana Detective menghitung biaya yang diproyeksikan”.

Biaya yang diproyeksikan untuk grafik perilaku

Biaya proyeksi semua akun menunjukkan total biaya yang diproyeksikan selama 30 hari data untuk seluruh grafik perilaku. Biaya yang diproyeksikan didasarkan pada volume rata-rata harian untuk setiap akun.

> **Important**
>
> Jumlah ini hanya biaya yang diproyeksikan. Ini memproyeksikan total biaya untuk data grafik perilaku untuk periode waktu 30 hari yang khas. Ini didasarkan pada penggunaan dari 30 hari sebelumnya. Biaya yang diproyeksikan tidak termasuk akun anggota yang dihapus dari grafik perilaku. Lihat the section called “Bagaimana Detective menghitung biaya yang diproyeksikan”.

Volume data yang dicerna oleh paket sumber

Pilih Berdasarkan paket sumber untuk melihat volume data yang dicerna terdaftar oleh paket sumber berbeda yang diaktifkan dalam grafik perilaku Anda.

Semua akun dapat melihat data ini untuk akun mereka sendiri. Akun administrator dapat melihat panel tambahan yang mencantumkan penggunaan berdasarkan paket sumber untuk setiap anggota. Itu tidak mencantumkan akun anggota yang telah dihapus.

Inti detektif

Panel inti Detektif menunjukkan volume data yang dicerna dari sumber inti Detektif (logCloudTrail , log Aliran VPC, dan GuardDuty temuan) selama 30 hari terakhir.

Log audit EKS

Panel log audit EKS menunjukkan volume data yang dicerna dari sumber log audit EKS selama 30 hari terakhir. Panel untuk paket sumber ini hanya tersedia jika log audit EKS diaktifkan untuk grafik perilaku Anda.

Memantau penggunaan dan biaya di seluruh grafik perilaku (akun anggota)

Amazon Detective menagih setiap akun untuk data yang digunakan dalam setiap grafik perilaku yang dimiliki akun tersebut. Detective mengenakan tarif flat berjenjang per GB untuk semua data terlepas dari sumbernya.

Untuk akun anggota, halaman Penggunaan menunjukkan volume data dan proyeksi biaya 30 hari untuk akun tersebut saja.

Untuk melihat informasi penggunaan Detektif

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, di bawah Pengaturan, pilih Penggunaan.

Volume tertelan untuk setiap grafik perilaku

Volume tertelan akun ini mencantumkan grafik perilaku yang dikontribusikan oleh akun anggota. Ini tidak termasuk keanggotaan yang Anda pasrahkan, atau keanggotaan yang dihapus oleh akun administrator.

Untuk setiap grafik perilaku, daftar menyertakan informasi berikut.

- Nomor akun akun administrator
- Volume data yang tertelan dari akun anggota selama 30 hari sebelumnya. Total mencakup semua jenis sumber.
- Tanggal ketika akun anggota diaktifkan untuk grafik perilaku.

Biaya yang diproyeksikan di seluruh grafik perilaku

Biaya yang diproyeksikan akun ini menunjukkan biaya yang diproyeksikan selama 30 hari data untuk akun anggota di semua grafik perilaku yang dikontribusikannya. Biaya yang diproyeksikan didasarkan pada volume rata-rata harian untuk akun anggota.

> **Important**
>
> Jumlah ini hanya biaya yang diproyeksikan. Ini memproyeksikan total biaya untuk data akun administrator untuk periode waktu 30 hari yang khas. Ini didasarkan pada penggunaan dari 30 hari sebelumnya. Lihat the section called “Bagaimana Detective menghitung biaya yang diproyeksikan”.

Bagaimana Amazon Detective menghitung biaya yang diproyeksikan

Untuk menghitung nilai biaya yang diproyeksikan yang ditampilkan pada halaman Penggunaan, Detective melakukan hal berikut.

1. Untuk mendapatkan biaya yang diproyeksikan untuk akun individu dalam grafik perilaku, Detective melakukan hal berikut.
   a. Menghitung volume rata-rata per hari. Ini menambahkan volume data di semua hari aktif dan kemudian membaginya dengan jumlah hari akun telah aktif.

Jika akun diaktifkan lebih dari 30 hari yang lalu, maka jumlah hari adalah 30. Jika akun diaktifkan kurang dari 30 hari yang lalu, maka itu adalah jumlah hari sejak tanggal penerimaan.

Misalnya, jika akun diaktifkan 12 hari yang lalu, maka Detective menambahkan volume yang dicerna selama 12 hari itu dan kemudian membaginya dengan 12.

b. Mengalikan rata-rata harian akun dengan 30. Ini adalah proyeksi penggunaan 30 hari untuk akun.

c. Menggunakan model harga untuk menghitung biaya 30 hari yang diproyeksikan untuk penggunaan 30 hari yang diproyeksikan.

2. Untuk mendapatkan total biaya yang diproyeksikan untuk grafik perilaku, Detective melakukan hal berikut:

   a. Menggabungkan proyeksi penggunaan 30 hari dari semua akun dalam grafik perilaku.

   b. Menggunakan model harga untuk menghitung biaya 30 hari yang diproyeksikan untuk total proyeksi penggunaan 30 hari.

3. Untuk mendapatkan total biaya yang diproyeksikan untuk akun anggota di seluruh grafik perilaku, Detective melakukan hal berikut:

   a. Menggabungkan proyeksi penggunaan 30 hari di semua grafik perilaku.

   b. Menggunakan model harga untuk menghitung proyeksi biaya 30 hari untuk total proyeksi penggunaan 30 hari.

4. Jika Anda menggunakan VPC Amazon bersama, Detektif menghitung biaya yang diproyeksikan berdasarkan aktivitas pemantauan. Kami menyarankan Anda meninjau biaya yang diproyeksikan untuk investigasi khusus untuk lingkungan Anda.

   a. Jika akun anggota Detektif memiliki VPC Amazon bersama dan ada akun Non-Detektif lainnya yang menggunakan VPC bersama, Detektif akan memantau semua lalu lintas dari VPC tersebut. Penggunaan dan biaya akan meningkat dan Detective akan memberikan visualisasi pada semua arus lalu lintas dalam VPC.

   b. Jika Anda memiliki instans EC2 di dalam VPC Amazon bersama dan pemilik bersama bukan anggota Detektif, Detektif tidak akan memantau lalu lintas apa pun dari VPC, dan penggunaan serta biaya akan berkurang. Jika Anda ingin melihat arus lalu lintas dalam VPC, Anda harus menambahkan pemilik Amazon VPC sebagai anggota grafik Detektif Anda.

Mencatat panggilan Amazon Detective API dengan AWS CloudTrail

Detective terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Detective. CloudTrail menangkap semua panggilan API untuk Detective sebagai event. Panggilan yang diambil termasuk panggilan dari konsol Detektif dan panggilan kode ke operasi Detective API.

- Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Detektif.
- Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara.

Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan yang berikut:

- Permintaan yang dibuat untuk Detektif
- Alamat IP dari mana permintaan itu dibuat
- Siapa yang membuat permintaan
- Ketika itu dibuat
- Detail tambahan tentang permintaan

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi Detektif di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Detektif, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa, bersama dengan peristiwa AWS layanan lainnya, dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS . Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Detektif, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3.

Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS . Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda juga dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log.

Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

CloudTrail mencatat semua operasi Detective, yang didokumentasikan dalam Referensi API Detective.

Misalnya, panggilan ke`CreateMembers`,`AcceptInvitation`, dan `DeleteMembers` operasi menghasilkan entri dalam file CloudTrail log.

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut:

- Apakah permintaan dibuat dengan root atau AWS Identity and Access Management (IAM) kredensional pengguna
- Apakah permintaan dibuat dengan kredensi keamanan sementara untuk peran atau pengguna federasi
- Apakah permintaan itu dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat Elemen CloudTrail UserIdentity.

Memahami entri file log Detektif

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log.

Peristiwa menunjukkan satu permintaan dari sumber mana pun. Acara mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga entri tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `AcceptInvitation` tindakan.

```
      {
            "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
            "Username": "JaneRoe",
            "EventTime": 1571956406.0,
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS:JaneRoe\",\"arn
\":\"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\",\"accountId
\":\"111122223333\",\"accessKeyId\":\"AKIAIOSFODNN7EXAMPLE\",\"sessionContext\":
{\"attributes\":{\"mfaAuthenticated\":\"false\",\"creationDate\":\"2019-10-24T21:54:56Z
\"},\"sessionIssuer\":{\"type\":\"Role\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS
\",\"arn\":\"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\",\"accountId\":
\"111122223333\",\"userName\":\"JaneRoe\"}}},\"eventTime\":\"2019-10-24T22:33:26Z
\",\"eventSource\":\"detective.amazonaws.com\",\"eventName\":\"AcceptInvitation
\",\"awsRegion\":\"us-east-2\",\"sourceIPAddress\":\"192.0.2.123\",\"userAgent
\":\"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-
Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/
AWS_Lambda_java8\",\"errorCode\":\"ValidationException\",\"requestParameters\":
{\"masterAccount\":\"111111111111\"},\"responseElements\":{\"message\":\"Invalid
 request body\"},\"requestID\":\"8437ff99-5ec4-4b1a-8353-173be984301f\",\"eventID\":
\"f2545ee3-170f-4340-8af4-a983c669ce37\",\"readOnly\":false,\"eventType\":\"AwsApiCall
\",\"recipientAccountId\":\"111122223333\"}",
            "EventName": "AcceptInvitation",
            "EventSource": "detective.amazonaws.com",
            "Resources": []
        },
```

Wilayah Detektif Amazon dan kuota

Saat menggunakan Amazon Detective, perhatikan kuota ini.

Daerah Detektif dan titik akhir

Untuk melihat daftar Wilayah AWS tempat Detektif tersedia, lihat Titik akhir layanan Detektif.

Kuota Detektif

Detektif memiliki kuota berikut, yang tidak dapat dikonfigurasi.

Sumber daya	Kuota	Komentar
Jumlah akun anggota	1.200	Jumlah akun anggota yang dapat ditambahkan oleh akun administrator ke grafik perilaku.
Volume data grafik perilaku - peringatan volume	9 TB per hari	Jika volume data grafik perilaku lebih besar dari 9 TB per hari, maka Detective menampilkan peringatan bahwa grafik perilaku mendekati volume maksimum yang diizinkan.
Volume data grafik perilaku - tidak ada akun baru	10 TB per hari	Jika volume data grafik perilaku lebih besar dari 10 TB per hari, maka Anda tidak dapat menambahkan akun anggota baru ke grafik perilaku.
Volume data grafik perilaku — hentikan konsumsi data ke dalam grafik perilaku	15 TB per hari	Jika volume data grafik perilaku lebih besar dari 15 TB per hari, maka Detective berhenti menelan data ke dalam grafik perilaku. 15 TB per hari mencerminkan volume data normal dan lonjakan volume data.

Sumber daya	Kuota	Komentar
		Untuk mengaktifkan kembali pengambil an data, Anda harus menghubungi. AWS Support

Internet Explorer 11 tidak didukung

Anda tidak dapat menggunakan Detective dengan Internet Explorer 11.

Mengelola tag untuk grafik perilaku

Anda dapat menetapkan tag ke grafik perilaku Anda. Anda kemudian dapat menggunakan nilai tag dalam kebijakan IAM untuk mengelola akses ke fungsi grafik perilaku di Detective. Lihat the section called “Otorisasi berdasarkan tag grafik perilaku Detektif”.

Anda juga dapat menggunakan tag sebagai alat untuk pelaporan biaya. Misalnya, untuk melacak biaya yang terkait dengan keamanan, Anda dapat menetapkan tag yang sama ke grafik perilaku Detektif, sumber daya hub AWS Security Hub , dan detektor Amazon GuardDuty . Di AWS Cost Explorer, Anda kemudian dapat mencari tag itu untuk melihat tampilan konsolidasi biaya di seluruh sumber daya tersebut.

Melihat tag untuk grafik perilaku (Konsol)

Anda mengelola tag untuk grafik perilaku Anda dari halaman Umum.

Untuk melihat daftar tag yang ditetapkan ke grafik perilaku

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi, pada Pengaturan, pilih Umum.

Membuat daftar tag untuk grafik perilaku (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS Command Line Interface untuk mendapatkan daftar tag untuk grafik perilaku Anda.

Untuk mendapatkan daftar tag untuk grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `ListTagsForResource` Anda harus memberikan ARN dari grafik perilaku Anda.
- AWS CLI: Pada baris perintah, jalankan `list-tags-for-resource` perintah.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

Contoh

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Menambahkan tag ke grafik perilaku (Konsol)

Dari daftar tag di halaman Umum, Anda dapat menambahkan nilai tag ke grafik perilaku.

Untuk menambahkan tag ke grafik perilaku Anda

1. Pilih Tambahkan tag baru.
2. Untuk Kunci, masukkan nama tag.
3. Untuk Nilai, masukkan nilai tag.

Menambahkan tag ke grafik perilaku (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS CLI untuk menambahkan nilai tag ke grafik perilaku Anda.

Untuk menambahkan tag ke grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `TagResource` Anda memberikan grafik perilaku ARN dan nilai tag untuk ditambahkan.
- AWS CLI: Pada baris perintah, jalankan `tag-resource` perintah.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior
 graph ARN> --tags '{"TagName":"TagValue"}'
```

Contoh

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

Menghapus tag dari grafik perilaku (Konsol)

Untuk menghapus tag dari daftar di halaman Umum, pilih opsi Hapus untuk tag itu.

Menghapus tag dari grafik perilaku (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS CLI untuk menghapus nilai tag dari grafik perilaku Anda.

Untuk menghapus tag dari grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `UntagResource` Anda memberikan grafik perilaku ARN, dan nama tag yang akan dihapus.
- AWS CLI: Pada baris perintah, jalankan `untag-resource` perintah.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys "TagName"
```

Contoh

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Menonaktifkan Detektif Amazon

Akun administrator untuk grafik perilaku dapat menonaktifkan Amazon Detective dari konsol Detective, Detective API, atau. AWS Command Line Interface Saat Anda menonaktifkan Detektif, grafik perilaku dan data Detektif terkait akan dihapus.

Setelah grafik perilaku dihapus, grafik tersebut tidak dapat dipulihkan.

Daftar Isi

Menonaktifkan Detektif (Konsol)

Anda dapat menonaktifkan Amazon Detective dari file. AWS Management Console

Untuk menonaktifkan Amazon Detective (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, di bawah Pengaturan, pilih Umum.
3. Pada halaman Umum, di bawah Nonaktifkan Detektif Amazon, pilih Nonaktifkan Detektif Amazon.
4. Saat diminta untuk mengonfirmasi, ketik**`disable`**.
5. Pilih Nonaktifkan Detektif Amazon.

Menonaktifkan Detektif (Detective API,) AWS CLI

Anda dapat menonaktifkan Amazon Detective dari Detective API atau file. AWS Command Line Interface Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk menonaktifkan Detective (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `DeleteGraph` Anda harus memberikan grafik ARN.

- AWS CLI: Pada baris perintah, jalankan `delete-graph`perintah.

```
aws detective delete-graph --graph-arn <graph ARN>
```

Contoh:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Menonaktifkan Detektif di Seluruh Wilayah (skrip Python aktif) GitHub

Detective menyediakan skrip sumber terbuka GitHub yang memungkinkan Anda menonaktifkan Detektif untuk akun administrator di seluruh daftar Wilayah tertentu.

Untuk informasi tentang cara mengkonfigurasi dan menggunakan GitHub skrip, lihatthe section called "Skrip Python Detektif Amazon".

Riwayat dokumen untuk Panduan Pengguna Detektif

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir Detective. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

- Pembaruan dokumentasi terbaru: 15 April 2024

Perubahan	Deskripsi	Tanggal
Pembaruan dokumentasi	Konten dari Panduan Administrasi Detektif Amazon sekarang dikonsolidasikan ke dalam Panduan Pengguna Detektif Amazon. Panduan Administrasi Detektif Amazon akan mencapai akhir dukungan standar pada 08 Mei 2024.	April 15, 2024
Menambahkan dukungan untuk GuardDuty temuan Amazon	Detective sekarang menyediakan dukungan untuk jenis pencarian GuardDuty Runtime Monitoring berikut. `Execution:Runtime/MaliciousFileExecuted` `Execution:Runtime/SuspiciousTool` `DefenseEvasion:Runtime/PtraceAntiDebugging` `Execution:Runtime/SuspiciousCommand` `DefenseEvasion:Runtime/SuspiciousCommand`	April 5, 2024

Menghapus persyaratan GuardDuty keanggotaan Amazon	Anda tidak lagi diharuskan menjadi GuardDuty pelanggan untuk mengaktifkan Amazon Detective. Persyaratan untuk GuardDuty mengaktifkan akun Anda selama 48 jam sebelum mengaktifkan Detektif telah dihapus.	Februari 2, 2024
Menambahkan dukungan untuk GuardDuty temuan Amazon	Detective memperlua s dukungan untuk jenis pencarian GuardDuty EC2 Runtime Monitoring ke sumber daya ECS dan EC2.	Januari 30, 2024
Fungsionalitas yang diperbarui	Anda sekarang dapat menjalankan investigasi Detektif dari halaman Investiga si untuk sumber daya tertentu yang ingin Anda selidiki. Detective merekomendasikan sumber daya berdasark an aktivitasnya dalam temuan dan menemukan kelompok. Investigasi Detektif memungkinkan Anda menyelidiki pengguna IAM dan peran IAM dengan indikator kompromi, yang dapat membantu Anda menentukan apakah sumber daya terlibat dalam insiden keamanan.	Januari 16, 2024

Fungsionalitas yang diperbarui	Anda sekarang dapat menjalankan investiga si Detektif dari halaman Investigasi pada sumber yang direkomendasikan. Detective merekomendasikan sumber daya berdasark an aktivitasnya dalam temuan dan menemukan kelompok. Investigasi Detektif memungkinkan Anda menyelidiki pengguna IAM dan peran IAM dengan indikator kompromi, yang dapat membantu Anda menentukan apakah sumber daya terlibat dalam insiden keamanan.	Desember 26, 2023
Perubahan cara Detektif membaca lalu lintas arus untuk VPC bersama	Jika Anda menggunakan VPC Amazon bersama, Anda mungkin melihat perubahan lalu lintas yang dipantau oleh Detektif. Kami menyarankan Anda meninjau perubahan dalam detail Aktivitas untuk volume aliran VPC secara keseluruhan guna memahami dampak potensial pada cakupan Anda, dan meninjau cara Detektif menghitung biaya yang diproyeksikan untuk memahami bagaimana hal itu dapat memengaruhi biaya layanan Anda.	Desember 20, 2023

Ketersediaan regional	Menambahkan Wilayah Eropa (Stockholm), Eropa (Paris), dan Kanada (Tengah) ke dalam daftar AWS Wilayah di mana integrasi Detektif dengan Security Lake tersedia.	8 Desember 2023
Fitur baru	Investigasi Detektif memungkinkan Anda menyelidiki pengguna IAM dan peran IAM dengan indikator kompromi, yang dapat membantu Anda menentukan apakah sumber daya terlibat dalam insiden keamanan.	26 November 2023
Fitur baru	Secara default, Detective secara otomatis menghasilkan ringkasan grup pencarian untuk menemukan grup, didukung oleh kecerdasan buatan generatif (AI generatif). Menemukan ringkasan kelompok, dengan cepat menganalisis hubungan antara temuan dan sumber daya yang terpengaruh, dan kemudian merangkum potensi ancaman dalam bahasa alami.	26 November 2023

Fitur baru	Integrasi Detektif dengan Security Lake memungkinkan Anda dapat melakukan kueri dan mengambil data log mentah yang disimpan oleh Security Lake. Dengan integrasi ini, Anda dapat mengumpulkan log dan peristiwa dari peristiwa CloudTrail manajemen dan Log Aliran Amazon Virtual Private Cloud (Amazon VPC).	26 November 2023
Menambahkan informasi kebijakan terkelola ke bagian keamanan	Menambahkan investigasi Detektif dan menemukan tindakan ringkasan kelompok ke kebijakan. `AmazonDetectiveInvestigatorAccess`	26 November 2023
Melihat ikhtisar temuan	Jika temuan berkorelasi dengan aktivitas yang lebih besar, Detektif sekarang memberi tahu Anda untuk menavigasi ke grup pencari itu.	18 September 2023
Titik akhir dan kuota Detektif Amazon	Detektif sekarang tersedia di Wilayah Israel (Tel Aviv).	Agustus 25, 2023
Visualisasi grup temuan yang ditingkatkan	Visualisasi kelompok temuan Detektif sekarang termasuk menemukan kelompok dengan temuan agregat sehingga lebih efisien untuk menganalisis bukti, entitas, dan temuan terkait.	8 Agustus 2023

Kelompok temuan yang ditingkatkan	Menemukan grup sekarang termasuk temuan kerentanan dari Amazon Inspector.	13 Juni 2023
Ditambahkan dukungan untuk Amazon GuardDuty Lambda Protection	Detective sekarang menyediakan dukungan untuk Lambda GuardDuty Protection.	26 Mei 2023
Menambahkan temuan AWS keamanan sebagai paket sumber data opsional baru.	Detective sekarang menyediakan temuan AWS keamanan sebagai paket sumber data opsional. Paket sumber data opsional ini memungkinkan Detective untuk menyerap data dari Security Hub dan menambahkan data tersebut ke grafik perilaku Anda.	16 Mei 2023
Menambahkan dukungan untuk jenis pencarian Amazon GuardDuty EKS Runtime Monitoring	Detective sekarang menyediakan dukungan untuk jenis pencarian GuardDuty EKS Runtime Monitoring.	3 Mei 2023
Menambahkan dukungan untuk jenis pencarian Amazon GuardDuty RDS Protection	Detective sekarang menyediakan dukungan untuk jenis pencarian Perlindungan GuardDuty RDS.	20 April 2023

Menambahkan dukungan untuk jenis GuardDuty pencarian Amazon tambahan	Detective sekarang menyediakan profil untuk jenis GuardDuty temuan tambahan berikut: `DefenseEvasion: EC2UnusualDNSResolver` `DefenseEvasion: EvasionEC2UnusualDoHActivity` `DefenseEvasion: DefenseEvasionEC2UnusualDoTActivity`	12 April 2023
Menambahkan panel konsol baru di konsol Detektif untuk membantu pengguna memilih kebijakan AWS terkelola yang sesuai untuk kasus penggunaan spesifik mereka.	Detective menawarkan kebijakan terkelola untuk aman pilih izin yang Anda butuhkan.	3 April 2023
Menampilkan lalu lintas arus VPC untuk kluster EKS	Menambahkan bagian baru untuk lalu lintas arus Amazon Virtual Private Cloud (Amazon VPC) dengan cluster Amazon Elastic Kubernetes Service (Amazon EKS).	2 Maret 2023
Kelompok pencarian sekarang mencakup representasi visual dinamis dari grafik perilaku Detektif	Kelompok temuan Detektif sekarang mencakup representasi visual dinamis dari grafik perilaku Detective untuk menekankan hubungan antara entitas dan temuan dalam kelompok temuan.	28 Februari 2023

Ekspor data dari halaman Ringkasan Detektif dan halaman hasil pencarian. Data diekspor dalam format nilai dipisahkan koma (CSV).	Detective sekarang menyediakan opsi untuk mengekspor data ke browser Anda dari konsol Detective.	7 Februari 2023
Menambahkan volume aliran VPC keseluruhan untuk beban kerja EKS Amazon EKS	Detective sekarang menambahkan ringkasan visual dan analitik tentang alur log Amazon Virtual Private Cloud (VPC) Amazon Virtual Cloud (VPC) dari beban kerja Amazon Elastic Kubernetes Service Amazon EKS Anda.	19 Januari 2023
Menambahkan informasi kebijakan terkelola ke bagian keamanan	Detektif sekarang mendukung tindakan GuardDuty mendapatkan temuan melalui kebijakan. AmazonDetectiveFullAccess Bab keamanan sekarang memberikan rincian tentang kebijakan terkelola baru berikut untuk Detektif: AmazonDetectiveMemberAccess dan. AmazonDetectiveInvestigatorAccess	Januari 17, 2023
Menambahkan retensi data	Dengan Detective, Anda dapat mengakses data peristiwa historis hingga satu tahun.	Desember 20, 2022

Ditambahkan pilihan untuk menyesuaikan waktu lingkup pada halaman ringkasan.	Detective sekarang menyediakan opsi untuk menyesuaikan waktu lingkup sehingga melihat aktivitas untuk setiap kerangka waktu 24 jam dalam 365 hari sebelumnya.	5 Oktober 2022
Mencari temuan atau entitas	Detective sekarang menyediakan pencarian yang tidak peka huruf besar/kecil.	3 Oktober 2022
Menambahkan kemampuan untuk mengatur stempel waktu lingkup	Detective sekarang menyediakan cara untuk mengonfigurasi preferensi format cap waktu lingkup. Preferensi ini akan diterapkan ke semua stempel waktu di Detective.	3 Oktober 2022
Menambahkan istilah yang terkait dengan menemukan grup	Detective sekarang mendukung pencarian grup yang menghubungkan temuan terkait bersama-sama dalam satu tampilan untuk membantu Anda menyelidiki potensi aktivitas berbahaya di lingkungan Anda. Dari profil grup pencarian, Anda dapat beralih ke profil entitas dan menemukan ikhtisar yang terkait dengan grup tersebut.	3 Agustus 2022

Menambahkan profil baru yang terkait dengan log audit Amazon EKS	Detective sekarang menyediakan profil untuk memungkinkan Anda menyelidiki aktivitas yang terkait dengan entitas terkait container berikut: klaster Amazon EKS, image container, pod Kubernetes, dan subjek Kubernetes.	26 Juli 2022
Menambahkan sumber data opsional baru	Detective sekarang mendukung log audit EKS sebagai paket sumber data opsional. Akun administrator dapat mengaktifkan sumber data baru ini untuk grafik perilaku yang ada. Grafik yang dibuat setelah tanggal ini akan mengaktifkan sumber data ini secara default. Administrator dapat menonaktifkan sumber data ini secara manual kapan saja.	26 Juli 2022
Peran terkait layanan baru dan kebijakan terkelola untuk Detektif	Detektif sekarang memiliki peran terkait layanan. `AWSServiceRoleForDetective` Peran terkait layanan digunakan untuk mengakses data Organizations atas nama Anda. Peran tersebut menggunakan kebijakan `AmazonDetectiveServiceLinkedRolePolicy` terkelola baru.	Desember 16, 2021

Integrasi ditambahkan dengan AWS Organizations	Detective sekarang terintegrasi dengan Organizations. Akun manajemen organisasi menunjuk akun administrator Detektif untuk organisasi. Akun administrator Detektif dapat melihat semua akun di organisasi, dan mengaktifkan akun tersebut sebagai akun anggota dalam grafik perilaku organisasi.	Desember 16, 2021
Mengganti profil pencarian dengan menemukan ikhtisar	Menemukan profil berisi visualisasi yang menganalisis aktivitas untuk sumber daya yang terlibat. Ikhtisar temuan baru berisi rincian temuan yang dicerna dari GuardDuty, dan daftar entitas yang terlibat. Dari ikhtisar temuan, Anda dapat beralih ke profil untuk entitas terkait.	September 20, 2021
Menghapus batas pada jenis GuardDuty temuan yang didukung	Detektif tidak lagi terbatas pada serangkaian jenis GuardDuty temuan yang dipilih. Detective secara otomatis mengumpulkan rincian pencarian untuk semua jenis temuan, dan menyediakan akses ke profil entitas untuk entitas terkait.	September 20, 2021

Tautan untuk menemukan detail dari panel profil temuan terkait	Pada profil entitas, ketika Anda memilih temuan dalam daftar temuan terkait, rincian temuan ditampilkan di panel di sebelah kanan. Waktu lingkup diatur ke jendela waktu pencarian.	September 20, 2021
Menambahkan bucket S3 ke tipe entitas yang tersedia di Detective	Detective sekarang menyediakan profil untuk ember S3. Profil bucket S3 memberikan detail tentang prinsipal yang berinteraksi dengan bucket S3 dan operasi API yang mereka lakukan pada bucket S3.	September 20, 2021
Opsi baru untuk menghasilkan URL Detektif di Splunk	Proyek Splunk Trumpet memungkinkan Anda mengirim AWS konten ke Splunk. Proyek ini sekarang memungkinkan Anda untuk menambahkan URL Detektif untuk menavigasi ke profil untuk temuan. GuardDuty	8 September 2021

AKID yang diganti dalam detail aktivitas untuk akun dan peran	Pada profil akun, detail aktivitas untuk Volume panggilan API Keseluruh an sekarang menampilkan pengguna atau peran, bukan pengidentifikasi kunci akses (AKID). Pada profil peran, detail aktivitas untuk volume panggilan API Keseluruhan sekarang menampilkan sesi peran, bukan AKID. Untuk aktivitas yang terjadi sebelum perubahan ini, pemanggil terdaftar sebagai Sumber daya tidak dikenal.	14 Juli 2021

Menambahkan layanan panggilan ke informasi tentang panggilan API	Pada konsol Detective, informasi tentang panggilan API sekarang mencakup layanan yang mengeluarkan panggilan. Menambahkan kolom Service ke daftar pada volume panggilan API Keseluruhan, Panggilan API yang baru diamati, dan panggilan API dengan volume yang meningkat. Pada detail aktivitas untuk Volume panggilan API Keseluruhan dan geolokasi yang baru diamati, metode API dikelompokkan di bawah layanan yang menerbitkannya. Untuk aktivitas yang terjadi sebelum perubahan ini, metode API dikelompokkan di bawah layanan Tidak Dikenal.	14 Juli 2021
Tab interaksi Sumber Daya baru untuk pengguna, peran, dan sesi peran	Tab interaksi sumber daya untuk pengguna, peran, dan sesi peran berisi informasi tentang aktivitas asumsi peran yang melibatkan entitas tersebut. Untuk sesi peran, ini adalah tab baru. Untuk pengguna dan peran, ini adalah tab yang ada dengan konten baru.	29 Juni 2021

Nilai yang diperbarui untuk kuota volume data grafik perilaku	Meningkatkan kuota volume data untuk grafik perilaku. Pada 3,24 TB per hari, Detektif mengeluarkan peringatan. Dengan 3,6 TB per hari, tidak ada akun baru yang dapat ditambahkan. Pada 4,5 TB per hari, Detective berhenti menelan data ke dalam grafik perilaku.	10 Juni 2021
Menambahkan nilai tag ke opsi skrip Python	Saat Anda menggunakan skrip Detective Python untuk `enableDetective.py` mengaktifkan Detective, Anda sekarang dapat menetapkan nilai tag ke grafik perilaku.	19 Mei 2021
Menambahkan pengaktifan otomatis akun anggota yang lolos pemeriksaan volume data	Ketika akun anggota menerima undangan, statusnya Diterima (Tidak diaktifkan) sampai Detektif memverifikasi bahwa data mereka tidak akan menyebabkan volume data grafik perilaku melebihi kuota. Jika volume data tidak menjadi masalah, Detektif secara otomatis mengubah status menjadi Diterima (Diaktifkan). Perhatikan bahwa akun anggota yang ada yang saat ini Diterima (Tidak diaktifkan) tidak dapat diaktifkan secara otomatis.	12 Mei 2021

Menambahkan informasi kebijakan terkelola ke bagian keamanan	Bagian baru di bagian keamanan memberikan rincian tentang kebijakan terkelola untuk Detektif. Detective saat ini menyediakan kebijakan terkelola tunggal,. `AmazonDetectiveFullAccess`	10 Mei 2021
Mengubah nilai volume data dalam daftar akun anggota	Pada halaman manajemen akun, daftar akun anggota sekarang menampilkan volume data harian untuk setiap akun anggota. Sebelumnya daftar menampilkan volume sebagai persentase dari total volume yang diizinkan.	29 April 2021
Opsi yang direvisi untuk mengelola akun anggota	Mengganti menu Kelola akun dengan menu Tindakan. Menggabungkan opsi untuk menambahkan akun individual dan menambahkan akun dari file.csv. Memindahkan Aktifkan akun dari Kelola akun ke opsi terpisah di samping Tindakan.	5 April 2021
Menambahkan tag grafik perilaku dan otorisasi berdasarkan tag	Saat mengaktifkan Detektif, Anda dapat menambahkan tag ke grafik perilaku. Anda dapat mengelola tag untuk grafik perilaku dari halaman Umum. Detective juga mendukung otorisasi berdasarkan nilai tag.	31 Maret 2021

Menambahkan dukungan untuk jenis GuardDuty pencarian Amazon tambahan	Detective sekarang menyediakan profil untuk jenis GuardDuty temuan tambahan berikut:`CredentialAccess:IAMUser/AnomalousBehavior` ,, `DefenseEvasion:IAMUser/AnomalousBehavior` ,`Discovery:IAMUser/AnomalousBehavior` ,`Exfiltration:IAMUser/AnomalousBehavior` ,`Impact:IAMUser/AnomalousBehavior` , `InitialAccess:IAMUser/AnomalousBehavior` `Persistence:IAMUser/AnomalousBehavior` `PrivilegeEscalation:IAMUser/AnomalousBehavior`	29 Maret 2021
Perbedaan tambahan untuk AWS GovCloud (US) Wilayah	Detektif sekarang tersedia di Wilayah. AWS GovCloud (US) Di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat), Detektif tidak mengirim email undangan ke akun anggota. Detektif juga tidak secara otomatis menghapus akun anggota yang dimatikan. AWS	24 Maret 2021

Menambahkan tab untuk memfilter daftar akun anggota berdasarkan status akun anggota	Daftar akun anggota sekarang menampilkan tab yang dapat Anda gunakan untuk memfilter daftar berdasarkan status akun anggota. Anda dapat melihat semua akun anggota, yang memiliki status Diterima (Diaktifkan), atau yang memiliki status selain Diterima (Diaktifkan).	16 Maret 2021
Menambahkan dukungan untuk jenis GuardDuty pencarian Amazon tambahan	Detective sekarang menyediakan profil untuk jenis GuardDuty temuan tambahan berikut:`Backdoor:EC2/C&CActivity.B` ,,`Impact:EC2/PortSweep` , dan `Impact:EC2/WinRMBruteForce` `Privilege Escalation:IAMUser/AdministrativePermissions`	4 Maret 2021
Menambahkan opsi ke skrip Python untuk menekan email undangan	`enableDetective.py` Script Detective sekarang menyediakan opsi. `--disable_email` Ketika Anda menyertakan opsi itu, Detektif tidak mengirim email undangan ke akun anggota.	26 Februari 2021
Mengubah “akun master” menjadi “akun administrator”	Istilah "akun utama" diubah menjadi "akun administrator." Istilah ini juga diubah di konsol Detective dan API.	25 Februari 2021

Mengubah “akun master” menjadi “akun administrator”	Istilah "akun utama" diubah menjadi "akun administrator." Istilah ini juga diubah di konsol Detective dan API.	25 Februari 2021
Menambahkan detail aktivitas untuk volume aliran VPC panel profil ke dan dari alamat IP temuan	Volume aliran VPC panel profil ke dan dari alamat IP temuan sekarang memungkinkan Anda untuk menampilkan detail aktivitas. Rincian aktivitas hanya tersedia jika temuan dikaitkan dengan satu alamat IP. Detail aktivitas menunjukkan volume untuk setiap kombinasi port, protokol, dan arah.	25 Februari 2021
Menambahkan opsi API untuk tidak mengirim email undangan ke akun anggota	Saat menggunakan Detective API untuk menambahkan akun anggota, akun administrator dapat memilih untuk tidak mengirim email undangan ke akun anggota.	25 Februari 2021
Detail aktivitas baru untuk panel profil volume panggilan API Keseluruhan pada profil alamat IP	Anda sekarang dapat menampilkan detail aktivitas untuk alamat IP dari panel profil volume panggilan API Keseluruhan. Detail aktivitas menunjukkan jumlah panggilan yang berhasil dan gagal untuk setiap sumber daya yang mengeluarkan panggilan dari alamat IP.	23 Februari 2021

Panel profil volume aliran VPC Keseluruhan Baru pada profil alamat IP	Profil alamat IP sekarang berisi panel profil volume aliran VPC Keseluruhan. Panel profil menunjukkan volume lalu lintas arus VPC ke dan dari alamat IP. Anda dapat menampilkan detail aktivitas untuk menampilkan volume untuk setiap instans EC2 yang dikomunikasikan dengan alamat IP.	21 Januari 2021
Ditambahkan halaman Ringkasan Detektif	Halaman Ringkasan Detektif berisi visualisasi untuk memandu analis ke entitas yang diminati berdasarkan geolokasi, jumlah panggilan API, dan volume lalu lintas Amazon EC2.	21 Januari 2021
Memperbarui opsi untuk beralih dari Amazon ke Detektif GuardDuty	Dalam GuardDuty, opsi Investigate in Detective dipindahkan dari menu Actions ke panel finding details. Ini menampilkan daftar entitas terkait. Jika jenis temuan didukung, daftar juga menyertakan temuan. Anda kemudian dapat memilih untuk menavigasi ke profil entitas atau profil pencarian.	15 Januari 2021

Ditambahkan pilihan untuk mengatur jendela rincian aktivitas untuk waktu lingkup default	Pada detail aktivitas untuk Volume panggilan API Keseluruhan dan Volume aliran VPC keseluruhan, Anda dapat mengatur jendela waktu untuk detail aktivitas ke waktu cakupan default untuk profil.	15 Januari 2021
Menambahkan penanganan interval waktu volume tinggi untuk entitas	Menambahkan pemberitahuan baru untuk menunjukkan kapan entitas memiliki satu atau lebih interval waktu volume tinggi. Halaman entitas bervolume tinggi baru menampilkan semua interval volume tinggi untuk waktu lingkup saat ini.	18 Desember 2020
Kuota akun member meningkat menjadi 1.200	Akun master sekarang dapat mengundang hingga 1.200 akun anggota ke grafik perilaku mereka. Sebelumnya kuota adalah 1.000.	11 Desember 2020
Menambahkan nilai untuk kuota volume data grafik perilaku	Memperbarui informasi tentang kuota volume data grafik perilaku untuk menambahkan nilai kuota tertentu.	11 Desember 2020

Menambahkan pemilihan rentang waktu untuk detail aktivitas pada panel profil volume panggilan API Keseluruhan	Pada panel volume aliran API Keseluruhan, Anda sekarang dapat menampilkan detail aktivitas untuk rentang waktu yang dipilih. Panel awalnya menampilkan opsi untuk menampilkan detail aktivitas untuk waktu lingkup.	29 September 2020
Menambahkan pemilihan interval waktu untuk detail aktivitas pada panel profil volume aliran VPC Keseluruhan	Pada panel Volume aliran VPC Keseluruhan, Anda dapat menampilkan detail aktivitas untuk interval waktu tunggal dari bagan. Untuk menampilkan detail interval waktu, pilih interval waktu.	25 September 2020
Sesi peran baru dan entitas pengguna federasi	Detective sekarang memungkinkan Anda untuk menjelajahi dan menyelidiki otentikasi federasi. Anda dapat melihat sumber daya apa yang telah mengambil alih setiap peran, dan kapan otentikasi tersebut terjadi.	17 September 2020
Pembaruan untuk manajemen waktu lingkup	Menghapus opsi untuk mengunci atau membuka ruang lingkup waktu. Itu selalu terkunci. Pada profil temuan, peringatan ditampilkan jika waktu lingkup berbeda dari jendela waktu pencarian.	Selasa, 04 September 2020

Header profil tetap terlihat saat Anda menggulir profil	Pada profil, jenis, pengenal, dan waktu lingkup tetap terlihat saat Anda menggulir panel profil pada tab. Ketika tab tidak terlihat, Anda dapat menggunakan daftar drop-down tab di remah roti untuk menavigasi ke tab yang berbeda.	Selasa, 04 September 2020
Pencarian selalu menampilkan hasil pencarian	Saat Anda melakukan pencarian, sekarang menampilkan hasilnya di halaman Pencarian. Dari hasil, Anda dapat beralih ke temuan atau profil entitas.	27 Agustus 2020
Ditambahkan ke kriteria yang diizinkan untuk pencarian	Kriteria yang diizinkan untuk pencarian telah diperluas. Anda dapat mencari AWS pengguna dan AWS peran berdasarkan nama. Anda dapat menggunakan ARN untuk mencari temuan, AWS peran, AWS pengguna, dan instans EC2.	27 Agustus 2020
Tautan ke konsol lain dari panel profil	Pada panel profil detail instans EC2, pengenal instans EC2 ditautkan ke konsol Amazon EC2. Pada panel profil Detail pengguna, dan Role details, nama pengguna dan nama peran ditautkan ke konsol IAM.	14 Agustus 2020

Detail aktivitas untuk data aliran VPC	Panel profil volume aliran VPC Keseluruhan sekarang menyediakan akses ke detail aktivitas. Detail aktivitas menunjukkan arus lalu lintas antara alamat IP dan instans EC2 selama periode waktu yang dipilih.	23 Juli 2020
Akun anggota sekarang dapat melihat penggunaan dan biaya yang diproyeksikan	Akun anggota sekarang dapat melihat informasi penggunaan mereka sendiri. Untuk akun anggota, halaman Penggunaan menunjukkan jumlah data yang dicerna ke dalam setiap grafik perilaku yang mereka kontribusikan. Akun anggota juga dapat melihat proyeksi biaya 30 hari mereka.	26 Mei 2020
Uji coba gratis sekarang per akun, bukan per grafik perilaku	Setiap akun Amazon Detective sekarang menerima uji coba gratis terpisah di setiap Wilayah. Uji coba gratis dimulai baik ketika akun mengaktifkan Detektif, atau pertama kali akun diaktifkan sebagai akun anggota.	26 Mei 2020

Skrip Python open source baru di GitHub	amazon-detective-multiaccount-scriptsRepositori baru di GitHub menyediakan skrip Python open source yang dapat Anda gunakan untuk mengelola grafik perilaku di seluruh Wilayah. Anda dapat mengaktifkan Detektif, menambahkan akun anggota, menghapus akun anggota, dan menonaktifkan Detektif.	21 Januari 2020
Memperkenalkan Detektif Amazon	Detective menggunakan pembelajaran mesin dan visualisasi yang dibuat khusus untuk membantu Anda menganalisis dan menyelidiki masalah keamanan di seluruh beban kerja Amazon Web Services () Anda.AWS	2 Desember 2019

Konten dari Panduan Administrasi Detektif Amazon sekarang dikonsolidasikan ke dalam Panduan Pengguna Detektif Amazon. Panduan Administrasi Detektif Amazon akan mencapai akhir dukungan standar pada 08 Mei 2024.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.