Panduan Implementasi

Respon Keamanan Otomatis di AWS

Respon Keamanan Otomatis di AWS: Panduan Implementasi

Table of Contents

Secara otomatis mengatasi ancaman keamanan dengan respons dan tindakan remediasi yang telah ditentukan sebelumnya di AWS Security Hub

Panduan implementasi ini memberikan gambaran umum tentang Respons Keamanan Otomatis pada solusi AWS, arsitektur referensi dan komponennya, pertimbangan untuk merencanakan penerapan, langkah-langkah konfigurasi untuk menerapkan solusi Automated Security Response on AWS ke Amazon Web Services (AWS) Cloud.

Gunakan tabel navigasi ini untuk menemukan jawaban atas pertanyaan-pertanyaan ini dengan cepat:

Jika kau mau.	Baca.
Ketahui biaya untuk menjalankan solusi ini	Biaya
Memahami pertimbangan keamanan untuk solusi ini	Keamanan
Ketahui cara merencanakan kuota untuk solusi ini	Kuota
Ketahui Wilayah AWS mana yang didukung untuk solusi ini	Wilayah AWS yang Didukung
Lihat atau unduh CloudFormation templat AWS yang disertakan dalam solusi ini untuk secara otomatis menerapkan sumber daya infrastru ktur (“tumpukan”) untuk solusi ini	CloudFormation Templat AWS
Akses kode sumber dan secara opsional gunakan AWS Cloud Development Kit (AWS CDK) untuk menerapkan solusi.	GitHub repositori

Evolusi keamanan yang berkelanjutan membutuhkan langkah-langkah proaktif untuk mengamankan data yang dapat menyulitkan, mahal, dan memakan waktu bagi tim keamanan untuk bereaksi. Solusi Respons Keamanan Otomatis pada AWS membantu Anda bereaksi dengan cepat untuk mengatasi

masalah keamanan dengan memberikan respons dan tindakan remediasi yang telah ditentukan berdasarkan standar kepatuhan industri dan praktik terbaik.

Respons Keamanan Otomatis di AWS adalah Solusi AWS yang bekerja dengan AWS Security Hub untuk meningkatkan keamanan Anda dan membantu menyelaraskan beban kerja Anda dengan praktik terbaik pilar Well-Architected Security (0). SEC1 Solusi ini memudahkan pelanggan AWS Security Hub untuk menyelesaikan temuan keamanan umum dan meningkatkan postur keamanan mereka di AWS.

Anda dapat memilih buku pedoman tertentu untuk diterapkan di akun utama Security Hub. Setiap buku pedoman berisi tindakan kustom yang diperlukan, peran Identity and Access Management (IAM), EventBridge aturan Amazon, dokumen otomatisasi AWS Systems Manager, fungsi AWS Lambda, dan AWS Step Functions yang diperlukan untuk memulai alur kerja remediasi dalam satu akun AWS, atau di beberapa akun. Remediasi berfungsi dari menu Tindakan di AWS Security Hub dan memungkinkan pengguna yang berwenang untuk memulihkan temuan di semua akun yang dikelola AWS Security Hub mereka dengan satu tindakan. Misalnya, Anda dapat menerapkan rekomendasi dari Pusat Keamanan Internet (CIS) AWS Foundations Benchmark, standar kepatuhan untuk mengamankan sumber daya AWS, untuk memastikan kata sandi kedaluwarsa dalam waktu 90 hari dan menerapkan enkripsi log peristiwa yang disimpan di AWS.

> **Note**
>
> Remediasi dimaksudkan untuk situasi yang muncul yang membutuhkan tindakan segera. Solusi ini membuat perubahan untuk memulihkan temuan hanya ketika Anda memulai melalui konsol AWS Security Hub Management, atau ketika remediasi otomatis telah diaktifkan menggunakan EventBridge aturan Amazon untuk kontrol tertentu. Untuk mengembalikan perubahan ini, Anda harus mengembalikan sumber daya secara manual ke keadaan semula. Saat memulihkan sumber daya AWS yang digunakan sebagai bagian dari CloudFormation tumpukan, ketahuilah bahwa ini dapat menyebabkan penyimpangan. Jika memungkinkan, memulihkan sumber daya tumpukan dengan memodifikasi kode yang mendefinisikan sumber daya tumpukan dan memperbarui tumpukan. Untuk informasi lebih lanjut, lihat Apa itu drift? di Panduan CloudFormation Pengguna AWS.

Respons Keamanan Otomatis di AWS mencakup remediasi buku pedoman untuk standar keamanan yang ditetapkan sebagai bagian dari hal berikut:

- Pusat Keamanan Internet (CIS) AWS Foundations Benchmark v1.2.0

- Tolok Ukur Yayasan CIS AWS v1.4.0
- Tolok Ukur Yayasan CIS AWS v3.0.0
- Praktik Terbaik Keamanan Dasar AWS (FSBP) v.1.0.0
- Standar Keamanan Data Industri Kartu Pembayaran (PCI-DSS) v3.2.1
- Institut Nasional Standar dan Teknologi (NIST) SP 800-53 Rev. 5

Solusi ini juga mencakup buku pedoman Kontrol Keamanan (SC) untuk fitur temuan kontrol konsolidasi AWS Security Hub. Untuk informasi lebih lanjut, lihat Playbooks.

Panduan implementasi ini membahas pertimbangan arsitektur dan langkah-langkah konfigurasi untuk menerapkan Respons Keamanan Otomatis pada solusi AWS di AWS Cloud. Ini mencakup tautan ke CloudFormation templat AWS yang meluncurkan, mengonfigurasi, dan menjalankan komputasi AWS, jaringan, penyimpanan, dan layanan lain yang diperlukan untuk menerapkan solusi ini di AWS, menggunakan praktik terbaik AWS untuk keamanan dan ketersediaan.

Panduan ini ditujukan untuk arsitek infrastruktur TI, administrator, dan DevOps profesional yang memiliki pengalaman praktis dalam merancang di AWS Cloud.

Fitur dan manfaat

Respons Keamanan Otomatis di AWS menyediakan fitur-fitur berikut:

Secara otomatis memulihkan temuan untuk kontrol tertentu

Aktifkan EventBridge aturan Amazon untuk kontrol untuk memulihkan temuan secara otomatis untuk kontrol tersebut segera setelah muncul di AWS Security Hub.

Kelola remediasi di beberapa akun dan Wilayah dari satu lokasi

Dari akun administrator AWS Security Hub yang dikonfigurasi sebagai tujuan agregasi untuk akun dan Wilayah organisasi Anda, lakukan remediasi untuk temuan di akun dan Wilayah mana pun tempat solusi diterapkan.

Dapatkan pemberitahuan tentang tindakan dan hasil remediasi

Berlangganan topik Amazon SNS yang digunakan oleh solusi untuk diberi tahu saat remediasi dimulai dan apakah remediasi berhasil atau tidak.

Integrasikan dengan sistem tiket seperti Jira atau ServiceNow

Untuk membantu organisasi Anda bereaksi terhadap remediasi (misalnya, memperbarui kode infrastruktur Anda), solusi ini dapat mendorong tiket ke sistem tiket eksternal Anda.

Gunakan AWSConfig Remediasi di partisi GovCloud dan Tiongkok

Beberapa remediasi yang termasuk dalam solusi adalah paket ulang dokumen AWSConfig Remediasi milik AWS yang tersedia di partisi komersial tetapi tidak di atau China. GovCloud Terapkan solusi ini untuk memanfaatkan dokumen-dokumen ini di partisi tersebut.

Perluas solusi dengan remediasi khusus dan implementasi Playbook

Solusinya dirancang agar dapat diperluas dan dapat disesuaikan. Untuk menentukan implementasi remediasi alternatif, terapkan dokumen otomatisasi AWS Systems Manager yang disesuaikan dan Peran AWS IAM. Untuk mendukung seluruh rangkaian kontrol baru yang tidak diimplementasikan oleh solusi, gunakan Playbook kustom.

Kasus penggunaan

Menegakkan kepatuhan terhadap standar di seluruh akun dan Wilayah organisasi Anda

Menerapkan Playbook untuk standar (misalnya, AWS Foundational Security Best Practices) agar dapat menggunakan remediasi yang disediakan. Memulai remediasi sumber daya secara otomatis atau manual di akun dan Wilayah mana pun di mana solusi tersebut digunakan untuk memperbaiki sumber daya yang tidak sesuai.

Menerapkan remediasi khusus atau Playbook untuk memenuhi kebutuhan kepatuhan organisasi Anda

Gunakan komponen Orchestrator yang disediakan sebagai kerangka kerja. Bangun remediasi khusus untuk menangani out-of-compliance sumber daya sesuai dengan kebutuhan spesifik organisasi Anda.

Konsep dan definisi

Bagian ini menjelaskan konsep-konsep kunci dan mendefinisikan terminologi khusus untuk solusi ini:

remediasi, runbook remediasi

Implementasi serangkaian langkah yang menyelesaikan temuan. Misalnya, remediasi untuk kontrol Kontrol Keamanan (SC) Lambda.1 “Kebijakan fungsi Lambda harus melarang akses publik” akan

mengubah kebijakan Fungsi AWS Lambda yang relevan untuk menghapus pernyataan yang memungkinkan akses publik.

buku runbook kontrol

Salah satu set dokumen otomatisasi AWS Systems Manager (SSM) yang digunakan Orchestrator untuk merutekan remediasi yang dimulai untuk kontrol tertentu ke runbook remediasi yang benar. Misalnya, remediasi untuk SC Lambda.1 dan AWS Foundational Security Best Practices (FSBP) Lambda.1 diimplementasikan dengan runbook remediasi yang sama. Orchestrator memanggil runbook kontrol untuk setiap kontrol, yang masing-masing diberi nama ASR-AFSBP_Lambda.1 dan ASR-SC_2.0.0_lambda.1. Setiap runbook kontrol memanggil runbook remediasi yang sama, yang dalam hal ini adalah ASR-. RemoveLambdaPublicAccess

orkestrator

Step Functions yang digunakan oleh solusi yang mengambil input objek pencarian dari AWS Security Hub dan memanggil runbook kontrol yang benar di akun target dan Wilayah. Orchestrator juga memberi tahu solusi SNS Topic ketika remediasi dimulai dan ketika remediasi berhasil atau gagal.

standar

Sekelompok kontrol yang didefinisikan oleh organisasi sebagai bagian dari kerangka kepatuhan. Misalnya, salah satu standar yang didukung oleh AWS Security Hub dan solusi ini adalah AWS FSBP.

kontrol

Deskripsi properti yang harus atau tidak harus dimiliki sumber daya agar sesuai. Misalnya, kontrol AWS FSBP Lambda.1 menyatakan bahwa AWS Lambda Functions harus melarang akses publik. Fungsi yang memungkinkan akses publik akan gagal kontrol ini.

temuan kontrol konsolidasi, kontrol keamanan, tampilan kontrol keamanan

Fitur AWS Security Hub yang, ketika diaktifkan, menampilkan temuan dengan kontrol konsolidasinya, IDs bukan IDs yang sesuai dengan standar tertentu. Misalnya, kontrol AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2, dan PCI-DSS v3.2.1 S3.1 semua peta ke kontrol konsolidasi (SC) S3.2 “Bucket S3 harus melarang akses baca publik.” Saat fitur ini diaktifkan, runbook SC digunakan.

Untuk referensi umum istilah AWS, lihat Glosarium AWS.

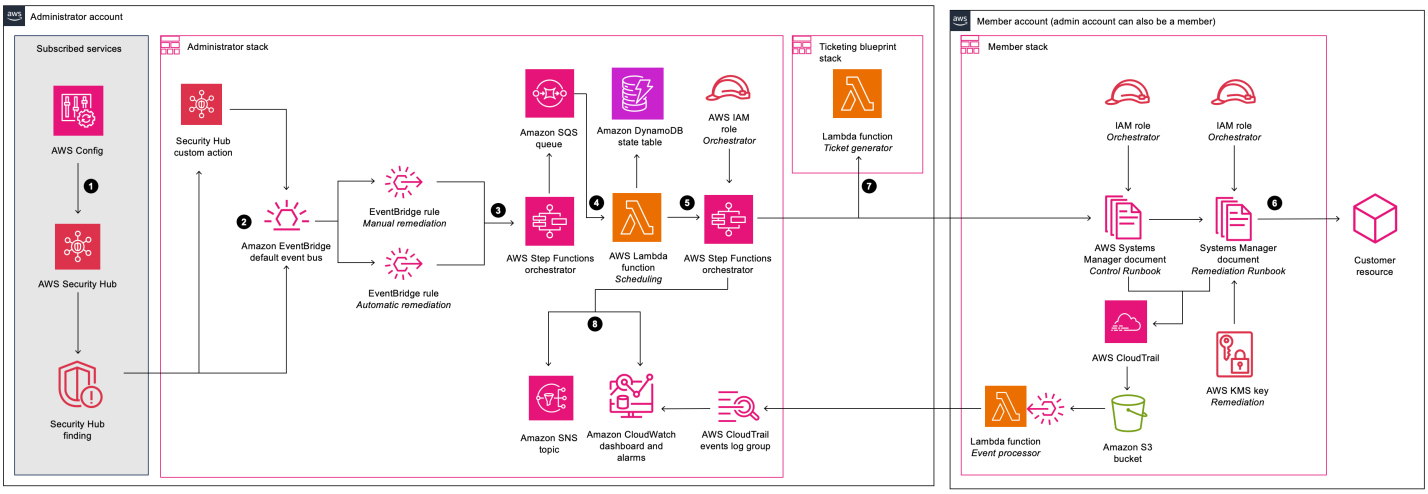
Gambaran umum arsitektur

Bagian ini menyediakan diagram arsitektur implementasi referensi untuk komponen yang digunakan dengan solusi ini.

Diagram arsitektur

Menerapkan solusi ini dengan parameter default membangun lingkungan berikut di AWS Cloud.

Respon Keamanan Otomatis pada arsitektur AWS



> **Note**
>
> CloudFormation Sumber daya AWS dibuat dari konstruksi AWS Cloud Development Kit (AWS CDK).

Alur proses tingkat tinggi untuk komponen solusi yang digunakan dengan CloudFormation template AWS adalah sebagai berikut:

1. Deteksi: AWS Security Hub memberi pelanggan pandangan komprehensif tentang status keamanan AWS mereka. Ini membantu mereka untuk mengukur lingkungan mereka terhadap standar industri keamanan dan praktik terbaik. Ini bekerja dengan mengumpulkan peristiwa dan data dari layanan AWS lainnya, seperti AWS Config, Amazon Guard Duty, dan AWS Firewall Manager. Peristiwa dan data ini dianalisis berdasarkan standar keamanan, seperti CIS AWS

Foundations Benchmark. Pengecualian ditegaskan sebagai temuan di konsol AWS Security Hub. Temuan baru dikirim sebagai EventBridge acara Amazon.

2. Memulai: Anda dapat memulai peristiwa terhadap temuan menggunakan tindakan khusus, yang menghasilkan peristiwa. EventBridge Tindakan dan EventBridge aturan khusus AWS Security Hub memulai Respons Keamanan Otomatis di playbook AWS untuk mengatasi temuan. Solusinya menyebarkan:

   a. Satu EventBridge aturan untuk mencocokkan acara tindakan kustom

   b. Satu aturan EventBridge acara untuk setiap kontrol yang didukung (dinonaktifkan secara default) agar sesuai dengan peristiwa pencarian real-time

   Anda dapat menggunakan menu Tindakan kustom di konsol Security Hub untuk memulai remediasi otomatis. Setelah pengujian yang cermat di lingkungan non-produksi, Anda juga dapat mengaktifkan remediasi otomatis. Anda dapat mengaktifkan otomatisasi untuk remediasi individual — Anda tidak perlu mengaktifkan inisiasi otomatis pada semua remediasi.

3. Pra-remediasi: Di akun admin, AWS Step Functions memproses peristiwa remediasi dan menyiapkannya untuk dijadwalkan.

4. Jadwal: Solusinya memanggil fungsi AWS Lambda penjadwalan untuk menempatkan peristiwa remediasi di tabel status Amazon DynamoDB.

5. Orchestrate: Di akun admin, Step Functions menggunakan peran AWS Identity and Access Management (IAM) lintas akun. Step Functions memanggil remediasi di akun anggota yang berisi sumber daya yang menghasilkan temuan keamanan.

6. Remediasi: Dokumen AWS Systems Manager Automation di akun anggota melakukan tindakan yang diperlukan untuk memulihkan temuan pada sumber daya target, seperti menonaktifkan akses publik Lambda.

   Secara opsional, Anda dapat mengaktifkan fitur Action Log di tumpukan anggota dengan parameter EnableCloudTrailForASRActionLog. Fitur ini menangkap tindakan yang diambil oleh solusi di akun Anggota Anda dan menampilkannya di CloudWatch dasbor Amazon solusi.

7. (Opsional) Buat tiket: Jika Anda menggunakan TicketGenFunctionNameparameter untuk mengaktifkan tiket di tumpukan Admin, solusinya akan memanggil fungsi Lambda generator tiket yang disediakan. Fungsi Lambda ini membuat tiket di layanan tiket Anda setelah remediasi berhasil dijalankan di akun Anggota. Kami menyediakan tumpukan untuk integrasi dengan Jira dan. ServiceNow

8. Beri tahu dan log: Buku pedoman mencatat hasilnya ke grup CloudWatch log, mengirimkan pemberitahuan ke topik Amazon Simple Notification Service (Amazon SNS), dan memperbarui temuan Security Hub. Solusinya mempertahankan jejak audit tindakan dalam catatan temuan.

Pertimbangan desain AWS Well-Architected

Solusi ini dirancang dengan praktik terbaik dari AWS Well-Architected Framework yang membantu pelanggan merancang dan mengoperasikan beban kerja yang andal, aman, efisien, dan hemat biaya di cloud. Bagian ini menjelaskan bagaimana prinsip-prinsip desain dan praktik terbaik Kerangka Well-Architected diterapkan saat membangun solusi ini.

Keunggulan operasional

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar keunggulan operasional.

- Sumber daya didefinisikan sebagai penggunaan CloudFormation IAc.
- Remediasi dilaksanakan dengan karakteristik sebagai berikut, jika memungkinkan:
  - Idempotensi
  - Penanganan dan pelaporan kesalahan
  - Pencatatan log
  - Memulihkan sumber daya ke keadaan yang diketahui pada kegagalan

Keamanan

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik pilar keamanan.

- IAM digunakan untuk otentikasi dan otorisasi.
- Izin peran dicakup sesempit mungkin, meskipun dalam banyak kasus solusi ini memerlukan izin wildcard untuk dapat bertindak atas sumber daya apa pun.

Keandalan

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar keandalan.

- Security Hub terus membuat temuan jika penyebab yang mendasari temuan tersebut tidak diselesaikan dengan remediasi.
- Layanan tanpa server memungkinkan solusi untuk skala sesuai kebutuhan.

Efisiensi kinerja

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar efisiensi kinerja.

- Solusi ini dirancang untuk menjadi platform bagi Anda untuk memperluas tanpa harus menerapkan orkestrasi dan izin sendiri.

Optimalisasi biaya

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar pengoptimalan biaya.

- Layanan tanpa server memungkinkan Anda membayar hanya untuk apa yang Anda gunakan.
- Gunakan tingkat gratis untuk otomatisasi SSM di setiap akun

Keberlanjutan

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik pilar keberlanjutan.

- Layanan tanpa server memungkinkan Anda untuk meningkatkan atau menurunkan skala sesuai kebutuhan.

Detail arsitektur

Bagian ini menjelaskan komponen dan layanan AWS yang membentuk solusi ini dan detail arsitektur tentang cara komponen ini bekerja sama.

Integrasi AWS Security Hub

Menerapkan `automated-security-response-admin` tumpukan menciptakan integrasi dengan fitur tindakan khusus AWS Security Hub. Saat pengguna konsol AWS Security Hub memilih Temuan untuk perbaikan, solusi akan merutekan catatan temuan untuk remediasi menggunakan AWS Step Functions.

Izin lintas akun dan runbook AWS Systems Manager harus diterapkan ke semua akun AWS Security Hub (admin dan anggota) menggunakan templat dan templat. `automated-security-response-member.template` `automated-security-response-member-roles.template` CloudFormation Untuk informasi lebih lanjut, lihat Playbooks. Template ini memungkinkan remediasi otomatis di akun target.

Pengguna dapat secara otomatis memulai remediasi otomatis berdasarkan per-remediasi menggunakan aturan peristiwa Amazon. CloudWatch Opsi ini mengaktifkan remediasi temuan yang sepenuhnya otomatis segera setelah dilaporkan ke AWS Security Hub. Secara default, inisiasi otomatis dimatikan. Opsi ini dapat diubah kapan saja selama atau setelah penginstalan buku pedoman dengan mengaktifkan aturan CloudWatch Acara di akun admin AWS Security Hub.

Remediasi lintas akun

Respons Keamanan Otomatis di AWS menggunakan peran lintas akun untuk bekerja di seluruh akun primer dan sekunder menggunakan peran lintas akun. Peran ini diterapkan ke akun anggota selama instalasi solusi. Setiap remediasi diberi peran individu. Proses remediasi di akun utama diberikan izin untuk mengambil peran remediasi dalam akun yang membutuhkan remediasi. Remediasi dilakukan oleh runbook AWS Systems Manager yang berjalan di akun yang memerlukan remediasi.

Buku pedoman

Satu set remediasi dikelompokkan ke dalam paket yang disebut playbook. Playbook diinstal, diperbarui, dan dihapus menggunakan templat solusi ini. Untuk informasi tentang remediasi yang

didukung di setiap buku pedoman, lihat Panduan Pengembang → Playbooks. Solusi ini saat ini mendukung pedoman berikut:

- Security Control, buku pedoman yang selaras dengan fitur temuan kontrol Konsolidasi AWS Security Hub, diterbitkan 23 Februari 2023.

> **Important**
>
> Ketika temuan kontrol Konsolidasi diaktifkan di Security Hub, ini adalah satu-satunya buku pedoman yang harus diaktifkan dalam solusi.

- Tolok ukur Yayasan Amazon Web Services Center for Internet Security (CIS), versi 1.2.0, diterbitkan 18 Mei 2018.
- Tolok ukur Yayasan Amazon Web Services Center for Internet Security (CIS), versi 1.4.0, diterbitkan 9 November 2022.
- Tolok ukur Yayasan Amazon Web Services Center for Internet Security (CIS), versi 3.0.0, diterbitkan 13 Mei 2024.
- AWS Foundational Security Best Practices (FSBP) versi 1.0.0, diterbitkan Maret 2021.
- Standar Keamanan Data Industri Kartu Pembayaran (PCI-DSS) versi 3.2.1, diterbitkan Mei 2018.
- Institut Standar dan Teknologi Nasional (NIST) versi 5.0.0, diterbitkan November 2023.

Penebangan terpusat

Respons Keamanan Otomatis pada log AWS ke satu grup CloudWatch Log, SO0111-ASR. Log ini berisi pencatatan terperinci dari solusi untuk pemecahan masalah dan pengelolaan solusi.

Notifikasi

Solusi ini menggunakan topik Amazon Simple Notification Service (Amazon SNS) untuk mempublikasikan hasil remediasi. Anda dapat menggunakan langganan untuk topik ini untuk memperluas kemampuan solusi. Misalnya, Anda dapat mengirim pemberitahuan email dan memperbarui tiket masalah.

- SO0111-ASR_Topic - Digunakan untuk mengirim pesan informasi dan kesalahan umum yang terkait dengan remediasi yang dieksekusi.

- SO0111-ASR_Alarm_topic — Digunakan untuk memberi tahu ketika salah satu alarm solusi dipicu, menunjukkan bahwa solusi tidak berfungsi seperti yang diharapkan.

Layanan AWS dalam solusi ini

Solusinya menggunakan layanan berikut. Layanan inti diperlukan untuk menggunakan solusi, dan layanan pendukung menghubungkan layanan inti.

AWS service	Deskripsi
Amazon EventBridge	Inti. Menyebarkan peristiwa yang akan memulai fungsi langkah orchestator saat temuan sedang diperbaiki.
AWS IAM	Inti. Menyebarkan banyak peran untuk memungkinkan remediasi pada sumber daya yang berbeda.
AWS Lambda	Inti. Menerapkan beberapa fungsi lambda yang akan digunakan oleh orchestator fungsi langkah untuk memperbaiki masalah.
AWS Security Hub	Inti. Memberikan pelanggan pandangan komprehensif tentang status keamanan AWS mereka.
AWS Step Functions	Inti. Menerapkan orkestrator yang akan memanggil dokumen remediasi dengan panggilan AWS Systems Manager API.
AWS Systems Manager	Inti. Menyebarkan Dokumen Manajer Sistem (tautan ke dokumen) yang berisi logika remediasi yang akan dijalankan.
AWS CloudTrail	Mendukung. Merekam perubahan yang dibuat solusi untuk sumber daya AWS Anda dan menampilkannya di CloudWatch dasbor.

AWS service	Deskripsi
Amazon CloudWatch	Mendukung. Menyebarkan grup log yang akan digunakan oleh pedoman berbeda untuk mencatat hasil. Mengumpulkan metrik untuk ditampilkan di dasbor khusus dengan alarm.
AWS DynamoDB	Mendukung. Menyimpan remediasi terakhir yang dijalankan di setiap akun dan Wilayah untuk mengoptimalkan penjadwalan remediasi.
Layanan Pemberitahuan Sederhana Amazon	Mendukung. Menyebarkan topik SNS yang menerima pemberitahuan setelah remediasi selesai.
AWS SQS	Mendukung. Membantu dengan menjadwalkan remediasi sehingga solusi dapat menjalankan remediasi secara paralel.
AWS Key Management Service	Mendukung. Digunakan untuk mengenkripsi data untuk remediasi.
AWS Config	Mendukung. Merekam semua sumber daya untuk digunakan dengan AWS Security Hub.

Rencanakan penyebaran Anda

Bagian ini menjelaskan biaya, keamanan jaringan, Wilayah AWS yang didukung, kuota, dan pertimbangan lainnya sebelum menerapkan solusi.

Biaya

Anda bertanggung jawab atas biaya layanan AWS yang digunakan untuk menjalankan solusi ini.

Pada revisi ini, perkiraan biaya bulanan adalah:

- Penyebaran kecil (10 akun, 1 wilayah - AS East/N. Virginia): Approximately $21.17 for 300 remediations/month
- Penyebaran sedang (100 akun, 1 wilayah - AS East/N. Virginia): Approximately $134.86 for 3,000 remediations/month
- Penyebaran besar (1.000 akun, 10 wilayah): Sekitar $10.271,70 untuk 30.000 remediasi/bulan

> **Important**
>
> Harga dapat berubah sewaktu-waktu. Untuk detail selengkapnya, lihat halaman harga untuk setiap layanan AWS yang digunakan dalam solusi ini.

> **Note**
>
> Banyak Layanan AWS menyertakan Tingkat Gratis - jumlah dasar layanan yang dapat digunakan pelanggan tanpa biaya. Biaya aktual mungkin lebih atau kurang dari contoh harga yang diberikan.

Sebaiknya buat anggaran melalui AWS Cost Explorer untuk membantu mengelola biaya. Harga dapat berubah sewaktu-waktu. Untuk detail selengkapnya, lihat halaman web harga untuk setiap layanan AWS yang digunakan dalam solusi ini.

Tabel biaya sampel

Total biaya untuk menjalankan solusi ini tergantung pada faktor-faktor berikut:

- Jumlah akun anggota AWS Security Hub
- Jumlah remediasi aktif yang dipanggil secara otomatis
- Frekuensi remediasi

Solusi ini menggunakan komponen AWS berikut, yang dikenakan biaya berdasarkan konfigurasi Anda. Contoh harga disediakan untuk organisasi kecil, menengah, dan besar.

Layanan	Tingkat Gratis	Harga [USD]
AWS Systems Manager Automation - Hitungan Langkah	100.000 langkah per akun per bulan	Di luar tingkat gratis, setiap langkah dasar dikenakan biaya $0,002 per langkah. Untuk otomatisasi multi-akun, semua langkah termasuk yang dijalankan di akun anak hanya dihitung di akun asal.
AWS Systems Manager Automation - Durasi Langkah	5.000 detik per bulan	Di luar tingkat gratis, setiap langkah tindakan AWS: ExecuteScript dikenakan biaya sebesar $0,00003 untuk setiap detik setelah tingkat gratis 5.000 detik per bulan.
AWS Systems Manager Automation - Penyimpanan	Tidak ada tingkat gratis	$0,046 per GB per bulan
AWS Systems Manager Automation - Transfer Data	Tidak ada tingkat gratis	$0.900 per GB yang ditransfer (untuk cross-account atau) out-of-Region
AWS Security Hub - Pemeriksaan Keamanan	Tidak ada tingkat gratis	100.000 pertama checks/account/Region/month berharga $0,0010 per cek

Layanan	Tingkat Gratis	Harga [USD]
		Berikutnya 400.000 checks/account/Region/month biaya $0.0008 per cek Lebih dari 500.000 checks/account/Region/month biaya $0.0005 per cek
AWS Security Hub - Menemukan Acara Penyerapan	10.000 yang pertama events/account/Region/month adalah gratis. Menemukan peristiwa konsumsi yang terkait dengan pemeriksaan keamanan Security Hub.	Lebih dari 10.000 events/account/Region/month biaya $0,00003 per acara
Amazon CloudWatch - Metrik	Metrik Pemantauan Dasar (pada frekuensi 5 menit) 10 Metrik Pemantauan Terperinci (pada frekuensi 1 menit) 1 Juta permintaan API (tidak berlaku untuk dan) GetMetricData GetMetricWidgetImage	10.000 metrik pertama berharga $0,30 metrik/bulan Berikutnya 240.000 metrik biaya $0,10 metrik/bulan Berikutnya 750.000 metrik biaya $0,05 metrik/bulan Lebih dari 1.000.000 metrik berharga $0,02 metrik/bulan Panggilan API berharga $0,01 per 1.000 permintaan
Amazon CloudWatch - Dasbor	3 Dasbor hingga 50 metrik per bulan	$3.00 per dasbor per bulan

Layanan	Tingkat Gratis	Harga [USD]
Amazon CloudWatch - Alarm	10 Metrik alarm (tidak berlaku untuk alarm resolusi tinggi)	Resolusi Standar (60 detik) berharga $0,10 per alarmmetr ic Resolusi Tinggi (10 detik) berharga $0,30 per metrik alarm Deteksi Anomali Resolusi Standar berharga $0,30 per alarm Deteksi Anomali Resolusi Tinggi berharga $0,90 per alarm Biaya komposit $0,50 per alarm
Amazon CloudWatch - Koleksi Log	Data 5GB (konsumsi, penyimpanan arsip, dan data yang dipindai oleh kueri Wawasan Log)	$0,50 per GB
Amazon CloudWatch - Penyimpanan Log	Data 5GB (konsumsi, penyimpanan arsip, dan data yang dipindai oleh kueri Wawasan Log)	$0,005 per GB data yang dipindai
Amazon CloudWatch - Acara	Semua acara kecuali acara khusus disertakan	$1,00 per juta acara untuk acara khusus $1,00 per juta acara untuk acara lintas akun
AWS Lambda - Permintaan	1M permintaan gratis per bulan	$0,20 per 1 juta permintaan

Layanan	Tingkat Gratis	Harga [USD]
AWS Lambda - Durasi	400.000 GB-detik waktu komputasi per bulan	$0.0000166667 untuk setiap GB-detik. Harga untuk Durasi tergantung pada jumlah memori yang Anda alokasikan ke fungsi Anda. Anda dapat mengalokasikan sejumlah memori ke fungsi Anda antara 128MB dan 10.240 MB, dengan peningkatan 1MB.
AWS Step Functions - Transisi Status	4.000 transisi status gratis per bulan	$0,025 per 1.000 transisi negara sesudahnya
Amazon EventBridge	Semua peristiwa perubahan status yang diterbitkan oleh layanan AWS gratis	Acara khusus menelan biaya $1.00/juta acara khusus yang diterbitkan Acara pihak ketiga (SaaS) menelan biaya $1,00/juta acara yang diterbitkan Acara lintas akun menelan biaya $1,00/juta acara lintas akun yang dikirim
Amazon SNS	1 juta permintaan Amazon SNS pertama per bulan gratis	$0,50 per 1 juta permintaan sesudahnya
Amazon SQS	1 juta permintaan Amazon SQS pertama per bulan gratis	$0,40 per 1 juta hingga 100 miliar permintaan sesudahnya
Amazon DynamoDB	Penyimpanan 25GB pertama gratis	$2,00 per 1 juta konsisten membaca dan menulis sesudahnya

Layanan	Tingkat Gratis	Harga [USD]
Harga AWS Key Management Service	20.000 permintaan/bulan	$1,00 per 1 KMS kunci. Untuk kunci KMS yang Anda putar secara otomatis atau sesuai permintaan, rotasi kunci pertama dan kedua menambahkan biaya $1/bulan (prorata per jam).

Contoh harga (bulanan)

Contoh 1:300 remediasi per bulan

- 10 akun, 1 Wilayah
- 30 remediasi per account/Region/month
- Total biaya $21,17 per bulan

Layanan	Asumsi	Biaya bulanan [USD]
AWS Systems Manager Automation	Langkah-langkah: ~ 4 langkah* 300 remediasi * $0,002 = $2,40 Durasi: 10-an * 300 remediasi * $0,00003 = $0,09	$2,49
AWS Security Hub	Tidak ada layanan yang dapat ditagih yang digunakan	$0
CloudWatch Log Amazon	300 remediasi * $0,000002 = $0,0006 $0,0006 * 0,03 = $0,000018	< $0,01
AWS Lambda - Permintaan	300 remediasi * 6 permintaan = 1.800 permintaan	$0,20

Layanan	Asumsi	Biaya bulanan [USD]
	$0,20 * 1.000.000 permintaan = $0,20	
AWS Lambda - Durasi	256M: 1.875 GB detik * 300 remediasi * $0.0000167 = $0.009375	< $0,01
AWS Step Functions	17 transisi negara* 300 remediasi = 5.100 $0,025 * (5.100/1.000) transisi status = $0,15	$0,15
EventBridge Aturan Amazon	Tidak ada biaya untuk aturan	$0
Layanan Manajemen Utama AWS	1 kunci * 10 akun * 1 Wilayah * $1 = $10	$10.00
Amazon DynamoDB	$2,00 * 1.000.000 membaca dan menulis = $2,00	$2,00
Amazon SQS	$0,40 * 1.000.000 permintaan = $0,40	$0,40
Amazon SNS	$0,50 * 1.000.000 pemberita huan = $0,50	$0,50
Amazon CloudWatch - Metrik	$0,30 * 7 metrik khusus = $2,10 $0,01 * (300 * 3/1.000) masukkan panggilan API metrik = $0,01	$2.11
Amazon CloudWatch - Dasbor	$3,00 * 1 dasbor = $3,00	$3,00
Amazon CloudWatch - Alarm	$0,10 * 3 alarm = $0,30	$0,30

Layanan	Asumsi	Biaya bulanan [USD]
Jumlah		$21.17

Contoh 2:3.000 remediasi per bulan

- 100 akun, 1 Wilayah
- 30 remediasi per account/Region/month
- Total biaya $134,86 per bulan

Layanan	Asumsi	Biaya bulanan [USD]
AWS Systems Manager Automation	Langkah: ~ 4 langkah* 3.000 remediasi * $0,002 = $24,00 Durasi: 10-an * 3.000 remediasi * $0,00003 = $0,90	$24,90
AWS Security Hub	Tidak ada layanan yang dapat ditagih yang digunakan	$0
CloudWatch Log Amazon	3.000 remediasi * $0,000002 = $0,006 $0,006 * 0,03 = $0,00018	< $0,01
AWS Lambda - Permintaan	3.000 remediasi * 6 permintaan = 18.000 permintaan $0,20 * 1.000.000 permintaan = $0,20	$0,20
AWS Lambda - Durasi	256M: 1.875 GB detik* 3.000 remediasi * $0.000167 = $0.09375	$0,09

Layanan	Asumsi	Biaya bulanan [USD]
AWS Step Functions	17 transisi negara* 3.000 remediasi = 51.000 $0,025 * (51.000/1.000) transisi negara = $1,275	$1.28
EventBridge Aturan Amazon	Tidak ada biaya untuk aturan	$0
Layanan Manajemen Utama AWS	1 kunci * 100 akun * 1 Wilayah * $1 = $100	$100
Amazon DynamoDB	$2,00 * 1.000.000 membaca dan menulis = $2,00	$2,00
Amazon SQS	$0,40 * 1.000.000 permintaan = $0,40	$0,40
Amazon SNS	$0,50 * 1.000.000 pemberita huan = $0,50	$0,50
Amazon CloudWatch - Metrik	$0,30 * 7 metrik khusus = $2,10 $0,01 * (3000 * 3/1.000) masukkan panggilan API metrik = $0,09	$2,19
Amazon CloudWatch - Dasbor	$3,00 * 1 dasbor = $3,00	$3,00
Amazon CloudWatch - Alarm	$0,10 * 3 alarm = $0,30	$0,30
Jumlah		$134,86

Contoh 3:30.000 remediasi per bulan

- 1.000 akun, 10 Wilayah
- 30 remediasi per account/Region/month

- Total biaya $1.271.70 per bulan

Layanan	Asumsi	Biaya bulanan [USD]
AWS Systems Manager Automation	Langkah-langkah: ~ 4 langkah* 30,000 remediasi * $0.002 = $240.00 Durasi: 10-an * 30.000 remediasi * $0,00003 = $9,00	$249.00
AWS Security Hub	Tidak ada layanan yang dapat ditagih yang digunakan	$0
CloudWatch Log Amazon	30.000 remediasi * $0,000002 = $0,06 $0,06 * 0,03 = $0,0018	< $0,01
AWS Lambda - Permintaan	30.000 remediasi * 6 permintaan = 180.000 permintaan $0,20 * 1.000.000 permintaan = $0,20	$0,20
AWS Lambda - Durasi	256M: 1.875 GB detik * 30.000 remediasi * $0.000167 = $0.9375	$0,94
AWS Step Functions	17 transisi negara* 30.000 remediasi = 510.000 $0,025 * (510.000/1.000) transisi status = $12,75	$12,75
EventBridge Aturan Amazon	Tidak ada biaya untuk aturan	$0

Layanan	Asumsi	Biaya bulanan [USD]
Layanan Manajemen Utama AWS	(1 kunci) $1 * 1.000 akun * 10 Wilayah = $10.000	$10.000
Amazon DynamoDB	$0.000002 * 1.000.000 membaca dan menulis = $2,00	$2,00
Amazon SQS	$0,000004 * 1.000.000 permintaan = $0,40	$0,40
Amazon SNS	$0.000005 * 1.000.000 pemberitahuan = $0,50	$0,50
Amazon CloudWatch - Metrik	$0,30 * 6 metrik khusus = $1,80 $0,01 * (30.000 * 3/1.000) menempatkan metrik panggilan API = $0,90	$2,70
Amazon CloudWatch - Dasbor	$3,00 * 1 dasbor = $3,00	$3,00
Amazon CloudWatch - Alarm	$0,10 * 2 alarm = $0,20	$0,20
Jumlah		$10.271,70

Important

Biaya Rotasi Kunci KMS AWS Key Management Service (KMS) AWS Key Management Service (KMS) secara otomatis memutar kunci yang dikelola pelanggan sekali per tahun saat rotasi diaktifkan. Setiap rotasi menimbulkan biaya $1,00 per kunci per tahun. Misalnya, dengan 1000 akun di satu wilayah, ini menghasilkan tambahan $1000/tahun (1 rotasi × 1000 kunci × $1,00).

Biaya tambahan untuk fitur opsional

Bagian ini mengidentifikasi biaya tambahan yang terkait dengan fitur opsional untuk solusi ini.

CloudWatch Metrik yang disempurnakan

Jika Anda `yes` memilih EnableEnhancedCloudWatchMetricsparameter saat menerapkan tumpukan admin, solusi akan membuat dua metrik khusus dan satu alarm untuk setiap ID kontrol. Biaya tergantung pada jumlah kontrol IDs yang Anda pulihkan. Dalam tabel berikut, kami berasumsi bahwa Anda memulihkan semua 96 kontrol yang berbeda IDs per bulan, untuk menentukan batas atas biaya.

Layanan	Asumsi 96 IDs kontrol* 2 = 192 metrik khusus	Biaya bulanan [USD]
Amazon CloudWatch - Metrik	$0,30 * 192 metrik khusus = $57,60	$57,60
Amazon CloudWatch - Alarm	$0,10 * 96 alarm = $9,60	$9,60
Jumlah		$67,20

CloudTrail Log Tindakan

Di setiap akun anggota tempat Anda mengaktifkan fitur Log Tindakan, solusi akan membuat CloudTrail jejak untuk mencatat semua peristiwa manajemen penulisan. Fungsi Lambda menyaring peristiwa yang tidak terkait dengan solusi. Ini berarti bahwa biaya terkait dengan jumlah total peristiwa manajemen di akun Anda, karena peristiwa yang tidak terkait dengan solusi masih ditangkap oleh jejak dan diproses oleh fungsi Lambda.

Untuk tabel berikut, kami mengasumsikan 150.000 peristiwa manajemen per bulan di akun. Biaya aktual tergantung pada aktivitas acara manajemen aktual di akun Anda.

Layanan	Asumsi	Biaya bulanan [USD]
AWS CloudTrail	150.000 * $2,00/100.000 = $3,00	$3,00

Layanan	Asumsi	Biaya bulanan [USD]
Lambda	150.000 * 0,2 * 0,125 = 3,750 GB-detik 3.750 * $0,0000166667 = $0,0625 biaya waktu komputasi 0,15 * $0,20 = $0,03 biaya permintaan $0,0625 + $0,03 = $0,0952 total biaya Lambda	$0,0925
Jumlah		$3.09 per akun anggota

Keamanan

Saat Anda membangun sistem pada infrastruktur AWS, tanggung jawab keamanan dibagi antara Anda dan AWS. Model bersama ini mengurangi beban operasional Anda karena AWS mengoperasikan, mengelola, dan mengontrol komponen termasuk sistem operasi host, lapisan virtualisasi, dan keamanan fisik fasilitas tempat layanan beroperasi. Untuk informasi selengkapnya tentang keamanan AWS, kunjungi AWS Cloud Security.

Peran IAM

Peran AWS Identity and Access Management (IAM) memungkinkan pelanggan menetapkan kebijakan akses terperinci dan izin untuk layanan dan pengguna di AWS Cloud. Solusi ini menciptakan peran IAM yang memberikan akses fungsi otomatis solusi untuk melakukan tindakan remediasi dalam serangkaian izin khusus untuk setiap remediasi.

Fungsi Langkah akun admin ditetapkan ke peran SO0111-. ASR-Orchestrator-Admin Hanya peran ini yang diizinkan untuk mengasumsikan SO0111-Orchestrator-member di setiap akun anggota. Peran anggota diizinkan oleh setiap peran remediasi untuk meneruskannya ke layanan AWS Systems Manager untuk menjalankan runbook remediasi tertentu. Nama peran remediasi dimulai dengan SO0111, diikuti dengan deskripsi yang cocok dengan nama runbook remediasi. Misalnya, SO0111-

remove VPCDefault SecurityGroupRules adalah peran untuk runbook remediasi ASR-Remove. VPCDefault SecurityGroupRules

Wilayah AWS yang Didukung

Nama wilayah	Kode Wilayah
AS Timur (Ohio)	us-east-2
US East (N. Virginia)	us-east-1
AS Barat (California Utara)	us-west-1
US West (Oregon)	as-barat-2
Afrika (Cape Town)	af-selatan-1
Asia Pasifik (Hong Kong)	ap-east-1
Asia Pasifik (Hyderabad)	ap-south-2
Asia Pasifik (Jakarta)	ap-southeast-3
Asia Pacific (Melbourne)	ap-southeast-4
Asia Pasifik (Mumbai)	ap-south-1
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-sentral-1
Europe (Frankfurt)	eu-central-1

Nama wilayah	Kode Wilayah
Europe (Ireland)	eu-west-1
Europe (London)	eu-barat-2
Eropa (Milan)	eu-selatan-1
Eropa (Paris)	eu-west-3
Eropa (Spanyol)	eu-south-2
Eropa (Stockholm)	eu-north-1
Europe (Zurich)	eu-central-2
Timur Tengah (Bahrain)	me-south-1
Timur Tengah (UEA)	me-central-1
Amerika Selatan (Sao Paulo)	sa-east-1
AWS GovCloud (AS-Timur)	us-gov-east-1
AWS GovCloud (AS-Barat)	us-gov-west-1
Tiongkok (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1
Israel (Tel Aviv)	il-central-1
Kanada Barat (Calgary)	ca-west-1
Meksiko (Kota Meksiko)	mx-pusat-1
Asia Pasifik (Thailand)	ap-tenggara 7

> **Note**
>
> Setiap wilayah AWS baru yang tidak terdaftar dapat didukung melalui penerapan lokal tetapi bukan penerapan satu klik.

Kuota

Service quotas, juga disebut batasan, adalah jumlah maksimum sumber daya layanan atau operasi untuk akun AWS Anda.

Kuota untuk layanan AWS dalam solusi ini

Pastikan Anda memiliki kuota yang cukup untuk setiap layanan yang diterapkan dalam solusi ini. Untuk informasi selengkapnya, lihat kuota layanan AWS.

Gunakan tautan berikut untuk membuka halaman untuk layanan itu. Untuk melihat Service Quotas untuk semua layanan AWS dalam dokumentasi tanpa berpindah halaman, lihat informasi di titik akhir Layanan dan halaman kuota di PDF sebagai gantinya.

CloudFormation Kuota AWS

Akun AWS Anda memiliki CloudFormation kuota AWS yang harus Anda ketahui saat meluncurkan tumpukan dalam solusi ini. Dengan memahami kuota ini, Anda dapat menghindari kesalahan pembatasan yang akan mencegah Anda menerapkan solusi ini dengan sukses. Untuk informasi selengkapnya, lihat CloudFormation kuota AWS di Panduan CloudFormation Pengguna AWS.

CloudWatch Kuota AWS

Akun AWS Anda memiliki CloudWatch kuota AWS yang terkait dengan Kebijakan CloudWatch Sumber Daya yang hanya mengizinkan 10 kebijakan sumber daya per wilayah per akun dan ini tidak dapat diminta untuk peningkatan kuota, lihat Kuota AWS CloudWatch Logs di Panduan Pengguna CloudWatch AWS. Sebelum penerapan Anda, periksa penggunaan Anda saat ini untuk memastikan Anda tidak akan melewati ambang batas ini saat menerapkan solusi.

Kuota EventBridge aturan Amazon

Akun AWS Anda memiliki kuota EventBridge aturan Amazon yang harus Anda ketahui saat memilih pedoman yang akan diterapkan dengan solusinya. Setiap buku pedoman akan membuat EventBridge

Aturan untuk setiap kontrol yang dapat diperbaiki. Saat menerapkan beberapa buku pedoman, dimungkinkan untuk mencapai kuota Aturan. Untuk informasi selengkapnya, lihat EventBridge Kuota Amazon di Panduan EventBridge Pengguna Amazon.

Penerapan AWS Security Hub

Penyebaran dan konfigurasi AWS Security Hub merupakan prasyarat untuk solusi ini. Untuk informasi selengkapnya tentang menyiapkan AWS Security Hub, lihat Menyiapkan AWS Security Hub di Panduan Pengguna AWS Security Hub.

Minimal, Anda harus memiliki Security Hub yang berfungsi yang dikonfigurasi di akun utama Anda. Anda dapat menerapkan solusi ini di akun yang sama (dan Wilayah AWS) dengan akun utama Security Hub. Di setiap akun primer dan sekunder Security Hub, Anda juga harus menerapkan template anggota yang memungkinkan AssumeRole izin ke AWS Step Functions solusi untuk menjalankan runbook remediasi di akun.

Tumpukan vs StackSets penyebaran

Kumpulan tumpukan memungkinkan Anda membuat tumpukan di akun AWS di seluruh Wilayah AWS dengan menggunakan satu CloudFormation templat AWS. Dimulai dengan versi 1.4, solusi ini mendukung penyebaran kumpulan tumpukan dengan memisahkan sumber daya berdasarkan di mana dan bagaimana mereka digunakan. Pelanggan multi-akun, terutama yang menggunakan AWS Organizations, dapat memperoleh manfaat dari menggunakan kumpulan tumpukan untuk penerapan di banyak akun. Ini mengurangi upaya yang diperlukan untuk menginstal dan memelihara solusi. Untuk informasi selengkapnya StackSets, lihat Menggunakan AWS CloudFormation StackSets.

Terapkan solusinya

> **Important**
>
> Jika fitur temuan kontrol konsolidasi diaktifkan di Security Hub (ini adalah default dalam penerapan baru), hanya aktifkan buku pedoman Kontrol Keamanan (CS) saat menerapkan solusi ini. Jika fitur tidak diaktifkan, hanya aktifkan pedoman untuk standar keamanan yang diaktifkan di Security Hub. Mengaktifkan pedoman tambahan dapat mengakibatkan tercapainya kuota Aturan. EventBridge

Solusi ini menggunakan CloudFormation templat dan tumpukan AWS untuk mengotomatiskan penerapannya. CloudFormation Template menentukan sumber daya AWS yang disertakan dalam solusi ini dan propertinya. CloudFormation Tumpukan menyediakan sumber daya yang dijelaskan dalam template.

Agar solusi berfungsi, tiga templat harus digunakan. Pertama, putuskan di mana harus menggunakan templat, lalu putuskan cara menerapkannya.

Ikhtisar ini akan menjelaskan template dan bagaimana memutuskan di mana dan bagaimana menerapkannya. Bagian selanjutnya akan memiliki instruksi yang lebih rinci untuk menyebarkan setiap tumpukan sebagai Stack atau StackSet.

Memutuskan di mana untuk menyebarkan setiap tumpukan

Tiga templat akan dirujuk dengan nama-nama berikut dan berisi sumber daya berikut:

- Tumpukan admin: fungsi langkah orkestrator, aturan acara, dan tindakan kustom Security Hub.
- Tumpukan anggota: remediasi dokumen Otomasi SSM.
- Tumpukan peran anggota: peran IAM untuk remediasi.

Tumpukan Admin harus digunakan sekali, dalam satu akun dan satu Wilayah. Ini harus diterapkan ke akun dan Wilayah yang telah Anda konfigurasikan sebagai tujuan agregasi untuk temuan Security Hub untuk organisasi Anda. Jika Anda ingin menggunakan fitur Log Tindakan untuk memantau peristiwa manajemen, Anda harus menerapkan tumpukan Admin di akun manajemen organisasi Anda atau akun administrator yang didelegasikan.

Solusi ini beroperasi pada temuan Security Hub, sehingga tidak akan dapat beroperasi pada temuan dari akun dan Wilayah tertentu jika akun atau Wilayah tersebut belum dikonfigurasi untuk mengumpulkan temuan di akun administrator Security Hub dan Wilayah.

Misalnya, organisasi memiliki akun yang beroperasi di Wilayah `us-east-1` dan`us-west-2`, dengan akun `111111111111` sebagai administrator yang didelegasikan oleh Security Hub di Region`us-east-1`. Akun `222222222222` dan `333333333333` harus merupakan akun anggota Security Hub untuk akun `111111111111` administrator yang didelegasikan. Ketiga akun harus dikonfigurasi untuk mengumpulkan temuan dari `us-west-2` ke`us-east-1`. Tumpukan Admin harus disebarkan ke akun`111111111111`. `us-east-1`

Untuk detail selengkapnya tentang menemukan agregasi, lihat dokumentasi untuk akun administrator yang didelegasikan Security Hub dan agregasi lintas wilayah.

Tumpukan Admin harus menyelesaikan penerapan terlebih dahulu sebelum menerapkan tumpukan anggota sehingga hubungan kepercayaan dapat dibuat dari akun anggota ke akun hub.

Tumpukan anggota harus disebarkan ke setiap akun dan Wilayah tempat Anda ingin memulihkan temuan. Ini dapat mencakup akun administrator yang didelegasikan Security Hub tempat Anda sebelumnya menggunakan tumpukan Admin ASR. Dokumen otomatisasi harus dijalankan di akun anggota untuk menggunakan tingkat gratis untuk Otomasi SSM.

Menggunakan contoh sebelumnya, jika Anda ingin memulihkan temuan dari semua akun dan Wilayah, tumpukan anggota harus disebarkan ke ketiga akun (`111111111111`,`222222222222`, dan`333333333333`) dan kedua Wilayah (`us-east-1`dan`us-west-2`).

Tumpukan peran anggota harus disebarkan ke setiap akun, tetapi berisi sumber daya global (peran IAM) yang hanya dapat digunakan sekali per akun. Tidak masalah di Wilayah mana Anda menerapkan tumpukan peran anggota, jadi untuk kesederhanaan, kami sarankan untuk menerapkan ke Wilayah yang sama di mana tumpukan Admin diterapkan.

Menggunakan contoh sebelumnya, kami sarankan untuk menerapkan tumpukan peran anggota ke ketiga akun (`111111111111`,`222222222222`, dan`333333333333`) di`us-east-1`.

Memutuskan cara menerapkan setiap tumpukan

Opsi untuk menerapkan tumpukan adalah

- CloudFormation StackSet (izin yang dikelola sendiri)

- CloudFormation StackSet (izin yang dikelola layanan)
- CloudFormation Tumpukan

StackSets dengan izin yang dikelola layanan adalah yang paling nyaman karena mereka tidak memerlukan penerapan peran Anda sendiri dan dapat secara otomatis menyebarkan ke akun baru di organisasi. Sayangnya, metode ini tidak mendukung tumpukan bersarang, yang kami gunakan di tumpukan Admin dan tumpukan anggota. Satu-satunya tumpukan yang dapat digunakan dengan cara ini adalah tumpukan peran anggota.

Ketahuilah bahwa saat menyebarkan ke seluruh organisasi, akun manajemen organisasi tidak disertakan, jadi jika Anda ingin memulihkan temuan di akun manajemen organisasi, Anda harus menyebarkan ke akun ini secara terpisah.

Tumpukan anggota harus diterapkan ke setiap akun dan Wilayah tetapi tidak dapat digunakan menggunakan izin yang dikelola layanan karena StackSets berisi tumpukan bersarang. Jadi kami sarankan untuk menerapkan tumpukan ini StackSets dengan izin yang dikelola sendiri.

Tumpukan Admin hanya digunakan sekali, sehingga dapat digunakan sebagai CloudFormation tumpukan biasa atau sebagai StackSet dengan izin yang dikelola sendiri dalam satu akun dan Wilayah.

Temuan kontrol konsolidasi

Akun di organisasi Anda dapat dikonfigurasi dengan fitur temuan kontrol konsolidasi dari Security Hub diaktifkan atau dinonaktifkan. Lihat Temuan kontrol konsolidasi di Panduan Pengguna AWS Security Hub.

> **Important**
>
> Jika diaktifkan, Anda harus menggunakan v2.0.0 dari solusi atau yang lebih baru. Selain itu, Anda harus menerapkan tumpukan bersarang Admin dan Anggota untuk standar “SC” atau “kontrol keamanan”. Ini menyebarkan dokumen otomatisasi dan EventBridge aturan untuk digunakan dengan kontrol konsolidasi IDs yang dihasilkan saat fitur ini dihidupkan. Tidak perlu menerapkan tumpukan bersarang Admin atau Anggota untuk standar tertentu (misalnya AWS FSBP) saat menggunakan fitur ini.

CloudFormation Templat AWS

View template

automa

security-response-admin.template - Gunakan template ini untuk meluncurkan solusi Automated Security Response pada AWS. Template menginstal komponen inti solusi, tumpukan bersarang untuk log AWS Step Functions, dan satu tumpukan bersarang untuk setiap standar keamanan yang Anda pilih untuk diaktifkan.

Layanan yang digunakan meliputi Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions, Amazon CloudWatch Logs, Amazon S3, dan AWS Systems Manager.

Dukungan akun admin

Templat berikut dipasang di akun admin AWS Security Hub untuk mengaktifkan standar keamanan yang ingin Anda dukung. Anda dapat memilih mana dari template berikut untuk menginstal saat menginstal`automated-security-response-admin.template`.

automated-security-response-orchestrator-log.template - Membuat grup CloudWatch log untuk Fungsi Langkah Orchestrator.

AFSBPStack.template - Aturan Praktik Terbaik Keamanan Dasar AWS v1.0.0.

CIS120Stack.Template - Tolok ukur Yayasan Amazon Web Services CIS, aturan v1.2.0.

CIS140Stack.Template - Tolok ukur Yayasan Amazon Web Services CIS, aturan v1.4.0.

CIS300Stack.Template - Tolok ukur Yayasan Amazon Web Services CIS, aturan v3.0.0.

PCI321Stack.template - aturan PCI-DSS v3.2.1.

NISTStack.template - Institut Nasional Standar dan Teknologi (NIST), aturan v5.0.0.

SCStack.template - Kontrol Keamanan aturan v2.0.0.

Peran anggota

View template

automa

security-response-member-roles.template - Mendefinisikan peran remediasi yang diperlukan di setiap akun anggota AWS Security Hub.

Akun anggota

View template

automa

security-response-member.template - Gunakan template ini setelah Anda menyiapkan solusi inti untuk menginstal runbook dan izin otomatisasi AWS Systems Manager di setiap akun anggota AWS Security Hub Anda (termasuk akun admin). Template ini memungkinkan Anda memilih pedoman standar keamanan mana yang akan dipasang.

`automated-security-response-member.template`Menginstal template berikut berdasarkan pilihan Anda:

automated-security-response-remediation-runbooks.template - Kode remediasi umum yang digunakan oleh satu atau lebih standar keamanan.

AFSBPMemberStack.template - AWS Foundational Security Best Practices v1.0.0 pengaturan, izin, dan runbook remediasi.

CIS120 MemberStack .template - Tolok ukur Yayasan Amazon Web Services CIS, pengaturan versi 1.2.0, izin, dan runbook remediasi.

CIS140 MemberStack .template - Tolok ukur Yayasan Amazon Web Services CIS, pengaturan versi 1.4.0, izin, dan runbook remediasi.

CIS300 MemberStack .template - Tolok ukur Yayasan Amazon Web Services CIS, pengaturan versi 3.0.0, izin, dan runbook remediasi.

PCI321MemberStack.template - Pengaturan PCI-DSS v3.2.1, izin, dan runbook remediasi.

NISTMemberStack.template - Institut Nasional Standar dan Teknologi (NIST), pengaturan v5.0.0, izin, dan runbook remediasi.

SCMemberStack.template - Pengaturan Kontrol Keamanan, izin, dan runbook remediasi.

automated-security-response-member-cloudtrail.template - Digunakan dalam fitur Action Log untuk melacak dan mengaudit dan aktivitas layanan.

Integrasi sistem tiket

Gunakan salah satu templat berikut untuk berintegrasi dengan sistem tiket Anda.

View template

JiraBlu

- Terapkan jika Anda menggunakan Jira sebagai sistem tiket Anda.

View template

Service

- Menyebarkan jika Anda menggunakan ServiceNow sebagai sistem tiket Anda.

Jika Anda ingin mengintegrasikan sistem tiket eksternal yang berbeda, Anda dapat menggunakan salah satu tumpukan ini sebagai cetak biru untuk memahami cara menerapkan integrasi kustom Anda sendiri.

Penerapan otomatis - StackSets

> **Note**
>
> Kami merekomendasikan untuk menerapkan dengan StackSets. Namun, untuk penerapan akun tunggal atau untuk tujuan pengujian atau evaluasi, pertimbangkan opsi penyebaran tumpukan.

Sebelum Anda meluncurkan solusi, tinjau arsitektur, komponen solusi, keamanan, dan pertimbangan desain yang dibahas dalam panduan ini. Ikuti step-by-step petunjuk di bagian ini untuk mengonfigurasi dan menerapkan solusi ke AWS Organizations Anda.

Waktu untuk menyebarkan: Sekitar 30 menit per akun, tergantung pada StackSet parameter.

Prasyarat

AWS Organizations membantu Anda mengelola dan mengatur lingkungan dan sumber daya AWS multi-akun secara terpusat. StackSets bekerja paling baik dengan AWS Organizations.

Jika sebelumnya Anda telah menerapkan v1.3.x atau sebelumnya dari solusi ini, Anda harus menghapus instalan solusi yang ada. Untuk informasi selengkapnya, lihat Perbarui solusinya.

Sebelum Anda menerapkan solusi ini, tinjau penerapan AWS Security Hub Anda:

- Harus ada akun admin Security Hub yang didelegasikan di AWS Organization Anda.
- Security Hub harus dikonfigurasi untuk mengumpulkan temuan di seluruh Wilayah. Untuk informasi selengkapnya, lihat Mengagregasi temuan di seluruh Wilayah dalam Panduan Pengguna AWS Security Hub.
- Anda harus mengaktifkan Security Hub untuk organisasi Anda di setiap Wilayah tempat Anda menggunakan AWS.

Prosedur ini mengasumsikan bahwa Anda memiliki beberapa akun yang menggunakan AWS Organizations, dan telah mendelegasikan akun admin AWS Organizations dan akun admin AWS Security Hub.

Ikhtisar penyebaran

> **Note**
>
> StackSets penyebaran untuk solusi ini menggunakan kombinasi layanan yang dikelola dan dikelola sendiri. StackSets Self-Managed StackSets harus digunakan saat ini karena mereka menggunakan nested StackSets, yang belum didukung dengan service-managed. StackSets

Menerapkan StackSets dari akun administrator yang didelegasikan di AWS Organizations Anda.

Perencanaan

Gunakan formulir berikut untuk membantu StackSets penyebaran. Siapkan data Anda, lalu salin dan tempel nilai selama penerapan.

```
AWS Organizations admin account ID: _________________
Security Hub admin account ID: _________________
CloudTrail Logs Group: ____________________________
Member account IDs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
```

```
____________________
AWS Organizations OUs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
```

(Opsional) Langkah 0: Menyebarkan tumpukan integrasi tiket

- Jika Anda ingin menggunakan fitur tiket, gunakan tumpukan integrasi tiket ke akun admin Security Hub Anda terlebih dahulu.
- Salin nama fungsi Lambda dari tumpukan ini dan berikan sebagai masukan ke tumpukan admin (lihat Langkah 1).

Langkah 1: Luncurkan tumpukan admin di akun admin Security Hub yang didelegasikan

- Menggunakan pengelolaan sendiri StackSet, luncurkan CloudFormation template `automated-security-response-admin.template` AWS ke akun admin AWS Security Hub Anda di Wilayah yang sama dengan admin Security Hub Anda. Template ini menggunakan tumpukan bersarang.
- Pilih Standar Keamanan mana yang akan dipasang. Secara default, hanya SC yang dipilih (Disarankan).
- Pilih grup log Orchestrator yang ada untuk digunakan. Pilih `Yes` jika `SO0111-ASR-Orchestrator` sudah ada dari instalasi sebelumnya.

Untuk informasi selengkapnya tentang pengelolaan sendiri StackSets, lihat Berikan izin yang dikelola sendiri di Panduan Pengguna CloudFormation AWS.

Langkah 2: Instal peran remediasi ke setiap akun anggota AWS Security Hub

Tunggu Langkah 1 menyelesaikan penerapan, karena template di Langkah 2 mereferensikan peran IAM yang dibuat oleh Langkah 1.

- Menggunakan layanan yang dikelola StackSet, luncurkan CloudFormation template `automated-security-response-member-roles.template` AWS ke dalam satu Wilayah di setiap akun di AWS Organizations Anda.
- Pilih untuk menginstal template ini secara otomatis ketika akun baru bergabung dengan organisasi.

- Masukkan ID akun akun admin AWS Security Hub Anda.

Langkah 3: Luncurkan tumpukan anggota ke setiap akun dan Wilayah anggota AWS Security Hub

- Menggunakan pengelolaan sendiri StackSets, luncurkan CloudFormation template `automated-security-response-member.template` AWS ke semua Wilayah tempat Anda memiliki sumber daya AWS di setiap akun di Organisasi AWS yang dikelola oleh admin Security Hub yang sama.

> **Note**
>
> Hingga tumpukan bersarang StackSets dukungan yang dikelola layanan, Anda harus melakukan langkah ini untuk setiap akun baru yang bergabung dengan organisasi.

- Pilih pedoman Standar Keamanan mana yang akan dipasang.
- Berikan nama grup CloudTrail log (digunakan oleh beberapa remediasi).
- Masukkan ID akun akun admin AWS Security Hub Anda.

(Opsional) Langkah 0: Luncurkan tumpukan integrasi sistem tiket

1. Jika Anda bermaksud menggunakan fitur tiket, luncurkan tumpukan integrasi masing-masing terlebih dahulu.
2. Pilih tumpukan integrasi yang disediakan untuk Jira atau ServiceNow, atau gunakan sebagai cetak biru untuk mengimplementasikan integrasi kustom Anda sendiri.

   Untuk menyebarkan tumpukan Jira:

   a. Masukkan nama untuk tumpukan Anda.

   b. Berikan URI ke instans Jira Anda.

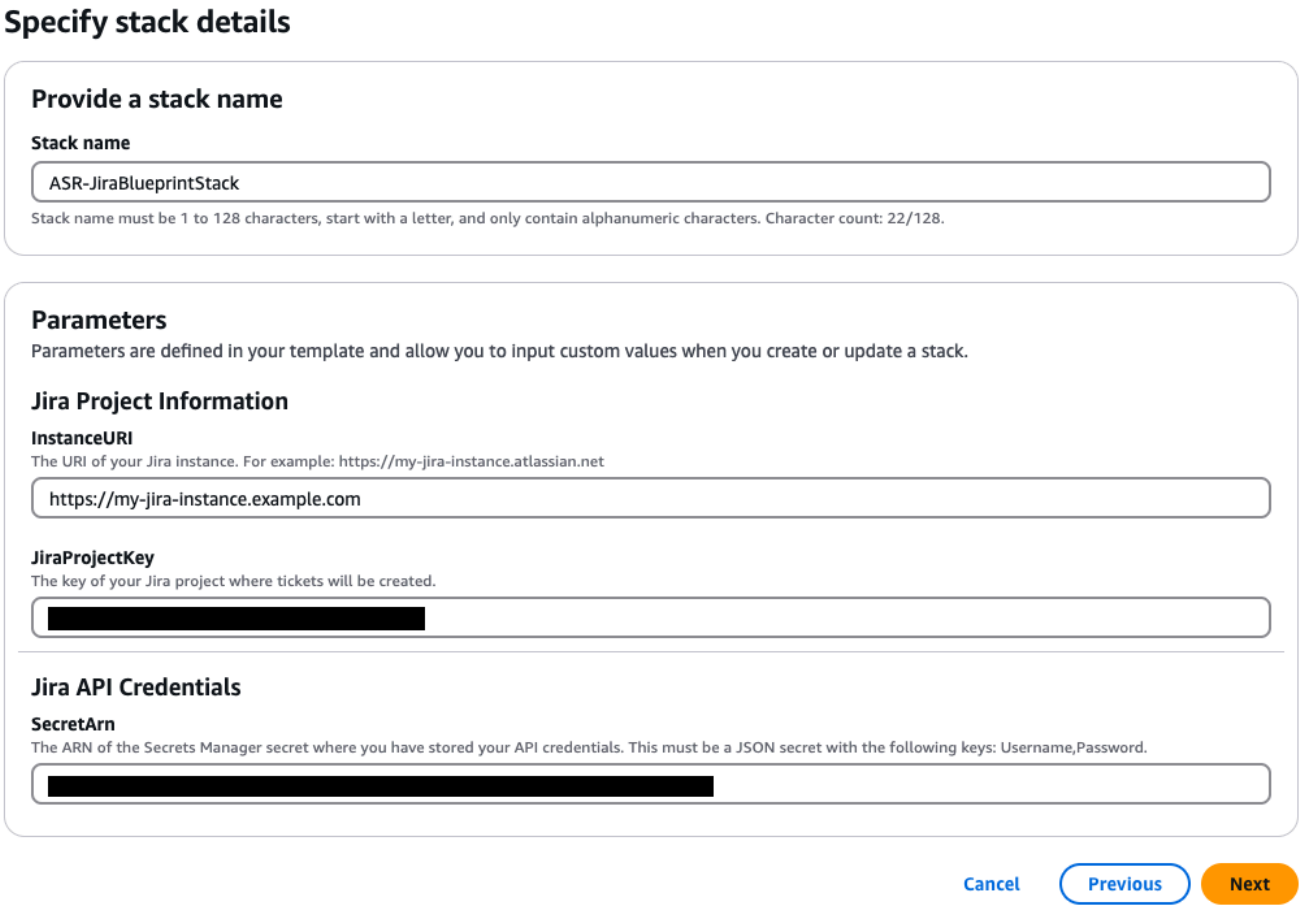
   c. Berikan kunci proyek untuk proyek Jira yang ingin Anda kirimi tiketnya.

   d. Buat rahasia nilai kunci baru di Secrets Manager yang menyimpan `Username` Jira dan. `Password`

> **Note**
>
> Anda dapat memilih untuk menggunakan kunci API JIRA sebagai pengganti kata sandi Anda dengan memberikan nama pengguna Anda sebagai `Username` dan kunci API Anda sebagai. `Password`

e. Tambahkan ARN rahasia ini sebagai masukan ke tumpukan.

Berikan nama tumpukan informasi proyek Jira, dan kredenal API Jira.



Untuk menyebarkan ServiceNow tumpukan:

f. Masukkan nama untuk tumpukan Anda.

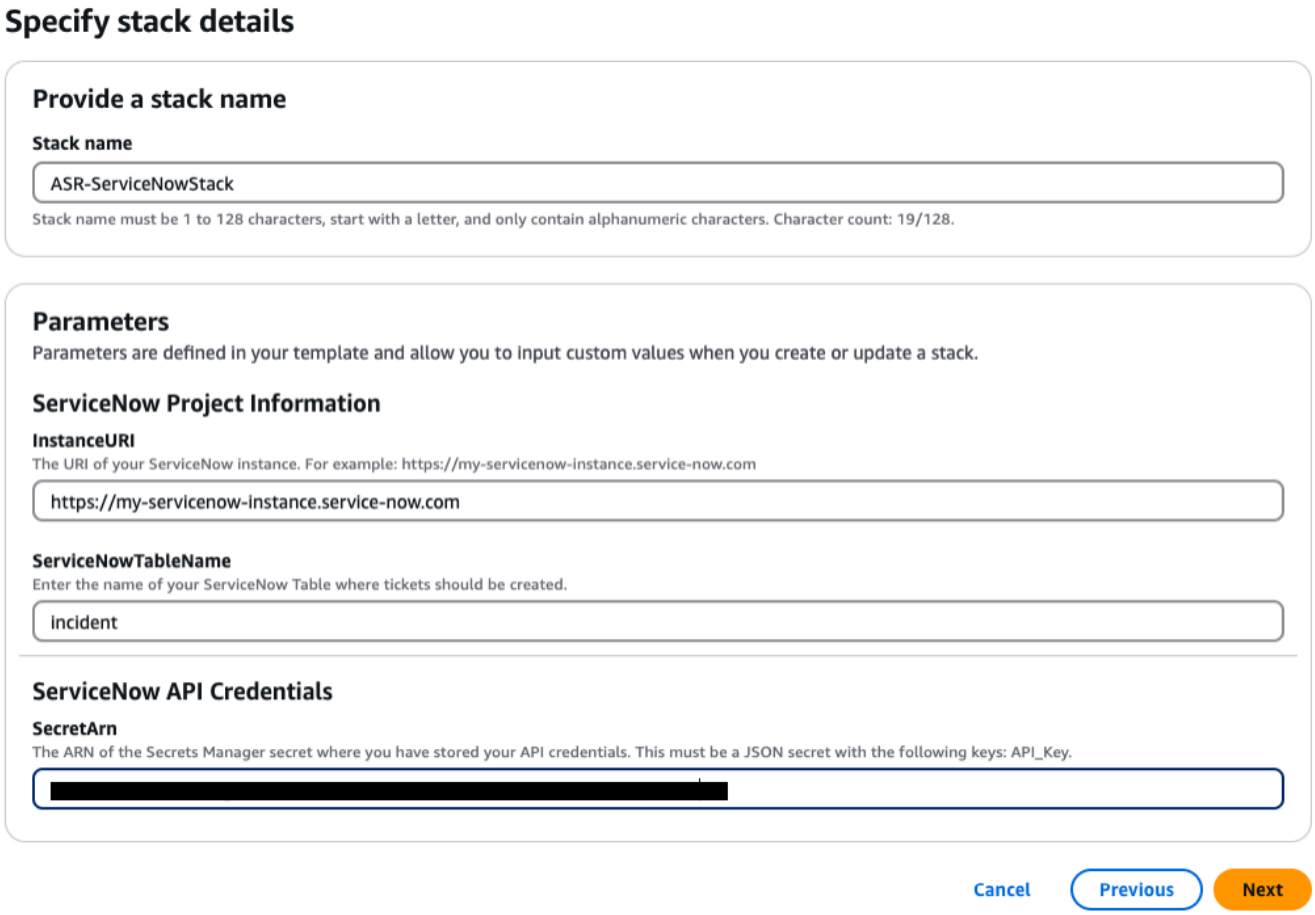
g. Berikan URI ServiceNow instance Anda.

h. Berikan nama ServiceNow tabel Anda.

i. Buat kunci API ServiceNow dengan izin untuk memodifikasi tabel yang ingin Anda tulis.

j. Buat rahasia di Secrets Manager dengan kunci `API_Key` dan berikan ARN rahasia sebagai masukan ke tumpukan.

   Berikan informasi ServiceNow proyek nama tumpukan, dan kredensi ServiceNow API.



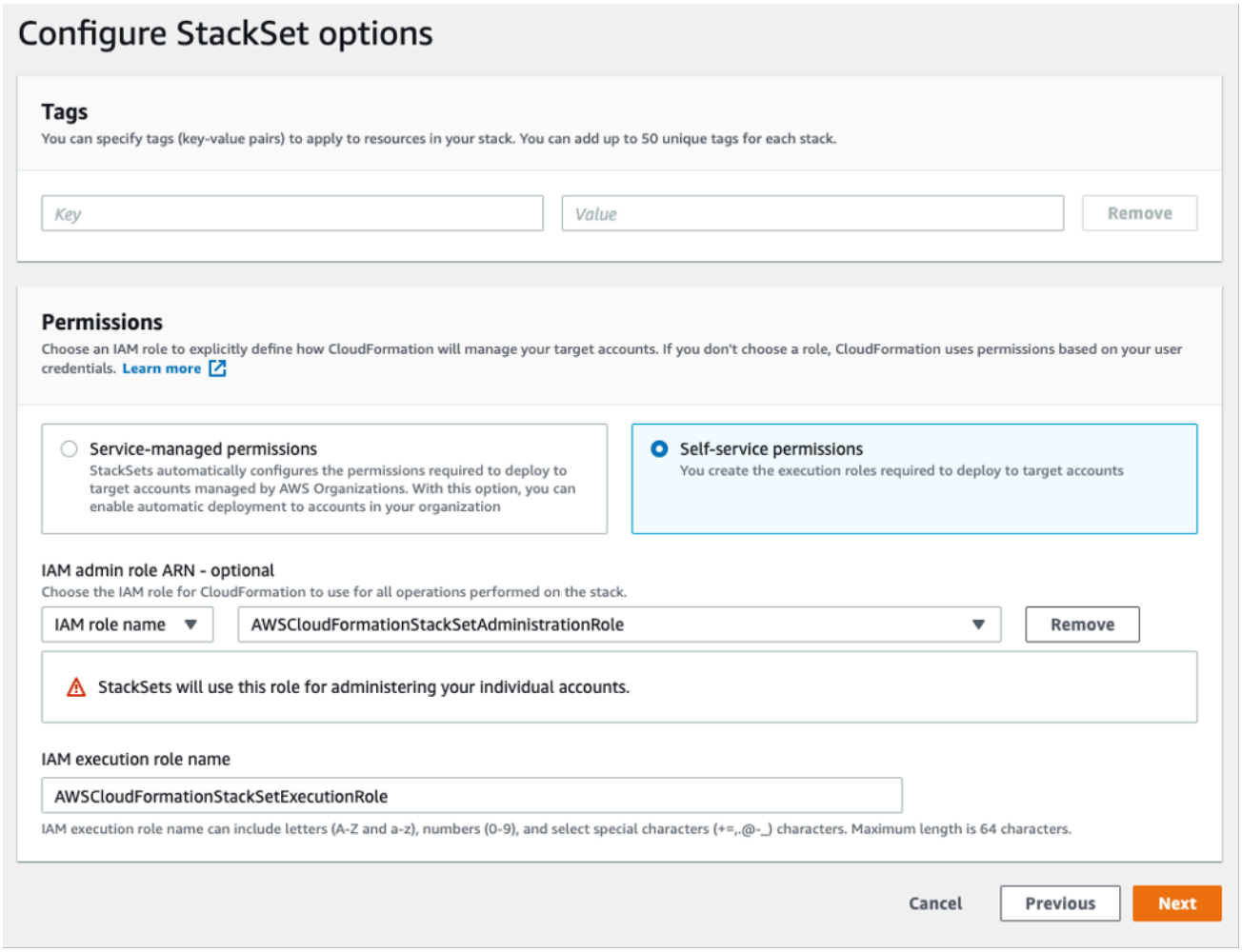
   Untuk membuat tumpukan integrasi kustom: Sertakan fungsi Lambda yang dapat dipanggil oleh Step Functions orkestrator solusi untuk setiap remediasi. Fungsi Lambda harus mengambil input yang disediakan oleh Step Functions, membuat payload sesuai dengan persyaratan sistem tiket Anda, dan membuat permintaan ke sistem Anda untuk membuat tiket.

Langkah 1: Luncurkan tumpukan admin di akun admin Security Hub yang didelegasikan

1. Luncurkan tumpukan admin,`automated-security-response-admin.template`, dengan akun admin Security Hub Anda. Biasanya, satu per organisasi dalam satu Wilayah. Karena

tumpukan ini menggunakan tumpukan bersarang, Anda harus menerapkan template ini sebagai pengelola sendiri. StackSet

Konfigurasikan StackSet opsi



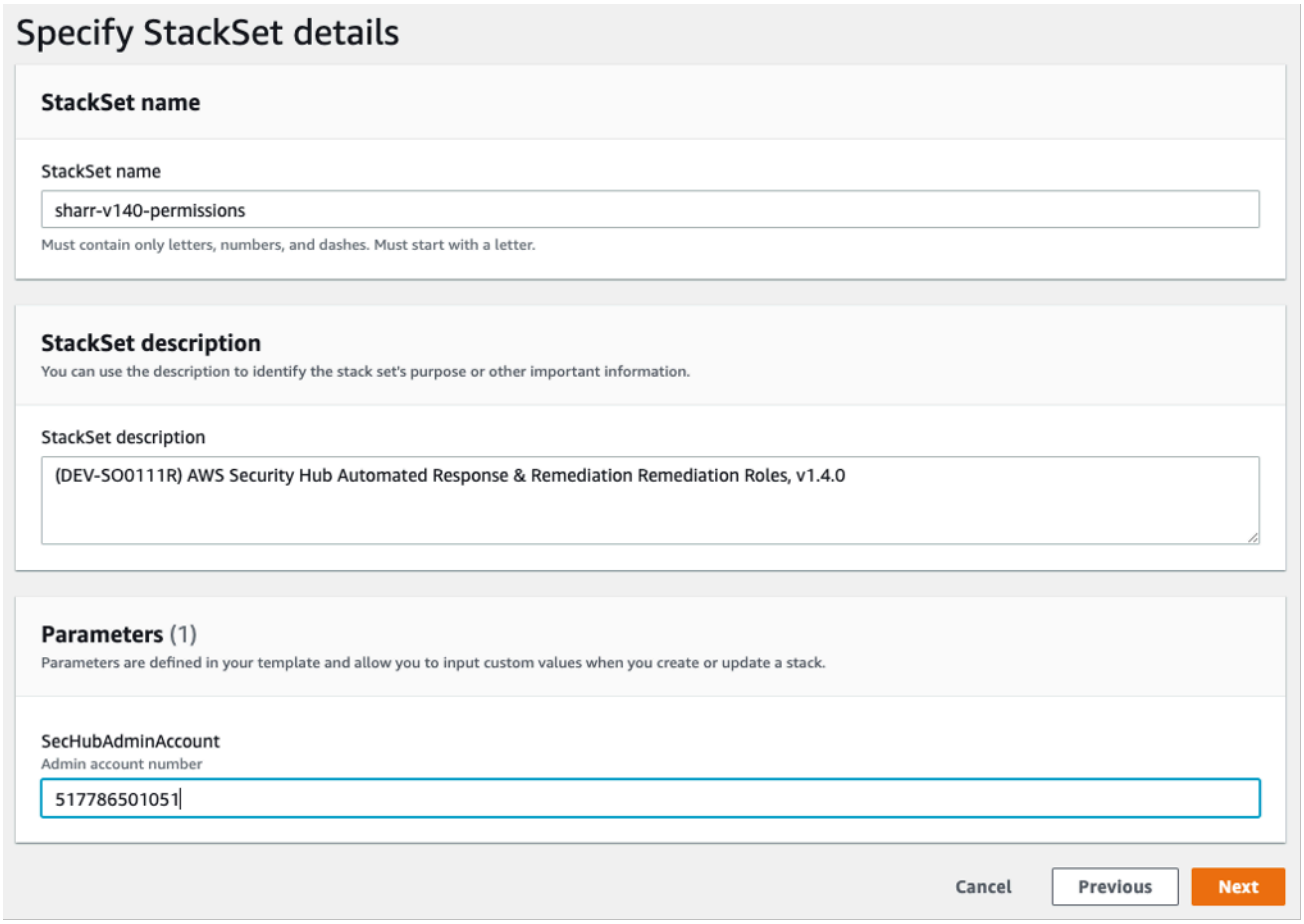
2. Untuk parameter Nomor akun, masukkan ID akun akun admin AWS Security Hub.
3. Untuk parameter Tentukan wilayah, pilih hanya Wilayah tempat admin Security Hub diaktifkan. Tunggu sampai langkah ini selesai sebelum melanjutkan ke Langkah 2.

Langkah 2: Instal peran remediasi ke setiap akun anggota AWS Security Hub

Gunakan layanan yang dikelola StackSets untuk menerapkan template peran anggota,. `automated-security-response-member-roles.template` Ini StackSet harus digunakan dalam satu Wilayah per akun anggota. Ini mendefinisikan peran global yang memungkinkan panggilan API lintas akun dari fungsi langkah ASR Orchestrator.

1. Menyebarkan ke seluruh organisasi (tipikal) atau ke unit organisasi, sesuai kebijakan organisasi Anda.
2. Aktifkan penerapan otomatis sehingga akun baru di AWS Organizations menerima izin ini.
3. Untuk parameter Tentukan wilayah, pilih satu Wilayah. Peran IAM bersifat global. Anda dapat melanjutkan ke Langkah 3 saat ini StackSet diterapkan.

Tentukan StackSet detail



Langkah 3: Luncurkan tumpukan anggota ke setiap akun dan Wilayah anggota AWS Security Hub

Karena tumpukan anggota menggunakan tumpukan bersarang, Anda harus menerapkan sebagai dikelola sendiri. StackSet Ini tidak mendukung penerapan otomatis ke akun baru di AWS Organization.

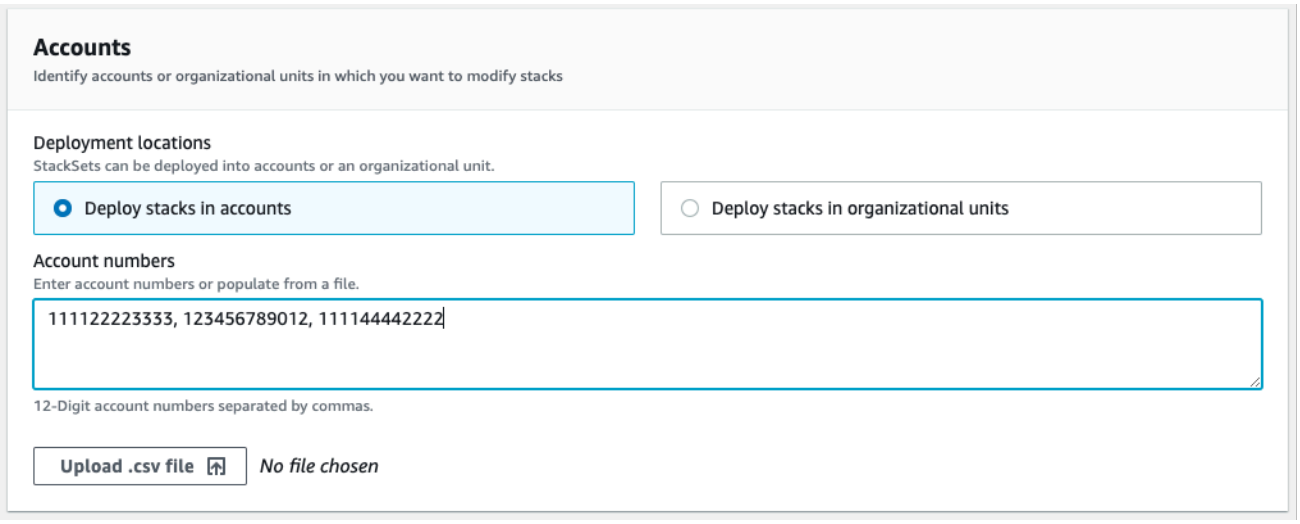
Parameter

LogGroup Konfigurasi: Pilih grup log yang menerima CloudTrail log. Jika tidak ada, atau jika grup log berbeda untuk setiap akun, pilih nilai yang nyaman. Administrator akun harus memperbarui parameter Systems Manager - Parameter Store/Solutions/SO0111/Metrics_ LogGroupName setelah membuat Grup CloudWatch Log untuk CloudTrail log. Ini diperlukan untuk remediasi yang membuat alarm metrik pada panggilan API.

Standar: Pilih standar untuk dimuat di akun anggota. Ini hanya menginstal runbook AWS Systems Manager - tidak mengaktifkan Standar Keamanan.

SecHubAdminAccount: Masukkan ID akun akun Admin AWS Security Hub tempat Anda menginstal templat admin solusi.

Akun



Lokasi penyebaran: Anda dapat menentukan daftar nomor akun atau unit organisasi.

Tentukan wilayah: Pilih semua Wilayah tempat Anda ingin memulihkan temuan. Anda dapat menyesuaikan opsi Deployment yang sesuai untuk jumlah akun dan Wilayah. Region Concurrency bisa paralel.

Penerapan otomatis - Tumpukan

> **Note**
>
> Untuk pelanggan multi-akun, kami sangat menyarankan penerapan dengan. StackSets

Sebelum Anda meluncurkan solusi, tinjau arsitektur, komponen solusi, keamanan, dan pertimbangan desain yang dibahas dalam panduan ini. Ikuti step-by-step petunjuk di bagian ini untuk mengonfigurasi dan menyebarkan solusi ke akun Anda.

Waktu untuk menyebarkan: Sekitar 30 menit

Prasyarat

Sebelum Anda menerapkan solusi ini, pastikan AWS Security Hub berada di Wilayah AWS yang sama dengan akun primer dan sekunder Anda. Jika sebelumnya Anda telah menerapkan solusi ini, Anda harus menghapus instalan solusi yang ada. Untuk informasi selengkapnya, lihat Perbarui solusinya.

Ikhtisar penyebaran

Gunakan langkah-langkah berikut untuk menerapkan solusi ini di AWS.

(Opsional) Langkah 0: Luncurkan tumpukan integrasi sistem tiket

- Jika Anda ingin menggunakan fitur tiket, gunakan tumpukan integrasi tiket ke akun admin Security Hub Anda terlebih dahulu.
- Salin nama fungsi Lambda dari tumpukan ini dan berikan sebagai masukan ke tumpukan admin (lihat Langkah 1).

Langkah 1: Luncurkan tumpukan admin

- Luncurkan CloudFormation template `automated-security-response-admin.template` AWS ke akun admin AWS Security Hub Anda.
- Pilih standar keamanan mana yang akan dipasang.
- Pilih grup log Orchestrator yang ada untuk digunakan (pilih `Yes` jika `SO0111-ASR-Orchestrator` sudah ada dari instalasi sebelumnya).

Langkah 2: Instal peran remediasi ke setiap akun anggota AWS Security Hub

- Luncurkan CloudFormation template `automated-security-response-member-roles.template` AWS ke dalam satu Wilayah per akun anggota.
- Masukkan IG akun 12 digit untuk akun admin AWS Security Hub.

Langkah 3: Luncurkan tumpukan anggota

- Tentukan nama grup CloudWatch Log yang akan digunakan dengan remediasi CIS 3.1-3.14. Itu harus nama grup CloudWatch log Log yang menerima CloudTrail log.
- Pilih apakah akan menginstal peran remediasi. Instal peran ini hanya sekali per akun.
- Pilih pedoman mana yang akan dipasang.
- Masukkan ID akun akun admin AWS Security Hub.

Langkah 4: (Opsional) Sesuaikan remediasi yang tersedia

- Hapus remediasi apa pun berdasarkan akun per anggota. Langkah ini bersifat opsional.

(Opsional) Langkah 0: Luncurkan tumpukan integrasi sistem tiket

1. Jika Anda bermaksud menggunakan fitur tiket, luncurkan tumpukan integrasi masing-masing terlebih dahulu.
2. Pilih tumpukan integrasi yang disediakan untuk Jira atau ServiceNow, atau gunakan sebagai cetak biru untuk mengimplementasikan integrasi kustom Anda sendiri.

   Untuk menyebarkan tumpukan Jira:

   a. Masukkan nama untuk tumpukan Anda.

   b. Berikan URI ke instans Jira Anda.

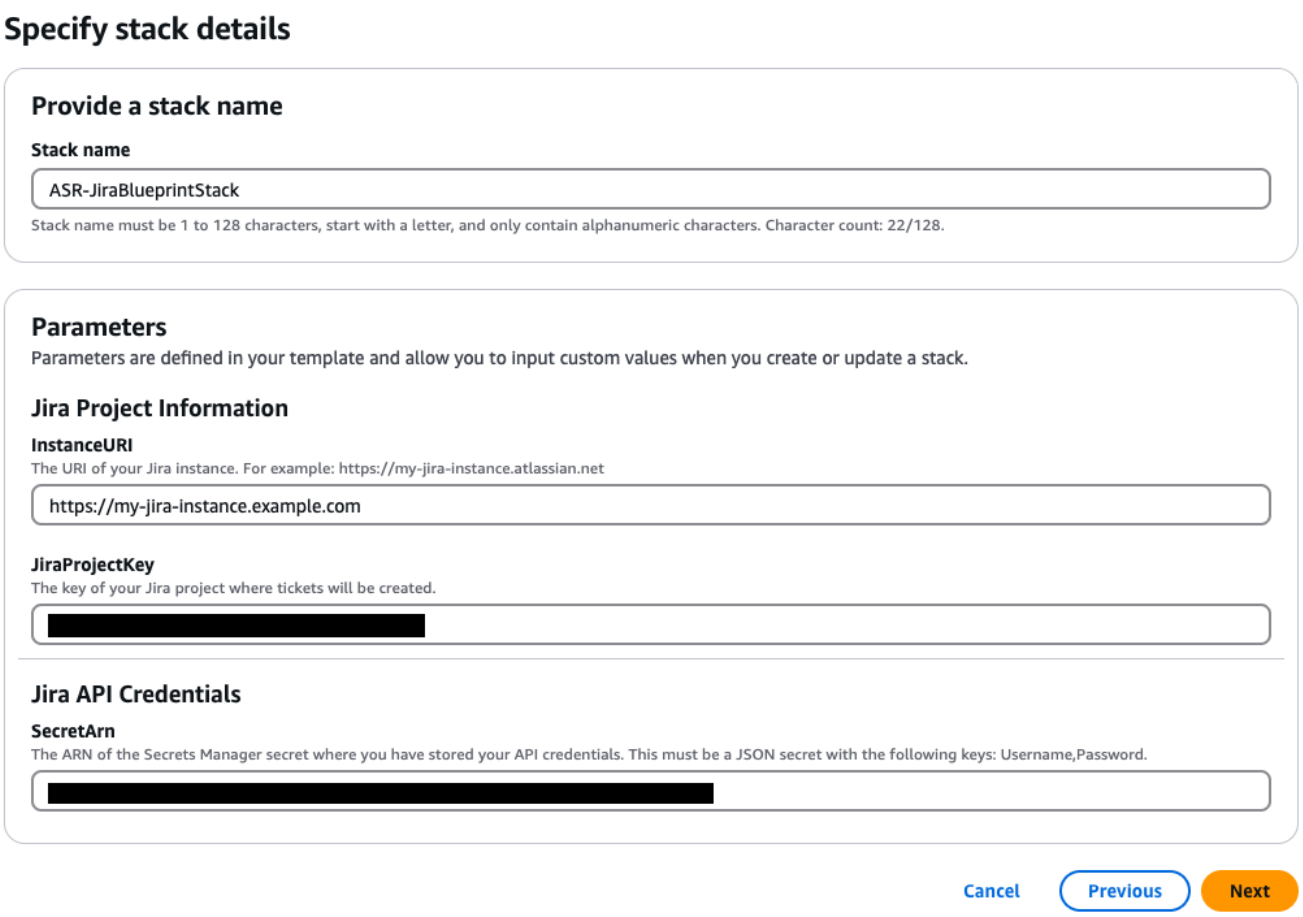
   c. Berikan kunci proyek untuk proyek Jira yang ingin Anda kirimi tiketnya.

   d. Buat rahasia nilai kunci baru di Secrets Manager yang menyimpan `Username` Jira dan. `Password`

   > **Note**
   >
   > Anda dapat memilih untuk menggunakan kunci API JIRA sebagai pengganti kata sandi Anda dengan memberikan nama pengguna Anda sebagai `Username` dan kunci API Anda sebagai. `Password`

   e. Tambahkan ARN rahasia ini sebagai masukan ke tumpukan.

   “Berikan nama tumpukan informasi proyek Jira, dan kredenal API Jira.



Untuk menyebarkan ServiceNow tumpukan:

f. Masukkan nama untuk tumpukan Anda.

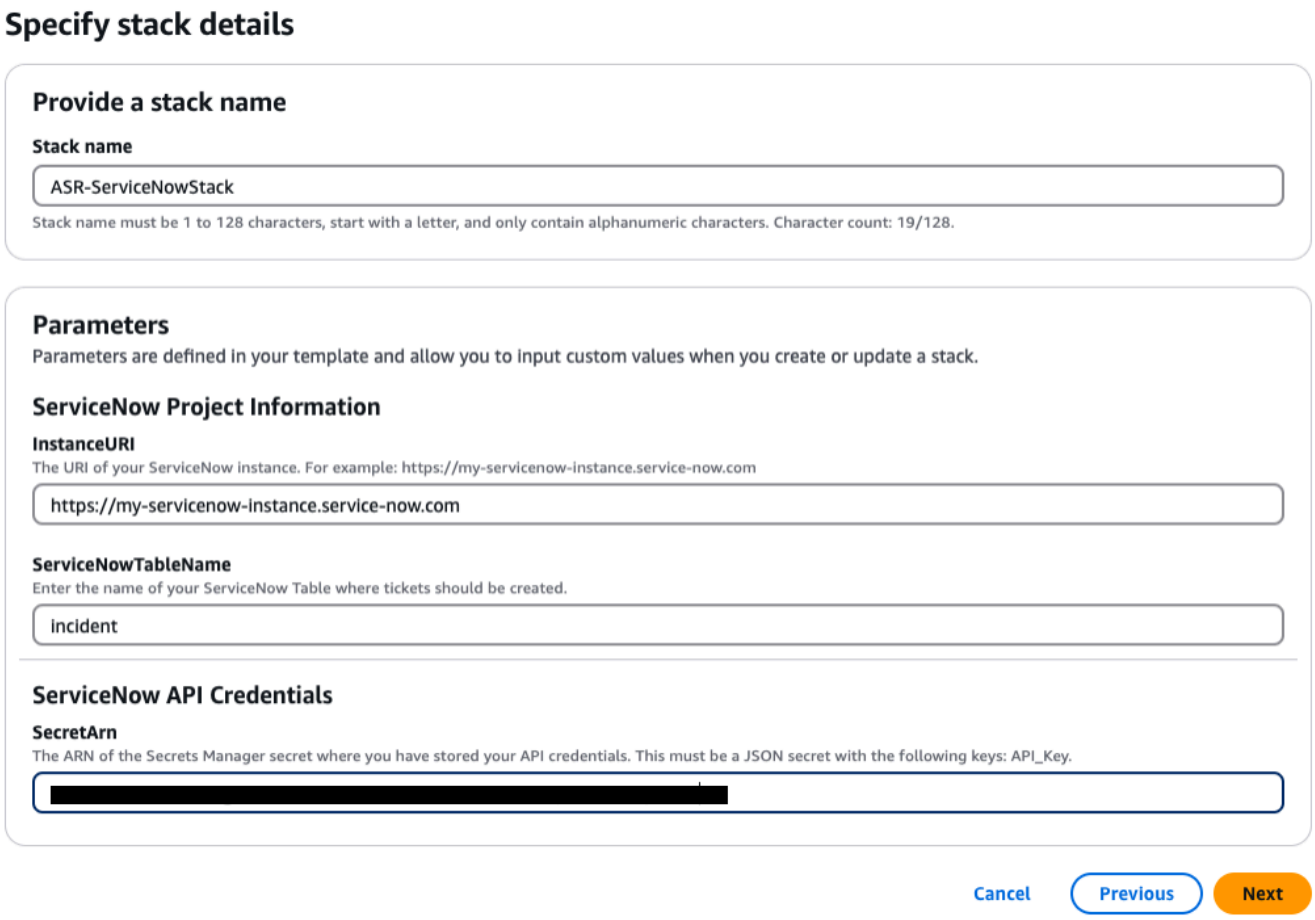
g. Berikan URI ServiceNow instance Anda.

h. Berikan nama ServiceNow tabel Anda.

i. Buat kunci API ServiceNow dengan izin untuk memodifikasi tabel yang ingin Anda tulis.

j. Buat rahasia di Secrets Manager dengan kunci `API_Key` dan berikan ARN rahasia sebagai masukan ke tumpukan.

Berikan informasi ServiceNow proyek nama tumpukan, dan kredensi ServiceNow API.



Untuk membuat tumpukan integrasi kustom: Sertakan fungsi Lambda yang dapat dipanggil oleh Step Functions orkestrator solusi untuk setiap remediasi. Fungsi Lambda harus mengambil input yang disediakan oleh Step Functions, membuat payload sesuai dengan persyaratan sistem tiket Anda, dan membuat permintaan ke sistem Anda untuk membuat tiket.

Langkah 1: Luncurkan tumpukan admin

Important

Solusi ini mencakup opsi untuk mengirim metrik operasional anonim ke AWS. Kami menggunakan data ini untuk lebih memahami bagaimana pelanggan menggunakan solusi ini dan layanan serta produk terkait. AWS memiliki data yang dikumpulkan melalui survei ini. Pengumpulan data tunduk pada Pemberitahuan Privasi AWS.
Untuk memilih keluar dari fitur ini, unduh templat, ubah bagian CloudFormation pemetaan AWS, lalu gunakan CloudFormation konsol AWS untuk mengunggah templat Anda dan

menerapkan solusinya. Untuk informasi lebih lanjut, lihat bagian pengumpulan data anonim dari panduan ini.

CloudFormation Template AWS otomatis ini menerapkan Respons Keamanan Otomatis pada solusi AWS di AWS Cloud. Sebelum Anda meluncurkan tumpukan, Anda harus mengaktifkan Security Hub dan menyelesaikan prasyarat.

> **Note**
>
> Anda bertanggung jawab atas biaya layanan AWS yang digunakan saat menjalankan solusi ini. Untuk detail selengkapnya, kunjungi bagian Biaya dalam panduan ini, dan lihat halaman web harga untuk setiap layanan AWS yang digunakan dalam solusi ini.

1. Masuk ke AWS Management Console dari akun tempat AWS Security Hub saat ini dikonfigurasi, dan gunakan tombol di bawah ini untuk meluncurkan CloudFormation template `automated-security-response-admin.template` AWS.

   Launch solution

   Anda juga dapat mengunduh template sebagai titik awal untuk implementasi Anda sendiri.
2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi ini di Wilayah AWS yang berbeda, gunakan pemilih Wilayah di bilah navigasi AWS Management Console.

   > **Note**
   >
   > Solusi ini menggunakan AWS Systems Manager yang saat ini hanya tersedia di Wilayah AWS tertentu. Solusinya bekerja di semua Wilayah yang mendukung layanan ini. Untuk ketersediaan terbaru menurut Wilayah, lihat Daftar Layanan Regional AWS.
3. Pada halaman Buat tumpukan, verifikasi bahwa URL templat yang benar ada di kotak teks URL Amazon S3 lalu pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat batas IAM dan STS di Panduan Pengguna AWS Identity and Access Management.

5. Pada halaman Parameter, pilih Berikutnya.

Parameter	Default	Deskripsi
Muat Tumpukan Admin SC	`yes`	Tentukan apakah akan menginstal komponen admin untuk remediasi otomatis kontrol SC.
Muat Tumpukan Admin AFSBP	no	Tentukan apakah akan menginstal komponen admin untuk remediasi otomatis kontrol FSBP.
Muat CIS12 0 Tumpukan Admin	no	Tentukan apakah akan menginstal komponen admin untuk remediasi otomatis CIS12 0 kontrol.
Muat CIS14 0 Tumpukan Admin	no	Tentukan apakah akan menginstal komponen admin untuk remediasi otomatis CIS14 0 kontrol.
Muat CIS3 00 Tumpukan Admin	no	Tentukan apakah akan menginstal komponen admin untuk remediasi otomatis dari CIS3 00 kontrol.
Muat Tumpukan PC1321 Admin	no	Tentukan apakah akan menginstal komponen admin untuk remediasi PC1321 kontrol otomatis.
Muat Tumpukan Admin NIST	no	Tentukan apakah akan menginstal komponen admin untuk remediasi otomatis kontrol NIST.

Parameter	Default	Deskripsi
Gunakan Kembali Grup Log Orkestrator	no	Pilih apakah akan menggunakan kembali grup `SO0111-ASR-Orchestrator` CloudWatch Log yang ada atau tidak. Ini menyederhanakan instalasi ulang dan upgrade tanpa kehilangan data log dari versi sebelumnya. Gunakan kembali `Orchestrator Log Group` pilihan yang ada `yes` jika `Orchestrator Log Group` masih ada dari penerapan sebelumnya di akun ini, jika tidak. `no` Jika Anda melakukan pembaruan tumpukan dari versi sebelumnya dari v2.3.0 pilih `no`
Gunakan CloudWatch Metrik	`yes`	Tentukan apakah akan mengaktifkan CloudWatch Metrik untuk memantau solusi. Ini akan membuat CloudWatch Dasbor untuk melihat metrik.
Gunakan CloudWatch Alarm Metrik	`yes`	Tentukan apakah akan mengaktifkan CloudWatch Alarm Metrik untuk solusinya. Ini akan membuat Alarm untuk metrik tertentu yang dikumpulkan oleh solusi.

Parameter	Default	Deskripsi
RemediationFailure AlarmThreshold	5	Tentukan ambang batas untuk persentase kegagalan remediasi per ID kontrol. Misalnya, jika Anda masuk5, Anda menerima alarm jika ID kontrol gagal lebih dari 5% perbaikan pada hari tertentu. Parameter ini hanya berfungsi jika alarm dibuat (lihat parameter Use CloudWatch Metrics Alarms).
EnableEnhancedClou dWatchMetrics	no	Jika`yes`, buat CloudWatc h metrik tambahan untuk melacak semua kontrol IDs satu per satu di CloudWatc h dasbor dan sebagai CloudWatch alarm. Lihat bagian Biaya untuk memahami biaya tambahan yang ditimbulkannya.
TicketGenFunctionName	(Masukan opsional)	Opsional. Biarkan kosong jika Anda tidak ingin menginteg rasikan sistem tiket. Jika tidak, berikan nama fungsi Lambda dari output tumpukan Langkah 0, misalnya:. `SO0111-ASR-Service Now-TicketGenerator`

Parameter	Default	Deskripsi
TargetAccountIDs	`ALL`	Daftar akun AWS IDs untuk mengontrol ruang lingkup remediasi otomatis. Gunakan “SEMUA” untuk menargetkan semua akun di organisasi. Atau berikan daftar Akun AWS 12 digit yang dipisahkan koma. IDs Contoh: “123456789012,098765432109"
TargetAccountIDsStrategi	`INCLUDE`	Mendefinisikan bagaimana solusi menerapkan remediasi otomatis berdasarkan daftar. TargetAccount IDs TERMASUK: Jalankan remediasi otomatis hanya untuk akun yang terdaftar. KECUALIKAN: Jalankan remediasi otomatis untuk semua akun kecuali yang terdaftar.

> **Note**
>
> Anda harus mengaktifkan remediasi otomatis secara manual di akun Admin setelah menerapkan atau memperbarui tumpukan solusi. CloudFormation

1. Pada halaman Konfigurasikan opsi tumpukan, pilih Berikutnya.

2. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang menyatakan bahwa template akan membuat sumber daya AWS Identity and Access Management (IAM).
3. Pilih Membuat tumpukan untuk menerapkannya.

Anda dapat melihat status tumpukan di CloudFormation konsol AWS di kolom Status. Anda akan menerima status CREATE_COMPLETE dalam waktu sekitar 15 menit.

Langkah 2: Instal peran remediasi ke setiap akun anggota AWS Security Hub

`automated-security-response-member-roles.template` StackSet Harus digunakan hanya di satu Wilayah per akun anggota. Ini mendefinisikan peran global yang memungkinkan panggilan API lintas akun dari fungsi langkah ASR Orchestrator.

1. Masuk ke AWS Management Console untuk setiap akun anggota AWS Security Hub (termasuk akun admin, yang juga merupakan anggota). Pilih tombol untuk meluncurkan CloudFormation template `automated-security-response-member-roles.template` AWS. Anda juga dapat mengunduh template sebagai titik awal untuk implementasi Anda sendiri.

2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi ini di Wilayah AWS yang berbeda, gunakan pemilih Wilayah di bilah navigasi AWS Management Console.
3. Pada halaman Buat tumpukan, verifikasi bahwa URL templat yang benar ada di kotak teks URL Amazon S3 lalu pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat batas IAM dan STS di Panduan Pengguna AWS Identity and Access Management.
5. Pada halaman Parameter, tentukan parameter berikut dan pilih Berikutnya.

Parameter	Default	Deskripsi
Namespace	*<Requires input>*	Masukkan string hingga 9 karakter alfanumerik huruf

Parameter	Default	Deskripsi
		kecil. Namespace unik yang akan ditambahkan sebagai akhiran untuk remediasi nama peran IAM. Namespace yang sama harus digunakan dalam Peran Anggota dan tumpukan Anggota. String ini harus unik untuk setiap penerapan solusi, tetapi tidak perlu diubah selama pembaruan tumpukan. Nilai namespace tidak harus unik per akun anggota.
Admin Akun Sec Hub	*<Requires input>*	Masukkan ID akun 12 digit untuk akun admin AWS Security Hub. Nilai ini memberikan izin ke peran solusi akun admin.

6. Pada halaman Konfigurasikan opsi tumpukan, pilih Berikutnya.
7. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang menyatakan bahwa template akan membuat sumber daya AWS Identity and Access Management (IAM).
8. Pilih Membuat tumpukan untuk menerapkannya.

   Anda dapat melihat status tumpukan di CloudFormation konsol AWS di kolom Status. Anda akan menerima status CREATE_COMPLETE dalam waktu sekitar 5 menit. Anda dapat melanjutkan dengan langkah berikutnya saat tumpukan ini dimuat.

Langkah 3: Luncurkan tumpukan anggota

> **Important**
>
> Solusi ini mencakup opsi untuk mengirim metrik operasional anonim ke AWS. Kami menggunakan data ini untuk lebih memahami bagaimana pelanggan menggunakan solusi

ini dan layanan serta produk terkait. AWS memiliki data yang dikumpulkan melalui survei ini. Pengumpulan data tunduk pada Kebijakan Privasi AWS.
Untuk memilih keluar dari fitur ini, unduh templat, ubah bagian CloudFormation pemetaan AWS, lalu gunakan CloudFormation konsol AWS untuk mengunggah templat Anda dan menerapkan solusinya. Untuk informasi selengkapnya, lihat bagian Pengumpulan metrik operasional dari panduan ini.

`automated-security-response-member`Tumpukan harus diinstal ke setiap akun anggota Security Hub. Tumpukan ini mendefinisikan runbook untuk remediasi otomatis. Admin untuk setiap akun anggota dapat mengontrol remediasi apa yang tersedia melalui tumpukan ini.

1. Masuk ke AWS Management Console untuk setiap akun anggota AWS Security Hub (termasuk akun admin, yang juga merupakan anggota). Pilih tombol untuk meluncurkan CloudFormation template `automated-security-response-member.template` AWS.

   Launch solution

Anda juga dapat mengunduh template sebagai titik awal untuk implementasi Anda sendiri. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi ini di Wilayah AWS yang berbeda, gunakan pemilih Wilayah di bilah navigasi AWS Management Console.

+

> **Note**
>
> Solusi ini menggunakan AWS Systems Manager, yang saat ini tersedia di sebagian besar Wilayah AWS. Solusinya bekerja di semua Wilayah yang mendukung layanan ini. Untuk ketersediaan terbaru menurut Wilayah, lihat Daftar Layanan Regional AWS.

1. Pada halaman Buat tumpukan, verifikasi bahwa URL templat yang benar ada di kotak teks URL Amazon S3 lalu pilih Berikutnya.
2. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat batas IAM dan STS di Panduan Pengguna AWS Identity and Access Management.

3. Pada halaman Parameter, tentukan parameter berikut dan pilih Berikutnya.

Parameter	Default	Deskripsi
Berikan nama yang akan digunakan LogGroup untuk membuat Filter Metrik dan Alarm	*<Requires input>*	Tentukan nama grup CloudWatch Log tempat CloudTrail log panggilan API. Ini digunakan untuk remediasi CIS 3.1-3.14.
Muat Tumpukan Anggota SC	yes	Tentukan apakah akan menginstal komponen anggota untuk remediasi otomatis kontrol SC.
Muat Tumpukan Anggota AFSBP	no	Tentukan apakah akan menginstal komponen anggota untuk remediasi otomatis kontrol FSBP.
Muat CIS12 0 Tumpukan Anggota	no	Tentukan apakah akan menginstal komponen anggota untuk remediasi otomatis CIS12 0 kontrol.
Muat CIS14 0 Tumpukan Anggota	no	Tentukan apakah akan menginstal komponen anggota untuk remediasi otomatis CIS14 0 kontrol.
Muat CIS3 00 Tumpukan Anggota	no	Tentukan apakah akan menginstal komponen anggota untuk remediasi otomatis dari CIS3 00 kontrol.

Parameter	Default	Deskripsi
Muat Tumpukan PC1321 Anggota	no	Tentukan apakah akan menginstal komponen anggota untuk remediasi PC1321 kontrol otomatis.
Muat Tumpukan Anggota NIST	no	Tentukan apakah akan menginstal komponen anggota untuk remediasi otomatis kontrol NIST.
Buat Bucket S3 Untuk Pencatatan Audit Redshift	no	Pilih `yes` apakah bucket S3 harus dibuat untuk remediasi FSBP RedShift .4. Untuk detail bucket S3 dan remediasi, tinjau remediasi Redshift.4 di Panduan Pengguna AWS Security Hub.
Akun Admin Sec Hub	*<Requires input>*	Masukkan ID akun 12 digit untuk akun admin AWS Security Hub.

Parameter	Default	Deskripsi
Namespace	*<Requires input>*	Masukkan string hingga 9 karakter alfanumerik huruf kecil. String ini menjadi bagian dari nama peran IAM dan bucket Action Log S3. Gunakan nilai yang sama untuk penerapan tumpukan anggota dan penerapan tumpukan peran anggota. String harus unik untuk setiap penerapan solusi, tetapi tidak perlu diubah selama pembaruan tumpukan.
EnableCloudTrailFo rASRActionLog	no	Pilih `yes` apakah Anda ingin memantau peristiwa manajemen yang dilakukan oleh solusi di CloudWatch dasbor. Solusinya membuat CloudTrail jejak di setiap akun anggota tempat Anda memilih`yes`. Anda harus menerapkan solusi ke AWS Organization untuk mengaktif kan fitur ini. Lihat bagian Biaya untuk memahami biaya tambahan yang ditimbulk annya.

4. Pada halaman Konfigurasikan opsi tumpukan, pilih Berikutnya.
5. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang menyatakan bahwa template akan membuat sumber daya AWS Identity and Access Management (IAM).
6. Pilih Membuat tumpukan untuk menerapkannya.

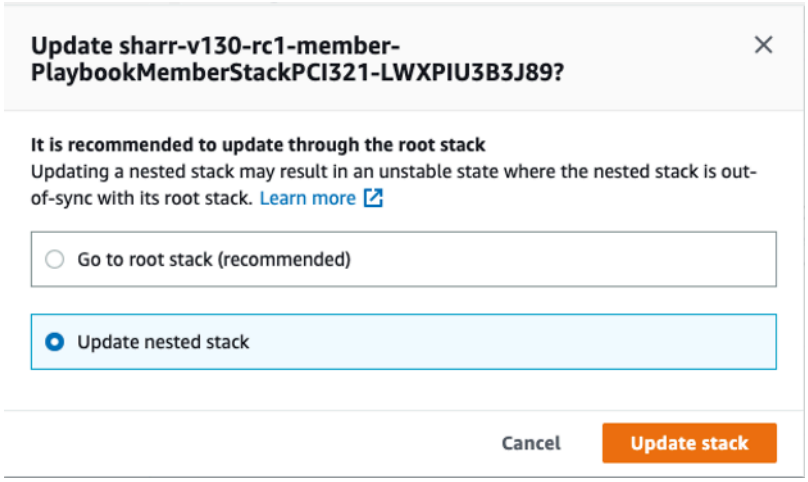
Anda dapat melihat status tumpukan di CloudFormation konsol AWS di kolom Status. Anda akan menerima status CREATE_COMPLETE dalam waktu sekitar 15 menit.

Langkah 4: (Opsional) Sesuaikan remediasi yang tersedia

Jika Anda ingin menghapus remediasi tertentu dari akun anggota, Anda dapat melakukannya dengan memperbarui tumpukan bersarang untuk standar keamanan. Untuk mempermudah, opsi tumpukan bersarang tidak disebarkan ke tumpukan root.

1. Masuk ke CloudFormation konsol AWS dan pilih tumpukan bersarang.
2. Pilih Perbarui.
3. Pilih Perbarui tumpukan bersarang dan pilih Perbarui tumpukan.

   Perbarui tumpukan bersarang



4. Pilih Gunakan templat saat ini dan pilih Berikutnya.
5. Sesuaikan remediasi yang tersedia. Ubah nilai untuk kontrol yang diinginkan ke `Available` dan kontrol yang tidak diinginkan ke`Not available`.

> **Note**
>
> Mematikan remediasi menghilangkan runbook remediasi solusi untuk standar keamanan dan kontrol.

6. Pada halaman Konfigurasikan opsi tumpukan, pilih Berikutnya.
7. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang menyatakan bahwa template akan membuat sumber daya AWS Identity and Access Management (IAM).
8. Pilih Perbarui tumpukan.

Anda dapat melihat status tumpukan di CloudFormation konsol AWS di kolom Status. Anda akan menerima status CREATE_COMPLETE dalam waktu sekitar 15 menit.

Penyebaran Control Tower (CT)

Panduan Kustomisasi untuk AWS Control Tower (CFCT) adalah untuk administrator, DevOps profesional, vendor perangkat lunak independen, arsitek infrastruktur TI, dan integrator sistem yang ingin menyesuaikan dan memperluas lingkungan AWS Control Tower mereka untuk perusahaan dan pelanggan mereka. Ini memberikan informasi tentang menyesuaikan dan memperluas lingkungan AWS Control Tower dengan paket kustomisasi CFCT.

Waktu untuk menyebarkan: Sekitar 30 menit

Prasyarat

Sebelum menerapkan solusi ini, pastikan solusi ini ditujukan untuk administrator AWS Control Tower.

Saat Anda siap menyiapkan landing zone menggunakan konsol AWS Control Tower atau APIs, ikuti langkah-langkah berikut:

Untuk memulai AWS Control Tower, lihat: Memulai AWS Control Tower

Untuk mempelajari cara menyesuaikan landing zone Anda, lihat: Menyesuaikan Zona Landing Anda

Untuk meluncurkan dan menerapkan landing zone Anda, lihat: Panduan Penyebaran Zona Landing

Ikhtisar penyebaran

Gunakan langkah-langkah berikut untuk menerapkan solusi ini di AWS.

Langkah 1: Bangun dan terapkan bucket S3

> **Note**
>
> Konfigurasi bucket S3 - hanya untuk ADMIN. Ini adalah langkah pengaturan satu kali dan tidak boleh diulang oleh pengguna akhir. Bucket S3 menyimpan paket penerapan, termasuk template AWS CloudFormation dan kode Lambda yang diperlukan agar ASR dapat dijalankan. Sumber daya ini digunakan menggunakan CfCt atau StackSet.

1. Konfigurasikan Bucket S3

Siapkan bucket S3 yang akan digunakan untuk menyimpan dan melayani paket penerapan Anda.

2. Siapkan Lingkungan

Siapkan variabel lingkungan yang diperlukan, kredensi, dan alat yang diperlukan untuk proses build dan deployment.

3. Konfigurasikan Kebijakan Bucket S3

Tentukan dan terapkan kebijakan bucket yang sesuai untuk mengontrol akses dan izin.

4. Siapkan Build

Kompilasi, paket, atau persiapkan aplikasi atau aset Anda untuk penerapan.

5. Menyebarkan Paket ke S3

Unggah artefak build yang sudah disiapkan ke bucket S3 yang ditentukan.

Langkah 2: Menumpuk penyebaran ke AWS Control Tower

1. Buat Manifes Build untuk Komponen ASR

Tentukan manifes build yang mencantumkan semua komponen ASR, versinya, dependensi, dan instruksi build.

2. Perbarui CodePipeline

Ubah CodePipeline konfigurasi AWS untuk menyertakan langkah, artefak, atau tahapan build baru yang diperlukan untuk menerapkan komponen ASR.

Langkah 1: Bangun dan terapkan ke bucket S3

AWS Solutions menggunakan dua bucket: bucket untuk akses global ke template, yang diakses melalui HTTPS, dan bucket regional untuk akses ke aset di wilayah tersebut, seperti kode Lambda.

1. Konfigurasikan Bucket S3

Pilih nama bucket yang unik, misalnya asr-staging. Tetapkan dua variabel lingkungan di terminal Anda, satu harus menjadi nama bucket dasar dengan -reference sebagai akhiran, yang lain dengan wilayah penerapan yang Anda inginkan sebagai akhiran:

```
export BASE_BUCKET_NAME=asr-staging-$(date +%s)
export TEMPLATE_BUCKET_NAME=$BASE_BUCKET_NAME-reference
```

```
export REGION=us-east-1
export ASSET_BUCKET_NAME=$BASE_BUCKET_NAME-$REGION
```

2. Pengaturan Lingkungan

Di akun AWS Anda, buat dua bucket dengan nama-nama ini, misalnya asr-staging-reference dan asr-staging-us-east -1. (Bucket referensi akan menampung CloudFormation template, bucket regional akan menampung semua aset lain seperti bundel kode lambda.) Bucket Anda harus dienkripsi dan melarang akses publik

```
aws s3 mb s3://$TEMPLATE_BUCKET_NAME/
aws s3 mb s3://$ASSET_BUCKET_NAME/
```

> **Note**
>
> Saat membuat ember Anda, pastikan mereka tidak dapat diakses publik. Gunakan nama bucket acak. Nonaktifkan akses publik. Gunakan enkripsi KMS. Dan verifikasi kepemilikan bucket sebelum mengunggah.

3. Pengaturan kebijakan bucket S3

Perbarui kebijakan bucket $TEMPLATE_BUCKET_NAME S3 untuk menyertakan izin untuk mengeksekusi ID akun. PutObject Tetapkan izin ini ke peran IAM dalam akun eksekusi yang diizinkan untuk menulis ke bucket. Pengaturan ini memungkinkan Anda menghindari pembuatan bucket di akun Manajemen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::<template bucket name>/*",
                "arn:aws:s3:::<template bucket name>"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "<org id>"
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::<template bucket name>/*",
                "arn:aws:s3:::<template bucket name>"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
            }
        }
    ]
}
```

Ubah kebijakan bucket aset S3 untuk menyertakan izin. Tetapkan izin ini ke peran IAM dalam akun eksekusi yang diizinkan untuk menulis ke bucket. Ulangi pengaturan ini untuk setiap bucket aset regional (misalnya, asr-staging-us-east asr-staging-eu-west -1, -1, dll.), yang memungkinkan penerapan di beberapa wilayah tanpa perlu membuat bucket di akun Manajemen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "<org id>"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
            "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
            }
        }
    ]
}
```

4. Membangun Persiapan

- Prasyarat:
  - AWS CLI v2
  - Python 3.11+ dengan pip
  - AWS CDK 2.171.1+
  - Node.js 20+ dengan npm
  - Puisi v2 dengan plugin untuk diekspor
- Git klon https://github.com/aws-solutions/ automated-security-response-on -aws.git

Pertama pastikan bahwa Anda telah menjalankan npm install di folder sumber.

Selanjutnya dari folder penerapan di repo kloning Anda, jalankan build-s3-dist.sh, berikan nama root bucket Anda (mis. mybucket) dan versi yang Anda buat (mis. v1.0.0). Kami merekomendasikan menggunakan versi semver berdasarkan versi yang diunduh dari GitHub (mis. GitHub: v1.0.0, build Anda: v1.0.0.mybuild)

```
chmod +x build-s3-dist.sh
export SOLUTION_NAME=automated-security-response-on-aws
export SOLUTION_VERSION=v1.0.0.mybuild
./build-s3-dist.sh -b $BASE_BUCKET_NAME -v $SOLUTION_VERSION
```

5. Menyebarkan paket ke S3

```
cd deployment
aws s3 cp global-s3-assets/  s3://$TEMPLATE_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
aws s3 cp regional-s3-assets/  s3://$ASSET_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
```

Langkah 2: Menumpuk penyebaran ke AWS Control Tower

1. Membangun manifes untuk komponen ASR

Setelah menerapkan artefak ASR ke bucket S3, perbarui manifes pipeline Control Tower untuk mereferensikan versi baru, lalu memicu proses pipeline, lihat: deployment controltower

> **Important**
>
> Untuk memastikan penerapan solusi ASR yang benar, lihat dokumentasi AWS resmi untuk informasi terperinci tentang ikhtisar CloudFormation templat dan deskripsi parameter. Tautan info di bawah ini: Panduan ikhtisar Parameter CloudFormation Template

Manifes untuk komponen ASR terlihat seperti ini:

```
region: us-east-1 #<HOME_REGION_NAME>
version: 2021-03-15

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDsStrategy
        parameter_value: "INCLUDE"
```

```
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDs
        parameter_value: "ALL"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

  - name:  <ROLE MEMBER STACK NAME>
    resource_file: s3://<ROLE MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
    deploy_method: stack_set
    deployment_targets:
      organizational_units:
        - <ORG UNIT>

  - name:  <MEMBER STACK NAME>
    resource_file: s3://<MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
```

```
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: LoadCIS120MemberStack
        parameter_value: "no"
      - parameter_key: LoadNIST80053MemberStack
        parameter_value: "no"
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
      - parameter_key: CreateS3BucketForRedshiftAuditLogging
        parameter_value: "no"
      - parameter_key: LoadAFSBPMemberStack
        parameter_value: "no"
      - parameter_key: LoadSCMemberStack
        parameter_value: "yes"
      - parameter_key: LoadPCI321MemberStack
        parameter_value: "no"
      - parameter_key: LoadCIS140MemberStack
        parameter_value: "no"
      - parameter_key: EnableCloudTrailForASRActionLog
        parameter_value: "no"
      - parameter_key: LogGroupName
        parameter_value: <LOG_GROUP_NAME>
      - parameter_key: LoadCIS300MemberStack
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    organizational_units:
      - <ORG UNIT>
    regions: # :type: list
      - <REGION_NAME>
```

2. Pembaruan pipa kode

Tambahkan file manifes custom-control-tower-configuration ke.zip dan jalankan CodePipeline, lihat: ikhtisar pipa kode

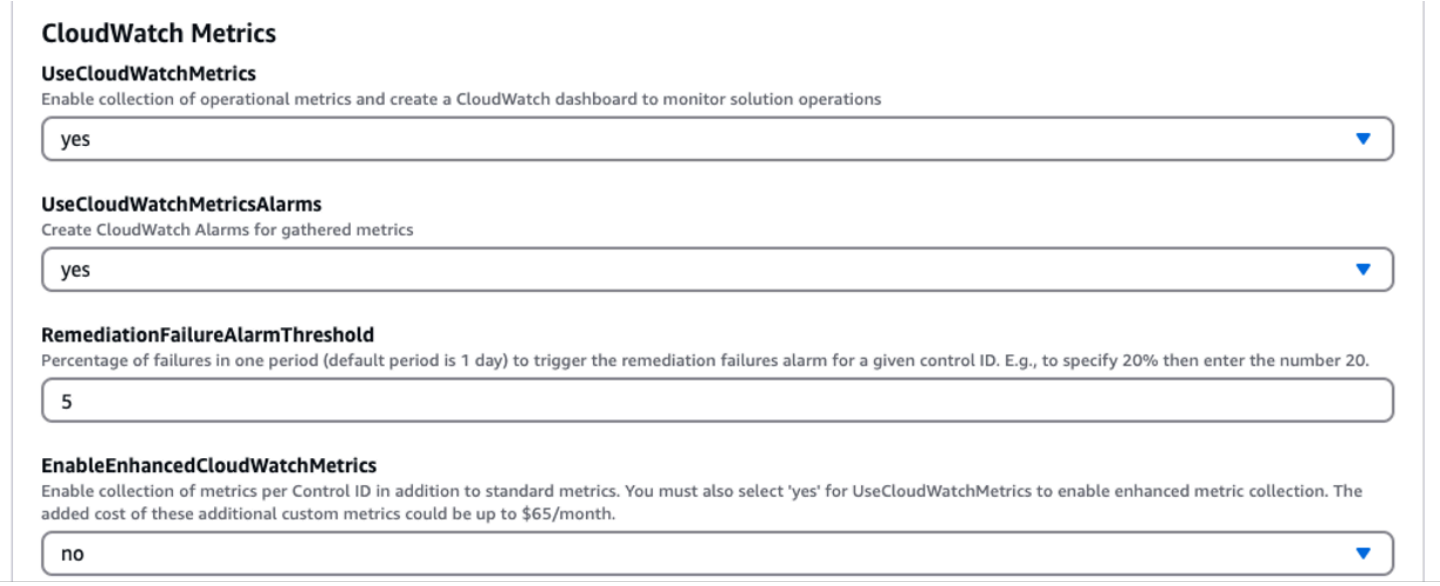
Pantau operasi solusi dengan CloudWatch dasbor Amazon

Solusi ini mencakup metrik dan alarm khusus yang ditampilkan di dasbor Amazon CloudWatch .

CloudWatch Dasbor dan alarm memantau operasi solusi dan peringatan ketika ada potensi masalah.

Mengaktifkan CloudWatch metrik, alarm, dan dasbor

Ada empat parameter CloudFormation template untuk CloudWatch fungsionalitas.



1. UseCloudWatchMetrics- Mengatur ini untuk `yes` memungkinkan pengumpulan metrik operasional dan membuat CloudWatch dasbor untuk melihat metrik ini.
2. UseCloudWatchAlarms- Mengatur ini untuk `yes` mengaktifkan alarm default solusi.
3. RemediationFailureAlarmThreshold- Persentase remediasi yang gagal dalam suatu periode untuk menaikkan alarm.
4. EnableEnhancedCloudWatchMetrics- Atur parameter ini `yes` untuk mengumpulkan metrik individual per ID kontrol. Secara default, parameter ini disetel keno, sehingga hanya metrik pada jumlah total remediasi di semua kontrol IDs yang dikumpulkan. Metrik dan alarm individual per ID kontrol dikenakan biaya tambahan.

Menggunakan CloudWatch dasbor

Untuk melihat dasbor:

1. Arahkan ke Amazon CloudWatch dan kemudian Dasbor.
2. Pilih dasbor bernama “ASR-remediation-metrics-dashboard”.

CloudWatch Dasbor berisi bagian-bagian berikut:

1. Total Successful Remediations - Memberi Anda wawasan tentang jumlah temuan Security Hub yang telah berhasil diperbaiki oleh solusi.
2. Kegagalan Remediasi - Menunjukkan berapa banyak remediasi telah gagal, baik secara total maupun sebagai persentase, dan penyebab kegagalan. Sejumlah besar kegagalan dapat mengisyaratkan masalah teknis dengan solusi yang mungkin perlu Anda selidiki secara lebih rinci.
3. Keberhasilan/Kegagalan Remediasi berdasarkan ID Kontrol - Jika Anda mengaktifkan Metrik yang Ditingkatkan pada waktu penerapan, bagian ini mencantumkan hasil remediasi berdasarkan ID kontrol. Ketika bagian Kegagalan Remediasi menunjukkan tingkat kegagalan yang tinggi secara umum, bagian ini menunjukkan kepada Anda apakah kegagalan didistribusikan di banyak kontrol IDs, atau jika hanya kontrol tertentu IDs yang gagal.
4. Runbook Mengasumsikan Kegagalan Peran - Menunjukkan jumlah kegagalan yang terjadi karena upaya remediasi di akun yang tidak memiliki solusi Peran anggota diinstal. Kegagalan berulang oleh upaya remediasi otomatis karena peran yang hilang menyebabkan biaya yang tidak perlu. Mengurangi hal ini dengan menginstal tumpukan peran Anggota di akun terkait, menonaktifkan semua EventBridge aturan yang dibuat oleh solusi, atau memisahkan akun di Security Hub.
5. Cloud Trail Management Actions by ASR - Mencantumkan tindakan manajemen berdasarkan solusi di semua akun anggota tempat Anda mengaktifkan Log Tindakan dengan parameter EnableCloudTrailForASRActionLog pada waktu penerapan. Saat Anda mengamati perubahan sumber daya yang tidak terduga di salah satu akun AWS Anda, widget ini dapat membantu Anda memahami apakah sumber daya dimodifikasi oleh solusi.

CloudWatch Dasbor juga dilengkapi dengan alarm yang telah ditentukan yang memperingatkan kesalahan operasional umum.

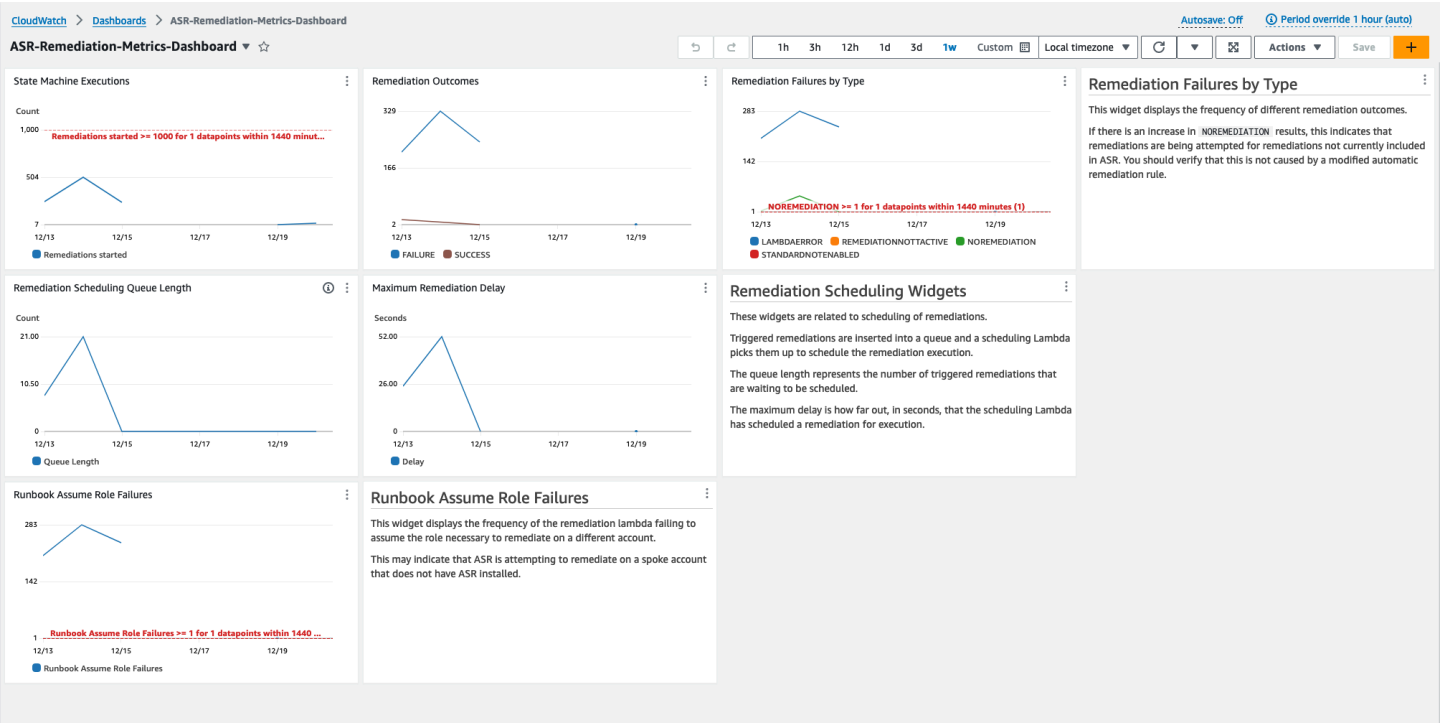
1. Eksekusi State Machine > 1000 dalam periode 24 jam.
   a. Lonjakan besar dalam eksekusi remediasi dapat mengindikasikan aturan peristiwa dimulai lebih sering daripada yang dimaksudkan.
   b. Ambang batas dapat diubah menggunakan CloudFormation parameter.
2. Kegagalan Remediasi berdasarkan Jenis = NOREMEDIASI > 0

a. Remediasi sedang dicoba untuk remediasi yang tidak termasuk dalam ASR. Ini bisa menunjukkan aturan acara telah dimodifikasi untuk memasukkan lebih dari perbaikan yang dimaksudkan.

3. Runbook Asumsikan Kegagalan Peran> 0

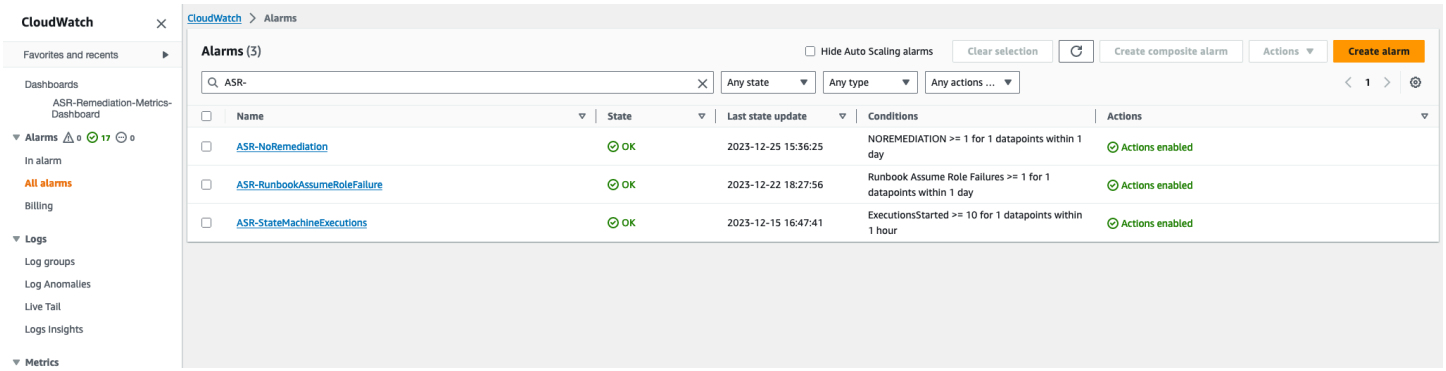
a. Remediasi sedang dicoba di akun atau Wilayah yang tidak memiliki solusi yang diterapkan dengan benar. Ini bisa menunjukkan aturan acara telah dimodifikasi untuk menyertakan lebih banyak akun daripada yang dimaksudkan.

Semua ambang alarm dapat dimodifikasi agar sesuai dengan kebutuhan penyebaran individu.

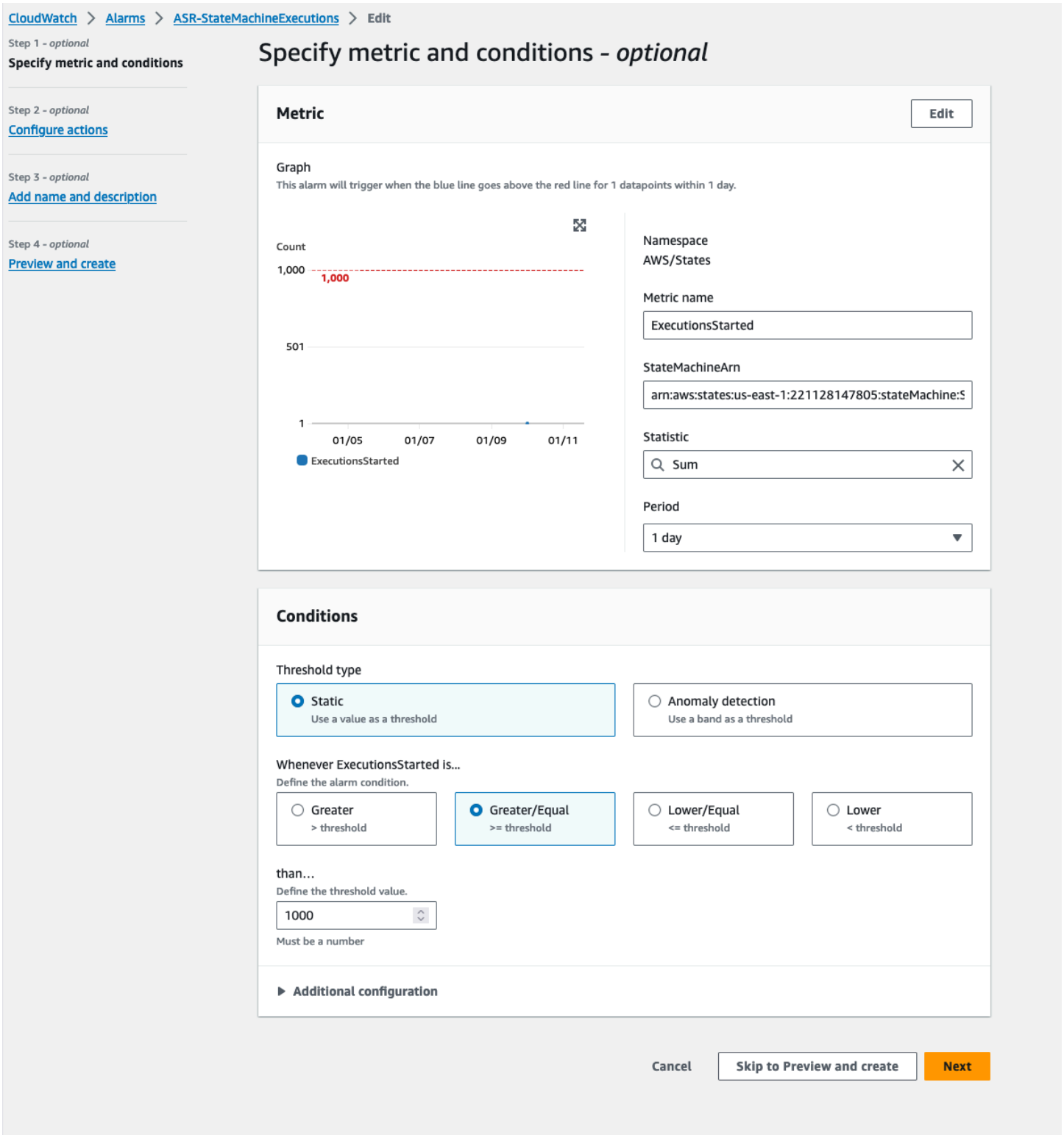


Memodifikasi ambang alarm

1. Arahkan ke Amazon CloudWatch → Alarm → Semua Alarm.
2. Pilih Alarm yang ingin Anda ubah, lalu pilih Tindakan → Edit.



1. Ubah ambang batas ke nilai yang diinginkan dan simpan.



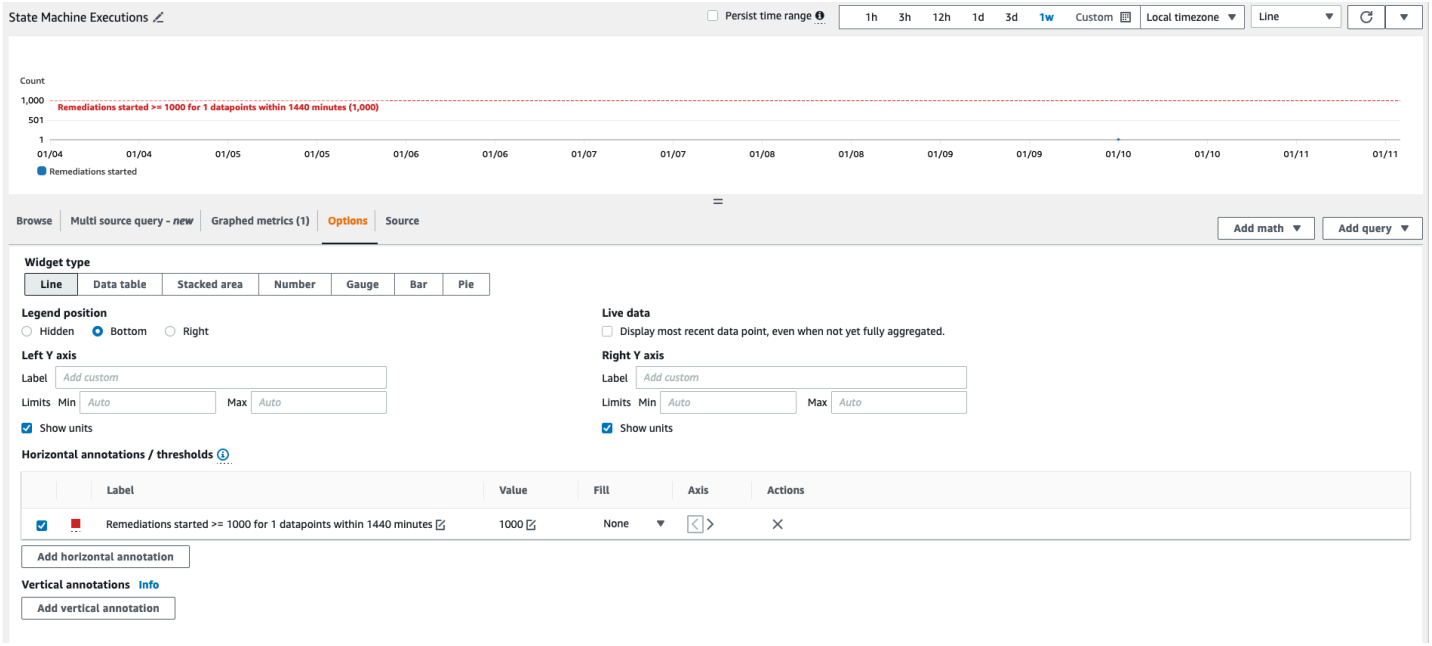
1. Arahkan ke CloudWatch dasbor untuk memodifikasi bagan di sana agar sesuai dengan pengaturan baru.

   a. Pilih elipsis di kanan atas widget yang sesuai.

b. Pilih Edit.

c. Ubah ke tab Opsi.

d. Ubah anotasi Alarm agar sesuai dengan pengaturan baru.



Berlangganan notifikasi Alarm

Di akun admin, berlangganan topik Amazon SNS yang dibuat oleh tumpukan admin, SO0111-ASR_Alarm_topic. Ini akan memberi tahu Anda ketika alarm memasuki status ALARM.

Perbarui solusinya

Memutakhirkan dari versi sebelum v1.4

Jika sebelumnya Anda telah menerapkan solusi sebelum v1.4.x, hapus instalan, lalu instal versi terbaru:

1. Copot pemasangan solusi yang digunakan sebelumnya. Lihat Uninstall solusinya.
2. Luncurkan template terbaru. Lihat Menyebarkan solusinya.

> **Note**
>
> Jika Anda memutakhirkan dari v1.2.1 atau sebelumnya ke v1.3.0 atau yang lebih baru, atur Gunakan Grup Log Orkestrator yang ada ke. No Jika Anda menginstal ulang v1.3.0 atau yang lebih baru, Anda dapat Yes memilih opsi ini. Opsi ini memungkinkan Anda untuk terus masuk ke Grup Log yang sama untuk Orchestrator Step Functions.

Upgrade dari v1.4 dan yang lebih baru

Jika Anda memutakhirkan dari v1.4.x, perbarui semua tumpukan atau sebagai berikut: StackSets

1. Perbarui tumpukan di akun admin Security Hub menggunakan template terbaru.
2. Di setiap akun anggota, perbarui izin dari template terbaru.
3. Di setiap akun anggota di semua Wilayah yang saat ini digunakan, perbarui tumpukan anggota dari templat terbaru.

Memutakhirkan dari v2.0.x

Jika Anda memutakhirkan dari v2.0.x, tingkatkan ke v2.1.2 atau yang lebih baru. Memperbarui ke v2.1.0 - v2.1.1 akan gagal di. CloudFormation

> **Note**
>
> - Saat memperbarui solusi, aturan remediasi otomatis mungkin perlu diaktifkan kembali secara manual di akun Admin. Lihat Aktifkan remediasi yang sepenuhnya otomatis.

- Jika Anda menggunakan `Reuse Orchestrator Log Group` parameter untuk menyimpan log, pastikan itu diatur dengan tepat selama pembaruan tumpukan untuk menghindari rekreasi grup log atau hilangnya pengaturan penyimpanan log. Lihat Menyebarkan solusinya. Jika Anda melakukan pembaruan tumpukan ke v2.3.0+dari versi sebelumnya pilih “tidak”

Pemecahan Masalah

Resolusi masalah yang diketahui memberikan instruksi untuk mengurangi kesalahan yang diketahui. Jika petunjuk ini tidak mengatasi masalah Anda, Hubungi AWS Support memberikan petunjuk untuk membuka kasus AWS Support untuk solusi ini.

Log solusi

Bagian ini mencakup informasi Pemecahan masalah untuk solusi ini, lihat navigasi kiri untuk topik.

Solusi ini mengumpulkan output dari runbook remediasi, yang berjalan di bawah AWS Systems Manager, dan mencatat hasilnya ke grup Log `SO0111-ASR` di CloudWatch akun admin AWS Security Hub. Ada satu aliran per kontrol per hari.

Step Functions Orchestrator mencatat semua transisi langkah ke Grup `SO0111-ASR-Orchestrator` CloudWatch Log di akun admin AWS Security Hub. Log ini adalah jejak audit untuk merekam transisi status untuk setiap instance Step Functions. Ada satu aliran log per eksekusi Step Functions.

Kedua grup log dienkripsi menggunakan AWS KMS Customer-Manager Key (CMK).

Informasi pemecahan masalah berikut menggunakan grup `SO0111-ASR` log. Gunakan log ini, serta konsol AWS Systems Manager Automation, log Eksekusi Otomasi, konsol Fungsi Langkah, dan log Lambda untuk memecahkan masalah.

Jika remediasi gagal, pesan yang mirip dengan berikut ini akan dicatat `SO0111-ASR` di aliran log untuk standar, kontrol, dan tanggal. Misalnya: CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

Pesan-pesan berikut memberikan detail tambahan. Output ini berasal dari runbook ASR untuk standar keamanan dan kontrol. Misalnya: ASR-CIS_1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

Informasi ini mengarahkan Anda ke kegagalan, yang dalam hal ini adalah otomatisasi anak yang berjalan di akun anggota. Untuk mengatasi masalah ini, Anda harus masuk ke AWS Management Console di akun anggota (dari pesan di atas), buka AWS Systems Manager, buka Automation, dan periksa keluaran log untuk ID Eksekusi. `eecdef79-9111-4532-921a-e098549f525`

Resolusi masalah yang diketahui

- Masalah: Penerapan solusi gagal dengan kesalahan yang menyatakan bahwa sumber daya sudah tersedia di Amazon. CloudWatch

  Resolusi: Periksa pesan kesalahan di bagian CloudFormation sumber daya/peristiwa yang menunjukkan grup log sudah ada. Template penerapan ASR memungkinkan penggunaan kembali grup log yang ada. Verifikasi bahwa Anda telah memilih penggunaan kembali.

- Masalah: Solusi gagal diterapkan dengan kesalahan di tumpukan bersarang buku pedoman di mana EventBridge Aturan gagal dibuat

  Resolusi: Anda mungkin telah mencapai kuota untuk EventBridge aturan dengan jumlah buku pedoman yang digunakan. Anda dapat menghindari hal ini dengan menggunakan temuan kontrol Konsolidasi di Security Hub yang dipasangkan dengan buku pedoman SC dalam solusi ini, hanya menerapkan buku pedoman untuk standar yang digunakan, atau meminta peningkatan kuota aturan. EventBridge

- Masalah: Saya menjalankan Security Hub di beberapa Wilayah di akun yang sama. Saya ingin menerapkan solusi ini di beberapa Wilayah.

  Resolusi: Terapkan tumpukan admin di akun dan Wilayah yang sama dengan admin Security Hub Anda. Instal template anggota ke setiap akun dan Wilayah tempat Anda memiliki anggota Security Hub yang dikonfigurasi. Aktifkan agregasi di Security Hub.

- Masalah: Segera setelah penerapan, SO0111-ASR-Orchestrator gagal dalam Status Dokumen Otomasi Dapatkan dengan kesalahan 502: “`Lambda tidak dapat mendekripsi variabel lingkungan karena akses KMS ditolak. Silakan periksa pengaturan tombol KMS fungsi. Pengecualian KMS: Pesan UnrecognizedClientException KMS: Token keamanan yang disertakan dalam permintaan tidak valid. (Layanan: AWSLambda; Kode Status: 502; Kode Kesalahan: KMSAccessDeniedException; Permintaan ID:... `”

Resolusi: Biarkan solusi sekitar 10 menit untuk menstabilkan sebelum menjalankan remediasi. Jika masalah berlanjut, buka tiket dukungan atau GitHub masalah.

- Masalah: Saya mencoba memulihkan temuan tetapi tidak ada yang terjadi.

  Resolusi: Periksa catatan temuan untuk alasan mengapa itu tidak diperbaiki. Penyebab umum adalah bahwa temuan tersebut tidak memiliki remediasi otomatis. Saat ini tidak ada cara untuk memberikan umpan balik langsung kepada pengguna ketika tidak ada perbaikan selain melalui catatan. Tinjau log solusi. Buka CloudWatch Log di konsol. Temukan Grup Log CloudWatch SO0111-ASR. Urutkan daftar sehingga aliran yang paling baru diperbarui muncul terlebih dahulu. Pilih aliran log untuk temuan yang Anda coba jalankan. Anda harus menemukan kesalahan di sana. Beberapa alasan kegagalan dapat berupa: ketidakcocokan antara menemukan kontrol dan kontrol remediasi, remediasi lintas akun (belum didukung), atau bahwa temuan tersebut telah diperbaiki. Jika tidak dapat menentukan alasan kegagalan, harap kumpulkan log dan buka tiket dukungan.

- Masalah: Setelah memulai remediasi, status di konsol Security Hub belum diperbarui.

  Resolusi: Konsol Security Hub tidak diperbarui secara otomatis. Segarkan tampilan saat ini. Status temuan harus diperbarui. Mungkin perlu beberapa jam untuk temuan beralih dari Gagal ke Lulus. Temuan dibuat dari data peristiwa yang dikirim oleh layanan lain, seperti AWS Config, ke AWS Security Hub. Waktu sebelum aturan dievaluasi kembali tergantung pada layanan yang mendasarinya. Jika ini tidak menyelesaikan masalah, lihat resolusi sebelumnya untuk “`Saya mencoba memperbaiki temuan tetapi tidak ada yang terjadi. `”

- Masalah: Fungsi langkah orkestrator gagal di Dapatkan Status Dokumen Otomasi: Terjadi kesalahan (AccessDenied) saat memanggil operasi. AssumeRole

  Resolusi: Template anggota belum diinstal di akun anggota tempat ASR mencoba memulihkan temuan. Ikuti instruksi untuk penyebaran template anggota.

- Masalah: Runbook Config.1 gagal karena Recorder atau Delivery Channel sudah ada.

  Resolusi: Periksa pengaturan AWS Config Anda dengan cermat untuk memastikan Config diatur dengan benar. Remediasi otomatis tidak dapat memperbaiki pengaturan AWS Config yang ada dalam beberapa kasus.

- Masalah: Remediasi berhasil tetapi mengembalikan pesan `"No output available yet because the step is not successfully executed."`

Resolusi: Ini adalah masalah yang diketahui dalam rilis ini di mana runbook remediasi tertentu tidak mengembalikan respons. Runbook remediasi akan gagal dengan benar dan memberi sinyal solusi jika tidak berfungsi.

- Masalah: Resolusi gagal dan mengirim jejak tumpukan.

  Resolusi: Terkadang, kami kehilangan kesempatan untuk menangani kondisi kesalahan yang menghasilkan jejak tumpukan daripada pesan kesalahan. Mencoba memecahkan masalah dari data jejak. Buka tiket dukungan jika Anda membutuhkan bantuan.

- Masalah: Penghapusan tumpukan v1.3.0 gagal pada sumber daya Tindakan Kustom.

  Resolusi: Penghapusan template admin mungkin gagal pada penghapusan Tindakan Kustom. Ini adalah masalah yang diketahui yang akan diperbaiki di rilis berikutnya. Jika ini terjadi:

  a. Masuk ke konsol manajemen AWS Security Hub.
  b. Di akun admin, buka Pengaturan.
  c. Pilih tab Tindakan kustom
  d. Hapus entri secara manual Remediate dengan ASR.
  e. Hapus tumpukan lagi.

- Masalah: Setelah menerapkan kembali tumpukan admin, fungsi langkah gagal. `AssumeRole`

  Resolusi: Menerapkan kembali tumpukan admin memutuskan hubungan kepercayaan antara peran admin di akun admin dan peran anggota di akun anggota. Anda harus menerapkan kembali tumpukan peran anggota di semua akun anggota.

- Masalah: Remediasi CIS 3.x tidak muncul `PASSED` setelah lebih dari 24 jam.

  Resolusi: Ini adalah kejadian umum jika Anda tidak memiliki langganan ke topik `SO0111-ASR_LocalAlarmNotification` SNS di akun anggota.

Masalah dengan remediasi khusus

Setel SSLBucket Kebijakan gagal dengan AccessDenied kesalahan

Kontrol terkait: AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI.S3.5, CIS v1.4.0 2.1.2, SC v2.0.0 S3.5

Masalah: SSLBucket Kebijakan Set gagal dengan AccessDenied kesalahan:

Terjadi kesalahan (AccessDenied) saat memanggil PutBucketPolicy operasi: Akses Ditolak

Jika setelan Blokir Akses Publik telah diaktifkan untuk bucket, mencoba untuk menempatkan kebijakan bucket yang menyertakan pernyataan yang memungkinkan akses publik gagal dengan kesalahan ini. Status ini dapat dicapai dengan meletakkan kebijakan bucket yang berisi pernyataan tersebut, lalu mengaktifkan blok akses publik untuk bucket tersebut.

Remediasi Configures3 BucketPublicAccessBlock (kontrol terkait: AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI.S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2) juga dapat menempatkan bucket ke status ini karena menetapkan setelan blok akses publik tanpa mengubah kebijakan bucket.

SSLBucketKebijakan Set menambahkan pernyataan ke kebijakan bucket untuk menolak permintaan yang tidak menggunakan SSL. Itu tidak mengubah pernyataan lain dalam kebijakan, jadi jika ada pernyataan yang memungkinkan akses publik, remediasi akan gagal mencoba untuk menempatkan bucket polic yang dimodifikasi yang masih menyertakan pernyataan tersebut.

Resolusi: Ubah kebijakan bucket untuk menghapus pernyataan yang memungkinkan akses publik bertentangan dengan setelan blokir akses publik di bucket.

putS3 gagal BucketPolicyDeny

Kontrol terkait: AWS FSBP v1.0.0 S3.6, NIST.800-53.r5 CA-9 (1), Nist.800-53.r5 CM-2

Masalah: PUTS3 BucketPolicyDeny dengan kesalahan berikut:

```
Unable to create an explicit deny statement for {bucket_name}.
```

Jika prinsip untuk semua kebijakan pada bucket target adalah “*”, solusinya tidak dapat menambahkan kebijakan penolakan ke keranjang target karena akan memblokir semua tindakan bucket untuk semua prinsip.

Resolusi: Ubah kebijakan bucket untuk mengizinkan tindakan ke akun tertentu alih-alih menggunakan prinsip “*” dan batasi tindakan yang ditolak.

Cara menonaktifkan solusinya

Jika terjadi insiden, Anda mungkin menemukan bahwa Anda perlu menonaktifkan solusi tanpa menghapus infrastruktur apa pun. Skenario ini merinci cara menonaktifkan komponen yang berbeda dalam solusi.

Skenario 1: Nonaktifkan remediasi otomatis untuk satu kontrol.

1. Arahkan ke EventBridge CloudFormation konsol AWS.
2. Pilih Aturan di sidebar.
3. Pilih bus acara default dan cari kontrol yang ingin Anda nonaktifkan.
4. Pilih pada aturan dan pilih tombol Nonaktifkan.

Skenario 2: Nonaktifkan remediasi otomatis untuk semua kontrol.

1. Arahkan ke EventBridge di konsol.
2. Pilih Aturan di sidebar.
3. Pilih bus acara “default” dan pilih semua aturan di bawah ini.
4. Pilih pada tombol “Nonaktifkan”. Perhatikan bahwa Anda mungkin harus melakukan ini untuk beberapa halaman aturan.

Skenario 3: Nonaktifkan remediasi manual untuk akun

1. Arahkan ke EventBridge di konsol.
2. Pilih Aturan di sidebar.
3. Pilih bus acara “default” dan cari “CustomActionRemediate_with_ASR_”
4. Pilih pada aturan dan pilih tombol “Nonaktifkan”.

Hubungi Support

Jika Anda memiliki AWS Developer Support, AWS Business Support, atau AWS Enterprise Support, Anda dapat menggunakan Support Center untuk mendapatkan bantuan ahli terkait solusi ini. Bagian berikut memberikan petunjuk.

Buat kasus

1. Masuk ke Support Center.
2. Pilih Buat kasus.

Bagaimana kami bisa membantu?

1. Pilih Teknis.

2. Untuk Layanan, pilih Solusi.
3. Untuk Kategori, pilih Solusi Lain.
4. Untuk Keparahan, pilih opsi yang paling cocok dengan kasus penggunaan Anda.
5. Saat Anda memasukkan Layanan, Kategori, dan Tingkat Keparahan, antarmuka akan mengisi tautan ke pertanyaan pemecahan masalah umum. Jika Anda tidak dapat menyelesaikan pertanyaan Anda dengan tautan ini, pilih Langkah selanjutnya: Informasi tambahan.

Informasi tambahan

1. Untuk Subjek, masukkan teks yang merangkum pertanyaan atau masalah Anda.
2. Untuk Deskripsi, jelaskan masalah ini secara rinci.
3. Pilih Lampirkan file.
4. Lampirkan informasi yang dibutuhkan Support untuk memproses permintaan.

Bantu kami menyelesaikan kasus Anda lebih cepat

1. Masukkan informasi yang diminta.
2. Pilih Langkah selanjutnya: Selesaikan sekarang atau hubungi kami.

Selesaikan sekarang atau hubungi kami

1. Tinjau solusi Selesaikan sekarang.
2. Jika Anda tidak dapat menyelesaikan masalah Anda dengan solusi ini, pilih Hubungi kami, masukkan informasi yang diminta, dan pilih Kirim.

Copot pemasangan solusinya

Gunakan prosedur berikut untuk menghapus instalan solusi dengan AWS Management Console.

V1.0.0-V1.2.1

Untuk rilis v1.0.0 ke v1.2.1, gunakan Service Catalog untuk menghapus Instalasi Playbooks CIS FSBP. and/or Dengan v1.3.0 Service Catalog tidak lagi digunakan.

1. Masuk ke CloudFormation konsol AWS dan navigasikan ke akun utama Security Hub.
2. Pilih Service Catalog untuk menghentikan pedoman yang disediakan, menghapus grup keamanan, peran, atau pengguna apa pun.
3. Hapus `CISPermissions.template` templat spoke dari akun anggota Security Hub.
4. Hapus `AFSBPMemberStack.template` templat spoke dari admin Security Hub dan akun anggota.
5. Arahkan ke akun utama Security Hub, pilih tumpukan instalasi solusi, lalu pilih Hapus.

> **Note**
>
> CloudWatch Log grup log dipertahankan. Sebaiknya simpan log ini seperti yang dipersyaratkan oleh kebijakan penyimpanan log organisasi Anda.

v1.3.x

1. Hapus `automated-security-response-member.template` dari setiap akun anggota.
2. Hapus `automated-security-response-admin.template` dari akun admin.

> **Note**
>
> Penghapusan template admin di v1.3.0 kemungkinan akan gagal pada penghapusan Tindakan Kustom. Ini adalah masalah yang diketahui yang akan diperbaiki di rilis berikutnya. Gunakan petunjuk berikut untuk memperbaiki masalah ini:
>
> 1. Masuk ke konsol manajemen AWS Security Hub.
> 2. Di akun admin, buka Pengaturan.

3. Pilih tab Tindakan kustom.
4. Hapus entri secara manual Remediate dengan ASR.
5. Hapus tumpukan lagi.

V1.4.0 dan yang lebih baru

Penyebaran tumpukan

1. Hapus `automated-security-response-member.template` dari setiap akun anggota.
2. Hapus `automated-security-response-admin.template` dari akun admin.

StackSet penyebaran

Untuk masing-masing StackSet, hapus tumpukan, lalu hapus StackSet dalam urutan penerapan terbalik.

Perhatikan bahwa peran IAM dari tetap `automated-security-response-member-roles.template` dipertahankan meskipun template dihapus. Ini agar remediasi menggunakan peran ini terus berfungsi. Peran SO0111-* ini dapat dihapus secara manual setelah memverifikasi bahwa mereka tidak lagi digunakan oleh remediasi aktif, seperti CloudTrail untuk CloudWatch logging, atau RDS Enhanced Monitoring.

Panduan administrator

Mengaktifkan dan menonaktifkan bagian dari solusi

Sebagai administrator solusi, Anda memiliki kontrol berikut atas fungsionalitas solusi mana yang diaktifkan.

Di mana tumpukan peran anggota dan anggota digunakan:

- Tumpukan admin hanya akan dapat memulai remediasi (melalui tindakan kustom atau EventBridge aturan otomatis sepenuhnya) di akun di mana tumpukan peran anggota dan anggota telah digunakan dengan nomor akun admin yang diberikan sebagai nilai parameter.
- Untuk membebaskan akun atau Wilayah dari kendali solusi sepenuhnya, jangan gunakan tumpukan peran anggota atau anggota ke akun atau Wilayah tersebut.

Konfigurasi agregasi pencarian Akun dan Wilayah di Security Hub:

- Tumpukan admin hanya akan dapat memulai remediasi (melalui tindakan khusus atau EventBridge aturan otomatis sepenuhnya) untuk temuan yang tiba di akun admin dan Wilayah.
- Untuk membebaskan akun atau Wilayah dari kendali solusi sepenuhnya, jangan sertakan akun atau Wilayah tersebut untuk mengirim temuan ke akun admin dan Wilayah yang sama tempat tumpukan admin digunakan.

Tumpukan bersarang standar mana yang digunakan:

- Tumpukan admin hanya akan dapat memulai remediasi (melalui tindakan khusus atau EventBridge aturan otomatis sepenuhnya) untuk kontrol yang memiliki runbook kontrol yang diterapkan di akun anggota target dan Wilayah. Ini digunakan oleh tumpukan anggota untuk setiap standar.
- Tumpukan admin hanya akan dapat memulai remediasi otomatis sepenuhnya menggunakan EventBridge aturan untuk kontrol yang memiliki aturan yang diterapkan oleh tumpukan admin untuk standar itu. Ini digunakan ke akun admin.
- Untuk mempermudah, kami sarankan untuk menerapkan standar secara konsisten di seluruh akun admin dan anggota Anda. Jika Anda peduli dengan AWS FSBP dan CIS v1.2.0, terapkan dua tumpukan admin bersarang tersebut ke akun admin, dan terapkan dua tumpukan anggota bersarang tersebut ke setiap akun anggota dan Wilayah.

Runbook Kontrol mana yang digunakan di setiap tumpukan anggota bersarang:

- Tumpukan admin hanya akan dapat memulai remediasi (melalui tindakan khusus atau EventBridge aturan otomatis sepenuhnya) untuk kontrol yang memiliki runbook kontrol yang diterapkan di akun anggota target dan Wilayah oleh tumpukan anggota untuk setiap standar.
- Untuk melakukan kontrol yang lebih halus atas kontrol mana yang diaktifkan untuk standar tertentu, setiap tumpukan bersarang untuk standar memiliki parameter yang runbook kontrol digunakan. Setel parameter untuk kontrol ke nilai “TIDAK Tersedia” untuk membatalkan penerapan runbook kontrol itu.

Parameter SSM untuk mengaktifkan dan menonaktifkan standar:

- Tumpukan admin hanya akan dapat memulai remediasi (melalui tindakan kustom atau EventBridge aturan otomatis penuh) untuk standar yang diaktifkan melalui Parameter SSM yang digunakan oleh tumpukan admin standar.
- <standard_name><standard_version>Untuk menonaktifkan standar, atur nilai untuk Parameter SSM dengan jalur “/solutions/SO0111///status" menjadi “Tidak”.

Contoh notifikasi SNS

Ketika remediasi dimulai


```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
```

```
}
```

Ketika remediasi berhasil

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Ketika remediasi gagal

```
{
 "severity": "ERROR",
 "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
```

```
  }
}
```

Gunakan solusinya

Ini adalah tutorial yang akan memandu Anda melalui penyebaran ASR pertama Anda. Ini akan dimulai dengan prasyarat untuk menerapkan solusi dan itu akan berakhir dengan Anda memulihkan temuan contoh di akun anggota.

Tutorial: Memulai Respons Keamanan Otomatis di AWS

Ini adalah tutorial yang akan memandu Anda melalui penyebaran pertama Anda. Ini akan dimulai dengan prasyarat untuk menerapkan solusi dan itu akan berakhir dengan Anda memulihkan temuan contoh di akun anggota.

Siapkan akun

Untuk menunjukkan kemampuan remediasi lintas akun dan lintas wilayah dari solusi, tutorial ini akan menggunakan dua akun. Anda juga dapat menerapkan solusi ke satu akun.

Contoh berikut menggunakan akun `111111111111` dan `222222222222` untuk menunjukkan solusinya. `111111111111`akan menjadi akun admin dan `222222222222` akan menjadi akun anggota. Kami akan menyiapkan solusi untuk memulihkan temuan sumber daya di Daerah `us-east-1` dan`us-west-2`.

Tabel di bawah ini adalah contoh untuk mengilustrasikan tindakan yang akan kami ambil untuk setiap langkah di setiap akun dan Wilayah.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
`111111111111`	Admin	Tidak ada	Tidak ada
`222222222222`	Anggota	Tidak ada	Tidak ada

Akun admin adalah akun yang akan melakukan tindakan administrasi solusi, yaitu memulai remediasi secara manual atau mengaktifkan remediasi otomatis sepenuhnya dengan aturan. EventBridge Akun ini juga harus merupakan akun administrator yang didelegasikan Security Hub untuk semua akun tempat Anda ingin memulihkan temuannya, tetapi akun tersebut tidak perlu juga bukan akun administrator AWS Organizations untuk AWS Organization tempat akun Anda berada.

Aktifkan AWS Config

Tinjau dokumentasi berikut:

- Dokumentasi AWS Config
- Harga AWS Config
- Mengaktifkan AWS Config

Aktifkan AWS Config di kedua akun dan kedua Wilayah. Ini akan dikenakan biaya.

> **Important**
>
> Pastikan Anda memilih opsi untuk “Sertakan sumber daya global (misalnya, sumber daya AWS IAM).” Jika Anda tidak memilih opsi ini saat mengaktifkan AWS Config, Anda tidak akan melihat temuan yang terkait dengan sumber daya global (misalnya sumber daya AWS IAM)

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Aktifkan AWS Config	Aktifkan AWS Config
222222222222	Anggota	Aktifkan AWS Config	Aktifkan AWS Config

Aktifkan hub keamanan AWS

Tinjau dokumentasi berikut:

- Dokumentasi AWS Security Hub
- Harga AWS Security Hub
- Mengaktifkan AWS Security Hub

Aktifkan AWS Security Hub di kedua akun dan kedua Wilayah. Ini akan dikenakan biaya.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Aktifkan AWS Security Hub	Aktifkan AWS Security Hub
222222222222	Anggota	Aktifkan AWS Security Hub	Aktifkan AWS Security Hub

Aktifkan temuan kontrol terkonsolidasi

Tinjau dokumentasi berikut:

- Menghasilkan dan memperbarui temuan kontrol

Untuk keperluan tutorial ini, kami akan mendemonstrasikan penggunaan solusi dengan fitur temuan kontrol konsolidasi AWS Security Hub diaktifkan, yang merupakan konfigurasi yang disarankan. Di partisi yang tidak mendukung fitur ini pada saat penulisan, Anda harus menggunakan buku pedoman khusus standar daripada SC (Kontrol Keamanan).

Aktifkan temuan kontrol konsolidasi di kedua akun dan kedua Wilayah.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Aktifkan temuan kontrol terkonsolidasi	Aktifkan temuan kontrol terkonsolidasi
222222222222	Anggota	Aktifkan temuan kontrol terkonsolidasi	Aktifkan temuan kontrol terkonsolidasi

Mungkin perlu beberapa waktu untuk temuan dihasilkan dengan fitur baru. Anda dapat melanjutkan dengan tutorial, tetapi Anda tidak akan dapat memulihkan temuan yang dihasilkan tanpa fitur baru. Temuan yang dihasilkan dengan fitur baru dapat diidentifikasi dengan nilai `GeneratorId` bidang`security-control/<control_id>`.

Konfigurasikan agregasi pencarian lintas wilayah

Tinjau dokumentasi berikut:

- Agregasi Lintas Wilayah
- Mengaktifkan agregasi lintas wilayah

Konfigurasikan agregasi pencarian dari us-west-2 ke us-east-1 di kedua akun.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Konfigurasikan agregasi dari us-west-2	Tidak ada
222222222222	Anggota	Konfigurasikan agregasi dari us-west-2	Tidak ada

Mungkin perlu beberapa waktu bagi temuan untuk menyebar ke Wilayah agregasi. Anda dapat melanjutkan dengan tutorial, tetapi Anda tidak akan dapat memulihkan temuan dari Wilayah lain sampai mereka mulai muncul di Wilayah agregasi.

Menetapkan akun administrator Security Hub

Tinjau dokumentasi berikut:

- Mengelola akun di AWS Security Hub
- Mengelola akun anggota organisasi
- Mengelola akun anggota dengan undangan

Dalam contoh proses, kita akan menggunakan metode undangan manual. Untuk satu set akun produksi, kami sarankan untuk mengelola admin yang didelegasikan Security Hub melalui AWS Organizations.

Dari konsol AWS Security Hub di akun admin (111111111111), undang akun anggota (222222222222) untuk menerima akun admin sebagai administrator yang didelegasikan Security Hub. Dari akun anggota, terima undangan.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Undang akun anggota	Tidak ada
222222222222	Anggota	Terima undangannya	Tidak ada

Mungkin perlu beberapa waktu untuk temuan menyebar ke akun admin. Anda dapat melanjutkan dengan tutorial, tetapi Anda tidak akan dapat memulihkan temuan dari akun anggota sampai mereka mulai muncul di akun admin.

Buat peran untuk izin yang dikelola sendiri StackSets

Tinjau dokumentasi berikut:

- AWS CloudFormation StackSets
- Berikan izin yang dikelola sendiri

Kami akan menyebarkan CloudFormation tumpukan ke beberapa akun, jadi kami akan menggunakannya. StackSets Kami tidak dapat menggunakan izin yang dikelola layanan karena tumpukan admin dan tumpukan anggota memiliki tumpukan bersarang, yang tidak didukung oleh layanan, jadi kami harus menggunakan izin yang dikelola sendiri.

Menyebarkan tumpukan untuk izin dasar untuk operasi. StackSet Untuk akun produksi, Anda mungkin ingin mempersempit izin sesuai dengan dokumentasi “opsi izin lanjutan”.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Menerapkan StackSet tumpukan peran administrator Menerapkan tumpukan peran StackSet Eksekusi	Tidak ada

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
222222222222	Anggota	Menerapkan StackSet tumpukan peran eksekusi	Tidak ada

Buat sumber daya tidak aman yang akan menghasilkan temuan contoh

Tinjau dokumentasi berikut:

- Referensi kontrol Security Hub
- Kontrol AWS Lambda

Contoh sumber daya berikut dengan konfigurasi tidak aman untuk menunjukkan remediasi. Contoh kontrol adalah Lambda.1: Kebijakan fungsi Lambda harus melarang akses publik.

> **Important**
>
> Kami akan dengan sengaja membuat sumber daya dengan konfigurasi yang tidak aman. Harap tinjau sifat kontrol dan evaluasi risiko menciptakan sumber daya seperti itu di lingkungan Anda untuk diri Anda sendiri. Waspadai alat apa pun yang mungkin dimiliki organisasi Anda untuk mendeteksi dan melaporkan sumber daya tersebut dan meminta pengecualian jika sesuai. Jika contoh kontrol yang kami pilih tidak sesuai untuk Anda, pilih kontrol lain yang didukung solusi.

Di Wilayah kedua akun anggota, navigasikan ke konsol AWS Lambda dan buat fungsi di runtime Python terbaru. Di bawah Konfigurasi → Izin, tambahkan pernyataan kebijakan untuk memungkinkan pemanggilan fungsi dari URL tanpa autentikasi.

Konfirmasikan pada halaman konsol bahwa fungsi tersebut memungkinkan akses publik. Setelah solusi mengatasi masalah ini, bandingkan izin untuk mengonfirmasi bahwa akses publik telah dicabut.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Tidak ada	Tidak ada

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
222222222222	Anggota	Tidak ada	Buat fungsi Lambda dengan konfigurasi yang tidak aman

AWS Config mungkin perlu beberapa waktu untuk mendeteksi konfigurasi yang tidak aman. Anda dapat melanjutkan dengan tutorial, tetapi Anda tidak akan dapat memulihkan temuan sampai Config mendeteksinya.

Buat grup CloudWatch log untuk kontrol terkait

Tinjau dokumentasi berikut:

- Memantau File CloudTrail Log dengan CloudWatch Log Amazon
- CloudTrail kontrol

Berbagai CloudTrail kontrol yang didukung oleh solusi mengharuskan ada grup CloudWatch Log yang merupakan tujuan Multi-wilayah CloudTrail. Dalam contoh berikut, kita akan membuat grup log placeholder. Untuk akun produksi, Anda harus mengonfigurasi CloudTrail integrasi dengan CloudWatch Log dengan benar.

Buat grup log di setiap akun dan Wilayah dengan nama yang sama, misalnya:`asr-log-group`.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Membuat grup log	Membuat grup log
222222222222	Anggota	Membuat grup log	Membuat grup log

Terapkan solusi ke akun tutorial

Kumpulkan tiga Amazon S3 URLs untuk tumpukan peran admin, anggota, dan anggota.

Menyebarkan tumpukan admin

View template

automa

security-response-admin.template

Di akun admin, navigasikan ke CloudFormation konsol dan terapkan tumpukan admin ke Wilayah agregasi pencarian Security Hub.

Pilih No nilai semua parameter untuk memuat tumpukan admin bersarang kecuali tumpukan “SC” atau “Kontrol Keamanan”. Tumpukan ini berisi sumber daya untuk temuan kontrol konsolidasi yang telah kami konfigurasikan di akun kami.

Pilih No untuk menggunakan kembali grup log orkestrator kecuali Anda telah menerapkan solusi ini di akun ini dan Wilayah sebelumnya.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Menyebarkan tumpukan admin	Tidak ada
222222222222	Anggota	Tidak ada	Tidak ada

Tunggu hingga tumpukan admin menyelesaikan penerapan sebelum melanjutkan sehingga hubungan kepercayaan dapat dibuat dari akun anggota ke akun admin.

Menyebarkan tumpukan anggota

View template

automa

security-response-member.template

Di akun admin, navigasikan ke CloudFormation StackSets konsol dan terapkan tumpukan anggota ke setiap akun dan Wilayah. Gunakan peran StackSets admin dan eksekusi yang dibuat dalam tutorial ini.

Masukkan nama grup log yang Anda buat sebagai nilai parameter untuk nama grup log.

Pilih No nilai semua parameter untuk memuat tumpukan anggota bersarang kecuali tumpukan “SC” atau “kontrol keamanan”. Tumpukan ini berisi sumber daya untuk temuan kontrol konsolidasi yang telah kami konfigurasikan di akun kami.

Masukkan ID akun admin sebagai nilai parameter untuk nomor akun admin. Dalam contoh kita, ini adalah111111111111.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Menyebarkan anggota StackSet /Konfirmasi tumpukan anggota yang digunakan	Konfirmasikan tumpukan anggota dikerahkan
222222222222	Anggota	Konfirmasikan tumpukan anggota dikerahkan	Konfirmasikan tumpukan anggota dikerahkan

Menerapkan tumpukan peran anggota

automated-security-response-member-roles.template tombol template -roles.template automated-security-response-member

Di akun admin, navigasikan ke CloudFormation StackSets konsol dan gunakan tumpukan anggota ke setiap akun. Gunakan peran StackSets admin dan eksekusi yang dibuat dalam tutorial ini. Masukkan ID akun admin sebagai nilai parameter untuk nomor akun admin. Dalam contoh kita, ini adalah111111111111.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Menyebarkan anggota StackSet /Konfirmasi tumpukan anggota yang digunakan	Tidak ada

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
222222222222	Anggota	Konfirmasikan tumpukan anggota dikerahkan	Tidak ada

Anda dapat melanjutkan, tetapi Anda tidak akan dapat memulihkan temuan sampai CloudFormation StackSets selesai digunakan.

Berlangganan topik SNS

Pembaruan Remediasi

Topik - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— topic-arn-aws-sns -US-timur-1-221128147805-SO0111-ASR-Topic} [SO0111-ASR_Topic]

Di akun admin, berlangganan topik Amazon SNS yang dibuat oleh tumpukan admin. Ini akan memberi tahu Anda ketika perbaikan dimulai dan ketika berhasil atau gagal.

Alarm

Topik - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— topic-arn-aws-sns -US-timur-1-221128147805-SO0111-ASR-alarm-topic} [SO0111-ASR_alarm_topic]

Di akun admin, berlangganan topik Amazon SNS yang dibuat oleh tumpukan admin. Ini akan memberi tahu Anda saat alarm metrik dimulai.

Memperbaiki temuan contoh

Di akun admin, navigasikan ke konsol Security Hub dan temukan temuan untuk sumber daya dengan konfigurasi tidak aman yang Anda buat sebagai bagian dari tutorial ini.

Ini dapat dilakukan dengan beberapa cara:

1. Di partisi yang mendukung fitur temuan kontrol terkonsolidasi, halaman berlabel “Kontrol” memungkinkan Anda menemukan temuan dengan ID kontrol terkonsolidasi.
2. Di halaman “Standar keamanan”, Anda dapat menemukan kontrol sesuai dengan standar mana yang dimilikinya.
3. Anda dapat melihat semua temuan di halaman “Temuan” dan mencari berdasarkan atribut.

ID kontrol konsolidasi untuk Fungsi Lambda publik yang kami buat adalah Lambda.1.

Memulai remediasi

Pilih kotak centang di sebelah kiri temuan yang terkait dengan sumber daya yang kami buat. Di menu tarik-turun “Tindakan”, pilih “Remediate with ASR”. Anda akan melihat pemberitahuan bahwa temuan itu dikirim ke Amazon EventBridge.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Memulai remediasi	Tidak ada
222222222222	Anggota	Tidak ada	Tidak ada

Konfirmasikan bahwa remediasi menyelesaikan temuan

Anda harus menerima dua notifikasi SNS. Yang pertama akan menunjukkan bahwa remediasi telah dimulai, dan yang kedua akan menunjukkan bahwa remediasi berhasil. Setelah menerima pemberitahuan kedua, arahkan ke konsol Lambda di akun anggota dan konfirmasikan bahwa akses publik telah dicabut.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Tidak ada	Tidak ada
222222222222	Anggota	Tidak ada	Konfirmasikan bahwa remediasi berhasil

Lacak eksekusi remediasi

Untuk lebih memahami cara kerja solusinya, Anda dapat melacak eksekusi remediasi.

EventBridge aturan

Di akun admin, cari EventBridge aturan bernama CustomActionRemediate_with_asr_. Aturan ini cocok dengan temuan yang Anda kirim dari Security Hub dan mengirimkannya ke Step Functions Orchestrator.

Eksekusi Step Functions

Di akun admin, cari AWS Step Functions bernama "SO0111-ASR-Orchestrator”. Fungsi langkah ini memanggil dokumen Otomasi SSM di akun target dan Wilayah. Anda dapat melacak eksekusi remediasi dalam riwayat eksekusi AWS Step Functions ini.

Otomatisasi SSM

Di akun anggota, navigasikan ke konsol Otomasi SSM. Anda akan menemukan dua eksekusi dokumen bernama “ASR-SC_2.0.0_lambda.1" dan satu eksekusi dokumen bernama “ASR-”. RemoveLambdaPublicAccess

Eksekusi pertama adalah dari fungsi langkah orkestrator di akun target. Eksekusi kedua terjadi di Wilayah target, yang mungkin bukan Wilayah dari mana temuan itu berasal. Eksekusi terakhir adalah remediasi yang mencabut kebijakan akses publik dari Fungsi Lambda.

CloudWatch Grup Log

Di akun admin, arahkan ke konsol CloudWatch Log dan temukan Grup Log bernama "SO0111-ASR”. Grup log ini adalah tujuan untuk log tingkat tinggi dari Step Functions Orchestrator.

Aktifkan remediasi yang sepenuhnya otomatis

Mode operasi lain untuk solusi ini adalah secara otomatis memulihkan temuan saat mereka tiba di Security Hub.

Konfirmasikan bahwa Anda tidak memiliki sumber daya, temuan ini dapat diterapkan secara tidak sengaja

Mengaktifkan remediasi otomatis akan memulai remediasi pada semua sumber daya yang cocok dengan kontrol yang Anda aktifkan (Lambda.1).

> **Important**
>
> Konfirmasikan bahwa Anda ingin semua Fungsi Lambda publik dalam lingkup solusi dicabut izin ini. Remediasi yang sepenuhnya otomatis tidak akan terbatas dalam cakupan Fungsi yang Anda buat. Solusinya akan memulihkan kontrol ini jika terdeteksi di salah satu akun dan Wilayah di mana ia diinstal.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Konfirmasikan tidak ada Fungsi publik yang diinginkan	Konfirmasikan tidak ada Fungsi publik yang diinginkan
222222222222	Anggota	Konfirmasikan tidak ada Fungsi publik yang diinginkan	Konfirmasikan tidak ada Fungsi publik yang diinginkan

Aktifkan aturan

Di akun Admin, cari EventBridge aturan bernama AutoTriggerSC_2.0.0_lambda.1_ dan aktifkan.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Aktifkan aturan remediasi otomatis	Tidak ada
222222222222	Anggota	Tidak ada	Tidak ada

Konfigurasikan sumber daya

Di akun anggota, konfigurasikan ulang Fungsi Lambda untuk memungkinkan akses publik.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Tidak ada	Tidak ada
222222222222	Anggota	Tidak ada	Konfigurasikan Fungsi Lambda untuk memungkinkan akses publik

Konfirmasikan bahwa remediasi menyelesaikan temuan

Mungkin perlu beberapa waktu bagi Config untuk mendeteksi konfigurasi yang tidak aman lagi. Anda harus menerima dua notifikasi SNS. Yang pertama akan menunjukkan bahwa remediasi telah dimulai. Yang kedua akan menunjukkan bahwa remediasi berhasil. Setelah menerima pemberitahuan kedua, arahkan ke konsol Lambda di akun anggota dan konfirmasikan bahwa akses publik telah dicabut.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Aktifkan aturan remediasi otomatis	Tidak ada
222222222222	Anggota	Tidak ada	Konfirmasikan bahwa remediasi berhasil

Bersihkan

Hapus sumber daya contoh

Di akun anggota, hapus contoh fungsi Lambda yang Anda buat.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Tidak ada	Tidak ada
222222222222	Anggota	Tidak ada	Hapus contoh Fungsi Lambda

Hapus tumpukan admin

Di akun admin, hapus tumpukan admin.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Hapus tumpukan admin	Tidak ada
222222222222	Anggota	Tidak ada	Tidak ada

Hapus tumpukan anggota

Di akun Admin, hapus anggota StackSet.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Hapus anggota StackSet Konfirmasikan tumpukan anggota dihapus	Konfirmasikan tumpukan anggota dihapus
222222222222	Anggota	Konfirmasikan tumpukan anggota dihapus	Konfirmasikan tumpukan anggota dihapus

Hapus tumpukan peran anggota

Di akun Admin, hapus peran anggota StackSet.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Hapus peran anggota StackSet Konfirmasikan tumpukan peran rmember dihapus	Tidak ada

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
222222222222	Anggota	Konfirmasikan tumpukan peran anggota dihapus	Tidak ada

Hapus peran yang dipertahankan

Di setiap akun, hapus peran IAM yang dipertahankan.

Penting: Peran ini dipertahankan untuk remediasi yang memerlukan peran agar remediasi dapat terus berfungsi (misalnya pencatatan aliran VPC). Konfirmasikan bahwa Anda tidak memerlukan fungsi lanjutan dari salah satu peran ini sebelum menghapusnya.

Hapus peran apa pun yang diawali dengan SO0111-.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Hapus peran yang dipertahankan	Tidak ada
222222222222	Anggota	Hapus peran yang dipertahankan	Tidak ada

Jadwalkan kunci KMS yang dipertahankan untuk dihapus

Tumpukan admin dan anggota membuat dan mempertahankan kunci KMS. Anda akan dikenakan biaya jika Anda menyimpan kunci ini.

Kunci ini disimpan untuk memberi Anda akses ke sumber daya apa pun yang dienkripsi oleh solusi. Konfirmasikan bahwa Anda tidak memerlukannya sebelum menjadwalkannya untuk dihapus.

Identifikasi kunci yang digunakan oleh solusi menggunakan alias yang dibuat oleh solusi atau dari riwayat. CloudFormation Jadwalkan mereka untuk dihapus.

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Identifikasi dan jadwalkan kunci admin untuk dihapus Identifikasi dan jadwalkan kunci anggota untuk dihapus	Identifikasi dan jadwalkan kunci anggota untuk dihapus
222222222222	Anggota	Identifikasi dan jadwalkan kunci anggota untuk dihapus	Identifikasi dan jadwalkan kunci anggota untuk dihapus

Hapus tumpukan untuk izin yang dikelola sendiri StackSets

Hapus tumpukan yang dibuat untuk memungkinkan izin yang dikelola sendiri StackSets

Akun	Tujuan	Aksi di us-east-1	Aksi di us-west-2
111111111111	Admin	Hapus tumpukan peran StackSet administrator	Tidak ada
222222222222	Anggota	Hapus tumpukan peran StackSet eksekusi	Tidak ada

Panduan pengembang

Bagian ini menyediakan kode sumber untuk solusi dan penyesuaian tambahan.

Kode sumber

Kunjungi GitHub repositori kami untuk mengunduh templat dan skrip untuk solusi ini, dan untuk berbagi penyesuaian Anda dengan orang lain.

Buku pedoman

Solusi ini mencakup remediasi buku pedoman untuk standar keamanan yang ditetapkan sebagai bagian dari Tolok Ukur Yayasan AWS Center for Internet Security (CIS) v1.2.0, Tolok Ukur Yayasan CIS AWS v1.4.0, TolokUkur Yayasan CIS AWS v3.0.0, AWS FoundationalSecurity Best Practices (FSBP) v.1.0.0, Standar Keamanan Data Industri Kartu Pembayaran (PCI-DSS) v3.2.1, dan Institut Standar Nasional dan Teknologi (NIST).

Jika Anda mengaktifkan temuan kontrol konsolidasi, maka kontrol tersebut didukung dalam semua standar. Jika fitur ini diaktifkan, maka hanya pedoman SC yang perlu digunakan. Jika tidak, maka pedoman didukung untuk standar yang tercantum sebelumnya.

> **Important**
>
> Hanya gunakan buku pedoman untuk standar yang diaktifkan untuk menghindari mencapai kuota layanan.

Untuk detail tentang remediasi tertentu, lihat dokumen otomatisasi Systems Manager dengan nama yang digunakan oleh solusi di akun Anda. Buka konsol AWS Systems Manager, lalu di panel navigasi pilih Documents.

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Remediasi Total	63	34	29	33	65	19	90

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-Periksa EnableAutoScalingGroup ELBHealth Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan load balancer	Penskalaan otomatis.1		Penskalaan otomatis.1		Penskalaan otomatis.1		Penskalaan otomatis.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-ConfigureAutoScalingLaunchConfigToRequireIMDSv2 Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi EC2 instance agar memerlukan Layanan Metadata Instance Versi 2 () IMDSv2					Penskalaan otomatis. 3		Penskalaan otomatis. 3

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateCloudTrailMultiRegionTrail CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya a satu jejak Multi-wilayah	CloudTrail.1	2.1	CloudTrail.2	3.1	CloudTrail.1	3.1	CloudTrail.1
ASR-EnableEncryption CloudTrail harus mengaktifkan enkripsi saat istirahat	CloudTrail.2	2.7	CloudTrail.1	3.7	CloudTrail.2	3.5	CloudTrail.2

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-EnableLogFileValidation Pastikan validasi file CloudTrail log diaktifkan	CloudTrail.4	2.2	CloudTrail.3	3.2	CloudTrail.4		CloudTrail.4
ASR-EnableCloudTrailToCloudWatchLogging Pastikan CloudTrail jalur terintegrasi dengan Amazon Logs CloudWatch	CloudTrail.5	2.4	CloudTrail.4	3.4	CloudTrail.5		CloudTrail.5

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-konfigurasi3BucketLogging Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3		2.6		3.6		3.4	CloudTrail.7
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild variabel lingkungan proyek tidak boleh mengandung kredensil teks yang jelas	CodeBuild.2		CodeBuild.2		CodeBuild.2		CodeBuild.2

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Aktifkan ASR AWSConfig Pastikan AWS Config diaktifkan	Konfigurasi.1	2.5	Konfigurasi.1	3.5	Konfigurasi.1	3.3	Konfigurasi.1
ASR-Make Pribadi EBSSnapshots Cuplikan Amazon EBS tidak boleh dipulihkan secara publik	EC2.1		EC2.1		EC2.1		EC2.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-Hapus VPCDefault SecurityGroupRules Grup keamanan default VPC harus melarang lalu lintas masuk dan keluar	EC2.2	4.3	EC2.2	5.3	EC2.2	5.4	EC2.2
Log Aktifkan ASR VPCFlow Pencatatan aliran VPC harus diaktifkan di semua VPCs	EC2.6	2.9	EC2.6	3.9	EC2.6	3.7	EC2.6

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-EnableEbsEncryptionByDefault Enkripsi default EBS harus diaktifkan	EC2.7	2.2.1			EC2.7	2.2.1	EC2.7
ASR-RevokeUnrotatedKeys Kunci akses pengguna harus diputar setiap 90 hari atau kurang	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Kebijakan ASR-Set IAMPasswo rd Kebijakan kata sandi default IAM	IAM.7	1,5-1,11	IAM.8	1.8	IAM.7	1.8	IAM.7
ASR-Kredensil RevokeUnu sed IAMUser Kredensi pengguna harus dimatikan jika tidak digunakan dalam waktu 90 hari	IAM.8	1.3	IAM.7		IAM.8		IAM.8

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-KredensilRevokeUnused IAMUser Kredensi pengguna harus dimatikan jika tidak digunakan dalam waktu 45 hari				1.12		1.12	IAM.22
ASR-RemoveLambdaPublicAccess Fungsi Lambda harus melarang akses publik	Lambda.1		Lambda.1		Lambda.1		Lambda.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-MakePribadiRDSSnapshot Snapshot RDS harus melarang akses publik	RDS.1		RDS.1		RDS.1		RDS.1
ASR-DisablePublicAccessToRDSInstance Instans RDS DB harus melarang akses publik	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-enkripsi RDSSnapshot Snapshot cluster RDS dan snapshot database harus dienkripsi saat istirahat	RDS.4				RDS.4		RDS.4
ASR-EnableMulti AZOn RDSInstance Instans RDS DB harus dikonfigurasi dengan beberapa Availability Zone	RDS.5				RDS.5		RDS.5

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-EnableEnhancedMonitoringOnRDSInstance Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans dan cluster RDS DB	RDS.6				RDS.6		RDS.6

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Aktifkan ASR RDSCluster DeletionProtection Cluster RDS harus mengaktifkan perlindungan penghapusan	RDS.7				RDS.7		RDS.7
Aktifkan ASR RDSInstance DeletionProtection Instans RDS DB harus mengaktifkan perlindungan penghapusan	RDS.8				RDS.8		RDS.8

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-EnableMinorVersionUpgradeOnRDSDBInstance Upgrade versi minor otomatis RDS harus diaktifkan	RDS.13				RDS.13	2.3.2	RDS.13
ASR-EnableCopyTagsToSnapshotOnRDSCluster Cluster RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot	RDS.16				RDS.16		RDS.16

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-DisablePublicAccessToRedshiftCluster Cluster Amazon Redshift harus melarang akses publik	Pergeseran merah.1		Pergeseran merah.1		Pergeseran merah.1		Pergeseran merah.1
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Cluster Amazon Redshift harus mengaktifkan snapshot otomatis	Pergeseran merah.3				Pergeseran merah.3		Pergeseran merah.3

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-EnableRedshiftClusterAuditLogging Cluster Amazon Redshift harus mengaktifkan pencatatan audit	Pergeseran merah.4				Pergeseran merah.4		Pergeseran merah.4
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama	Pergeseran Merah.6				Pergeseran Merah.6		Pergeseran Merah.6

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-konfigurasi3 PublicAccessBlock Pengaturan Akses Publik Blok S3 harus diaktifkan	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
ASR-konfigurasi3 BucketPublicAccessBlock Bucket S3 harus melarang akses baca publik	S3.2		S3.2	2.1.5.2	S3.2		S3.2

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-konfigurasi3 BucketPublicAccessBlock Bucket S3 harus melarang akses tulis publik		S3.3					S3.3
ASR- S3 EnableDefaultEncryption Bucket S3 harus mengaktifkan enkripsi sisi server	S3.4		S3.4	2.1.1	S3.4		S3.4

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Kebijakan ASR-Set SSLBucket Bucket S3 harus memerlukan permintaan untuk menggunakan SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5
ASR-S3 BlockDenylist Izin Amazon S3 yang diberikan ke akun AWS lain dalam kebijakan bucket harus dibatasi	S3.6				S3.6		S3.6

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Pengaturan Akses Publik Blok S3 harus diaktifkan pada tingkat bucket	S3.8				S3.8		S3.8
ASR-konfigurasi3 BucketPublicAccessBlock Pastikan CloudTrail log bucket S3 tidak dapat diakses publik		2.3					CloudTrail.6

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateAccessLoggingBucket Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3		2.6					CloudTrail.7
ASR-EnableKeyRotation Pastikan rotasi untuk dibuat pelanggan diaktifkan CMKs		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah		3.1		4.1			Cloudwatch.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk login AWS Management Console tanpa MFA		3.2		4.2			Cloudwatch.2

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk penggunaan pengguna “root”		3.3	CW.1	4.3			Cloudwatch.3
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM		3.4		4.4			Cloudwatch.4

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi		3.5		4,5			Cloudwatch.5

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan ada filter metrik log dan alarm untuk kegagalan autentikasi AWS Management Console		3.6		4.6			Cloudwatch.6

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau terjadwal penghapusan pelanggan yang dibuat CMKs		3.7		4.7			Cloudwatch.7

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3		3.8		4.8			Cloudwatch.8

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk perubahan konfigurasi AWS Config		3.9		4.9			Cloudwatch.9
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan		3.10		4.10			Cloudwatch.10

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)		3.11		4.11			Cloudwatch.11

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan		3.12		4.12			Cloudwatch.12
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute		3.13		4.13			Cloudwatch.13

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-CreateLogMetricFilterAndAlarm Pastikan filter metrik log dan alarm ada untuk perubahan VPC		3.14		4.14			Cloudwatch.14
AWS-DisablePublicAccessForSecurityGroup Pastikan tidak ada grup keamanan yang mengizinkan masuknya dari 0.0.0.0/0 ke port 22		4.1	EC2.5		EC2.13		EC2.13

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
AWS-DisablePublicAccessForSecurityGroup Pastikan tidak ada grup keamanan yang mengizinkan masuknya dari 0.0.0.0/0 ke port 3389		4.2			EC2.14		EC2.14
Konfigurasi ASR SNSTopicForStack	CloudFormation.1				CloudFormation.1		CloudFormation.1
ASR-BuatIAMSupportPeran		1.20		1.17		1.17	IAM.18

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-DisablePublic IPAuto Tetapkan EC2 Subnet Amazon seharusnya tidak secara otomatis menetapkan alamat IP publik	EC2.15				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail.4	2.2	CloudTrail.3	3.2			CloudTrail.4
ASR-EnableEncryptionFor SNSTopic	SNS.1				SNS.1		SNS.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-EnableDeliveryStatusLoggingForSNSTopic Pencatatan status pengiriman harus diaktifkan untuk pesan notifikasi yang dikirim ke topik	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionForSQSQueue	SQS.1				SQS.1		SQS.1
SnapshotASR-MakeRDSSnapshotPrivate RDS harus bersifat pribadi	RDS.1		RDS.1				RDS.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Blok ASR SSMDocument PublicAccess Dokumen SSM seharusnya tidak bersifat publik	SSM.4				SSM.4		SSM.4
ASR-EnableCloudFrontDefaultRootObject CloudFront distribusi harus memiliki objek root default yang dikonfigurasi	CloudFront.1				CloudFront.1		CloudFront.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-SetCloudFrontOriginDomain CloudFront distribusi seharusnya tidak menunjukkan asal S3 yang tidak ada	CloudFront.12				CloudFront.12		CloudFront.12
ASR-RemoveCodeBuildPrivilegedMode CodeBuild lingkungan proyek harus memiliki Konfigurasi AWS logging	CodeBuild.5				CodeBuild.5		CodeBuild.5

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Instans ASR-Mengakhiri EC2 EC2 Instans yang dihentikan harus dihapus setelah periode waktu tertentu	EC2.4				EC2.4		EC2.4
Aktifkan ASR IMDSV2 OnInstance EC2 instance harus menggunakan Instance Metadata Service Version 2 () IMDSv2	EC2.8				EC2.8	5.6	EC2.8

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-RevokeUnauthorizedInboudRules Grup keamanan hanya boleh mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi	EC2.18				EC2.18		EC2.18

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
MASUKKAN JUDUL DI SINI Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi	EC2.19				EC2.19		EC2.19

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-menonaktifkan TGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC	EC2.23				EC2.23		EC2.23

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-EnablePrivateRepositoryScanning Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi	ECR.1				ECR.1		ECR.1
ASR-EnableGuardDuty GuardDuty harus diaktifkan	GuardDuty.1		GuardDuty.1		GuardDuty.1		GuardDuty.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-konfigurasi3 BucketLogging Pencatatan akses server bucket S3 harus diaktifkan	S3.9				S3.9		S3.9
ASR-EnableBucketEventNotifications Bucket S3 harus mengaktifkan notifikasi acara	S3.11				S3.11		S3.11

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-Sets3 Lifecycle Policy Bucket S3 harus memiliki kebijakan siklus hidup yang dikonfigurasi	S3.13				S3.13		S3.13
ASR-EnableAutoSecretRotation Rahasia Secrets Manager harus mengaktifkan rotasi otomatis	SecretsManager.1				SecretsManager.1		SecretsManager.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-RemoveUnsedSecret Hapus rahasia Secrets Manager yang tidak digunakan	SecretsManager.3				SecretsManager.3		SecretsManager.3
ASR-UpdateSecretRotationPeriod Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu	SecretsManager.4				SecretsManager.4		SecretsManager.4

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Aktifkan ASR APIGateway CacheDataEncryption Data cache API Gateway REST API harus dienkripsi saat istirahat					APIGateway.5		APIGateway.5
ASR-SetLogGroupRetentionDays CloudWatch grup log harus dipertahankan untuk jangka waktu tertentu					CloudWatch.16		CloudWatch.16

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-AttachService VPCEndpoint Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2	EC2.10				EC2.10		EC2.10
ASR-TagGuardDutyResource GuardDuty filter harus diberi tag							GuardDuty.2

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-TagGuardDutyResource GuardDuty detektor harus diberi tag							GuardDuty.4
ASR-melampirkan SSMPermissions ke EC2 EC2 Instans Amazon harus dikelola oleh Systems Manager	SSM.1		SSM.3				SSM.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-ConfigureLaunchConfigNoPublicIPDocument EC2 Instans Amazon yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP publik					Penskalaan otomatis.5		Penskalaan otomatis.5
Aktifkan ASR APIGatewayExecutionLogs	APIGateway.1						APIGateway.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-EnableMacie Amazon Macie harus diaktifkan	Macie.1				Macie.1		Macie.1
ASR-EnableAthenaWorkGroupLogging Kelompok kerja Athena seharusnya mengaktifkan logging	Athena.4						Athena.4

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR menegakkan ALB HTTPSFor Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS	ELB.1		ELB.1		ELB.1		ELB.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
Batas ASR ECSRootFilesystemAccess Kontainer ECS harus dibatasi pada akses hanya-baca ke sistem file root	ECS.5				ECS.5		ECS.5
ASR-EnableElastiCacheBackups ElastiCache Cluster (Redis OSS) harus mengaktifkan pencadangan otomatis	ElastiCache.1				ElastiCache.1		ElastiCache.1

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-EnableElastiCacheVersionUpgrades ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis	ElastiCache.2				ElastiCache.2		ElastiCache.2
ASR-EnableElastiCacheReplicationGroupFailover ElastiCache grup replikasi harus mengaktifkan failover otomatis	ElastiCache.3				ElastiCache.3		ElastiCache.3

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-Configure DynamoDBAuto Penskalaan Tabel DynamoDB harus secara otomatis menskalakan kapasitas dengan permintaan	DynamoDB.1				DynamoDB.1		DynamoDB.1
ASR-Sumber Daya TagDynamoDBTable Tabel DynamoDB harus diberi tag							DynamoDb.5

Deskripsi	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID kontrol keamanan
ASR-Perlindungan EnableDynamoDBDeletion Tabel DynamoDB harus mengaktifkan perlindungan penghapusan					DynamoDb.6		DynamoDb.6

Menambahkan remediasi baru

Remediasi dapat ditambahkan secara manual dengan memperbarui file buku pedoman yang sesuai, atau secara terprogram dengan memperluas solusi melalui konstruksi CDK, tergantung pada alur kerja pilihan Anda.

> **Note**
>
> Instruksi yang mengikuti sumber daya leverage yang dipasang oleh solusi sebagai titik awal. Menurut konvensi, sebagian besar nama sumber daya solusi berisi ASR and/or SO0111 untuk membuatnya mudah untuk menemukan dan mengidentifikasi mereka.

Ikhtisar alur kerja manual

Respons Keamanan Otomatis pada runbook AWS harus mengikuti penamaan standar berikut:

ASR- *<standard>* - - *<version>* *<control>*

Standar: Singkatan untuk standar keamanan. Ini harus sesuai dengan standar yang didukung oleh ASR. Itu harus salah satu dari “CIS”, “AFSBP”, “PCI”, “NIST”, atau “SC”.

Versi: Versi standar. Sekali lagi, ini harus cocok dengan versi yang didukung oleh ASR dan versi dalam data temuan.

Kontrol: ID kontrol kontrol yang akan diperbaiki. Ini harus sesuai dengan data temuan.

1. Buat runbook di akun anggota.
2. Buat peran IAM di akun anggota.
3. (Opsional) Buat aturan remediasi otomatis di akun admin.

Langkah 1. Buat runbook di akun anggota

1. Masuk ke konsol AWS Systems Manager dan dapatkan contoh pencarian JSON.
2. Buat runbook otomatisasi yang memulihkan temuan. Di tab Dimiliki oleh saya, gunakan salah satu `ASR-` dokumen di bawah tab Dokumen sebagai titik awal.
3. AWS Step Functions di akun admin akan menjalankan runbook Anda. Runbook Anda harus menentukan peran remediasi agar dapat diteruskan saat memanggil runbook.

Langkah 2. Buat peran IAM di akun anggota

1. Masuk ke konsol AWS Identity and Access Management.
2. Dapatkan contoh dari peran IAM SO0111 dan buat peran baru. Nama peran harus dimulai dengan SO0111-remediate- - -. *<standard>* *<version>* *<control>* Misalnya, jika menambahkan CIS v1.2.0 kontrol 5.6 peran harus. `SO0111-Remediate-CIS-1.2.0-5.6`
3. Dengan menggunakan contoh, buat peran dengan cakupan yang benar yang hanya memungkinkan panggilan API yang diperlukan untuk melakukan remediasi.

Pada titik ini, remediasi Anda aktif dan tersedia untuk remediasi otomatis dari Tindakan Kustom ASR di AWS Security Hub.

Langkah 3: (Opsional) Buat aturan remediasi otomatis di akun admin

Remediasi otomatis (bukan “otomatis”) adalah eksekusi langsung dari remediasi segera setelah temuan diterima oleh AWS Security Hub. Pertimbangkan risikonya dengan cermat sebelum menggunakan opsi ini.

1. Lihat aturan contoh untuk standar keamanan yang sama di CloudWatch Acara. Standar penamaan untuk aturan adalah`standard_control_*AutoTrigger*`.
2. Salin pola acara dari contoh yang akan digunakan.
3. Ubah `GeneratorId` nilai agar sesuai dengan Finding JSON Anda. `GeneratorId`
4. Simpan dan aktifkan aturan.

Ikhtisar alur kerja CDK

Singkatnya, file-file berikut dalam repo ASR akan dimodifikasi atau ditambahkan. Dalam contoh ini, remediasi baru untuk ElastiCache .2 ditambahkan ke pedoman SC dan AFSBP.

> **Note**
>
> Semua remediasi baru harus ditambahkan ke buku pedoman SC, karena menggabungkan semua remediasi yang tersedia di ASR. Jika Anda bermaksud untuk menerapkan hanya satu set buku pedoman tertentu (misalnya, AFSBP), maka Anda dapat: (1) menambahkan remediasi hanya ke buku pedoman yang Anda inginkan, atau (2) menambahkan remediasi ke semua buku pedoman yang ada di Standar Security Hub terkait, selain buku pedoman SC. Opsi kedua direkomendasikan untuk fleksibilitas.

Dalam contoh ini, ElastiCache .2 disertakan dalam Standar Security Hub berikut:

- AFSBP
- NIST.800-53.R5 SI-2
- NIST.800-53.R5 SI-2 (2)
- NIST.800-53.R5 SI-2 (4)
- NIST.800-53.R5 SI-2 (5)
- PCI DSS v4.0.1/6.3.3

Karena, secara default, ASR hanya mengimplementasikan buku pedoman untuk AFSBP dan NIST.800-53, kami akan menambahkan remediasi baru ini ke buku pedoman tersebut selain SC.

Memodifikasi

- source/lib/remediation-runbook-stack.ts
- source/playbooks/AFSBP/lib/[nama standar] _remediations.ts
- source/playbooks/NIST80053/lib/control_runbooks-construct.ts
- source/playbooks/NIST80053/lib/[nama standar] _remediations.ts
- source/playbooks/SC/lib/control_runbooks-construct.ts
- source/playbooks/SC/lib/sc_remediations.ts
- source/test/regex_registry.ts

Menambahkan

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/SC/ssmdocs/descriptions/ElastiCache.2.md
- source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml

> **Note**
>
> Nama yang dipilih untuk runbook dapat berupa string apa saja, asalkan konsisten dengan sisa perubahan yang dibuat.

- source/playbooks/NIST80053/ssmdocs/NIST80053_ .2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Langkah-langkah pengembangan

1. Buat Runbook Remediasi.
2. Buat Runbook Kontrol.
3. Integrasikan Setiap Runbook Kontrol dengan Playbook.
4. Buat Peran IAM Remediasi & Integrasikan Runbook Remediasi

5. Perbarui Tes Unit

Langkah 1: Buat Runbook Remediasi

Ini adalah dokumen SSM yang digunakan untuk memulihkan sumber daya. Ini harus menyertakan `AutomationAssumeRole` parameter, yang merupakan peran IAM dengan izin untuk menjalankan remediasi. Lihat file yang ada `source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml` sebagai referensi saat membuat runbook remediasi baru.

Semua runbook baru harus ditambahkan ke `source/remediation_runbooks/` direktori.

Langkah 2: Buat Runbook Kontrol

Runbook kontrol adalah runbook khusus playbook yang mem-parsing data temuan dari standar yang diberikan dan mengeksekusi Runbook Remediation yang sesuai. Karena kami menambahkan remediasi ElastiCache .2 ke pedoman SC, AFSBP, dan NIST8 0053, kami harus membuat runbook kontrol baru untuk masing-masing. File-file berikut dibuat:

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ .2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Example

Penamaan file-file ini penting dan harus mengikuti format <PLAYBOOK_NAME>_ <CONTROL.ID>.ts/yaml

Beberapa buku pedoman di ASR mendukung runbook kontrol IAC di TypeScript, sementara yang lain harus ditulis dalam YAMG mentah. Referensikan remediasi yang ada di buku pedoman masing-masing sebagai contoh. Dalam contoh ini, kita akan membahas pedoman SC, yang menggunakan IAc.

Di buku pedoman SC, runbook kontrol baru Anda harus mengekspor kelas yang diperluas ControlRunbookDocument dan cocok dengan nama runbook remediasi Anda. Lihatlah contoh di bawah ini:

```
export class EnableElastiCacheVersionUpgrades extends ControlRunbookDocument {
  constructor(scope: Construct, id: string, props: ControlRunbookProps) {
```

```
    super(scope, id, {
      ...props,
      securityControlId: 'ElastiCache.2',
      remediationName: 'EnableElastiCacheVersionUpgrades',
      scope: RemediationScope.REGIONAL,
      resourceIdRegex: <Regex>,
      resourceIdName: 'ClusterId',
      updateDescription: new StringFormat('Automatic minor version upgrades enabled for
 cluster %s.', [
        StringVariable.of(`ParseInput.ClusterId`),
      ]),
    });
  }
}
```

- `securityControlId`adalah ID kontrol untuk remediasi yang Anda tambahkan, seperti yang didefinisikan dalam tampilan kontrol konsolidasi di Security Hub.
- `remediationName`adalah nama yang telah Anda pilih untuk runbook remediasi Anda.
- `scope`adalah ruang lingkup sumber daya yang Anda pulihkan, yang menunjukkan apakah itu ada secara global atau di wilayah tertentu.
- `resourceIdRegex`adalah regex yang digunakan untuk menangkap ID sumber daya yang ingin Anda teruskan ke runbook remediasi sebagai parameter. Hanya satu kelompok yang harus ditangkap, semua kelompok lain harus tidak menangkap. Jika Anda ingin melewati seluruh ARN, hilangkan bidang ini.
- `resourceIdName`adalah nama yang ingin Anda setel untuk ID sumber daya yang diambil menggunakan`resourceIdRegex`, ini harus cocok dengan nama parameter ID sumber daya di buku runbook remediasi Anda.
- `updateDescription`adalah string yang ingin Anda tetapkan ke bagian “catatan” dari temuan di Security Hub setelah remediasi berhasil.

Anda juga harus mengekspor fungsi `createControlRunbook` yang disebut yang mengembalikan instance baru kelas Anda. Untuk ElastiCache .2, ini terlihat seperti:

```
export function createControlRunbook(scope: Construct, id: string, props:
 PlaybookProps): ControlRunbookDocument {
  return new EnableElastiCacheVersionUpgrades(scope, id, { ...props, controlId:
 'ElastiCache.2' });
}
```

di `controlId` mana ID kontrol sebagaimana didefinisikan dalam Standar Keamanan yang terkait dengan buku pedoman tempat Anda beroperasi.

Jika kontrol Security Hub memiliki parameter yang ingin diteruskan ke runbook remediasi, Anda dapat meneruskannya dengan menambahkan penggantian ke metode berikut: -`getExtraSteps`: mendefinisikan nilai default untuk setiap parameter yang diterapkan untuk kontrol di Security Hub

> **Note**
>
> Setiap parameter dari Security Hub harus diberi nilai default

- `getInputParamsStepOutput`: mendefinisikan output untuk GetInputParams langkah runbook kontrol
- Setiap output memilikiname,`outputType`, dan`selector`. `selector`Harus menjadi pemilih yang sama yang digunakan dalam `getExtraSteps` metode override.
- `getRemediationParams`: mendefinisikan parameter yang diteruskan ke runbook remediasi, diambil dari output langkah. GetInputParams

Untuk melihat contoh, navigasikan ke `source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts` file.

Langkah 3: Integrasikan Setiap Runbook Kontrol dengan Playbook

Untuk setiap runbook kontrol yang dibuat pada langkah sebelumnya, Anda sekarang harus mengintegrasikannya dengan definisi infrastruktur di buku pedoman terkait. Ikuti langkah-langkah di bawah ini untuk setiap runbook kontrol.

> **Important**
>
> Jika Anda membuat runbook kontrol menggunakan YAMG mentah alih-alih TypeScript IAC, lewati ke bagian berikutnya.

Di */<playbook_name>*`/control_runbooks-construct.ts` Impor file runbook kontrol yang baru dibuat seperti:

```
import * as elasticache_2 from '../ssmdocs/SC_ElastiCache.2';
```

Selanjutnya, pergi ke array untuk

```
const controlRunbooksRecord: Record<string, any>
```

Dan tambahkan entri baru yang memetakan ID kontrol (khusus playbook) ke `createControlRunbook` metode yang Anda buat:

```
'ElastiCache.2': elasticache_2.createControlRunbook,
```

Tambahkan ID kontrol khusus playbook ke daftar remediasi seperti di bawah ini: *<playbook_name>*`\_remediations.ts`

```
{ control: 'ElastiCache.2', versionAdded: '2.3.0' },
```

`versionAdded`Bidang harus menjadi versi terbaru dari solusi. Jika menambahkan remediasi melanggar batas ukuran template, tingkatkan. `versionAdded` Anda dapat menyesuaikan jumlah remediasi yang disertakan dalam setiap tumpukan anggota playbook. `solution_env.sh`

Langkah 4: Buat Peran IAM Remediasi & Integrasikan Runbook Remediasi

Setiap remediasi memiliki peran IAM sendiri dengan izin khusus yang diperlukan untuk menjalankan runbook remediasi. Selain itu, `RunbookFactory.createRemediationRunbook` metode ini perlu dipanggil untuk menambahkan runbook remediasi yang Anda buat di Langkah 1 ke template solusi. CloudFormation

Dalam`remediation-runook-stack.ts`, setiap remediasi memiliki blok kode sendiri di `RemediationRunbookStack` kelas. Blok kode berikut menunjukkan pembuatan peran IAM baru dan integrasi runbook remediasi untuk remediasi .2: ElastiCache

```
    //-----------------------
    // EnableElastiCacheVersionUpgrades
    //
    {
      const remediationName = 'EnableElastiCacheVersionUpgrades'; // should match the
 name of your remediation runbook
      const inlinePolicy = new Policy(props.roleStack, `ASR-Remediation-Policy-
${remediationName}`);

      const remediationPolicy = new PolicyStatement();
```

```
      remediationPolicy.addActions('elasticache:ModifyCacheCluster');
      remediationPolicy.effect = Effect.ALLOW;
      remediationPolicy.addResources(`arn:${this.partition}:elasticache:*:
${this.account}:cluster:*`);
      inlinePolicy.addStatements(remediationPolicy);

      new SsmRole(props.roleStack, 'RemediationRole ' + remediationName, { // creates
 the remediation IAM role
        solutionId: props.solutionId,
        ssmDocName: remediationName,
        remediationPolicy: inlinePolicy,
        remediationRoleName: `${remediationRoleNameBase}${remediationName}`,
      });

      RunbookFactory.createRemediationRunbook(this, 'ASR ' + remediationName, { // adds
 the remediation runbook to the solution's cloudformation templates
        ssmDocName: remediationName,
        ssmDocPath: ssmdocs,
        ssmDocFileName: `${remediationName}.yaml`,
        scriptPath: `${ssmdocs}/scripts`,
        solutionVersion: props.solutionVersion,
        solutionDistBucket: props.solutionDistBucket,
        solutionId: props.solutionId,
        namespace: namespace,
      });
    }
```

Langkah 5: Perbarui Tes Unit

Kami merekomendasikan memperbarui dan menjalankan pengujian unit setelah menambahkan remediasi baru.

Pertama, Anda harus menambahkan ekspresi reguler baru (yang belum ditambahkan) ke dalam `source/test/regex_registry.ts` file. File ini memberlakukan pengujian untuk setiap ekspresi reguler baru yang disertakan dalam runbook solusi. Lihatlah `addElastiCacheClusterTestCases` fungsi sebagai contoh, yang digunakan untuk menguji ekspresi reguler yang digunakan dalam ElastiCache remediasi.

Terakhir, Anda harus memperbarui snapshot untuk setiap tumpukan. Snapshot adalah definisi CloudFormation template yang dikontrol versi yang digunakan untuk melacak perubahan yang dibuat pada infrastruktur ASR. Anda dapat memperbarui file snapshot ini dengan menjalankan perintah berikut dari `deployment` direktori:

```
./run-unit-tests.sh update
```

Sekarang Anda siap untuk menyebarkan remediasi baru Anda! Arahkan ke bagian Build and Deploy di bawah ini untuk mengetahui petunjuk tentang membangun dan menerapkan solusi dengan perubahan baru Anda.

Menambahkan buku pedoman baru

Unduh Respons Keamanan Otomatis di buku pedoman solusi AWS dan kode sumber penerapan dari repositori. GitHub

CloudFormation Sumber daya AWS dibuat dari komponen AWS CDK, dan sumber daya berisi kode template playbook yang dapat Anda gunakan untuk membuat dan mengonfigurasi buku pedoman baru. Untuk informasi selengkapnya tentang menyiapkan proyek Anda dan menyesuaikan buku pedoman Anda, lihat file README.md di. GitHub

AWS Systems Manager Parameter Store

Respons Keamanan Otomatis di AWS menggunakan AWS Systems Manager Parameter Store untuk penyimpanan data operasional. Parameter berikut disimpan di Parameter Store:

Nama	Nilai	Gunakan
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	Kunci AWS KMS yang akan mengenkripsi data untuk remediasi FSBP	Enkripsi data pelanggan, seperti CloudTrail log, sebagai bagian dari remediasi
`/Solutions/SO0111/CMK_ARN`	Kunci AWS KMS yang akan digunakan ASR untuk mengenkripsi data	Enkripsi data solusi
`/Solutions/SO0111/SNS_Topic_ARN`	ARN dari topik Amazon SNS untuk solusinya	Pemberitahuan peristiwa remediasi
`/Solutions/SO0111/SNS_Topic_Config.1`	Topik SNS untuk pembaruan AWS Config	Remediasi Config.1

Nama	Nilai	Gunakan
`/Solutions/SO0111/sendAnonymousMetrics`	`Yes`	Koleksi metrik anonim
`/Solutions/SO0111/version`	Versi solusi	
`/Solutions/SO0111/`*`<security standard long name>`*`/`*`<version>`* /status	`enabled`	Menunjukkan apakah standar aktif dalam solusi. Standar dapat dinonaktifkan untuk remediasi otomatis dengan mengubahnya menjadi `disabled`
`/Solutions/SO0111/`*`<security standard long name>`*`/` nama pendek	`String`	Nama singkat untuk standar keamanan. Sebagai contoh:`CIS`,`AFSBP`, `PCI`
`/Solutions/SO0111//`*`<security standard long name><version>`* */`*`<control>`* /remap	`String`	Ketika satu kontrol menggunakan remediasi yang sama dengan yang lain, parameter ini menyelesaikan pemetaan ulang

Topik Amazon SNS - Kemajuan Remediasi

Respons Keamanan Otomatis di AWS membuat topik Amazon SNS, SO0111-ASR_Topic. Topik ini digunakan untuk memposting pembaruan tentang kemajuan remediasi. Berikut ini adalah tiga pemberitahuan yang mungkin dikirim ke topik ini.

```
Remediation queued for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
Remediation failed for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
[.replaceable]`<control_ID>` remediation was successfully invoke via AWS Systems
 Manager in account [.replaceable]`<account_ID>`
```

Ini adalah pesan penyelesaian. Ini menunjukkan bahwa remediasi selesai tanpa kesalahan; namun, pengujian definitif untuk remediasi yang berhasil adalah validasi manual pemeriksaan AWS Config. and/or

Memfilter langganan topik SNS

Kebijakan filter langganan Amazon SNS:

1. Arahkan ke langganan topik SNS.
2. Di bawah Kebijakan filter langganan, pilih “Edit”.
3. Perluas “Kebijakan filter langganan” dan alihkan opsi “Kebijakan filter langganan” untuk mengaktifkan filter.
4. Pilih lingkup “Badan Pesan”.
5. Tambahkan kebijakan Anda ke editor JSON.
6. Simpan perubahan.

Contoh kebijakan:

Filter berdasarkan akun

```
{
"finding": {
"account": [
"111111111111",
"222222222222"
]
}
```

Filter untuk kesalahan

```
{
```

```
"severity": ["ERROR"]
}
```

Filter berdasarkan kontrol

```
{
"finding": {
"standard_control": ["S3.9","S3.6"]
}
}
```

Topik Amazon SNS - Alarm CloudWatch

Solusi ini menciptakan topik Amazon SNS,. `SO0111-ASR_Alarm_Topic` Topik ini digunakan untuk memposting peringatan alarm.

Rincian Alarm apa pun yang memasuki status ALARM akan dikirim ke topik ini.

Memulai Runbook pada Temuan Config

Solusi ini dapat memulai runbook berdasarkan temuan AWS Config kustom. Untuk melakukan ini, Anda perlu:

1. Temukan nama aturan AWS Config yang ingin Anda perbaiki. Ini dapat ditemukan di AWS Config atau dalam temuan yang dihasilkan oleh Security Hub untuk aturan ini.
2. Arahkan ke AWS Systems Manager Parameter Store dan pilih Create Parameter.
3. Nama aturan Anda harus `/Solutions/SO0111/` [.replaceable] `Rule name from Step 1`
4. Nilai harus diformat seperti itu:

```
{
"RunbookName":"Name of SSM runbook",
"RunbookRole": "Role that Orchestrator will assume"
}
```

1. RunbookName adalah bidang wajib dan akan menjadi runbook yang dijalankan saat Anda memperbaiki aturan Config ini. RunbookRole adalah peran yang akan diambil orkestrator saat

menjalankan peran ini. Ini bukan bidang wajib, dan jika ditinggalkan, orkestrator akan default menggunakan peran anggota akun.

2. Setelah ini diterapkan, Anda dapat memperbaiki aturan Config Anda menggunakan tindakan kustom “Remeate with ASR” yang ditemukan di Security Hub.

Referensi

Bagian ini mencakup informasi tentang fitur opsional untuk mengumpulkan metrik unik untuk solusi ini, petunjuk ke sumber daya terkait, dan daftar pembangun yang berkontribusi pada solusi ini.

Pengumpulan data anonim

Solusi ini mencakup opsi untuk mengirim metrik operasional anonim ke AWS. Kami menggunakan data ini untuk lebih memahami bagaimana pelanggan menggunakan solusi ini dan layanan serta produk terkait. Saat diaktifkan, informasi berikut dikumpulkan dan dikirim ke AWS:

- ID Solusi - Pengidentifikasi solusi AWS
- Unique ID (UUID) - Pengidentifikasi unik yang dibuat secara acak untuk setiap penerapan Respons dan Remediasi AWS Security Hub
- Timestamp - Stempel waktu pengumpulan data
- Data Instance - Informasi tentang penerapan tumpukan ini
- Konfigurasi solusi - Fitur diaktifkan dan parameter ditetapkan selama peluncuran awal
- Status - Status penerapan (solusi lulus atau gagal) atau (perbaikan lulus atau gagal)
- Pesan galat - Pesan kesalahan umum di bidang status
- Generator_ID - Informasi aturan Security Hub
- Jenis - Jenis dan nama remediasi
- ProductArn - Wilayah tempat Security Hub dikerahkan
- finding_triggered_by - Jenis remediasi yang dilakukan (tindakan kustom atau pemicu otomatis)

AWS memiliki data yang dikumpulkan melalui survei ini. Pengumpulan data tunduk pada Pemberitahuan Privasi AWS. Untuk memilih keluar dari fitur ini, selesaikan langkah-langkah berikut sebelum meluncurkan CloudFormation template AWS.

1. Unduh CloudFormation template AWS ke hard drive lokal Anda.
2. Buka CloudFormation template AWS dengan editor teks.
3. Ubah bagian pemetaan CloudFormation template AWS dari:

```
Mappings:
```

```
Solution:
Data:
SendAnonymizedUsageData: 'Yes'
```

ke:

```
Mappings:
Solution:
Data:
SendAnonymizedUsageData: 'No'
```

4. Masuk ke CloudFormation konsol AWS.
5. Pilih Buat tumpukan.
6. Pada halaman Buat tumpukan, Tentukan templat bagian, pilih Unggah file templat.
7. Di bawah Unggah file templat, pilih Pilih file dan pilih templat yang diedit dari drive lokal Anda.
8. Pilih Berikutnya dan ikuti langkah-langkah dalam Luncurkan tumpukan di bagian Automated deployment dari panduan ini.

Sumber daya terkait

- Respons dan Remediasi Otomatis dengan AWS Security Hub
- Tolok ukur Yayasan Amazon Web Services CIS, versi 1.2.0
- Standar Praktik Terbaik AWS Foundational Security
- Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)
- Institut Nasional Standar dan Teknologi (NIST) SP 800-53 Rev. 5

Kontributor

Individu-individu berikut berkontribusi pada dokumen ini:

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat

- Tim Mekari
- Aaron Schuetter
- Andrew Yankowsky
- Josh Lumut
- Ryan Garay
- Thiemo Belmega
- Mykhailo Markhain

Revisi

Tanggal publikasi: Agustus 2020 (pembaruan terakhir: Januari 2025)

Kunjungi ChangeIOG.md di GitHub repositori kami untuk melacak peningkatan dan perbaikan khusus versi.

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa jaminan, pernyataan, atau ketentuan dalam bentuk apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

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