Panduan Teknis AWS

Panduan Respons Insiden Keamanan AWS

Panduan Respons Insiden Keamanan AWS: Panduan Teknis AWS

Table of Contents

Panduan Respons Insiden Keamanan AWS

Tanggal publikasi: 1 Januari 2023 (Revisi dokumen)

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 cloud, layanan, dan mekanisme yang tersedia bagi pelanggan yang merespons masalah keamanan.

Laporan ini ditujukan bagi mereka yang memiliki peran teknis dan mengasumsikan bahwa Anda sudah memahami prinsip-prinsip umum keamanan informasi, memiliki pemahaman dasar tentang respons insiden keamanan di lingkungan on-premise Anda saat ini, dan sudah lumayan memahami layanan cloud.

Apakah Anda sudah Well-Architected?

AWS Well-Architected Framework membantu Anda memahami pro dan kontra dari keputusan yang Anda buat saat membangun sistem di cloud. Enam pilar dari Framework ini memungkinkan Anda mempelajari praktik terbaik arsitektural untuk merancang dan mengoperasikan sistem yang andal, aman, efisien, hemat biaya, dan berkelanjutan. Dengan menggunakan AWS Well-Architected Tool, tersedia tanpa biaya di AWS Management Console, 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. Pelanggan AWS diuntungkan dengan pusat data dan arsitektur jaringan yang dibangun untuk membantu mendukung kebutuhan organisasi yang paling peka dalam urusan keamanan. AWS memiliki model tanggung jawab bersama: AWS mengelola keamanan dari cloud, sedangkan 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, membangun kemampuan deteksi dan respons dasar, kemudian mengembangkan playbook untuk membuat pustaka awal mekanisme respons insiden yang dapat diiterasi dan ditingkatkan.

Sebelum Anda mulai

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

Standar dan kerangka kerja keamanan AWS

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

AWS CAF menyediakan panduan yang mendukung koordinasi antara berbagai bagian organisasi yang berpindah ke cloud. Panduan AWS CAF dibagi menjadi beberapa area fokus, yang disebut sebagai perspektif, yang relevan untuk membangun sistem IT 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 berguna. Konsep dan praktik terbaik dari panduan NIST ini akan diterapkan pada teknologi AWS dalam laporan ini. Namun, skenario insiden on-premise tidak tercakup dalam panduan ini.

Ikhtisar respons insiden AWS

Sebagai awal, penting untuk memahami bagaimana operasi keamanan dan respons insiden merupakan hal yang berbeda di cloud. Untuk membangun kemampuan respons yang efektif di AWS, Anda perlu memahami perbedaannya dengan respons on-premise tradisional dan dampaknya terhadap program respons insiden Anda. Setiap perbedaan ini, serta prinsip desain respons insiden AWS inti, dijelaskan secara mendetail dalam bagian ini.

Aspek-aspek respons insiden AWS

Semua pengguna AWS dalam suatu organisasi harus memiliki pemahaman dasar tentang proses respons insiden keamanan, dan staf keamanan harus memahami bagaimana merespons 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.

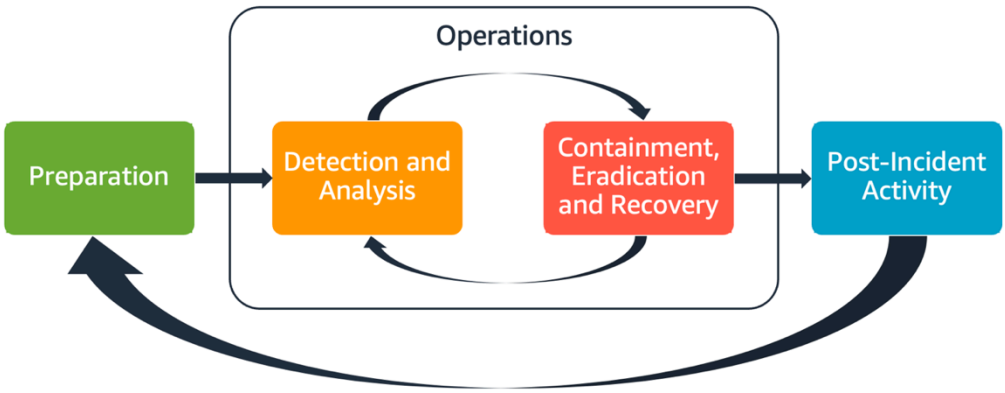
Untuk memahami setiap aspek ini, lihat deskripsi berikut:

- Persiapan – Persiapkan tim respons insiden Anda untuk mendeteksi dan merespons insiden dalam AWS dengan mengaktifkan kontrol detektif dan memverifikasi akses yang sesuai 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 setelah 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-aspek respons insiden AWS

Prinsip respons insiden AWS 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, lalu mengidentifikasi persyaratan untuk menginvestigasi 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 varians 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 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 merespons 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 mempersiapkan dan merespons peristiwa keamanan secara efektif di lingkungan AWS Anda, Anda perlu memahami jenis umum insiden keamanan cloud. 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 akun AWS Anda, izin AWS Identity and Access Management (IAM), metadata sumber daya, penagihan, atau area lainnya. Peristiwa domain layanan adalah peristiwa yang Anda respons secara eksklusif dengan mekanisme AWS API, atau ketika Anda memiliki akar penyebab yang terkait dengan konfigurasi atau izin sumber daya, dan mungkin memiliki pencatatan log 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 (Amazon EC2), lalu lintas ke instans Amazon EC2 Anda dalam cloud privat virtual (VPC), dan area lainnya, seperti kontainer atau layanan lain ke depannya. Respons Anda terhadap peristiwa domain infrastruktur sering kali melibatkan perolehan data terkait insiden untuk analisis forensik. Hal ini mungkin mencakup interaksi dengan sistem operasi sebuah instans, dan, dalam berbagai kasus, mungkin juga melibatkan mekanisme AWS API. Dalam domain infrastruktur, Anda dapat menggunakan kombinasi AWS API dan alat forensik/respons insiden (DFIR) digital dalam sistem operasi tamu, seperti instans Amazon EC2 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 cermat, Anda dapat mengelola domain ini dengan alat cloud menggunakan akuisisi, pemulihan, dan deployment otomatis.

Dalam domain ini, pertimbangkan aktor yang mungkin bertindak melawan data, sumber daya, atau akun AWS. 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 respons insiden di AWS

Respons insiden merupakan bagian integral dari strategi keamanan siber, baik on-premise maupun di cloud. Prinsip keamanan seperti hak istimewa paling rendah dan defense-in-depth bermaksud untuk melindungi kerahasiaan, integritas, dan ketersediaan data baik lokal 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 respons insiden di AWS.

Perbedaan #1: Keamanan sebagai tanggung jawab bersama

Tanggung jawab atas keamanan dan kepatuhan dibagi antara AWS dan pelanggannya. Model tanggung jawab bersama ini mengurangi beban operasional pelanggan karena AWS mengoperasikan, mengelola, dan mengontrol komponen dari sistem operasi host dan lapisan virtualisasi hingga keamanan fisik fasilitas tempat 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 partner atau pihak lain yang mengembangkan, mengelola, atau mengoperasikan beberapa teknologi cloud Anda.

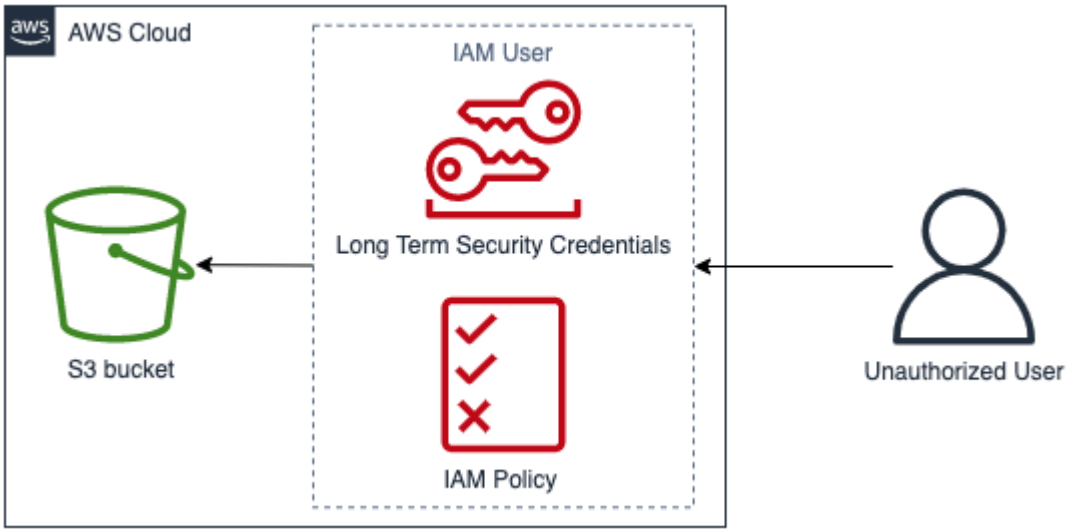
Membuat dan menguji rencana respons insiden yang sesuai dan playbook yang sesuai dengan model operasi Anda sangatlah penting.

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 akun AWS 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 merespons peristiwa keamanan ini, Anda akan menggunakan AWS API untuk menganalisis log AWS seperti AWS CloudTrail dan log akses Amazon S3. Anda juga akan menggunakan AWS API untuk melakukan penahanan dan pemulihan dari insiden tersebut.



Contoh domain layanan

Perbedaan #3: API untuk penyediaan infrastruktur

Perbedaan lain berasal dari Karakteristik cloud layanan mandiri on-demand. Pelanggan fasilitas utama berinteraksi dengan AWS Cloud menggunakan API RESTful melalui titik akhir publik dan privat yang tersedia di banyak lokasi geografis di seluruh dunia. Pelanggan dapat mengakses API ini dengan kredensial AWS. Berbeda dengan kontrol akses on-premise, kredensial ini tidak harus terikat oleh jaringan atau domain Microsoft Active Directory. Kredensial dikaitkan dengan pengguna utama 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 AWS yang berbasis API, sumber log yang penting untuk merespons peristiwa keamanan adalah AWS CloudTrail, yang melacak panggilan API manajemen yang dibuat di akun AWS Anda dan tempat 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 dinaikkan dan diturunkan 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 sumber daya AWS yang fana dan bagaimana Anda dapat melacak pembuatan dan penghapusan sumber daya AWS akan menjadi hal yang penting untuk analisis insiden. Anda dapat menggunakan AWS Config untuk melacak riwayat konfigurasi sumber daya AWS 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 melalui API agar siap menghadapi pergeseran ini, dan memverifikasi penyimpanan yang sesuai untuk pengumpulan dan akses yang efektif.

Perbedaan #6: Pentingnya otomatisasi

Agar pelanggan dapat sepenuhnya menyadari manfaat adopsi cloud, strategi operasional mereka harus menerapkan otomatisasi. I nfrastructure-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 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, agar respons bisa efektif, sangat penting agar mereka dilatih tentang teknologi AWS dan lingkungan AWS 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, menyertakan pemilik/developer aplikasi dan sumber daya yang terkena dampak adalah hal utama karena mereka merupakan ahli materi (subject matter experts/SME) yang dapat memberikan informasi dan konteks untuk membantu mengukur dampak. Pastikan untuk mempraktikkan dan membangun hubungan dengan developer serta pemilik aplikasi sebelum Anda mengandalkan keahlian mereka untuk respons insiden. Pemilik aplikasi atau SME, seperti administrator atau rekayasawan cloud Anda, mungkin perlu bertindak dalam situasi ketika lingkungan tidak dikenal atau memiliki kompleksitas, atau ketika responden tidak memiliki akses.

Terakhir, partner tepercaya mungkin terlibat dalam penyelidikan atau respons 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 layanan AWS dan lingkungan AWS 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 bagian the section called “Menjalankan simulasi reguler” di dokumen ini.

Memahami teknologi AWS Cloud

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 berjalan efektif, penting untuk memahami fondasi AWS, IAM, AWS Organizations, layanan log dan pemantauan AWS, serta layanan keamanan AWS.

AWS menyediakan lokakarya keamanan online (lihat Lokakarya Keamanan AWS) yang memberikan Anda pengalaman untuk praktik langsung dengan layanan keamanan dan pemantauan AWS. AWS juga menyediakan sejumlah opsi pelatihan dan jalur pembelajaran melalui pelatihan digital, pelatihan di ruang kelas, partner APN, dan sertifikasi. Untuk mempelajari lebih lanjut, lihat AWS Training and Certification.

Memahami lingkungan AWS Anda

Selain memahami layanan AWS, kasus penggunaannya, dan bagaimana layanan tersebut berintegrasi satu sama lain, sama pentingnya untuk memahami seperti apa arsitektur lingkungan AWS organisasi Anda dan proses operasional apa saja 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 agar analis Anda dapat mengakses dan memahami diagram serta proses operasional yang terkait dengan lingkungan AWS Anda.

Memahami tim respons dan dukungan AWS

AWS Support

AWS Support menawarkan berbagai rencana yang menyediakan akses ke alat dan keahlian yang mendukung keberhasilan dan kesehatan operasional solusi AWS. Jika Anda memerlukan dukungan teknis dan sumber daya lainnya untuk membantu merencanakan, melakukan deployment, dan mengoptimalkan lingkungan AWS, Anda dapat memilih paket dukungan yang paling sesuai dengan kasus penggunaan AWS Anda.

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

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

Tim Respons Insiden Pelanggan (CIRT) AWS

Tim Respons Insiden Pelanggan (CIRT) AWS adalah tim AWS global khusus yang selalu siap memberikan dukungan kepada pelanggan selama terjadinya peristiwa keamanan aktif di sisi pelanggan dalam Model Tanggung Jawab Bersama AWS.

Bantuan yang diberikan CIRT AWS kepada Anda dilengkapi dengan triase dan pemulihan untuk peristiwa keamanan aktif di AWS. Mereka akan membantu analisis penyebab masalah melalui penggunaan log layanan AWS dan memberi Anda rekomendasi untuk pemulihan. Mereka juga akan memberikan rekomendasi keamanan dan praktik terbaik untuk membantu Anda menghindari peristiwa keamanan ke depannya.

Pelanggan AWS dapat menggunakan CIRT AWS melalui kasus dukungan AWS.

Dukungan respons DDoS

AWS menawarkan AWS Shield, yang menyediakan layanan perlindungan distributed denial of service (DDoS) terkelola yang melindungi aplikasi web yang berjalan di AWS. AWS Shield menyediakan deteksi selalu aktif dan mitigasi inline otomatis yang dapat meminimalkan waktu henti serta latensi aplikasi, sehingga tidak perlu melibatkan AWS Support untuk mendapatkan manfaat dari perlindungan DDoS. AWS Shield memiliki dua tingkatan: 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 infrastruktur AWS 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 deployment serangkaian kontrol detektif keamanan dan memberikan respons baris pertama 24/7 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 sendiri. 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 perlu diambil – Mengenumerasi 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:

- Struktur akun AWS - Anda perlu mengetahui:

  - Berapa banyak akun AWS yang Anda miliki?
  - Bagaimana akun-akun AWS tersebut diatur?
  - Siapa pemilik bisnis akun AWS tersebut?
  - Apakah Anda menggunakan Kebijakan Kontrol Layanan (SCP)? Jika iya, pagar pembatas organisasi apa yang diterapkan dengan menggunakan SCP?
  - Apakah Anda membatasi wilayah dan layanan yang dapat digunakan?
  - Apa perbedaan antara unit bisnis dan lingkungan (dev/tes/prod)?
- Pola layanan AWS
  - Layanan AWS apa yang Anda gunakan?
  - Apa layanan AWS yang paling banyak digunakan?
- Pola arsitektur
  - Arsitektur cloud apa yang Anda gunakan?
- Pola autentikasi AWS
  - Bagaimana developer Anda biasanya mengautentikasi ke AWS?
  - Apakah Anda menggunakan pengguna atau peran IAM (atau keduanya)? Apakah autentikasi ke AWS terhubung ke penyedia identitas (IdP)?
  - Bagaimana Anda memetakan pengguna atau peran IAM ke karyawan atau sistem?
  - Bagaimana cara akses dicabut ketika seseorang tidak lagi diotorisasi?
- Pola otorisasi AWS
  - 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 menggabungkan log AWS CloudTrail? 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 dengan AWS?
  - Bagaimana lalu lintas jaringan disaring antarlingkungan?
- Infrastruktur eksternal
  - Bagaimana deployment untuk aplikasi yang digunakan secara eksternal?
  - Apa sumber daya AWS yang dapat diakses publik?
  - Apa akun AWS yang berisi infrastruktur yang digunakan secara eksternal?
  - Apa penyaringan eksternal atau DDoS 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 (TTP) aktor ancaman dan memungkinkan organisasi untuk melatih dan mengevaluasi kemampuan respons insiden mereka dengan merespons peristiwa siber tiruan ini yang mungkin saja akan benar-benar terjadi.

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. Penyelenggaraan latihan biasanya dapat dilakukan dalam sehari penuh di tempat virtual, bangunan fisik, atau kombinasi keduanya. 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. Fokus utama dalam latihan Tim Ungu adalah pada mekanisme deteksi, alat, dan prosedur operasi standar (SOP) 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. Tim pertahanan (Tim Biru) tidak harus memiliki pengetahuan tentang cakupan dan durasi latihan, sehingga memberikan penilaian yang lebih realistis tentang bagaimana mereka akan merespons insiden aktual. 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 uji penetrasi yang tersedia di situs web Uji 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 tingkat tinggi atau	Penawaran yang lebih realistis dibanding kan dengan latihan meja. Selama latihan Tim Ungu, fasilitat or bekerja secara kolaboratif dengan	Penawaran simulasi yang umumnya lebih canggih. Biasanya ada informasi yang disamarkan, sehingga para peserta mungkin

	Latihan meja	Latihan Tim Ungu	Latihan Tim Merah
	teknis, dan dijalankan dengan serangkaian skenario tertulis.	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 terjadi, staf respons insiden Anda akan dapat menyelidiki, memahami cakupan, dan mengambil tindakan dengan cepat.

Mengembangkan struktur akun AWS

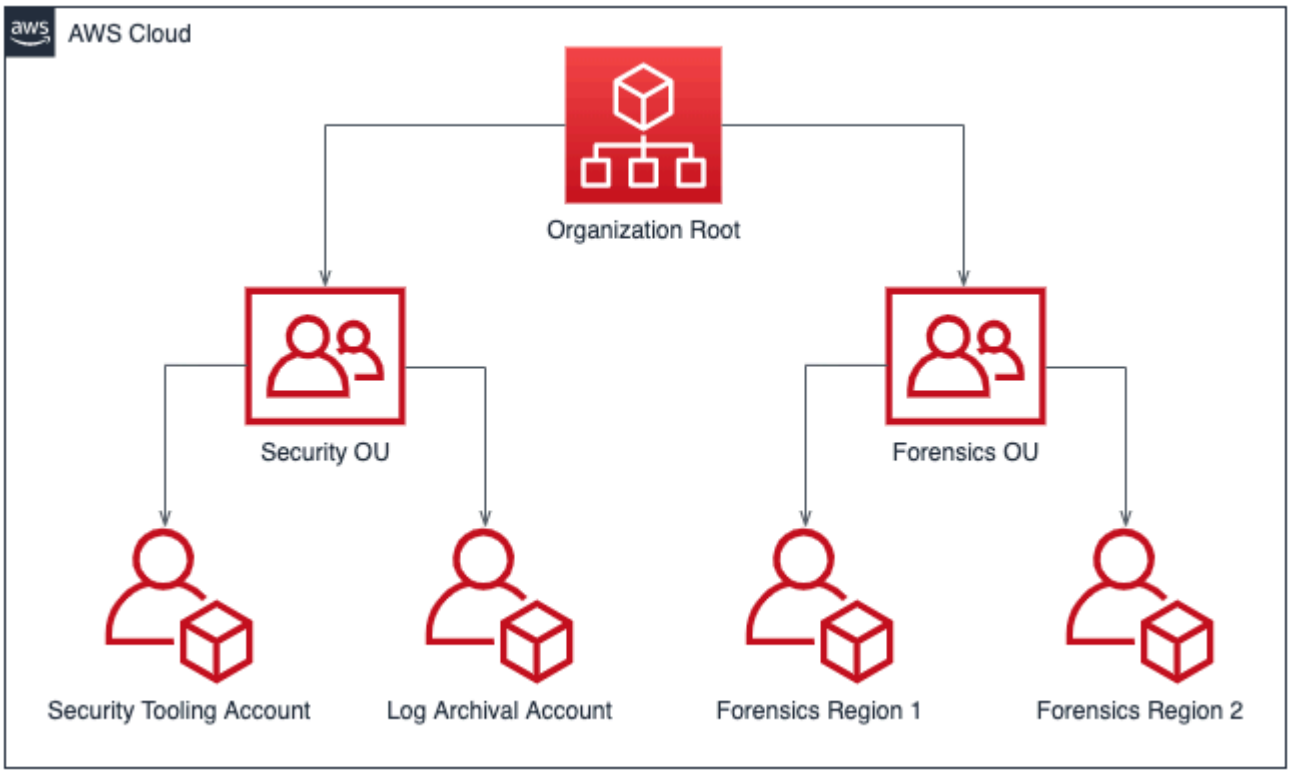
AWS Organizations membantu mengelola dan mengatur lingkungan AWS secara terpusat seiring pertumbuhan Anda dan peningkatan skala sumber daya AWS. Organisasi AWS mengonsolidasikan akun AWS Anda agar Anda dapat mengelolanya sebagai satu unit. Anda dapat menggunakan unit organisasi (OU) untuk mengelompokkan akun agar dapat mengelolanya sebagai satu unit.

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

- Pengarsipan log – Menggabungkan log dalam akun AWS pengarsipan.
- Alat keamanan – Memusatkan layanan keamanan di akun AWS alat 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 sumber daya AWS bisa menjadi hal yang sulit. Salah satu cara untuk melakukannya adalah dalam bentuk tag, yang menetapkan metadata ke sumber daya AWS 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.

Strategi pemberian tag yang konsisten dapat memangkas waktu respons dengan memudahkan Anda untuk mengidentifikasi dan membedakan informasi kontekstual tentang sumber daya AWS dengan cepat. Tag juga dapat berfungsi sebagai mekanisme untuk memulai otomatisasi respons. Untuk informasi lebih lanjut tentang apa yang harus diberi tag, lihat dokumentasi tentang pemberian tag pada sumber daya AWS. 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 blog AWS Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs).

Memperbarui informasi kontak akun AWS

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 akun AWS, Anda memiliki kontak utama dan kontak alternatif untuk keamanan, penagihan, dan operasi. Perbedaan antara kontak ini dijelaskan di Panduan Referensi Manajemen Akun AWS.

Untuk detail tentang mengelola kontak alternatif, lihat dokumentasi AWS 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 kredensial untuk setiap akun AWS. Anda juga perlu memverifikasi bahwa akun yang baru dibuat memiliki informasi kontak yang akurat. Lihat posting blog Automatically update alternate contacts for newly created Akun AWS.

Menyiapkan 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 menyediakan hak akses paling rendah 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 AWS Partner untuk pemodelan ancaman. Untuk mencari partner AWS, 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. Layanan AWS lainnya, seperti firewall DNS dan aturan AWS WAF, juga mengambil masukan dari kelompok intelijen ancaman canggih AWS. 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 blog AWS Logging strategies for security incident response.

Memilih dan mengaktifkan sumber log

Menjelang 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 akun AWS-nya.

AWS CloudTrail adalah layanan pencatatan log yang melacak panggilan API yang dilakukan terhadap akun AWS yang menangkap aktivitas layanan AWS. Ini diaktifkan secara default dengan retensi 90 hari peristiwa manajemen yang dapat diambil melalui CloudTrail fasilitas Riwayat Acara menggunakanAWS 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.

AWSmerekomendasikan 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.

Log AWS CloudTrail, Log Alur VPC, dan log kueri Route 53 resolver adalah trifecta pencatatan log dasar untuk mendukung investigasi keamanan di AWS.

AWSlayanan dapat menghasilkan log yang tidak ditangkap oleh trifecta logging dasar, seperti log Elastic Load BalancingAWS WAF, log, log perekam, temuan AmazonAWS Config, log audit GuardDuty Amazon Elastic Kubernetes Service (Amazon EKS), dan sistem operasi instans Amazon EC2 dan log aplikasi. Lihat daftar lengkap opsi pencatatan log dan pemantauan di 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 Amazon Service untuk data yang disimpan di OpenSearch 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

AWSsecara 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 di AWS

Konsep dari forensik on-premise tradisional berlaku untuk AWS. Posting blog Forensic investigation environment strategies in the AWS Cloud memberi Anda informasi penting untuk mulai memigrasikan keahlian forensiknya ke AWS.

Setelah lingkungan dan struktur akun AWS Anda disiapkan untuk forensik, Anda sebaiknya menentukan teknologi yang diperlukan agar dapat melakukan metodologi forensik yang sehat secara efektif dalam empat fase:

- Pengumpulan – Mengumpulkan log AWS yang relevan, seperti AWS CloudTrail, AWS Config, Log Alur VPC, dan log tingkat host. Kumpulkan snapshot, cadangan, dan dump memori dari sumber daya AWS yang terkena dampak.
- 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. Di 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 hal 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 posting blog 10 security best practices for securing backups

in AWS untuk panduan tentang 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 di 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 bagian 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,

Domain	Item persiapan	Item tindakan
		akuntabel, terinformasi, berdasarkan konsultasi (RACI) untuk suatu insiden.
Orang	Melatih staf respons insiden tentang AWS.	• Melatih pemangku kepentingan respons insiden tentang fondasi AWS. • Melatih pemangku kepentingan respons insiden tentang layanan keamanan dan pemantauan AWS. • Melatih pemangku kepentingan respons insiden di lingkungan AWS Anda dan bagaimana hal tersebut dirancang.
Orang	Memahami opsi dukungan AWS.	• Memahami perbedaan dalam dukungan AWS, Customer Incident Response Team (CIRT), tim respons DDoS (DRT) dan AMS. • Memahami jalur triase dan eskalasi untuk menghubungi CIRT selama peristiwa 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.	• Mendokumentasikan secara mendetail tentang bagaimana lingkungan AWS Anda dikonfigurasi di seluruh struktur akun, penggunaan layanan, pola IAM, dan fungsionalitas inti lainnya ke konfigurasi AWS Anda. • Mengembangkan diagram arsitektur untuk arsitektur cloud Anda.
Proses	Mengembangkan playbook respons insiden.	• Membuat templat sebagai struktur playbook 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	Mengembangkan struktur akun AWS.	• Merencanakan struktur akun untuk pemisahan beban kerja berdasarkan akun AWS. • 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.	• Merencanakan strategi untuk memberi tag dan tag apa yang ingin Anda kaitkan dengan sumber daya AWS Anda. • Menerapkan dan menegakkan strategi pemberian tag.

Domain	Item persiapan	Item tindakan
Teknologi	Memperbarui informasi kontak akun AWS.	• Memverifikasi bahwa akun AWS memiliki informasi kontak yang terdaftar. • Membuat daftar distribusi email untuk informasi kontak untuk menghapus satu titik kegagalan. • Melindungi akun email yang terkait dengan informasi akun AWS.
Teknologi	Menyiapkan akses ke akun AWS.	• Menentukan apa yang diperlukan oleh responden akses insiden untuk merespons suatu insiden. • Menerapkan, 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 serta mengueri 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	Menentukan apakah peristiwa keamanan merupakan insiden dan menilai cakupan 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	Mengembalikan sistem ke keadaan aman yang diketahui dan memantau 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. Peringatan menghasilkan pemberitahuan untuk memulai proses respons insiden berdasarkan aktivitas yang menarik di akun AWS.

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-pola kejahatan muncul melalui taktik, teknik, dan prosedur (TTP) aktor ancaman baru atau yang dimodifikasi.
- 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 - Layanan AWS 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 — Layanan AWS, infrastruktur, dan log 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 biaya AWS Anda guna 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.

- Kepercayaan dan keamanan AWS – AWS Support dapat menghubungi pelanggan apabila kami mengidentifikasi aktivitas penyalahgunaan atau yang 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 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 akun AWS, yang seharusnya hanya digunakan untuk aktivitas spesifik dan terdefinisi dengan sangat baik. Mereka mengaitkannya dengan kontrol pencegahan yang diterapkan dengan kebijakan kontrol layanan (SCP) organisasi AWS. 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 instans EC2 yang merupakan bagian dari beban kerja. Temuan `Impact:EC2/SuspiciousDomainRequest.Reputation` ini dibuat, menginformasikan Anda bahwa instans Amazon EC2 yang terdaftar dalam beban kerja Anda sedang melakukan kueri terhadap nama domain yang dicurigai berbahaya. Peringatan ini ditetapkan secara default sebagai tingkat keparahan rendah, dan saat fase analisis berlangsung, ditentukan bahwa beberapa ratus instans EC2 jenis `p4d.24xlarge` telah digunakan oleh aktor yang tidak memiliki otorisasi, meningkatkan biaya operasi organisasi tersebut secara signifikan. 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. Sebaliknya, peringatan organisasi berdasarkan temuan tersebut harus disesuaikan tingkat kekritisannya.

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”. Ketika Anda melihat lebih jauh ke dalam dokumentasi, hal 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 pihak penyerang," yang mengindikasikan 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 keamanan. defense-in-depth

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 sebaiknya menggunakan kerangka kerja seperti MITRE ATT&CK untuk memahami taktik, teknik, dan prosedur (TTP) aktor ancaman. Kerangka 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 cakupan, dan menilai dampak dari kemungkinan penyusupan.

- 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 diuntungkan dengan adanya pekerjaan AWS Glue untuk memuat informasi intelijen ancaman dalam bentuk 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 secara 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

Otomatisasi merupakan bagian integral dari tata kelola AWS Cloud. 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 posting blog How to enrich AWS Security Hub findings with account metadata untuk mengetahui contoh penggunaan otomatisasi untuk memperkaya temuan keamanan dan menyederhanakan analisis.

Mengumpulkan dan menganalisis bukti forensik

Forensik, sebagaimana disebutkan di bagian Persiapan dokumen ini, adalah proses mengumpulkan dan menganalisis artefak selama respons insiden. Di AWS, hal 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 menjaga lacak balak 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/bidang kontrol (, peristiwa data Amazon S3CloudTrail, Log Aliran VPC), data (metadata dan objek Amazon S3), dan sumber daya (database, instans Amazon EC2).

Log layanan/bidang kontrol dapat dikumpulkan untuk analisis lokal atau, idealnya, langsung dikueri menggunakan layanan AWS native (jika berlaku). Data (termasuk metadata) dapat langsung dikueri untuk mendapatkan informasi yang relevan atau untuk memperoleh objek sumber; misalnya, gunakan AWS CLI untuk memperoleh bucket Amazon S3 serta metadata objek dan secara langsung memperoleh objek sumber. Sumber daya perlu dikumpulkan dengan cara yang konsisten dengan jenis sumber daya dan metode analisis yang dimaksudkan. Misalnya, basis data dapat dikumpulkan dengan membuat salinan/snapshot dari sistem yang menjalankan basis data, membuat salinan/snapshot dari seluruh basis data itu sendiri, atau mengueri dan mengekstrak data serta log tertentu dari basis data yang relevan dengan penyelidikan.

Untuk instans Amazon EC2, ada set data tertentu yang harus dikumpulkan dan urutan spesifik untuk pengumpulan yang harus dilakukan guna memperoleh dan mempertahankan jumlah data terbanyak untuk analisis dan penyelidikan.

Secara khusus, urutan respons untuk memperoleh dan mempertahankan jumlah data terbanyak dari instans Amazon EC2 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) Melakukan pengumpulan respons langsung/artefak – Lakukan pengumpulan data yang ditargetkan (disk/memori/log) melalui respons langsung pada sistem hanya jika disk atau memori tidak dapat diperoleh, atau jika ada alasan bisnis atau operasional yang valid. Melakukan hal ini akan memodifikasi data sistem dan artefak yang berharga.
6. Menonaktifkan instans – Lepaskan instans dari grup penskalaan otomatis, batalkan register instans dari penyeimbang beban, 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 ke depannya dari instans terhadap lingkungan.
   - Terus jalankan instans dalam lingkungan terisolasi yang diinstrumentasi untuk pemantauan.

     Meskipun tidak direkomendasikan sebagai pendekatan standar, jika suatu situasi memerlukan pengamatan instans secara berkelanjutan (seperti ketika data atau indikator tambahan diperlukan untuk melakukan penyelidikan dan analisis instans secara komprehensif), Anda dapat mempertimbangkan untuk mematikan instans, membuat AMI instans, dan meluncurkan kembali instans tersebut di akun forensik khusus Anda dalam lingkungan sandbox yang telah diinstrumentasi sebelumnya agar sepenuhnya diisolasi dan dikonfigurasi dengan instrumentasi untuk memfasilitasi pemantauan instans secara berkelanjutan (misalnya, Log Alur VPC atau Pencerminan Lalu Lintas VPC).

> **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. NIST SP 800-61 Computer Security

Incident Handling Guide 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)

Namun, mengenai layanan di AWS, langkah-langkah penahanan mendasar dapat dikerucutkan 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.

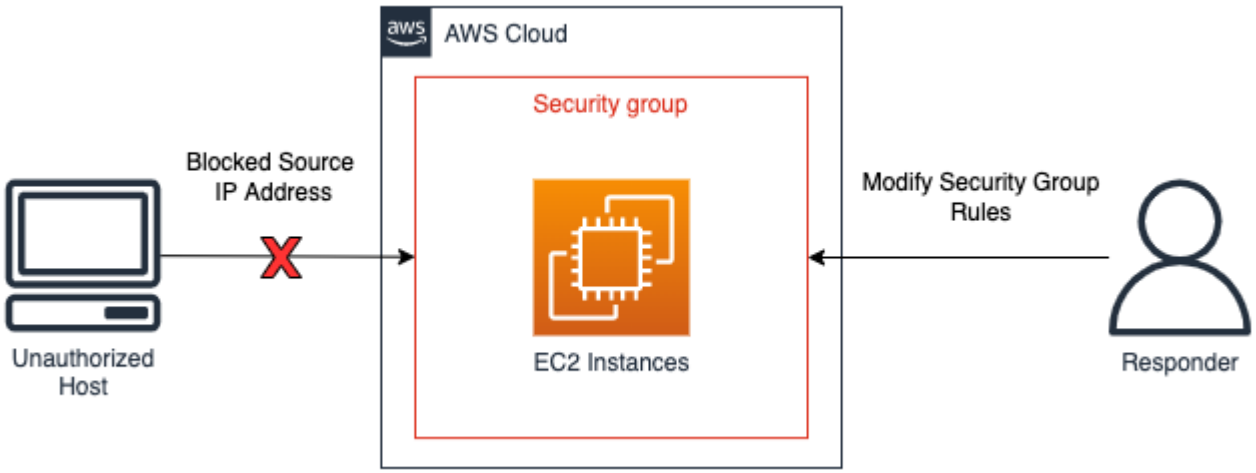
Penahanan sumber

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 layanan AWS disorot di sini:

- Grup keamanan – Membuat dan menerapkan grup keamanan isolasi ke instans Amazon EC2 atau menghapus aturan dari grup keamanan yang ada dapat membantu menahan lalu lintas yang tidak sah ke instans Amazon EC2 atau sumber daya AWS. 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 (ACL web) dapat dikonfigurasi di AWS WAF untuk memberikan kontrol ketat atas permintaan web yang ditanggapi sumber daya. Anda dapat menambahkan alamat IP atau rentang jaringan ke set IP yang dikonfigurasi di 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 ini dengan analis respons insiden yang memodifikasi grup keamanan pada instans Amazon EC2 untuk membatasi koneksi baru hanya untuk 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

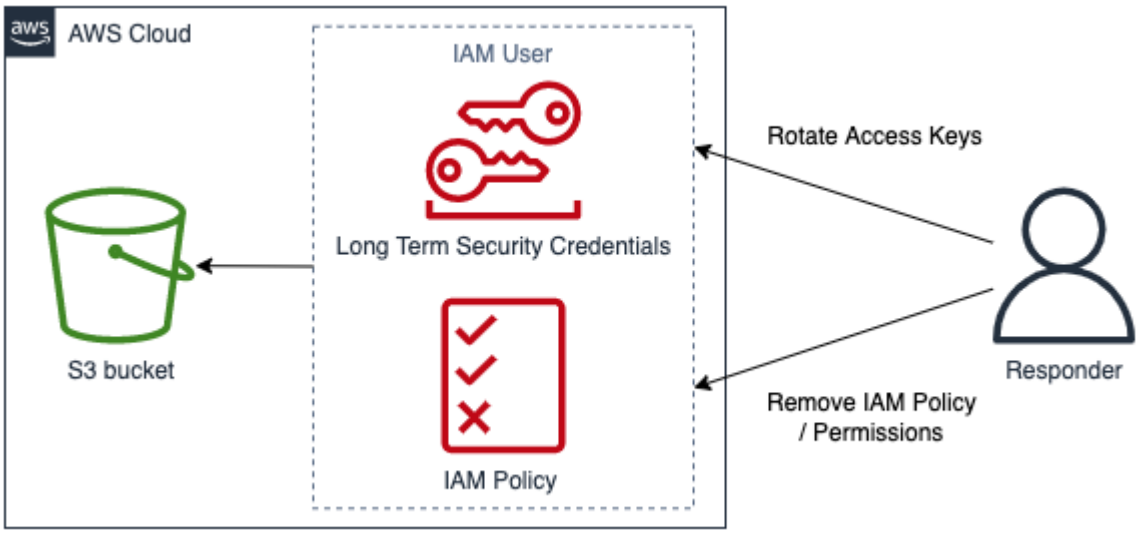
Teknik dan penahanan akses

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 penahanan akses menggunakan layanan AWS 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. Hal 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 kredensial statis jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI atau API AWS 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 kredensial keamanan sementara – Kredensial keamanan sementara dapat digunakan oleh organisasi untuk mengontrol akses ke sumber daya AWS dan dimulai dengan awalan ASIA (untuk informasi tambahan, lihat bagian Memahami awalan ID unik di pengidentifikasi 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 dan buat ulang pengguna IAM dengan kunci akses yang disusupi.
- AWS WAF - Teknik tertentu yang digunakan oleh pengguna yang tidak diotorisasi termasuk pola lalu lintas berbahaya yang umum, seperti permintaan yang berisi injeksi SQL dan pembuatan skrip lintas situs (XSS). AWS WAF dapat dikonfigurasi untuk mencocokkan dan menolak lalu lintas dengan menerapkan teknik ini menggunakan pernyataan aturan bawaan AWS WAF.

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

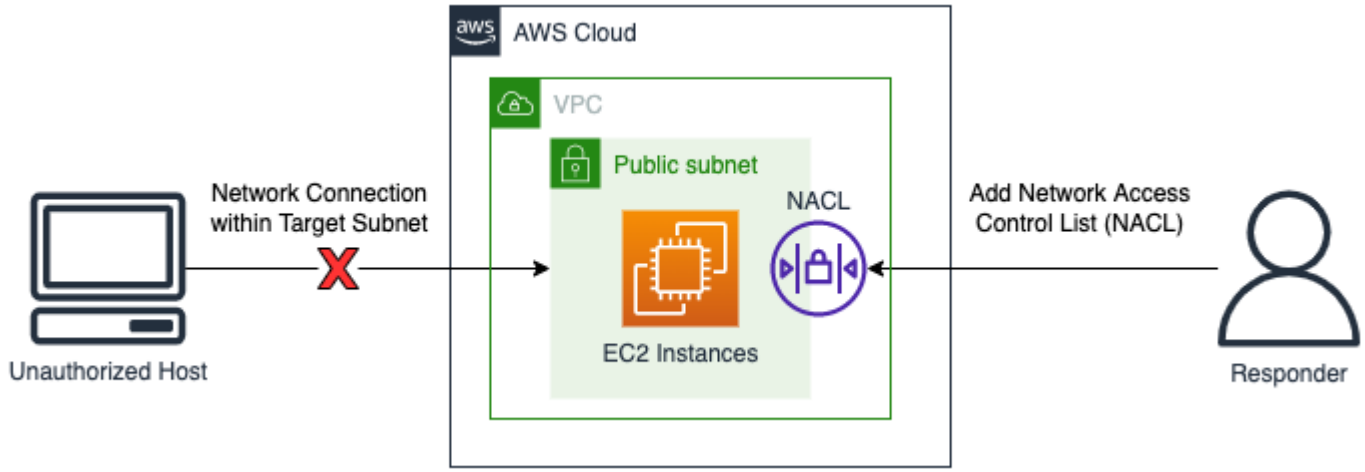
Penahanan tujuan adalah aplikasi penyaringan atau perutean dalam suatu lingkungan untuk mencegah akses ke host atau sumber daya yang ditargetkan. Dalam beberapa kasus, penahanan tujuan juga melibatkan suatu bentuk ketahanan untuk memverifikasi bahwa sumber daya yang sah direplikasi untuk ketersediaan;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

- ACL Jaringan – ACL jaringan (NACL) yang dikonfigurasi pada subnet yang berisi sumber daya AWS dapat ditambahkan dengan aturan penolakan. Aturan penolakan ini dapat diterapkan untuk mencegah akses ke sumber daya AWS tertentu; tetapi, menerapkan NACL akan memengaruhi setiap sumber daya di subnet, tidak hanya sumber daya yang diakses tanpa otorisasi. Aturan yang tercantum dalam NACL diproses dalam urutan top-down, sehingga aturan pertama dalam NACL

yang ada harus dikonfigurasi untuk menolak lalu lintas yang tidak sah ke sumber daya dan subnet yang ditargetkan. Sebagai alternatif, NACL yang benar-benar baru dapat dibuat dengan aturan penolakan tunggal untuk lalu lintas masuk dan keluar dan dikaitkan dengan subnet yang berisi sumber daya yang ditargetkan untuk mencegah akses ke subnet menggunakan NACL 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.
- VPC Isolasi – VPC isolasi dapat digunakan untuk menyediakan penahanan sumber daya yang efektif sambil menyediakan akses ke lalu lintas yang sah (seperti solusi anti-virus (AV) atau EDR yang memerlukan akses ke internet atau konsol manajemen eksternal). VPC isolasi dapat dikonfigurasikan terlebih dahulu sebelum peristiwa keamanan untuk mengizinkan alamat IP dan port yang valid, dan sumber daya yang ditargetkan dapat segera dipindahkan ke dalam VPC isolasi ini selama peristiwa keamanan aktif untuk menahan sumber daya sambil memungkinkan lalu lintas yang sah dikirim dan diterima oleh sumber daya yang ditargetkan selama fase respons insiden berikutnya. Aspek penting dalam menggunakan VPC isolasi adalah sumber daya, seperti instans EC2, harus dimatikan dan diluncurkan kembali di VPC isolasi yang baru sebelum digunakan. Instans EC2 yang ada tidak dapat dipindahkan ke VPC atau Zona Ketersediaan lainnya. Untuk melakukannya, ikuti langkah-langkah yang diuraikan dalam Bagaimana cara memindahkan instans Amazon EC2 saya ke subnet, Zona Ketersediaan, atau VPC lainnya?
- Grup penskalaan otomatis dan penyeimbang beban – Sumber daya AWS yang terlampir pada grup penskalaan otomatis dan penyeimbang beban harus dilepas dan dideregistrasi sebagai bagian dari prosedur penahanan tujuan. Pelepasan dan deregistrasi sumber daya AWS dapat dilakukan menggunakan AWS Management Console, AWS CLI, dan AWS SDK.

Contoh penahanan tujuan ditunjukkan pada diagram berikut dengan analis respons insiden yang menambahkan NACL 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 sumber daya AWS, 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 instans Amazon EC2 untuk alasan peraturan, kepatuhan, atau hukum, buat snapshot Amazon EBS sebelum menghapus instans tersebut.

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

Setelah Anda memberantas sumber daya terpengaruh yang teridentifikasi, AWS menyarankan 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 munculnya kembali 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 menerapkan ulang dari sumber tepercaya menggunakan otomatisasi, terkadang di akun AWS yang baru.
- 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 • 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 peningkatan berkelanjutan adalah melakukan iterasi pada hasil insiden dan simulasi untuk meningkatkan kemampuan Anda agar dapat 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 peningkatan 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?

- Bagaimana garis waktu untuk implementasi dan pengujian kontrol/proses pemantauan/preventif tambahan?

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 yang disebutkan sebelumnya, persiapan adalah kunci untuk respons yang efektif. Lihat bagian 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 kerusakan lebih lanjut dari penyerang atau sistem yang disusupi.

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 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
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

Metrik	Deskripsi
Waktu tinggal penyerang	Waktu rata-rata pengguna yang tidak sah memiliki akses ke sistem atau lingkungan

Menggunakan indikator penyusupan (IOC)

Indikator penyusupan (IOC) adalah artefak yang diamati di dalam atau pada jaringan, sistem, atau lingkungan yang dapat (dengan tingkat kepercayaan tinggi) mengidentifikasi aktivitas berbahaya atau insiden keamanan. IOC dapat muncul dalam berbagai bentuk, termasuk alamat IP, domain, artefak tingkat jaringan seperti bendera TCP atau payload, artefak sistem atau tingkat host seperti file eksekusi, 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.

Seiring dengan upaya Anda untuk meningkatkan program tanggap insiden secara iteratif, Anda harus menerapkan kerangka kerja untuk mengumpulkan, mengelola, dan menggunakan IOC sebagai mekanisme untuk terus membangun dan meningkatkan pendeteksian dan peringatan, serta meningkatkan kecepatan dan keampuhan penyelidikan. Anda dapat memulai dengan memasukkan pengumpulan dan pengelolaan IOC ke dalam fase analisis dan investigasi proses respons insiden Anda. Dengan mengidentifikasi, mengumpulkan, dan menyimpan IOC secara proaktif 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 sudah ada, membangun deteksi dan peringatan tambahan, mengidentifikasi di mana dan kapan sebuah artefak terlihat sebelumnya, membuat dan mereferensikan dokumentasi tentang bagaimana investigasi yang pernah dilakukan yang melibatkan pencocokan IOC, dan masih banyak lagi.

Terus melakukan pendidikan dan pelatihan

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 dalam mendeteksi, merespons, dan menyelidiki insiden dalam 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 awal di atas meja 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

Dalam perjalanan cloud Anda, penting bagi Anda untuk mempertimbangkan konsep respons insiden keamanan yang mendasar untuk lingkungan AWS 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, Senior Security Consultant, Amazon Web Services
- Jonathon Poling, Principal Security Consultant, Amazon Web Services
- Josh Du Lac, Senior Manager, Security Solutions Architecture, Amazon Web Services
- Paco Hope, Principal Security Consultant, Amazon Web Services
- Ryan Tick, Senior Security Engineer, Amazon Web Services
- Steve de Vera, Senior Security Consultant, 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 subset dari layanan yang paling relevan dengan respons insiden di cloud.

Topik

Pencatatan log dan peristiwa

AWS CloudTrail – Layanan AWS CloudTrail yang memungkinkan tata kelola, kepatuhan, audit operasional, dan audit risiko akun AWS. Anda dapat CloudTrail menggunakan data log yang dilakukan berdasarkan sumber daya AWS Anda, dengan mengirim pesan untuk merespons lingkungan Anda, membuat perubahan pada sumber daya AWS Anda. CloudTrail Kegiatan manajemen memberikan visibilitas ke dalam operasi manajemen yang dilakukan AWS Management Console berdasarkan sumber daya AWS Anda, serta layanan AWS Anda. 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 memberikan visibilitas ke dalam operasi manajemen memberikan visibilitas ke dalam sumber daya di akun AWS Anda. Hal ini termasuk tindakan seperti membuat bucket Amazon S3 dan menyiapkan pencatatan.
- CloudTrail Peristiwa manajemen memberikan visibilitas ke dalam operasi sumber daya yang dilakukan berdasarkan sumber daya 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.

Amazon CloudWatch CloudWatch CloudTrick memberikan visibilitas ke dalam operasi yang dilakukan berdasarkan AWS AWS CloudTrail sumber daya di akun AWS Anda. Dengan menggunakan aturan sederhana yang dapat Anda siapkan dengan cepat, Anda dapat mencocokkan kejadian dan merutekannya ke satu atau beberapa fungsi atau pengaliran target. CloudWatch CloudTroudTrent menjadi sadar akan perubahan operasional yang terjadi. CloudWatch CloudTrents merespons perubahan operasional ini dan mengambil tindakan korektif yang diperlukan, dengan mengirim pesan untuk merespons lingkungan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan, membuat perubahan Beberapa layanan keamanan, seperti Amazon GuardDuty, menghasilkan output mereka dalam bentuk CloudWatch Acara. Banyak layanan keamanan juga menyediakan opsi untuk mengirim output-nya ke Amazon S3.

AWS Config – AWS Config adalah layanan yang memungkinkan pelanggan menilai, mengaudit, dan mengevaluasi konfigurasi sumber daya AWS Anda. AWS Config terus memantau dan mencatat konfigurasi sumber daya AWS Anda dan memungkinkan Anda untuk mengotomatiskan evaluasi konfigurasi yang tercatat terhadap konfigurasi yang diinginkan. Dengan AWS Config, pelanggan dapat meninjau perubahan konfigurasi dan hubungan antara sumber daya AWS, secara manual atau otomatis, riwayat konfigurasi sumber daya yang mendetail, 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.

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 instans Amazon EC2 dengan CloudWatch agen Log. CloudWatch Log dapat menjadi tujuan untukAWS CloudTrail, Kueri DNS Route 53, Log Aliran VPC, fungsi Lambda, dan lainnya. Anda kemudian dapat mengambil data log terkait dari CloudWatch CloudTroudTroudTrick.

Log Alur VPC Amazon – Log Alur VPC memungkinkan pelanggan untuk menangkap informasi tentang lalu lintas IP ke dan dari antarmuka jaringan di VPC. data log alur dapat dipublikasikan ke Amazon CloudTroudTrick, Amazon CloudTrick, Amazon CloudWatch CloudTrick, dan Amazon S3. Log Alur VPC membantu pelanggan dengan sejumlah tugas seperti pemecahan masalah lalu lintas tertentu yang tidak mencapai instans, mendiagnosis aturan grup keamanan yang terlalu ketat, dan menggunakannya sebagai alat keamanan untuk memantau lalu lintas ke instans EC2. Gunakan pencatatan alur VPC versi terbaru untuk mendapatkan bidang yang paling kuat.

Log AWS WAF – 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 instans Amazon EC2, fungsi AWS Lambda, atau kontainer, jika berada di Amazon VPC Anda dan membuat kueri DNS, fitur ini akan mencatatnya; Anda kemudian dapat menjelajahi dan lebih memahami bagaimana aplikasi Anda beroperasi.

Log AWS lainnya – AWS terus merilis fitur dan kemampuan layanan untuk pelanggan dengan kemampuan pencatatan dan pemantauan baru. Untuk informasi tentang fitur yang tersedia untuk setiap layanan AWS, 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. AWS Security Hub memungkinkan pengguna untuk melihat temuan keamanan dari layanan AWS seperti Amazon Inspector, serta solusi Partner AWS seperti Amazon Inspector, serta solusi Partner AWS seperti Amazon Inspector, serta solusi Partner AWS seperti Amazon GuardDuty Inspector, serta solusi Partner AWS. 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 terbaik AWS dan standar industri yang diikuti organisasi Anda.

Amazon GuardDuty — Amazon GuardDuty adalah layanan deteksi ancaman terkelola yang terus memantau perilaku berbahaya atau tidak sah untuk membantu pelanggan melindungi akun dan

beban kerja AWS. Layanan ini memantau aktivitas seperti panggilan API yang tidak biasa atau deployment yang berpotensi tidak sah yang menunjukkan kemungkinan pembobolan akun atau sumber daya instans Amazon EC2, bucket Amazon S3, atau pengintaian oleh pihak yang tidak bertanggung jawab.

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. Anda dapat menggunakan GuardDuty CloudTroudTrate CloudTrate untuk mengumpulkan sumber daya AWS Anda. 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 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 – Aturan AWS Config mewakili konfigurasi pilihan 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 aturan AWS Config, 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 mematuhi aturan.

AWS Trusted Advisor – AWS Trusted Advisor adalah sumber daya online untuk membantu Anda mengurangi biaya, meningkatkan kinerja, dan memperketat keamanan dengan mengoptimalkan lingkungan AWS Anda. Trusted Advisor memberikan panduan waktu nyata untuk membantu penyediaan sumber daya Anda dengan mengikuti praktik terbaik AWS. Set lengkap Trusted Advisor pemeriksaan, termasuk integrasi CloudWatch Acara, tersedia untuk pelanggan paket dukungan Bisnis dan Perusahaan.

Amazon CloudWatch — Amazon CloudWatch adalah layanan pemantauan untuk AWS Cloud sumber daya dan aplikasi yang Anda jalankan di AWS. Anda dapat menggunakan file log, CloudWatch membuat perubahan pada sumber daya AWS Anda dapat menggunakan file log, membuat perubahan, dan secara otomatis bereaksi terhadap perubahan pada sumber daya AWS Anda. CloudWatch Anda dapat menggunakan file log apa pun yang dihasilkan oleh aplikasi dan layanan AWS seperti Amazon Inspector, serta solusi Partner AWS seperti Amazon Inspector, serta solusi Partner AWS seperti Amazon Inspector, serta instans DB, Amazon DB;, serta instans DB;, serta instans DB;, serta metrik kustom yang dihasilkan oleh aplikasi dan layanan AWS seperti Amazon Inspector, serta solusi Partner AWS seperti Amazon Inspector, serta solusi Partner AWS seperti instans DB. Anda dapat menggunakan CloudWatch CloudTroudTrate memberikan visibilitas di seluruh sistem ke dalam pemanfaatan sumber daya, kinerja aplikasi, dan kesehatan operasi Anda. Anda dapat menggunakan wawasan ini untuk bereaksi dengan tepat dan menjaga aplikasi Anda tetap berjalan dengan lancar.

Amazon Inspector – Amazon Inspector adalah layanan penilaian keamanan otomatis yang membantu meningkatkan keamanan dan kepatuhan aplikasi yang di-deploy di 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 sumber daya AWS Anda dan menggunakan machine learning, analisis statistik, dan teori grafik untuk membangun kumpulan data tertaut yang memungkinkan Anda melakukan investigasi keamanan yang lebih cepat dan 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 nirserver yang menjalankan kode Anda sebagai respons terhadap peristiwa, dan secara otomatis mengelola sumber daya komputasi yang

mendasarinya untuk Anda. Anda dapat menggunakan Lambda untuk memperluas layanan AWS lainnya dengan logika kustom, atau membuat layanan backend Anda sendiri yang beroperasi dalam skala, performa, dan keamanan AWS. 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 memudahkan untuk mengoordinasikan komponen-komponen aplikasi terdistribusi dan layanan mikro 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 Serverless, dan membuatnya mudah untuk mengorkestrasi fungsi AWS Lambda untuk aplikasi nirserver. Anda juga dapat menggunakan Step Functions untuk orkestrasi layanan mikro menggunakan sumber daya komputasi seperti Amazon EC2 dan Amazon ECS.

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 dengan mudah dan berinovasi lebih cepat. AWS Step Functions adalah bagian dari platform AWS Serverless, dan membuatnya mudah untuk mengorkestrasi fungsi AWS Lambda untuk aplikasi nirserver. Anda juga dapat menggunakan Step Functions untuk orkestrasi layanan mikro menggunakan sumber daya komputasi seperti Amazon EC2 dan Amazon ECS.

AWS Systems Manager – AWS Systems Manager memberi Anda visibilitas dan kontrol atas infrastruktur Anda di AWS. Systems Manager menyediakan antarmuka pengguna terpadu sehingga Anda dapat melihat data operasional dari beberapa layanan AWS, dan memungkinkan Anda untuk mengotomatiskan tugas operasional di seluruh sumber daya AWS Anda. 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. Layanan ini memberikan keleluasaan bagi pelanggan untuk memilih metode untuk pengelolaan 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, partner integrator sistem, dan layanan AWS lainnya.

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.

Kustom

Layanan dan fitur yang disebutkan di atas bukanlah daftar lengkap. AWS terus menambahkan kemampuan baru. Untuk informasi selengkapnya, sebaiknya kunjungi halaman Apa yang Baru di AWS dan AWS Cloud Security. Selain layanan keamanan yang ditawarkan AWS sebagai layanan cloud native, Anda mungkin tertarik untuk membangun kemampuan Anda sendiri di atas layanan AWS.

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 ditawarkan AWS, Anda bisa melakukan hal-hal tersebut dengan begitu mudah. Ada banyak layanan AWS tambahan yang dapat membantu Anda melakukan 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 insiden AWS

AWS menerbitkan sumber daya untuk membantu pelanggan mengembangkan kemampuan respons insiden. Sebagian besar contoh kode dan prosedur dapat ditemukan di repositori GitHub publik eksternal AWS. Berikut ini adalah beberapa sumber daya yang memberikan contoh cara melakukan respons insiden.

Sumber daya playbook

- Framework for Incident Response Playbooks - Kerangka kerja contoh bagi pelanggan untuk membuat, mengembangkan, dan mengintegrasikan pedoman keamanan sebagai persiapan untuk skenario serangan potensial saat menggunakan layanan AWS.
- Develop your own Incident Response Playbooks - Lokakarya ini dirancang untuk membantu Anda makin memahami pengembangan playbook respons insiden untuk AWS.
- Incident Response Playbook Samples - Playbook yang membahas skenario umum yang dihadapi oleh pelanggan AWS.
- Membangun runbook respons insiden AWS menggunakan buku pedoman Jupyter dan CloudTrail Lake - Lokakarya ini memandu Anda membuat buku pedoman respons insiden untuk lingkungan AWS Anda menggunakan notebook Jupyter dan Lake. CloudTrail

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. Solusi ini memanfaatkan fungsi AWS Lambda untuk memicu proses respons insiden dengan cara yang dapat diulang secara otomatis. Hal ini menyediakan segregasi akun untuk mengoperasikan langkah-langkah otomatisasi, menyimpan artefak, dan menciptakan lingkungan forensik.
- Orkestrator Forensik Otomatis untuk Amazon EC2 – Panduan implementasi ini menyediakan solusi swalayan untuk menangkap dan memeriksa data dari instans EC2 dan volume terlampir untuk analisis forensik jika terjadi potensi masalah keamanan yang terdeteksi. Ada CloudFormation template AWS untuk menerapkan solusi.
- Cara mengotomatiskan pengumpulan disk forensik di AWS – Blog AWS ini memerinci cara menyiapkan alur kerja otomatisasi untuk menangkap bukti disk untuk analisis guna menentukan

cakupan dan dampak potensi insiden keamanan. Ada juga CloudFormation template AWS yang disertakan untuk menerapkan solusi.

Revisi dokumen

Untuk mengetahui jika ada perubahan pada laporan resmi ini, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Pembaruan kecil	Beberapa perubahan dan penambahan untuk mengembangkan panduan.	11 Mei 2023
Revisi besar	Hampir semua konten diganti agar lebih selaras dengan standar industri, seperti NIST. Panduan preskriptif tambahan tentang cara mempersiapkan dan merespons peristiwa keamanan di lingkungan AWS.	1 Januari 2023
Pembaruan kecil	Perbaikan bug dan berbagai perubahan kecil.	1 April 2022
Pembaruan kecil	Perbaikan bug dan berbagai perubahan kecil.	2 Juni 2021
Pembaruan kecil	Perbaikan tautan yang rusak.	5 Maret 2021
Laporan resmi diperbarui	Perbaikan berbagai tautan yang rusak dan banyak perubahan pada teks untuk meningkatkan keterbacaan.	23 November 2020
Pembaruan kecil	Memperbaiki tautan ke "Respons Insiden dengan Konsol AWS dan CLI".	30 Juni 2020
Laporan resmi diperbarui	Diperbarui dengan layanan keamanan baru, intelijen	11 Juni 2020

	ancaman, tanggung jawab bersama untuk kontainer , otomatisasi, dan CCPA. Menambahkan lampiran dengan contoh pohon keputusan dan runbook.	
Publikasi awal	Pertama kali laporan resmi dipublikasikan	1 Juni 2019

Pemberitahuan

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

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