Respons Insiden Keamanan AWS Panduan Pengguna

Versi December 1, 2024

Respons Insiden Keamanan AWS Panduan Pengguna:

Table of Contents

Apa itu Respons Insiden Keamanan AWS?

Respons Insiden Keamanan AWS membantu Anda dengan cepat mempersiapkan, menanggapi, dan menerima panduan untuk membantu memulihkan diri dari insiden keamanan. Ini termasuk insiden seperti pengambilalihan akun, pelanggaran data, dan serangan ransomware.

Respons Insiden Keamanan AWS triase temuan, meningkatkan peristiwa keamanan, dan mengelola kasus yang membutuhkan perhatian segera Anda. Selain itu, Anda memiliki akses ke Tim Respons Insiden AWS Pelanggan (CIRT), yang akan menyelidiki sumber daya yang terkena dampak.

> **Note**
>
> Tidak ada jaminan sumber daya yang terkena dampak dapat dipulihkan. Kami merekomendasikan untuk membuat dan memelihara cadangan untuk sumber daya yang dapat memengaruhi kebutuhan bisnis Anda.

Respons Insiden Keamanan AWS bekerja dengan layanan AWS Deteksi dan Respons lainnya, memandu Anda melalui seluruh siklus hidup insiden — mulai dari deteksi hingga pemulihan.

Daftar Isi

Konfigurasi yang didukung

Respons Insiden Keamanan AWS mendukung konfigurasi bahasa dan wilayah berikut:

- Bahasa: Respons Insiden Keamanan AWS menyediakan dukungan bahasa Inggris khusus. Dukungan bahasa Jepang terbatas pada jam kerja Waktu Standar Jepang dan dilengkapi dengan batasan khusus:
-
  > **Note**
  >
  > Dukungan bahasa Jepang diberikan dengan upaya terbaik selama jam kerja (09:00-17:00, Senin-Jumat, tidak termasuk hari libur)
- AWS Wilayah yang Didukung:

Respons Insiden Keamanan AWS tersedia dalam subset dari. Wilayah AWS Di Wilayah yang didukung ini, Anda membuat keanggotaan, membuat dan melihat kasus, dan mengakses dasbor.

- AS Timur (Ohio)
- AS Barat (Oregon)
- AS Timur (Virginia)
- EU (Frankfurt)
- EU (Ireland)
- EU (London)
- Eropa (Paris)
- EU (Stockholm)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- (Canada (Central)
- Amerika Selatan (Sao Paulo)

Saat Anda mengaktifkan fitur pemantauan dan investigasi, Respons Insiden Keamanan AWS pantau GuardDuty temuan Amazon dari semua iklan aktif Wilayah AWS. Sebagai praktik keamanan terbaik, AWS rekomendasikan untuk mengaktifkan GuardDuty di semua AWS Wilayah yang didukung. Konfigurasi ini memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa, bahkan di Wilayah AWS tempat Anda tidak aktif menyebarkan sumber daya. Dengan demikian, Anda meningkatkan postur keamanan Anda secara keseluruhan dan mempertahankan cakupan deteksi ancaman yang komprehensif di seluruh AWS lingkungan Anda.

> **Note**
>
> Amazon GuardDuty melaporkan temuan untuk wilayah yang dikonfigurasi. Jika Anda memilih untuk tidak mengaktifkan layanan di wilayah tertentu, maka peringatan tidak akan tersedia.

Ringkasan Fitur

Monitoring dan Investigasi

Respons Insiden Keamanan AWS dengan cepat meninjau peringatan keamanan dari Amazon GuardDuty dan integrasi pihak ketiga dengan AWS Security Hub, mengurangi jumlah yang perlu dianalisis tim Anda. Ini mengonfigurasi aturan penekanan berdasarkan lingkungan Anda untuk mengurangi peringatan prioritas rendah yang perlu Anda lakukan triase dan selidiki.

Merampingkan respons insiden

Skala dan jalankan respons insiden dalam hitungan menit dengan pemangku kepentingan, layanan pihak ketiga, dan alat yang relevan.

Solusi keamanan untuk swalayan

Respons Insiden Keamanan AWS menyediakan APIs untuk mengintegrasikan dan memungkinkan Anda untuk membangun solusi keamanan khusus Anda sendiri.

Dasbor untuk visibilitas

Pantau dan ukur kesiapan respons insiden.

Postur keamanan

Akses praktik AWS terbaik dan alat yang diperiksa untuk penilaian keamanan dan investigasi respons insiden cepat.

Bantuan yang dipercepat

Connect dengan AWS Customer Incident Response Team (CIRT) untuk menyelidiki, memuat, dan menerima panduan tentang cara memulihkan diri dari peristiwa keamanan.

Kesiapan dan kesiapan

Terapkan pemberitahuan yang disederhanakan dengan menyiapkan tim Respons Insiden Anda yang memicu peringatan ke individu atau grup yang ditunjuk, dengan kebijakan izin yang telah ditentukan sebelumnya.

Konsep dan Terminologi

Istilah dan konsep berikut ini penting untuk memahami Respons Insiden Keamanan AWS layanan dan cara kerjanya.

Lingkup: Respons Insiden Keamanan AWS sejalan dengan National Institute of Standards and Techology (NIST) 800-61 Computer Security Incident Handling Guide, memberikan pendekatan yang konsisten untuk manajemen acara keamanan yang terkait dengan praktik terbaik industri.

Analisis: Investigasi terperinci dan pemeriksaan peristiwa keamanan untuk memahami ruang lingkup, dampak, dan akar penyebabnya.

Respons Insiden Keamanan AWS portal layanan: Portal swalayan bagi Anda untuk memulai dan mengelola kasus peristiwa keamanan. Komunikasi dan pelaporan yang sedang berlangsung difasilitasi melalui sistem tiket, pemberitahuan otomatis, dan keterlibatan langsung dengan tim layanan.

Komunikasi: Dialog yang sedang berlangsung dan berbagi informasi antara tim AWS Security Incident Response dan pelanggan selama proses respons insiden.

Penahanan, Pemberantasan, dan Pemulihan: Pencegahan aktivitas tambahan yang tidak sah (penahanan), ditambah dengan penghapusan sumber daya yang tidak sah dan kerentanan asli (pemberantasan), dan memulihkan sumber daya untuk kembali ke bisnis seperti biasa.

Continuous Improvement: Respons Insiden Keamanan AWS menggabungkan umpan balik dan pelajaran dari keterlibatan sebelumnya untuk meningkatkan kemampuan deteksi, proses investigasi, dan tindakan remediasi. Respons Insiden Keamanan AWS juga tetap up-to-date dengan ancaman keamanan terbaru dan praktik terbaik untuk mengatasi tantangan keamanan yang berkembang.

Peristiwa Keamanan Siber: Tindakan yang menggunakan sistem informasi atau jaringan untuk menghasilkan efek buruk pada sistem, jaringan, atau informasi yang dikandungnya.

Insiden Keamanan Siber: Pelanggaran atau ancaman pelanggaran kebijakan keamanan komputer, kebijakan penggunaan yang dapat diterima, atau praktik keamanan standar.

Tim Respons Insiden: Sekelompok individu yang memberikan dukungan selama acara keamanan aktif. Untuk kasus yang AWS didukung, ini adalah Tim Respons Insiden AWS Pelanggan (CIRT).

Alur Kerja Respons Insiden: Urutan langkah dan aktivitas yang ditentukan yang terlibat dalam end-to-end pengelolaan peristiwa keamanan, selaras dengan standar NIST 800-61.

Investigative Tooling: Respons Insiden Keamanan AWS alat dan peran terkait layanan yang digunakan untuk meninjau kesehatan operasional akun dan sumber daya Anda.

Pelajaran yang Dipelajari: Tinjauan dan dokumentasi respons peristiwa keamanan untuk mengidentifikasi area untuk perbaikan dan menginformasikan perencanaan respons insiden di masa depan.

Pemantauan dan Investigasi: Respons Insiden Keamanan AWS dengan cepat meninjau peringatan keamanan dari Amazon GuardDuty, membawa ke garis depan peringatan paling penting yang perlu dianalisis tim Anda. Ini mengonfigurasi aturan penekanan berdasarkan spesifikasi lingkungan Anda untuk mencegah peringatan yang tidak perlu.

Persiapan: Kegiatan yang dilakukan untuk membuat organisasi siap merespons dan mengelola peristiwa keamanan secara efektif, seperti mengembangkan rencana respons insiden dan prosedur pengujian.

Pelaporan dan Komunikasi: Proses yang digunakan untuk memberi Anda informasi selama proses respons insiden, termasuk pemberitahuan otomatis, jembatan panggilan, dan pengiriman artefak investigasi. Respons Insiden Keamanan AWS menyediakan satu dasbor terpusat AWS Management Console untuk mengelola semua Respons Insiden Keamanan AWS upaya Anda.

Responder Generated Intelligence: indikator kompromi; taktik, teknik, dan prosedur; dan pola terkait yang diamati oleh investigasi AWS CIRT.

Keahlian Acara Keamanan: Pengetahuan dan keterampilan khusus yang diperlukan untuk merespons dan mengelola peristiwa keamanan secara efektif, terutama dalam konteks AWS cloud.

Model Tanggung Jawab Bersama: Pembagian tanggung jawab keamanan antara AWS dan pelanggan, di mana AWS bertanggung jawab atas keamanan cloud, dan pelanggan bertanggung jawab atas keamanan di cloud.

Ancaman Intelijen: Umpan data internal dan eksternal yang berisi rincian aktivitas yang tidak sah untuk membantu mengidentifikasi dan menanggapi ancaman keamanan yang berkembang.

Sistem Tiket: Platform manajemen kasus khusus yang memungkinkan Anda melakukan onboard dan mengelola kasus peristiwa keamanan, menambahkan lampiran, dan melacak siklus hidup respons insiden.

Triase: Penilaian awal dan prioritas peristiwa keamanan untuk menentukan respons yang tepat dan langkah selanjutnya.

Alur Kerja: Urutan yang ditentukan dari langkah-langkah dan kegiatan yang terlibat dalam end-to-end pengelolaan peristiwa keamanan.

Memulai

Daftar Isi

Pilih akun keanggotaan

Akun keanggotaan adalah AWS akun yang digunakan untuk mengonfigurasi detail akun, menambah dan menghapus detail untuk tim respons insiden Anda, dan tempat semua peristiwa keamanan aktif dan historis dapat dibuat dan dikelola. Disarankan agar Anda menyelaraskan akun Respons Insiden Keamanan AWS keanggotaan Anda ke akun yang sama yang telah Anda aktifkan untuk layanan seperti Amazon GuardDuty dan AWS Security Hub.

Anda memiliki dua opsi untuk memilih akun keanggotaan AWS Security Incident Response Anda menggunakan AWS Organizations. Anda dapat membuat keanggotaan di akun manajemen Organisasi atau di akun administrator yang didelegasikan Organizations.

Gunakan akun administrator yang didelegasikan: Tugas administratif Respons Insiden AWS Keamanan dan manajemen kasus terletak di akun administrator yang didelegasikan. Sebaiknya gunakan administrator terdelegasi yang sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya. Berikan 12 digit ID akun administrator yang didelegasikan dan kemudian masuk ke akun itu untuk melanjutkan.

> **Important**
>
> Bila Anda menggunakan akun administrator yang didelegasikan sebagai bagian dari penyiapan, Respons Insiden Keamanan AWS tidak dapat secara otomatis membuat peran terkait layanan triase yang diperlukan di akun AWS Organizations manajemen Anda. Anda dapat menggunakan IAM untuk membuat peran ini di akun AWS Organizations manajemen Anda
>
> Untuk membuat peran terkait layanan (konsol)
>
> 1. Masuk ke akun AWS Organizations manajemen Anda.

2. Akses AWS CloudShell jendela atau akses akun melalui CLI dengan metode pilihan Anda.
3. Gunakan perintah CLI `aws iam create-service-linked-role --aws-service-name triage.security-ir.amazonaws.com`
4. (Opsional) Untuk memverifikasi perintah bekerja Anda dapat menjalankan perintah `aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage`
5. Tinjau peran, lalu pilih Buat peran.

Gunakan akun yang saat ini masuk: Memilih akun ini berarti akun saat ini akan ditetapkan sebagai akun keanggotaan pusat untuk Respons Insiden Keamanan AWS keanggotaan Anda. Individu dalam organisasi Anda perlu mengakses layanan melalui akun ini untuk membuat, mengakses, dan mengelola kasus yang aktif dan diselesaikan.

Pastikan Anda memiliki izin yang memadai untuk dikelola Respons Insiden Keamanan AWS.

Lihat Menambahkan dan menghapus izin identitas IAM untuk langkah-langkah spesifik untuk menambahkan izin.

Lihat kebijakan Respons Insiden Keamanan AWS terkelola.

Untuk memverifikasi izin IAM, Anda dapat mengikuti langkah-langkah berikut:

- Periksa Kebijakan IAM: Tinjau kebijakan IAM yang dilampirkan pada pengguna, grup, atau peran Anda untuk memastikannya memberikan izin yang diperlukan. Anda dapat melakukan ini dengan menavigasi ke, pilih `Users` opsi https://console.aws.amazon.com/iam/, pilih pengguna tertentu, dan kemudian pada halaman ringkasan mereka, buka `Permissions` tab di mana Anda dapat melihat daftar semua kebijakan terlampir; Anda dapat memperluas setiap baris kebijakan untuk melihat detailnya.
- Uji Izin: Cobalah untuk melakukan tindakan yang Anda perlukan untuk memverifikasi izin. Misalnya, jika Anda perlu mengakses kasing, cobalah`ListCases`. Jika Anda tidak memiliki izin yang diperlukan, Anda akan menerima pesan kesalahan.
- Gunakan AWS CLI atau SDK: Anda dapat menggunakan AWS Command Line Interface atau AWS SDK dalam bahasa pemrograman pilihan Anda untuk menguji izin. Misalnya, dengan AWS Command Line Interface, Anda dapat menjalankan `aws sts get-caller-identity` perintah untuk memverifikasi izin pengguna Anda saat ini.

- Periksa AWS CloudTrail log: Tinjau CloudTrail log untuk melihat apakah tindakan yang Anda coba lakukan sedang dicatat. Hal ini dapat membantu Anda mengidentifikasi masalah izin apa pun.
- Gunakan simulator kebijakan IAM: Simulator kebijakan IAM adalah alat yang memungkinkan Anda menguji kebijakan IAM dan melihat efeknya terhadap izin Anda.

> **Note**
>
> Langkah-langkah spesifik dapat bervariasi tergantung pada AWS layanan dan tindakan yang Anda coba lakukan.

Menyiapkan rincian keanggotaan

- Pilih Wilayah AWS tempat keanggotaan dan kasus Anda akan disimpan.

> **Warning**
>
> Anda tidak dapat mengubah default Wilayah AWS setelah pendaftaran keanggotaan awal.

- Anda dapat memilih nama untuk keanggotaan ini secara opsional.
- Kontak Primer dan Sekunder harus disediakan sebagai bagian dari alur kerja membuat keanggotaan. Kontak ini secara otomatis disertakan sebagai bagian dari tim respons insiden Anda. Setidaknya dua kontak harus ada untuk satu keanggotaan yang juga memastikan minimal dua kontak dimasukkan dalam tim respons insiden.
- Tentukan tag opsional untuk keanggotaan Anda. Tag membantu Anda melacak AWS biaya dan mencari sumber daya.

Mengaitkan akun dengan AWS Organizations

Keanggotaan Anda memberikan hak cakupan pada semua yang Akun AWS ditautkan AWS Organizations. Akun terkait akan diperbarui secara otomatis saat akun ditambahkan atau dihapus dari organisasi Anda.

Siapkan respons proaktif dan alur kerja triaging peringatan

Respons proaktif dan alur kerja triaging peringatan adalah fitur opsional untuk mengaktifkan dalam organisasi Anda untuk memantau layanan keamanan yang diaktifkan. Pilih sakelar di sebelah fitur untuk mengaktifkan.

Jika Anda mengalami masalah orientasi, silakan buat AWS Dukungan kasus untuk bantuan tambahan. Pastikan untuk menyertakan detail termasuk Akun AWS ID dan kesalahan apa pun yang mungkin Anda lihat selama proses penyiapan.

Respons proaktif dan triaging peringatan: Respons Insiden Keamanan AWS memantau dan menyelidiki peringatan yang dihasilkan dari integrasi Amazon dan Security GuardDuty Hub. Untuk menggunakan fitur ini, Amazon GuardDuty harus diaktifkan. Respons Insiden Keamanan AWS melakukan triase peringatan prioritas rendah dengan otomatisasi layanan sehingga tim Anda dapat fokus pada masalah yang paling kritis. Untuk informasi tambahan tentang cara Respons Insiden Keamanan AWS kerja dengan Amazon GuardDuty dan AWS Security Hub, silakan tinjau bagian Deteksi dan Analisis pada panduan pengguna.

Fitur ini memungkinkan Respons Insiden Keamanan AWS untuk memantau dan menyelidiki temuan di semua akun dan aktif didukung Wilayah AWS di organisasi Anda. Untuk memfasilitasi fungsi ini, Respons Insiden Keamanan AWS secara otomatis membuat peran terkait layanan di semua akun anggota di akun Anda. AWS Organizations Namun, untuk akun manajemen, Anda harus membuat peran terkait layanan secara manual untuk mengaktifkan pemantauan.

Layanan tidak dapat membuat peran terkait layanan di akun manajemen. Anda harus membuat peran ini secara manual di akun manajemen dengan bekerja dengan set AWS CloudFormation tumpukan.

Penahanan: Jika terjadi insiden keamanan, Respons Insiden Keamanan AWS dapat melakukan tindakan penahanan untuk mengurangi dampak dengan cepat, seperti mengisolasi host yang dikompromikan atau memutar kredensional. Security Incident Response tidak mengaktifkan kemampuan penahanan secara default. Untuk menjalankan tindakan penahanan ini, Anda harus terlebih dahulu memberikan izin yang diperlukan ke layanan. Ini dapat dilakukan dengan menerapkan AWS CloudFormation StackSet, yang menciptakan peran yang diperlukan.

Tugas pengguna

Daftar Isi

Dasbor

Di Respons Insiden Keamanan AWS konsol, dasbor memberi Anda gambaran umum tentang tim respons insiden Anda, status respons proaktif Anda, dan hitungan kasus bergulir empat minggu.

Pilih `View incident response team` untuk mengakses detail rekan tim respons insiden Anda.

Pilih `proactive response` untuk mengidentifikasi apakah triaging peringatan diaktifkan. Jika `alert triaging` alur kerja tidak diaktifkan, Anda dapat memantau statusnya dan memilih `Proactive Response` untuk mengaktifkannya.

Bagian Kasus Saya di dasbor menunjukkan jumlah kasus yang AWS didukung terbuka dan tertutup, bersama dengan kasus yang dikelola sendiri yang ditetapkan kepada Anda dalam periode yang ditentukan. Ini juga menunjukkan waktu yang dibutuhkan untuk menyelesaikan kasus tertutup dalam beberapa jam.

Mengelola Tim Respons Insiden saya

Tim respons insiden Anda berisi pemangku kepentingan untuk proses respons insiden. Anda dapat mengonfigurasi hingga sepuluh pemangku kepentingan sebagai bagian dari keanggotaan Anda.

Contoh untuk pemangku kepentingan internal termasuk anggota tim respons insiden Anda, analis keamanan, pemilik aplikasi, dan tim kepemimpinan keamanan Anda.

Contoh untuk pemangku kepentingan eksternal termasuk individu dari vendor perangkat lunak independen (ISV) dan penyedia layanan terkelola (MSP) yang ingin Anda sertakan dalam proses respons insiden.

> **Note**
>
> Menyiapkan tim respons insiden Anda tidak secara otomatis memberi rekan tim akses ke sumber daya layanan seperti keanggotaan dan kasus. Anda dapat menggunakan kebijakan AWS terkelola Respons Insiden Keamanan AWS untuk memberikan akses baca dan tulis ke sumber daya. Klik di sini untuk mempelajari lebih lanjut.

Rekan tim respons insiden Anda yang ditentukan pada tingkat keanggotaan akan ditambahkan secara otomatis ke kasus apa pun. Anda dapat menambahkan atau menghapus rekan tim kapan saja setelah kasus dibuat.

Tim respons insiden akan menerima pemberitahuan email tentang peristiwa berikut:

- Kasus (buat, hapus, perbarui)
- Komentar (buat, hapus, perbarui)
- Lampiran (buat, hapus, perbarui)
- Keanggotaan (buat, perbarui, batalkan, lanjutkan)

Asosiasi akun ke AWS Organizations

Saat Anda mengaktifkan Respons Insiden Keamanan AWS, keanggotaan akan dibuat dan disejajarkan dengan Anda AWS Organizations. Semua akun dalam Organizations Anda selaras dengan Respons Insiden Keamanan AWS keanggotaan Anda.

Untuk detail lebih lanjut, silakan lihat Mengelola Respons Insiden Keamanan AWS akun dengan AWS Organizations.

Monitoring dan Investigasi

Respons Insiden Keamanan AWS ulasan dan triase peringatan keamanan dari Amazon GuardDuty dan AWS Security Hub, kemudian mengonfigurasi aturan penekanan berdasarkan lingkungan Anda untuk mencegah peringatan yang tidak perlu. Tim AWS CIRT menyelidiki temuan non-triaged

dan dengan cepat meningkatkan dan memandu tim Anda untuk dengan cepat mengatasi masalah potensial. Jika diinginkan, Anda dapat memberikan Respons Insiden Keamanan AWS izin untuk menerapkan tindakan penahanan atas nama Anda.

Respons Insiden Keamanan AWS sejajar dengan Panduan Penanganan peristiwa Keamanan Komputer NIST 800-61r2 untuk Respons peristiwa Keamanan. Dengan menyelaraskan standar industri ini, Respons Insiden Keamanan AWS memberikan pendekatan yang konsisten untuk manajemen acara keamanan dan mematuhi praktik terbaik dalam mengamankan dan menanggapi peristiwa keamanan di lingkungan Anda. AWS

Ketika Respons Insiden Keamanan AWS layanan mengidentifikasi peringatan keamanan atau Anda meminta bantuan keamanan, AWS CIRT menyelidiki. Tim mengumpulkan peristiwa log dan data layanan seperti GuardDuty peringatan, triase dan analisis data tersebut, melakukan aktivitas remediasi dan penahanan, dan menyediakan pelaporan pasca-insiden.

Daftar Isi

Persiapkan

Respons Insiden Keamanan AWS Tim menyelidiki dan bermitra dengan Anda selama siklus hidup respons peristiwa keamanan. Disarankan agar Anda mengatur tim ini dan menetapkan izin yang diperlukan sebelum peristiwa keamanan terjadi.

Mendeteksi dan Menganalisis

Respons Insiden Keamanan AWS monitor, triase, menyelidiki temuan keamanan dari Amazon GuardDuty dan integrasi melalui. AWS Security Hub Tindakan tambahan yang secara signifikan dapat meningkatkan ruang lingkup dan efektivitas Respons Insiden Keamanan AWS kemampuan pemantauan dan investigasi meliputi:

Mengaktifkan sumber deteksi yang didukung

> **Note**
>
> Respons Insiden Keamanan AWS Biaya layanan tidak termasuk penggunaan dan biaya dan biaya lain yang terkait dengan sumber deteksi atau penggunaan AWS layanan lain yang didukung. Silakan merujuk ke fitur individual atau halaman layanan untuk detail biaya.

Amazon GuardDuty

GuardDuty adalah layanan deteksi ancaman yang terus memantau, menganalisis, dan memproses sumber data dan log di AWS lingkungan Anda. Pengaktifan tidak GuardDuty diperlukan untuk digunakan Respons Insiden Keamanan AWS; namun, untuk menggunakan respons proaktif dan fitur triaging peringatan Amazon GuardDuty harus diaktifkan.

Untuk mengaktifkan GuardDuty di seluruh organisasi Anda, silakan lihat `Setting up GuardDuty` bagian Panduan GuardDuty Pengguna Amazon.

Kami sangat menyarankan agar Anda mengaktifkan GuardDuty semua yang didukung Wilayah AWS. Hal ini memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa bahkan di wilayah yang tidak aktif Anda gunakan. Untuk informasi selengkapnya, rujuk GuardDuty Wilayah Amazon dan titik akhir

Mengaktifkan GuardDuty menyediakan Respons Insiden Keamanan AWS akses ke data deteksi ancaman kritis, meningkatkan kemampuannya untuk mengidentifikasi dan menanggapi potensi masalah keamanan di lingkungan Anda AWS .

AWS Security Hub

Security Hub dapat menangkap temuan keamanan dari beberapa AWS layanan dan mendukung solusi keamanan pihak ketiga. Integrasi ini dapat membantu Respons Insiden Keamanan AWS memantau dan menyelidiki temuan yang berasal dari alat deteksi lainnya.

Untuk mengaktifkan integrasi Security Hub with Organizations, silakan lihat Panduan AWS Security Hub Pengguna.

Ada beberapa cara untuk mengaktifkan integrasi di Security Hub. Untuk integrasi produk pihak ketiga, Anda mungkin perlu membeli integrasi dari AWS Marketplace, dan kemudian mengkonfigurasi integrasi. Informasi integrasi menyediakan tautan untuk menyelesaikan tugas-tugas ini. Pelajari lebih lanjut tentang cara mengaktifkan AWS Security Hub integrasi.

Respons Insiden Keamanan AWS dapat memantau dan menyelidiki temuan dari alat-alat berikut ketika mereka terintegrasi dengan AWS Security Hub:

- CrowdStrike — CrowdStrike Elang
- Lacework — Lacework
- Trend Micro - Cloud One

Dengan mengaktifkan integrasi ini, Anda dapat secara signifikan meningkatkan ruang lingkup dan efektivitas Respons Insiden Keamanan AWS kemampuan pemantauan dan investigasi.

Menganalisis temuan.

Respons Insiden Keamanan AWS otomatisasi dan tim layanan AWS CIRT akan menganalisis semua temuan dari alat yang didukung. Kami akan mulai belajar tentang lingkungan Anda dengan berkomunikasi dengan Anda menggunakan AWS Support Cases. Misalnya, ketika kita perlu memahami apakah suatu temuan adalah perilaku yang diharapkan atau harus ditingkatkan menjadi suatu insiden. Saat kami belajar lebih banyak dari lingkungan Anda, kami akan menyesuaikan layanan dan mengurangi jumlah komunikasi.

Melaporkan suatu peristiwa.

Anda dapat meningkatkan acara keamanan melalui portal Respons Insiden Keamanan AWS layanan. Penting untuk tidak menunggu selama acara keamanan. Respons Insiden Keamanan AWS menggunakan teknik otomatis dan manual untuk menyelidiki peristiwa keamanan, menganalisis log, dan mencari pola anomali. Kemitraan dan pemahaman Anda tentang lingkungan Anda mempercepat analisis ini.

Berkomunikasi.

Respons Insiden Keamanan AWS membuat Anda mendapat informasi selama penyelidikan dengan melibatkan kontak keamanan Anda melalui kasus kejadian. Beberapa rekan tim dapat mendukung acara Anda, semua menggunakan tiket acara untuk konten dan pembaruan yang disediakan pelanggan. AWS

Komunikasi dapat mencakup pemberitahuan otomatis ketika peringatan keamanan dihasilkan; komunikasi selama analisis acara; membangun jembatan panggilan; analisis artefak yang sedang berlangsung seperti file log; dan mendapatkan hasil investigasi kepada Anda selama acara keamanan.

Layanan ini akan membuat Respons Insiden Keamanan AWS kasus untuk berkomunikasi dengan tim Anda. Kami akan membuat kasus terhadap akun keanggotaan Anda. Pendekatan ini memusatkan komunikasi dari semua akun Anda ke satu tempat. Awalan “[Kasus proaktif]” membantu mengidentifikasi kasus yang diprakarsai oleh. Respons Insiden Keamanan AWS

Dengan terlibat secara aktif dengan komunikasi ini dan memberikan tanggapan tepat waktu, Anda dapat membantu Respons Insiden Keamanan AWS layanan untuk:

- Lebih memahami lingkungan Anda dan perilaku yang diharapkan.
- Kurangi positif palsu dari waktu ke waktu.
- Meningkatkan akurasi dan relevansi peringatan.
- Pastikan respons cepat terhadap insiden keamanan asli.
- Ingat, efektivitas Respons Insiden Keamanan AWS layanan meningkat dengan kolaborasi Anda, yang mengarah ke AWS lingkungan yang lebih aman dan dipantau secara efisien.

Mengandung

Respons Insiden Keamanan AWS bermitra dengan Anda untuk memuat acara. Anda dapat mengonfigurasi peran layanan Respons Insiden Keamanan AWS untuk mengambil tindakan otomatis dan manual di akun Anda sebagai respons terhadap peringatan. Anda juga dapat melakukan penahanan sendiri atau dalam kemitraan dengan hubungan pihak ketiga Anda dengan menggunakan dokumen SSM.

Bagian penting dari penahanan adalah pengambilan keputusan; seperti apakah akan mematikan sistem, mengisolasi sumber daya dari jaringan, mematikan akses, atau mengakhiri sesi. Keputusan ini dibuat lebih mudah ketika ada strategi dan prosedur yang telah ditentukan untuk menahan acara tersebut. Respons Insiden Keamanan AWS menyediakan strategi penahanan, memberi tahu Anda tentang dampak potensial, dan memandu Anda untuk memaksakan solusi hanya setelah Anda mempertimbangkan dan menyetujui risiko yang terlibat.

Respons Insiden Keamanan AWS mengeksekusi tindakan penahanan yang didukung atas nama Anda untuk mempercepat respons dan mengurangi waktu yang dimiliki pelaku ancaman untuk berpotensi menyebabkan kerusakan di lingkungan Anda. Kemampuan ini memungkinkan mitigasi ancaman yang teridentifikasi dengan lebih cepat, meminimalkan potensi dampak, dan meningkatkan postur keamanan Anda secara keseluruhan. Ada opsi penahanan yang berbeda tergantung pada sumber daya yang dianalisis. Tindakan penahanan yang didukung adalah:

- EC2 Penahanan: Otomatisasi `AWSSupport-ContainEC2Instance` penahanan melakukan penahanan jaringan reversibel dari sebuah EC2 instance, membiarkan instance utuh dan berjalan, tetapi mengisolasinya dari aktivitas jaringan baru dan mencegahnya berkomunikasi dengan sumber daya di dalam dan di luar VPC Anda.

  > **Important**
  >
  > Penting untuk dicatat bahwa koneksi yang dilacak yang ada tidak akan dimatikan sebagai akibat dari perubahan kelompok keamanan - hanya lalu lintas future yang akan diblokir secara efektif oleh grup keamanan baru dan dokumen SSM ini. Informasi lebih lanjut tersedia di bagian penahanan sumber dari panduan teknis layanan.

- Penahanan IAM: Otomatisasi `AWSSupport-ContainIAMPrincipal` penahanan melakukan penahanan jaringan reversibel dari pengguna atau peran IAM, meninggalkan pengguna atau peran dalam IAM, tetapi mengisolasinya dari berkomunikasi dengan sumber daya dalam akun Anda.
- Penahanan S3: Otomatisasi `AWSSupport-ContainS3Resource` penahanan melakukan penahanan yang dapat dibalik dari bucket S3, meninggalkan objek di bucket, dan mengisolasi bucket atau objek Amazon S3 dengan memodifikasi kebijakan aksesnya.

> **Important**
>
> Respons Insiden Keamanan AWS tidak mengaktifkan kemampuan penahanan secara default, untuk menjalankan tindakan penahanan ini, Anda harus terlebih dahulu memberikan izin yang diperlukan untuk layanan menggunakan peran. Anda dapat membuat peran ini secara individual per akun atau di seluruh organisasi Anda dengan Bekerja dengan AWS CloudFormation stacksets, yang membuat peran yang diperlukan.

Respons Insiden Keamanan AWS mendorong Anda untuk mempertimbangkan strategi penahanan untuk setiap jenis acara besar yang sesuai dengan selera risiko Anda. Dokumentasikan kriteria yang jelas untuk membantu pengambilan keputusan selama suatu acara. Kriteria yang perlu dipertimbangkan meliputi:

- Potensi kerusakan sumber daya
- Pelestarian bukti dan persyaratan peraturan
- Ketidaktersediaan layanan (misalnya, konektivitas jaringan, layanan yang diberikan kepada pihak eksternal)

- Waktu dan sumber daya yang dibutuhkan untuk mengimplementasikan strategi
- Efektivitas strategi (misalnya, penahanan sebagian vs penuh)
- Permanen solusi (misalnya, reversibel vs. ireversibel)
- Durasi solusi (misalnya, solusi darurat, solusi sementara, solusi permanen) Terapkan kontrol keamanan yang dapat menurunkan risiko dan memberikan waktu untuk menentukan dan menerapkan strategi penahanan yang lebih efektif.

Respons Insiden Keamanan AWS menyarankan pendekatan bertahap untuk mencapai penahanan yang efisien dan efektif, yang melibatkan strategi jangka pendek dan jangka panjang berdasarkan jenis sumber daya.

- Strategi penahanan
  - Dapat Respons Insiden Keamanan AWS mengidentifikasi ruang lingkup acara keamanan?
    - Jika ya, identifikasi semua sumber daya (pengguna, sistem, sumber daya).
    - Jika tidak, selidiki secara paralel dengan mengeksekusi langkah berikutnya pada sumber daya yang diidentifikasi.
  - Bisakah sumber daya diisolasi?
    - Jika ya, maka lanjutkan untuk mengisolasi sumber daya yang terpengaruh.
    - Jika tidak, maka bekerja dengan pemilik dan manajer sistem untuk menentukan tindakan lebih lanjut yang diperlukan untuk mengatasi masalah.
  - Apakah semua sumber daya yang terpengaruh terisolasi dari sumber daya yang tidak terpengaruh?
    - Jika ya, lanjutkan ke langkah berikutnya.
    - Jika tidak, maka teruslah mengisolasi sumber daya yang terkena dampak untuk menyelesaikan penahanan jangka pendek dan mencegah peristiwa meningkat lebih lanjut.
- Pencadangan sistem
  - Apakah salinan cadangan dari sistem yang terpengaruh dibuat untuk analisis lebih lanjut?
  - Apakah salinan forensik dienkripsi dan disimpan di lokasi yang aman?
    - Jika ya, lanjutkan ke langkah berikutnya.
    - Jika tidak, enkripsi gambar forensik, lalu simpan di lokasi yang aman untuk mencegah penggunaan, kerusakan, dan gangguan yang tidak disengaja.

Membasmi

Selama fase pemberantasan, penting untuk mengidentifikasi dan menangani semua akun, sumber daya, dan contoh yang terpengaruh - seperti dengan menghapus malware, menghapus akun pengguna yang disusupi, dan mengurangi kerentanan yang ditemukan - untuk menerapkan remediasi seragam di seluruh lingkungan.

Ini adalah praktik terbaik untuk menggunakan pendekatan bertahap untuk pemberantasan dan pemulihan, dan untuk memprioritaskan langkah-langkah remediasi. Tujuan dari fase awal adalah untuk meningkatkan keamanan secara keseluruhan dengan cepat (hari ke minggu) dengan perubahan bernilai tinggi untuk mencegah kejadian di masa depan. Fase selanjutnya dapat berfokus pada perubahan jangka panjang (misalnya, perubahan infrastruktur), dan pekerjaan berkelanjutan untuk menjaga perusahaan seaman mungkin. Setiap kasus unik dan AWS CIRT akan bekerja dengan Anda untuk menilai tindakan yang diperlukan.

Pertimbangkan hal berikut:

- Bisakah Anda mencitrakan ulang sistem dan mengeraskannya dengan tambalan atau tindakan pencegahan lainnya untuk mencegah atau mengurangi risiko serangan?
- Bisakah Anda mengganti sistem yang terinfeksi dengan instance atau sumber daya baru, mengaktifkan garis dasar yang bersih saat menghentikan item yang terinfeksi?
- Sudahkah Anda menghapus semua malware dan artefak lain yang ditinggalkan oleh penggunaan yang tidak sah, dan mengeraskan sistem yang terpengaruh terhadap serangan lebih lanjut?
- Apakah ada persyaratan untuk forensik pada sumber daya yang terkena dampak?

Memulihkan

Respons Insiden Keamanan AWS memberi Anda panduan untuk membantu memulihkan sistem ke operasi normal, mengonfirmasi bahwa sistem berfungsi dengan baik, dan memulihkan kerentanan apa pun untuk mencegah kejadian serupa di masa mendatang. Respons Insiden Keamanan AWS tidak secara langsung membantu pemulihan sistem. Pertimbangan kunci meliputi:

- Apakah sistem yang terpengaruh ditambal dan dikeraskan terhadap serangan baru-baru ini?
- Apa garis waktu yang layak untuk mengembalikan sistem ke produksi?
- Alat apa yang akan Anda gunakan untuk menguji, memantau, dan memverifikasi sistem yang dipulihkan?

Laporan Insiden

Respons Insiden Keamanan AWS memberikan ringkasan acara setelah berakhirnya kegiatan keamanan antara tim Anda dan kami.

Pada akhir setiap bulan, Respons Insiden Keamanan AWS layanan akan mengirimkan laporan bulanan ke titik kontak utama untuk setiap pelanggan melalui email. Laporan akan dikirimkan dalam format PDF menggunakan metrik yang dijelaskan di bawah ini. Pelanggan akan menerima satu laporan per AWS Organizations.

Metrik Kasus

- Kasus dibuat
  - Nama dimensi: Jenis
  - Nilai dimensi: AWS didukung, didukung sendiri
  - Unit: Jumlah
  - Keterangan: Jumlah kasus yang dibuat.
- Kasus ditutup
  - Nama dimensi: Jenis
  - Nilai dimensi: AWS didukung, dikelola sendiri
  - Unit: Jumlah
  - Deskripsi: Ukuran jumlah total kasus ditutup.
- Kasus terbuka
  - Nama dimensi: Jenis
  - Nilai dimensi: AWS didukung, didukung sendiri
  - Unit: Jumlah
  - Deskripsi: Jumlah kasus terbuka.

Metrik triaging

- Temuan diterima
  - Unit: Jumlah
  - Keterangan: Jumlah temuan yang dikirim ke triaging.
- Temuan diarsipkan

  - Unit: Jumlah
  - Keterangan: Jumlah temuan yang diarsipkan setelah diproses tanpa investigasi manual.
- Temuan Diselidiki Secara Manual
  - Unit: Jumlah
  - Keterangan: Jumlah temuan dengan investigasi manual dilakukan.
- Investigasi diarsipkan
  - Unit: Jumlah
  - Keterangan: Jumlah investigasi manual yang menghasilkan false positive dan dikirim untuk pengarsipan
- Investigasi meningkat
  - Unit: Jumlah
  - Deskripsi: Jumlah investigasi manual yang mengakibatkan insiden keamanan

Kasus

Respons Insiden Keamanan AWS memungkinkan Anda membuat dua jenis kasus - kasus yang AWS didukung atau dikelola sendiri.

Buat kasus yang AWS didukung

Anda dapat membuat kasus yang AWS didukung Respons Insiden Keamanan AWS melalui Konsol, API, atau AWS Command Line Interface. AWS kasus yang didukung memungkinkan Anda menerima dukungan dari Tim Respons Insiden AWS Pelanggan (CIRT).

> **Note**
>
> AWS CIRT akan menanggapi kasus Anda dalam waktu 15 menit. Waktu respons adalah untuk respons pertama dari AWS CIRT. Kami akan melakukan segala upaya yang wajar untuk menanggapi permintaan awal Anda dalam jangka waktu ini. Waktu respons ini tidak berlaku untuk tanggapan berikutnya.

Contoh berikut mencakup penggunaan konsol.

1. Masuk ke AWS Management Console. Buka konsol Security Incident Response di https://console.aws.amazon.com/security-ir/.

2. Pilih Buat Kasus
3. Pilih Selesaikan kasus dengan AWS
4. Pilih jenis permintaan
    a. Insiden Keamanan Aktif: Jenis ini untuk dukungan dan layanan respons insiden mendesak.
    b. Investigasi: Investigasi memungkinkan Anda untuk mendapatkan dukungan untuk insiden keamanan yang dirasakan di mana AWS CIRT dapat mendukung dalam penyelaman log dan konfirmasi sekunder dari investigasi respons insiden.
5. Tetapkan perkiraan tanggal mulai ke tanggal indikator awal insiden Anda. Misalnya, ketika Anda mengalami perilaku abnormal untuk pertama kalinya atau ketika Anda menerima peringatan keamanan terkait pertama.
6. Tentukan judul untuk kasus ini
7. Berikan deskripsi mendetail tentang kasus ini. Pertimbangkan aspek-aspek berikut yang dapat membantu responden insiden dengan penyelesaian kasus:
    a. Apa yang terjadi?
    b. Siapa yang menemukan dan melaporkan kejadian itu?
    c. Siapa yang terpengaruh oleh kasus ini?
    d. Apa dampaknya?
    e. Apa urgensi untuk kasus ini?
    f. Tambahkan satu atau beberapa Akun AWS IDs yang berada dalam lingkup kasus.
8. Tambahkan detail kasus opsional:
    a. Pilih layanan utama yang terpengaruh dari daftar tarik-turun.
    b. Pilih wilayah utama yang terpengaruh dari daftar tarik-turun.
    c. Tambahkan satu atau banyak alamat IP aktor ancaman yang Anda identifikasi sebagai bagian dari kasus ini.
9. Tambahkan responden insiden tambahan opsional ke kasus yang akan menerima pemberitahuan. Untuk menambahkan individu, lakukan hal berikut:
    a. Tambahkan alamat email.
    b. Tambahkan nama depan dan belakang opsional.
    c. Pilih Tambahkan baru untuk menambahkan individu lain.
    d. Untuk menghapus individu, pilih opsi Hapus untuk individu.
    e. Pilih Tambahkan untuk menambahkan semua individu yang terdaftar ke kasing.
        i. Anda dapat memilih beberapa individu dan memilih Hapus untuk menghapusnya dari daftar.

10. Tambahkan tag opsional ke kasing.
    a. Untuk menambahkan tanda, lakukan hal berikut:
    b. Pilih Tambahkan tag baru.
    c. Untuk Kunci, masukkan nama dari tanda.
    d. Untuk Nilai, masukkan nilai dari tanda.
    e. Untuk menghapus sebuah tag, pilih Hapus untuk tanda tersebut.

Setelah kasus yang AWS didukung dibuat, AWS CIRT dan tim respons insiden Anda segera diberi tahu.

Membuat kasus yang dikelola sendiri

Anda dapat membuat untuk yang dikelola sendiri Respons Insiden Keamanan AWS melalui Konsol, API, atau AWS Command Line Interface. Jenis kasus ini TIDAK melibatkan AWS CIRT. Contoh berikut mencakup penggunaan konsol.

1. Masuk ke AWS Management Console. Buka konsol Security Incident Response di https://console.aws.amazon.com/security-ir/.
2. Pilih Buat Kasus.
3. Pilih Selesaikan kasus dengan tim respons insiden saya sendiri.
4. Tetapkan perkiraan tanggal mulai ke tanggal indikator awal insiden Anda. Misalnya, ketika Anda mengalami perilaku abnormal untuk pertama kalinya atau ketika Anda menerima peringatan keamanan terkait pertama.
5. Tentukan judul untuk kasus ini. Disarankan untuk memasukkan data ke dalam judul kasus seperti yang disarankan saat memilih opsi Hasilkan Judul.
6. Masukkan Akun AWS IDs yang merupakan bagian dari kasus ini. Untuk menambahkan ID akun, lakukan hal berikut:
    a. Masukkan ID akun 12 digit dan pilih Tambahkan akun.
    b. Untuk menghapus akun, pilih Hapus di samping akun yang ingin Anda hapus dari kasing.
7. Berikan deskripsi mendetail tentang kasus ini.
    a. Pertimbangkan aspek-aspek berikut yang dapat membantu responden insiden dengan penyelesaian kasus:
        i. Apa yang terjadi?
        ii. Siapa yang menemukan dan melaporkan kejadian itu?

iii. Siapa yang terpengaruh oleh kasus ini?

iv. Apa dampaknya?

v. Apa urgensi untuk kasus ini?

8. Tambahkan detail kasus opsional:
   a. Pilih layanan utama yang terpengaruh dari daftar tarik-turun.
   b. Pilih wilayah utama yang terpengaruh dari daftar tarik-turun.
   c. Tambahkan satu atau banyak alamat IP aktor ancaman yang Anda identifikasi sebagai bagian dari kasus ini.
9. Tambahkan responden insiden tambahan opsional ke kasus yang akan menerima pemberitahuan. Untuk menambahkan individu, lakukan hal berikut:
   a. Tambahkan alamat email.
   b. Tambahkan nama depan dan belakang opsional.
   c. Pilih Tambahkan baru untuk menambahkan individu lain.
   d. Untuk menghapus individu, pilih opsi Hapus untuk individu.
   e. Pilih Tambahkan untuk menambahkan semua individu yang terdaftar ke kasing. Anda dapat memilih beberapa individu dan memilih Hapus untuk menghapusnya dari daftar.
10. Tambahkan tag opsional ke kasing. Untuk menambahkan tanda, lakukan hal berikut:
    a. Pilih Tambahkan tag baru.
    b. Untuk Kunci, masukkan nama dari tanda.
    c. Untuk Nilai, masukkan nilai dari tanda.
    d. Untuk menghapus sebuah tag, pilih Hapus untuk tanda tersebut.

Tim respons insiden akan diberitahukan melalui email setelah kasus dibuat.

Menanggapi kasus yang AWS dihasilkan

Respons Insiden Keamanan AWS dapat membuat pemberitahuan atau kasus keluar ketika Anda perlu bertindak atau mengetahui sesuatu yang mungkin memengaruhi akun atau sumber daya Anda. Ini hanya akan terjadi jika Anda telah mengaktifkan respons proaktif dan alur kerja triaging peringatan sebagai bagian dari langganan Anda.

Pemberitahuan ini akan muncul sebagai kasus Respons Insiden Keamanan dengan awalan “[Kasus proaktif]” di Respons Insiden Keamanan AWS konsol. Untuk melihat dan mengelola kasus ini:

- Buka konsol Security Incident Response di https://console.aws.amazon.com/security-ir/
- Klik “Kasus” di menu.
- Anda harus dapat melihat semua kasus, termasuk yang memiliki awalan “[Kasus proaktif]”.

Kasus ini memungkinkan Anda memperbarui, menyelesaikan, dan membukanya kembali sesuai kebutuhan. Anda dapat berkomunikasi langsung dengan Respons Insiden Keamanan AWS tim melalui kasus-kasus ini, memastikan penanganan yang efisien dari potensi masalah keamanan.

Mengelola Kasus

Daftar Isi

Mengubah status kasus

Kasus akan berada di salah satu status berikut:

- Dikirim: Ini adalah status awal suatu kasus. Kasus dalam status ini telah diajukan oleh yang diminta, tetapi belum dikerjakan.
- Deteksi dan Analisis: Status ini menunjukkan responden insiden telah mulai mengerjakan kasus ini. Fase ini mencakup pengumpulan data, triaging acara, dan melakukan analisis untuk membuat kesimpulan berbasis data.
- Penahanan, Pemberantasan dan Pemulihan: Dalam status ini responden insiden telah mengidentifikasi aktivitas mencurigakan yang membutuhkan upaya tambahan untuk

menghapusnya. Responden insiden akan memberikan rekomendasi kepada Anda untuk analisis risiko bisnis dan tindakan tambahan. Jika Anda telah mengaktifkan fitur opt-in untuk layanan, maka AWS responden insiden akan meminta persetujuan Anda untuk melakukan tindakan penahanan dengan dokumen SSM di akun yang terkena dampak.

- Kegiatan pasca-insiden: Dalam status ini peristiwa keamanan utama telah dibendung. Fokusnya sekarang adalah memulihkan dan mengembalikan operasi bisnis ke normal. Ringkasan dan analisis akar penyebab disediakan jika resolver untuk kasus ini didukung AWS.
- Ditutup: Ini adalah status akhir dari alur kerja. Kasus dalam status tertutup menunjukkan pekerjaan telah selesai. Kasus tertutup tidak dapat dibuka kembali, jadi pastikan semua tindakan selesai sebelum beralih ke status ini.

Pilih Status Tindakan/Pembaruan untuk mengubah status kasus untuk kasus yang dikelola sendiri. Untuk kasus yang AWS didukung, status ditetapkan oleh responden AWS CIRT.

Mengubah resolver

Untuk kasus yang dikelola sendiri, tim respons insiden Anda dapat meminta bantuan AWS. Pilih Dapatkan bantuan dari AWS untuk mengubah resolver untuk kasus ini menjadi. AWS Setelah kasus diperbarui ke AWS didukung, status diubah menjadi Kirim. Riwayat kasus yang ada akan tersedia untuk AWS CIRT. Setelah Anda meminta bantuan dari AWS Anda tidak akan dapat mengubahnya kembali ke yang dikelola sendiri.

Item Tindakan

Responden AWS CIRT yang menangani kasus ini dapat meminta tindakan dari tim internal Anda.

Item tindakan yang muncul setelah kasus dibuat meliputi:

- Permintaan untuk memberikan izin bagi responden insiden untuk mengakses kasus
- Permintaan untuk memberikan informasi lebih lanjut tentang kasus ini

Item tindakan saat tindakan pelanggan tertunda:

- Permintaan untuk bertindak atas komentar baru untuk melanjutkan kasus

Item tindakan saat kasing siap ditutup:

- Permintaan untuk meninjau laporan kasus

- Permintaan untuk menutup kasus

Menyunting kasus

Pilih Edit untuk mengubah detail kasus.

Untuk kasus AWS yang didukung dan dikelola sendiri:

Anda dapat mengubah detail kasus berikut setelah kasus dibuat:

- Judul
- Deskripsi

Hanya untuk kasus yang AWS didukung:

Anda dapat mengubah bidang tambahan:

- Jenis permintaan:
  - Insiden Keamanan Aktif: Jenis ini untuk dukungan dan layanan respons insiden mendesak.
  - Investigasi: Investigasi memungkinkan Anda untuk mendapatkan dukungan untuk insiden keamanan yang dirasakan di mana AWS CIRT dapat mendukung dalam penyelaman log dan konfirmasi sekunder dari peristiwa keamanan.
- Estimasi tanggal mulai: Ubah bidang ini jika Anda menerima indikator untuk kasus ini yang mendahului tanggal mulai awal yang disediakan. Pertimbangkan untuk memberikan rincian tambahan sehubungan dengan indikator yang baru terdeteksi di bidang deskripsi atau menambahkan komentar di tab komunikasi.

Komunikasi

AWS CIRT dapat menambahkan komentar untuk mendokumentasikan aktivitas mereka saat mengerjakan sebuah kasus. Responden AWS CIRT yang berbeda dapat mengerjakan kasus pada saat yang bersamaan. Mereka direpresentasikan sebagai AWS Responder dalam log komunikasi.

Izin

Tab izin mencantumkan semua individu yang akan diberi tahu untuk setiap perubahan pada kasus ini. Anda dapat menambah dan menghapus individu dari daftar sampai kasing ditutup.

> **Note**
>
> Kasus individual memungkinkan Anda untuk memasukkan hingga 30 pemangku kepentingan total. Konfigurasi izin tambahan diperlukan untuk memberikan akses tingkat kasus ke pemangku kepentingan ini.

Berikan akses ke kasing di konsol

Untuk memberikan akses ke kasus di AWS Management Console, Anda dapat menyalin templat kebijakan izin IAM dan menambahkan izin ini ke pengguna atau peran.

Menambahkan kebijakan IAM ke pengguna atau peran:

1. Salin kebijakan izin IAM.
2. Buka IAM di via https://console.aws.amazon.com/iam/.
3. Di panel navigasi, pilih Pengguna atau Peran.
4. Pilih pengguna atau peran untuk membuka halaman detail.
5. Di tab izin, pilih Tambahkan izin.
6. Pilih Lampirkan kebijakan.
7. Pilih kebijakan Respons Insiden Keamanan AWS terkelola yang sesuai.
8. Pilih Tambahkan kebijakan.

Lampiran

Responden insiden Anda dapat menambahkan lampiran pada kasus yang membantu responden insiden lainnya dengan penyelidikan mereka untuk kasus yang dikelola sendiri.

> **Note**
>
> Jika Anda memilih kasus yang AWS didukung, AWS tidak dapat melihat lampiran. Semua detail untuk kasus yang AWS didukung harus dibagikan melalui komentar kasus atau melalui Anda menyediakan screenshare menggunakan teknologi komunikasi pilihan Anda.

Pilih Unggah untuk memilih file dari komputer Anda untuk ditambahkan ke kasing.

> **Note**
>
> Lampiran apa pun yang diunggah akan dihapus tujuh hari setelah kasus terjadi. `Closed`

Tanda

Tanda adalah label opsional yang dapat Anda tugaskan ke kasus Anda untuk menyimpan metadata tentang sumber daya tersebut. Setiap tag adalah label yang terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tag untuk mencari, mengalokasikan biaya, dan mengautentikasi izin untuk sumber daya.

Untuk menambahkan tanda, lakukan hal berikut:

1. Pilih Tambahkan tag baru.
2. Untuk Kunci, masukkan nama dari tanda.
3. Untuk Nilai, masukkan nilai dari tanda.

Untuk menghapus sebuah tag, pilih Hapus untuk tanda tersebut.

Kegiatan Kasus

Jejak audit memberikan catatan kronologis terperinci dari semua kegiatan kasus. Mereka memberikan informasi penting dalam kegiatan pasca-acara dan membantu mengidentifikasi potensi perbaikan. Waktu, pengguna, tindakan, dan detail dari setiap perubahan kasus dicatat dalam jejak audit kasus.

Menutup Kasus

Untuk kasus yang AWS didukung, pilih Tutup Kasus pada halaman detail kasus untuk menutup kasus secara permanen pada status apa pun. Kasus biasanya mencapai status Siap Tutup sebelum ditutup secara permanen. Jika Anda menutup kasus sebelum waktunya di status lain selain Siap Tutup, Anda meminta AWS CIRT berhenti mengerjakan kasus yang didukung ini. AWS

Jika tim respons insiden Anda adalah responden, pilih Tindakan/Tutup Kasus pada halaman detail kasus.

> **Note**
>
> Status “Siap Tutup” menandakan bahwa suatu kasus dapat ditutup secara permanen dan tidak ada pekerjaan tambahan yang harus dilakukan pada suatu kasus.

Kasus tidak dapat dibuka kembali setelah ditutup secara permanen. Semua informasi akan tersedia hanya-baca. Untuk mencegah penutupan yang tidak disengaja, Anda akan diminta mengonfirmasi bahwa Anda ingin menutup kasus ini.

Bekerja dengan AWS CloudFormation stacksets

> **Important**
>
> Respons Insiden Keamanan AWS tidak mengaktifkan kemampuan penahanan secara default, untuk menjalankan tindakan penahanan ini, Anda harus terlebih dahulu memberikan izin yang diperlukan untuk layanan menggunakan peran. Anda dapat membuat peran ini secara individual per akun atau di seluruh organisasi dengan menerapkan AWS CloudFormation StackSets, yang membuat peran yang diperlukan.

Anda dapat menemukan petunjuk spesifik tentang cara Membuat set tumpukan dengan izin yang dikelola layanan.

Berikut ini adalah template stacksets untuk membuat AWSSecurityIncidentResponseContainmentdan AWSSecurityIncidentResponseContainmentExecutionperan.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for Respons Insiden Keamanan AWS containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
```

```
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
                    'Resource':
                      [
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainEC2Instance:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainS3Resource:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainIAMPrincipal:$DEFAULT',
                      ],
                  },
                  {
                    'Effect': 'Allow',
                    'Action':
                      ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
                    'Resource': '*',
                  },
                  {
                    'Effect': 'Allow',
```

```
                    'Action': ['iam:PassRole'],
                    'Resource': !GetAtt
AWSSecurityIncidentResponseContainmentExecution.Arn,
                    'Condition': { 'StringEquals': { 'iam:PassedToService':
'ssm.amazonaws.com' } },
                  },
                ],
            }
 AWSSecurityIncidentResponseContainmentExecution:
   Type: 'AWS::IAM::Role'
   Properties:
     RoleName: AWSSecurityIncidentResponseContainmentExecution
     AssumeRolePolicyDocument:
       {
         'Version': '2012-10-17',
         'Statement':
           [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
'Action': 'sts:AssumeRole' }],
       }
     ManagedPolicyArns:
       - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
     Policies:
       - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
         PolicyDocument:
           {
             'Version': '2012-10-17',
             'Statement':
               [
                 {
                   'Sid': 'AllowIAMContainment',
                   'Effect': 'Allow',
                   'Action':
                     [
                       'iam:AttachRolePolicy',
                       'iam:AttachUserPolicy',
                       'iam:DeactivateMFADevice',
                       'iam:DeleteLoginProfile',
                       'iam:DeleteRolePolicy',
                       'iam:DeleteUserPolicy',
                       'iam:GetLoginProfile',
                       'iam:GetPolicy',
                       'iam:GetRole',
                       'iam:GetRolePolicy',
                       'iam:GetUser',
```

```
                'iam:GetUserPolicy',
                'iam:ListAccessKeys',
                'iam:ListAttachedRolePolicies',
                'iam:ListAttachedUserPolicies',
                'iam:ListMfaDevices',
                'iam:ListPolicies',
                'iam:ListRolePolicies',
                'iam:ListUserPolicies',
                'iam:ListVirtualMFADevices',
                'iam:PutRolePolicy',
                'iam:PutUserPolicy',
                'iam:TagMFADevice',
                'iam:TagPolicy',
                'iam:TagRole',
                'iam:TagUser',
                'iam:UntagMFADevice',
                'iam:UntagPolicy',
                'iam:UntagRole',
                'iam:UntagUser',
                'iam:UpdateAccessKey',
                'identitystore:CreateGroupMembership',
                'identitystore:DeleteGroupMembership',
                'identitystore:IsMemberInGroups',
                'identitystore:ListUsers',
                'identitystore:ListGroups',
                'identitystore:ListGroupMemberships',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowOrgListAccounts',
            'Effect': 'Allow',
            'Action': 'organizations:ListAccounts',
            'Resource': '*',
          },
          {
            'Sid': 'AllowSSOContainment',
            'Effect': 'Allow',
            'Action':
              [
                'sso:CreateAccountAssignment',
                'sso:DeleteAccountAssignment',
                'sso:DeleteInlinePolicyFromPermissionSet',
                'sso:GetInlinePolicyForPermissionSet',
```

```
                        'sso:ListAccountAssignments',
                        'sso:ListInstances',
                        'sso:ListPermissionSets',
                        'sso:ListPermissionSetsProvisionedToAccount',
                        'sso:PutInlinePolicyToPermissionSet',
                        'sso:TagResource',
                        'sso:UntagResource',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSORead',
                    'Effect': 'Allow',
                    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Read',
                    'Effect': 'Allow',
                    'Action':
                      [
                        's3:GetAccountPublicAccessBlock',
                        's3:GetBucketAcl',
                        's3:GetBucketLocation',
                        's3:GetBucketOwnershipControls',
                        's3:GetBucketPolicy',
                        's3:GetBucketPolicyStatus',
                        's3:GetBucketPublicAccessBlock',
                        's3:GetBucketTagging',
                        's3:GetEncryptionConfiguration',
                        's3:GetObject',
                        's3:GetObjectAcl',
                        's3:GetObjectTagging',
                        's3:GetReplicationConfiguration',
                        's3:ListBucket',
                        's3express:GetBucketPolicy',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Write',
                    'Effect': 'Allow',
                    'Action':
```

```
                    [
                      's3:CreateBucket',
                      's3:DeleteBucketPolicy',
                      's3:DeleteObjectTagging',
                      's3:PutAccountPublicAccessBlock',
                      's3:PutBucketACL',
                      's3:PutBucketOwnershipControls',
                      's3:PutBucketPolicy',
                      's3:PutBucketPublicAccessBlock',
                      's3:PutBucketTagging',
                      's3:PutBucketVersioning',
                      's3:PutObject',
                      's3:PutObjectAcl',
                      's3express:CreateSession',
                      's3express:DeleteBucketPolicy',
                      's3express:PutBucketPolicy',
                    ],
                  'Resource': '*',
                },
                {
                  'Sid': 'AllowAutoScalingWrite',
                  'Effect': 'Allow',
                  'Action':
                    [
                      'autoscaling:CreateOrUpdateTags',
                      'autoscaling:DeleteTags',
                      'autoscaling:DescribeAutoScalingGroups',
                      'autoscaling:DescribeAutoScalingInstances',
                      'autoscaling:DescribeTags',
                      'autoscaling:EnterStandby',
                      'autoscaling:ExitStandby',
                      'autoscaling:UpdateAutoScalingGroup',
                    ],
                  'Resource': '*',
                },
                {
                  'Sid': 'AllowEC2Containment',
                  'Effect': 'Allow',
                  'Action':
                    [
                      'ec2:AuthorizeSecurityGroupEgress',
                      'ec2:AuthorizeSecurityGroupIngress',
                      'ec2:CopyImage',
                      'ec2:CreateImage',
```

```
                    'ec2:CreateSecurityGroup',
                    'ec2:CreateSnapshot',
                    'ec2:CreateTags',
                    'ec2:DeleteSecurityGroup',
                    'ec2:DeleteTags',
                    'ec2:DescribeImages',
                    'ec2:DescribeInstances',
                    'ec2:DescribeSecurityGroups',
                    'ec2:DescribeSnapshots',
                    'ec2:DescribeTags',
                    'ec2:ModifyNetworkInterfaceAttribute',
                    'ec2:RevokeSecurityGroupEgress',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowKMSActions',
                'Effect': 'Allow',
                'Action':
                  [
                    'kms:CreateGrant',
                    'kms:DescribeKey',
                    'kms:GenerateDataKeyWithoutPlaintext',
                    'kms:ReEncryptFrom',
                    'kms:ReEncryptTo',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowSSMActions',
                'Effect': 'Allow',
                'Action': ['ssm:DescribeAutomationExecutions'],
                'Resource': '*',
              },
            ],
        }
```

Batalkan Keanggotaan

Peran yang memiliki CancelMembership izin Respons Insiden Keamanan AWS dapat membatalkan keanggotaan dari konsol, API, atau AWS Command Line Interface.

Important

Setelah keanggotaan dibatalkan, Anda tidak akan dapat melihat data kasus historis. Jika Anda membatalkan selama sebulan, keanggotaan Anda akan tersedia hingga akhir bulan. Setiap sumber daya atau investigasi yang `ready to close` akan `Active` atau akan dihentikan setelah pembatalan keanggotaan akhir pada akhir siklus penagihan.

Important

Respons Insiden Keamanan AWS tidak mengikuti siklus penagihan ulang tahun standar yang terjadi setiap bulan. Penagihan layanan berjalan dari bulan ke bulan. Beberapa contoh:

- 29 Des, 29 Jan
- 29 Jan, 26 Feb (Tahun bukan kabisat)
- 26 Feb, 29 Maret

Important

Jika Anda berlangganan kembali ke layanan, keanggotaan baru akan dibuat dan sumber daya kasus yang berada di bawah keanggotaan sebelumnya hanya dapat diakses jika Anda mengunduhnya sebelum pembatalan.

Setelah keanggotaan dibatalkan, semua orang di tim respons insiden keanggotaan akan diberitahu melalui email.

Important

Jika Anda membuat keanggotaan menggunakan akun administrator yang didelegasikan dan Anda menggunakan AWS Organizations API untuk menghapus penunjukan administrator yang didelegasikan dari akun, keanggotaan akan segera dihentikan.

Sumber daya penandaan Respons Insiden Keamanan AWS

Tag adalah label metadata yang Anda tetapkan atau yang ditetapkan ke sumber AWS daya. AWS Setiap tanda terdiri dari kunci dan nilai. Untuk tanda yang Anda tetapkan, Anda menentukan kunci dan nilai. Misalnya, Anda dapat menentukan kunci sebagai `stage` dan nilai untuk satu sumber daya sebagai `test`.

Tanda membantu Anda melakukan hal berikut:

- Identifikasi dan atur AWS sumber daya Anda. Banyak penandaan Layanan AWS dukungan, sehingga Anda dapat menetapkan tag yang sama ke sumber daya dari layanan yang berbeda untuk menunjukkan bahwa sumber daya terkait.
- Lacak AWS biaya Anda. Anda mengaktifkan tag ini di AWS Billing dasbor. AWS menggunakan tag untuk mengkategorikan biaya Anda dan mengirimkan laporan alokasi biaya bulanan kepada Anda. Untuk informasi selengkapnya, lihat Menggunakan tag alokasi biaya di Panduan Pengguna AWS Penagihan.
- Kontrol akses ke AWS sumber daya Anda. Untuk informasi selengkapnya, lihat Mengontrol akses menggunakan tag di Panduan Pengguna IAM.

Lihat referensi Respons Insiden Keamanan AWS API untuk penandaan.

Menggunakan AWS CloudShell untuk bekerja dengan AWS Security Incident Response

AWS CloudShell adalah shell pra-otentikasi berbasis browser yang dapat Anda luncurkan langsung dari file. AWS Management Console Anda dapat menjalankan AWS CLI perintah terhadap AWS layanan (termasuk AWS Security Incident Response) menggunakan shell pilihan Anda (Bash, PowerShell atau Z shell). Anda juga dapat melakukan ini tanpa perlu mengunduh atau menginstal alat baris perintah.

Anda meluncurkan AWS CloudShell dari AWS Management Console, dan AWS kredenal yang Anda gunakan untuk masuk ke konsol secara otomatis tersedia di sesi shell baru. Pra-otentikasi AWS CloudShell pengguna ini memungkinkan Anda untuk melewati konfigurasi kredensional saat berinteraksi dengan AWS layanan seperti Security Incident Response menggunakan AWS CLI versi 2 (pra-instal pada lingkungan komputasi shell).

Daftar Isi

Memperoleh izin IAM untuk AWS CloudShell

Dengan menggunakan sumber daya manajemen akses yang disediakan oleh AWS Identity and Access Management, administrator dapat memberikan izin kepada pengguna IAM sehingga mereka dapat mengakses AWS CloudShell dan menggunakan fitur lingkungan.

Cara tercepat bagi administrator untuk memberikan akses ke pengguna adalah melalui kebijakan AWS terkelola. Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. Kebijakan AWS terkelola berikut ini CloudShell dapat dilampirkan ke identitas IAM:

- `AWSCloudShellFullAccess`: Memberikan izin untuk menggunakan AWS CloudShell dengan akses penuh ke semua fitur.

Jika ingin membatasi cakupan tindakan yang dapat dilakukan oleh pengguna IAM AWS CloudShell, Anda dapat membuat kebijakan kustom yang menggunakan kebijakan `AWSCloudShellFullAccess` terkelola sebagai templat. Untuk informasi selengkapnya tentang

membatasi tindakan yang tersedia bagi pengguna CloudShell, lihat Mengelola AWS CloudShell akses dan penggunaan dengan kebijakan IAM di Panduan AWS CloudShell Pengguna.

> **Note**
>
> Identitas IAM Anda juga memerlukan kebijakan yang memberikan izin untuk melakukan panggilan ke Security Incident Response.

Berinteraksi dengan Respons Insiden Keamanan menggunakan AWS CloudShell

Setelah Anda meluncurkan AWS CloudShell dari AWS Management Console, Anda dapat segera mulai berinteraksi dengan Security Incident Response menggunakan antarmuka baris perintah.

> **Note**
>
> Saat menggunakan AWS CLI in AWS CloudShell, Anda tidak perlu mengunduh atau menginstal sumber daya tambahan apa pun. Selain itu, karena Anda sudah diautentikasi di dalam shell, Anda tidak perlu mengonfigurasi kredensional sebelum melakukan panggilan.

Bekerja dengan AWS CloudShell dan Respon Insiden Keamanan

- Dari AWS Management Console, Anda dapat meluncurkan CloudShell dengan memilih opsi berikut yang tersedia di bilah navigasi:
  - Pilih CloudShell ikon.
  - Mulai mengetik “cloudshell” di kotak Pencarian dan kemudian pilih opsi. CloudShell

Pencatatan panggilan API Respons Insiden AWS Keamanan menggunakan AWS CloudTrail

AWS Security Incident Response terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan dalam Security Incident Response. CloudTrail menangkap semua panggilan API untuk Security Incident Response sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Security Incident Response dan panggilan kode ke operasi Security Incident Response API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Respons Insiden Keamanan. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Respons Insiden Keamanan, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi Respons Insiden Keamanan di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Security Incident Response, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrailDanau.

CloudTrail jalan setapak

> Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan AWS Management Console Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak. Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat Membuat jejak untuk Anda Akun AWS dan Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Semua tindakan Respons Insiden Keamanan dicatat oleh CloudTrail dan didokumentasikan dalam Referensi API Respons Insiden AWS Keamanan. Misalnya, panggilan ke`CreateMembership`, `CreateCase` dan `UpdateCase` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log Respons Insiden Keamanan

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateCase tindakan.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA0000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA0000000000000000",
                "arn": "arn:aws:iam::123412341234:role/Admin",
                "accountId": "123412341234",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-10-13T06:32:53Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-10-13T06:40:45Z",
    "eventSource": "security-ir.amazonaws.com",
    "eventName": "CreateCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/
arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#security-ir.create-case",
    "requestParameters": {
        "impactedServices": [
```

```
            "Amazon GuardDuty"
        ],
        "impactedAccounts": [],
        "clientToken": "testToken112345679",
        "resolverType": "Self",
        "description": "***",
        "engagementType": "Investigation",
        "watchers": [
            {
                "email": "***",
                "name": "***",
                "jobTitle": "***"
            }
        ],
        "membershipId": "m-r1abcdabcd",
        "title": "***",
        "impactedAwsRegions": [
            {
                "region": "ap-southeast-1"
            }
        ],
        "reportedIncidentStartDate": 1711553521,
        "threatActorIpAddresses": [
            {
                "ipAddress": "***",
                "userAgent": "browser"
            }
        ]
    },
    "responseElements": {
        "caseId": "0000000001"
    },
    "requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
    "eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123412341234",
            "type": "AWS::SecurityResponder::Case",
            "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "123412341234",
    "eventCategory": "Management"
}
```

Mengelola Respons Insiden Keamanan AWS akun dengan AWS Organizations

Respons Insiden Keamanan AWS terintegrasi dengan AWS Organizations. Akun AWS Organizations manajemen untuk organisasi dapat menunjuk akun sebagai administrator yang didelegasikan untuk. Respons Insiden Keamanan AWS Tindakan ini memungkinkan Respons Insiden Keamanan AWS sebagai layanan tepercaya di AWS Organizations. Untuk informasi tentang cara izin ini diberikan, lihat Menggunakan AWS Organizations dengan AWS layanan lain.

Bagian berikut akan memandu Anda melalui berbagai tugas yang dapat Anda lakukan sebagai akun administrator Respons Insiden Keamanan yang didelegasikan.

Daftar Isi

Pertimbangan dan rekomendasi untuk digunakan dengan Respons Insiden Keamanan AWSAWS Organizations

Pertimbangan dan rekomendasi berikut dapat membantu Anda memahami cara akun administrator Respons Insiden Keamanan yang didelegasikan beroperasi di: Respons Insiden Keamanan AWS

Akun administrator Respons Insiden Keamanan yang didelegasikan bersifat regional.

> Akun administrator Security Incident Response dan akun anggota yang didelegasikan harus ditambahkan. AWS Organizations

Akun administrator yang didelegasikan untuk Respons Insiden Keamanan AWS.

Anda dapat menetapkan satu akun anggota sebagai akun administrator Respons Insiden Keamanan yang didelegasikan. Misalnya, jika Anda menunjuk akun *111122223333* anggota*Europe (Ireland)*, Anda tidak dapat menunjuk akun *555555555555* anggota lain. *Canada (Central)* Anda harus menggunakan akun yang sama dengan akun administrator Respons Insiden Keamanan yang didelegasikan di semua Wilayah lainnya.

Tidak disarankan untuk menetapkan manajemen organisasi Anda sebagai akun administrator Respons Insiden Keamanan yang didelegasikan.

Manajemen organisasi Anda dapat berupa akun administrator Respons Insiden Keamanan yang didelegasikan. Namun, praktik terbaik AWS keamanan mengikuti prinsip hak istimewa paling sedikit dan tidak merekomendasikan konfigurasi ini.

Menghapus akun administrator Respons Insiden Keamanan yang didelegasikan dari langganan langsung akan segera membatalkan langganan.

Jika Anda menghapus akun administrator Respons Insiden Keamanan yang didelegasikan, Respons Insiden Keamanan AWS hapus semua akun anggota yang terkait dengan akun administrator Respons Insiden Keamanan yang didelegasikan ini. Respons Insiden Keamanan AWS tidak akan lagi diaktifkan untuk semua akun anggota ini.

Mengaktifkan akses tepercaya untuk AWS Account Management

Mengaktifkan akses tepercaya untuk Respons Insiden Keamanan AWS memungkinkan administrator yang didelegasikan dari akun manajemen untuk memodifikasi informasi dan metadata (misalnya, detail kontak utama atau alternatif) khusus untuk setiap akun anggota di. AWS Organizations

Gunakan prosedur berikut untuk mengaktifkan akses tepercaya Respons Insiden Keamanan AWS di organisasi Anda.

Izin minimum

Untuk melakukan tugas-tugas ini, Anda harus memenuhi persyaratan berikut:

- Anda dapat melakukan ini hanya dari akun manajemen organisasi.
- Organisasi Anda harus mengaktifkan semua fitur.

Console

Untuk mengaktifkan akses tepercaya untuk Respons Insiden Keamanan AWS

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pilih Layanan di panel navigasi.
3. Pilih Respons Insiden Keamanan AWSdalam daftar layanan.
4. Pilih Aktifkan akses terpercaya.
5. Di kotak Respons Insiden Keamanan AWS dialog Aktifkan akses tepercaya untuk, ketik aktifkan untuk mengonfirmasinya, lalu pilih Aktifkan akses tepercaya.

API/CLI

Untuk mengaktifkan akses tepercaya untuk AWS Account Management

Setelah menjalankan perintah berikut, Anda dapat menggunakan kredensi dari akun manajemen organisasi untuk memanggil operasi API Manajemen Akun yang menggunakan `--accountId` parameter untuk mereferensikan akun anggota dalam organisasi.

- AWS CLI: enable-aws-service-access

  Contoh berikut memungkinkan akses tepercaya untuk Respons Insiden Keamanan AWS di organisasi akun panggilan.

```
$ aws organizations enable-aws-service-access \
                                        --service-principal security-
ir.amazonaws.com
```

  Perintah ini tidak menghasilkan output jika berhasil.

Izin yang diperlukan untuk menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan

Anda dapat memilih untuk mengatur Respons Insiden Keamanan AWS keanggotaan Anda menggunakan administrator yang didelegasikan untuk AWS Organizations. Untuk informasi tentang cara izin ini diberikan, lihat Menggunakan AWS Organizations dengan AWS layanan lain.

> **Note**
>
> Respons Insiden Keamanan AWS secara otomatis mengaktifkan hubungan AWS Organizations tepercaya saat menggunakan konsol untuk pengaturan dan manajemen. Jika Anda menggunakan CLI/SDK maka Anda harus mengaktifkannya secara manual dengan menggunakan API Aktifkan AWSService Akses untuk dipercaya. `security-ir.amazonaws.com`

Sebagai AWS Organizations manajer, sebelum Anda menetapkan akun administrator Respons Insiden Keamanan yang didelegasikan untuk organisasi Anda, verifikasi bahwa Anda dapat melakukan Respons Insiden Keamanan AWS tindakan berikut: `security-ir:CreateMembership` dan. `security-ir:UpdateMembership` Tindakan ini memungkinkan Anda untuk menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan untuk organisasi Anda dengan menggunakan. Respons Insiden Keamanan AWS Anda juga harus memastikan bahwa Anda diizinkan untuk melakukan AWS Organizations tindakan yang membantu Anda mengambil informasi tentang organisasi Anda.

Untuk memberikan izin ini, sertakan pernyataan berikut dalam kebijakan AWS Identity and Access Management (IAM) untuk akun Anda:

```
{
    "Sid": "PermissionsForSIRAdmin",
    "Effect": "Allow",
    "Action": [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
```

```
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Jika Anda ingin menetapkan akun AWS Organizations manajemen Anda sebagai akun administrator Respons Insiden Keamanan yang didelegasikan, akun Anda juga akan memerlukan tindakan IAM:. `CreateServiceLinkedRole` Tinjau Pertimbangan dan rekomendasi untuk digunakan dengan Respons Insiden Keamanan AWSAWS Organizations sebelum Anda melanjutkan untuk menambahkan izin.

Untuk melanjutkan penunjukan akun AWS Organizations manajemen Anda sebagai akun administrator Respons Insiden Keamanan yang didelegasikan, tambahkan pernyataan berikut ke kebijakan IAM dan ganti *111122223333* dengan Akun AWS ID akun manajemen Anda AWS Organizations :

```
{
 "Sid": "PermissionsToEnableSecurityIncidentResponse"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-
ir.amazonaws.com/AWSServiceRoleForSecurityIncidentResponse",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "security-ir.amazonaws.com"
  }
 }
}
```

Menunjuk administrator yang didelegasikan untuk Respons Insiden Keamanan AWS

Bagian ini menyediakan langkah-langkah untuk menunjuk administrator yang didelegasikan dalam organisasi. Respons Insiden Keamanan AWS

Sebagai manajer AWS organisasi, pastikan Anda membaca Pertimbangan dan rekomendasi tentang cara akun administrator Respons Insiden Keamanan yang didelegasikan beroperasi. Sebelum melanjutkan, pastikan Anda memilikinyaIzin yang diperlukan untuk menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan.

Pilih metode akses yang disukai untuk menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan untuk organisasi Anda. Hanya manajemen yang dapat melakukan langkah ini.

Console

1. Buka konsol Security Incident Response di https://console.aws.amazon.com/security-ir/

   Untuk masuk, gunakan kredensi manajemen untuk organisasi Anda AWS Organizations .
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menunjuk akun administrator Respons Insiden Keamanan yang didelegasikan untuk organisasi Anda.
3. Ikuti panduan penyiapan untuk membuat keanggotaan Anda, termasuk akun administrator yang didelegasikan.

API/CLI

- Jalankan CreateMembership menggunakan kredensil Akun AWS manajemen organisasi.
  - Atau, Anda dapat menggunakan AWS Command Line Interface untuk melakukan ini. AWS CLI Perintah berikut menunjuk akun administrator Security Incident Response yang didelegasikan. Berikut ini adalah opsi string yang tersedia untuk mengonfigurasi keanggotaan Anda:

```
{
  "customerAccountId": "stringstring",
  "membershipName": "stringstring",
  "customerType": "Standalone",
```

```
    "organizationMetadata": {
      "organizationId": "string",
      "managementAccountId": "stringstring",
      "delegatedAdministrators": [
        "stringstring"
      ]
    },
    "membershipAccountsConfigurations": {
      "autoEnableAllAccounts": true,
      "organizationalUnits": [
        "string"
      ]
    },
    "incidentResponseTeam": [
      {
        "name": "string",
        "jobTitle": "stringstring",
        "email": "stringstring"
      }
    ],
    "internalIdentifier": "string",
    "membershipId": "stringstring",
    "optInFeatures": [
      {
        "featureName": "RuleForwarding",
        "isEnabled": true
      }
    ]
  }
```

Jika tidak Respons Insiden Keamanan AWS diaktifkan untuk akun administrator Respons Insiden Keamanan yang didelegasikan, akun tersebut tidak akan dapat mengambil tindakan apa pun. Jika belum dilakukan, pastikan Respons Insiden Keamanan AWS untuk mengaktifkan akun administrator Security Incident Response yang baru ditunjuk.

Menambahkan anggota ke Respons Insiden Keamanan AWS

Ada hubungan satu lawan satu dengan AWS Organizations dan Respons Insiden Keamanan AWS keanggotaan Anda. Karena akun ditambahkan (atau dihapus) dari Organizations Anda, ini akan tercermin dalam akun yang tercakup untuk Respons Insiden Keamanan AWS keanggotaan Anda.

Untuk menambahkan akun ke keanggotaan Anda, ikuti salah satu opsi untuk Mengelola akun di organisasi dengan AWS Organizations.

Menghapus anggota dari Respons Insiden Keamanan AWS

Untuk menghapus akun dari keanggotaan Anda, ikuti prosedur untuk menghapus akun anggota dari organisasi.

Amazon EventBridge

Menggunakan Amazon EventBridge, Anda dapat bereaksi, memantau, dan mengatur peristiwa yang terkait dengan Respons Insiden Keamanan AWS kasus dan keanggotaan. Anda dapat merutekan peristiwa ini melalui Aturan (untuk skenario fan-out ke satu atau beberapa target) atau melalui Pipes (untuk point-to-point integrasi dengan kemampuan penyaringan, pengayaan, dan transformasi yang ditingkatkan).

Anda dapat membuat integrasi antara Security Incident Response dan tooling pihak ketiga atau data agregat untuk dianalisis menggunakan AI generatif dan perkakas lainnya. AWS Misalnya, ketika Security Incident Response secara proaktif membuat kasus, Anda dapat menggunakan EventBridge otomatisasi untuk memicu sistem untuk memberi tahu pemangku kepentingan. Selain itu, jika Anda mengelola beberapa AWS lingkungan, Anda dapat menggunakan EventBridge integrasi Amazon untuk memantau Respons Insiden Keamanan AWS keanggotaan guna memastikan semua lingkungan mempertahankan postur keamanan yang kuat.

Untuk informasi lebih lanjut, Anda dapat meninjau Apa itu Amazon EventBridge?

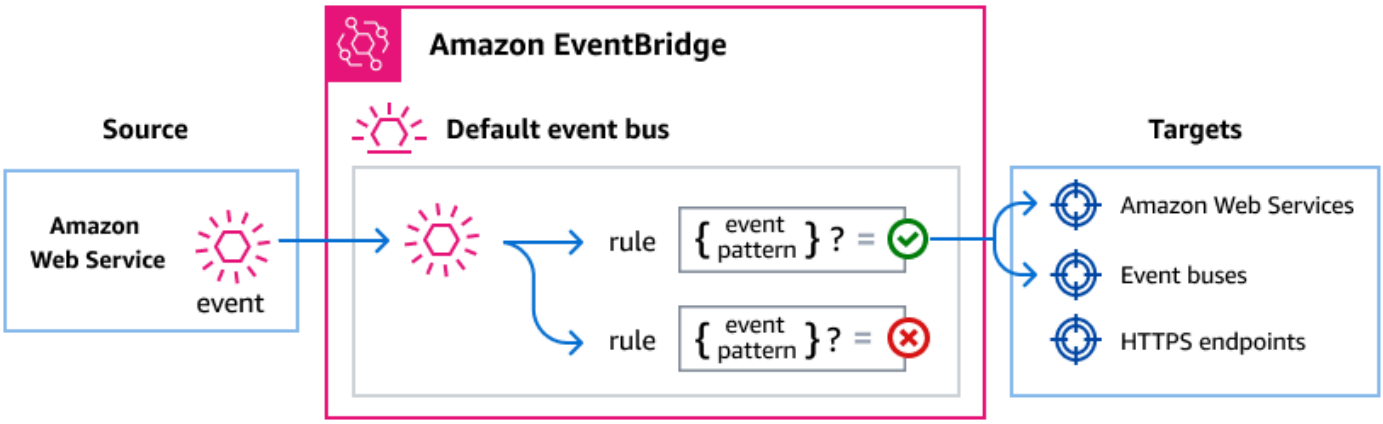
Daftar Isi

Mengelola peristiwa Respons Insiden Keamanan menggunakan Amazon EventBridge

Amazon EventBridge adalah layanan tanpa server yang menggunakan peristiwa untuk menghubungkan komponen aplikasi bersama-sama, sehingga memudahkan Anda untuk membangun aplikasi berbasis peristiwa yang dapat diskalakan. Arsitektur berbasis peristiwa adalah gaya membangun sistem perangkat lunak yang digabungkan secara longgar yang bekerja sama dengan memancarkan dan menanggapi peristiwa. Peristiwa mewakili perubahan dalam sumber daya atau lingkungan.

Begini cara kerjanya:

Seperti banyak AWS layanan, Security Incident Response menghasilkan dan mengirim acara ke bus acara EventBridge default. (Bus acara default secara otomatis disediakan di AWS akun Anda.) Bus acara adalah router yang menerima acara dan mengirimkannya ke nol atau lebih tujuan, atau target. Aturan yang Anda tentukan untuk bus acara mengevaluasi peristiwa saat mereka tiba. Setiap aturan memeriksa apakah suatu peristiwa cocok dengan pola acara aturan. Jika acara tidak cocok, bus acara mengirimkan acara ke target yang ditentukan.



Menyampaikan peristiwa Security Incident Response menggunakan EventBridge aturan

Agar bus acara EventBridge default mengirim peristiwa Respons Insiden Keamanan ke target, Anda harus membuat aturan. Setiap aturan berisi pola acara, yang EventBridge cocok dengan setiap acara yang diterima di bus acara. Jika data peristiwa cocok dengan pola peristiwa yang ditentukan, EventBridge mengirimkan peristiwa itu ke target aturan.

Untuk petunjuk komprehensif tentang cara membuat aturan bus acara, lihat Membuat aturan yang bereaksi terhadap peristiwa di Panduan EventBridge Pengguna Amazon.

Membuat pola acara yang cocok dengan peristiwa Security Incident Response

Setiap pola acara adalah objek JSON yang berisi:

- `source`Atribut yang mengidentifikasi layanan yang mengirim acara. Untuk kejadian Security Incident Response, sumbernya adalah`"aws.security-ir"`.
- (Opsional): `detail-type` Atribut yang berisi array jenis acara yang cocok.
- (Opsional): `detail` Atribut yang berisi data acara lain yang cocok.

Misalnya, pola acara berikut cocok dengan semua `Case Updated by Respons Insiden Keamanan AWS Service` peristiwa untuk yang ditentukan Akun AWS:

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Untuk informasi selengkapnya tentang penulisan pola acara, lihat Pola acara di Panduan EventBridge Pengguna.

Referensi detail peristiwa Respon Insiden Keamanan

Semua peristiwa dari AWS layanan memiliki seperangkat bidang umum yang berisi metadata tentang acara tersebut, seperti AWS layanan yang merupakan sumber acara, waktu acara dibuat, akun dan wilayah tempat acara berlangsung, dan lainnya. Untuk definisi bidang umum ini, lihat Referensi struktur acara di Panduan EventBridge Pengguna Amazon.

Selain itu, setiap acara memiliki `detail` bidang yang berisi data khusus untuk peristiwa tertentu. Referensi di bawah ini mendefinisikan bidang detail untuk berbagai peristiwa Security Incident Response.

Saat menggunakan EventBridge untuk memilih dan mengelola peristiwa Security Incident Response, penting untuk mengingat hal berikut:

- `source`Bidang untuk semua peristiwa dari Security Incident Response diatur ke`"aws.security-ir"`.
- `detail-type`Bidang menentukan jenis acara.

Misalnya, `"Case Updated"`.

- `detail`Bidang berisi data yang spesifik untuk peristiwa tertentu.

Untuk informasi tentang membuat pola peristiwa yang memungkinkan aturan agar sesuai dengan peristiwa Respons Insiden Keamanan, lihat Pola peristiwa di Panduan EventBridge Pengguna Amazon.

Untuk informasi selengkapnya tentang peristiwa dan cara EventBridge memprosesnya, lihat EventBridge peristiwa di Panduan EventBridge Pengguna Amazon.

Bidang Umum: Semua Respons Insiden Keamanan AWS acara menyertakan EventBridge bidang Amazon standar ini

- versi: versi format EventBridge acara
- id: Pengenal unik untuk acara tersebut
- detail-type: Deskripsi yang dapat dibaca manusia dari jenis acara
- sumber: Selalu “aws.security-ir” untuk acara Respons Insiden Keamanan
- akun: ID AWS akun tempat kejadian terjadi
- waktu: Stempel waktu ISO 8601 saat peristiwa terjadi
- wilayah: Wilayah AWS di mana sumber daya ada
- sumber daya: Array yang berisi ARN dari sumber daya yang terpengaruh

Bidang Detail: `detail` Objek berisi informasi spesifik Respons Insiden Keamanan

- caseId: Pengidentifikasi unik untuk kasus ini (hanya peristiwa kasus)
- Membershipid: Pengidentifikasi unik untuk keanggotaan (hanya acara keanggotaan)
- UpdatedBy: Siapa yang melakukan pembaruan (acara pembaruan kasus dan komentar saja)
- CreatedBy: Siapa yang membuat entitas (hanya acara pembuatan kasus dan komentar)

Nilai Aktor: `createdBy` Bidang `updatedBy` dan dapat berisi

- AWS Responder: Tindakan yang dilakukan oleh responden AWS keamanan
- *`security-ir.amazonaws.com`*: Tindakan dilakukan secara otomatis oleh layanan
- ID Akun: Tindakan yang dilakukan oleh pelanggan (mis., “111122223333")

Nilai ARN sumber daya: Respons Insiden Keamanan AWS sumber daya menggunakan format ARN ini

- Kasus: `arn:aws:security-ir:{region}:{account-id}:case/{case-id}`
- Keanggotaan: `arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`

Peristiwa Kasus

Kasus Dibuat oleh AWS Responder

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

Kasus Dibuat oleh Layanan

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
```

```
        "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
      ],
      "detail": {
        "caseId": "1234567890",
        "createdBy": "security-ir.amazonaws.com"
      }
    }
```

Kasus yang Dibuat oleh Pelanggan

```
    {
      "version": "0",
      "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "detail-type": "Case Created",
      "source": "aws.security-ir",
      "account": "111122223333",
      "time": "2023-05-12T00:00:00Z",
      "region": "us-west-2",
      "resources": [
        "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
      ],
      "detail": {
        "caseId": "1234567890",
        "createdBy": "111122223333"
      }
    }
```

Kasus Diperbarui oleh AWS Responder

```
    {
      "version": "0",
      "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "detail-type": "Case Updated",
      "source": "aws.security-ir",
      "account": "111122223333",
      "time": "2023-05-12T01:30:00Z",
      "region": "us-west-2",
      "resources": [
        "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
```

```
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "AWS Responder"
    }
  }
```

Kasus Diperbarui oleh AWS Pelanggan

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Updated",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T02:15:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "111122223333"
    }
  }
```

Kasus Diperbarui oleh Respons Insiden Keamanan AWS Layanan

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Updated",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T03:45:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
```

```
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Kasus Tertutup

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Closed",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-15T14:22:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890"
  }
}
```

Acara Komentar Kasus

Komentar Kasus Dibuat oleh AWS Responder

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T04:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
```

```
    "detail": {
      "caseId": "1234567890",
      "createdBy": "AWS Responder"
    }
  }
```

Komentar Kasus Dibuat oleh Pelanggan

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

Komentar Kasus Dibuat oleh Respons Insiden Keamanan AWS Layanan

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
```

```
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

Komentar Kasus Diperbarui oleh Pelanggan

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

Komentar Kasus Diperbarui oleh Respons Insiden Keamanan AWS Layanan

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
```

```
            "updatedBy": "security-ir.amazonaws.com"
          }
        }
```

Komentar Kasus Dibuat oleh AWS Responder

```
        {
          "version": "0",
          "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
          "detail-type": "Case Comment Updated",
          "source": "aws.security-ir",
          "account": "111122223333",
          "time": "2023-05-12T02:45:00Z",
          "region": "us-west-2",
          "resources": [
            "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
          ],
          "detail": {
            "caseId": "1234567890",
            "updatedBy": "AWS Responder"
          }
        }
```

Acara Keanggotaan

Keanggotaan Dibuat

```
        {
          "version": "0",
          "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
          "detail-type": "Membership Created",
          "source": "aws.security-ir",
          "account": "111122223333",
          "time": "2023-04-01T10:00:00Z",
          "region": "us-west-2",
          "resources": [
            "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
          ],
```

```
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

Keanggotaan Diperbarui

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Updated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-04-15T16:30:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

Keanggotaan Dibatalkan

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Closed",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-06-30T23:59:59Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
```

```
            "membershipId": "m-1234567890abcdef0"
          }
        }
```

Keanggotaan Diakhiri

```
        {
          "version": "0",
          "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
          "detail-type": "Membership Terminated",
          "source": "aws.security-ir",
          "account": "111122223333",
          "time": "2023-07-01T00:00:00Z",
          "region": "us-west-2",
          "resources": [
            "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
          ],
          "detail": {
            "membershipId": "m-1234567890abcdef0"
          }
        }
```

Menggunakan Respons Insiden Keamanan AWS Acara

Anda dapat membuat EventBridge aturan untuk mencocokkan peristiwa ini dan memicu tindakan otomatis. Berikut adalah beberapa contoh kasus penggunaan:

Cocokkan semua Respons Insiden Keamanan AWS acara:

```
    {
      "source": ["aws.security-ir"]
    }
```

Cocokkan acara kasus saja:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

Kasus kecocokan diperbarui oleh AWS Responden:

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Case Updated"],
  "detail": {
    "updatedBy": ["AWS Responder"]
  }
}
```

Pertandingan acara untuk kasus tertentu:

```
{
  "source": ["aws.security-ir"],
  "detail": {
    "caseId": ["1234567890"]
  }
}
```

Tutorial: Mengirim peringatan Amazon Simple Notification Service untuk acara **`Membership Updated`**

Dalam tutorial ini, Anda mengonfigurasi aturan EventBridge acara Amazon yang hanya menangkap peristiwa di mana langganan Anda memasuki `Membership Updated` status.

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki langganan yang berfungsi dan AWS akun aktif dalam keanggotaan Anda.

Topik

- Tutorial: Membuat dan berlangganan topik Amazon SNS
- Tutorial: Daftarkan aturan acara
- Tutorial: Uji aturan Anda
- Aturan alternatif: Pembaruan Kasus Respons Insiden Keamanan

Tutorial: Membuat dan berlangganan topik Amazon SNS

Untuk tutorial ini, Anda mengonfigurasi topik Amazon SNS yang berfungsi sebagai target peristiwa untuk aturan peristiwa baru Anda.

Untuk membuat topik Amazon SNS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Pilih Topics (Topik), Create topic (Buat topik).
3. Untuk Tipe, pilih Standar.
4. Untuk Nama, masukkan **`MembershipUpdated`** dan pilih Buat topik.
5. Di MembershipUpdatedlayar, pilih Buat langganan.
6. Untuk Protokol, pilih Email.
7. UntukTitik akhir, masukkan alamat email yang Anda dapat mengaksesnya dan pilih Buat langganan.
8. Periksa akun email Anda dan tunggu sampai Anda menerima pesan email konfirmasi langganan. Saat Anda menerimanya, pilih Konfirmasi langganan.

Tutorial: Daftarkan aturan acara

Selanjutnya, daftarkan aturan acara yang hanya menangkap `Membership Updated` peristiwa.

Untuk mendaftarkan EventBridge aturan Anda

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.

2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan nama dan deskripsi untuk aturan.

> **Note**
>
> Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus kejadian yang sama.

5. Untuk bus acara, pilih bus acara yang ingin Anda kaitkan dengan aturan ini. Jika Anda ingin aturan ini cocok dengan acara yang berasal dari akun Anda, pilih bus acara AWS default. Ketika AWS layanan di akun Anda memancarkan suatu acara, itu selalu masuk ke bus acara default akun Anda.

> **Note**
>
> Ini harus diatur di akun administrator Anda AWS Organizations atau yang didelegasikan tempat Anda membuat Respons Insiden Keamanan AWS keanggotaan.

6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Untuk sumber acara, pilih Lainnya.
9. Untuk pola Acara, pilih Pola kustom (editor JSON).
10. Tempel pola peristiwa berikut ke area teks.

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Membership Updated"]
}
```

Kode ini mendefinisikan EventBridge aturan yang cocok dengan acara apa pun di mana keanggotaan layanan Anda diperbarui atau dimodifikasi. Untuk informasi selengkapnya tentang pola peristiwa, lihat Peristiwa dan Pola Peristiwa di Panduan EventBridge Pengguna Amazon.

11. Pilih Berikutnya.
12. Untuk Jenis target, pilih Layanan AWS .

13. Untuk Pilih target, pilih topik SNS, dan untuk Topik, pilih MembershipUpdated.
14. (Opsional) Untuk pengaturan tambahan, lakukan hal berikut:
    a. Untuk Masa peristiwa maksimal, masukkan nilai antara satu menit (00:01) dan 24 jam (24:00).
    b. Untuk Upaya coba lagi, masukkan angka antara 0 dan 185.
    c. Untuk antrian Dead-letter, pilih apakah akan menggunakan antrean Amazon SQS standar sebagai antrian huruf mati. EventBridge mengirimkan peristiwa yang cocok dengan aturan ini ke antrian huruf mati jika tidak berhasil dikirim ke target. Lakukan salah satu tindakan berikut:
        - Pilih Tidak ada untuk tidak menggunakan antrean surat mati.
        - Pilih Pilih antrean Amazon SQS di AWS akun saat ini untuk digunakan sebagai antrian huruf mati dan kemudian pilih antrian yang akan digunakan dari tarik-turun.
        - Pilih Pilih antrean Amazon SQS di AWS akun lain sebagai antrian huruf mati dan kemudian masukkan ARN antrian yang akan digunakan. Anda harus melampirkan kebijakan berbasis sumber daya ke antrian yang memberikan EventBridge izin untuk mengirim pesan ke antrean tersebut. Untuk informasi selengkapnya, lihat Memberikan izin untuk antrean huruf mati di Panduan Pengguna Amazon. EventBridge
15. Pilih Berikutnya.
16. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat EventBridge tag Amazon di Panduan EventBridge Pengguna Amazon.
17. Pilih Berikutnya.
18. Tinjau detail aturan dan pilih Buat aturan.

Tutorial: Uji aturan Anda

Untuk menguji aturan Anda, kirimkan pembaruan Respons Insiden Keamanan AWS keanggotaan Anda. Jika aturan Anda dikonfigurasi dengan benar, Anda akan menerima pesan email dalam beberapa menit dengan teks acara.

Aturan alternatif: Pembaruan Kasus Respons Insiden Keamanan

Untuk membuat aturan acara yang memantau semua pembaruan kasus, ulangi tutorial ini dengan perubahan berikut:

1. Di Tutorial: Membuat dan berlangganan topik Amazon SNS, gunakan *CaseUpdates* sebagai nama topik.
2. Dalam Tutorial: Daftarkan aturan acara, gunakan pola berikut di editor JSON:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

Pemecahan Masalah

Ketika Anda mengalami masalah yang terkait dengan melakukan tindakan khusus Respons Insiden Keamanan AWS, lihat topik di bagian ini.

ERROR adalah status operasi yang menunjukkan kesalahan dalam beberapa atau semua operasi. Atau, Anda menerima peringatan ketika masalah terjadi tetapi tugas masih selesai.

Daftar Isi

Masalah

Tidak mengirim permintaan dari konteks yang benar.

Semua panggilan ke Respons Insiden Keamanan AWS APIs harus berasal dari kepala IAM di administrator atau akun keanggotaan yang didelegasikan layanan. Pastikan bahwa Anda beroperasi dari kepala IAM yang benar di akun administrator atau keanggotaan Akun AWS yang Respons Insiden Keamanan AWS didelegasikan organisasi Anda.

Kesalahan

AccessDeniedException

Anda tidak memiliki akses yang memadai untuk melakukan tindakan ini.

Silakan bekerja sama dengan AWS administrator Anda untuk memastikan bahwa Anda memiliki izin untuk mengambil Peran IAM di administrator atau akun keanggotaan Respons Insiden Keamanan AWS yang didelegasikan. Juga periksa peran memiliki kebijakan IAM yang mengizinkan tindakan yang diminta. Untuk informasi lebih lanjut lihat Respons Insiden Keamanan AWS IAM.

ConflictException

Permintaan menyebabkan keadaan tidak konsisten.

Harap periksa apakah nama file lampiran kasus atau anggota tim respons default yang telah Anda tentukan adalah unik. Periksa juga apakah keanggotaan Respons Insiden Keamanan

AWS layanan Anda belum dikonfigurasi. Buka konsol Security Incident Response di https://console.aws.amazon.com/security-ir/ dan navigasikan ke`Membership Details`.

InternalServerException

Terjadi kesalahan tak terduga selama pemrosesan permintaan. Silakan coba lagi dalam beberapa menit. Jika masalah berlanjut, angkat kasus dengan Dukungan.

ResourceNotFoundException

Permintaan mereferensikan sumber daya yang tidak ada.

Satu atau lebih sumber daya yang ditentukan dalam permintaan Anda tidak ada. Harap periksa apakah semua sumber daya IDs yang diberikan ARNs atau benar. Ini berlaku untuk AWS Organizations IDs, akun IDs, peran IAM, keanggotaan, kasus, anggota tim respons, kasus, responden kasus, lampiran kasus, dan komentar kasus.

ThrottlingException

Permintaan ditolak karena throttling permintaan.

Terlalu banyak permintaan telah dibuat oleh prinsipal IAM Anda ke fungsi API tersebut dalam periode tertentu. Tunggu sebentar dan coba lagi. Jika masalah berlanjut, harap pertimbangkan untuk menerapkan backoff eksponensial dan algoritma coba lagi.

ValidationException

Input gagal memenuhi kendala yang ditentukan oleh file. Layanan AWS

Satu atau beberapa bidang data dalam permintaan Anda tidak memenuhi persyaratan validasi dan/atau kombinasi logis. Harap periksa apakah semua sumber daya ARNs lengkap, dan bahwa nilai teks memenuhi batasan ukuran dan format dari Panduan Referensi Respons Insiden Keamanan AWS API. Periksa juga apakah pembaruan nilai apa pun diizinkan. Misalnya, mengubah kasus dari AWS didukung menjadi dikelola sendiri tidak dimungkinkan.

Dukungan

Jika Anda memerlukan bantuan tambahan, hubungi Dukungan Pusat untuk tujuan pemecahan masalah. Harap memiliki informasi berikut yang tersedia:

- Wilayah AWS Yang Anda gunakan

- Akun AWS ID keanggotaan
- Konten sumber Anda, jika berlaku dan tersedia
- Detail lain tentang masalah yang mungkin membantu pemecahan masalah

Keamanan

Daftar Isi

Perlindungan Data di Respons Insiden Keamanan AWS

Daftar Isi

Model tanggung jawab AWS bersama berlaku untuk perlindungan data untuk layanan Respons Insiden AWS Keamanan. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan yang ditawarkan di AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, silakan lihat Pertanyaan Umum Privasi Data. Untuk informasi tentang perlindungan data di Eropa, lihat AWS postingan blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan .

Untuk tujuan perlindungan data, praktik terbaik AWS keamanan menyatakan bahwa Anda harus melindungi kredensil AWS akun dan menyiapkan pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara ini, setiap pengguna hanya diberikan izin yang diperlukan untuk memenuhi tugas pekerjaan mereka. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default dalam AWS layanan.
- FIPS 140-3 saat ini tidak didukung oleh layanan.

Anda tidak boleh memasukkan informasi rahasia atau sensitif, seperti alamat email Anda, ke dalam tag atau bidang teks bentuk bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan AWS Support atau AWS layanan lain menggunakan konsol, API, AWS CLI, atau. AWS SDKs Data apa pun yang Anda masukkan tag atau bidang teks bentuk bebas yang digunakan untuk nama dapat digunakan untuk penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensil dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi data

Daftar Isi

Enkripsi diam

Data dienkripsi saat istirahat menggunakan enkripsi sisi server transparan. Hal ini membantu mengurangi beban operasional dan kompleksitas yang terlibat dalam melindungi data sensitif. Dengan enkripsi saat istirahat, Anda dapat membangun aplikasi yang sensitif terhadap keamanan yang memenuhi persyaratan kepatuhan enkripsi dan peraturan.

Enkripsi bergerak

Data yang dikumpulkan dan diakses oleh Respons Insiden Keamanan AWS secara eksklusif melalui saluran yang dilindungi Transport Layer Security (TLS).

Manajemen kunci

Respons Insiden Keamanan AWS mengimplementasikan integrasi dengan AWS KMS untuk menyediakan enkripsi saat istirahat untuk data kasus dan lampiran.

Respons Insiden Keamanan AWS tidak mendukung kunci yang dikelola pelanggan.

Privasi lalu lintas antar jaringan

Lalu lintas antara layanan dan aplikasi serta klien on-premise

Anda memiliki dua opsi konektivitas antara jaringan pribadi Anda dan AWS:

- AWS Site-to-Site VPN Koneksi. Untuk informasi selengkapnya, lihat Apa itu AWS Site-to-Site VPN? dalam Panduan Pengguna AWS Site-to-Site VPN .
- AWS Direct Connect Koneksi. Untuk informasi selengkapnya, lihat Apa itu AWS Direct Connect? dalam Panduan Pengguna AWS Direct Connect .

Akses ke Respons Insiden Keamanan AWS melalui jaringan melalui AWS dipublikasikan APIs. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.2. Kami merekomendasikan TLS 1.3. Klien juga harus mendukung suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan versi yang lebih baru support mode ini. Selain itu, Anda harus menandatangani permintaan menggunakan kunci akses ID dan kunci akses rahasia yang terkait dengan IAM pengguna utama, atau Anda dapat menggunakan AWS Security Token Service (STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Lalu lintas antara sumber daya AWS di Wilayah yang sama

Titik akhir Amazon Virtual Private Cloud (Amazon VPC) untuk Respons Insiden Keamanan AWS adalah entitas logis dalam VPC yang memungkinkan konektivitas hanya untuk. Respons Insiden Keamanan AWS Rutekan VPC Amazon meminta Respons Insiden Keamanan AWS dan merutekan respons kembali ke VPC. Untuk informasi selengkapnya, lihat Titik akhir VPC di Panduan Pengguna

Amazon VPC. Misalnya, kebijakan yang dapat Anda gunakan untuk mengontrol akses dari titik akhir VPC, lihat Menggunakan Kebijakan IAM untuk mengontrol akses ke DynamoDB.

> **Note**
>
> Titik akhir Amazon VPC tidak dapat diakses melalui atau. AWS Site-to-Site VPN AWS Direct Connect

Identity and Access Management

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke sumber daya. AWS Administrator IAM mengontrol prinsip yang diautentikasi (masuk) dan resmi (memiliki izin) untuk menggunakan sumber daya. Respons Insiden Keamanan AWS IAM adalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Daftar Isi

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. Respons Insiden Keamanan AWS

Administrator Keamanan

Pengguna ini disarankan untuk menggunakan kebijakan AWSSecurityIncidentResponseFullAccessterkelola untuk memastikan mereka memiliki akses baca dan tulis ke sumber daya keanggotaan dan kasus.

Pengamat Kasus

Orang-orang ini tidak memiliki akses otoritatif ke semua kasus tetapi kasus individual yang Anda berikan izin eksplisit.

Anggota Tim Respons Insiden

Anggota tim dapat diberikan keanggotaan penuh dan akses kasus. Disarankan bahwa tidak semua individu memiliki tindakan otoritatif pada keanggotaan layanan tetapi harus memiliki akses ke setiap

dan semua kasus yang dibuat dan dikelola melalui layanan. Untuk informasi selengkapnya, lihat kebijakan Respons Insiden Keamanan AWS terkelola.

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai pengguna root AWS akun, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS Pengguna IAM Identity Center (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke Konsol AWS Manajemen atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke AWS akun Anda di Panduan Pengguna AWS Masuk.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan API AWS dalam Panduan Pengguna IAM.

Terlepas dari metode otentikasi yang Anda gunakan, Anda mungkin diminta untuk memberikan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor di Panduan Pengguna Pusat AWS Identitas IAM dan Menggunakan otentikasi multi-faktor (MFA) di Panduan Pengguna IAM. AWS

AWS pengguna root akun

Saat Anda membuat AWS akun, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini disebut pengguna root AWS akun dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Jangan pernah menggunakan pengguna root untuk tugas sehari-hari Anda dan mengambil langkah-langkah untuk melindungi kredensyal pengguna root Anda. Hanya gunakan

mereka untuk melakukan tugas-tugas yang hanya dapat dilakukan oleh pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas federasi

Ini adalah praktik terbaik untuk meminta pengguna manusia, termasuk mereka yang membutuhkan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS layanan dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, AWS Directory Service, direktori Pusat Identitas, atau pengguna mana pun yang mengakses AWS layanan dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses AWS akun, mereka mengambil peran, dan peran tersebut memberikan kredensyal sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua AWS akun dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas IAM? di Panduan Pengguna Pusat AWS Identitas IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam AWS akun Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Kami merekomendasikan untuk mengandalkan kredensi sementara daripada membuat pengguna IAM yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensil jangka panjang dengan pengguna IAM, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan kumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna

memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari lebih lanjut, lihat Kapan membuat pengguna IAM (bukan peran) di Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam AWS akun Anda yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara waktu di Konsol AWS Manajemen dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL khusus. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi — Untuk menetapkan izin ke identitas federasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga di Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin di Panduan Pengguna Pusat AWS Identitas IAM.
- Izin pengguna IAM sementara — Pengguna atau peran IAM dapat mengambil peran IAM untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan peran IAM untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa AWS layanan, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa AWS layanan menggunakan fitur di AWS layanan lain. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Peran layanan — Peran layanan adalah peran IAM yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus

peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke layanan AWS dalam Panduan Pengguna IAM.

- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke layanan. AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di AWS akun Anda dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat permintaan AWS CLI atau API. AWS Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM.

Untuk mempelajari apakah akan menggunakan peran IAM atau pengguna IAM, lihat Kapan membuat peran IAM (bukan pengguna) di Panduan Pengguna IAM.

Bagaimana Respons Insiden Keamanan AWS Bekerja dengan IAM

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke sumber daya dengan aman. AWS Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Respons Insiden AWS Keamanan. IAM adalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Fitur IAM yang dapat Anda gunakan dengan AWS Security Incident Response	
Fitur IAM	Penyelarasan layanan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya

Fitur IAM yang dapat Anda gunakan dengan AWS Security Incident Response	
Kunci kondisi kebijakan	Ya (global)
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Daftar Isi

Kebijakan berbasis identitas untuk Respons Insiden Keamanan AWS

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Daftar Isi

- Contoh kebijakan berbasis identitas
- Praktik terbaik kebijakan
- Menggunakan Respons Insiden Keamanan AWS konsol
- Mengizinkan pengguna melihat izin mereka sendiri
- Kebijakan Berbasis Sumber Daya
- Tindakan Kebijakan

Contoh kebijakan berbasis identitas

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi Respons Insiden Keamanan AWS sumber daya. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Administrator IAM dapat membuat kebijakan IAM untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Respons Insiden AWS Keamanan, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi Respons Insiden Keamanan AWS di Referensi Otorisasi Layanan.

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus Respons Insiden Keamanan AWS sumber daya di akun Anda. Tindakan ini dapat menimbulkan biaya untuk AWS akun Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di AWS akun Anda. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan terkelola AWS pelanggan yang spesifik untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.

Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.

Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui AWS layanan tertentu, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.

Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.

Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di akun Anda AWS , aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam IAM dalam Panduan Pengguna IAM.

Menggunakan Respons Insiden Keamanan AWS konsol

Untuk mengakses https://console.aws.amazon.com/security-ir/, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang Respons Insiden Keamanan AWS sumber daya di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Lampirkan kebijakan Respons Insiden Keamanan AWS Akses atau ReadOnly AWS terkelola untuk memastikan bahwa pengguna dan peran dapat menggunakan konsol layanan. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan CLI AWS atau API secara terprogram. AWS

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "ViewOwnUserInfo",
"Effect": "Allow",
"Action": [
"iam:GetUserPolicy",
"iam:ListGroupsForUser",
"iam:ListAttachedUserPolicies",
"iam:ListUserPolicies",
"iam:GetUser"
],
"Resource": ["arn:AWS:iam::*:user/${AWS:username}"]
},
{
"Sid": "NavigateInConsole",
"Effect": "Allow",
"Action": [
"iam:GetGroupPolicy",
"iam:GetPolicyVersion",
"iam:GetPolicy",
"iam:ListAttachedGroupPolicies",
"iam:ListGroupPolicies",
"iam:ListPolicyVersions",
"iam:ListPolicies",
"iam:ListUsers"
],
```

```
"Resource": "*"
}
]
}
```

Kebijakan Berbasis Sumber Daya

Kebijakan berbasis sumber daya dalam Respons Insiden Keamanan AWS

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Principal dapat meliputi akun, pengguna, peran, pengguna gabungan, atau layanan AWS .

Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Tindakan Kebijakan

Tindakan kebijakan untuk Respons Insiden Keamanan AWS

Tindakan kebijakan Support: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen Tindakan kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar Respons Insiden Keamanan AWS tindakan, lihat Tindakan yang ditentukan oleh Respons Insiden Keamanan AWS dalam Referensi Otorisasi Layanan.

Tindakan kebijakan Respons Insiden Keamanan AWS menggunakan awalan berikut sebelum tindakan:

Respons Insiden Keamanan AWS -identitas

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

“Action”: ["Respons Insiden Keamanan AWS -identity:action1"," -identity:action2"]Respons Insiden Keamanan AWS

Sumber daya kebijakan untuk Respons Insiden AWS Keamanan Amazon

Mendukung sumber daya kebijakan: Ya Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan Resource JSON menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan Sumber Daya atau NotResource elemen. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

“Sumber Daya”: “*”

Kunci kondisi kebijakan untuk Respons Insiden AWS Keamanan

Mendukung kunci kondisi kebijakan khusus layanan: Tidak

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen Kondisi (atau blok Kondisi) memungkinkan Anda menentukan kondisi di mana pernyataan berlaku. Elemen Syarat bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen Kondisi dalam pernyataan, atau beberapa kunci dalam satu elemen Kondisi, AWS mengevaluasi mereka menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan operasi OR logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tanda dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Daftar kontrol akses (ACLs) di Respons Insiden Keamanan AWS

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Kontrol akses berbasis atribut (ABAC) dengan AWS Respons Insiden Keamanan

Mendukung ABAC (tag dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tanda ke entitas IAM (pengguna atau peran) dan ke banyak sumber daya AWS . Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian Anda merancang kebijakan ABAC untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses. ABAC sangat membantu dalam lingkungan yang berkembang pesat dan membantu situasi di mana manajemen kebijakan menjadi rumit.

Untuk mengontrol akses berdasarkan tag, Anda memberikan informasi tag dalam elemen kondisi kebijakan menggunakan kunci kondisi: /key-name, AWS: ResourceTag /key-name, atau AWS:RequestTag. AWS TagKeys Jika layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, maka nilainya adalah Ya untuk layanan tersebut. Jika layanan mendukung ketiga kunci kondisi hanya untuk beberapa jenis sumber daya, maka nilainya adalah Partial. Untuk informasi lebih lanjut tentang ABAC, lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Kredensyal sementara dengan Respons Insiden AWS Keamanan Amazon

Mendukung kredensial sementara: Ya

AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk AWS layanan mana yang bekerja dengan kredensi sementara, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM. Anda menggunakan kredensi sementara jika masuk ke Konsol AWS Manajemen menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan AWS CLI atau API. AWS Anda kemudian dapat menggunakan kredensil sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensyal sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk Respons Insiden AWS Keamanan

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari prinsipal yang memanggil AWS layanan, dikombinasikan dengan layanan yang meminta untuk membuat permintaan ke AWS layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan AWS layanan atau sumber daya lain untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Memecahkan masalah Respons Insiden Keamanan AWS identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Security Incident Response dan IAM.

Topik

- Saya tidak berwenang untuk melakukan suatu tindakan
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses Respons Insiden Keamanan AWS sumber daya saya

Saya tidak berwenang untuk melakukan suatu tindakan

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM mateojackson mencoba menggunakan konsol untuk melihat detail tentang my-example-widget sumber daya fiksi tetapi tidak memiliki izin AWS Security Incident Response: fiksi. GetWidget

User: arn ::iam AWS: :123456789012:user/mateojackson tidak berwenang untuk melakukan:: on resource: my -example-widget Respons Insiden Keamanan AWS GetWidget

Dalam hal ini, kebijakan untuk pengguna mateojackson harus diperbarui untuk mengizinkan akses ke my-example-widget sumber daya dengan menggunakan tindakan Respons Insiden Keamanan AWS :GetWidget .

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan PassRole tindakan iam:, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran. Respons Insiden Keamanan AWS

Beberapa AWS layanan memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama marymajor mencoba menggunakan konsol untuk melakukan tindakan di AWS Security Incident Response. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

Pengguna: arn ::iam: :123456789012 AWS: user/marymajor tidak diizinkan untuk melakukan: iam: PassRole

Dalam hal ini, kebijakan Mary harus diperbarui untuk memungkinkannya melakukan iam: PassRole action. Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Respons Insiden AWS Keamanan saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Amazon Respons Insiden Keamanan AWS mendukung fitur ini, lihat Cara Respons Insiden AWS Keamanan bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh AWS akun yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di AWS akun lain yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda ke AWS akun pihak ketiga, lihat Menyediakan akses ke AWS akun yang dimiliki oleh pihak ketiga di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Menggunakan peran layanan

Mendukung peran layanan: Tidak

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan di Panduan Pengguna IAM.

Menggunakan peran terkait layanan

Peran terkait layanan untuk Respons Insiden Keamanan AWS

Daftar Isi

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke layanan. AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Peran terkait layanan membuat pengaturan Respons Insiden Keamanan AWS lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Respons Insiden Keamanan AWS mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Respons Insiden Keamanan AWS dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM dan cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

AWS SLR: AWSService RoleForSecurityIncidentResponse

Respons Insiden Keamanan AWS menggunakan Respons Insiden Keamanan AWS kebijakan peran terkait layanan (SLR) bernama AWSService RoleForSecurityIncidentResponse — untuk mengidentifikasi akun yang dilanggan, membuat kasus, dan menandai sumber daya terkait.

Izin

Peran AWSService RoleForSecurityIncidentResponse terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `triage.security-ir.amazonaws.com`

Terlampir pada peran ini adalah kebijakan AWS terkelola bernama AWSSecurityIncidentResponseServiceRolePolicy. Layanan menggunakan peran untuk melakukan tindakan pada sumber daya berikut:

- AWS Organizations: Memungkinkan layanan untuk mencari akun keanggotaan untuk digunakan dengan layanan.
- CreateCase: Memungkinkan layanan membuat kasus layanan atas nama akun keanggotaan.
- TagResource: Memungkinkan sumber daya tag layanan yang dikonfigurasi sebagai bagian dari layanan.

Mengelola peran

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda melakukan onboard ke Respons Insiden Keamanan AWS dalam AWS Management Console, the AWS CLI, atau AWS API, layanan akan membuat peran terkait layanan untuk Anda.

> **Note**
>
> Jika Anda membuat keanggotaan menggunakan akun administrator yang didelegasikan, maka peran terkait layanan harus dibuat secara manual di AWS Organizations akun Manajemen.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Ketika Anda onboard ke layanan, itu menciptakan peran terkait layanan untuk Anda lagi.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage

Respons Insiden Keamanan AWS menggunakan peran terkait layanan (SLR) bernama AWSServiceRoleForSecurityIncidentResponse_Triage — Respons Insiden Keamanan AWS kebijakan untuk terus memantau lingkungan Anda dari ancaman keamanan, menyesuaikan layanan keamanan untuk mengurangi kebisingan peringatan, dan mengumpulkan informasi untuk menyelidiki potensi insiden.

Izin

Peran AWSServiceRoleForSecurityIncidentResponse_Triage terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `triage.security-ir.amazonaws.com`

Terlampir pada peran ini adalah kebijakan yang AWS dikelola AWSSecurityIncidentResponseTriageServiceRolePolicy. Layanan menggunakan peran untuk melakukan tindakan pada sumber daya berikut:

- Acara: Memungkinkan layanan untuk membuat aturan Amazon EventBridge terkelola. Aturan ini adalah infrastruktur yang diperlukan di AWS akun Anda untuk mengirimkan acara dari akun Anda ke layanan. Tindakan ini dilakukan pada AWS sumber daya apa pun yang dikelola oleh`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: Memungkinkan layanan untuk menyetel layanan keamanan untuk mengurangi kebisingan peringatan dan mengumpulkan informasi untuk menyelidiki potensi insiden. Tindakan ini dilakukan pada AWS sumber daya apa pun.
- AWS Security Hub: Memungkinkan layanan untuk menyetel layanan keamanan untuk mengurangi kebisingan peringatan dan mengumpulkan informasi untuk menyelidiki potensi insiden. Tindakan ini dilakukan pada AWS sumber daya apa pun.

Mengelola peran

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda melakukan onboard ke Respons Insiden Keamanan AWS dalam AWS Management Console, the AWS CLI, atau AWS API, layanan akan membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Ketika Anda onboard ke layanan, itu menciptakan peran terkait layanan untuk Anda lagi.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Wilayah yang didukung untuk Respons Insiden Keamanan AWS peran terkait layanan

Respons Insiden Keamanan AWS mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia.

- AS Timur (Ohio)

- AS Barat (Oregon)
- AS Timur (Virginia)
- EU (Frankfurt)
- EU (Ireland)
- EU (London)
- Eropa (Paris)
- EU (Stockholm)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- (Canada (Central)
- Amerika Selatan (Sao Paulo)

AWS Kebijakan Terkelola

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di AWS akun Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola terkait. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

Daftar Isi

AWS kebijakan terkelola: AWSSecurity IncidentResponseServiceRolePolicy

Respons Insiden Keamanan AWS menggunakan kebijakan AWSSecurity IncidentResponseServiceRolePolicy AWS terkelola. Kebijakan AWS terkelola ini dilampirkan pada peran AWSServiceRoleForSecurityIncidentResponseterkait layanan. Kebijakan ini menyediakan akses Respons Insiden Keamanan AWS untuk mengidentifikasi akun yang dilanggan, membuat kasus, dan menandai sumber daya terkait.

> **Important**
>
> Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- AWS Organizations: Memungkinkan layanan untuk mencari akun keanggotaan untuk digunakan dengan layanan.
- CreateCase: Memungkinkan layanan membuat kasus layanan atas nama akun keanggotaan.

- TagResource: Memungkinkan sumber daya tag layanan yang dikonfigurasi sebagai bagian dari layanan.

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk AWSSecurityIncidentResponseServiceRolePolicy.

AWS kebijakan terkelola: AWSSecurity IncidentResponseFullAccess

Respons Insiden Keamanan AWS menggunakan kebijakan AWSSecurity IncidentResponseAdmin AWS terkelola. Kebijakan ini memberikan akses penuh ke sumber daya layanan dan akses ke yang terkait Layanan AWS. Anda dapat menggunakan kebijakan ini dengan prinsipal IAM Anda untuk menambahkan izin dengan cepat. Respons Insiden Keamanan AWS

> **Important**
>
> Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- Akses read-only utama IAM: Memberi pengguna layanan kemampuan untuk melakukan tindakan hanya-baca terhadap sumber daya yang ada. Respons Insiden Keamanan AWS
- Akses tulis utama IAM: Memberikan pengguna layanan kemampuan untuk memperbarui, memodifikasi, menghapus, dan membuat Respons Insiden Keamanan AWS sumber daya.

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk AWSSecurityIncidentResponseFullAccess.

AWS kebijakan terkelola: AWSSecurity IncidentResponseReadOnlyAccess

Respons Insiden Keamanan AWS menggunakan kebijakan AWSSecurity IncidentResponseReadOnlyAccess AWS terkelola. Kebijakan ini memberikan akses hanya-baca ke sumber daya kasus layanan. Anda dapat menggunakan kebijakan ini dengan prinsipal IAM Anda untuk menambahkan izin dengan cepat. Respons Insiden Keamanan AWS

> **Important**
>
> Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- Akses read-only utama IAM: Memberi pengguna layanan kemampuan untuk melakukan tindakan hanya-baca terhadap sumber daya yang ada. Respons Insiden Keamanan AWS

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk AWSSecurityIncidentResponseReadOnlyAccess.

AWS kebijakan terkelola: AWSSecurity IncidentResponseCaseFullAccess

Respons Insiden Keamanan AWS menggunakan kebijakan AWSSecurity IncidentResponseCaseFullAccess AWS terkelola. Kebijakan ini memberikan akses penuh ke sumber daya kasus layanan. Anda dapat menggunakan kebijakan ini dengan prinsipal IAM Anda untuk menambahkan izin dengan cepat. Respons Insiden Keamanan AWS

> **Important**
>
> Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- Akses hanya-baca kasus utama IAM: Memberi pengguna layanan kemampuan untuk melakukan tindakan hanya-baca terhadap kasus yang ada. Respons Insiden Keamanan AWS
- Akses tulis kasus utama IAM: Memberikan pengguna layanan kemampuan untuk memperbarui, memodifikasi, menghapus, dan membuat Respons Insiden Keamanan AWS kasus.

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk AWSSecurityIncidentResponseCaseFullAccess.

AWS kebijakan terkelola: AWSSecurity IncidentResponseTriageServiceRolePolicy

Respons Insiden Keamanan AWS menggunakan kebijakan AWSSecurity IncidentResponseTriageServiceRolePolicy AWS terkelola. Kebijakan AWS terkelola ini dilampirkan pada peran AWSServiceRoleForSecurityIncidentResponse_Triageterkait layanan.

Kebijakan ini menyediakan akses Respons Insiden Keamanan AWS untuk terus memantau lingkungan Anda untuk ancaman keamanan, menyesuaikan layanan keamanan untuk mengurangi kebisingan peringatan, dan mengumpulkan informasi untuk menyelidiki potensi insiden. Anda tidak dapat melampirkan kebijakan ini ke entitas IAM Anda.

> **Important**
>
> Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Respons Insiden Keamanan AWS menggunakan tag untuk memberi Anda layanan administrasi. Tag tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif

Rincian izin

Layanan menggunakan kebijakan ini untuk melakukan tindakan pada sumber daya berikut:

- Acara: Memungkinkan layanan untuk membuat aturan EventBridge terkelola Amazon. Aturan ini adalah infrastruktur yang diperlukan di AWS akun Anda untuk mengirimkan acara dari akun Anda ke layanan. Tindakan ini dilakukan pada AWS sumber daya apa pun yang dikelola oleh`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: Memungkinkan layanan untuk menyetel layanan keamanan untuk mengurangi kebisingan peringatan dan mengumpulkan informasi untuk menyelidiki potensi insiden. Tindakan ini dilakukan pada AWS sumber daya apa pun.
- AWS Security Hub: Memungkinkan layanan untuk menyetel layanan keamanan untuk mengurangi kebisingan peringatan dan mengumpulkan informasi untuk menyelidiki potensi insiden. Tindakan ini dilakukan pada AWS sumber daya apa pun.

Anda dapat melihat izin yang terkait dengan kebijakan ini dalam kebijakan AWS terkelola untuk AWSSecurityIncidentResponseTriageServiceRolePolicy.

Respons Insiden Keamanan AWS pembaruan SLRs dan kebijakan terkelola

Lihat detail tentang pembaruan Respons Insiden Keamanan AWS SLRs dan peran kebijakan terkelola sejak layanan ini mulai melacak perubahan ini.

Perubahan	Deskripsi	Tanggal
Pembaruan untuk SLR menambahkan izin untuk mendukung hak layanan.	AWSSecurityIncidentResponseTriageServiceRolePolicytelah diperbarui untuk menambahkan security-ir:GetMembership, security-ir:, security-ir:ListMemberships, guardduty:, guarduty:, guardduty:UpdateCase, dan guardduty: ListFilters izin. guardduty: UpdateFilter DeleteFilter ditambahkan untuk memfasilitasi pengelolaan filter Arsip Otomatis di akun yang didelegasikan. GetAdministratorAccount GetAdministratorAccount GuardDuty	02 Juni 2025
SLR baru — AWSServiceRoleForSecurityIncidentResponse Kebijakan terkelola baru — AWSSecurityIncidentResponseServiceRolePolicy.	Peran terkait layanan baru dan kebijakan terlampir yang memungkinkan akses layanan ke AWS Organizations akun Anda untuk mengidentifikasi keanggotaan.	Desember 1, 2024
SLR baru — AWSServiceRoleForSecurityIn	Peran terkait layanan baru dan kebijakan terlampir yang memungkinkan akses layanan ke AWS Organizations akun Anda untuk melakukan triase peristiwa keamanan.	Desember 1, 2024

Perubahan	Deskripsi	Tanggal
cidentRes ponse_Triage Kebijakan terkelola baru - AWSSecuri tyInciden tResponse TriageSer viceRolePolicy		
Kebijakan terkelola baru - AWSSecuri tyInciden tResponse FullAccess	Respons Insiden Keamanan AWS tambahkan SLR baru untuk dilampirkan ke prinsipal IAM untuk tindakan baca dan tulis untuk layanan.	Desember 1, 2024
Peran kebijakan terkelola baru - AWSSecuri tyInciden tResponse ReadOnlyAccess	Respons Insiden Keamanan AWS tambahkan SLR baru untuk dilampirkan ke prinsipal IAM untuk tindakan baca	Desember 1, 2024
Peran kebijakan terkelola baru - AWSSecuri tyInciden tResponse CaseFullAccess	Respons Insiden Keamanan AWS tambahkan SLR baru untuk dilampirkan ke prinsip IAM untuk tindakan baca dan tulis untuk kasus layanan.	Desember 1, 2024
Mulai melacak perubahan.	Mulai melacak perubahan untuk Respons Insiden Keamanan AWS SLRs dan kebijakan terkelola	Desember 1, 2024

Respons insiden

Keamanan dan Kepatuhan adalah tanggung jawab bersama antara AWS dan pelanggan. Model bersama ini dapat membantu meringankan beban operasional pelanggan saat AWS mengoperasikan, mengelola, dan mengontrol komponen dari sistem operasi host dan lapisan virtualisasi hingga keamanan fisik fasilitas tempat layanan beroperasi. Pelanggan memikul tanggung jawab dan pengelolaan sistem operasi tamu (termasuk pembaruan dan patch keamanan), perangkat lunak aplikasi terkait lainnya serta konfigurasi firewall grup keamanan yang AWS disediakan. Untuk informasi tambahan lihat model tanggung jawab AWS bersama.

Dengan menetapkan garis dasar keamanan yang memenuhi tujuan aplikasi Anda yang berjalan di cloud, Anda dapat mendeteksi penyimpangan yang dapat Anda tanggapi. Karena respons insiden keamanan dapat menjadi topik yang kompleks, kami mendorong Anda untuk meninjau sumber daya berikut sehingga Anda lebih dapat memahami dampak respons insiden dan pilihan Anda terhadap tujuan perusahaan Anda: whitepaper Praktik Terbaik AWS Keamanan, dan white paper Perspektif Keamanan AWS Cloud Adoption Framework (CAF).

Validasi kepatuhan

Auditor pihak ketiga menilai keamanan dan kepatuhan AWS layanan sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Respons Insiden Keamanan AWS belum dievaluasi untuk kepatuhan dengan program-program yang disebutkan di atas.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWS layanan dalam lingkup oleh program kepatuhan. Untuk informasi umum, lihat program AWS kepatuhan.

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh laporan di AWS Artifak.

Tanggung jawab kepatuhan Anda saat menggunakan AWS layanan ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan l AWS dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan memulai cepat keamanan dan kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS

- Arsitektur untuk whitepaper keamanan dan kepatuhan HIPAA - Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan untuk membuat aplikasi yang sesuai dengan HIPAA. AWS
- AWS sumber daya kepatuhan - Kumpulan buku kerja dan panduan yang berlaku berdasarkan and/or lokasi industri.
- Mengevaluasi sumber daya dengan Aturan AWS Config dalam Panduan Pengembang AWS Config — AWS Config; menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub — AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk mengevaluasi AWS sumber daya Anda dan untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — AWS Layanan ini mendeteksi potensi ancaman terhadap AWS akun, beban kerja, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit Manager — AWS Layanan ini membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Pencatatan dan pemantauan dalam Respons Insiden AWS Keamanan

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja Respons Insiden Keamanan AWS dan AWS solusi Anda yang lain. Respons Insiden Keamanan AWS saat ini mendukung AWS layanan berikut untuk memantau organisasi Anda dan aktivitas yang terjadi di dalamnya.

AWS CloudTrail — Dengan CloudTrail Anda dapat menangkap panggilan API dari konsol AWS Security Incident Response. Misalnya, ketika pengguna mengautentikasi, CloudTrail dapat merekam detail seperti alamat IP dalam permintaan, siapa yang membuat permintaan, dan kapan itu dibuat.

Amazon CloudWatch Metrics — Dengan CloudWatch metrik, Anda dapat memantau, melaporkan, dan mengambil tindakan otomatis jika terjadi peristiwa dalam waktu dekat. Misalnya, Anda dapat

membuat CloudWatch dasbor pada metrik yang disediakan untuk memantau Respons Insiden Keamanan AWS penggunaan Anda, atau Anda dapat membuat CloudWatch alarm pada metrik yang disediakan untuk memberi tahu Anda tentang pelanggaran ambang batas yang ditetapkan.

Namespace untuk layanan ini adalah AWS/Usage/. ServiceName Nama metrik yang tersedia adalah ActiveManagedCases dan SelfManagedCases.

Sesuai dengan Ketentuan AWS Layanan, tim Respons Insiden Keamanan AWS responden akan memiliki akses ke riwayat, data log VPC CloudTrail, DNS, dan S3 Anda. Data ini dapat digunakan selama insiden keamanan aktif ketika kasus terbuka di portal layanan AWS Security Incident Response.

Ketahanan

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat infrastruktur AWS global.

Keamanan infrastruktur

Respons Insiden Keamanan AWS dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Respons Insiden Keamanan AWS melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.

- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredenal keamanan sementara untuk menandatangani permintaan.

Konfigurasi dan analisis kerentanan

Anda bertanggung jawab untuk mengelola peran penahanan layanan dan kumpulan AWS CloudFormation tumpukan terkait.

AWS menangani tugas-tugas keamanan dasar, seperti sistem operasi tamu (OS) dan patch database, konfigurasi firewall, dan pemulihan bencana. Prosedur ini telah ditinjau dan disertifikasi oleh pihak ketiga yang sesuai. Untuk detail selengkapnya, lihat AWS sumber daya berikut:

- Model tanggung jawab bersama
- Praktik terbaik untuk keamanan, identitas, & kepatuhan

Pencegahan "confused deputy" lintas layanan

Masalah "confused deputy" adalah masalah keamanan saat entitas yang tidak memiliki izin untuk melakukan suatu tindakan dapat memaksa entitas yang memilik hak akses lebih tinggi untuk melakukan tindakan tersebut. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS sediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsip layanan yang telah diberikan akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi SourceAccount global AWSAWS: SourceArn dan: dalam kebijakan sumber daya untuk membatasi izin yang diberikan Amazon Connect kepada layanan lain ke sumber daya. Jika Anda menggunakan kedua kunci konteks kondisi global, SourceAccount nilai AWS: dan akun dalam SourceArn nilai AWS: harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

Cara paling efektif untuk melindungi dari masalah wakil yang membingungkan adalah dengan menggunakan Nama Sumber Daya Amazon (ARN) yang tepat dari sumber daya yang ingin Anda izinkan. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks SourceArn global AWS: dengan wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, arn ::servicename: :region-name AWS: :your account ID: *. AWS

Untuk contoh kebijakan peran asumsi yang menunjukkan bagaimana Anda dapat mencegah masalah wakil yang membingungkan, lihat Kebijakan pencegahan wakil yang bingung.

Service Quotas

Respons Insiden Keamanan AWS

Tabel berikut mencantumkan kuota, untuk Respons Insiden Keamanan AWS sumber daya untuk Anda Akun AWS. Beberapa kuota dapat ditingkatkan di atas yang dinyatakan di bawah ini dengan persetujuan manajer layanan. Kecuali dinyatakan lain, kuota ini adalah per Wilayah.

	Nama	Default	Dapat disesuaikan	Komentar
1	Kasus aktif AWS yang didukung	10	Ya (hingga 50)	Jumlah kasus aktif yang meminta bantuan dari AWS CIRT.
2	Kasus aktif yang dikelola sendiri	50	Ya (hingga 100)	Jumlah kasus aktif yang menggunakan platform tanpa bantuan dari AWS CIRT.
3	Kasus yang didukung layanan dibuat dalam waktu 24 jam	10	Tidak	Jumlah kasus yang dibuat meminta bantuan dari AWS CIRT dibuat dalam jendela bergulir 24 jam.
4	Jumlah maksimum entitas dalam tim	10	Tidak	Jumlah maksimum entitas dalam tim

	Nama	Default	Dapat disesuaikan	Komentar
	respons insiden default			respons insiden default.
5	Jumlah maksimum anggota tambahan pada suatu kasus	30	Tidak	Jumlah maksimum entitas yang terkait dengan kasus. Ini awalnya akan diisi dengan entitas dari tim respons insiden default Anda.
6	Jumlah Lampiran Kasus	50	Ya (hingga 100)	Jumlah maksimum file yang dapat dilampirkan ke kasing.
7	Ukuran komentar kasus maksimum	1000	Tidak	Jumlah karakter maksimum dalam komentar kasus.
8	Ukuran nama file Lampiran Kasus Maksimum	255	Tidak	Jumlah karakter maksimum dalam nama file.

Respons Insiden Keamanan AWS Panduan teknis

Daftar Isi

Abstrak

Panduan ini menyajikan ikhtisar dasar-dasar menanggapi insiden keamanan dalam lingkungan Amazon Web Services (AWS) Cloud pelanggan. Panduan ini memberikan ikhtisar tentang keamanan cloud dan konsep respons insiden serta mengidentifikasi kemampuan, layanan, dan mekanisme cloud yang tersedia bagi pelanggan yang merespons masalah keamanan.

Panduan ini ditujukan bagi mereka yang memiliki peran teknis dan mengasumsikan bahwa Anda terbiasa dengan prinsip-prinsip umum keamanan informasi, memiliki pemahaman dasar tentang respons insiden keamanan di lingkungan lokal Anda saat ini, dan memiliki keakraban dengan layanan cloud.

Apakah Anda sudah Well-Architected?

Kerangka Kerja AWS Well-Architected membantu Anda memahami pro dan kontra dari keputusan yang Anda buat saat membangun sistem di cloud. Enam pilar dari Kerangka Kerja ini memungkinkan Anda mempelajari praktik terbaik arsitektural untuk merancang dan mengoperasikan sistem yang

andal, aman, efisien, hemat biaya, dan berkelanjutan. Menggunakan AWS Well-Architected Tool, tersedia tanpa biaya di AWS Well-Architected Tool konsol, Anda dapat meninjau beban kerja Anda terhadap praktik terbaik ini dengan menjawab serangkaian pertanyaan untuk setiap pilar.

Untuk panduan lebih lanjut dari para ahli dan praktik terbaik untuk arsitektur cloud Anda—referensi penerapan arsitektur, diagram, dan laporan resmi—lihat Pusat Arsitektur AWS.

Pengantar

Keamanan adalah prioritas utama di AWS. AWS pelanggan mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk membantu mendukung kebutuhan organisasi yang paling sensitif terhadap keamanan. AWS memiliki model tanggung jawab bersama: AWS mengelola keamanan cloud, dan pelanggan bertanggung jawab atas keamanan di cloud. Artinya, Anda memiliki kendali penuh atas implementasi keamanan Anda, termasuk akses ke beberapa alat dan layanan untuk membantu memenuhi tujuan keamanan Anda. Berbagai kemampuan ini membantu Anda menetapkan garis dasar keamanan untuk aplikasi yang berjalan di AWS Cloud.

Ketika terjadi penyimpangan dari garis dasar, misalnya karena kesalahan konfigurasi atau perubahan faktor eksternal, Anda perlu merespons dan menyelidikinya. Agar bisa melakukannya dengan baik, Anda perlu memahami konsep dasar respons insiden keamanan di lingkungan AWS Anda dan persyaratan untuk mempersiapkan, mengedukasi, dan melatih tim cloud sebelum masalah keamanan terjadi. Penting untuk mengetahui kontrol dan kemampuan mana yang dapat Anda gunakan, meninjau contoh topikal untuk mengatasi masalah potensial, dan mengidentifikasi metode remediasi yang menggunakan otomatisasi untuk meningkatkan kecepatan dan konsistensi respons. Selain itu, Anda harus memahami persyaratan kepatuhan dan peraturan karena hal ini berkaitan dengan pembuatan program respons insiden keamanan untuk memenuhi persyaratan tersebut.

Respons insiden keamanan bisa menjadi hal yang kompleks, jadi kami mendorong Anda untuk menerapkan pendekatan iteratif: mulai dengan layanan keamanan inti, bangun kemampuan deteksi dan respons dasar, kemudian kembangkan playbook untuk membuat pustaka awal mekanisme respons insiden yang dapat diiterasi dan ditingkatkan.

Sebelum Anda mulai

Sebelum Anda mulai belajar tentang respons insiden untuk peristiwa keamanan di AWS, biasakan diri Anda dengan standar dan kerangka kerja yang relevan untuk AWS keamanan dan respons insiden. Fondasi ini akan membantu Anda memahami konsep dan praktik terbaik yang disajikan dalam panduan ini.

AWS standar keamanan dan kerangka kerja

Untuk memulai, kami mendorong Anda untuk meninjau Praktik Terbaik untuk Keamanan, Identitas, dan Kepatuhan, Pilar Keamanan - Kerangka Kerja AWS Well-Architected dan Perspektif Keamanan dari whitepaper Ikhtisar Cloud Adoption Framework AWS (CAF). AWS

AWS CAF menyediakan panduan yang mendukung koordinasi antara berbagai bagian organisasi yang bergerak ke cloud. Panduan AWS CAF dibagi menjadi beberapa area fokus, yang disebut sebagai perspektif, yang relevan untuk membangun sistem TI berbasis cloud. Perspektif keamanan menjelaskan cara menerapkan program keamanan di seluruh alur kerja, salah satunya adalah respons insiden. Dokumen ini merupakan produk dari pengalaman kami bekerja dengan pelanggan untuk membantu mereka membangun kemampuan serta program respons insiden keamanan yang efektif dan efisien.

Standar dan kerangka kerja respons insiden industri

Laporan resmi ini mengikuti standar respons insiden dan praktik terbaik dari Computer Security Incident Handling Guide SP 800-61 r2, yang dibuat oleh National Institute of Standards and Technology (NIST). Membaca dan memahami konsep yang diperkenalkan oleh NIST adalah prasyarat yang bermanfaat. Konsep dan praktik terbaik dari panduan NIST ini akan diterapkan pada AWS teknologi dalam paper ini. Namun, skenario insiden on-premise tidak tercakup dalam panduan ini.

AWS Ikhtisar respons insiden

Sebagai awal, penting untuk memahami bagaimana operasi keamanan dan respons insiden merupakan hal yang berbeda di cloud. Untuk membangun kemampuan respons yang efektif AWS, Anda perlu memahami penyimpangan dari respons lokal tradisional dan dampaknya terhadap program respons insiden Anda. Masing-masing perbedaan ini, serta prinsip-prinsip desain respons AWS insiden inti, dirinci dalam bagian ini.

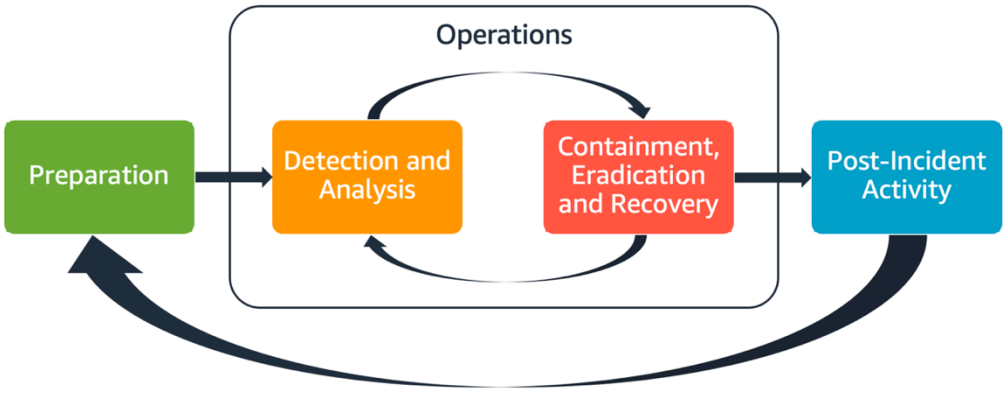
Aspek respon AWS insiden

Semua AWS pengguna dalam suatu organisasi harus memiliki pemahaman dasar tentang proses respons insiden keamanan, dan staf keamanan harus memahami bagaimana menanggapi masalah keamanan. Pendidikan, pelatihan, dan pengalaman sangat penting agar program respons insiden cloud berjalan dengan baik, dan idealnya diimplementasikan dengan baik sebelum harus menangani kemungkinan insiden keamanan. Fondasi program respons insiden yang baik di cloud adalah Persiapan, Operasi, dan Aktivitas Pascainsiden.

Untuk memahami setiap aspek ini, lihat deskripsi berikut:

- Persiapan — Siapkan tim respons insiden Anda untuk mendeteksi dan menanggapi insiden di dalamnya AWS dengan mengaktifkan kontrol detektif dan memverifikasi akses yang tepat ke alat dan layanan cloud yang diperlukan. Selain itu, siapkan playbook yang diperlukan, baik manual maupun otomatis, untuk memverifikasi respons yang andal dan konsisten.
- Operasi – Beroperasi pada peristiwa keamanan dan insiden potensial dengan mengikuti fase respons insiden NIST: mendeteksi, menganalisis, menahan, memberantas, dan memulihkan.
- Aktivitas pascainsiden – Lakukan iterasi pada hasil simulasi dan peristiwa keamanan Anda untuk meningkatkan efektivitas respons Anda, sehingga respons dan investigasi yang dilakukan bisa lebih bernilai, dan mengurangi risiko lebih lanjut. Anda harus belajar dari insiden dan memiliki sikap kepemilikan yang kuat terhadap aktivitas perbaikan.

Setiap aspek ini dikupas dan dibahas secara mendetail dalam panduan ini. Diagram berikut menunjukkan alur aspek-aspek ini, selaras dengan siklus hidup respons insiden NIST yang disebutkan sebelumnya, tetapi dengan operasi yang mencakup deteksi dan analisis dengan penahanan, pemberantasan, dan pemulihan.



Aspek respon AWS insiden

AWS prinsip respons insiden dan tujuan desain

Meskipun proses umum dan mekanisme respons insiden sebagaimana didefinisikan oleh NIST SP 800-61 Computer Security Incident Handling Guide sudah baik, kami mendorong Anda untuk juga mempertimbangkan tujuan desain spesifik ini, yang relevan untuk merespons insiden keamanan di lingkungan cloud:

- Menetapkan tujuan respons – Bekerja sama dengan pemangku kepentingan, penasihat hukum, dan kepemimpinan organisasi untuk menentukan tujuan dalam merespons suatu insiden. Beberapa tujuan umum termasuk menahan dan memitigasi masalah, memulihkan sumber daya yang terkena dampak, menyimpan data untuk forensik, kembali ke operasi aman yang diketahui, dan belajar dari insiden.
- Merespons menggunakan cloud – Menerapkan pola respons di dalam cloud, tempat peristiwa dan data terjadi.
- Ketahui apa yang Anda miliki dan apa yang Anda butuhkan – Simpan log, sumber daya, snapshot, dan bukti lainnya dengan menyalin dan menyimpannya di akun cloud terpusat khusus untuk respons. Gunakan tag, metadata, dan mekanisme yang menerapkan kebijakan retensi. Anda harus memahami layanan apa yang Anda gunakan dan kemudian mengidentifikasi persyaratan untuk menyelidiki layanan tersebut. Untuk membantu Anda memahami lingkungan Anda, Anda juga dapat menggunakan tag, yang akan dibahas nanti dalam dokumen ini di bagian the section called “Mengembangkan dan menerapkan strategi pemberian tag”.
- Gunakan mekanisme deployment ulang – Jika anomali keamanan dapat dikaitkan dengan kesalahan konfigurasi, remediasinya mungkin cukup dengan menghapus perbedaan konfigurasi ini dengan deployment ulang sumber daya menggunakan konfigurasi yang tepat. Jika teridentifikasi adanya kemungkinan penyusupan, verifikasi bahwa deployment ulang Anda mencakup mitigasi akar penyebab yang berhasil dan terverifikasi.
- Otomatiskan jika memungkinkan – Ketika masalah muncul atau insiden berulang, bangun mekanisme untuk melakukan triase secara terprogram dan merespons peristiwa umum. Gunakan respons manusia untuk insiden unik, kompleks, atau sensitif yang tidak cukup dengan otomatisasi.
- Pilih solusi yang dapat diskalakan – Berusahalah untuk mengimbangi skalabilitas pendekatan organisasi Anda terhadap komputasi cloud. Terapkan mekanisme deteksi dan respons yang dapat diskalakan di seluruh lingkungan Anda agar dapat memangkas waktu antara deteksi dan respons secara efektif.
- Pelajari dan tingkatkan proses Anda – Bersikaplah proaktif ketika mengidentifikasi kesenjangan dalam proses, alat, atau orang Anda, dan terapkan rencana untuk memperbaikinya. Simulasi adalah metode yang aman untuk menemukan kesenjangan dan memperbaiki proses. Lihat bagian the section called “Aktivitas pascainsiden” di dokumen ini untuk detail tentang cara melakukan iterasi proses Anda.

Sasaran desain ini merupakan pengingat untuk meninjau implementasi arsitektur Anda agar dapat melakukan respons insiden dan deteksi ancaman. Saat Anda merencanakan implementasi cloud Anda, pikirkan tentang menanggapi suatu insiden, idealnya dengan metodologi respons yang baik

secara forensik. Dalam beberapa kasus, ini berarti Anda mungkin memiliki beberapa organisasi, akun, dan alat yang secara khusus disiapkan untuk tugas respons ini. Alat dan fungsi ini harus tersedia bagi responden insiden melalui alur deployment. Alat dan fungsi tersebut tidak boleh statis karena dapat menyebabkan risiko yang lebih besar.

Domain insiden keamanan cloud

Untuk secara efektif mempersiapkan dan menanggapi peristiwa keamanan di AWS lingkungan Anda, Anda perlu memahami jenis insiden keamanan cloud bersama. Ada tiga domain dalam tanggung jawab pelanggan tempat insiden keamanan dapat terjadi: layanan, infrastruktur, dan aplikasi. Domain yang berbeda membutuhkan pengetahuan, alat, dan proses respons yang berbeda. Pertimbangkan domain berikut:

- Domain layanan — Insiden dalam domain layanan dapat memengaruhi izin AWS Identity and Access Management(IAM) Akun AWS, metadata sumber daya, penagihan, atau area lainnya. Peristiwa domain layanan adalah peristiwa yang Anda tanggapi secara eksklusif dengan mekanisme AWS API, atau di mana Anda memiliki akar penyebab yang terkait dengan konfigurasi atau izin sumber daya, dan mungkin memiliki logging berorientasi layanan terkait.
- Domain infrastruktur — Insiden dalam domain infrastruktur mencakup data atau aktivitas terkait jaringan, seperti proses dan data pada instans Amazon Elastic Compute Cloud (EC2Amazon), lalu lintas ke instans EC2 Amazon Anda dalam virtual private cloud (VPC), dan area lainnya, seperti container atau layanan future lainnya. Respons Anda terhadap peristiwa domain infrastruktur sering kali melibatkan perolehan data terkait insiden untuk analisis forensik. Ini mungkin mencakup interaksi dengan sistem operasi sebuah instance, dan, dalam berbagai kasus, mungkin juga melibatkan mekanisme AWS API. Dalam domain infrastruktur, Anda dapat menggunakan kombinasi alat AWS APIs forensik/respons insiden (DFIR) digital dalam sistem operasi tamu, seperti EC2 instans Amazon yang didedikasikan untuk melakukan analisis dan investigasi forensik. Insiden domain infrastruktur mungkin melibatkan analisis tangkapan paket jaringan, blok disk pada volume Amazon Elastic Block Store (Amazon EBS), atau memori volatil yang diperoleh dari sebuah instans.
- Domain aplikasi – Insiden dalam domain aplikasi terjadi dalam kode aplikasi atau dalam perangkat lunak yang di-deploy untuk layanan atau infrastruktur. Domain ini harus disertakan dalam playbook deteksi dan respons ancaman cloud Anda, dan dapat menyertakan respons serupa dengan yang ada di domain infrastruktur. Dengan arsitektur aplikasi yang tepat dan bijaksana, Anda dapat mengelola domain ini dengan alat cloud dengan menggunakan akuisisi, pemulihan, dan penerapan otomatis.

Dalam domain ini, pertimbangkan aktor yang mungkin bertindak melawan AWS akun, sumber daya, atau data. Baik internal maupun eksternal, gunakan kerangka risiko untuk menentukan risiko spesifik bagi organisasi dan melakukan persiapan sebagaimana mestinya. Selain itu, Anda harus mengembangkan model ancaman, yang dapat membantu perencanaan respons insiden dan pembangunan arsitektur yang cermat.

Perbedaan utama dari respons insiden di AWS

Respons insiden merupakan bagian integral dari strategi keamanan siber, baik on-premise maupun di cloud. Prinsip-prinsip keamanan seperti hak istimewa terkecil dan pertahanan secara mendalam dimaksudkan untuk melindungi kerahasiaan, integritas, dan ketersediaan data baik di tempat maupun di cloud. Beberapa pola respons insiden yang mendukung prinsip-prinsip keamanan ini mengikuti, termasuk retensi log, pemilihan peringatan yang berasal dari pemodelan ancaman, pengembangan playbook, serta integrasi informasi keamanan dan manajemen peristiwa (SIEM). Perbedaannya dimulai ketika pelanggan mulai merancang dan merekayasa pola-pola ini di cloud. Berikut ini adalah perbedaan utama dari respons insiden di AWS.

Perbedaan #1: Keamanan sebagai tanggung jawab bersama

Tanggung jawab untuk keamanan dan kepatuhan dibagi antara AWS dan pelanggannya. Model tanggung jawab bersama ini meringankan beberapa beban operasional pelanggan karena AWS mengoperasikan, mengelola, dan mengendalikan komponen dari sistem operasi host dan lapisan virtualisasi hingga keamanan fisik fasilitas di mana layanan beroperasi. Untuk detail lebih lanjut tentang model tanggung jawab bersama, lihat dokumentasi Model Tanggung Jawab Bersama.

Saat tanggung jawab bersama Anda di cloud berubah, opsi Anda untuk respons insiden juga berubah. Merencanakan dan memahami timbal balik ini serta mencocokkannya dengan kebutuhan tata kelola Anda adalah langkah penting dalam respons insiden.

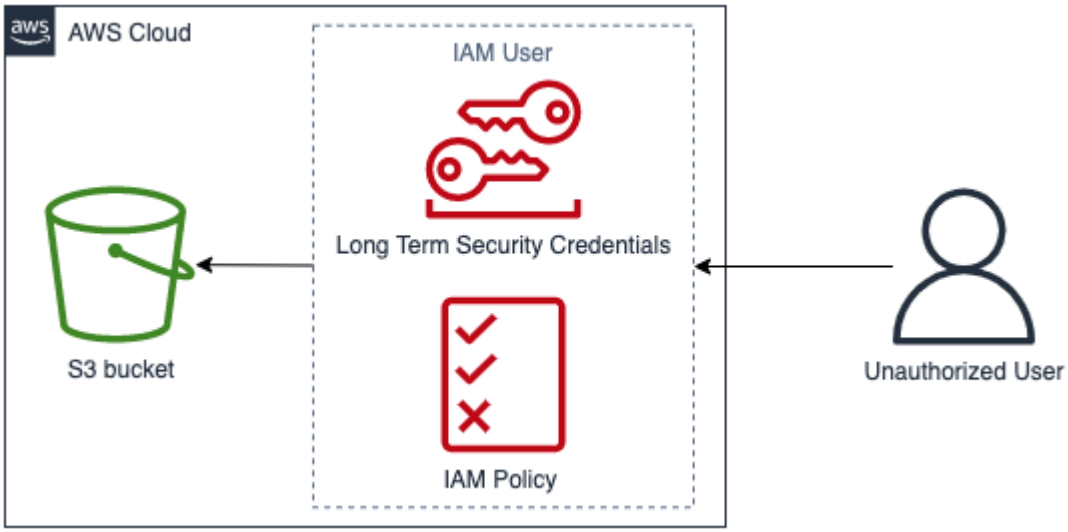
Selain hubungan langsung yang Anda miliki dengan AWS, mungkin ada entitas lain yang memiliki tanggung jawab dalam model tanggung jawab khusus Anda. Misalnya, Anda mungkin memiliki unit organisasi internal yang bertanggung jawab atas beberapa aspek operasi Anda. Anda mungkin juga memiliki hubungan dengan pihak lain yang mengembangkan, mengelola, atau mengoperasikan beberapa teknologi cloud Anda.

Membuat dan menguji rencana respons insiden yang sesuai dan playbook yang sesuai dengan model operasi Anda sangatlah penting.

Perbedaan #2: Domain layanan cloud

Karena perbedaan tanggung jawab keamanan yang ada di layanan cloud, diperkenalkanlah domain baru untuk insiden keamanan: domain layanan, yang dijelaskan sebelumnya di bagian Domain insiden. Domain layanan mencakup AWS akun pelanggan, izin IAM, metadata sumber daya, penagihan, dan area lainnya. Domain ini berbeda untuk respons insiden karena cara meresponsnya. Respons dalam domain layanan biasanya dilakukan dengan meninjau dan mengeluarkan panggilan API, bukan respons berbasis host dan berbasis jaringan tradisional. Dalam domain layanan, Anda tidak akan berinteraksi dengan sistem operasi sumber daya yang terpengaruh.

Diagram berikut menunjukkan contoh peristiwa keamanan dalam domain layanan berdasarkan anti-pola arsitektur. Dalam peristiwa ini, pengguna yang tidak sah mendapatkan kredensial keamanan jangka panjang dari pengguna IAM. Pengguna IAM memiliki kebijakan IAM yang memungkinkan mereka mengambil objek dari bucket Amazon Simple Storage Service (Amazon S3). Untuk menanggapi peristiwa keamanan ini, Anda akan menggunakan AWS APIs untuk menganalisis AWS log seperti AWS CloudTraildan log akses Amazon S3. Anda juga akan menggunakan AWS APIs untuk menahan dan memulihkan dari insiden tersebut.



Contoh domain layanan

Perbedaan #3: APIs untuk penyediaan infrastruktur

Perbedaan lain berasal dari Karakteristik cloud layanan mandiri on-demand. Pelanggan fasilitas utama berinteraksi dengan menggunakan RESTful API melalui titik akhir publik dan pribadi yang tersedia di banyak lokasi geografis di seluruh dunia. AWS Cloud Pelanggan dapat mengaksesnya APIs dengan AWS kredensil. Berbeda dengan kontrol akses on-premise, kredensial ini tidak harus terikat oleh jaringan atau domain Microsoft Active Directory. Kredensi malah dikaitkan dengan

prinsipal IAM di dalam akun. AWS Titik akhir API ini dapat diakses di luar jaringan perusahaan Anda, yang penting untuk dipahami ketika Anda merespons insiden di mana kredensial digunakan di luar jaringan atau geografi yang Anda harapkan.

Karena sifat berbasis API AWS, sumber log penting untuk menanggapi peristiwa keamanan adalah AWS CloudTrail, yang melacak panggilan API manajemen yang dibuat di AWS akun Anda dan di mana Anda dapat menemukan informasi tentang lokasi sumber panggilan API.

Perbedaan #4: Sifat dinamis cloud

Cloud bersifat dinamis; memungkinkan Anda membuat dan menghapus sumber daya dengan cepat. Dengan penskalaan otomatis, sumber daya dapat diputar dan diputar berdasarkan peningkatan lalu lintas. Dengan infrastruktur berumur pendek dan perubahan yang serbacepat, sumber daya yang Anda selidiki mungkin sudah tidak ada lagi atau mungkin telah dimodifikasi. Memahami sifat AWS sumber daya yang fana dan bagaimana Anda dapat melacak pembuatan dan penghapusan AWS sumber daya akan menjadi penting untuk analisis insiden. Anda dapat menggunakan AWS Configuntuk melacak riwayat konfigurasi AWS sumber daya Anda.

Perbedaan #5: Akses data

Akses data juga berbeda di cloud. Anda tidak dapat terhubung ke server untuk mengumpulkan data yang Anda butuhkan untuk penyelidikan keamanan. Data dikumpulkan melalui kabel dan melalui panggilan API. Anda harus berlatih dan memahami cara melakukan pengumpulan data agar siap menghadapi shift ini, dan memverifikasi penyimpanan yang sesuai untuk pengumpulan dan akses yang efektif. APIs

Perbedaan #6: Pentingnya otomatisasi

Agar pelanggan dapat sepenuhnya menyadari manfaat adopsi cloud, strategi operasional mereka harus menerapkan otomatisasi. Infrastructure as code (IAc) adalah pola lingkungan otomatis yang sangat efisien di mana AWS layanan dikerahkan, dikonfigurasi, dikonfigurasi ulang, dan dihancurkan menggunakan kode yang difasilitasi oleh layanan IAc asli seperti atau solusi pihak ketiga. AWS CloudFormation Hal ini mendorong implementasi respons insiden menjadi sangat otomatis, yang diinginkan untuk menghindari kesalahan manusia, terutama saat menangani bukti. Meskipun otomatisasi digunakan di lingkungan on-premise, otomatisasi sangat penting dan lebih sederhana di AWS Cloud.

Mengatasi perbedaan-perbedaan ini

Untuk mengatasi perbedaan ini, ikuti langkah-langkah yang diuraikan di bagian berikutnya untuk memverifikasi bahwa program respons insiden Anda untuk orang, proses, dan teknologi dipersiapkan dengan baik.

Persiapan

Persiapan untuk menghadapi insiden merupakan hal yang sangat penting agar respons insiden bisa dilakukan dengan cepat dan efektif. Persiapan dilakukan di tiga domain:

- Orang – Dalam mempersiapkan orang-orang Anda untuk menghadapi insiden keamanan, pemangku kepentingan yang relevan perlu diidentifikasi untuk respons insiden, dan dilatih tentang respons insiden dan teknologi cloud.
- Proses – Dalam mempersiapkan proses Anda untuk menghadapi insiden keamanan, perlu adanya pendokumentasian arsitektur, pengembangan rencana respons insiden menyeluruh, dan pembuatan playbook agar respons terhadap peristiwa keamanan bisa dilakukan secara konsisten.
- Teknologi – Dalam mempersiapkan teknologi Anda untuk menghadapi insiden keamanan, perlu adanya pengaturan akses, agregasi dan pemantauan log yang diperlukan, penerapan mekanisme peringatan yang efektif, dan pengembangan respons serta kemampuan penyelidikan.

Setiap domain ini sama pentingnya agar respons insiden berjalan efektif. Tanpa ketiga domain ini, program respons insiden tidak akan lengkap atau efektif. Anda perlu mempersiapkan orang, proses, dan teknologi dengan integrasi yang erat agar siap menghadapi suatu insiden.

Orang

Untuk merespons peristiwa keamanan, Anda perlu mengidentifikasi pemangku kepentingan yang akan mendukung respons terhadap peristiwa keamanan. Selain itu, sangat penting untuk respons yang efektif agar mereka dilatih tentang AWS teknologi dan AWS lingkungan Anda.

Menentukan peran dan tanggung jawab

Menangani peristiwa keamanan membutuhkan disiplin lintas organisasi dan komitmen untuk bertindak. Dalam struktur organisasi Anda, harus ada banyak orang yang bertanggung jawab, akuntabel, dimintai pendapat, atau diinformasikan saat terjadi insiden, seperti perwakilan dari sumber daya manusia (SDM), tim eksekutif, dan hukum. Pertimbangkan peran dan tanggung jawab ini, dan apakah ada pihak ketiga yang harus dilibatkan. Perhatikan bahwa di banyak geografi, ada

hukum setempat yang mengatur apa yang harus dan tidak boleh dilakukan. Meskipun upaya untuk membangun bagan yang bertanggung jawab, akuntabel, berdasarkan konsultasi, dan terinformasi (RACI) untuk rencana respons keamanan Anda terasa birokratis, hal itu memungkinkan komunikasi yang cepat dan langsung serta dengan jelas menguraikan kepemimpinan di berbagai tahap peristiwa.

Selama insiden, termasuk pemilik/pengembang aplikasi dan sumber daya yang terkena dampak adalah kunci karena mereka adalah ahli materi pelajaran (SMEs) yang dapat memberikan informasi dan konteks untuk membantu dalam mengukur dampak. Pastikan untuk mempraktikkan dan membangun hubungan dengan developer serta pemilik aplikasi sebelum Anda mengandalkan keahlian mereka untuk respons insiden. Pemilik aplikasi atau SMEs, seperti administrator atau insinyur cloud Anda, mungkin perlu bertindak dalam situasi di mana lingkungan tidak dikenal atau memiliki kompleksitas, atau di mana responden tidak memiliki akses.

Terakhir, hubungan tepercaya mungkin terlibat dalam penyelidikan atau tanggapan karena mereka dapat memberikan keahlian tambahan dan pengawasan yang berharga. Ketika tidak ada orang yang memiliki keterampilan ini dalam tim Anda sendiri, ada baiknya Anda menyewa pihak eksternal untuk bantuan.

Melatih staf respons insiden

Melatih staf respons insiden Anda tentang teknologi yang digunakan organisasi mereka akan sangat penting agar mereka mampu merespons peristiwa keamanan secara memadai. Respons mungkin akan berlarut-larut jika anggota staf Anda tidak memahami teknologi yang mendasarinya. Selain konsep respons insiden tradisional, penting juga bagi mereka untuk memahami AWS layanan dan AWS lingkungan mereka. Ada sejumlah mekanisme tradisional untuk melatih staf insiden Anda, seperti pelatihan online dan pelatihan di ruang kelas. Anda juga dapat mempertimbangkan untuk menjalankan simulasi atau gameday sebagai mekanisme untuk pelatihan. Untuk detail tentang cara menjalankan simulasi, lihat the section called “Menjalankan simulasi reguler” bagian dokumen ini.

Memahami AWS Cloud teknologi

Untuk mengurangi ketergantungan dan memangkas waktu respons, pastikan tim keamanan dan responden Anda diedukasi tentang layanan cloud dan memiliki kesempatan untuk praktik langsung dengan lingkungan cloud spesifik yang digunakan organisasi Anda. Agar responden insiden menjadi efektif, penting untuk memahami AWS yayasan, IAM,, layanan AWS penebangan dan pemantauan, dan layanan AWS keamanan. AWS Organizations

AWS menyediakan lokakarya keamanan online (lihat Lokakarya AWS Keamanan) di mana Anda bisa mendapatkan pengalaman langsung dengan layanan AWS keamanan dan pemantauan. AWS juga menyediakan sejumlah opsi pelatihan dan jalur pembelajaran melalui pelatihan digital, pelatihan

kelas, mitra AWS pelatihan, dan sertifikasi. Untuk mempelajari lebih lanjut, lihat AWS Training and Certification.

AWS menyediakan pelatihan berbasis gratis dan berlangganan yang mendukung banyak persona dan area fokus. Kunjungi AWS Skillbuilder untuk mempelajari lebih lanjut.

Pahami AWS lingkungan Anda

Selain memahami AWS layanan, kasus penggunaannya, dan bagaimana mereka berintegrasi satu sama lain, sama pentingnya untuk memahami bagaimana AWS lingkungan organisasi Anda sebenarnya dirancang dan proses operasional apa yang ada. Sering kali, pengetahuan internal seperti ini tidak didokumentasikan dan hanya dipahami oleh beberapa pakar domain, yang dapat menciptakan ketergantungan, menghambat inovasi, dan memperlambat waktu respons.

Untuk menghindari ketergantungan ini dan mempercepat waktu respons, pengetahuan internal tentang lingkungan AWS Anda harus didokumentasikan, dapat diakses, dan dipahami oleh analis keamanan Anda. Memahami cakupan cloud Anda secara menyeluruh akan membutuhkan kolaborasi antara pemangku kepentingan keamanan yang relevan dan administrator cloud. Bagian dari mempersiapkan proses Anda untuk respons insiden mencakup mendokumentasikan dan memusatkan diagram arsitektur, yang the section called “Mendokumentasikan dan memusatkan diagram arsitektur” nantinya dalam laporan resmi ini. Namun, dari perspektif orang, penting bagi analis Anda untuk mengakses dan memahami diagram dan proses operasional yang terkait dengan lingkungan Anda AWS .

Memahami tim AWS respons dan dukungan

Dukungan

Dukunganmenawarkan berbagai rencana yang menyediakan akses ke alat dan keahlian yang mendukung kesuksesan dan kondisi operasional AWS solusi. Jika Anda membutuhkan dukungan teknis dan sumber daya lainnya untuk membantu merencanakan, menerapkan, dan mengoptimalkan AWS lingkungan, Anda dapat memilih paket dukungan yang paling sesuai dengan kasus AWS penggunaan Anda.

Pertimbangkan Pusat Dukungan di AWS Management Console (diperlukan login) sebagai titik kontak utama untuk mendapatkan dukungan untuk masalah yang memengaruhi AWS sumber daya Anda. Akses ke Dukungan dikendalikan oleh IAM. Untuk informasi selengkapnya tentang mendapatkan akses ke fitur AWS Support, lihat Memulai dengan Dukungan.

Selain itu, jika Anda perlu melaporkan penyalahgunaan, hubungi tim AWS Tust and Safety.

AWS Tim Respons Insiden Pelanggan (CIRT)

AWS Customer Incident Response Team (CIRT) adalah AWS tim global khusus yang selalu tersedia yang memberikan dukungan kepada pelanggan selama acara keamanan aktif di sisi pelanggan Model Tanggung Jawab AWS Bersama.

Ketika AWS CIRT mendukung Anda, Anda akan menerima bantuan dengan triase dan pemulihan untuk acara keamanan aktif. AWS Mereka akan membantu dalam analisis akar penyebab melalui penggunaan log AWS layanan dan memberi Anda rekomendasi untuk pemulihan. Mereka juga akan memberikan rekomendasi keamanan dan praktik terbaik untuk membantu Anda menghindari peristiwa keamanan ke depannya.

AWS pelanggan dapat melibatkan AWS CIRT melalui kasus AWS dukungan.

- Semua Pelanggan:
  1. Akun dan penagihan
  2. Layanan
  3. Keamanan kategori
  4. Keparahan: Pertanyaan umum

- Pelanggan dengan Dukungan paket Pengembang:
  1. Akun dan penagihan
  2. Layanan
  3. Keamanan kategori
  4. Keparahan: Pertanyaan penting

- Pelanggan dengan Dukungan rencana Bisnis:
  1. Akun dan penagihan
  2. Layanan
  3. Keamanan kategori
  4. Keparahan: Pertanyaan berdampak bisnis yang mendesak

- Pelanggan dengan Dukungan paket Enterprise:
  1. Akun dan penagihan
  2. Layanan

3. Keamanan kategori
4. Keparahan: Pertanyaan risiko bisnis kritis

- Pelanggan dengan Respons Insiden Keamanan AWS langganan: Buka konsol Security Incident Response di https://console.aws.amazon.com/security-ir/

DDoDukungan respons S

AWS penawaran AWS Shield, yang menyediakan layanan perlindungan penolakan layanan terdistribusi (DDoS) terkelola yang melindungi aplikasi web yang berjalan. AWS AWS Shield menyediakan deteksi selalu aktif dan mitigasi inline otomatis yang dapat meminimalkan waktu henti dan latensi aplikasi, sehingga tidak perlu terlibat untuk mendapatkan manfaat dari perlindungan S. Dukungan DDo Ada dua tingkatan AWS Shield: Shield Standard dan Shield Advanced. Untuk mengetahui perbedaan antara kedua tingkatan ini, lihat Dokumentasi fitur Shield.

AWS Managed Services (AMS)

AWS Managed Services(AMS) menyediakan pengelolaan AWS infrastruktur yang berkelanjutan sehingga Anda dapat fokus pada aplikasi Anda. Dengan menerapkan praktik terbaik untuk memelihara infrastruktur Anda, AMS membantu mengurangi biaya operasional dan risiko Anda. AMS mengotomatiskan aktivitas umum seperti permintaan perubahan, pemantauan, manajemen patch, keamanan, dan layanan pencadangan, serta menyediakan layanan siklus hidup penuh untuk menyediakan, menjalankan, dan mendukung infrastruktur Anda.

AMS bertanggung jawab untuk menyebarkan serangkaian kontrol detektif keamanan dan memberikan respons pertama setiap hari terhadap peringatan. Saat peringatan dimulai, AMS mengikuti seperangkat standar playbook otomatis dan manual untuk memverifikasi respons yang konsisten. Playbook ini dibagikan kepada pelanggan AMS saat orientasi agar mereka dapat mengembangkan dan mengoordinasikan respons dengan AMS.

Proses

Mengembangkan proses respons insiden yang menyeluruh dan jelas adalah kunci untuk program respons insiden yang sukses dan terukur. Ketika peristiwa keamanan terjadi, langkah dan alur kerja yang jelas akan membantu Anda merespons secara tepat waktu. Anda mungkin sudah memiliki proses respons insiden yang ada. Terlepas dari keadaan saat ini, penting untuk memperbarui, mengulangi, dan menguji proses respons insiden Anda secara teratur.

Mengembangkan dan menguji rencana respons insiden

Dokumen pertama yang dikembangkan untuk respons insiden adalah rencana respons insiden. Rencana respons insiden dirancang untuk menjadi dasar bagi program dan strategi respons insiden Anda. Rencana respons insiden adalah dokumen komprehensif yang biasanya mencakup bagian-bagian ini:

- ikhtisar tim respons insiden – Menguraikan tujuan dan fungsi tim respons insiden
- Peran dan tanggung jawab – Membuat daftar pemangku kepentingan respons insiden dan menjabarkan peran mereka ketika insiden terjadi
- Rencana komunikasi – Detail informasi kontak dan bagaimana mekanisme komunikasi selama insiden

  Ini adalah praktik terbaik untuk memiliki out-of-band komunikasi sebagai cadangan untuk komunikasi insiden. Contoh aplikasi yang menyediakan saluran out-of-band komunikasi aman adalah AWS Wickr.
- Fase respons insiden dan tindakan yang harus diambil - Menghitung fase respons insiden - misalnya, mendeteksi, menganalisis, memberantas, menahan, dan memulihkan - termasuk tindakan tingkat tinggi yang harus diambil dalam fase-fase tersebut
- Definisi keparahan insiden dan prioritas – Memerinci cara mengklasifikasikan tingkat keparahan suatu insiden, bagaimana memprioritaskan insiden, lalu bagaimana definisi keparahan mempengaruhi prosedur eskalasi

Meskipun bagian-bagian ini umumnya ada di perusahaan dalam berbagai ukuran dan industri yang berbeda, rencana respons insiden akan berbeda-beda di setiap organisasi. Anda perlu membuat rencana respons insiden yang paling sesuai untuk organisasi Anda.

Mendokumentasikan dan memusatkan diagram arsitektur

Untuk merespons peristiwa keamanan dengan cepat dan akurat, Anda perlu memahami bagaimana sistem dan jaringan Anda dirancang. Memahami pola internal ini tidak hanya penting untuk respons insiden, tetapi juga untuk memverifikasi konsistensi di seluruh aplikasi yang dirancang dengan pola tersebut, sesuai dengan praktik terbaik. Anda juga harus memverifikasi bahwa dokumentasi ini aktual dan diperbarui secara berkala sesuai pola arsitektur baru. Anda sebaiknya mengembangkan dokumentasi dan repositori internal yang menjabarkan item-item seperti:

- AWS struktur akun - Anda perlu tahu:

  - Berapa banyak AWS akun yang Anda miliki?
  - Bagaimana AWS akun-akun itu diatur?
  - Siapa pemilik bisnis AWS akun tersebut?
  - Apakah Anda menggunakan Kebijakan Kontrol Layanan (SCPs)? Jika demikian, pagar pembatas organisasi apa yang diterapkan dengan menggunakan? SCPs
  - Apakah Anda membatasi Wilayah dan layanan yang dapat digunakan?
  - Apa perbedaan antara unit bisnis dan lingkungan (dev/test/prod)?
- AWS pola layanan
  - AWS Layanan apa yang Anda gunakan?
  - Apa AWS layanan yang paling banyak digunakan?
- Pola arsitektur
  - Arsitektur cloud apa yang Anda gunakan?
- AWS pola otentikasi
  - Bagaimana developer Anda biasanya mengautentikasi ke AWS?
  - Apakah Anda menggunakan pengguna atau peran IAM (atau keduanya)? Apakah otentikasi Anda AWS terhubung ke Identity Provider (IdP)?
  - Bagaimana Anda memetakan pengguna atau peran IAM ke karyawan atau sistem?
  - Bagaimana cara akses dicabut ketika seseorang tidak lagi diotorisasi?
- AWS pola otorisasi
  - Kebijakan IAM apa yang digunakan developer Anda?
  - Apakah Anda menggunakan kebijakan berbasis sumber daya?
- Pencatatan dan pemantauan
  - Sumber pencatatan apa yang Anda gunakan dan di mana sumber tersebut disimpan?
  - Apakah Anda mengumpulkan AWS CloudTrail log? Jika iya, di mana log tersebut disimpan?
  - Bagaimana Anda menanyakan CloudTrail log?
  - Apakah Anda GuardDuty mengaktifkan Amazon?
  - Bagaimana Anda mengakses GuardDuty temuan (misalnya, konsol, sistem tiket, SIEM)?
  - Apakah temuan atau peristiwa dikumpulkan dalam SIEM?
  - Apakah tiket dibuat secara otomatis?
  - Alat apa yang ada untuk menganalisis log dalam sebuah penyelidikan?
- Topologi jaringan

  - Bagaimana perangkat, titik akhir, dan koneksi di jaringan Anda diatur secara fisik atau logis?
  - Bagaimana jaringan Anda terhubung AWS?
  - Bagaimana lalu lintas jaringan disaring antarlingkungan?
- Infrastruktur eksternal
  - Bagaimana aplikasi yang menghadap ke luar digunakan?
  - AWS Sumber daya apa yang dapat diakses publik?
  - AWS Akun apa yang mengandung infrastruktur yang dihadapi secara eksternal?
  - Apa DDo S atau penyaringan eksternal yang ada?

Mendokumentasikan diagram dan proses teknis internal memudahkan pekerjaan analis respons insiden, membantu mereka dengan cepat memperoleh pengetahuan kelembagaan untuk merespons peristiwa keamanan. Dokumentasi proses teknis internal secara menyeluruh tidak hanya menyederhanakan investigasi keamanan, tetapi juga menyesuaikan rasionalisasi dan evaluasi proses.

Mengembangkan playbook respons insiden

Bagian penting dari mempersiapkan proses respons insiden Anda adalah mengembangkan playbook. Playbook respons insiden memberikan serangkaian panduan preskriptif dan langkah-langkah yang harus diikuti ketika terjadi peristiwa keamanan. Struktur dan langkah yang jelas akan menyederhanakan respons dan mengurangi kemungkinan kesalahan manusia.

Untuk apa saja playbook dibuat

Playbook sebaiknya dibuat untuk skenario insiden seperti:

- Insiden yang diantisipasi – Playbook harus dibuat untuk insiden yang Anda antisipasi. Hal ini termasuk ancaman seperti denial of service (DoS), ransomware, dan pembobolan kredensial.
- Temuan atau peringatan keamanan yang diketahui — Buku pedoman harus dibuat untuk temuan dan peringatan keamanan Anda yang diketahui, seperti temuan. GuardDuty Anda mungkin menerima GuardDuty temuan dan berpikir, “Sekarang apa?” Untuk mencegah kesalahan penanganan GuardDuty temuan atau mengabaikan temuan, buat buku pedoman untuk setiap temuan potensial. GuardDuty Beberapa rincian remediasi dan panduan dapat ditemukan dalam GuardDutydokumentasi. Perlu dicatat bahwa tidak GuardDuty diaktifkan secara default dan menimbulkan biaya. Detail lebih lanjut tentang GuardDuty dapat ditemukan di Lampiran A: Definisi kemampuan cloud -. the section called “Visibilitas dan peringatan”

Apa saja yang perlu dimasukkan dalam playbook

Playbook harus berisi langkah-langkah teknis yang akan dijalankan oleh analis keamanan untuk menyelidiki dan merespons insiden keamanan potensial secara memadai.

Item yang akan disertakan dalam playbook meliputi:

- Gambaran umum playbook – Skenario risiko atau insiden apa yang ditangani oleh playbook ini? Apa tujuan dari playbook ini?
- Prasyarat – Log dan mekanisme deteksi apa yang diperlukan untuk skenario insiden ini? Apa notifikasi yang diharapkan?
- Informasi pemangku kepentingan – Siapa yang terlibat dan apa informasi kontak mereka? Apa saja tanggung jawab setiap pemangku kepentingan?
- Langkah respons – Di seluruh fase respons insiden, langkah taktis apa yang perlu diambil? Kueri apa yang perlu dijalankan analis? Kode apa yang perlu dijalankan untuk mencapai hasil yang diinginkan?
  - Deteksi – Bagaimana insiden tersebut akan terdeteksi?
  - Analisis – Bagaimana cakupan dampak akan ditentukan?
  - Tahan – Bagaimana insiden akan diisolasi untuk membatasi cakupan?
  - Berantas – Bagaimana ancaman akan dihilangkan dari lingkungan?
  - Pulihkan – Bagaimana sistem atau sumber daya yang terpengaruh akan dibawa kembali ke produksi?
- Hasil yang diharapkan – Setelah kueri dan kode dijalankan, apa hasil yang diharapkan dari playbook tersebut?

Untuk memverifikasi informasi yang konsisten di setiap playbook, sebaiknya buat templat playbook yang dapat digunakan di seluruh playbook keamanan Anda yang lainnya. Beberapa item yang sudah terdaftar, seperti informasi pemangku kepentingan, dapat digunakan di beberapa playbook. Jika demikian, Anda dapat membuat dokumentasi terpusat untuk informasi tersebut dan merujuknya di dalam playbook, lalu menyebutkan perbedaan eksplisitnya di dalam playbook. Dengan begitu, Anda tidak perlu memperbarui informasi yang sama di setiap playbook Anda. Dengan membuat templat dan mengidentifikasi informasi umum atau bersama di playbook, Anda dapat menyederhanakan dan mempercepat pengembangan playbook. Terakhir, playbook Anda kemungkinan akan berkembang seiring waktu; setelah Anda memastikan bahwa langkah-langkahnya konsisten, hal ini membentuk persyaratan untuk otomatisasi.

Contoh playbook

Sejumlah contoh playbook dapat ditemukan di Lampiran B di the section called “Sumber daya playbook”. Contoh-contoh di sini dapat digunakan sebagai referensi Anda untuk playbook apa yang perlu dibuat dan apa yang perlu disertakan dalam playbook Anda. Namun, penting bagi Anda untuk membuat playbook yang menggabungkan risiko yang paling relevan dengan bisnis Anda. Anda perlu memverifikasi bahwa langkah-langkah dan alur kerja dalam playbook Anda mencakup teknologi dan proses Anda.

Menjalankan simulasi reguler

Organisasi tumbuh dan berkembang dari waktu ke waktu, begitu pun halnya dengan ancaman. Karena itu, penting bagi Anda untuk terus meninjau kemampuan respons insiden Anda. Simulasi adalah salah satu metode yang dapat digunakan untuk melakukan penilaian ini. Simulasi menggunakan skenario peristiwa keamanan dunia nyata yang dirancang untuk meniru taktik, teknik, dan prosedur aktor ancaman (TTPs) dan memungkinkan organisasi untuk melatih dan mengevaluasi kemampuan respons insiden mereka dengan menanggapi peristiwa cyber tiruan ini karena mungkin terjadi dalam kenyataan.

Simulasi memiliki berbagai manfaat, termasuk:

- Memvalidasi kesiapan siber dan mengembangkan kepercayaan diri responden insiden Anda.
- Menguji akurasi dan efisiensi alat serta alur kerja.
- Menyempurnakan metode komunikasi dan eskalasi yang selaras dengan rencana respons insiden Anda.
- Memberikan kesempatan untuk merespons vektor yang kurang umum.

Jenis simulasi

Ada tiga jenis simulasi utama:

- Latihan meja – Pendekatan latihan meja dalam simulasi adalah sesi berbasis diskusi yang melibatkan berbagai pemangku kepentingan respons insiden untuk mempraktikkan peran dan tanggung jawab serta menggunakan alat komunikasi dan playbook yang telah ditetapkan. Fasilitasi latihan biasanya dapat dilakukan dalam sehari penuh di tempat virtual, tempat fisik, atau kombinasi. Karena sifatnya yang berbasis diskusi, latihan meja berfokus pada proses, orang, dan kolaborasi. Teknologi adalah bagian integral dari diskusi; tetapi, latihan meja umumnya tidak menggunakan alat atau skrip respons insiden yang sebenarnya.

- Latihan Tim Ungu – Latihan Tim Ungu meningkatkan level kolaborasi antara tim responden insiden (Tim Biru) dan tim aktor ancaman simulasi (Tim Merah). Tim Biru umumnya terdiri dari anggota Security Operations Center (SOC), tetapi juga dapat mencakup pemangku kepentingan lain yang akan terlibat dalam peristiwa siber yang sebenarnya. Tim Merah umumnya terdiri dari tim uji penetrasi atau pemangku kepentingan utama yang dilatih dalam keamanan ofensif. Tim Merah bekerja secara kolaboratif dengan fasilitator latihan dalam merancang skenario yang akurat dan memungkinkan. Selama latihan Tim Ungu, fokus utamanya adalah pada mekanisme deteksi, alat, dan prosedur operasi standar (SOPs) yang mendukung upaya respons insiden.
- Latihan Tim Merah – Dalam latihan Tim Merah, penyerang (Tim Merah) melakukan simulasi untuk mencapai tujuan tertentu atau serangkaian tujuan dari cakupan yang telah ditentukan sebelumnya. Pembela (Tim Biru) belum tentu mengetahui ruang lingkup dan durasi latihan, yang memberikan penilaian yang lebih realistis tentang bagaimana mereka akan menanggapi insiden yang sebenarnya. Karena latihan Tim Merah dapat menjadi uji invasif, Anda harus berhati-hati dan menerapkan kontrol untuk memverifikasi bahwa latihan tersebut tidak menyebabkan kerusakan nyata pada lingkungan Anda.

> **Note**
>
> AWS mengharuskan pelanggan untuk meninjau kebijakan pengujian penetrasi yang tersedia di situs web Pengujian Penetrasi sebelum mereka melakukan latihan Tim Ungu atau Tim Merah.

Tabel 1 merangkum beberapa perbedaan utama dalam jenis simulasi ini. Penting untuk dicatat bahwa definisinya secara umum dianggap lentur dan dapat disesuaikan dengan kebutuhan organisasi Anda.

Tabel 1 — Jenis simulasi

	Latihan meja	Latihan Tim Ungu	Latihan Tim Merah
Ringkasan	Latihan berbasis kertas yang berfokus pada satu skenario insiden keamanan tertentu. Latihan ini dapat berupa latihan	Penawaran yang lebih realistis dibanding kan dengan latihan meja. Selama latihan Tim Ungu, fasilitat or bekerja secara	Penawaran simulasi yang umumnya lebih canggih. Biasanya ada informasi yang disamarkan, sehingga para peserta mungkin

	Latihan meja	Latihan Tim Ungu	Latihan Tim Merah
	tingkat tinggi atau teknis, dan dijalankan dengan serangkaian skenario tertulis.	kolaboratif dengan para peserta untuk meningkatkan keterlibatan latihan dan menawarkan pelatihan jika diperlukan.	tidak mengetahui semua detail latihan.
Sumber daya yang diperlukan	Diperlukan sumber daya teknis terbatas	Diperlukan berbagai pemangku kepentingan dan sumber daya teknis tingkat tinggi	Diperlukan berbagai pemangku kepentingan dan sumber daya teknis tingkat tinggi
Kompleksitas	Rendah	Sedang	Tinggi

Pertimbangkan untuk memfasilitasi simulasi siber secara reguler. Setiap jenis latihan dapat memberikan manfaat tersendiri bagi peserta dan organisasi secara keseluruhan, sehingga Anda dapat memilih untuk memulai dengan jenis simulasi yang kurang kompleks (seperti latihan meja) lalu beralih ke jenis simulasi yang lebih kompleks (latihan Tim Merah). Anda sebaiknya memilih jenis simulasi berdasarkan kematangan keamanan, sumber daya, dan hasil yang Anda inginkan. Beberapa pelanggan mungkin tidak memilih untuk melakukan latihan Tim Merah karena kompleksitas dan biayanya.

Siklus hidup latihan

Apa pun jenis simulasi yang Anda pilih, simulasi umumnya mengikuti langkah-langkah berikut:

1. Menentukan elemen latihan inti – Tentukan skenario simulasi dan tujuan simulasi. Dua hal ini harus disetujui oleh kepemimpinan.
2. Mengidentifikasi pemangku kepentingan utama – Latihan setidaknya membutuhkan fasilitator dan peserta latihan. Tergantung skenarionya, pemangku kepentingan tambahan seperti pimpinan dari departemen hukum, komunikasi, atau eksekutif dapat dilibatkan.
3. Membangun dan menguji skenario – Skenario mungkin perlu disesuaikan jika elemen tertentu tidak memungkinkan dalam pengembangannya. Tahap ini diharapkan menghasilkan skenario final.
4. Memfasilitasi simulasi – Jenis simulasi menentukan fasilitas yang digunakan (skenario tertulis atau skenario simulasi yang sangat teknis). Fasilitator harus menyelaraskan taktik fasilitasi mereka

dengan objek latihan dan harus sebisa mungkin melibatkan semua peserta latihan agar hasilnya bisa optimal.

5. Mengembangkan laporan setelah tindakan (AAR) – Identifikasi area yang berjalan dengan baik, area yang dapat ditingkatkan lagi, dan potensi kesenjangan. AAR harus mengukur efektivitas simulasi serta respons tim terhadap peristiwa simulasi agar kemajuan dapat dilacak dari waktu ke waktu dengan simulasi mendatang.

Teknologi

Jika Anda mengembangkan dan menerapkan teknologi yang tepat sebelum insiden keamanan, staf respons insiden Anda akan dapat menyelidiki, memahami ruang lingkup, dan mengambil tindakan tepat waktu.

Kembangkan struktur AWS akun

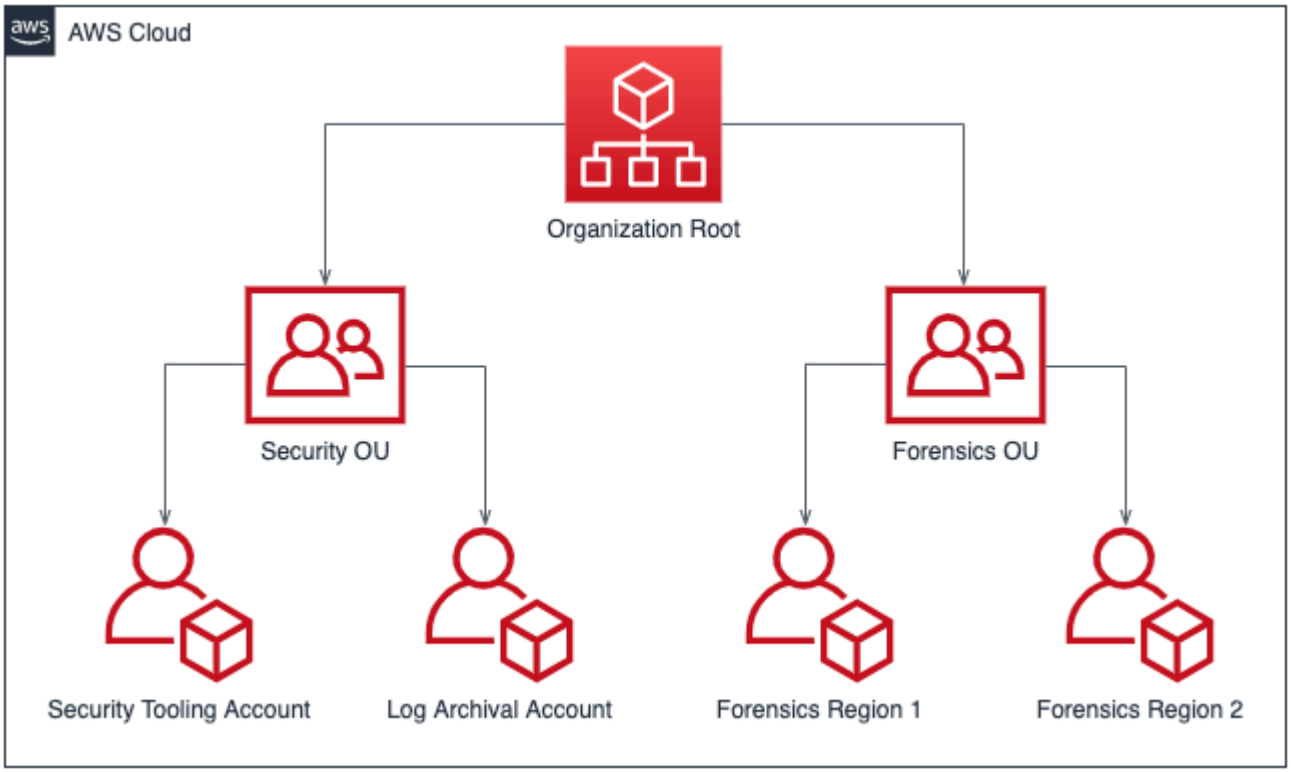
AWS Organizationsmembantu mengelola dan mengatur AWS lingkungan secara terpusat saat Anda tumbuh dan meningkatkan AWS sumber daya. AWS Organisasi mengkonsolidasikan AWS akun Anda sehingga Anda dapat mengelola mereka sebagai satu unit. Anda dapat menggunakan unit organisasi (OUs) untuk mengelompokkan akun bersama-sama untuk mengelola sebagai satu unit.

Untuk respons insiden, akan sangat membantu untuk memiliki struktur AWS akun yang mendukung fungsi respons insiden, yang mencakup OU keamanan dan OU forensik. Dalam unit organisasi keamanan, Anda harus memiliki akun untuk:

- Pengarsipan log – Menggabungkan log dalam akun AWS pengarsipan.
- Perkakas keamanan — Memusatkan layanan keamanan di akun alat AWS keamanan. Akun ini beroperasi sebagai administrator yang didelegasikan untuk layanan keamanan.

Dalam forensik unit organisasi, Anda memiliki opsi untuk menerapkan satu akun forensik atau akun-akun untuk setiap Wilayah tempat Anda beroperasi, bergantung pada mana yang paling sesuai untuk model bisnis dan operasional Anda. Untuk contoh pendekatan akun per Wilayah, jika Anda hanya beroperasi di AS Timur (Virginia Utara) (us-east-1) dan AS Barat (Oregon) (us-west-2), Anda akan memiliki dua akun di forensik unit organisasi: satu untuk us-east-1 dan satu untuk us-west-2. Karena penyediaan akun baru membutuhkan waktu, akun forensik harus dibuat dan digunakan jauh sebelum insiden, sehingga bisa siap digunakan oleh responden secara efektif ketika merespons insiden.

Diagram berikut menampilkan struktur akun sampel, termasuk unit organisasi forensik dengan akun forensik per Wilayah:



Struktur akun per wilayah untuk respons insiden

Mengembangkan dan menerapkan strategi pemberian tag

Memperoleh informasi kontekstual tentang kasus penggunaan bisnis dan pemangku kepentingan internal yang relevan di sekitar AWS sumber daya bisa jadi sulit. Salah satu cara untuk melakukannya adalah dalam bentuk tag, yang menetapkan metadata ke AWS sumber daya Anda dan terdiri dari kunci dan nilai yang ditentukan pengguna. Anda dapat menggunakan tag untuk mengelompokkan sumber daya berdasarkan tujuan, pemilik, lingkungan, jenis data yang diproses, dan kriteria lainnya yang Anda pilih.

Memiliki strategi penandaan yang konsisten dapat mempercepat waktu respons dengan memungkinkan Anda mengidentifikasi dan membedakan informasi kontekstual tentang sumber daya dengan cepat. AWS Tag juga dapat berfungsi sebagai mekanisme untuk memulai otomatisasi respons. Untuk informasi lebih lanjut tentang apa yang harus diberi tag, lihat dokumentasi tentang AWS sumber daya penandaan. Anda harus terlebih dahulu menentukan tag yang ingin Anda terapkan di organisasi Anda. Setelah itu, Anda akan menerapkan dan menegakkan strategi pemberian tag ini. Detail tentang implementasi dan penegakan dapat ditemukan di AWS blog Menerapkan strategi penandaan AWS sumber daya menggunakan Kebijakan AWS Tag dan Kebijakan Kontrol Layanan (SCPs).

Perbarui informasi kontak AWS akun

Untuk setiap AWS akun Anda, penting untuk memiliki informasi up-to-date kontak yang akurat sehingga pemangku kepentingan yang benar menerima pemberitahuan penting dari AWS topik seperti keamanan, penagihan, dan operasi. Untuk setiap AWS akun, Anda memiliki kontak utama dan kontak alternatif untuk keamanan, penagihan, dan operasi. Perbedaan antara kontak ini dapat ditemukan di Panduan Referensi Manajemen AWS Akun.

Untuk detail tentang mengelola kontak alternatif, lihat AWS dokumentasi tentang menambahkan, mengubah, atau menghapus kontak alternatif. Jika tim Anda mengelola penagihan, operasi, dan masalah terkait keamanan, penggunaan daftar distribusi email merupakan praktik terbaik. Dengan daftar distribusi email, ketergantungan pada satu orang bisa dihindari, karena hal ini dapat menyulitkan apabila orang tersebut sedang tidak di kantor atau sudah keluar dari perusahaan. Anda juga harus memverifikasi bahwa informasi kontak email dan akun, termasuk nomor telepon, terlindungi dengan baik untuk berjaga-jaga jika terjadi pengaturan ulang kata sandi akun root dan pengaturan ulang autentikasi multi-faktor (MFA).

Untuk pelanggan yang menggunakan AWS Organizations, administrator organisasi dapat secara terpusat mengelola kontak alternatif untuk akun anggota menggunakan akun manajemen atau akun administrator yang didelegasikan tanpa memerlukan kredensil untuk setiap akun. AWS Anda juga perlu memverifikasi bahwa akun yang baru dibuat memiliki informasi kontak yang akurat. Lihat Perbarui kontak alternatif secara otomatis untuk posting Akun AWS blog yang baru dibuat.

Siapkan akses ke Akun AWS

Selama insiden, tim respons insiden Anda harus memiliki akses ke lingkungan dan sumber daya yang terlibat dalam insiden tersebut. Pastikan tim Anda memiliki akses yang tepat untuk melakukan tugas mereka sebelum suatu peristiwa terjadi. Untuk melakukan itu, Anda harus tahu tingkat akses apa yang dibutuhkan anggota tim Anda (misalnya, jenis tindakan apa yang mungkin mereka ambil) dan harus memberikan akses hak istimewa paling sedikit terlebih dahulu.

Untuk menerapkan dan menyediakan akses ini, Anda harus mengidentifikasi dan mendiskusikan strategi akun AWS dan strategi identitas cloud dengan arsitek cloud organisasi Anda untuk memahami metode autentikasi dan otorisasi yang dikonfigurasi. Karena kredensial ini bersifat istimewa, Anda sebaiknya mempertimbangkan untuk menggunakan alur persetujuan atau mengambil kredensial dari brankas sebagai bagian dari implementasi Anda. Setelah implementasi, Anda perlu mendokumentasikan dan menguji akses anggota tim dengan baik sebelum peristiwa terjadi untuk memastikan mereka dapat merespons tanpa penundaan.

Terakhir, pengguna yang dibuat khusus untuk merespons insiden keamanan sering kali diberi hak istimewa agar dapat memiliki akses yang memadai. Oleh karena itu, penggunaan kredensial ini harus dibatasi, dipantau, dan tidak digunakan untuk kegiatan sehari-hari.

Memahami lanskap ancaman

Mengembangkan model ancaman

Dengan mengembangkan model ancaman, organisasi dapat mengidentifikasi ancaman dan mitigasi sebelum pengguna yang tidak sah dapat melakukannya. Ada sejumlah strategi dan pendekatan untuk pemodelan ancaman; lihat posting blog How to approach threat modeling. Untuk respons insiden, model ancaman dapat membantu mengidentifikasi vektor serangan yang mungkin digunakan aktor ancaman dalam insiden. Memahami apa yang Anda pertahankan akan sangat penting agar dapat merespons dengan segera. Anda juga dapat menggunakan pemodelan ancaman. AWS Partner Untuk mencari AWS pasangan, gunakan AWS Partner Network.

Mengintegrasikan dan menggunakan intelijen ancaman siber

Intelijen ancaman siber adalah data dan analisis intensi, peluang, dan kemampuan aktor ancaman. Memperoleh dan menggunakan intelijen ancaman sangat membantu untuk mendeteksi insiden sejak dini dan memahami perilaku aktor ancaman dengan lebih baik. Intelijen ancaman siber mencakup indikator statis seperti alamat IP atau hash file malware. Hal ini juga mencakup informasi tingkat tinggi, seperti pola perilaku dan intensi. Anda dapat mengumpulkan intelijen ancaman dari sejumlah vendor keamanan siber dan dari repositori sumber terbuka.

Untuk mengintegrasikan dan memaksimalkan kecerdasan ancaman untuk AWS lingkungan Anda, Anda dapat menggunakan beberapa out-of-the-box kemampuan dan mengintegrasikan daftar intelijen ancaman Anda sendiri. Amazon GuardDuty menggunakan sumber intelijen ancaman AWS internal dan pihak ketiga. AWS Layanan lain, seperti firewall dan AWS WAF aturan DNS, juga mengambil masukan dari AWS'kelompok intelijen ancaman canggih. Beberapa GuardDuty temuan dipetakan ke MITRE ATT&CK Framework, yang memberikan informasi tentang pengamatan dunia nyata tentang taktik dan teknik musuh.

Memilih dan mengatur log untuk analisis dan peringatan

Selama penyelidikan keamanan, Anda harus dapat meninjau log yang relevan untuk mencatat dan memahami cakupan serta garis waktu lengkap insiden tersebut. Log juga diperlukan untuk pembuatan peringatan, yang menunjukkan terjadinya tindakan tertentu yang menarik. Sangat penting untuk memilih, mengaktifkan, menyimpan, serta mengatur mekanisme kueri dan pengambilan,

serta mengatur peringatan. Setiap tindakan ini ditinjau di bagian ini. Untuk detail selengkapnya, lihat posting AWS blog Strategi pencatatan untuk respons insiden keamanan.

Memilih dan mengaktifkan sumber log

Sebelum penyelidikan keamanan, Anda perlu menangkap log yang relevan untuk merekonstruksi aktivitas secara surut di akun. AWS Pilih dan aktifkan sumber log yang relevan dengan beban kerja AWS akun mereka.

AWS CloudTrail adalah layanan logging yang melacak panggilan API yang dilakukan terhadap aktivitas AWS layanan pengambilan AWS akun. Ini diaktifkan secara default dengan retensi 90 hari peristiwa manajemen yang dapat diambil melalui CloudTrail fasilitas Riwayat Acara menggunakan AWS Management Console, AWS CLI, atau SDK. AWS Untuk retensi dan visibilitas peristiwa data yang lebih lama, Anda perlu membuat CloudTrail Trail dan dikaitkan dengan bucket Amazon S3, dan secara opsional, dengan CloudWatch grup log. Atau, Anda dapat membuat CloudTrail Danau, yang menyimpan CloudTrail log hingga tujuh tahun dan menyediakan fasilitas kueri berbasis SQL.

AWS merekomendasikan agar pelanggan yang menggunakan VPC mengaktifkan lalu lintas jaringan dan log DNS masing-masing menggunakan Log Aliran VPC dan log kueri penyelesai Amazon Route 53, mengalirkannya ke bucket Amazon S3 atau grup log. CloudWatch Anda dapat membuat log alur VPC untuk VPC, subnet, atau antarmuka jaringan. Untuk Log Alur VPC, Anda dapat bersikap selektif tentang bagaimana dan di mana Anda mengaktifkan Log Alur untuk mengurangi biaya.

AWS CloudTrail Log, Log Aliran VPC, dan log kueri resolver Route 53 adalah trifecta logging dasar untuk mendukung penyelidikan keamanan. AWS

AWS layanan dapat menghasilkan log yang tidak ditangkap oleh trifecta logging dasar, seperti log Elastic Load Balancing AWS WAF , log, log perekam, temuan Amazon AWS Config , log audit GuardDuty Amazon Elastic Kubernetes Service (Amazon EKS), EC2 dan sistem operasi instans Amazon dan log aplikasi. Lihat daftar lengkap opsi pencatatan log dan pemantauan di the section called “Lampiran A: Definisi kemampuan cloud”.

Memilih penyimpanan log

Pilihan penyimpanan log umumnya terkait dengan alat kueri yang Anda gunakan, kemampuan retensi, pemahaman, dan biaya. Saat Anda mengaktifkan log AWS layanan, sediakan fasilitas penyimpanan; biasanya bucket atau grup CloudWatch log Amazon S3.

Bucket Amazon S3 menyediakan penyimpanan tahan lama yang hemat biaya dengan kebijakan siklus hidup opsional. Log yang disimpan di bucket Amazon S3 dapat dikueri secara native

menggunakan layanan seperti Amazon Athena. Grup CloudWatch log menyediakan penyimpanan yang tahan lama dan fasilitas kueri bawaan melalui Wawasan CloudWatch Log.

Mengidentifikasi retensi log yang sesuai

Saat Anda menggunakan bucket S3 atau grup CloudWatch log untuk menyimpan log, Anda harus menetapkan siklus hidup yang memadai untuk setiap sumber log guna mengoptimalkan biaya penyimpanan dan pengambilan. Pelanggan umumnya memiliki antara 3 dan 12 bulan log yang tersedia untuk kueri, dengan retensi hingga tujuh tahun. Pilihan ketersediaan dan retensi harus selaras dengan persyaratan keamanan Anda serta gabungan mandat hukum, peraturan, dan bisnis.

Memilih dan menerapkan mekanisme kueri untuk log

Di AWS, layanan utama yang dapat Anda gunakan untuk menanyakan CloudWatch log adalah Wawasan Log untuk data yang disimpan dalam grup CloudWatch log, serta Amazon Athena dan Layanan OpenSearch Amazon untuk data yang disimpan di Amazon S3. Anda juga dapat menggunakan alat kueri pihak ketiga seperti informasi keamanan dan manajemen peristiwa (SIEM).

Proses untuk memilih alat kueri log harus mempertimbangkan aspek orang, proses, dan teknologi dalam operasi keamanan Anda. Pilih alat yang memenuhi persyaratan operasional, bisnis, dan keamanan, serta dapat diakses dan dipelihara dalam jangka panjang. Perlu diingat bahwa alat kueri log bekerja secara optimal ketika jumlah log yang akan dipindai tidak melebihi batas alat. Tidak jarang pelanggan memiliki beberapa alat kueri karena kendala biaya atau teknis. Misalnya, pelanggan mungkin menggunakan SIEM pihak ketiga untuk melakukan kueri data selama 90 hari terakhir, dan menggunakan Athena untuk melakukan kueri melebihi 90 hari karena biaya penyerapan log SIEM. Apa pun implementasinya, verifikasi bahwa pendekatan Anda meminimalkan jumlah alat yang diperlukan untuk memaksimalkan efisiensi operasional, terutama selama penyelidikan peristiwa keamanan.

Menggunakan log untuk peringatan

AWS secara native memberikan peringatan melalui layanan keamanan, seperti Amazon, GuardDuty AWS Security Hub, dan. AWS Config Anda juga dapat menggunakan mesin pembuat peringatan kustom untuk peringatan keamanan yang tidak tercakup oleh layanan ini atau untuk peringatan spesifik yang relevan dengan lingkungan Anda. Membangun peringatan dan deteksi ini tercakup dalam bagian bernama the section called “Deteksi” dalam dokumen ini.

Mengembangkan kemampuan forensik

Menjelang insiden keamanan, pertimbangkan untuk mengembangkan kemampuan forensik guna mendukung investigasi peristiwa keamanan. Guide to Integrating Forensic Techniques into Incident Response dari NIST menyediakan panduan tersebut.

Forensik pada AWS

Konsep dari forensik lokal tradisional berlaku untuk. AWSStrategi lingkungan investigasi forensik dalam posting AWS Cloud blog memberi Anda informasi penting untuk mulai memigrasikan keahlian forensik mereka ke. AWS

Setelah lingkungan dan struktur AWS akun Anda disiapkan untuk forensik, Anda akan ingin menentukan teknologi yang diperlukan untuk secara efektif melakukan metodologi forensik yang sehat di empat fase:

- Koleksi — Kumpulkan AWS log yang relevan, seperti AWS CloudTrail, AWS Config, Log Aliran VPC, dan log tingkat host. Kumpulkan snapshot, backup, dan dump memori dari sumber daya yang terkena dampak. AWS
- Pemeriksaan – Memeriksa data yang dikumpulkan dengan mengekstraksi dan menilai informasi yang relevan.
- Analisis – Menganalisis data yang dikumpulkan untuk memahami insiden dan menarik kesimpulan dari insiden tersebut.
- Pelaporan – Menyajikan informasi yang dihasilkan dari fase analisis.

Menangkap cadangan dan snapshot

Menyiapkan cadangan sistem kunci dan basis data sangat penting untuk pemulihan dari insiden keamanan dan untuk tujuan forensik. Dengan memiliki cadangan, Anda dapat memulihkan sistem Anda ke keadaan aman sebelumnya. Pada AWS, Anda dapat mengambil snapshot dari berbagai sumber daya. Snapshot memberi Anda point-in-time cadangan sumber daya tersebut. Ada banyak layanan AWS yang dapat mendukung Anda dalam pencadangan dan pemulihan. Lihat Panduan Preskriptif Pencadangan dan Pemulihan untuk detail tentang layanan ini dan pendekatan untuk pencadangan dan pemulihan. Untuk detail selengkapnya, lihat posting blog Use backups to recover from security incidents.

Terutama ketika berhubungan dengan situasi seperti ransomware, sangat penting agar cadangan Anda dilindungi dengan baik. Lihat 10 praktik terbaik keamanan teratas untuk mengamankan cadangan di posting AWS blog untuk panduan mengamankan cadangan Anda. Selain mengamankan

cadangan, Anda juga sebaiknya menguji proses pencadangan dan pemulihan Anda secara teratur untuk memverifikasi bahwa teknologi dan proses yang Anda miliki berfungsi sesuai harapan.

Otomatisasi forensik pada AWS

Ketika terjadi peristiwa keamanan, tim respons insiden Anda harus dapat mengumpulkan dan menganalisis bukti dengan cepat sambil mempertahankan akurasi untuk periode waktu yang mengitari peristiwa tersebut. Mengumpulkan bukti yang relevan di lingkungan cloud, terutama di sejumlah besar contoh dan akun secara manual merupakan hal yang menyulitkan sekaligus memakan waktu bagi tim respons insiden. Selain itu, kesalahan manusia rentan terjadi dalam pengumpulan secara manual. Untuk alasan ini, pelanggan harus mengembangkan dan menerapkan otomatisasi untuk forensik.

AWS menawarkan sejumlah sumber daya otomatisasi untuk forensik, yang dikonsolidasikan dalam Lampiran di bawah. the section called “Sumber daya forensik” Sumber daya ini adalah contoh pola forensik yang telah kami kembangkan dan telah diterapkan pelanggan. Meskipun sumber daya ini mungkin merupakan arsitektur referensi yang berguna untuk memulai, pertimbangkan untuk memodifikasinya atau membuat pola otomatisasi forensik baru berdasarkan lingkungan, persyaratan, alat, dan proses forensik Anda.

Ringkasan item persiapan

Persiapan menyeluruh untuk merespons peristiwa keamanan sangat penting agar respons insiden bisa dilakukan tepat waktu dan efektif. Persiapan respons insiden melibatkan orang, proses, dan teknologi. Ketiga domain ini sama pentingnya dalam persiapan. Anda harus mempersiapkan dan mengembangkan program respons insiden Anda di ketiga domain tersebut.

Tabel 2 merangkum item persiapan yang dijabarkan dalam bagian ini.

Tabel 2 – Item persiapan respons insiden

Domain	Item persiapan	Item tindakan
Orang	Menentukan peran dan tanggung jawab.	• Mengidentifikasi pemangku kepentingan respons insiden yang relevan. • Mengembangkan bagan yang bertanggung jawab, akuntabel, terinformasi,

Domain	Item persiapan	Item tindakan
		berdasarkan konsultasi (RACI) untuk suatu insiden.
Orang	Latih staf respons insiden di AWS.	• Melatih pemangku kepentingan respons insiden di AWS yayasan. • Melatih pemangku kepentingan respons insiden pada layanan AWS keamanan dan pemantaua n. • Latih pemangku kepenting an respons insiden di AWS lingkungan Anda dan bagaimana hal itu dirancang .
Orang	Memahami opsi AWS dukungan.	• Memahami perbedaan AWS dukungan, Tim Respons Insiden Pelanggan (CIRT), tim respons DDo S (DRT) dan AMS. • Memahami jalur triase dan eskalasi untuk mencapai CIRT selama acara keamanan aktif jika diperlukan.

Domain	Item persiapan	Item tindakan
Proses	Mengembangkan rencana respons insiden.	• Buat dokumen tingkat tinggi yang mendefini sikan program dan strategi respons insiden Anda. • Sertakan RACI, rencana komunikasi, definisi insiden, dan fase respons insiden dalam rencana respons insiden.
Proses	Mendokumentasikan dan memusatkan diagram arsitektu r.	• Dokumentasikan detail tentang bagaimana AWS lingkungan Anda dikonfigu rasi di seluruh struktur akun, penggunaan layanan, pola IAM, dan fungsionalitas inti lainnya ke konfigurasi Anda AWS . • Mengembangkan diagram arsitektur untuk arsitektur cloud Anda.
Proses	Mengembangkan playbook respons insiden.	• Buat template untuk struktur buku pedoman Anda. • Membuat playbook untuk peristiwa keamanan yang diharapkan. • Buat buku pedoman untuk peringatan keamanan yang diketahui, seperti GuardDuty temuan.

Domain	Item persiapan	Item tindakan
Proses	Menjalankan simulasi reguler.	• Mengembangkan jadwal reguler untuk menjalankan simulasi insiden. • Menggunakan output dan pelajaran yang didapatkan untuk mengiterasi program respons insiden Anda.
Teknologi	Kembangkan struktur AWS akun.	• Rencanakan struktur akun untuk bagaimana beban kerja dipisahkan oleh AWS akun. • Membuat unit organisasi keamanan dengan alat keamanan dan akun pengarsipan log. • Membuat unit organisasi forensik dengan akun forensik untuk setiap Wilayah tempat Anda beroperasi.
Teknologi	Mengembangkan dan menerapkan strategi pemberian tag yang membantu responden untuk mengidentifikasi kepemilikan dan konteks temuan.	• Rencanakan strategi untuk menandai dan tag apa yang Anda inginkan terkait dengan AWS sumber daya Anda. • Menerapkan dan menegakkan strategi pemberian tag.

Domain	Item persiapan	Item tindakan
Teknologi	Perbarui informasi kontak AWS akun.	• Verifikasi bahwa AWS akun memiliki informasi kontak yang terdaftar. • Membuat daftar distribusi email untuk informasi kontak untuk menghapus satu titik kegagalan. • Lindungi akun email yang terkait dengan informasi AWS akun.
Teknologi	Siapkan akses ke AWS akun.	• Menentukan apa yang diperlukan oleh responden akses insiden untuk merespons suatu insiden. • Melaksanakan, menguji, dan memantau akses.
Teknologi	Memahami lanskap ancaman.	• Mengembangkan model ancaman untuk lingkungan dan aplikasi Anda. • Mengintegrasikan dan menggunakan intelijen ancaman siber.

Domain	Item persiapan	Item tindakan
Teknologi	Memilih dan mengatur log.	• Mengidentifikasi dan mengaktifkan log untuk penyelidikan. • Memilih penyimpanan log. • Mengidentifikasi dan menerapkan retensi log. • Mengembangkan mekanisme untuk mengambil dan query log dan artefak. • Menggunakan log untuk peringatan.
Teknologi	Mengembangkan kemampuan forensik.	• Mengidentifikasi artefak yang diperlukan untuk pengumpulan forensik. • Menangkap dan mengamankan cadangan sistem kunci. • Menentukan mekanisme untuk analisis log dan artefak yang diidentifikasi. • Menerapkan otomatisasi untuk analisis forensik.

Pendekatan berulang direkomendasikan untuk persiapan respons insiden. Semua item persiapan ini tidak dapat dilakukan dalam waktu singkat; Anda harus membuat rencana untuk memulai dari yang kecil dan terus meningkatkan kemampuan respons insiden Anda dari waktu ke waktu.

Operasi

Operasi adalah hal inti dalam melakukan respons insiden. Di sinilah tindakan merespons dan meremediasi insiden keamanan terjadi. Operasi meliputi lima fase berikut: deteksi, analisis,

penahanan, pemberantasan, dan pemulihan. Deskripsi fase dan tujuan ini dapat ditemukan pada Tabel 3.

Tabel 3 – Fase operasi

Fase	Tujuan
Deteksi	Mengidentifikasi peristiwa keamanan potensial.
Analisis	Tentukan apakah peristiwa keamanan adalah insiden dan menilai ruang lingkup insiden tersebut.
Penahanan	Meminimalkan dan membatasi cakupan peristiwa keamanan.
Pemberantasan	Menghapus sumber daya atau artefak tidak sah yang terkait dengan peristiwa keamanan. Menerapkan mitigasi yang menyebabkan insiden keamanan tersebut.
Pemulihan	Kembalikan sistem ke keadaan aman yang diketahui dan pantau sistem ini untuk memverifikasi bahwa ancaman tidak kembali.

Fase-fase ini akan berfungsi sebagai panduan ketika Anda merespons dan beroperasi pada insiden keamanan untuk merespons dengan cara yang efektif dan kuat. Tindakan aktual yang Anda ambil akan bervariasi, tergantung insiden Anda. Insiden yang melibatkan ransomware, misalnya, akan memiliki serangkaian langkah respons yang berbeda untuk diikuti dibandingkan insiden yang melibatkan bucket Amazon S3 publik. Selain itu, fase-fase ini tidak selalu terjadi secara berurutan. Setelah penahanan dan pemberantasan, Anda mungkin perlu kembali ke analisis untuk mengetahui apakah tindakan Anda efektif.

Deteksi

Peringatan adalah komponen utama dari fase deteksi. Ini menghasilkan pemberitahuan untuk memulai proses respons insiden berdasarkan aktivitas AWS akun yang menarik.

Akurasi peringatan merupakan hal yang menantang; terjadinya, berlangsungnya, atau akan terjadinya suatu insiden tidak selalu dapat ditentukan dengan pasti. Berikut ini beberapa alasannya:

- Mekanisme deteksi didasarkan pada simpangan dasar, pola yang diketahui, dan pemberitahuan dari entitas internal atau eksternal.
- Karena sifat teknologi dan manusia yang tidak dapat diprediksi, yaitu cara dan aktor insiden keamanan, garis dasar berubah seiring waktu. Pola nakal muncul melalui taktik, teknik, dan prosedur aktor ancaman baru atau yang dimodifikasi ()TTPs.
- Perubahan pada orang, teknologi, dan proses tidak segera dimasukkan ke dalam proses respons insiden. Sebagian di antaranya ditemukan dalam proses penyelidikan.

Sumber peringatan

Anda sebaiknya mempertimbangkan sumber berikut untuk menentukan peringatan:

- Temuan — AWS layanan seperti Amazon GuardDuty, Amazon Macie AWS Security Hub, Amazon Inspector,, IAM Access Analyzer AWS Config, dan Network Access Analyzer menghasilkan temuan yang dapat digunakan untuk membuat peringatan.
- Log — log AWS layanan, infrastruktur, dan aplikasi yang disimpan di bucket Amazon S3 dan grup CloudWatch log dapat diuraikan dan dikorelasikan untuk menghasilkan peringatan.
- Aktivitas penagihan – Perubahan mendadak dalam aktivitas penagihan dapat mengindikasikan adanya peristiwa keamanan. Ikuti dokumentasi tentang Membuat alarm penagihan untuk memantau perkiraan AWS biaya Anda untuk memantau hal ini.
- Intelijen ancaman siber – Jika Anda berlangganan feed intelijen ancaman siber pihak ketiga, Anda dapat menghubungkan informasi tersebut dengan alat pencatatan dan pemantauan lainnya untuk mengidentifikasi indikator potensial peristiwa.
- Alat partner – Partner di AWS Partner Network (APN) menawarkan produk unggulan yang dapat membantu Anda memenuhi tujuan keamanan Anda. Untuk respons insiden, produk partner dengan deteksi dan respons titik akhir (EDR) atau SIEM dapat membantu mendukung tujuan respons insiden Anda. Untuk informasi selengkapnya, lihat Solusi Partner Keamanan dan Solusi Keamanan di AWS Marketplace.
- AWS kepercayaan dan keamanan — Dukungan dapat menghubungi pelanggan jika kami mengidentifikasi aktivitas yang kasar atau berbahaya.
- Sekali kontak – Karena sesuatu yang tidak biasa mungkin saja diperhatikan oleh pelanggan, developer, atau staf lain di organisasi Anda, penting agar Anda memiliki metode yang dikenali dan dipublikasikan dengan baik untuk menghubungi tim keamanan Anda. Pilihan populer

termasuk sistem tiket, alamat email kontak, dan formulir web. Jika organisasi Anda bekerja dengan masyarakat umum, Anda mungkin juga memerlukan mekanisme kontak keamanan yang digunakan publik.

Untuk informasi selengkapnya tentang kemampuan cloud yang dapat Anda gunakan selama penyelidikan, lihat the section called “Lampiran A: Definisi kemampuan cloud” di dokumen ini.

Deteksi sebagai bagian dari rekayasa kontrol keamanan

Mekanisme deteksi merupakan bagian integral dari pengembangan kontrol keamanan. Ketika kontrol direktif dan pencegahan ditentukan, kontrol detektif dan responsif terkait harus dibangun. Sebagai contoh, sebuah organisasi menetapkan kontrol direktif yang terkait dengan pengguna root AWS akun, yang seharusnya hanya digunakan untuk aktivitas spesifik dan sangat terdefinisi dengan baik. Mereka mengaitkannya dengan kontrol preventif yang diterapkan dengan menggunakan kebijakan kontrol layanan AWS organisasi (SCP). Jika aktivitas pengguna root di luar baseline yang diharapkan terjadi, kontrol detektif yang diterapkan dengan EventBridge aturan dan topik SNS akan memperingatkan pusat operasi keamanan (SOC). Dalam kontrol responsif, SOC memilih playbook yang sesuai, melakukan analisis, dan bekerja sampai insiden terselesaikan.

Kontrol keamanan paling baik ditentukan oleh pemodelan ancaman beban kerja yang berjalan di AWS. Tingkat kekritisan kontrol detektif akan ditetapkan dengan melihat analisis dampak bisnis (BIA) untuk beban kerja tertentu. Peringatan yang dihasilkan oleh kontrol detektif tidak ditangani saat masuk, melainkan berdasarkan kekritisan awalnya, untuk disesuaikan selama analisis. Set kekritisan awal adalah bantuan untuk menentukan prioritas; konteks terjadinya peringatan akan menentukan kekritisan yang sebenarnya. Sebagai contoh, sebuah organisasi menggunakan Amazon GuardDuty sebagai komponen kontrol detektif yang digunakan untuk EC2 instance yang merupakan bagian dari beban kerja. Temuan `Impact:EC2/SuspiciousDomainRequest.Reputation` ini dibuat, menginformasikan bahwa EC2 instans Amazon yang terdaftar dalam beban kerja Anda menanyakan nama domain yang diduga berbahaya. Peringatan ini ditetapkan secara default sebagai tingkat keparahan rendah, dan ketika fase analisis berlangsung, ditentukan bahwa beberapa ratus EC2 contoh tipe `p4d.24xlarge` telah digunakan oleh aktor yang tidak sah, secara signifikan meningkatkan biaya operasi organisasi. Pada titik ini, tim respons insiden membuat keputusan untuk menyesuaikan kekritisan peringatan ini menjadi tinggi, meningkatkan rasa urgensi dan mempercepat tindakan lebih lanjut. Perhatikan bahwa tingkat keparahan GuardDuty temuan tidak dapat diubah.

Menerapkan kontrol detektif

Penting untuk memahami bagaimana kontrol detektif diterapkan karena kontrol tersebut membantu menentukan bagaimana peringatan akan digunakan untuk peristiwa tertentu. Ada dua implementasi utama untuk kontrol detektif teknis:

- Deteksi perilaku bergantung pada model matematika yang biasa disebut sebagai machine learning (ML) atau kecerdasan buatan (AI). Deteksi dilakukan dengan inferensi; oleh karena itu, peringatan mungkin tidak mencerminkan peristiwa yang sebenarnya.
- Deteksi berbasis aturan bersifat deterministik; pelanggan dapat mengatur parameter yang tepat dari aktivitas apa yang akan memunculkan peringatan, dan itu bersifat pasti.

Implementasi modern sistem detektif, seperti sistem deteksi intrusi (IDS), umumnya memiliki dengan kedua mekanisme tersebut. Berikut adalah beberapa contoh untuk deteksi berbasis aturan dan perilaku dengan. GuardDuty

- Ketika temuan `Exfiltration:IAMUser/AnomalousBehavior` dibuat, temuan tersebut menginformasikan bahwa “terdapat permintaan API anomali di akun Anda”. Saat Anda melihat lebih jauh ke dalam dokumentasi, ini memberi tahu Anda bahwa “Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh,” yang menunjukkan bahwa temuan ini bersifat perilaku.
- Untuk temuan GuardDuty ini`Impact:S3/MaliciousIPCaller`, menganalisis panggilan API dari layanan Amazon S3 di CloudTrail, membandingkan elemen `SourceIPAddress` log dengan tabel alamat IP publik yang mencakup umpan intelijen ancaman. Setelah menemukan kecocokan langsung dengan sebuah entri, temuan akan dihasilkan.

Kami merekomendasikan untuk menerapkan campuran peringatan berbasis perilaku dan aturan, karena menerapkan peringatan berbasis aturan untuk setiap aktivitas dalam model ancaman Anda bukanlah hal yang selalu memungkinkan.

Deteksi berbasis orang

Pada titik ini, kita telah membahas deteksi berbasis teknologi. Sumber deteksi penting lainnya berasal dari orang-orang di dalam atau di luar organisasi pelanggan. Orang dalam dapat didefinisikan sebagai karyawan atau kontraktor, dan orang luar adalah entitas seperti peneliti keamanan, penegak hukum, berita, dan media sosial.

Meskipun deteksi berbasis teknologi dapat dikonfigurasi secara sistematis, deteksi berbasis orang datang dalam berbagai bentuk seperti email, tiket, surat, kiriman berita, panggilan telepon, dan interaksi langsung. Notifikasi deteksi berbasis teknologi dapat diharapkan untuk dikirimkan secara hampir waktu nyata, tetapi deteksi berbasis orang tidak memiliki jadwal yang bisa diacu secara pasti. Sangat penting bahwa budaya keamanan menggabungkan, memfasilitasi, dan memberdayakan mekanisme deteksi berbasis orang untuk pendekatan pertahanan yang mendalam terhadap keamanan.

Ringkasan

Dengan deteksi, penting untuk memiliki campuran peringatan berbasis aturan dan perilaku. Selain itu, Anda harus memiliki mekanisme untuk orang, baik secara internal maupun eksternal, untuk mengirimkan tiket tentang masalah keamanan. Manusia dapat menjadi salah satu sumber paling berharga untuk peristiwa keamanan, jadi penting untuk memiliki proses bagi orang untuk mengeskalasikan kekhawatirannya. Anda sebaiknya menggunakan model ancaman lingkungan Anda untuk mulai membangun deteksi. Model ancaman akan membantu Anda membangun peringatan berdasarkan ancaman yang paling relevan dengan lingkungan Anda. Terakhir, Anda dapat menggunakan kerangka kerja seperti MITRE ATT&CK untuk memahami taktik, teknik, dan prosedur aktor ancaman (). TTPs Kerangka kerja MITRE ATT&CK dapat membantu untuk digunakan sebagai bahasa umum di berbagai mekanisme deteksi Anda.

Analisis

Log, kemampuan kueri, dan intelijen ancaman adalah beberapa komponen pendukung yang dibutuhkan oleh fase analisis. Banyak log yang digunakan untuk deteksi juga digunakan untuk analisis, dan akan memerlukan orientasi dan konfigurasi alat kueri.

Memvalidasi, menentukan cakupan, dan menilai dampak peringatan

Selama fase analisis, analisis log komprehensif dilakukan dengan tujuan untuk memvalidasi peringatan, menentukan ruang lingkup, dan menilai dampak dari kemungkinan kompromi.

- Validasi peringatan adalah titik masuk fase analisis. Responden insiden akan mencari entri log dari berbagai sumber dan langsung terlibat dengan pemilik beban kerja yang terdampak.
- Pencakupan adalah langkah berikutnya, ketika semua sumber daya yang terlibat diinventarisasi dan kekritisan peringatan disesuaikan setelah pemangku kepentingan setuju bahwa peringatan tersebut tidak mungkin bersifat positif palsu.
- Terakhir, analisis dampak memerinci gangguan yang sebenarnya pada bisnis.

Setelah komponen beban kerja yang terpengaruh diidentifikasi, hasil pencakupan dapat dikorelasikan dengan sasaran titik pemulihan (RPO) beban kerja terkait dan sasaran waktu pemulihan (RTO), menyesuaikan tingkat kekritisan peringatan, yang akan memulai alokasi sumber daya dan semua aktivitas yang terjadi selanjutnya. Tidak semua insiden akan secara langsung mengganggu operasi beban kerja yang mendukung proses bisnis. Insiden seperti pengungkapan data sensitif, pencurian kekayaan intelektual, atau pembajakan sumber daya (seperti dalam penambangan mata uang kripto) mungkin tidak segera menghentikan atau melemahkan proses bisnis, tetapi dapat mengakibatkan konsekuensi ke depannya.

Memperkaya log dan temuan keamanan

Pengayaan dengan intelijen ancaman dan konteks organisasi

Selama proses analisis, hal yang menarik untuk diamati memerlukan pengayaan untuk meningkatkan kontekstualisasi peringatan. Sebagaimana dinyatakan dalam bagian Persiapan, mengintegrasikan dan memanfaatkan intelijen ancaman siber dapat membantu untuk memahami lebih lanjut tentang temuan keamanan. Layanan intelijen ancaman digunakan untuk menetapkan reputasi dan atribut kepemilikan ke alamat IP publik, nama domain, dan hash file. Alat-alat ini tersedia sebagai layanan berbayar dan tanpa biaya.

Pelanggan yang mengadopsi Amazon Athena sebagai alat kueri log mendapatkan keuntungan dari pekerjaan AWS Glue untuk memuat informasi intelijen ancaman sebagai tabel. Tabel intelijen ancaman dapat digunakan dalam kueri SQL untuk menghubungkan elemen log seperti alamat IP dan nama domain, sehingga memberikan tampilan yang diperkaya dari data yang akan dianalisis.

AWS tidak memberikan intelijen ancaman langsung kepada pelanggan, tetapi layanan seperti Amazon GuardDuty memanfaatkan intelijen ancaman untuk pengayaan dan generasi pencarian. Anda juga dapat mengunggah daftar ancaman khusus GuardDuty berdasarkan intelijen ancaman Anda sendiri.

Pengayaan dengan otomatisasi

Otomasi merupakan bagian integral dari AWS Cloud tata kelola. Hal ini dapat digunakan di berbagai fase siklus respons insiden.

Untuk fase deteksi, otomatisasi berbasis aturan mencocokkan pola yang menarik dari model ancaman dalam log dan mengambil tindakan yang sesuai, seperti mengirim pemberitahuan. Fase analisis dapat memanfaatkan mekanisme deteksi dan meneruskan isi peringatan ke mesin yang mampu mengueri log dan memperkaya hal-hal yang dapat diamati untuk kontekstualisasi peristiwa.

Isi peringatan, dalam bentuk fundamentalnya, terdiri dari sumber daya dan identitas. Sebagai contoh, Anda dapat menerapkan otomatisasi CloudTrail untuk kueri aktivitas AWS API yang dilakukan oleh identitas atau sumber daya badan peringatan di sekitar waktu peringatan, memberikan wawasan tambahan termasuk`eventSource`, `eventNameSourceIPAddress`, dan aktivitas API `userAgent` yang diidentifikasi. Dengan melakukan kueri ini secara otomatis, responden dapat menghemat waktu selama triase dan mendapatkan konteks tambahan untuk membantu membuat keputusan yang lebih tepat.

Lihat Cara memperkaya temuan AWS Security Hub dengan posting blog metadata akun untuk contoh tentang cara menggunakan otomatisasi untuk memperkaya temuan keamanan dan menyederhanakan analisis.

Mengumpulkan dan menganalisis bukti forensik

Forensik, sebagaimana disebutkan di bagian the section called “Persiapan” dokumen ini, adalah proses mengumpulkan dan menganalisis artefak selama respons insiden. Pada AWS, ini berlaku untuk sumber daya domain infrastruktur seperti tangkapan paket lalu lintas jaringan, dump memori sistem operasi, dan untuk sumber daya domain layanan seperti log. AWS CloudTrail

Proses forensik memiliki karakteristik mendasar sebagai berikut:

- Konsisten – Mengikuti langkah-langkah tepat yang didokumentasikan, tanpa menyimpang.
- Dapat Diulang – Menciptakan hasil yang sama persis ketika diulang terhadap artefak yang sama.
- Menjadi Norma – Didokumentasikan secara publik dan diadopsi secara luas.

Penting untuk mempertahankan rantai penahanan untuk artefak yang dikumpulkan selama respons insiden. Menggunakan otomatisasi dan membuat dokumentasi otomatis dari pengumpulan ini dapat membantu, selain menyimpan artefak dalam repositori hanya-baca. Analisis hanya boleh dilakukan pada replika yang tepat dari artefak yang dikumpulkan untuk menjaga integritas.

Mengumpulkan artefak yang relevan

Dengan mempertimbangkan karakteristik ini, dan berdasarkan peringatan yang relevan serta penilaian dampak dan cakupannya, Anda perlu mengumpulkan data yang relevan untuk penyelidikan dan analisis lebih lanjut. Berbagai jenis dan sumber data yang mungkin relevan dengan investigasi, termasuk log layanan/kontrol pesawat (CloudTrail, peristiwa data Amazon S3, Log Aliran VPC), data (metadata dan objek Amazon S3), dan sumber daya (database, instans Amazon). EC2

Log pesawat layanan/kontrol dapat dikumpulkan untuk analisis lokal atau, idealnya, langsung ditanyakan menggunakan AWS layanan asli (jika berlaku). Data (termasuk metadata) dapat langsung

ditanyakan untuk mendapatkan informasi yang relevan atau untuk memperoleh objek sumber; misalnya, gunakan untuk memperoleh bucket Amazon S3 dan metadata objek dan langsung memperoleh objek sumber. AWS CLI Sumber daya perlu dikumpulkan dengan cara yang konsisten dengan jenis sumber daya dan metode analisis yang dimaksudkan. Misalnya, database dapat dikumpulkan dengan membuat seluruh database itu sendiri, atau menanyakan dan mengekstrak data dan log tertentu dari database yang relevan dengan penyelidikan. copy/snapshot of the system running the database, creating a copy/snapshot

Untuk EC2 contoh Amazon, ada kumpulan data tertentu yang harus dikumpulkan dan urutan pengumpulan khusus yang harus dilakukan untuk memperoleh dan melestarikan jumlah data terbanyak untuk analisis dan investigasi.

Secara khusus, urutan respons untuk memperoleh dan mempertahankan jumlah data terbanyak dari EC2 instans Amazon adalah sebagai berikut:

1. Mendapatkan metadata instans – Dapatkan metadata instans yang relevan dengan penyelidikan dan kueri data (ID instans, jenis, alamat IP, ID VPC/subnet, Wilayah, ID Amazon Machine Image (AMI), grup keamanan yang terlampir, waktu peluncuran).
2. Mengaktifkan perlindungan instans dan tag – Aktifkan perlindungan instans seperti perlindungan dari penghentian, mengatur perilaku shutdown agar berhenti (jika diatur untuk melakukan penghentian), menonaktifkan atribut Delete on Termination untuk volume EBS yang terlampir, dan menerapkan tag yang sesuai untuk denotasi visual dan penggunaan dalam kemungkinan otomatisasi respons (misalnya, setelah menerapkan tag dengan nama `Status` dan nilai `Quarantine`, melakukan akuisisi data secara forensik dan mengisolasi instans).
3. Mendapatkan disk (snapshot EBS) – Dapatkan snapshot EBS dari volume EBS yang terlampir. Setiap snapshot berisi informasi yang Anda perlukan untuk memulihkan data Anda (dari saat ketika snapshot diambil) ke volume EBS baru. Lihat langkah untuk melakukan pengumpulan respons langsung/artefak jika Anda menggunakan volume penyimpanan instans.
4. Memperoleh memori – Karena snapshot EBS hanya menangkap data yang telah ditulis ke volume Amazon EBS Anda, yang mungkin mengecualikan data yang disimpan atau di-cache dalam memori oleh aplikasi atau OS Anda, sangat penting untuk memperoleh gambar memori sistem menggunakan alat sumber terbuka atau komersial pihak ketiga yang sesuai untuk memperoleh data yang tersedia dari sistem.
5. (Opsional) Lakukan pengumpulan respons langsung/artefak — Lakukan pengumpulan data yang ditargetkan (disk/memory/logs) melalui respons langsung pada sistem hanya jika disk atau memori tidak dapat diperoleh sebaliknya, atau ada alasan bisnis atau operasional yang valid. Melakukan hal ini akan memodifikasi data sistem dan artefak yang berharga.

6. Menonaktifkan instance — Lepaskan instance dari grup Auto Scaling, deregister instance dari load balancer, dan sesuaikan atau terapkan profil instans yang dibuat sebelumnya dengan izin yang diminimalkan atau tanpa izin.
7. Mengisolasi atau memuat instans – Verifikasi bahwa instans secara efektif diisolasi dari sistem dan sumber daya lain dalam lingkungan dengan mengakhiri dan mencegah koneksi saat ini dan mendatang ke dan dari instans tersebut. Lihat bagian the section called “Penahanan” dari dokumen ini untuk lebih jelasnya.
8. Pilihan responden – Berdasarkan situasi dan tujuan, pilih salah satu dari yang berikut ini:
   - Nonaktifkan dan matikan sistem (disarankan).

     Matikan sistem setelah bukti yang tersedia diperoleh untuk memverifikasi mitigasi paling efektif terhadap kemungkinan dampak masa depan terhadap lingkungan oleh instans.
   - Terus jalankan instans dalam lingkungan terisolasi yang diinstrumentasi untuk pemantauan.

     Meskipun tidak direkomendasikan sebagai pendekatan standar, jika suatu situasi memerlukan pengamatan lanjutan dari instance (seperti ketika data atau indikator tambahan diperlukan untuk melakukan penyelidikan dan analisis komprehensif instance), Anda dapat mempertimbangkan untuk mematikan instance, membuat AMI dari instance, dan meluncurkan kembali instance di akun forensik khusus Anda dalam lingkungan kotak pasir yang telah diinstrumentasi sebelumnya untuk sepenuhnya diisolasi dan dikonfigurasi dengan instrumentasi untuk memfasilitasi hampir terus menerus pemantauan instance (untuk contoh, VPC Flow Logs atau VPC Traffic Mirroring).

> **Note**
>
> Sangat penting untuk mengambil memori sebelum aktivitas respons langsung atau isolasi sistem atau mematikan sistem untuk mengambil data yang mudah menguap (dan berharga) yang tersedia.

Mengembangkan narasi

Selama analisis dan investigasi, dokumentasikan tindakan yang diambil, analisis yang dilakukan, dan informasi yang diidentifikasi, untuk digunakan oleh fase berikutnya dan laporan final. Narasi ini harus ringkas dan presisi, menegaskan bahwa informasi yang relevan disertakan untuk memverifikasi pemahaman yang efektif tentang insiden tersebut dan untuk mempertahankan garis waktu yang akurat. Narasi juga membantu ketika Anda melibatkan orang-orang di luar tim respons insiden inti. Inilah contohnya:

Departemen pemasaran dan penjualan menerima surat pemerasan pada 15 Maret 2022 yang menuntut pembayaran dalam mata uang kripto jika tidak ingin data yang berpotensi sensitif dibocorkan ke publik. SOC menetapkan bahwa basis data Amazon RDS milik pemasaran dan penjualan dapat diakses publik pada 20 Februari 2022. SOC mengueri log akses RDS dan menentukan bahwa alamat IP 198.51.100.23 digunakan pada 20 Februari 2022 dengan kredensial *mm03434* milik Major Mary, salah satu developer web. SOC mengueri Log Alur VPC dan menentukan bahwa data berukuran sekitar 256 MB keluar ke alamat IP yang sama pada tanggal yang sama (cap waktu 2022-02-20T15:50+00Z). SOC menentukan melalui intelijen ancaman sumber terbuka bahwa kredensial saat ini tersedia dalam teks biasa di repositori publik *https[:]//example[.]com/majormary/rds-utils*.

Penahanan

Salah satu definisi penahanan, yang berkaitan dengan respons insiden, adalah proses atau implementasi strategi selama penanganan peristiwa keamanan yang bertindak untuk meminimalkan cakupan peristiwa keamanan dan menahan efek penggunaan yang tidak sah dalam lingkungan.

Strategi penahanan tergantung pada segudang faktor dan penerapan taktik penahanan, waktu, dan tujuannya dapat berbeda dari satu organisasi ke organisasi lain. Panduan Penanganan Insiden Keamanan Komputer NIST SP 800-61 menguraikan beberapa kriteria untuk menentukan strategi penahanan yang tepat, yang meliputi:

- Potensi kerusakan dan pencurian sumber daya
- Kebutuhan preservasi bukti
- Ketersediaan layanan (konektivitas jaringan, layanan yang diberikan kepada pihak eksternal)
- Waktu dan sumber daya yang dibutuhkan untuk mengimplementasikan strategi
- Efektivitas strategi (penahanan sebagian atau penuh)
- Durasi solusi (solusi darurat akan dihapus dalam empat jam, solusi sementara akan dihapus dalam dua minggu, solusi permanen)

Mengenai layanan AWS, bagaimanapun, langkah-langkah penahanan mendasar dapat disuling menjadi tiga kategori:

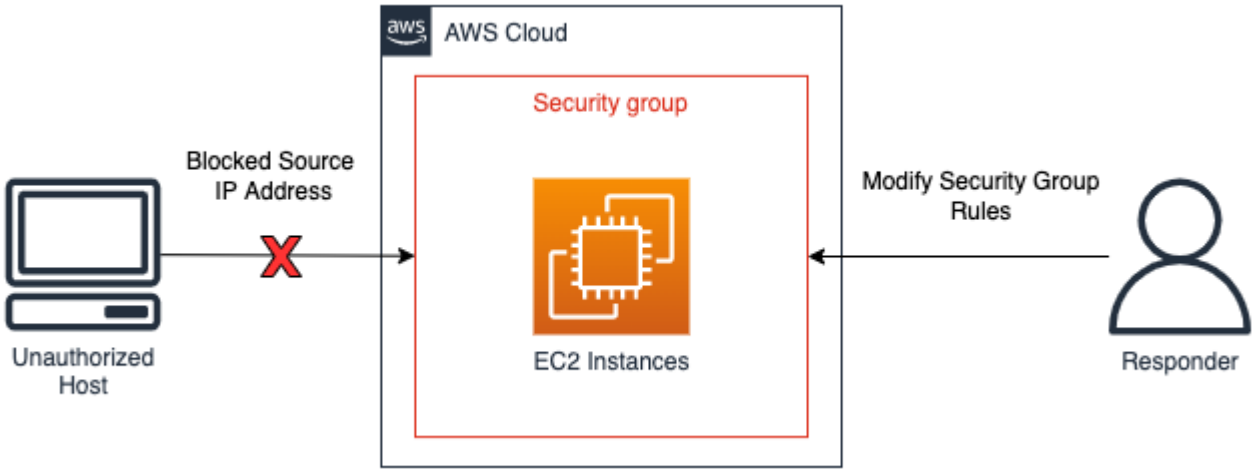
- Penahanan sumber – Gunakan penyaringan dan perutean untuk mencegah akses dari sumber tertentu.
- Teknik dan penahanan akses – Hapus akses untuk mencegah akses tidak sah ke sumber daya yang terpengaruh.
- Penahanan tujuan – Gunakan penyaringan dan perutean untuk mencegah akses ke sumber daya target.

Penahanan sumber

Penahanan sumber adalah penggunaan dan aplikasi penyaringan atau perutean dalam suatu lingkungan untuk mencegah akses ke sumber daya dari alamat IP sumber tertentu atau jangkauan jaringan. Contoh penahanan sumber menggunakan AWS layanan disorot di sini:

- Grup keamanan — Membuat dan menerapkan grup keamanan isolasi ke EC2 instans Amazon atau menghapus aturan dari grup keamanan yang ada dapat membantu memuat lalu lintas yang tidak sah ke EC2 instans atau AWS sumber daya Amazon. Penting untuk dicatat bahwa koneksi terlacak yang ada tidak akan dimatikan sebagai akibat dari perubahan grup keamanan - hanya lalu lintas mendatang yang akan diblokir secara efektif oleh grup keamanan baru (lihat Playbook Respons Insiden ini dan Pelacakan koneksi grup keamanan untuk informasi tambahan tentang koneksi terlacak dan tidak terlacak).
- Kebijakan – Kebijakan bucket Amazon S3 dapat dikonfigurasi untuk memblokir atau mengizinkan lalu lintas dari alamat IP, rentang jaringan, atau titik akhir VPC. Kebijakan menciptakan kemampuan untuk memblokir alamat dan akses yang mencurigakan ke bucket Amazon S3. Informasi selengkapnya tentang kebijakan bucket dapat dilihat di Menambahkan kebijakan bucket menggunakan konsol Amazon S3.
- AWS WAF Daftar kontrol akses web (web ACLs) dapat dikonfigurasi AWS WAF untuk memberikan kontrol halus atas permintaan web yang ditanggapi sumber daya. Anda dapat menambahkan alamat IP atau rentang jaringan ke set IP yang dikonfigurasi AWS WAF, dan menerapkan kondisi kecocokan, seperti blok, ke set IP. Hal ini akan memblokir permintaan web ke sumber daya jika alamat IP atau rentang jaringan dari lalu lintas asal sesuai dengan yang dikonfigurasi dalam aturan set IP.

Contoh penahanan sumber dapat dilihat pada diagram berikut dengan analis respons insiden memodifikasi grup keamanan EC2 instance Amazon untuk membatasi koneksi baru hanya ke alamat IP tertentu. Sebagaimana dinyatakan dalam poin grup keamanan, koneksi terlacak yang ada tidak akan dimatikan sebagai akibat dari perubahan grup keamanan.



Contoh penahanan sumber

> **Note**
>
> Grup Keamanan dan Jaringan ACLs tidak memfilter lalu lintas ke Amazon Route 53. Saat berisi EC2 instance, jika Anda ingin mencegahnya menghubungi host eksternal, pastikan Anda juga memblokir komunikasi DNS secara eksplisit.

Teknik dan penahanan akses

Mencegah penggunaan sumber daya yang tidak sah dengan membatasi fungsi dan pengguna utama IAM dengan akses ke sumber daya. Hal ini termasuk membatasi izin pengguna utama IAM yang memiliki akses ke sumber daya; juga termasuk pencabutan kredensial keamanan sementara. Contoh teknik dan akses penahanan menggunakan AWS layanan disorot di sini:

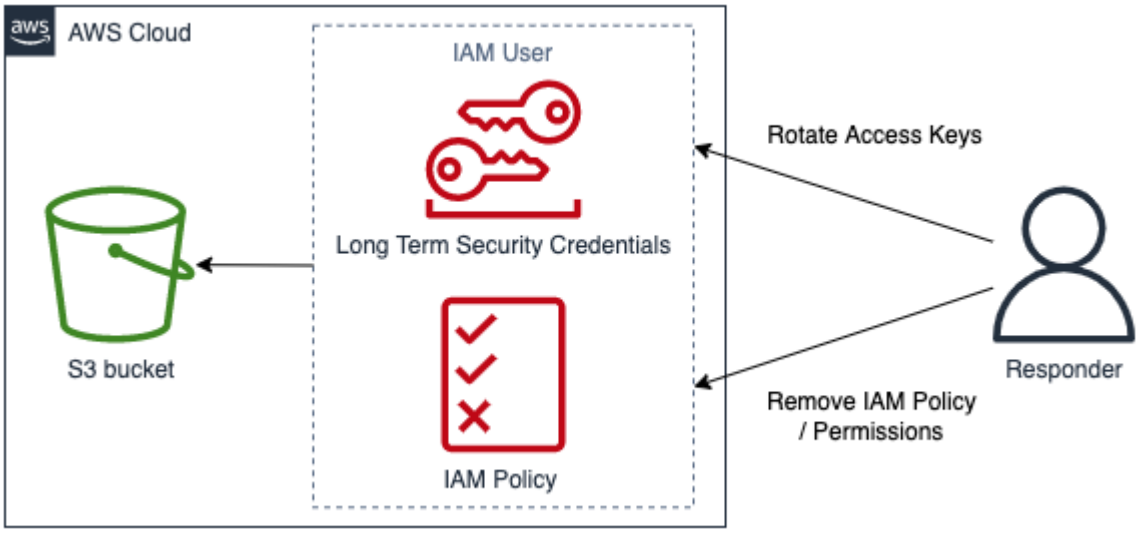
- Membatasi izin – Izin yang ditetapkan ke pengguna utama IAM harus mengikuti Prinsip Hak Akses Paling Rendah. Namun, selama peristiwa keamanan aktif, Anda mungkin perlu membatasi akses ke sumber daya yang ditargetkan dari pengguna utama IAM tertentu lebih jauh. Dalam hal ini, akses ke sumber daya bisa ditahan dengan menghapus izin dari pengguna utama IAM yang akan ditahan. Ini dilakukan dengan layanan IAM dan dapat diterapkan menggunakan AWS Management Console, AWS CLI, atau AWS SDK.
- Mencabut kunci – Kunci akses IAM digunakan oleh pengguna utama IAM untuk mengakses atau mengelola sumber daya. Ini adalah kredensil statis jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI atau AWS API dan dimulai dengan awalan AKIA (untuk informasi tambahan, lihat bagian Memahami awalan ID unik di pengidentifikasi IAM). Untuk

menahan akses bagi pengguna utama IAM yang kunci akses IAM-nya telah disusupi, kunci akses dapat dinonaktifkan atau dihapus. Penting untuk memperhatikan hal-hal berikut ini:

- Kunci akses dapat diaktifkan kembali setelah dinonaktifkan.
- Kunci akses tidak dapat dipulihkan setelah dihapus.
- Seorang pengguna utama IAM dapat memiliki hingga dua kunci akses kapan saja.
- Pengguna atau aplikasi yang menggunakan kunci akses akan kehilangan akses setelah kunci tersebut dinonaktifkan atau dihapus.

- Mencabut kredensil keamanan sementara — Kredensil keamanan sementara dapat digunakan oleh organisasi untuk mengontrol akses ke AWS sumber daya dan mulai dengan awalan ASIA (untuk informasi tambahan, lihat bagian Memahami awalan ID unik di pengenal IAM). Kredensial sementara biasanya digunakan oleh peran IAM dan tidak harus dirotasi atau dicabut secara eksplisit karena masa pakainya terbatas. Jika terjadi peristiwa keamanan yang melibatkan kredensial keamanan sementara sebelum masa berlaku kredensial keamanan sementara habis, Anda mungkin perlu mengubah izin efektif kredensial keamanan sementara yang ada. Hal ini dapat diselesaikan menggunakan layanan IAM di dalam AWS Management Console. Kredensial keamanan sementara juga dapat dikeluarkan untuk pengguna IAM (berlawanan dengan peran IAM); namun, pada saat artikel ini ditulis, tidak ada opsi untuk mencabut kredensial keamanan sementara untuk pengguna IAM di dalam AWS Management Console. Untuk peristiwa keamanan di mana kunci akses IAM pengguna disusupi oleh pengguna yang tidak sah yang membuat kredensial keamanan sementara, kredensial keamanan sementara dapat dicabut menggunakan dua metode:
  - Lampirkan kebijakan sebaris ke pengguna IAM yang mencegah akses berdasarkan waktu penerbitan token keamanan (lihat bagian Menolak akses ke kredensial keamanan sementara yang dikeluarkan sebelum waktu spesifik di Menonaktifkan izin untuk kredensial keamanan sementara untuk detail selengkapnya).
  - Hapus pengguna IAM yang memiliki kunci akses yang disusupi. Buat ulang pengguna jika diperlukan.
- AWS WAF- Teknik tertentu yang digunakan oleh pengguna yang tidak sah termasuk pola lalu lintas berbahaya yang umum, seperti permintaan yang berisi injeksi SQL dan skrip lintas situs (XSS). AWS WAF dapat dikonfigurasi untuk mencocokkan dan menolak lalu lintas menggunakan teknik ini menggunakan pernyataan aturan AWS WAF bawaan.

Contoh teknik dan penahanan akses dapat dilihat pada diagram berikut, dengan responden insiden merotasi kunci akses atau menghapus kebijakan IAM untuk mencegah pengguna IAM mengakses bucket Amazon S3.



Contoh teknik dan penahanan akses

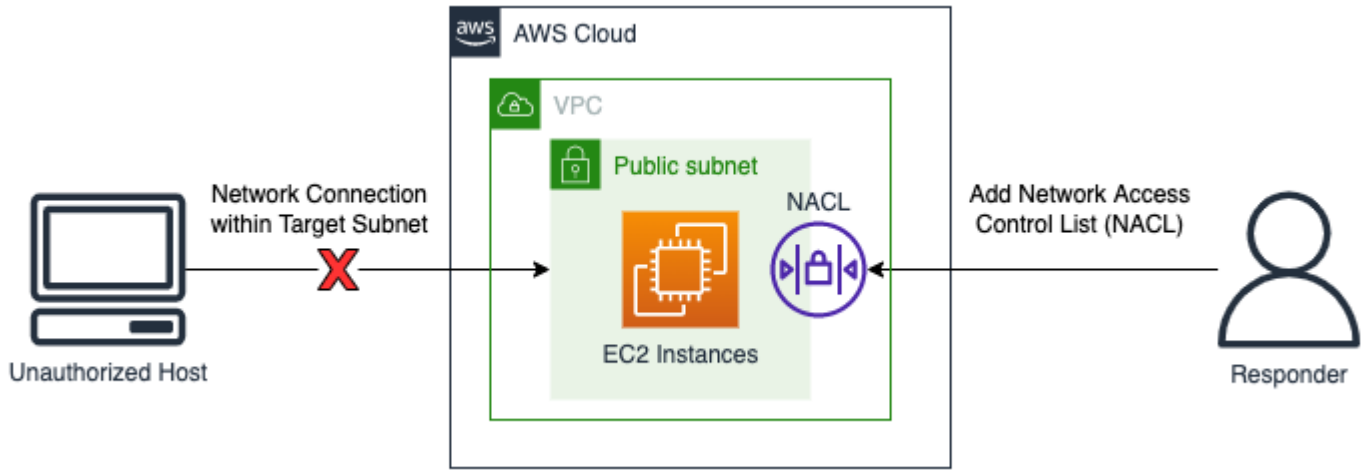
Penahanan tujuan

Penahanan tujuan adalah aplikasi penyaringan atau perutean dalam suatu lingkungan untuk mencegah akses ke host atau sumber daya yang ditargetkan. Dalam beberapa kasus, penahanan tujuan juga melibatkan suatu bentuk ketahanan untuk memverifikasi bahwa sumber daya yang sah direplikasi untuk ketersediaan; sumber daya harus dilepaskan dari bentuk-bentuk ketahanan ini untuk isolasi dan penahanan. Contoh penahanan tujuan menggunakan AWS layanan meliputi:

- Jaringan ACLs — Jaringan ACLs (jaringan ACLs) yang dikonfigurasi pada subnet yang berisi AWS sumber daya dapat memiliki aturan penolakan yang ditambahkan. Aturan penolakan ini dapat diterapkan untuk mencegah akses ke AWS sumber daya tertentu; Namun, menerapkan daftar kontrol akses jaringan (ACL jaringan) akan memengaruhi setiap sumber daya di subnet, tidak hanya sumber daya yang diakses tanpa otorisasi. Aturan yang tercantum dalam ACL jaringan diproses dalam urutan top-down, sehingga aturan pertama dalam ACL jaringan yang ada harus dikonfigurasi untuk menolak lalu lintas yang tidak sah ke sumber daya dan subnet yang ditargetkan. Atau, ACL jaringan yang sama sekali baru dapat dibuat dengan aturan penolakan tunggal untuk lalu lintas masuk dan keluar dan terkait dengan subnet yang berisi sumber daya yang ditargetkan untuk mencegah akses ke subnet menggunakan ACL jaringan baru.
- Mematikan sumber daya – Mematikan sumber daya sepenuhnya dapat efektif dalam menahan efek penggunaan yang tidak sah. Mematikan sumber daya juga akan mencegah akses yang sah untuk kebutuhan bisnis dan mencegah diperolehnya data forensik yang mudah berubah, jadi ini harus merupakan keputusan yang disengaja dan harus dinilai berdasarkan kebijakan keamanan organisasi.

- VPCs Isolasi VPCs dapat digunakan untuk menyediakan penahanan sumber daya yang efektif sambil menyediakan akses ke lalu lintas yang sah (seperti anti-virus (AV) atau solusi EDR yang memerlukan akses ke internet atau konsol manajemen eksternal). Isolasi VPCs dapat dikonfigurasi sebelumnya dari peristiwa keamanan untuk mengizinkan alamat IP dan port yang valid, dan sumber daya yang ditargetkan dapat segera dipindahkan ke VPC isolasi ini selama peristiwa keamanan aktif untuk memuat sumber daya sambil memungkinkan lalu lintas yang sah dikirim dan diterima oleh sumber daya yang ditargetkan selama fase respons insiden berikutnya. Aspek penting dari penggunaan VPC isolasi adalah bahwa sumber daya, seperti EC2 instance, perlu dimatikan dan diluncurkan kembali dalam VPC isolasi baru sebelum digunakan. EC2 Instance yang ada tidak dapat dipindahkan ke VPC lain atau Availability Zone lainnya. Untuk melakukannya, ikuti langkah-langkah yang diuraikan dalam Bagaimana cara memindahkan EC2 instans Amazon saya ke subnet lain, Availability Zone, atau VPC?
- Grup Auto Scaling dan penyeimbang beban — AWS sumber daya yang melekat pada grup Auto Scaling dan penyeimbang beban harus dilepas dan dideregistrasi sebagai bagian dari prosedur penahanan tujuan. Detasemen dan deregistrasi AWS sumber daya dapat dilakukan dengan menggunakan,, dan SDK. AWS Management Console AWS CLI AWS

Contoh penahanan tujuan ditunjukkan dalam diagram berikut dengan analis respons insiden menambahkan ACL jaringan ke subnet untuk memblokir permintaan koneksi jaringan dari host yang tidak sah.



Contoh penahanan tujuan

Ringkasan

Penahanan adalah salah satu langkah dari proses respons insiden dan dapat dilakukan secara manual atau otomatis. Strategi penahanan keseluruhan harus selaras dengan kebijakan keamanan

organisasi dan kebutuhan bisnis, dan memverifikasi bahwa efek negatif dikurangi seefisien mungkin sebelum pemberantasan dan pemulihan.

Pemberantasan

Pemberantasan, dalam kaitannya dengan respons insiden keamanan, adalah penghapusan sumber daya yang mencurigakan atau tidak sah dalam upaya mengembalikan akun ke kondisi aman yang diketahui. Strategi pemberantasan bergantung pada beberapa faktor, yang berkaitan dengan persyaratan bisnis untuk organisasi Anda.

Beberapa langkah pemberantasan tersedia di NIST SP 800-61 Computer Security Incident Handling Guide:

1. Identifikasi dan mitigasi semua kerentanan yang dieksploitasi.
2. Hapus malware, materi yang tidak pantas, dan komponen lainnya.
3. Jika ternyata ada banyak host yang terpengaruh (misalnya, infeksi malware baru), ulangi langkah-langkah deteksi dan analisis untuk mengidentifikasi semua host lain yang terkena dampak, lalu tahan dan berantas insiden untuk host-host tersebut.

Untuk AWS sumber daya, ini dapat disempurnakan lebih lanjut melalui peristiwa yang terdeteksi dan dianalisis melalui log yang tersedia atau perkakas otomatis seperti CloudWatch Log dan Amazon GuardDuty. Peristiwa-peristiwa tersebut harus menjadi dasar untuk menentukan remediasi mana yang harus dilakukan untuk memulihkan lingkungan ke kondisi aman yang diketahui.

Langkah pertama pemberantasan adalah menentukan sumber daya mana yang terpengaruh dalam akun. AWS Hal ini dicapai melalui analisis sumber data log yang tersedia, sumber daya, dan alat otomatis.

- Identifikasi tindakan tidak sah yang diambil oleh identitas IAM di akun Anda.
- Identifikasi akses yang tidak sah atau perubahan pada akun Anda.
- Identifikasi pembuatan sumber daya atau pengguna IAM yang tidak sah.
- Identifikasi sistem atau sumber daya dengan perubahan yang tidak sah.

Setelah daftar sumber daya diidentifikasi, Anda harus menilai setiap sumber daya untuk menentukan dampak bisnis jika sumber daya dihapus atau dipulihkan. Sebagai contoh, jika server web menghosting aplikasi bisnis Anda dan menghapus server tersebut akan menyebabkan waktu henti, Anda harus mempertimbangkan untuk memulihkan sumber daya dari cadangan aman yang

diverifikasi atau meluncurkan ulang sistem dari AMI yang bersih sebelum menghapus server yang terkena dampak.

Setelah Anda menyimpulkan analisis dampak bisnis Anda, maka, dengan menggunakan peristiwa dari analisis log Anda, Anda harus masuk ke akun dan melakukan remediasi yang sesuai, seperti:

- Merotasi atau menghapus kunci - langkah ini menghilangkan kemampuan aktor untuk terus melakukan aktivitas di dalam akun.
- Merotasi kredensial pengguna IAM yang berpotensi tidak sah.
- Menghapus sumber daya yang tidak dikenal atau tidak sah.

> **Important**
>
> Jika Anda harus menyimpan sumber daya untuk penyelidikan Anda, pertimbangkan untuk mencadangkan sumber daya tersebut. Misalnya, jika Anda harus mempertahankan EC2 instans Amazon untuk alasan peraturan, kepatuhan, atau hukum, buat snapshot Amazon EBS sebelum menghapus instans.

- Untuk infeksi malware, Anda mungkin perlu menghubungi vendor AWS Partner atau vendor lain. AWS tidak menawarkan alat asli untuk analisis atau penghapusan malware. Namun, jika Anda menggunakan modul GuardDuty Malware untuk Amazon EBS, rekomendasi mungkin tersedia untuk temuan yang disediakan.

Setelah Anda menghapus sumber daya yang teridentifikasi, AWS sarankan Anda melakukan tinjauan keamanan akun Anda. Ini dapat dilakukan dengan menggunakan AWS Config aturan, menggunakan solusi open-source seperti Prowler dan ScoutSuite, atau melalui vendor lain. Anda juga dapat mempertimbangkan untuk melakukan pemindaian kerentanan terhadap sumber daya yang digunakan publik (internet) untuk menilai risiko residual.

Pemberantasan adalah salah satu langkah dari proses respons insiden dan dapat dilakukan secara manual atau otomatis, tergantung insiden dan sumber daya yang terpengaruh. Strategi keseluruhan harus selaras dengan kebijakan keamanan dan kebutuhan bisnis organisasi, dan memverifikasi bahwa efek negatif dimitigasi saat sumber daya atau konfigurasi yang tidak sesuai dihapus.

Pemulihan

Pemulihan adalah proses memulihkan sistem ke keadaan aman yang diketahui, memvalidasi bahwa cadangan aman atau tidak terpengaruh oleh insiden sebelum restorasi, pengujian untuk

memverifikasi bahwa sistem berfungsi dengan baik setelah restorasi, dan mengatasi kerentanan yang terkait dengan peristiwa keamanan.

Urutan pemulihan bergantung pada kebutuhan organisasi Anda. Sebagai bagian dari proses pemulihan, Anda harus melakukan analisis dampak bisnis untuk menentukan, setidaknya:

- Prioritas bisnis atau dependensi
- Rencana restorasi
- Autentikasi dan otorisasi

NIST SP 800-61 Computer Security Incident Handling Guide menyediakan beberapa langkah untuk memulihkan sistem, termasuk:

- Memulihkan sistem dari cadangan bersih.
  - Verifikasi bahwa cadangan dievaluasi sebelum memulihkan ke sistem untuk memastikan bahwa infeksi tidak ada dan untuk mencegah kebangkitan peristiwa keamanan.

    Cadangan harus dievaluasi secara teratur sebagai bagian dari pengujian pemulihan bencana untuk memverifikasi bahwa mekanisme cadangan berfungsi dengan baik dan integritas data memenuhi tujuan titik pemulihan.
  - Jika memungkinkan, gunakan cadangan dari sebelum stempel waktu kejadian pertama yang diidentifikasi sebagai bagian dari analisis akar masalah.
- Membangun kembali sistem dari awal, termasuk memindahkan dari sumber tepercaya menggunakan otomatisasi, kadang-kadang di akun baru. AWS
- Mengganti file yang disusupi dengan versi bersih.

  Anda harus sangat berhati-hati saat melakukan ini. Anda harus benar-benar yakin bahwa file yang Anda pulihkan diketahui aman dan tidak terpengaruh oleh insiden tersebut
- Menginstal patch.
- Mengubah kata sandi.
  - Hal ini termasuk kata sandi untuk pengguna utama IAM yang mungkin telah disalahgunakan.
  - Jika memungkinkan, sebaiknya gunakan peran untuk pengguna utama dan federasi IAM sebagai bagian dari strategi hak akses paling rendah.
- Memperketat keamanan perimeter jaringan (aturan firewall, daftar kontrol akses router batas).

Setelah sumber daya dipulihkan, penting untuk mengambil pelajaran yang dapat dipetik untuk memperbarui kebijakan, prosedur, dan panduan respons insiden.

Singkatnya, sangat penting untuk menerapkan proses pemulihan yang memfasilitasi kembalinya ke operasi aman yang diketahui. Pemulihan dapat memakan waktu lama dan membutuhkan hubungan yang erat dengan strategi penahanan untuk menyeimbangkan dampak bisnis terhadap risiko infeksi ulang. Prosedur pemulihan harus mencakup langkah-langkah untuk memulihkan sumber daya dan layanan, pengguna utama IAM, dan melakukan tinjauan keamanan akun untuk menilai risiko residual.

Kesimpulan

Setiap fase operasi memiliki tujuan, teknik, metodologi, dan strategi yang unik. Tabel 4 merangkum fase-fase ini dan beberapa teknik serta metodologi yang tercakup dalam bagian ini.

Tabel 4 – Fase operasi: Tujuan, teknik, dan metodologi

Fase	Tujuan	Teknik dan metodologi
Deteksi	Mengidentifikasi peristiwa keamanan potensial.	• Kontrol keamanan untuk deteksi • Deteksi berbasis perilaku dan aturan • Deteksi berbasis orang
Analisis	Menentukan apakah peristiwa keamanan tersebut merupakan insiden dan menilai cakupan insiden tersebut.	• Memvalidasi dan membuat cakupan peringatan • Log kueri • Intelijen ancaman • Otomatisasi
Penahanan	Meminimalkan dan membatasi dampak peristiwa keamanan.	• Penahanan sumber • Teknik dan penahanan akses • Penahanan tujuan
Pemberantasan	Menghapus sumber daya atau artefak tidak sah yang terkait dengan peristiwa keamanan.	• Rotasi atau penghapusan kredensial yang disusupi atau tidak sah

Fase	Tujuan	Teknik dan metodologi
		• Penghapusan sumber daya yang tidak sah • Penghapusan malware • Pemindaian keamanan
Pemulihan	Mengembalikan sistem ke kondisi yang diketahui baik dan pantau sistem ini untuk memastikan ancaman tidak kembali.	• Pemulihan sistem dari cadangan • Sistem dibangun kembali dari awal • File yang disusupi diganti dengan versi bersih

Aktivitas pascainsiden

Lanskap ancaman terus berubah dan penting agar organisasi Anda memiliki kemampuan yang juga dinamis untuk melindungi lingkungan Anda secara efektif. Kunci untuk perbaikan berkelanjutan adalah mengulangi hasil insiden dan simulasi Anda untuk meningkatkan kemampuan Anda untuk secara efektif mendeteksi, merespons, dan menyelidiki kemungkinan insiden keamanan, mengurangi kemungkinan kerentanan Anda, waktu untuk merespons, dan kembali ke operasi yang aman. Mekanisme berikut dapat membantu Anda memverifikasi bahwa organisasi Anda tetap siap dengan kemampuan dan pengetahuan terbaru untuk merespons secara efektif, apa pun situasinya.

Menetapkan kerangka kerja untuk belajar dari insiden

Menerapkan kerangka kerja dan metodologi pembelajaran tidak hanya akan membantu meningkatkan kemampuan respons insiden, tetapi juga membantu mencegah insiden terulang kembali. Dengan belajar dari setiap kejadian, Anda dapat membantu menghindari terulangnya kesalahan, eksposur, atau kesalahan konfigurasi, yang tidak hanya meningkatkan postur keamanan Anda, tetapi juga meminimalkan waktu yang terbuang untuk situasi yang dapat dicegah.

Penting untuk menerapkan kerangka kerja pembelajaran dan meraih poin-poin berikut di tingkatan tinggi:

- Kapan pembelajaran diadakan?
- Apa saja yang terlibat dalam proses pembelajaran tersebut?

- Bagaimana pembelajaran dilakukan?
- Siapa yang terlibat dalam proses tersebut dan bagaimana caranya?
- Bagaimana cara mengenali area yang perlu ditingkatkan?
- Bagaimana Anda memastikan perbaikan dilacak dan diimplementasikan secara efektif?

Selain dari hasil tingkat tinggi yang tercantum di atas, penting untuk memastikan bahwa Anda mengajukan pertanyaan yang tepat untuk mendapatkan nilai terbaik (informasi yang mengarah pada peningkatan yang dapat ditindaklanjuti) dari proses tersebut. Pertimbangkan pertanyaan-pertanyaan ini untuk membantu Anda memulai dalam mendorong diskusi pembelajaran Anda:

- Apa insiden yang terjadi?
- Kapan insiden tersebut pertama kali diidentifikasi?
- Bagaimana insiden tersebut diidentifikasi?
- Sistem apa yang memunculkan peringatan tentang aktivitas tersebut?
- Sistem, layanan, dan data apa yang terlibat?
- Secara khusus, apa yang terjadi?
- Apa yang berjalan dengan baik?
- Apa yang tidak berjalan dengan baik?
- Proses atau prosedur mana yang gagal atau tidak dapat diskalakan untuk merespons insiden tersebut?
- Apa yang dapat ditingkatkan dalam bidang berikut:
  - Orang
    - Apakah orang-orang yang perlu dihubungi benar-benar tersedia dan apakah daftar kontak sudah aktual?
    - Apakah orang-orang tidak mendapatkan pelatihan atau tidak memiliki kemampuan yang diperlukan untuk merespons dan menyelidiki insiden tersebut secara efektif?
    - Apakah sumber daya yang sesuai siap dan tersedia?
  - Proses
    - Apakah proses dan prosedur diikuti?
    - Apakah proses dan prosedur didokumentasikan dan tersedia untuk (jenis) insiden ini?
    - Apakah proses dan prosedur yang diperlukan tidak ada?
    - Apakah responden dapat memperoleh akses tepat waktu ke informasi yang diperlukan untuk merespons masalah ini?

  - Teknologi
    - Apakah sistem peringatan yang ada mampu mengidentifikasi dan memperingatkan tentang aktivitas tersebut secara efektif?
    - Apakah peringatan yang ada perlu ditingkatkan atau apakah peringatan baru perlu dibangun untuk (jenis) insiden ini?
    - Apakah alat yang ada membuat penyelidikan (pencarian/analisis) insiden tersebut dapat dilakukan secara efektif?
- Apa yang dapat dilakukan untuk membantu mengidentifikasi (jenis) insiden ini lebih cepat?
- Apa yang dapat dilakukan untuk membantu mencegah (jenis) insiden ini terjadi lagi?
- Siapa yang bertanggung jawab atas rencana peningkatan dan bagaimana cara untuk menguji apakah rencana tersebut telah diimplementasikan?
- Apa garis waktu untuk tambahan yang akan monitoring/preventative controls/process diimplementasikan dan diuji?

Daftar ini tidak mencakup semua; hal ini dimaksudkan untuk berfungsi sebagai titik awal guna mengidentifikasi kebutuhan organisasi dan bisnis dan bagaimana Anda dapat menganalisisnya agar dapat belajar secara efektif dari insiden dan terus meningkatkan postur keamanan Anda. Yang paling penting adalah memulai dengan memasukkan pembelajaran yang diambil sebagai bagian standar dari proses respons insiden, dokumentasi, dan ekspektasi di seluruh pemangku kepentingan.

Menetapkan metrik keberhasilan

Metrik diperlukan untuk mengukur, menilai, dan meningkatkan kemampuan respons insiden Anda secara efektif. Tanpa metrik, Anda tidak memiliki referensi untuk mengukur secara akurat atau bahkan mengidentifikasi seberapa baik (atau buruk) performa organisasi Anda. Ada beberapa metrik umum untuk respons insiden yang merupakan titik awal yang baik bagi organisasi yang ingin menetapkan ekspektasi serta referensi untuk berupaya mewujudkan keunggulan operasional.

Waktu rata-rata untuk mendeteksi

Waktu rata-rata untuk mendeteksi adalah waktu rata-rata yang diperlukan untuk menemukan kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara terjadinya indikator penyusupan pertama dan identifikasi atau peringatan awal.

Anda dapat menggunakan metrik ini untuk melacak seberapa efektif performa sistem deteksi dan peringatan Anda. Mekanisme deteksi dan peringatan yang efektif adalah kunci untuk memverifikasi bahwa kemungkinan insiden keamanan tidak berlangsung lama di lingkungan Anda.

Makin tinggi waktu rata-rata deteksi, makin besar kebutuhan untuk membangun peringatan dan mekanisme tambahan atau yang lebih efektif untuk mengidentifikasi dan menemukan kemungkinan insiden keamanan. Makin rendah waktu rata-rata deteksi, makin baik fungsi mekanisme deteksi dan peringatan Anda.

Waktu rata-rata untuk mengakui

Waktu rata-rata untuk mengakui adalah waktu rata-rata yang diperlukan untuk mengakui dan memprioritaskan kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara pembuatan peringatan dan anggota SOC Anda atau staf respons insiden mengidentifikasi dan memprioritaskan peringatan untuk diproses.

Anda dapat menggunakan metrik ini untuk melacak seberapa baik tim Anda memproses dan memprioritaskan peringatan. Jika tim Anda tidak dapat mengidentifikasi dan memprioritaskan peringatan secara efektif, respons akan tertunda dan menjadi tidak efektif.

Makin tinggi waktu rata-rata untuk mengakui, makin besar kebutuhan untuk memverifikasi bahwa tim Anda memiliki sumber daya yang memadai dan terlatih untuk dengan cepat mengetahui dan memprioritaskan kemungkinan insiden keamanan untuk direspons. Makin rendah waktu rata-rata untuk mengakui, makin baik tim Anda dalam merespons peringatan keamanan, yang menunjukkan bahwa mereka melakukan persiapan secara efektif dan mampu menentukan prioritas dengan baik.

Waktu rata-rata untuk merespons

Waktu rata-rata untuk merespons adalah waktu rata-rata yang diperlukan untuk memulai respons awal terhadap kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara peringatan awal atau penemuan kemungkinan insiden keamanan dan tindakan pertama yang diambil untuk merespons. Ini mirip dengan waktu rata-rata untuk mengakui, tetapi ini merupakan pengukuran tindakan responsif tertentu (misalnya, memperoleh data sistem, menahan sistem), bukan pengenalan atau pengakuan sederhana atas situasinya.

Anda dapat menggunakan metrik ini untuk melacak kesiapan Anda dalam merespons insiden keamanan. Seperti disebutkan, persiapan adalah kunci untuk respons yang efektif. Lihat bagian the section called “Persiapan” dari dokumen ini.

Makin tinggi waktu rata-rata untuk merespons, makin besar kebutuhan untuk memverifikasi bahwa tim Anda dilatih dengan baik tentang cara merespons sehingga proses respons didokumentasikan dan digunakan secara efektif. Makin rendah waktu rata-rata untuk merespons, makin baik tim Anda dalam mengidentifikasi respons yang tepat terhadap peringatan yang teridentifikasi dan melakukan tindakan responsif yang diperlukan untuk memulai pengembalian ke operasi yang aman.

Waktu rata-rata untuk menahan

Waktu rata-rata untuk menahan adalah waktu rata-rata yang diperlukan untuk menahan kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara peringatan awal atau penemuan kemungkinan insiden keamanan dan penyelesaian tindakan responsif yang secara efektif mencegah penyerang atau sistem yang dikompromikan dari melakukan kerusakan lebih lanjut.

Anda dapat menggunakan metrik ini untuk melacak seberapa baik tim Anda dapat memitigasi atau menahan kemungkinan insiden keamanan. Ketidakmampuan untuk menahan kemungkinan insiden keamanan secara cepat dan efektif akan meningkatkan dampak, cakupan, dan eksposur dari kemungkinan penyusupan lebih lanjut.

Makin tinggi waktu rata-rata untuk menahan, makin besar kebutuhan untuk membangun pengetahuan dan kemampuan agar dapat mengurangi dan menahan insiden keamanan yang Anda alami dengan cepat dan efektif. Makin rendah waktu rata-rata untuk menahan, makin baik tim Anda dalam memahami dan menggunakan langkah-langkah yang diperlukan untuk memitigasi dan menahan ancaman yang teridentifikasi guna mengurangi dampak, cakupan, dan risiko terhadap bisnis.

Waktu rata-rata untuk pulih

Waktu rata-rata untuk memulihkan adalah waktu rata-rata yang diperlukan untuk sepenuhnya kembali ke operasi yang aman dari kemungkinan insiden keamanan. Secara khusus, ini adalah waktu antara peringatan awal atau penemuan kemungkinan insiden keamanan dan ketika bisnis kembali beroperasi secara normal dan aman tanpa terpengaruh oleh insiden tersebut.

Anda dapat menggunakan metrik ini untuk melacak seberapa efektif tim Anda dalam mengembalikan sistem, akun, dan lingkungan ke operasi yang aman setelah insiden keamanan terjadi. Ketidakmampuan untuk kembali ke operasi yang aman dengan cepat atau efektif tidak hanya dapat berdampak pada keamanan, tetapi juga dapat meningkatkan dampak dan biaya bagi bisnis dan operasinya.

Makin tinggi waktu rata-rata untuk pulih, makin besar kebutuhan untuk mempersiapkan tim dan lingkungan Anda untuk memiliki mekanisme yang sesuai (misalnya, proses failover dan alur CI/CD untuk melakukan deployment kembali sistem bersih yang aman) guna meminimalkan dampak insiden keamanan terhadap operasi dan bisnis. Makin rendah waktu rata-rata untuk pulih, makin efektif tim Anda dalam meminimalkan dampak insiden keamanan pada operasi dan bisnis Anda.

Waktu tinggal penyerang

Waktu tinggal penyerang adalah waktu rata-rata bahwa pengguna yang tidak sah memiliki akses ke sistem atau lingkungan. Hal ini mirip dengan waktu rata-rata untuk menahan, tetapi kerangka waktu ini dimulai dengan waktu awal penyerang memperoleh akses ke sistem atau lingkungan, yang mungkin lebih awal dari peringatan atau penemuan awal.

Anda dapat menggunakan metrik ini untuk melacak seberapa baik sistem dan mekanisme Anda bekerja sama untuk mengurangi jumlah waktu, akses, dan kesempatan yang dimiliki penyerang atau ancaman untuk memengaruhi lingkungan Anda. Mengurangi waktu tinggal penyerang harus menjadi prioritas utama bagi tim dan bisnis Anda.

Makin tinggi waktu tinggal penyerang, makin besar kebutuhan untuk mengidentifikasi bagian mana dari proses respons insiden yang perlu ditingkatkan untuk memastikan kemampuan tim Anda dalam meminimalkan dampak dan cakupan ancaman atau serangan di lingkungan Anda. Makin rendah waktu tinggal penyerang, makin baik tim Anda meminimalkan waktu dan peluang yang dimiliki ancaman atau penyerang dalam lingkungan Anda, yang pada akhirnya mengurangi risiko dan dampak terhadap operasi dan bisnis Anda.

Ringkasan metrik

Membuat dan melacak metrik untuk respons insiden memungkinkan Anda mengukur, menilai, dan meningkatkan kemampuan respons insiden secara efektif. Untuk mencapai hal ini, ada sejumlah metrik respons insiden umum yang disorot di bagian ini. Tabel 5 merangkum metrik-metrik ini.

Tabel 5 – Metrik respons insiden

Metrik	Deskripsi
Waktu rata-rata untuk mendeteksi	Waktu rata-rata yang diperlukan untuk menemukan kemungkinan insiden keamanan
Waktu rata-rata untuk mengakui	Waktu rata-rata yang diperlukan untuk mengakui (dan memprioritaskan) kemungkinan insiden keamanan
Waktu rata-rata untuk merespons	Waktu rata-rata yang diperlukan untuk memulai respons awal terhadap kemungkinan insiden keamanan

Metrik	Deskripsi
Waktu rata-rata untuk menahan	Waktu rata-rata yang diperlukan untuk menahan kemungkinan insiden keamanan
Waktu rata-rata untuk pulih	Waktu rata-rata yang diperlukan untuk sepenuhnya kembali ke operasi yang aman dari kemungkinan insiden keamanan
Waktu tinggal penyerang	Waktu rata-rata pengguna yang tidak sah memiliki akses ke sistem atau lingkungan

Gunakan indikator kompromi () IOCs

Indikator kompromi (IOC) adalah artefak yang diamati di dalam atau pada jaringan, sistem, atau lingkungan yang dapat (dengan tingkat kepercayaan tinggi) mengidentifikasi aktivitas berbahaya atau insiden keamanan. IOCs dapat ada dalam berbagai bentuk, termasuk alamat IP, domain, artefak tingkat jaringan seperti bendera atau muatan TCP, artefak sistem atau tingkat host seperti executable, nama file dan hash, entri file log, atau entri registri, dan banyak lagi. IOC juga dapat berupa kombinasi item atau aktivitas, seperti keberadaan item atau artefak tertentu pada sistem (file tertentu atau set file dan item registri), tindakan yang dilakukan dalam urutan tertentu (masuk ke sistem dari IP tertentu diikuti oleh perintah anomali tertentu), atau aktivitas jaringan (lalu lintas masuk atau keluar anomali ke atau dari domain tertentu) yang dapat menunjukkan ancaman, serangan, atau metodologi penyerang tertentu.

Saat Anda bekerja untuk meningkatkan program respons insiden secara berulang, Anda harus menerapkan kerangka kerja untuk mengumpulkan, mengelola, dan memanfaatkan IOCs sebagai mekanisme untuk terus membangun dan meningkatkan deteksi dan peringatan serta meningkatkan kecepatan dan kemanjuran investigasi. Anda dapat mulai dengan memasukkan pengumpulan dan pengelolaan IOCs ke dalam fase analisis dan investigasi dari proses respons insiden Anda. Dengan secara proaktif mengidentifikasi, mengumpulkan, dan menyimpan IOCs sebagai bagian standar dari proses Anda, Anda dapat membangun repositori data (sebagai bagian dari program intelijen ancaman yang lebih komprehensif) yang pada gilirannya dapat digunakan untuk meningkatkan deteksi dan peringatan yang ada, membangun deteksi dan peringatan tambahan, mengidentifikasi di mana dan kapan artefak terlihat sebelumnya, membangun dan mereferensikan dokumentasi tentang bagaimana investigasi sebelumnya dilakukan yang melibatkan pencocokan, dan banyak lagi. IOCs

Pendidikan dan pelatihan berkelanjutan

Pendidikan dan pelatihan merupakan upaya yang terus berkembang dan berkelanjutan yang harus diupayakan dan dipertahankan. Ada berbagai mekanisme untuk memverifikasi bahwa tim Anda menjaga kewaspadaan, pengetahuan, dan kemampuan yang sejalan dengan perkembangan teknologi serta lanskap ancaman.

Salah satu mekanismenya adalah menggunakan pendidikan berkelanjutan sebagai bagian standar dari tujuan dan operasi tim Anda. Seperti yang disebutkan di bagian Persiapan, staf dan pemangku kepentingan respons insiden Anda harus dilatih secara efektif untuk mendeteksi, menanggapi, dan menyelidiki insiden di dalamnya. AWS Namun, pendidikan bukanlah upaya yang “sekali jadi”. Pendidikan harus terus dijalankan untuk memverifikasi bahwa tim Anda dapat mengikuti kemajuan teknologi terbaru, informasi terbaru, dan peningkatan yang dapat dimanfaatkan untuk meningkatkan efektivitas dan efisiensi respons, serta penambahan atau pembaruan pada data yang dapat dimanfaatkan untuk meningkatkan penyelidikan dan analisis.

Mekanisme lain adalah memverifikasi bahwa simulasi dilakukan secara teratur (misalnya, setiap triwulan) dan berfokus pada hasil spesifik untuk bisnis. Lihat bagian the section called “Menjalankan simulasi reguler” dari dokumen ini.

Meskipun menjalankan latihan meja awal adalah cara terbaik untuk menghasilkan dasar awal untuk perbaikan, pengujian berkelanjutan adalah kunci untuk perbaikan berkelanjutan dan mempertahankan refleksi yang up-to-date akurat dari keadaan operasi saat ini. Pengujian terhadap situasi keamanan terbaru dan paling kritis serta kemampuan yang paling penting atau terbaru untuk respons, dan menggabungkan pembelajaran ke dalam pendidikan, operasi, dan proses/prosedur akan memverifikasi bahwa Anda dapat terus meningkatkan proses dan program respons Anda secara keseluruhan.

Kesimpulan

Saat Anda melanjutkan perjalanan cloud Anda, penting bagi Anda untuk mempertimbangkan konsep respons insiden keamanan mendasar untuk AWS lingkungan Anda. Anda dapat menggabungkan kontrol yang tersedia, kemampuan cloud, dan opsi remediasi untuk membantu Anda meningkatkan keamanan lingkungan cloud Anda. Anda juga dapat memulai dari yang kecil dan melakukan iterasi saat Anda mengadopsi kemampuan otomatisasi yang meningkatkan kecepatan respons Anda, sehingga Anda menjadi lebih siap saat peristiwa keamanan terjadi.

Kontributor

Kontributor saat ini dan terdahulu untuk dokumen ini meliputi:

- Anna McAbee, Arsitek Solusi Keamanan Senior, Amazon Web Services
- Freddy Kasprzykowski, Senior Security Consultant, Amazon Web Services
- Jason Hurst, Insinyur Keamanan Senior, Amazon Web Services
- Jonathon Poling, Principal Security Consultant, Amazon Web Services
- Josh Du Lac, Senior Manager, Security Solutions Architecture, Amazon Web Services
- Paco Hope, Kepala Insinyur Keamanan, Amazon Web Services
- Ryan Tick, Senior Security Engineer, Amazon Web Services
- Steve de Vera, Insinyur Keamanan Senior, Amazon Web Services

Lampiran A: Definisi kemampuan cloud

AWS menawarkan lebih dari 200 layanan cloud dan ribuan fitur. Banyak di antaranya menyediakan kemampuan detektif, pencegahan, dan responsif native, dan lainnya dapat digunakan untuk merancang solusi keamanan khusus. Bagian ini mencakup sebagian dari layanan yang paling relevan dengan respons insiden di cloud.

Topik

Pencatatan log dan peristiwa

AWS CloudTrail— AWS CloudTrail layanan yang memungkinkan tata kelola, kepatuhan, audit operasional, dan audit risiko akun. AWS Dengan CloudTrail, Anda dapat mencatat, terus memantau, dan mempertahankan aktivitas akun yang terkait dengan tindakan di seluruh AWS layanan. CloudTrail menyediakan riwayat peristiwa aktivitas AWS akun Anda, termasuk tindakan yang diambil melalui AWS Management Console, AWS SDKs, alat baris perintah, dan AWS layanan lainnya.

Riwayat peristiwa ini menyederhanakan analisis keamanan, pelacakan perubahan sumber daya, dan pemecahan masalah. CloudTrail mencatat dua jenis tindakan AWS API yang berbeda:

- CloudTrail Peristiwa manajemen (juga dikenal sebagai operasi bidang kontrol) menunjukkan operasi manajemen yang dilakukan pada sumber daya di AWS akun Anda. Hal ini termasuk tindakan seperti membuat bucket Amazon S3 dan menyiapkan pencatatan log.
- CloudTrail Peristiwa data (juga dikenal sebagai operasi bidang data) menunjukkan operasi sumber daya yang dilakukan pada atau di dalam sumber daya di AWS akun Anda. Operasi ini sering kali merupakan aktivitas bervolume tinggi. Hal ini mencakup tindakan seperti aktivitas API tingkat objek Amazon S3 (misalnya, operasi API `GetObject`, `DeleteObject`, dan `PutObject`) dan aktivitas invokasi fungsi Lambda.

AWS Config— AWS Config adalah layanan yang memungkinkan pelanggan menilai, mengaudit, dan mengevaluasi konfigurasi sumber daya Anda AWS . AWS Config terus memantau dan mencatat konfigurasi AWS sumber daya Anda dan memungkinkan Anda untuk mengotomatiskan evaluasi konfigurasi yang direkam terhadap konfigurasi yang diinginkan. Dengan AWS Config, pelanggan dapat meninjau perubahan dalam konfigurasi dan hubungan antara AWS sumber daya, secara manual atau otomatis, riwayat konfigurasi sumber daya yang detail, dan menentukan kepatuhan secara keseluruhan terhadap konfigurasi yang ditentukan dalam pedoman pelanggan. Hal ini memungkinkan penyederhanaan audit kepatuhan, analisis keamanan, manajemen perubahan, dan pemecahan masalah operasional.

Amazon EventBridge — Amazon EventBridge mengirimkan pengaliran peristiwa sistem yang mendeskripsikan perubahan dalam AWS sumber daya, atau saat panggilan API dipublikasikan oleh AWS CloudTrail. Dengan menggunakan aturan sederhana yang dapat Anda siapkan dengan cepat, Anda dapat mencocokkan kejadian dan merutekannya ke satu atau beberapa fungsi atau pengaliran target. EventBridge menjadi sadar akan perubahan operasional saat terjadi. EventBridge dapat merespons perubahan operasional ini dan mengambil tindakan korektif seperlunya, dengan mengirim pesan untuk merespons lingkungan, mengaktifkan fungsi, membuat perubahan, dan menangkap informasi status. Beberapa layanan keamanan, seperti Amazon GuardDuty, menghasilkan output mereka dalam bentuk EventBridge acara. Banyak layanan keamanan juga menyediakan opsi untuk mengirim output-nya ke Amazon S3.

Log akses Amazon S3 – Jika informasi sensitif disimpan dalam bucket Amazon S3, pelanggan dapat mengaktifkan log akses Amazon S3 untuk merekam setiap unggahan, unduhan, dan modifikasi data tersebut. Log ini terpisah dari, dan sebagai tambahan, CloudTrail log yang mencatat perubahan pada bucket itu sendiri (seperti mengubah kebijakan akses dan kebijakan siklus hidup). Perlu diketahui bahwa catatan log akses server disampaikan atas dasar upaya terbaik. Sebagian besar permintaan

bucket yang dikonfigurasi dengan benar untuk mencatat hasil dalam catatan log yang dikirim. Kelengkapan dan ketepatan waktu pencatatan server tidak dijamin.

CloudWatch Log Amazon — Pelanggan dapat menggunakan CloudWatch Log Amazon untuk memantau, menyimpan, dan mengakses file log yang berasal dari sistem operasi, aplikasi, dan sumber lain yang berjalan di EC2 instans Amazon dengan agen CloudWatch Log. CloudWatch Log dapat menjadi tujuan untuk AWS CloudTrail, Kueri DNS Route 53, Log Aliran VPC, fungsi Lambda, dan lainnya. Pelanggan kemudian dapat mengambil data log terkait dari CloudWatch Log.

Log Alur Amazon — Log Alur VPC memungkinkan pelanggan untuk menangkap informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan. VPCs Setelah mengaktifkan log alur, mereka dapat dialirkan ke Amazon CloudWatch Logs dan Amazon S3. VPC Flow Logs membantu pelanggan dengan sejumlah tugas seperti pemecahan masalah mengapa lalu lintas tertentu tidak mencapai instance, mendiagnosis aturan grup keamanan yang terlalu ketat, dan menggunakannya sebagai alat keamanan untuk memantau lalu lintas ke instance. EC2 Gunakan pencatatan alur VPC versi terbaru untuk mendapatkan bidang yang paling kuat.

AWS WAF Log — AWS WAF mendukung pencatatan penuh dari semua permintaan web yang diperiksa oleh layanan. Pelanggan dapat menyimpannya di Amazon S3 untuk memenuhi persyaratan kepatuhan dan audit, serta debugging dan forensik. Log ini membantu pelanggan menentukan akar penyebab aturan yang dimulai dan permintaan web yang diblokir. Log dapat diintegrasikan dengan SIEM pihak ketiga dan alat analisis log.

Log kueri Route 53 Resolver – Log kueri Route 53 Resolver akan memungkinkan Anda mencatat semua kueri DNS yang dibuat oleh sumber daya dalam Amazon Virtual Private Cloud (Amazon VPC). Baik itu EC2 instance Amazon, AWS Lambda fungsi, atau wadah, jika itu hidup di VPC Amazon Anda dan membuat kueri DNS, maka fitur ini akan mencatatnya; Anda kemudian dapat menjelajahi dan lebih memahami bagaimana aplikasi Anda beroperasi.

AWS Log lain — AWS terus merilis fitur dan kemampuan layanan untuk pelanggan dengan kemampuan logging dan pemantauan baru. Untuk informasi tentang fitur yang tersedia untuk setiap AWS layanan, lihat dokumentasi publik kami.

Visibilitas dan peringatan

AWS Security Hub— AWS Security Hub memberi pelanggan pandangan komprehensif tentang peringatan keamanan prioritas tinggi dan status kepatuhan di seluruh akun. AWS Security Hub mengumpulkan, mengatur, dan memprioritaskan temuan dari layanan AWS seperti Amazon, Amazon GuardDuty Inspector, Amazon Macie, dan solusi. AWS Partner Temuan dirangkum secara visual

pada dasbor terintegrasi dengan grafik dan tabel yang dapat ditindaklanjuti. Anda juga dapat terus memantau lingkungan Anda menggunakan pemeriksaan kepatuhan otomatis berdasarkan praktik AWS terbaik dan standar industri yang diikuti organisasi Anda.

Amazon GuardDuty GuardDuty adalah layanan deteksi ancaman terkelola yang terus memantau perilaku berbahaya atau tidak sah untuk membantu pelanggan melindungi AWS akun dan beban kerja. Ini memantau aktivitas seperti panggilan API yang tidak biasa atau penerapan yang berpotensi tidak sah yang menunjukkan kemungkinan kompromi akun atau sumber daya dari instans Amazon, bucket EC2 Amazon S3, atau pengintaian oleh aktor jahat.

GuardDuty mengidentifikasi tersangka pelaku jahat melalui umpan intelijen ancaman terintegrasi menggunakan pembelajaran mesin untuk mendeteksi anomali dalam aktivitas akun dan beban kerja. Ketika ancaman potensial terdeteksi, layanan memberikan peringatan keamanan terperinci ke GuardDuty konsol dan CloudWatch Acara. Hal ini membuat peringatan dapat ditindaklanjuti dan mudah diintegrasikan ke dalam manajemen peristiwa dan sistem alur kerja yang ada.

GuardDuty juga menawarkan dua add-on untuk memantau ancaman dengan layanan tertentu: Amazon GuardDuty untuk perlindungan Amazon S3 dan Amazon GuardDuty untuk perlindungan Amazon EKS. Perlindungan Amazon S3 memungkinkan GuardDuty untuk memantau operasi API tingkat objek untuk mengidentifikasi potensi risiko keamanan data dalam bucket Amazon S3. Perlindungan Kubernetes memungkinkan GuardDuty untuk mendeteksi aktivitas mencurigakan dan potensi kompromi klaster Kubernetes di Amazon EKS.

Amazon Macie - Amazon Macie adalah layanan keamanan bertenaga AI yang membantu mencegah kehilangan data dengan secara otomatis menemukan, mengklasifikasikan, dan melindungi data sensitif yang disimpan di dalamnya. AWS Macie menggunakan machine learning (ML) untuk mengenali data sensitif seperti informasi pengenal pribadi (PII) atau kekayaan intelektual, menetapkan nilai bisnis, dan memberikan visibilitas ke tempat data ini disimpan dan bagaimana data tersebut digunakan dalam organisasi Anda. Amazon Macie terus memantau adanya anomali dalam aktivitas akses data, dan memberikan peringatan ketika mendeteksi risiko akses tidak sah atau kebocoran data yang tidak disengaja.

Aturan AWS Config AWS Config Aturan mewakili konfigurasi yang disukai untuk sumber daya dan dievaluasi terhadap perubahan konfigurasi pada sumber daya yang relevan, seperti yang dicatat oleh. AWS Config Anda dapat melihat hasil evaluasi aturan terhadap konfigurasi sumber daya di dasbor. Dengan menggunakan AWS Config aturan, Anda dapat menilai kepatuhan dan status risiko secara keseluruhan dari perspektif konfigurasi, melihat tren kepatuhan dari waktu ke waktu, dan menemukan perubahan konfigurasi mana yang menyebabkan sumber daya tidak sesuai dengan aturan.

AWS Trusted Advisor— AWS Trusted Advisor adalah sumber daya online untuk membantu Anda mengurangi biaya, meningkatkan kinerja, dan meningkatkan keamanan dengan mengoptimalkan AWS lingkungan Anda. Trusted Advisor memberikan panduan waktu nyata untuk membantu Anda menyediakan sumber daya dengan mengikuti praktik AWS terbaik. Set lengkap Trusted Advisor pemeriksaan, termasuk integrasi CloudWatch Acara, tersedia untuk pelanggan paket Business and Enterprise Support.

Amazon CloudWatch — Amazon CloudWatch adalah layanan pemantauan untuk AWS Cloud sumber daya dan aplikasi yang Anda jalankan AWS. Anda dapat menggunakan CloudWatch untuk mengumpulkan dan melacak metrik, mengumpulkan dan memantau file log, mengatur alarm, dan secara otomatis bereaksi terhadap perubahan dalam sumber daya Anda AWS . CloudWatch dapat memantau AWS sumber daya, seperti EC2 instans Amazon, tabel Amazon DynamoDB, dan instans Amazon RDS DB, serta metrik khusus yang dihasilkan oleh aplikasi dan layanan Anda, dan file log apa pun yang dihasilkan aplikasi Anda. Anda dapat menggunakan Amazon CloudWatch untuk mendapatkan visibilitas di seluruh sistem ke dalam pemanfaatan sumber daya, performa aplikasi, dan kondisi operasional. Anda dapat menggunakan wawasan ini untuk bereaksi dengan tepat dan menjaga aplikasi Anda tetap berjalan dengan lancar.

Amazon Inspector adalah layanan penilaian keamanan otomatis yang membantu meningkatkan keamanan dan kepatuhan aplikasi yang di-deploy. AWS Amazon Inspector secara otomatis menilai kerentanan atau penyimpangan dari praktik terbaik pada aplikasi. Setelah melakukan penilaian, Amazon Inspector menghasilkan daftar detail temuan keamanan yang diprioritaskan berdasarkan tingkat keparahan. Temuan ini dapat ditinjau secara langsung atau sebagai bagian dari laporan penilaian terperinci yang tersedia melalui konsol Amazon Inspector atau API.

Amazon Detective — Amazon Detective adalah layanan keamanan yang secara otomatis mengumpulkan data log dari AWS sumber daya Anda dan menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk membangun kumpulan data terkait yang memungkinkan Anda melakukan investigasi keamanan yang lebih cepat dan lebih efisien. Detective dapat menganalisis triliunan peristiwa dari berbagai sumber data seperti VPC Flow Logs, dan, dan CloudTrail GuardDuty, dan secara otomatis membuat tampilan interaktif terpadu dari sumber daya, pengguna, dan interaksi Anda di antara mereka dari waktu ke waktu. Dengan pandangan terpadu ini, Anda dapat memvisualisasikan semua detail dan konteks di satu tempat untuk mengidentifikasi alasan yang mendasari temuan, menggali aktivitas historis yang relevan, dan menentukan akar penyebabnya dengan cepat.

Otomatisasi

AWS Lambda— AWS Lambda adalah layanan komputasi tanpa server yang menjalankan kode Anda sebagai respons atas peristiwa, dan secara otomatis mengelola sumber daya komputasi yang mendasarinya. Anda dapat menggunakan Lambda untuk memperluas AWS layanan lainnya dengan logika khusus, atau membuat layanan backend Anda sendiri yang beroperasi di AWS skala, performa, dan keamanan. Lambda menjalankan kode Anda pada infrastruktur komputasi dengan ketersediaan tinggi dan melakukan administrasi sumber daya komputasi untuk Anda. Hal ini termasuk pemeliharaan server dan sistem operasi, penyediaan kapasitas dan penskalaan otomatis, deployment kode dan patch keamanan, serta pemantauan dan pencatatan kode. Anda hanya tinggal menyediakan kode.

AWS Step Functions— AWS Step Functions membuatnya mudah untuk mengkoordinasikan komponen aplikasi dan microservices terdistribusi menggunakan alur kerja visual. Step Functions menyediakan konsol grafis bagi Anda untuk mengatur dan memvisualisasikan komponen aplikasi Anda sebagai serangkaian langkah. Hal ini memudahkan Anda untuk membangun dan menjalankan aplikasi multilangkah. Step Functions secara otomatis memulai dan melacak setiap langkah, dan mencoba kembali ketika ada kesalahan, sehingga aplikasi Anda berjalan sesuai urutan dan seperti yang diharapkan.

Step Functions mencatat status setiap langkah, jadi ketika terjadi kesalahan, Anda dapat mendiagnosis dan melakukan debug masalah dengan cepat. Anda dapat mengubah dan menambahkan langkah-langkah tanpa menulis kode, sehingga Anda dapat mengembangkan aplikasi Anda dan berinovasi lebih cepat. AWS Step Functions adalah bagian dari AWS Tanpa Server, dan membuatnya mudah untuk mengatur fungsi untuk aplikasi tanpa server. AWS Lambda Anda juga dapat menggunakan Step Functions untuk orkestrasi layanan mikro menggunakan sumber daya komputasi seperti Amazon dan Amazon ECS. EC2

AWS Systems Manager — AWS Systems Manager memberi Anda visibilitas dan kontrol atas AWS infrastruktur Anda. Systems Manager menyediakan antarmuka pengguna terpadu sehingga Anda dapat melihat data operasional dari beberapa AWS layanan, dan memungkinkan Anda untuk mengotomatiskan tugas operasional di seluruh sumber daya Anda AWS . Dengan Systems Manager, Anda dapat mengelompokkan sumber daya berdasarkan aplikasi, melihat data operasional untuk pemantauan dan pemecahan masalah, dan bertindak pada kelompok sumber daya Anda. Systems Manager dapat menyimpan instans Anda dalam status yang ditentukan, melakukan perubahan sesuai permintaan, seperti memperbarui aplikasi atau menjalankan skrip shell, serta melakukan tugas otomatisasi dan patching lainnya.

Penyimpanan aman

Amazon Simple Storage Service – Amazon S3 adalah penyimpanan objek yang dibuat untuk menyimpan dan mengambil sejumlah data dari mana saja. Penyimpanan ini dirancang untuk memberikan daya tahan 99,999999999%, dan menyimpan data untuk jutaan aplikasi yang digunakan oleh para pemimpin pasar di setiap industri. Amazon S3 memberikan keamanan komprehensif dan dirancang untuk membantu Anda memenuhi persyaratan peraturan Anda. Ini memberi pelanggan fleksibilitas dalam metode yang mereka gunakan untuk mengelola data untuk pengoptimalan biaya, kontrol akses, dan kepatuhan. Amazon S3 menyediakan query-in-place fungsionalitas, yang memungkinkan Anda menjalankan analitik yang kuat langsung pada data Anda saat istirahat di Amazon S3. Amazon S3 adalah layanan penyimpanan cloud yang sangat didukung, dengan integrasi dari salah satu komunitas terbesar solusi pihak ketiga, mitra integrator sistem, dan layanan lainnya. AWS

Amazon S3 Glacier – Amazon S3 Glacier adalah layanan penyimpanan cloud yang aman, tahan lama, dan sangat murah untuk pengarsipan data dan pencadangan jangka panjang. Layanan ini dirancang untuk memberikan ketahanan 99,999999999%, keamanan komprehensif dan dirancang untuk membantu Anda memenuhi persyaratan peraturan Anda. S3 Glacier menyediakan query-in-place fungsionalitas, yang memungkinkan Anda menjalankan analitik yang kuat langsung pada data arsip Anda saat istirahat. Untuk menjaga biaya tetap rendah namun cocok untuk berbagai kebutuhan pengambilan, S3 Glacier menyediakan tiga opsi untuk akses ke arsip, dari beberapa menit hingga beberapa jam.

Kemampuan Keamanan Masa Depan dan Kustom

Layanan dan fitur yang disebutkan di atas bukanlah daftar lengkap. AWS terus menambahkan kemampuan baru. Untuk informasi lebih lanjut, kami mendorong Anda untuk meninjau halaman Apa yang Baru di AWS dan Keamanan AWS Cloud. Selain layanan keamanan yang AWS menawarkan layanan cloud asli, Anda mungkin tertarik untuk membangun kemampuan Anda sendiri di atas AWS layanan.

Meskipun kami menyarankan untuk mengaktifkan serangkaian layanan keamanan dasar dalam akun Anda, seperti Amazon AWS CloudTrail GuardDuty, dan Amazon Macie, Anda mungkin ingin memperluas kemampuan ini untuk mendapatkan nilai tambahan dari aset log Anda. Ada sejumlah alat partner yang tersedia, seperti yang tercantum dalam program Kompetensi Keamanan APN kami. Anda mungkin juga ingin menulis kueri Anda sendiri untuk mencari log Anda. Dengan banyaknya layanan terkelola yang AWS menawarkan, ini tidak pernah semudah ini. Ada banyak AWS layanan tambahan yang dapat membantu Anda dengan penyelidikan yang berada di luar cakupan paper

ini, seperti Amazon Athena, Amazon OpenSearch Service, Amazon QuickSight, Amazon Machine Learning, dan Amazon EMR.

Lampiran B: sumber daya respons AWS insiden

AWS menerbitkan sumber daya untuk membantu pelanggan mengembangkan kemampuan respons insiden. Sebagian besar contoh kode dan prosedur dapat ditemukan di repositori GitHub publik AWS eksternal. Berikut ini adalah beberapa sumber daya yang memberikan contoh cara melakukan respons insiden.

Sumber daya playbook

- Framework for Incident Response Playbooks - Contoh kerangka kerja bagi pelanggan untuk membuat, mengembangkan, dan mengintegrasikan buku pedoman keamanan dalam persiapan untuk skenario serangan potensial saat menggunakan AWS layanan.
- Sampel Playbook Respon Insiden - Buku pedoman yang mencakup skenario umum yang dihadapi oleh AWS pelanggan.
- AWS CIRT mengumumkan rilis lima lokakarya yang tersedia untuk umum.

Sumber daya forensik

- Automated Incident Response and Forensics Framework – Kerangka kerja dan solusi ini menyediakan proses forensik digital standar, yang terdiri dari fase-fase berikut: penahanan, akuisisi, pemeriksaan, dan analisis. Ini memanfaatkan fungsi AWS Λ untuk memicu proses respons insiden dengan cara berulang otomatis. Hal ini menyediakan segregasi akun untuk mengoperasikan langkah-langkah otomatisasi, menyimpan artefak, dan menciptakan lingkungan forensik.
- Automated Forensics Orchestrator for EC2 Amazon — Panduan implementasi ini menyediakan solusi swalayan untuk menangkap dan memeriksa data EC2 dari instans dan volume terlampir untuk analisis forensik jika terjadi potensi masalah keamanan yang terdeteksi. Ada AWS CloudFormation template untuk menyebarkan solusi.
- Cara mengotomatiskan pengumpulan disk forensik di AWS — AWS Blog ini merinci cara mengatur alur kerja otomatisasi untuk menangkap bukti disk untuk analisis guna menentukan ruang lingkup dan dampak potensi insiden keamanan. Ada juga AWS CloudFormation template yang disertakan untuk menyebarkan solusi.

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 AWS produk saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. AWS produk atau layanan disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau kondisi apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh AWS perjanjian, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Riwayat dokumen

Perubahan	Deskripsi	Tanggal
Menambahkan halaman untuk EventBridge integrasi Amazon dengan AWS Security Incident Response.	Bagian konten baru untuk menjelaskan bagaimana Amazon EventBridge mengintegasi dalam AWS Security Incident Response.	Juni 26, 2025
Pembaruan untuk SLR menambahkan izin untuk mendukung hak layanan.	AWSSecurityIncidentResponseTriageServiceRolePolicytelah diperbarui untuk menambahkan security-ir:GetMembership, security-ir:, security-ir:ListMemberships, guardduty:, guarduty:, guardduty:UpdateCase, dan guardduty: ListFilters izin. guardduty: UpdateFilter DeleteFilter ditambahkan untuk memfasilitasi pengelolaan filter Arsip Otomatis di akun yang didelegasikan. GetAdministratorAccount GetAdministratorAccount GuardDuty	02 Juni 2025
Pembaruan Sumber Daya.	Diperbarui https://docs.aws.amazon.com/security-ir/ latest/ userguide/appendix - b-incident-response-resources .html #playbook -resources untuk mencerminkan lokakarya aktif yang tersedia untuk pelanggan.	Mei 23, 2025

Perubahan	Deskripsi	Tanggal
Layanan mendukung bahasa Jepang.	Memperbarui konfigurasi yang didukung untuk mengident ifikasi dukungan bahasa Jepang di waktu setempat Jepang. Bahasa Inggris didukung secara global.	13 Mei 2025
Pembaruan konten dan umpan balik pelanggan.	Menambahkan catatan ke https://docs.aws.amazon.com /security-ir/ latest/userguide/ select - a-membership-accou nt .html untuk mencermin kan tugas tambahan saat menggunakan akun administr ator yang didelegasikan sebagai bagian dari pengatura n. Memperbarui pengalama n pelanggan saat bekerja dengan kasus yang dihasilka n layanan dan Mendeteksi dan Menganalisis. Detail pembatalan akun yang diperbarui untuk memberikan kejelasan yang lebih baik tentang implikasi penagihan dalam membatalk an keanggotaan.	9 Mei 2025

Perubahan	Deskripsi	Tanggal
Menambahkan tiga wilayah baru yang didukung.	Menambahkan tiga wilayah baru baru ke https://docs.aws.amazon.com/security-ir/ latest/userguide/supported-configs.html. Mumbai, Paris, dan Sao Paulo.	7 Mei 2025
Diperbarui: Pembaruan dari komentar pelanggan pada dokumen.	Kesalahan ejaan dan tata bahasa pada beberapa halaman benar. https://docs.aws.amazon.com/en_us/Keamanan yang diperbarui- ir/latest/userguide/organizations _permissions.html untuk secara akurat mencerminkan security-ir sebagai awalan layanan. Menambahkan catatan ke https://docs.aws.amazon.com/security-ir/ latest/userguide/source -containment.html mengenai Route53 dan DNS.	Februari 7, 2025

Perubahan	Deskripsi	Tanggal
Diperbarui: Pembaruan dari komentar pelanggan pada dokumen.	Diperbarui https://docs.aws.amazon.com/security-ir/ latest/ userguide/setup - monitoring-and-investigation-workflows .html untuk stackset template. Entri yang diperbaiki triage.security-ir.com ke triage.security-ir.amazonaws.com Menambahkan catatan koneksi yang dilacak untuk AWSSupport-ContainEC2Reversible pada.html. https://docs.aws.amazon.com/ security-ir/ latest/userguide/contain Memperbaiki tautan rusak pada https://docs.aws.amazon.com/security-ir/ latest/ userguide/managing -associated-accounts.html. Ditambahkan definisi untuk akun keanggotaan di https://docs.aws.amazon.com/security-ir/ latest/userguide/select - a-membership-account .html. Menambahkan catatan klarifikasi ke https://docs.aws.amazon.com/en_us/ keamanan- ir/latest/userguide/using - service-linked-rol	Desember 20, 2024

Perubahan	Deskripsi	Tanggal
	es .html untuk akun AWS Organizations manajemen.	

Perubahan	Deskripsi	Tanggal
Diperbarui: Pembaruan dari komentar pelanggan pada dokumen.	Menghapus beberapa duplikat AWS AWS dalam teks. Tetap link rusak pada https://docs.aws.amazon.com/security-ir/ latest/userguide/sir_tagging.html and https://docs.aws.amazon.com/security-ir/latest/userguide/service - name-info-in-cloudtrail .html. Pembaruan https://docs.aws.amazon.com/security-ir/ latest/userguide/contain untuk.html. Menghapus > dari paragraf pertama. Diganti AWSSupport-ContainEC 2Reversible dengan AWSSupport-ContainEC 2Instance. Diganti AWSSupport-ContainIAMReversible dengan AWSSupport-ContainIAMPrincipal. Diganti AWSSupport-Contain S 3Reversible dengan AWSSupport-ContainS 3Resource. Diperbarui pemformatan pada https://docs.aws.amazon.com/en_us/ keamanan- ir/latest/userguide/issues .html Saat memberi tahu pelanggan untuk menghubungi CIRT melalui tiket dukungan, https://	Desember 10, 2024

Perubahan	Deskripsi	Tanggal
	docs.aws.amazon.com/ security-ir/ latest/userguide/ understand - response-teams-and-support .html sekarang menyediakan opsi untuk memilih dalam formulir dukungan. CloudWatch Peristiwa yang Dihapus dan diganti dengan EventBridge pada https://d ocs.aws.amazon.com/security -ir/ latest/userguide/logging - and-events.html. Pembaruan tata bahasa pada https://docs.aws.amazon.com /security-ir/ latest/userguide/t echnique -access-containmen t.html. Tanggal publikasi dihapus dari https://docs.aws.amazon.com /security-ir/ latest/userguide/ security - incident-response-guide .html, digantikan oleh pembaruan dalam tabel ini.	
Diperbarui: kebijakan AWS terkelola dan peran terkait layanan.	Pembaruan kebijakan terkelola dan peran terkait layanan.	Desember 1, 2024
Peluncuran Layanan	Dokumen layanan awal untuk peluncuran layanan di re:Invent 2024	Desember 1, 2024

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