Berbagi intelijen ancaman cyber di AWS

AWS Panduan Preskriptif

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Panduan Preskriptif: Berbagi intelijen ancaman cyber di AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Pengantar 1
Model berbagi CTI 3
Keamanan cloud 3
Keamanan cloud 4
Arsitektur CTI 5
Menyebarkan platform intelijen ancaman 6
Menelan CTI 7
Mengotomatiskan kontrol keamanan 8
Amazon GuardDuty 11
Amazon Route 53 Resolver Firewall DNS 13
AWS Network Firewall 14
Mendapatkan visibilitas 16
Logging lalu lintas jaringan 16
Memusatkan temuan keamanan di AWS 16
Mengintegrasikan AWS data keamanan dengan data perusahaan lainnya 19
Berbagi CTI 19
Langkah selanjutnya 22
AWS sumber daya 22
Layanan AWS dokumentasi 22
Sumber daya STIX 23
Platform intelijen ancaman 23
Kontributor 24
Mengotorisasi 24
Meninjau 24
Penulisan teknis 24
Riwayat dokumen 25
..... xxvi

Berbagi intelijen ancaman cyber di AWS

Amazon Web Services (kontributor)

Desember 2024 (riwayat dokumen)

Ketika risiko baru muncul, praktik terbaik untuk melindungi beban kerja cloud kritis terus berkembang. Karena jumlah aset yang terhubung ke internet yang memerlukan perlindungan meningkat, demikian juga risiko peristiwa keamanan yang terkait dengan pelaku ancaman. Cyber Threat Intelligence (CTI) adalah pengumpulan dan analisis data yang menunjukkan niat, peluang, dan kemampuan aktor ancaman. Ini berbasis bukti dan dapat ditindaklanjuti, dan menginformasikan kegiatan pertahanan dunia maya. Ini sering mencakup informasi yang berkaitan dengan atribusi aktor, teknik dan prosedur taktik, motif, atau target.

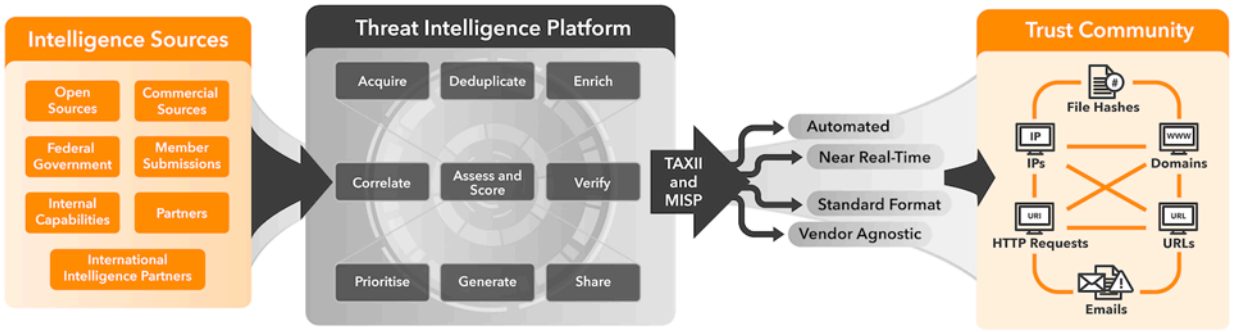
CTI dapat dibagi dalam suatu organisasi, antara organisasi dalam komunitas kepercayaan, dengan Pusat Berbagi Informasi dan Analisis (ISAC), atau dengan entitas lain, seperti otoritas pemerintah. Contoh otoritas pemerintah termasuk Australian Cyber Security Centre (ACSC) dan American Cybersecurity and Infrastructure Security Agency (CISA).

Seperti semua bentuk intelijen, konteks ancaman sangat penting. Berbagi CTI menginformasikan manajemen risiko keamanan siber yang dinamis. Ini penting untuk pertahanan, respons, dan pemulihan keamanan siber yang tepat waktu. Ini meningkatkan efisiensi dan efektivitas kemampuan keamanan siber. Konteks ancaman juga penting untuk membedakan antara persyaratan kemampuan CTI yang berkaitan dengan target yang berbeda. Misalnya, aktor canggih mungkin menargetkan perusahaan atau pemerintah tertentu sedangkan pelaku komoditas menggunakan alat dan teknik yang tersedia untuk menyerang individu dan organisasi secara luas.

Perencanaan keamanan, observabilitas, analisis intelijen ancaman, otomatisasi kontrol keamanan, dan berbagi dalam komunitas kepercayaan adalah bagian penting dari siklus hidup intelijen ancaman. AWS membantu Anda mengotomatiskan tugas keamanan manual untuk mendeteksi ancaman dengan akurasi yang lebih tinggi, merespons lebih cepat, dan menghasilkan intelijen ancaman berkualitas tinggi yang dapat Anda bagikan. Anda dapat menemukan serangan siber baru, menganalisisnya, menghasilkan CTI, membagikannya, dan menerapkannya — semuanya dengan kecepatan yang dirancang untuk mencegah serangan kedua terjadi.

Panduan ini menjelaskan cara menyebarkan platform intelijen ancaman. AWS Komunitas kepercayaan menyediakan CTI, dan platform mencernanya untuk mengidentifikasi kecerdasan yang dapat ditindaklanjuti dan mengotomatiskan kontrol protektif dan detektif di lingkungan. AWS Gambar

berikut menunjukkan siklus hidup intelijen ancaman. CTI datang dari sumbernya, dan kemudian platform intelijen ancaman memprosesnya. Dengan menggunakan protokol Trusted Automated Exchange of Intelligence Information (TAXII) atau Platform Berbagi Informasi Malware (MISP), CTI dibagikan dengan komunitas kepercayaan untuk bertindak.



Platform intelijen ancaman menggunakan CTI untuk secara otomatis menerapkan kontrol keamanan di AWS lingkungan Anda atau untuk memberi tahu tim keamanan Anda jika tindakan manual diperlukan. Kontrol preventif adalah kontrol keamanan yang dirancang untuk mencegah suatu peristiwa terjadi. Contohnya termasuk otomatisasi memblokir daftar alamat IP buruk atau nama domain yang diketahui dengan menggunakan firewall jaringan, penyelesai DNS, dan sistem pencegahan intrusi lainnya (IPS). Kontrol detektif adalah kontrol keamanan yang dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi. Contohnya termasuk pemantauan terus menerus untuk aktivitas berbahaya dan mencari log untuk bukti masalah atau peristiwa.

Anda dapat mengumpulkan temuan apa pun dalam alat observabilitas keamanan terpusat, seperti. AWS Security Hub CSPM Kemudian, Anda dapat berbagi temuan dengan komunitas kepercayaan untuk secara kolaboratif membangun gambaran ancaman yang komprehensif.

Model tanggung jawab bersama untuk berbagi CTI

Model tanggung jawab AWS bersama mendefinisikan bagaimana Anda berbagi tanggung jawab AWS untuk keamanan dan kepatuhan di cloud. AWS mengamankan infrastruktur yang menjalankan semua layanan yang ditawarkan di AWS Cloud, yang dikenal sebagai keamanan cloud. Anda bertanggung jawab untuk mengamankan penggunaan layanan tersebut, seperti data dan aplikasi Anda. Ini dikenal sebagai keamanan di cloud.

Keamanan cloud

Keamanan adalah prioritas utama di AWS. Kami bekerja keras untuk membantu mencegah masalah keamanan menyebabkan gangguan pada organisasi Anda. Saat kami berupaya mempertahankan infrastruktur dan data Anda, kami menggunakan wawasan skala global kami untuk mengumpulkan intelijen keamanan bervolume tinggi—dalam skala besar dan real time—untuk membantu melindungi Anda secara otomatis. Bila memungkinkan, AWS dan sistem keamanannya mengganggu ancaman di mana tindakan itu paling berdampak. Seringkali, pekerjaan ini terjadi di belakang layar.

Setiap hari, di seluruh AWS Cloud infrastruktur, kami mendeteksi dan berhasil menggagalkan ratusan serangan siber yang mungkin mengganggu dan mahal. Kemenangan penting tetapi sebagian besar tak terlihat ini dicapai dengan jaringan sensor global dan seperangkat alat gangguan terkait. Dengan menggunakan kemampuan ini, kami membuatnya lebih sulit dan mahal untuk serangan siber yang dilakukan terhadap jaringan dan infrastruktur kami.

AWS memiliki jejak jaringan publik terbesar dari penyedia cloud mana pun. Ini memberikan wawasan real-time AWS yang tak tertandingi tentang aktivitas tertentu di internet. MadPotadalah jaringan sensor ancaman yang didistribusikan secara global (dikenal sebagai honeypots). MadPot membantu tim AWS keamanan memahami taktik dan teknik penyerang. Setiap kali penyerang mencoba menargetkan salah satu sensor ancaman, AWS mengumpulkan dan menganalisis data.

Sonaris adalah alat internal lain yang AWS digunakan untuk menganalisis lalu lintas jaringan. Ini mengidentifikasi dan menghentikan upaya yang tidak sah untuk mengakses sejumlah besar akun dan sumber daya. Antara Mei 2023 dan April 2024, Sonaris membantah lebih dari 24 miliar upaya untuk memindai data pelanggan yang disimpan di Amazon Simple Storage Service (Amazon S3). Ini juga mencegah hampir 2,6 triliun upaya untuk menemukan beban kerja rentan yang berjalan di Amazon Elastic Compute Cloud (Amazon EC2).

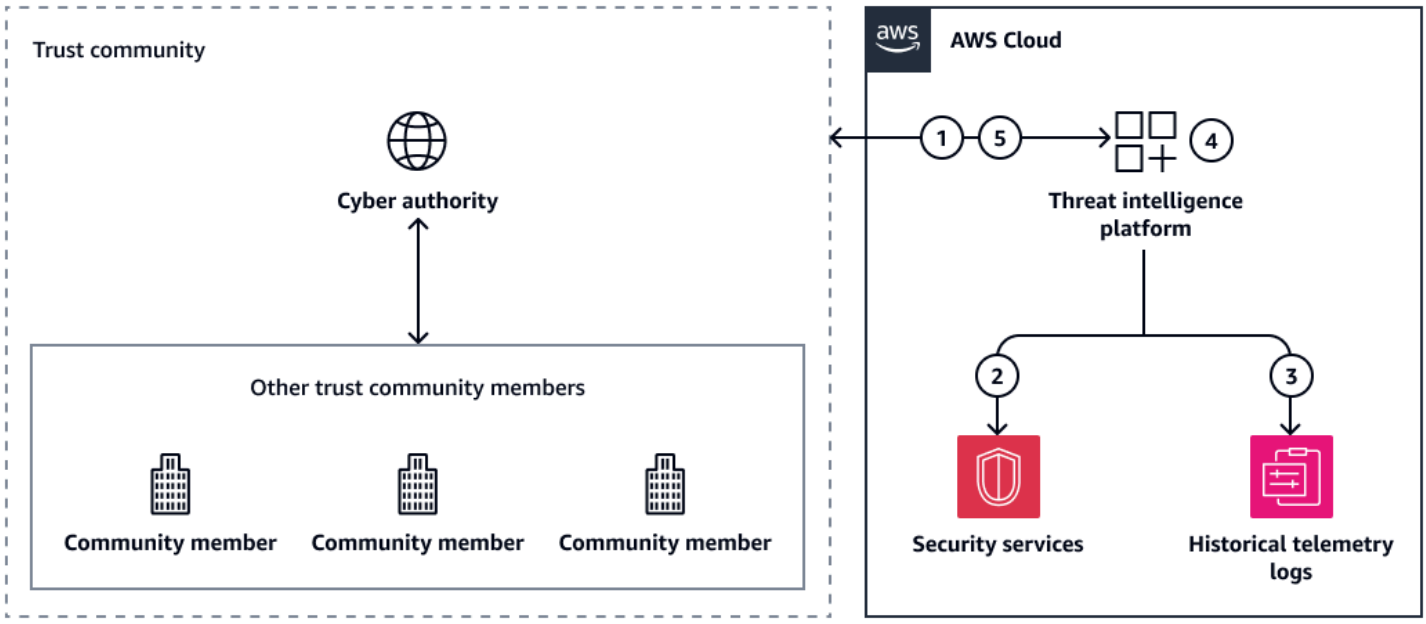
Keamanan cloud

Panduan ini berfokus pada praktik terbaik untuk intelijen ancaman cyber (CTI) di. AWS Cloud Anda bertanggung jawab untuk menghasilkan CTI yang dilokalkan dan dikontekstualisasikan. Anda mengontrol di mana data Anda disimpan, bagaimana itu diamankan, dan siapa yang memiliki akses ke sana. AWS tidak memiliki visibilitas ke data pencatatan, pemantauan, dan audit Anda, yang penting untuk keamanan berbasis CTI di cloud.

Structured Threat Information Expression (STIX) adalah bahasa open source dan format serialisasi yang digunakan untuk bertukar CTI. Indikator seperti hash file, domain, permintaan HTTP URLs, dan alamat IP adalah output penting untuk dibagikan untuk pemblokiran ancaman. Namun, tindakan efektif bergantung pada kecerdasan tambahan, seperti peringkat kepastian dan korelasi set intrusi. STIX 2.1 mendefinisikan 18 Objek Domain STIX, termasuk pola serangan, tindakan, aktor ancaman, lokasi geografis, dan informasi malware. Ini juga memperkenalkan konsep, seperti peringkat kepercayaan dan hubungan, yang membantu entitas menentukan sinyal dari kebisingan dalam volume besar data yang dikumpulkan oleh platform intelijen ancaman. Anda dapat mendeteksi, menganalisis, dan membagikan tingkat detail tentang ancaman di AWS lingkungan Anda. Untuk informasi selengkapnya, lihat Mengotomatiskan kontrol keamanan preventif dan detektif dalam panduan ini.

Arsitektur intelijen ancaman cyber di AWS

Gambar berikut menggambarkan arsitektur umum untuk menggunakan umpan ancaman untuk mengintegrasikan intelijen ancaman dunia maya (CTI) ke lingkungan Anda. AWS CTI dibagi antara platform intelijen ancaman Anda di AWS Cloud, otoritas cyber yang dipilih, dan anggota komunitas kepercayaan lainnya.



Ini menunjukkan alur kerja berikut:

1. Platform intelijen ancaman menerima CTI yang dapat ditindaklanjuti dari otoritas cyber atau dari anggota komunitas kepercayaan lainnya.
2. Platform intelijen ancaman AWS menugaskan layanan keamanan untuk mendeteksi dan mencegah peristiwa.
3. Platform intelijen ancaman menerima intelijen ancaman dari Layanan AWS.
4. Jika suatu peristiwa terjadi, platform intelijen ancaman mengkurasi CTI baru.
5. Platform intelijen ancaman berbagi CTI baru dengan otoritas cyber. Itu juga dapat berbagi CTI dengan anggota komunitas kepercayaan lainnya.

Ada banyak otoritas cyber yang menawarkan umpan CTI. Contohnya termasuk Australian Cyber Security Centre (ACSC), program Connect Inform Share Protect (CISP) yang ditawarkan oleh Pusat Keamanan Cyber Nasional Inggris, dan program Malware Free Networks (MFN) yang ditawarkan

oleh Biro Keamanan Komunikasi Pemerintah Selandia Baru. Banyak AWS Mitra juga menawarkan umpan berbagi CTI.

Untuk memulai berbagi CTI, kami sarankan Anda melakukan hal berikut:

1. Menyebarkan platform intelijen ancaman — Menyebarkan platform yang menyerap, mengumpulkan, dan mengatur data intelijen ancaman dari berbagai sumber dan dalam format yang berbeda.
2. Menelan intelijen ancaman dunia maya — Integrasikan platform intelijen ancaman Anda dengan satu atau lebih penyedia umpan ancaman. Saat Anda menerima umpan ancaman, gunakan platform intelijen ancaman Anda untuk memproses CTI baru dan mengidentifikasi intelijen yang dapat ditindaklanjuti yang relevan dengan operasi keamanan di lingkungan Anda. Otomatiskan sebanyak mungkin, tetapi ada beberapa situasi yang memerlukan keputusan manusia-in-the-loop.
3. Mengotomatiskan kontrol keamanan preventif dan detektif — Menyebarkan CTI ke layanan keamanan dalam arsitektur Anda yang menyediakan kontrol preventif dan detektif. Layanan ini umumnya dikenal sebagai sistem pencegahan intrusi (IPS). Pada AWS, Anda menggunakan API layanan untuk mengonfigurasi daftar blokir yang menolak akses dari alamat IP dan nama domain yang disediakan di feed ancaman.
4. Mendapatkan visibilitas dengan mekanisme observabilitas — Sementara operasi keamanan berlangsung di lingkungan Anda, Anda mengumpulkan CTI baru. Misalnya, Anda mungkin mengamati ancaman yang termasuk dalam umpan ancaman, atau Anda mungkin mengamati indikator kompromi yang terkait dengan intrusi (seperti eksploitasi zero-day). Sentralisasi intelijen ancaman memberikan peningkatan kesadaran situasional di seluruh lingkungan Anda, sehingga Anda dapat meninjau CTI yang ada dan CTI yang baru ditemukan dalam satu sistem.
5. Berbagi CTI dengan komunitas kepercayaan Anda — Untuk menyelesaikan siklus hidup berbagi CTI, buat CTI Anda sendiri dan bagikan kembali ke komunitas kepercayaan Anda.

Video berikut, Scaling cyber threat intelligence sharing dengan AUS Cyber Security Center, membahas langkah-langkah ini secara lebih rinci. Meskipun video ini membahas kemampuan berbagi CTI dari Pusat Keamanan Cyber Australia, langkah-langkahnya sama terlepas dari umpan ancaman yang Anda pilih atau lokasi Anda.

Menyebarkan platform intelijen ancaman

Platform intelijen ancaman menyerap, mengumpulkan, dan mengatur data intelijen ancaman dari berbagai sumber dan dalam format yang berbeda. Hal ini memungkinkan analis untuk melihat,

memprioritaskan, dan bertindak atas intelijen ancaman cyber (CTI) yang telah diterima dari komunitas kepercayaan mereka.

OpenCTI dan MISP adalah platform intelijen ancaman open source yang umum. Ada juga solusi yang tersedia dari AWS Mitra di AWS Marketplace. Anda harus mempertimbangkan tingkat keterampilan tim keamanan Anda saat memilih platform intelijen ancaman. MISP dapat menjadi kuat namun kompleks, dan OpenCTI memiliki antarmuka pengguna yang lebih intuitif.

Saat memilih platform intelijen ancaman, pertimbangkan hal berikut:

- Fitur — Apakah platform menawarkan fitur seperti pemantauan waktu nyata, deteksi ancaman, dan analisis?
- Sumber data — Apakah platform menggunakan berbagai sumber, termasuk umpan ancaman, kecerdasan web gelap, media sosial, dan intelijen sumber terbuka?
- Kualitas data — Apakah platform memiliki proses untuk memastikan bahwa informasi tersebut akurat dan dapat diandalkan?
- Skalabilitas — Dapatkah platform beradaptasi dengan perubahan kebutuhan organisasi Anda, seperti pertumbuhan dan ancaman yang berkembang?
- Integrasi — Dapatkah platform dapat berintegrasi dengan alat dan infrastruktur keamanan yang ada?
- Pengalaman pengguna — Apakah platform ini mudah dinavigasi dan digunakan?
- Kustomisasi — Dapatkah platform disesuaikan untuk memenuhi kebutuhan spesifik organisasi Anda?
- Biaya — Apakah platform ini hemat biaya, termasuk biaya lisensi dan persyaratan pemeliharaan?

Anda dapat menyebarkan platform intelijen ancaman Anda dalam virtual private cloud (VPC) Anda. Anda dapat menerapkannya langsung di instans Amazon Elastic Compute Cloud (Amazon EC2) atau dengan menggunakan teknologi container, seperti Amazon Elastic Container Service (Amazon ECS) atau. AWS Fargate Untuk informasi selengkapnya tentang memilih layanan AWS kontainer yang tepat untuk pengembangan aplikasi modern Anda, lihat Memilih layanan AWS kontainer.

Menelan intelijen ancaman cyber

Langkah pertama dalam proses konsumsi adalah mengubah data intelijen ancaman cyber (CTI) dari umpan ancaman ke dalam format yang dapat dikonsumsi oleh platform intelijen ancaman Anda. Ini disebut konversi CTI. Data umpan ancaman dapat datang dalam berbagai format, seperti Structured

Threat Information Expression (STIX). Anda harus merestrukturisasi data yang masuk ke dalam format yang dapat diprediksi dan mudah dikonsumsi yang sesuai untuk produk keamanan yang Anda gunakan di lingkungan Anda. AWS

Untuk kompatibilitas maksimum, kami sarankan Anda mengonversi data menjadi format JSON. Misalnya, AWS Step Functionsdapat mengkonsumsi data yang dalam format JSON, dan alur kerja otomatisasi dapat lebih mudah dan konsisten mengkonsumsi format ini. Informasi lebih lanjut tentang membangun alur kerja otomatis disediakan di bagian berikutnya, Mengotomatiskan kontrol keamanan preventif dan detektif.

Untuk mempercepat konsumsi data CTI, Anda dapat mengotomatiskan transformasi data. Data dikonversi saat dicerna dan kemudian diteruskan langsung ke platform intelijen ancaman. Anda dapat menggunakan AWS Lambda fungsi untuk menyelesaikan transformasi, dan Anda dapat mengatur proses melalui Layanan AWS seperti atau AWS Step Functions Amazon. EventBridge

Saat Anda menelan CTI, Anda dapat memilih atribut mana yang akan diekstrak dan dipertahankan. Jumlah detail yang diperlukan dapat bervariasi tergantung pada kebutuhan bisnis Anda. Namun, untuk melakukan pembaruan pada firewall dan layanan keamanan lainnya, kami merekomendasikan atribut minimum berikut:

- Alamat IP dan domain
- Ancaman
- Menambahkan atau menghapus dari daftar ancaman internal Anda

Ekstrak atribut yang ingin Anda gunakan, lalu format ke dalam template JSON terstruktur.

Mengotomatiskan kontrol keamanan preventif dan detektif

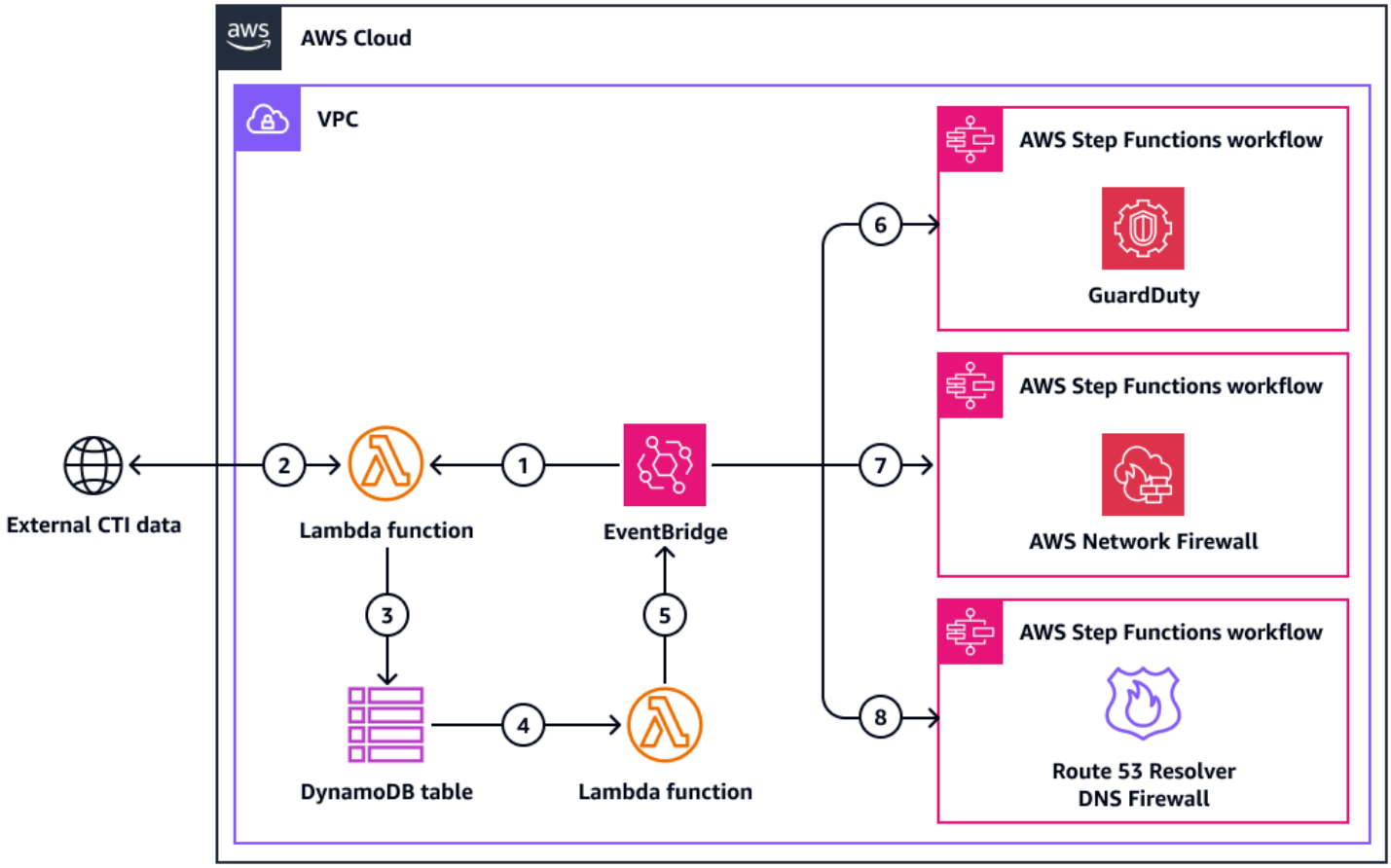
Setelah intelijen ancaman dunia maya (CTI) tertelan ke platform intelijen ancaman, Anda dapat mengotomatiskan proses membuat perubahan konfigurasi sebagai respons terhadap data. Platform intelijen ancaman membantu Anda mengelola intelijen ancaman dunia maya dan mengamati lingkungan Anda. Mereka menyediakan kemampuan untuk menyusun, menyimpan, mengatur dan memvisualisasikan informasi teknis dan non-teknis tentang ancaman cyber. Mereka dapat membantu Anda membangun gambaran ancaman dan menggabungkan berbagai sumber intelijen untuk membuat profil dan melacak ancaman, seperti ancaman persisten lanjutan (APT).

Otomatisasi dapat mengurangi waktu antara menerima intelijen ancaman dan menerapkan perubahan konfigurasi di lingkungan. Tidak semua respons CTI dapat diotomatisasi. Namun,

mengotomatiskan tanggapan sebanyak mungkin membantu tim keamanan Anda memprioritaskan dan menilai CTI yang tersisa dengan cara yang lebih tepat waktu. Setiap organisasi harus menentukan jenis respons CTI mana yang dapat diotomatisasi dan mana yang memerlukan analisis manual. Buat keputusan ini berdasarkan konteks organisasi, seperti risiko, aset, dan sumber daya. Misalnya, beberapa organisasi mungkin memilih untuk mengotomatiskan blok untuk domain buruk atau alamat IP yang diketahui, tetapi mereka mungkin memerlukan penyelidikan analis sebelum memblokir alamat IP internal.

Bagian ini memberikan contoh cara mengatur respons CTI otomatis di Amazon GuardDuty, AWS Network Firewall, dan Amazon Route 53 Resolver DNS Firewall. Anda dapat menerapkan contoh-contoh ini secara independen satu sama lain. Biarkan persyaratan dan kebutuhan keamanan organisasi Anda memandu keputusan Anda. Anda dapat mengotomatiskan perubahan konfigurasi Layanan AWS melalui AWS Step Functionsalur kerja (juga disebut mesin status). Ketika AWS Lambdafungsi selesai mengonversi format CTI ke JSON, fungsi akan memicu EventBridge peristiwa Amazon yang memulai alur kerja Step Functions.

Diagram berikut menunjukkan contoh arsitektur. Alur kerja Step Functions secara otomatis memperbarui daftar ancaman GuardDuty, daftar domain di Route 53 Resolver DNS Firewall, dan grup aturan di Network Firewall.



Gambar tersebut menunjukkan alur kerja berikut:

1. Sebuah EventBridge acara dimulai dengan jadwal reguler. Acara ini memulai sebuah AWS Lambda fungsi.
2. Fungsi Lambda mengambil data CTI dari umpan ancaman eksternal.
3. Fungsi Lambda menulis data CTI yang diambil ke tabel Amazon DynamoDB.
4. Menulis data ke tabel DynamoDB memulai peristiwa aliran pengambilan data perubahan yang memulai fungsi Lambda.
5. Jika perubahan terjadi, fungsi Lambda memulai acara baru di. EventBridge Jika tidak ada perubahan yang terjadi, maka alur kerja selesai.
6. Jika CTI terkait dengan catatan alamat IP, EventBridge mulailah alur kerja Step Functions yang secara otomatis memperbarui daftar ancaman di Amazon. GuardDuty Untuk informasi selengkapnya, lihat Amazon GuardDuty di bagian ini.
7. Jika CTI terkait dengan alamat IP atau catatan domain, EventBridge mulailah alur kerja Step Functions yang secara otomatis memperbarui grup aturan. AWS Network Firewall Untuk informasi lebih lanjut, lihat AWS Network Firewalldi bagian ini.

8. Jika CTI berhubungan dengan catatan domain, maka EventBridge mulailah alur kerja Step Functions yang secara otomatis memperbarui daftar domain di Amazon Route 53 Resolver DNS Firewall. Untuk informasi selengkapnya, lihat Amazon Route 53 Resolver DNS Firewall di bagian ini.

Amazon GuardDuty

Amazon GuardDuty adalah layanan deteksi ancaman yang terus memantau Anda Akun AWS dan beban kerja untuk aktivitas yang tidak sah dan memberikan temuan keamanan terperinci untuk visibilitas dan remediasi. Dengan memperbarui daftar GuardDuty ancaman secara otomatis dari umpan CTI, Anda dapat memperoleh wawasan tentang ancaman yang mungkin mengakses beban kerja Anda. GuardDuty meningkatkan kemampuan kontrol detektif Anda.

> **Tip**
>
> GuardDuty secara native terintegrasi dengan. AWS Security Hub CSPM Security Hub CSPM memberikan pandangan komprehensif tentang keadaan keamanan Anda AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Ketika Anda berintegrasi GuardDuty dengan Security Hub CSPM, GuardDuty temuan Anda secara otomatis dikirim ke Security Hub CSPM. Security Hub CSPM kemudian dapat memasukkan temuan-temuan tersebut dalam analisisnya tentang postur keamanan Anda. Untuk informasi selengkapnya, lihat Mengintegrasikan dengan AWS Security Hub CSPM dalam GuardDuty dokumentasi. Di Security Hub CSPM, Anda dapat menggunakan otomatisasi untuk meningkatkan kemampuan kontrol keamanan detektif dan responsif Anda.

Gambar berikut menunjukkan bagaimana alur kerja Step Functions dapat menggunakan CTI dari umpan ancaman untuk memperbarui daftar ancaman. GuardDuty Ketika fungsi Lambda selesai mengonversi CTI ke format JSON, itu memicu peristiwa yang memulai alur kerja. EventBridge

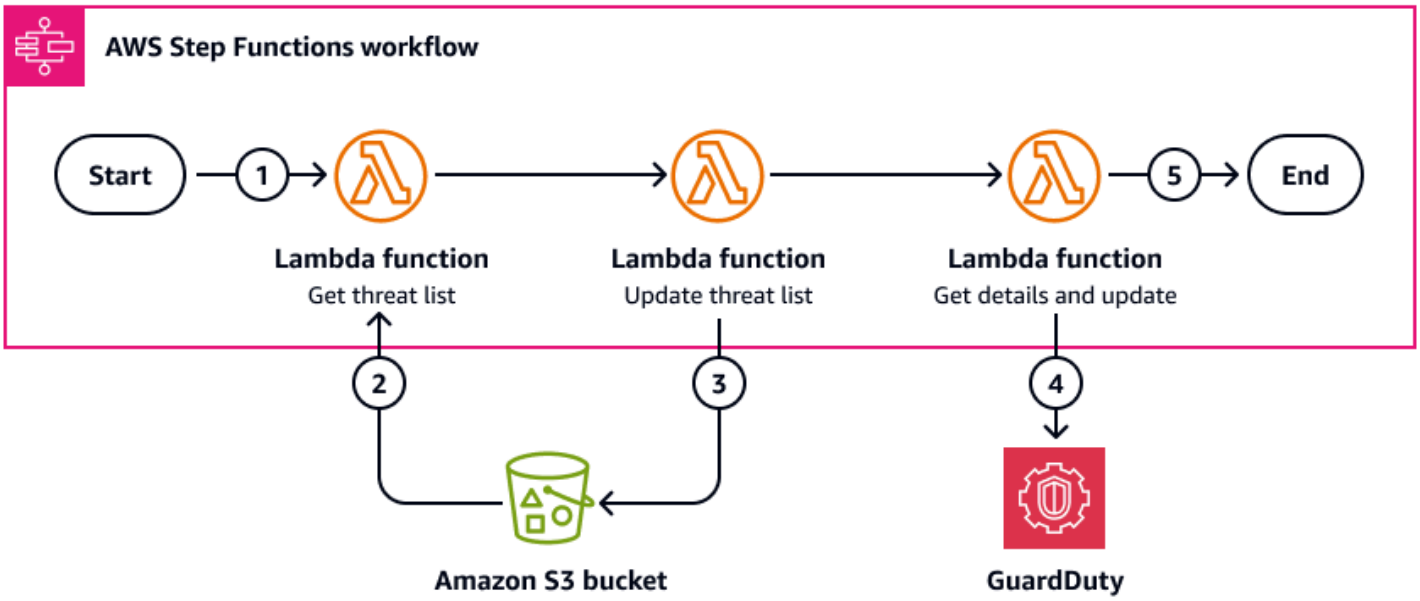


Diagram menunjukkan langkah-langkah berikut:

1. Jika CTI berhubungan dengan catatan alamat IP, maka EventBridge mulailah alur kerja Step Functions.
2. Fungsi Lambda mengambil daftar ancaman, yang disimpan sebagai objek di bucket Amazon Simple Storage Service (Amazon S3).
3. Fungsi Lambda memperbarui daftar ancaman dengan perubahan alamat IP di CTI. Ini menyimpan daftar ancaman sebagai versi baru dari objek di ember Amazon S3 asli. Nama objek tidak berubah.
4. Fungsi Lambda menggunakan panggilan API untuk mengambil ID GuardDuty detektor dan mengancam intel set ID. Ini menggunakan ID ini untuk memperbarui GuardDuty untuk merujuk ke versi baru dari daftar ancaman.

> **Note**
>
> Anda tidak dapat mengambil GuardDuty detektor tertentu dan daftar alamat IP karena mereka diambil sebagai array. Oleh karena itu, kami menyarankan Anda hanya memiliki satu dari masing-masing target Akun AWS. Jika Anda lebih dari itu, maka Anda perlu memastikan bahwa data yang benar diekstraksi dalam fungsi Lambda akhir dalam alur kerja ini.

5. Alur kerja Step Functions berakhir.

Amazon Route 53 Resolver Firewall DNS

Amazon Route 53 Resolver DNS Firewall membantu Anda memfilter dan mengatur lalu lintas DNS keluar untuk virtual private cloud (VPC) Anda. Di DNS Firewall, Anda membuat grup aturan yang memblokir alamat domain yang diidentifikasi oleh umpan CTI. Anda mengonfigurasi alur kerja Step Functions untuk menambahkan dan menghapus domain secara otomatis dari grup aturan ini.

Gambar berikut menunjukkan bagaimana alur kerja Step Functions dapat menggunakan CTI dari umpan ancaman untuk memperbarui daftar domain di Amazon Route 53 Resolver DNS Firewall. Ketika fungsi Lambda selesai mengonversi CTI ke format JSON, itu memicu peristiwa yang memulai alur kerja. EventBridge

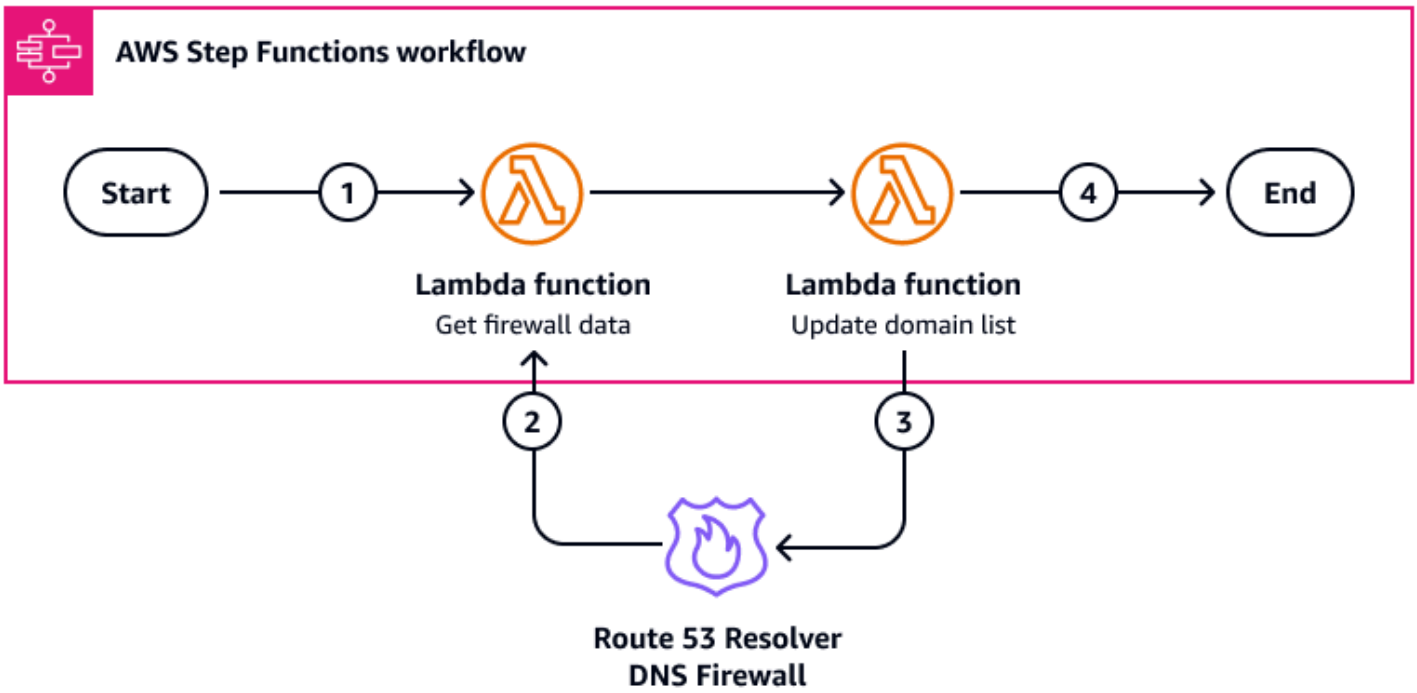


Diagram menunjukkan langkah-langkah berikut:

1. Jika CTI berhubungan dengan catatan domain, maka EventBridge mulailah alur kerja Step Functions.
2. Fungsi Lambda mengambil data daftar domain untuk firewall. Untuk informasi selengkapnya tentang membuat fungsi Lambda ini, lihat get_firewall_domain_list di dokumentasi. AWS SDK untuk Python (Boto3)
3. Fungsi Lambda menggunakan CTI dan data yang diambil untuk memperbarui daftar domain. Untuk informasi selengkapnya tentang membuat fungsi Lambda ini, lihat update_firewall_domains di dokumentasi Boto3. Fungsi Lambda dapat menambah, menghapus, atau mengganti domain.

4. Alur kerja Step Functions berakhir.

Kami merekomendasikan praktik terbaik berikut:

- Kami menyarankan Anda menggunakan Route 53 Resolver DNS Firewall dan. AWS Network Firewall DNS Firewall menyaring lalu lintas DNS, dan Network Firewall menyaring semua lalu lintas lainnya.
- Kami menyarankan Anda mengaktifkan logging untuk DNS Firewall. Anda dapat membuat kontrol detektif yang memantau data log dan memperingatkan Anda jika domain terbatas mencoba mengirim lalu lintas melalui firewall. Untuk informasi selengkapnya, lihat Memantau grup aturan DNS Firewall Resolver Route 53 dengan Amazon. CloudWatch

AWS Network Firewall

AWS Network Firewalladalah firewall jaringan stateful, dikelola, dan layanan deteksi dan pencegahan intrusi untuk VPC di. AWS Cloud Ini menyaring lalu lintas di perimeter VPC Anda, membantu Anda memblokir ancaman. Menggunakan feed intelijen ancaman untuk memperbarui grup aturan Network Firewall secara otomatis dapat membantu melindungi beban kerja dan data cloud organisasi Anda dari pelaku jahat.

Gambar berikut menunjukkan bagaimana alur kerja Step Functions dapat menggunakan CTI dari umpan ancaman untuk memperbarui satu atau beberapa grup aturan di Network Firewall. Ketika fungsi Lambda selesai mengonversi CTI ke format JSON, itu memicu peristiwa yang memulai alur kerja. EventBridge

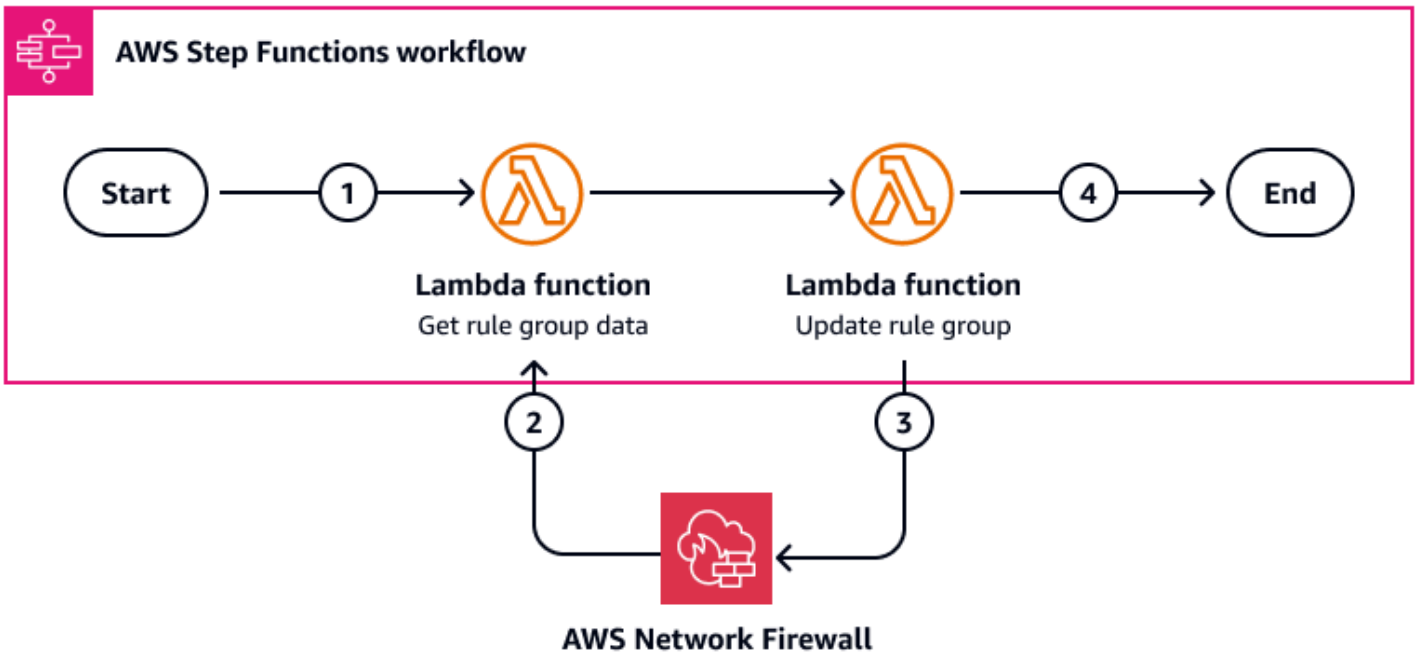


Diagram menunjukkan langkah-langkah berikut:

1. Jika CTI berhubungan dengan alamat IP atau catatan domain, maka EventBridge mulailah alur kerja Step Functions yang secara otomatis memperbarui grup aturan di Network Firewall.
2. Fungsi Lambda mengambil data grup aturan dari Network Firewall.
3. Fungsi Lambda menggunakan CTI untuk memperbarui grup aturan. Ini menambah atau menghapus alamat IP atau domain.
4. Alur kerja Step Functions berakhir.

Kami merekomendasikan praktik terbaik berikut:

- Network Firewall dapat memiliki beberapa grup aturan. Buat grup aturan terpisah untuk domain dan alamat IP.
- Kami menyarankan Anda mengaktifkan logging untuk Network Firewall. Anda dapat membuat kontrol detektif yang memantau data log dan memperingatkan Anda jika domain terbatas atau alamat IP mencoba mengirim lalu lintas melalui firewall. Untuk informasi selengkapnya, lihat Mencatat lalu lintas jaringan dari AWS Network Firewall.
- Kami menyarankan Anda menggunakan Route 53 Resolver DNS Firewall dan. AWS Network Firewall DNS Firewall menyaring lalu lintas DNS, dan Network Firewall menyaring semua lalu lintas lainnya.

Mendapatkan visibilitas dengan mekanisme observabilitas

Kemampuan untuk melihat peristiwa keamanan yang telah terjadi sama pentingnya dengan menetapkan kontrol keamanan yang tepat. Dalam pilar keamanan AWS Well-Architected Framework, praktik terbaik deteksi mencakup Configure service dan application logging dan Capture log, temuan, dan metrik di lokasi standar. Untuk menerapkan praktik terbaik ini, Anda harus mencatat informasi yang membantu Anda mengidentifikasi peristiwa dan kemudian memproses informasi tersebut ke dalam format yang dapat dikonsumsi manusia, idealnya di lokasi terpusat.

Panduan ini merekomendasikan agar Anda menggunakan Amazon Simple Storage Service (Amazon S3) untuk memusatkan data log. Amazon S3 mendukung penyimpanan log untuk keduanya AWS Network Firewall dan Amazon Route 53 Resolver DNS Firewall. Kemudian, Anda menggunakan AWS Security Hub CSPMdan Amazon Security Lake untuk memusatkan GuardDuty temuan Amazon dan temuan keamanan lainnya ke dalam satu lokasi.

Logging lalu lintas jaringan

Bagian Kontrol Keamanan Pencegahan dan Detektif Otomatis dari panduan ini menjelaskan penggunaan AWS Network Firewall dan Amazon Route 53 Resolver DNS Firewall untuk mengotomatiskan respons terhadap intelijen ancaman cyber (CTI). Kami menyarankan Anda mengonfigurasi pencatatan untuk kedua layanan ini. Anda dapat membuat kontrol detektif yang memantau data log dan memperingatkan Anda jika domain terbatas atau alamat IP mencoba mengirim lalu lintas melalui firewall.

Saat mengonfigurasi sumber daya ini, pertimbangkan persyaratan pencatatan individual Anda. Misalnya, logging untuk Network Firewall hanya tersedia untuk lalu lintas yang Anda teruskan ke mesin aturan stateful. Kami menyarankan Anda mengikuti model zero-trust dan meneruskan semua lalu lintas ke mesin aturan stateful. Namun, jika Anda ingin mengurangi biaya, Anda dapat mengecualikan lalu lintas yang dipercaya organisasi Anda.

Baik Network Firewall dan DNS Firewall mendukung pencatatan ke Amazon S3. Untuk informasi selengkapnya tentang menyiapkan pencatatan untuk layanan ini, lihat Mencatat lalu lintas jaringan dari AWS Network Firewall dan Mengonfigurasi logging untuk DNS Firewall. Untuk kedua layanan, Anda dapat mengonfigurasi logging ke bucket Amazon S3 melalui file. Konsol Manajemen AWS

Memusatkan temuan keamanan di AWS

AWS Security Hub CSPMmemberikan pandangan komprehensif tentang keadaan keamanan Anda AWS dan membantu Anda menilai AWS lingkungan Anda terhadap standar industri keamanan

dan praktik terbaik. Security Hub CSPM dapat menghasilkan temuan yang terkait dengan kontrol keamanan Anda. Itu juga dapat menerima temuan dari orang lain Layanan AWS, seperti Amazon GuardDuty. Anda dapat menggunakan Security Hub CSPM untuk memusatkan temuan dan data dari seluruh produk pihak ketiga Anda Akun AWS Layanan AWS, dan didukung. Untuk informasi selengkapnya tentang integrasi, lihat Memahami integrasi di CSPM Security Hub di dokumentasi CSPM Security Hub.

Security Hub CSPM juga menyertakan fitur otomatisasi yang membantu Anda melakukan triase dan memulihkan masalah keamanan. Misalnya, Anda dapat menggunakan aturan otomatisasi untuk memperbarui temuan penting secara otomatis saat pemeriksaan keamanan gagal. Anda juga dapat menggunakan integrasi dengan Amazon EventBridge untuk memulai respons otomatis terhadap temuan tertentu. Untuk informasi selengkapnya, lihat Secara otomatis memodifikasi dan bertindak atas temuan CSPM Security Hub di dokumentasi CSPM Security Hub.

Jika Anda menggunakan Amazon GuardDuty, kami sarankan Anda mengonfigurasi GuardDuty untuk mengirim temuannya ke Security Hub CSPM. Security Hub CSPM kemudian dapat memasukkan temuan-temuan tersebut dalam analisisnya tentang postur keamanan Anda. Untuk informasi selengkapnya, lihat Mengintegrasikan dengan AWS Security Hub CSPM dalam GuardDuty dokumentasi.

Untuk Network Firewall dan Route 53 Resolver DNS Firewall, Anda dapat membuat temuan kustom dari lalu lintas jaringan yang Anda log. Amazon Athena adalah layanan kueri interaktif yang membantu Anda menganalisis data secara langsung di Amazon S3 dengan menggunakan SQL standar. Anda dapat membuat kueri di Athena yang memindai log di Amazon S3 dan mengekstrak data yang relevan. Untuk petunjuk, lihat Memulai di dokumentasi Athena. Kemudian, Anda dapat menggunakan AWS Lambda fungsi untuk mengonversi data log yang relevan menjadi AWS Security Finding Format (ASFF) dan mengirim temuan ke Security Hub CSPM. Berikut ini adalah contoh fungsi Lambda yang mengubah data log dari Network Firewall menjadi temuan CSPM Security Hub:

```
Import { SecurityHubClient, BatchImportFindingsCommand, GetFindingsCommand } from
 "@aws-sdk/client-securityhub";

Export const handler = async(event) => {
   const date = new Date().toISOString();

   const config = {
      Region: REGION
   };

   const input = {
```

```
      Findings: [
         {
            SchemaVersion: '2018-10-08',
            Id: ALERTLOGS3BUCKETID,
            ProductArn: FIREWALLMANAGERARN,
            GeneratorId: 'alertlogs-to-findings',
            AwsAccountId: ACCOUNTID,
            Types: 'Unusual Behaviours/Network Flow/Alert',
            CreatedAt: date,
            UpdatedAt: date,
            Severity: {
               Normalized: 80,
               Product: 8
            },
            Confidence: 100,
            Title: 'Alert Log to Findings',
            Description: 'Network Firewall Alert Log into Finding - add
               top level dynamic detail',
            Resources: [
               {
                  /*these are custom resources. Contain deeper details of your event
 here*/
                  firewallName: 'Example Name',
                  event: 'Example details here'
               }
            ]
         }
      ]
   };

   const client = new SecurityHubClient(config);
   const command = new BatchImportFindingsCommand(input);
   const response = await client.send(command);
   return { statusCode: 200, response };
};
```

Pola yang Anda ikuti untuk mengekstraksi dan mengirim informasi ke Security Hub CSPM tergantung pada kebutuhan bisnis pribadi Anda. Jika Anda membutuhkan data untuk dikirim pada jadwal reguler, Anda dapat menggunakannya EventBridge untuk memulai proses. Jika ingin menerima peringatan saat informasi ditambahkan, Anda dapat menggunakan Amazon Simple Notification Service (Amazon SNS). Ada banyak cara untuk mendekati arsitektur ini, jadi penting untuk merencanakan dengan benar sehingga kebutuhan bisnis Anda tercapai.

Mengintegrasikan AWS data keamanan dengan data perusahaan lainnya

Amazon Security Lake dapat mengotomatiskan pengumpulan data log dan peristiwa terkait keamanan dari layanan terintegrasi Layanan AWS dan pihak ketiga. Ini juga membantu Anda mengelola siklus hidup data dengan pengaturan retensi dan replikasi yang dapat disesuaikan. Security Lake mengubah data yang dicerna ke dalam format Apache Parquet dan skema open-source standar yang disebut Open Cybersecurity Schema Framework (OCSF). Dengan dukungan OCSF, Security Lake menormalkan dan menggabungkan data keamanan dari AWS dan berbagai sumber data keamanan perusahaan. Layanan lain Layanan AWS dan pihak ketiga dapat berlangganan data yang disimpan di Security Lake untuk respons insiden dan analisis data keamanan.

Anda dapat mengonfigurasi Security Lake untuk menerima temuan dari Security Hub CSPM. Untuk mengaktifkan integrasi ini, Anda harus mengaktifkan kedua layanan dan menambahkan Security Hub CSPM sebagai sumber di Security Lake. Setelah Anda menyelesaikan langkah-langkah ini, Security Hub CSPM mulai mengirimkan semua temuan ke Security Lake. Security Lake secara otomatis menormalkan temuan CSPM Security Hub dan mengubahnya menjadi OCSF. Di Security Lake, Anda dapat menambahkan satu atau lebih pelanggan untuk mengkonsumsi temuan CSPM Security Hub. Untuk informasi selengkapnya, lihat Integrasi dengan AWS Security Hub CSPM di dokumentasi Security Lake.

Video berikut, re AWS : Inforce 2024 - Berbagi intelijen ancaman dunia maya AWS, membahas bagaimana Anda dapat menggunakan Security Hub CSPM dan integrasi Security Lake untuk berbagi CTI.

Berbagi CTI dengan komunitas kepercayaan Anda

Komunitas tempat Anda mengirim cyber threat intelligence (CTI) biasanya sama dengan yang Anda terima CTI. Namun, Anda dapat memilih untuk berbagi ke lebih banyak. Misalnya, Anda dapat memilih untuk berbagi dengan pemerintah atau organisasi pengatur yang Anda percayai, seperti pusat keamanan siber nasional atau Pusat Berbagi dan Analisis Informasi (ISAC). Tujuannya adalah untuk menyebarkan dan menerapkan CTI dengan cepat dengan mengumpulkan temuan dari berbagai organisasi. Platform intelijen ancaman Anda mengelola integrasi API untuk dibagikan dengan beberapa feed.

Mengirim CTI ke komunitas kepercayaan terjadi pada saat yang sama dengan menerapkan kontrol pencegahan dan detektif. Anda menggunakan log untuk membantu mengidentifikasi peristiwa keamanan. Kemudian, Anda memusatkan peristiwa dan temuan sehingga Anda dapat dengan cepat

mendapatkan gambaran tentang postur keamanan Anda Akun AWS. Kemudian, tim keamanan Anda, seperti analis cyber Anda, dapat mengidentifikasi informasi apa pun yang mungkin berharga. Karena Anda sudah memiliki temuan AWS Security Hub CSPM, Anda dapat mengubah temuan ini ke dalam format yang digunakan oleh umpan ancaman, seperti JSON atau STIX. Kemudian, Anda mengirim CTI ke penyedia umpan. Platform intelijen ancaman mereka menelan, menganonimkan, dan memvalidasi CTI yang Anda berikan. Kemudian, CTI Anda dibagikan dengan komunitas yang lebih luas.

Gambar berikut menunjukkan bagaimana Anda dapat menggunakan Layanan AWS untuk menghasilkan CTI dan kemudian membagikannya dengan komunitas kepercayaan Anda, termasuk otoritas cyber dan anggota komunitas lainnya.

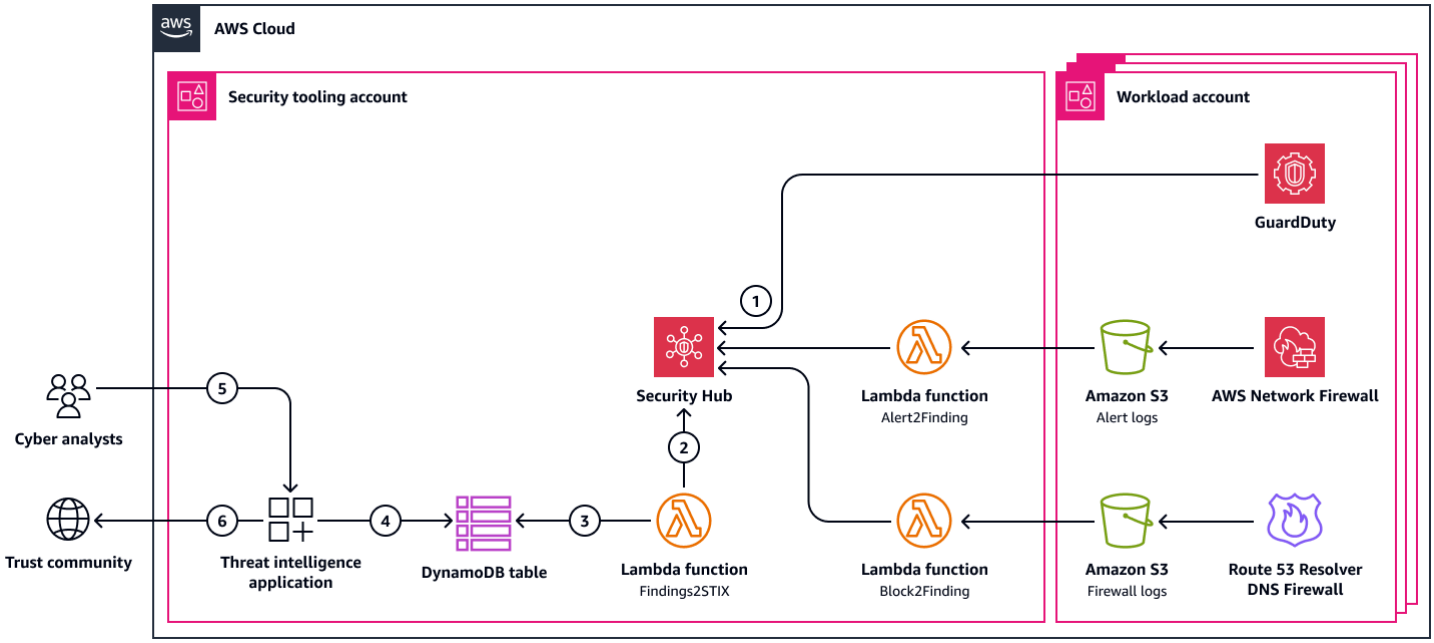


Diagram ini menunjukkan alur kerja berikut:

1. Temuan dibuat di AWS Security Hub CSPM.
2. AWS Lambda Fungsi mengambil temuan dari Security Hub CSPM dan mengubahnya menjadi format yang dapat dibagikan, seperti JSON atau STIX.
3. Fungsi Lambda menyimpan temuan dalam tabel Amazon DynamoDB.
4. Platform intelijen ancaman pihak ketiga, yang berjalan di Amazon Elastic Compute Cloud (Amazon EC2) atau Amazon Elastic Container Service (Amazon ECS), mengambil temuan dari tabel DynamoDB.
5. Seorang analis cyber meninjau CTI di platform intelijen ancaman.

6. Platform intelijen ancaman menerbitkan CTI ke komunitas kepercayaan, yang terdiri dari produsen dan konsumen CTI lainnya.

Langkah dan sumber daya selanjutnya

Pertimbangkan aset, sektor, dan lingkungan ancaman organisasi Anda. Faktor-faktor ini harus menginformasikan komunitas kepercayaan yang Anda pilih untuk bergabung dalam berbagi intelijen ancaman cyber. Banyak otoritas cyber di seluruh dunia menawarkan umpan intelijen ancaman. Pertimbangkan apa yang ditawarkan dan pilih yang terbaik untuk kasus penggunaan organisasi Anda. Gunakan panduan ini sebagai pendekatan modular, dan sesuaikan sesuai untuk organisasi Anda.

Kami menyarankan Anda meninjau sumber daya tambahan berikut. Sumber daya ini dapat membantu Anda membangun atau menyebarkan platform intelijen ancaman di AWS lingkungan Anda dan membantu Anda mengatur berbagi intelijen ancaman cyber.

AWS sumber daya

- AWS Pusat Arsitektur
- AWS RE: inforce 2024 - Berbagi intelijen ancaman dunia maya di (video) AWS
- AWS Summit ANZ 2023: Menskalakan berbagi intelijen ancaman cyber dengan AUS Cyber Security Center (video)

Layanan AWS dokumentasi

- Dokumentasi Amazon DynamoDB
- EventBridge Dokumentasi Amazon
- GuardDuty Dokumentasi Amazon
- Dokumentasi AWS Lambda
- AWS Network Firewall dokumentasi
- Amazon Route 53 Resolver Dokumentasi DNS Firewall
- Dokumentasi AWS Security Hub CSPM
- Dokumentasi Amazon Security Lake
- Dokumentasi Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions dokumentasi

Sumber daya STIX

- STIX 2.1 Contoh
- Indikator untuk URL Berbahaya

Platform intelijen ancaman

- OpenCTI
- MISP

Kontributor

Individu berikut berkontribusi pada panduan ini.

Mengotorisasi

- Jess Modini, Teknolog Senior, AWS
- Alexa Donovan, Arsitek Solusi Asosiasi, AWS
- Steven Ryan, Arsitek Solusi Mitra, AWS
- Byron Pogson, Arsitek Solusi Keamanan, AWS

Meninjau

- Brian Farnhill, Insinyur Pengembangan Perangkat Lunak Senior, AWS
- Marc Luescher, Arsitek Solusi Senior, AWS
- Stefan Mijic, Spesialis Jaminan Keamanan, AWS
- Timothy Woodill, Arsitek Solusi Sektor Publik, AWS

Penulisan teknis

- Lilly AbouHarb, Penulis Teknis Senior, AWS

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Desember 12, 2024

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.