Konsep dan Prosedur Deteksi Insiden dan Respons AWS

Panduan Pengguna Deteksi dan Respons Insiden AWS

Versi May 26, 2026

Panduan Pengguna Deteksi dan Respons Insiden AWS: Konsep dan Prosedur Deteksi Insiden dan Respons AWS

Table of Contents

Apa itu Deteksi dan Respons Insiden AWS?

AWS Incident Detection and Response menawarkan keterlibatan insiden proaktif kepada pelanggan Dukungan AWS Perusahaan yang memenuhi syarat untuk mengurangi potensi kegagalan dan mempercepat pemulihan beban kerja kritis dari gangguan. Deteksi dan Respons Insiden memfasilitasi kolaborasi Anda AWS untuk mengembangkan runbook dan rencana respons yang disesuaikan dengan setiap beban kerja yang terpasang.

Deteksi dan Respons Insiden menawarkan fitur-fitur utama berikut:

- Peningkatan observabilitas: AWS para ahli memberikan panduan untuk membantu Anda menentukan dan mengkorelasikan metrik dan alarm antara lapisan aplikasi dan infrastruktur beban kerja Anda untuk mendeteksi gangguan lebih awal.
- Waktu respons 5 menit: Insinyur Manajemen Insiden secara proaktif melibatkan Anda dalam waktu 5 menit setelah alarm, dari beban kerja Anda, atau sebagai tanggapan atas kasus kritis yang Anda kirimkan.
- Resolusi lebih cepat: IME menggunakan runbook yang telah ditentukan sebelumnya dan khusus yang dikembangkan untuk beban kerja Anda, membuat kasus Support atas nama Anda, dan mengelola insiden pada beban kerja Anda. IME menyediakan kepemilikan single-threaded untuk insiden dan membuat Anda tetap terlibat dengan AWS ahli yang tepat sampai insiden diselesaikan.
- Mengurangi potensi kegagalan: Setelah resolusi, IME memberi Anda tinjauan pasca-insiden (berdasarkan permintaan). Dan, AWS para ahli bekerja dengan Anda untuk menerapkan pelajaran yang dipetik untuk meningkatkan rencana respons insiden dan runbook. Anda juga dapat memanfaatkan AWS Resilience Hub pelacakan ketahanan berkelanjutan pada beban kerja Anda.

Topik

Mendaftar untuk Akun AWS

Untuk memulai AWS, Anda membutuhkan Akun AWS. Untuk informasi tentang membuat Akun AWS, lihat Memulai dengan Akun AWS di Panduan AWS Account Management Referensi.

Ketentuan Penggunaan untuk Deteksi dan Respon Insiden

Daftar berikut menguraikan persyaratan dan batasan utama untuk menggunakan AWS Incident Detection and Response. Informasi ini penting untuk Anda pahami sebelum menggunakan layanan, karena mencakup aspek-aspek seperti persyaratan rencana dukungan, proses orientasi, dan durasi berlangganan minimum.

- AWS Incident Detection and Response tersedia untuk akun langsung dan Partner-resold Enterprise Support.
- Deteksi dan Respons Insiden AWS tidak tersedia untuk akun di Partner Led Support.
- Anda harus mempertahankan AWS Enterprise Support setiap saat selama jangka waktu layanan Deteksi dan Respons Insiden Anda. Untuk selengkapnya, lihat Dukungan Perusahaan. Pengakhiran Dukungan Perusahaan menghasilkan penghapusan secara bersamaan dari layanan AWS Incident Detection and Response.
- Semua beban kerja pada AWS Incident Detection and Response harus melalui proses orientasi beban kerja.
- Durasi minimum untuk berlangganan akun AWS Incident Detection and Response adalah sembilan puluh (90) hari. Semua permintaan pembatalan harus diajukan tiga puluh (30) hari sebelum tanggal efektif pembatalan yang dimaksudkan.
- AWS menangani informasi Anda seperti yang dijelaskan dalam Pemberitahuan AWS Privasi.

> **Note**
>
> Untuk pertanyaan terkait Deteksi Insiden dan penagihan Respons, lihat Mendapatkan bantuan terkait AWS Penagihan.

Arsitektur Deteksi dan Respon Insiden

AWS Incident Detection and Response terintegrasi dengan lingkungan Anda yang ada seperti yang ditunjukkan pada grafik berikut. Arsitektur mencakup layanan berikut:

- Amazon EventBridge: Amazon EventBridge berfungsi sebagai satu-satunya titik integrasi antara beban kerja Anda dan Deteksi dan Respons Insiden AWS. Alarm dicerna dari alat pemantauan Anda, seperti Amazon, melalui Amazon CloudWatch EventBridge menggunakan aturan yang telah ditentukan yang dikelola oleh. AWS Untuk mengizinkan Deteksi dan Respons Insiden membangun dan mengelola EventBridge aturan, Anda menginstal peran terkait layanan. Untuk mempelajari selengkapnya tentang layanan ini, lihat Apa itu EventBridge aturan Amazon EventBridge dan Amazon, Apa itu Amazon CloudWatch, dan Menggunakan peran terkait layanan. AWS Health
- AWS Health: AWS Health memberikan visibilitas berkelanjutan ke kinerja sumber daya Anda dan ketersediaan akun Anda Layanan AWS . Deteksi dan Respons Insiden digunakan AWS Health untuk melacak peristiwa yang Layanan AWS digunakan oleh beban kerja Anda dan untuk memberi tahu Anda ketika peringatan telah diterima dari beban kerja Anda. Untuk mempelajari lebih lanjut tentang AWS Health, lihat Apa itu AWS Health.
- AWS Systems Manager Systems Manager menyediakan antarmuka pengguna terpadu untuk otomatisasi dan manajemen tugas di seluruh AWS sumber daya Anda. AWS Incident Detection and Response menyimpan informasi tentang beban kerja Anda termasuk detail arsitektur beban kerja, detail alarm, dan runbook manajemen insiden terkait dalam AWS Systems Manager dokumen (untuk detailnya, lihat AWS Systems Manager Dokumen). Untuk mempelajari lebih lanjut tentang AWS Systems Manager, lihat Apa itu AWS Systems Manager.
- Runbook spesifik Anda: Runbook manajemen insiden menentukan tindakan yang dilakukan AWS Incident Detection and Response selama manajemen insiden. Runbook spesifik Anda memberi tahu Deteksi dan Respons Insiden AWS siapa yang harus dihubungi, cara menghubungi mereka, dan informasi apa yang harus dibagikan.

Peran dan tanggung jawab dalam Deteksi dan Respons Insiden

Tabel AWS Incident Detection and Response RACI (Responsible, Accountable, Consulted, and Informed) menguraikan peran dan tanggung jawab untuk berbagai aktivitas yang terkait dengan deteksi dan respons insiden. Tabel ini membantu menentukan keterlibatan pelanggan dan tim Deteksi dan Respons Insiden AWS untuk tugas-tugas seperti pengumpulan data, tinjauan kesiapan operasi, konfigurasi akun, manajemen insiden, dan peninjauan pasca-insiden.

Aktivitas	Pelanggan	Deteksi dan Respon Insiden
Pengumpulan data		
Pengenalan pelanggan dan beban kerja	Dikonsultasikan	Bertanggung jawab
Arsitektur	Bertanggung jawab	Bertanggung jawab
Operasi	Bertanggung jawab	Bertanggung jawab
Tentukan CloudWatch alarm yang akan dikonfigurasi	Bertanggung jawab	Bertanggung jawab
Tentukan rencana respons insiden	Bertanggung jawab	Bertanggung jawab
Tinjauan kesiapan operasi		
Melakukan tinjauan yang dirancang dengan baik (WAR) pada beban kerja	Dikonsultasikan	Bertanggung jawab
Validasi respons insiden	Dikonsultasikan	Bertanggung jawab
Validasi matriks alarm	Dikonsultasikan	Bertanggung jawab
Identifikasi AWS layanan utama yang digunakan oleh beban kerja	Bertanggung jawab	Bertanggung jawab
Konfigurasi akun		

Aktivitas	Pelanggan	Deteksi dan Respon Insiden
Buat peran IAM di akun pelanggan	Bertanggung jawab	Diinformasikan
Instal EventBridge aturan terkelola menggunakan peran yang dibuat	Diinformasikan	Bertanggung jawab
Uji alarm onboard (atau APM) CloudWatch	Bertanggung jawab	Diinformasikan
Verifikasi bahwa alarm pelanggan melibatkan deteksi dan respons insiden	Diinformasikan	Bertanggung jawab
Perbarui alarm	Bertanggung jawab	Dikonsultasikan
Perbarui runbook	Dikonsultasikan	Bertanggung jawab
Manajemen insiden		
Secara proaktif memberi tahu Insiden yang terdeteksi oleh Deteksi dan Respons Insiden	Diinformasikan	Bertanggung jawab
Berikan respon insiden	Diinformasikan	Bertanggung jawab
Memberikan resolusi insiden/pemulihan infrastruktur	Bertanggung jawab	Dikonsultasikan
Post-incident ulasan		
Minta peninjauan pasca-insiden	Bertanggung jawab	Diinformasikan

Aktivitas	Pelanggan	Deteksi dan Respon Insiden
Berikan tinjauan pasca-insiden	Diinformasikan	Bertanggung jawab

Ketersediaan wilayah untuk Deteksi dan Respons Insiden

AWS Incident Detection and Response tersedia dalam bahasa Inggris, Jepang, Mandarin, dan Korea untuk akun Enterprise AWS Support yang dihosting di salah satu dari berikut ini: Wilayah AWS

Wilayah AWS	Nama
Wilayah US East (N. Virginia)	us-east-1
Wilayah US East (Ohio)	us-east-2
Wilayah US West (N. California)	us-west-1
Wilayah US West (Oregon)	us-west-2
Wilayah Kanada (Pusat)	ca-central-1
Wilayah Kanada Barat (Calgary)	ca-west-1
Wilayah Amerika Selatan (Sao Paulo)	sa-east-1
Wilayah Eropa (Frankfurt)	eu-central-1
Wilayah Eropa (Irlandia)	eu-west-1
Wilayah Eropa (London)	eu-west-2
Wilayah Eropa (Paris)	eu-west-3
Wilayah Eropa (Stockholm)	eu-north-1

Wilayah AWS	Nama
Wilayah Eropa (Zürich)	eu-central-2
Wilayah Eropa (Milan)	eu-south-1
Wilayah Eropa (Spanyol)	eu-south-2
Asia Pasifik (Mumbai)	ap-south-1
Asia Pasifik (Tokyo)	ap-northeast-1
Asia Pasifik (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pasifik (Hong Kong)	ap-east-1
Asia Pacific (Osaka)	ap-northeast-3
Asia Pasifik (Hyderabad)	ap-south-2
Asia Pasifik (Jakarta)	ap-southeast-3
Asia Pacific (Melbourne)	ap-southeast-4
Asia Pasifik (Malaysia)	ap-southeast-5
Africa (Cape Town)	af-south-1
Israel (Tel Aviv)	il-central-1
Timur Tengah (UAE)	me-central-1
Timur Tengah (Bahrain)	me-south-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1

Memulai Deteksi dan Respons Insiden

Beban kerja dan alarm merupakan pusat Deteksi dan Respons Insiden AWS. AWS bekerja sama dengan Anda untuk menentukan dan memantau beban kerja tertentu yang penting untuk bisnis Anda. AWS membantu Anda mengatur alarm yang memberi tahu tim Anda tentang masalah kinerja yang signifikan atau dampak pelanggan. Alarm yang dikonfigurasi dengan benar sangat penting untuk pemantauan proaktif dan respons insiden yang cepat dalam Deteksi dan Respons Insiden.

Tentang beban kerja di Deteksi dan Respons Insiden

Anda dapat memilih beban kerja tertentu untuk pemantauan dan manajemen insiden kritis menggunakan AWS Incident Detection and Response. Beban kerja adalah kumpulan sumber daya dan kode yang bekerja sama untuk memberikan nilai bisnis. Beban kerja mungkin semua sumber daya dan kode yang membentuk portal pembayaran perbankan Anda atau sistem manajemen hubungan pelanggan (CRM). Anda dapat meng-host beban kerja dalam satu Akun AWS atau beberapa Akun AWS.

Misalnya, Anda mungkin memiliki aplikasi monolitik yang dihosting dalam satu akun (misalnya, Aplikasi Kinerja Karyawan dalam diagram berikut). Atau, Anda mungkin memiliki aplikasi (misalnya, Webapp Storefront dalam diagram) dipecah menjadi layanan mikro yang membentang di berbagai akun. Beban kerja mungkin berbagi sumber daya, seperti database, dengan aplikasi atau beban kerja lain, seperti yang ditunjukkan pada diagram berikut.

Untuk memulai dengan orientasi beban kerja, lihat. Beban kerja onboard untuk Deteksi dan Respons Insiden

Tentang alarm dalam Deteksi dan Respon Insiden

Alarm adalah bagian penting dari Deteksi dan Respons Insiden. Alarm memberikan visibilitas ke kinerja aplikasi Anda dan infrastruktur yang mendasarinya AWS . AWS bekerja dengan Anda untuk menentukan metrik dan ambang alarm yang sesuai yang hanya memicu ketika ada dampak penting pada beban kerja Anda yang dipantau. Tujuannya adalah agar alarm dapat melibatkan resolver yang Anda tentukan, yang kemudian berkolaborasi dengan tim manajemen insiden untuk mengurangi masalah dengan cepat. Konfigurasikan alarm Anda untuk hanya memasukkan status Alarm ketika ada penurunan kinerja atau pengalaman pelanggan yang signifikan yang memerlukan perhatian segera. Beberapa jenis alarm utama termasuk alarm yang menunjukkan dampak bisnis, CloudWatch kenari Amazon, dan alarm agregat yang memantau dependensi.

Untuk memulai dengan menelan alarm, lihat. Alarm Tertelan

Beban kerja onboard untuk Deteksi dan Respons Insiden

AWS Incident Detection and Response memungkinkan pemantauan dan manajemen insiden kritis untuk beban kerja yang Anda pilih. Beban kerja adalah kumpulan sumber daya yang bekerja sama untuk memberikan nilai bisnis, seperti portal pembayaran atau sistem manajemen hubungan pelanggan (CRM). Anda dapat meng-host beban kerja ini dalam satu Akun AWS atau didistribusikan di beberapa akun, tergantung pada arsitektur Anda.

Daftar Isi

Onboard untuk Deteksi dan Respons Insiden dengan CLI IDR

AWS Incident Detection and Response Customer Command Line Interface (IDR CLI) adalah alat antarmuka baris perintah yang menyederhanakan orientasi ke AWS Incident Detection and Response.

IDR CLI berjalan AWS CloudShell untuk menjalankan fungsi-fungsi berikut:

- Kumpulkan informasi orientasi
- Mengumpulkan data AWS sumber daya melalui Resource Groups Tagging API
- Kelola AWS Dukungan kasus
- Buat alarm Amazon baru atau telan CloudWatch alarm Anda yang sudah ada
- Menyebarkan dan menguji infrastruktur AWS CloudFormation untuk memungkinkan alat pihak ketiga mengirim peringatan ke Deteksi dan Respons Insiden.

IDR CLI dapat berjalan dalam mode interaktif untuk memandu Anda melalui langkah-langkah orientasi, atau dalam mode offline untuk kasus massal atau DevOps penggunaan.

Untuk informasi selengkapnya tentang cara menggunakan CLI IDR, termasuk instalasi, prasyarat, dan contoh end-to-end, lihat CLI for AWS Incident Detection and Response.

Dukungan bahasa untuk IDR CLI

AWS Incident Detection and Response tersedia dalam bahasa Inggris, Jepang, Mandarin, dan Korea. Jika Anda memerlukan dukungan dalam bahasa Jepang, Mandarin, atau Korea, hubungi AWS melalui AWS Dukungan kasus yang dibuat oleh CLI IDR, atau hubungi Manajer Akun Teknis (TAM) Anda.

Opsi alternatif untuk beban kerja orientasi

Jika Anda tidak dapat menggunakan IDR CLI untuk orientasi, konsultasikan dengan Technical Account Manager (TAM) Anda untuk opsi alternatif. Untuk informasi selengkapnya, lihat Kuesioner orientasi beban kerja dan konsumsi alarm di Deteksi dan Respons Insiden (jalur pengecualian)

Alarm Tertelan

AWS Incident Detection and Response Customer Command Line Interface (IDR CLI) dapat membuat CloudWatch alarm Amazon baru atau mencerna alarm Anda yang sudah ada dan dapat menerapkan dan menguji infrastruktur melalui alat pihak ketiga untuk mengirim peringatan AWS CloudFormation ke AWS Incident Detection and Response.

AWS Incident Detection and Response dapat menyerap alarm dari Amazon CloudWatch dan alat Application Performance Monitoring (APM) pihak ketiga melalui Amazon: EventBridge

- Menelan alarm CloudWatch
- Menelan Alarm Pemantauan Kinerja Aplikasi Pihak Ketiga

Langkah-langkah untuk menelan alarm

Langkah-langkah berikut harus diselesaikan untuk menelan alarm:

- Definisi alarm
- Penyerapan alarm menggunakan IDR CLI
- Ulasan alarm dan umpan balik
- Menyediakan akses untuk menelan alarm ke Deteksi dan Respons Insiden
- Alarm ditayangkan

Opsi alternatif untuk menelan alarm

Jika Anda tidak dapat menggunakan IDR CLI untuk menelan alarm, konsultasikan dengan Technical Account Manager (TAM) Anda untuk opsi alternatif. Untuk informasi selengkapnya, lihat Kuesioner orientasi beban kerja dan konsumsi alarm di Deteksi dan Respons Insiden (jalur pengecualian)

Menyediakan akses untuk menelan alarm ke Deteksi dan Respons Insiden

> **Note**
>
> Jika Anda tidak membuat peran terkait layanan (SLR) selama onboarding IDR CLI, ikuti langkah-langkah di bawah ini untuk menyediakan akses secara manual.

Untuk mengizinkan Deteksi dan Respons Insiden AWS menyerap alarm dari akun Anda, buat SLR. `AWSServiceRoleForHealth_EventProcessor` AWS mengasumsikan SLR untuk membuat EventBridge aturan Terkelola di akun Anda. EventBridge Aturan terkelola mengirimkan notifikasi dari akun Anda ke AWS Incident Detection and Response. Untuk informasi tentang SLR ini, termasuk kebijakan AWS terkelola terkait, lihat Menggunakan peran terkait layanan di Panduan Pengguna.

Anda dapat membuat peran terkait layanan ini di akun Anda dengan mengikuti petunjuk di Buat peran terkait layanan di Panduan Pengguna.AWS Identity and Access Management Atau, Anda dapat menggunakan perintah AWS Command Line Interface (AWS CLI) berikut:

```
aws iam create-service-linked-role --aws-service-name event-
processor.health.amazonaws.com
```

Output kunci

- Pembuatan peran terkait layanan yang berhasil di akun Anda.

> **Note**
>
> Peran terkait layanan - AWSServiceRoleForHealth _ EventProcessor harus dibuat di setiap akun yang akan Anda gunakan untuk mengirim alarm ke AWS Incident Detection and Response.

Informasi terkait

Untuk informasi selengkapnya, lihat topik berikut:

- Menggunakan peran tertaut layanan untuk
- Membuat peran terkait layanan
- AWS kebijakan terkelola: AWS Health_EventProcessorServiceRolePolicy

Definisi alarm

Saat melakukan onboarding alarm ke AWS Incident Detection and Response, Anda bertanggung jawab untuk menentukan metrik dan konfigurasi alarm yang memberikan visibilitas ke kinerja aplikasi Anda. Sebagai bagian dari proses ini, Anda juga harus mengidentifikasi tim dalam organisasi Anda yang bertanggung jawab untuk menanggapi alarm ini.

Saat menyiapkan alarm, kami merekomendasikan praktik terbaik berikut:

- Alarm hanya masuk ke status “Alarm” ketika ada dampak kritis yang berkelanjutan terhadap beban kerja Anda yang dipantau yang memerlukan perhatian segera dari tim Anda dan. AWS Alarm yang memicu dan tidak pulih secara otomatis mengharuskan tim Anda untuk bergabung dengan jembatan insiden dengan AWS Incident Detection and Response.
- Pastikan informasi kontak yang Anda berikan memungkinkan Deteksi dan Respons Insiden AWS untuk secara andal melibatkan tim yang sesuai dalam organisasi Anda ke jembatan 24/7 insiden.

Output kunci

- Daftar alarm dan detail kontak, yang Anda berikan kepada AWS Incident Detection and Response menggunakan IDR CLI.

Untuk informasi selengkapnya tentang mendefinisikan dan menelan CloudWatch alarm Amazon, lihat. Menelan alarm CloudWatch

Untuk informasi selengkapnya tentang menelan alarm Pemantauan Kinerja Aplikasi pihak ketiga, lihat. Menelan Alarm Pemantauan Kinerja Aplikasi Pihak Ketiga

Menelan alarm CloudWatch

Deteksi dan Respons Insiden AWS dapat menyerap CloudWatch alarm Amazon untuk menyediakan pemantauan proaktif untuk beban kerja penting Anda. Dengan menelan CloudWatch alarm Amazon Anda untuk pemantauan, Deteksi dan Respons Insiden AWS dapat:

- Secara otomatis mendeteksi ketika alarm Anda memasuki status “Alarm”.
- Libatkan tim Anda untuk merespons dan menyelesaikan insiden secara kolaboratif.

Untuk memastikan alarm yang Anda gunakan efektif, AWS Incident Detection and Response merekomendasikan praktik terbaik berikut:

- Konfigurasikan alarm dengan ekspresi matematika metrik untuk menekannya selama periode pemeliharaan rutin atau eksekusi pekerjaan batch untuk menghindari keterlibatan alarm positif palsu.
- Atur Perlakuan Data Hilang pada alarm berdasarkan frekuensi pengiriman titik data yang diharapkan. Misalnya, metrik pemantauan alarm yang menghasilkan aliran titik data yang berkelanjutan harus memperlakukan data yang hilang sebagai “Pelanggaran” (buruk) karena titik data yang hilang dapat menunjukkan masalah dengan sumber daya dasar yang dipantau. Sebaliknya, metrik pemantauan alarm yang jarang melaporkan titik data, misalnya metrik pemantauan alarm yang hanya merekam titik data ketika terjadi kegagalan atau kesalahan, harus memperlakukan data yang hilang sebagai (baik). NotBreaching
- Tentukan alarm yang masuk ke status “Alarm” ketika ada dampak kritis dan berkelanjutan terhadap beban kerja Anda. Misalnya, konfigurasikan alarm untuk dipicu setelah waktu yang diharapkan diperlukan untuk mengganti sumber daya yang tidak sehat secara otomatis, bukan pada deteksi awal sumber daya yang tidak sehat.
- Identifikasi dan buat alarm untuk metrik kustom yang secara langsung mewakili pengalaman pelanggan untuk beban kerja Anda.

Untuk mengetahui daftar CloudWatch alarm Amazon yang direkomendasikan untuk umum Layanan AWS, lihat Praktik Terbaik Deteksi Insiden dan Alarm Respons di AWS re:Post.

Menelan Alarm Pemantauan Kinerja Aplikasi Pihak Ketiga

AWS Incident Detection and Response mendukung konsumsi alarm dari alat Application Performance Monitoring (APM) pihak ketiga melalui Amazon. EventBridge Integrasi ini memberikan

fleksibilitas dengan menelan peringatan APM, memungkinkan perutean acara APM melalui berbagai ke bus EventBridge acara Amazon di Layanan AWS akun Anda.

Contoh jalur integrasi:

- Sumber (APM) → AWS Layanan (Contoh: Amazon API Gateway atau Amazon SNS) → Ubah Fungsi Lambda → Bus EventBridge Acara Amazon Kustom → Deteksi dan Respons Insiden AWS
- Sumber (APM) → Partner Amazon EventBridge Event Bus → Transform Lambda Function → Custom EventBridge Amazon Event Bus → AWS Insiden Deteksi dan Respons

AWS Incident Detection and Response menginstal aturan terkelola pada bus peristiwa khusus untuk menerima peringatan yang dikirim kepadanya oleh Transform Lambda Functions. Penting untuk dicatat bahwa untuk EventBridge Integrasi SaaS Amazon, bus acara mitra bukanlah bus acara yang memiliki aturan terkelola yang diinstal. Untuk daftar lengkap APM dengan integrasi mitra ke Amazon EventBridge, lihat Integrasi Amazon EventBridge .

Contoh integrasi menggunakan bus acara mitra atau sumber bus AWS acara lainnya

Diagram berikut menunjukkan contoh integrasi menggunakan bus acara mitra atau sumber bus AWS acara lainnya.

Untuk daftar lengkap APM dengan integrasi mitra ke Amazon EventBridge, lihat Integrasi Amazon EventBridge .

Contoh integrasi menggunakan Amazon API Gateway

Diagram berikut menunjukkan contoh integrasi menggunakan API Gateway.

Contoh integrasi menggunakan Amazon Simple Notification Service

Diagram berikut menunjukkan contoh integrasi menggunakan Amazon SNS.

Untuk menyederhanakan proses integrasi, AWS Incident Detection and Response menyediakan CloudFormation template untuk jenis integrasi yang paling umum digunakan. Template ini mengotomatiskan pengaturan AWS sumber daya, dan peran IAM yang diperlukan.

CloudFormation Template dan instruksi untuk membuat berbagai jenis integrasi secara manual dapat ditemukan di dokumentasi integrasi yang sesuai di bawah ini:

- Ingest Alarm dari APM dengan integrasi langsung EventBridge
- Menelan alarm dari APM tanpa integrasi langsung dengan EventBridge
- Ingest Alarm dari APM dengan integrasi Amazon SNS langsung

> **Note**
>
> CloudFormation Template membutuhkan modifikasi. Modifikasi ini dijelaskan dalam topik sebelumnya. Untuk informasi selengkapnya tentang format payload yang diperlukan untuk mengirim peringatan APM ke AWS Incident Detection and Response lihat. Persyaratan Muatan Untuk Menelan Peringatan APM dengan EventBridge

Persyaratan Muatan Untuk Menelan Peringatan APM dengan EventBridge

Dari mana Deteksi dan Respons Insiden menyerap peringatan APM?

AWS Incident Detection and Response menginstal aturan terkelola pada bus acara tempat Anda mengirim payload terakhir yang diubah. Ini adalah praktik terbaik untuk membuat bus acara khusus untuk tujuan ini.

Format apa yang harus diisi muatan?

Kunci JSON minimum berikut: pasangan nilai diperlukan jika peristiwa bus tertelan oleh Deteksi dan Respons Insiden AWS:

```
{
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent"
    "detail": {
        "incident-detection-response-identifier": "Your alarm name from your APM",
    }
}
```

Contoh berikut menunjukkan acara dari bus acara mitra sebelum dan sesudah itu diubah.

Sebelum transformasi:

```
{
    "version": "0",
    "id": "a6150a80-601d-be41-1a1f-2c5527a99199",
```

```
    "detail-type": "Datadog Alert Notification",
    "source": "aws.partner/datadog.com/Datadog-aaa111bbbc",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "alert_type": "error",
        "event_type": "query_alert_monitor",
        "meta": {
            "monitor": {
                "id": 222222,
                "org_id": 3333333333,
                "type": "query alert",
                "name": "UnHealthyHostCount",
                "message": "@awseventbridge-Datadog-aaa111bbbc",
                "query":
"max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
<= 1",
                "created_at": 1686884769000,
                "modified": 1698244915000,
                "options": {
                    "thresholds": {
                        "critical": 1.0
                    }
                },
            },
            "result": {
                "result_id": 7281010972796602670,
                "result_ts": 1698244878,
                "evaluation_ts": 1698244868,
                "scheduled_ts": 1698244938,
                "metadata": {
                    "monitor_id": 222222,
                    "metric": "aws.applicationelb.un_healthy_host_count"
                }
            },
            "transition": {
                "trans_name": "Triggered",
                "trans_type": "alert"
            },
            "states": {
                "source_state": "OK",
                "dest_state": "Alert"
```

```
            },
            "duration": 0
        },
        "priority": "normal",
        "source_type_name": "Monitor Alert",
        "tags": [
            "aws_account:123456789012",
            "monitor"
        ]
    }
}
```

Perhatikan bahwa sebelum acara diubah, `detail-type` dan `source` menunjukkan rincian APM di mana peringatan berasal. Ini harus dimodifikasi sebelum dikonsumsi. `incident-detection-response-identifier`Kuncinya belum ada dan juga harus ditambahkan sebelum konsumsi.

Fungsi Lambda mengubah peristiwa di atas dan memasukkannya ke bus acara khusus atau default target. Muatan yang diubah harus menyertakan pasangan kunci:value yang diperlukan.

Setelah transformasi:

```
{
    "version": "0",
    "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "incident-detection-response-identifier": "UnHealthyHostCount",
        "alert_type": "error",
        "event_type": "query_alert_monitor",
        "meta": {
            "monitor": {
                "id": 222222,
                "org_id": 3333333333,
                "type": "query alert",
                "name": "UnHealthyHostCount",
                "message": "@awseventbridge-Datadog-aaa111bbbc",
```

```
                "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 <= 1",
                "created_at": 1686884769000,
                "modified": 1698244915000,
                "options": {
                    "thresholds": {
                        "critical": 1.0
                    }
                },
            },
            "result": {
                "result_id": 7281010972796602670,
                "result_ts": 1698244878,
                "evaluation_ts": 1698244868,
                "scheduled_ts": 1698244938,
                "metadata": {
                    "monitor_id": 222222,
                    "metric": "aws.applicationelb.un_healthy_host_count"
                }
            },
            "transition": {
                "trans_name": "Triggered",
                "trans_type": "alert"
            },
            "states": {
                "source_state": "OK",
                "dest_state": "Alert"
            },
            "duration": 0
        },
        "priority": "normal",
        "source_type_name": "Monitor Alert",
        "tags": [
            "aws_account:123456789012",
            "monitor"
        ]
    }
}
```

Perhatikan bahwa `detail-type` sekarang`ams.monitoring/generic-apm`, sumber sekarang`GenericAPMEvent`, dan di bawah detail ada pasangan key:value baru:. `incident-detection-response-identifier`

`incident-detection-response-identifier`Nilai diambil dari nama peringatan berdasarkan muatan apa pun yang dikirim APM Anda. Jalur nama peringatan APM berbeda dari satu APM ke APM lainnya. Fungsi Lambda harus diatur untuk mengambil nama alarm dari jalur yang benar di payload APM JSON yang diterima oleh Lambda dan menggunakannya untuk nilainya. `incident-detection-response-identifier`

`incident-detection-response-identifier`nilai harus unik per jenis alarm yang dikirim ke AWS Incident Detection and Response. Setiap nama unik yang ditetapkan `incident-detection-response-identifier` harus diberikan kepada tim AWS Incident Detection and Response selama on-boarding. Peristiwa yang memiliki nilai `incident-detection-response-identifier` kunci yang tidak diketahui atau hilang tidak diproses.

Ingest Alarm dari APM dengan integrasi langsung EventBridge

Topik berikut menunjukkan proses pengiriman alarm ke alat AWS Incident Detection and Response from Application Performance Monitoring (APM) yang memiliki integrasi langsung dengan Amazon. EventBridge Untuk daftar lengkap APM yang memiliki integrasi langsung dengan Amazon EventBridge, lihat Integrasi Amazon EventBridge.

Anda dapat menerapkan CloudFormation template yang disediakan atau mengatur integrasi ini secara manual. Sebelum menyiapkan integrasi, verifikasi bahwa peran AWS terkait layanan (SLR)`AWSServiceRoleForHealth_EventProcessor`, dibuat di akun Anda.

Opsi 1: Menggunakan CloudFormation

CloudFormation Template tersedia untuk menyederhanakan proses pembuatan infrastruktur integrasi yang diperlukan untuk menyerap alarm ke AWS Incident Detection and Response dari APM Anda dengan integrasi Amazon. EventBridge

> **Note**
>
> - Biaya tambahan dikeluarkan untuk sumber daya yang digunakan melalui CloudFormation template ini (misalnya: Lambda dan). EventBridge Untuk informasi selengkapnya tentang harga layanan ini, lihat AWS Harga.
> - Terapkan CloudFormation template ini di setiap AWS akun dan Wilayah di mana Deteksi dan Respons Insiden AWS perlu menyerap alarm. Insiden dan Kasus Dukungan dibuka di AWS Akun tempat peringatan APM diterima.

- Dokumen ini menggunakan New Relic sebagai contoh, namun CloudFormation template dapat digunakan untuk APM apa pun yang memiliki integrasi SaaS dengan Amazon. EventBridge
- Setelah menguji integrasi, hapus pernyataan logger.info () dari file `TransformLambdaFunction` untuk mencegah payload muncul di Amazon Logs. CloudWatch

Prasyarat untuk menerapkan template ini: CloudFormation

- Sumber Acara Mitra harus disiapkan di Amazon EventBridge. Untuk petunjuk cara menyiapkan APM Anda sebagai sumber acara, lihat Menerima acara dari mitra SaaS dengan EventBridge Amazon di Panduan Pengguna EventBridge Amazon.
- `TransformLambdaFunction`(Fungsi Lambda) dalam template harus dimodifikasi untuk disetel `["detail"]["incident-detection-response-identifier"]` ke nilai yang diinginkan berdasarkan jalur JSON dari nama peringatan di payload APM.

Langkah Prasyarat:

1. Buka EventBridge Konsol. Di bawah menu Integrasi, pilih Sumber acara mitra.
   - Cari APM Anda di kotak EventBridge mitra Amazon.
   - Pilih Pengaturan, lalu ikuti instruksi yang diberikan.
     - Catatan: langkah terakhir adalah memilih Associate with Event Bus di konsol untuk sumber acara Partner. Memilih opsi ini secara otomatis membuat Bus Acara Mitra dengan nama yang sama dengan sumber acara Mitra (nama harus cocok).
   - Salin nama Bus Acara Mitra atau sumber. Event Bus atau sumber digunakan sebagai parameter, bernama`PartnerEventBusNameParameter`, saat menerapkan CloudFormation template.
     - Contoh untuk New Relic: `aws.partner/newrelic.com/1234567/source_name`
   - Salin bagian pertama dari Bus Acara Mitra atau sumber untuk dimasukkan ke dalam `PartnerEventBusPrefixParameter` saat menerapkan CloudFormation template.
     - Contoh dari New Relic adalah `aws.partner/newrelic.com`
2. Unduh dan edit CloudFormation template.
   - Temukan `TransformLambdaFunction` di template

- Di bawah `def lambda_handler(event, context)` diatur `event["detail"]["incident-detection-response-identifier"]` ke jalur json di mana nama alarm muncul di payload JSON dari alarm APM. Setiap APM akan memiliki jalur yang berbeda. Beberapa contoh dapat dilihat di bawah ini, namun muatan spesifik Anda mungkin berbeda.
  - Contoh Relik Baru:`event["detail"]["incident-detection-response-identifier"] = event["detail"]["workflowName"]`.
  - Contoh Datadog: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["meta"]["monitor"]["name"]`
  - Contoh Splunk: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["ruleName"]`
- Simpan CloudFormation template.

Menyebarkan CloudFormation Template:

1. Buka CloudFormation konsol di akun target dan Wilayah Anda.
2. Pilih Buat tumpukan, Dengan sumber daya baru (standar)
   - Pilih Pilih templat yang ada, Unggah file templat, Pilih file, lalu unggah CloudFormation templat yang Anda simpan secara lokal.
3. Tentukan detail tumpukan:
   - Masukkan nama tumpukan (Contoh:`NewRelicIntegrationForIDR`).
   - Tentukan nilai Parameter yang diperoleh selama penyelesaian Prasyarat.
     - APMNameParameter(Contoh:`NewRelic`)
     - PartnerEventBusNameParameter(Contoh:`aws.partner/newrelic.com/1234567/source_name`)
     - PartnerEventBusPrefixParameter(Contoh:`aws.partner/newrelic.com`)
   - Pilih Berikutnya.
4. Konfigurasikan opsi tumpukan:
   - Gulir ke bagian bawah halaman dan centang kotak CloudFormation untuk memungkinkan membuat sumber daya IAM dengan nama khusus.
5. Tinjau dan buat:
   - Validasi nilai parameter dikonfigurasi dengan benar dan pilih Kirim.

6. CloudFormation Tumpukan menyebarkan sumber daya yang diperlukan untuk mengintegrasikan peristiwa APM Anda ke Deteksi dan Respons Insiden AWS. Tunggu status tumpukan ditampilkan`CREATE_COMPLETE`.
7. CloudFormation Tumpukan membuat sumber daya berikut, dengan asumsi nilai contoh dimasukkan ke dalam parameter untuk New Relic dan dijalankan di Region. US-EAST-1
   - CustomEventBus: NewRelic-AWSIncidentDetectionResponse-EventBus
   - EventBridgeRule: aws. partner/newrelic. com/1234567/source_name | NewRelic-AWSIncidentDetectionResponse-EventBridgeRule
   - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
   - TransformLambdaFunction: NewRelic-AWSIncidentDetectionResponse-Lambda-Transform
   - TransformLambdaPermission: NewRelicIntegrationForIDR-TransformLambdaPermission - [random_string]

Pengujian integrasi

Setelah menerapkan tumpukan, uji integrasi dengan mengirimkan payload pengujian dari APM Anda:

1. Arahkan ke Konsol Lambda dan pilih fungsinya. `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` Pilih tab Pantau.
2. Cari pemanggilan yang berhasil dalam grafik metrik.
3. Pilih Lihat CloudWatch Log Amazon untuk memeriksa aliran Log untuk muatan pengujian Anda atau kesalahan apa pun.

Berbagi ARN Bus Acara Anda ke Deteksi dan Respons Insiden AWS

1. Buka EventBridge Konsol Amazon. Pilih bus acara.
2. Salin ARN dari bus acara Kustom yang dibuat sebagai bagian dari CloudFormation tumpukan, (contoh: *`arn:aws:events:us-east-1:123456789123:event-bus/NewRelic-AWSIncidentDetectionResponse-EventBus`*.)
   - Tambahkan ARN ini ke bidang "EventBridge Event Bus ARN” di bagian "Third-Party Alarm APM” di bagian Anda. Kuesioner konsumsi alarm - Ikhtisar
3. Selama proses orientasi, AWS Incident Detection and Response membuat EventBridge aturan terkelola pada bus acara khusus ini untuk menyerap alarm APM Anda.

Opsi 2: Integrasi manual

Selesaikan langkah-langkah berikut untuk setiap AWS akun dan AWS Wilayah tempat Deteksi dan Respons Insiden AWS perlu menyerap alarm. AWS Incident Detection and Response merekomendasikan untuk menyiapkan alarm di AWS akun dan Wilayah yang sama dengan sumber daya aplikasi Anda agar lebih cepat mengidentifikasi dan menyelidiki sumber daya yang terkena dampak. Insiden dan Kasus Dukungan dibuka di AWS Akun tempat peringatan APM diterima.

1. Buat bus acara EventBridge mitra dengan menyiapkan APM Anda sebagai sumber acara EventBridge mitra Amazon (misalnya,`aws.partner/apm_name/integrationName`). Untuk panduan cara menyiapkan APM Anda sebagai sumber acara, lihat Menerima acara dari mitra SaaS dengan Amazon. EventBridge
2. Lakukan salah satu hal berikut:
   - (Disarankan) Buat bus acara EventBridge khusus bernama`$YourApmName-AWSIncidentDetectionResponse-EventBus`.
   - (Alternatif) Gunakan bus EventBridge acara default alih-alih bus acara khusus.

   AWS Incident Detection and Response akan menginstal aturan terkelola (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) pada bus peristiwa kustom atau default melalui `AWSServiceRoleForHealth_EventProcessor` SLR. Sumber aturan akan menjadi bus peristiwa khusus atau default, tujuan aturan adalah AWS Incident Detection and Response, dan aturan akan cocok dengan pola untuk menelan peristiwa APM pihak ke-3.
3. Buat fungsi Lambda bernama `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` untuk mengubah acara bus acara mitra Anda. Peristiwa yang diubah akan cocok dengan aturan yang dikelolaAWSHealthEventProcessorEventSource-DO-NOT-DELETE.
   - Peristiwa yang diubah menyertakan pengenal Deteksi Insiden dan Respons AWS yang unik, dan menetapkan jenis sumber dan detail peristiwa ke nilai yang diperlukan. Hal ini memungkinkan struktur payload JSON yang diubah agar sesuai dengan pola aturan terkelola.
   - Tetapkan target fungsi Lambda ke bus acara khusus (Disarankan) yang dibuat di Langkah 2 atau ke bus acara default Anda.
4. Buat EventBridge aturan dan tentukan pola peristiwa yang cocok dengan daftar peristiwa yang ingin Anda dorong ke AWS Incident Detection and Response. Sumber aturan adalah bus acara mitra yang Anda buat di Langkah 1 (`aws.partner/apm_name/integrationName`). Target aturan adalah fungsi Lambda yang Anda buat di Langkah 3 ()`[apm_name]-`

`AWSIncidentDetectionResponse-LambdaFunction`. Untuk panduan tentang menentukan EventBridge aturan Anda, lihat EventBridge Aturan Amazon.

Untuk contoh langkah demi langkah tentang cara mengatur integrasi bus acara mitra secara manual dengan AWS Incident Detection and Response, lihat Mengintegrasikan notifikasi dari Datadog dan Splunk.

Menelan alarm dari APM tanpa integrasi langsung dengan EventBridge

AWS Incident Detection and Response mendukung penggunaan webhook untuk menelan alarm dari APM pihak ketiga yang tidak memiliki integrasi langsung dengan Amazon. EventBridge

Anda dapat menerapkan CloudFormation template atau mengatur integrasi secara manual. Sebelum menyiapkan integrasi, verifikasi bahwa peran AWS terkait layanan (SLR)`AWSServiceRoleForHealth_EventProcessor`, dibuat di akun Anda.

Opsi 1: Menggunakan CloudFormation Templat

CloudFormation Template tersedia untuk menyederhanakan proses pembuatan infrastruktur integrasi yang diperlukan untuk menyerap alarm ke AWS Incident Detection and Response dari APM Anda yang tidak memiliki integrasi Amazon langsung. EventBridge

Pertimbangan sebelum menyebarkan Template ini CloudFormation

- Solusi ini menggunakan API Gateway Lambda Authorizer untuk membandingkan token rahasia yang diteruskan dalam payload dari APM Anda dengan token di. AWS Secrets Manager Jika token tidak cocok, kebijakan dengan penolakan eksplisit akan dikembalikan. Untuk informasi selengkapnya, lihat Lambda Authorizers.
- Di bawah model Tanggung Jawab AWS Bersama, Anda bertanggung jawab untuk memastikan Anda menggunakan pendekatan otentikasi yang memenuhi persyaratan keamanan organisasi Anda. Sebaiknya gunakan AWS Secrets Manager atau layanan serupa, daripada menyimpan informasi sensitif seperti kunci API atau token otorisasi sebagai variabel hard-code. Untuk informasi selengkapnya, lihat Membuat dan mengelola rahasia dengan AWS Secrets Manager.
- Untuk contoh tambahan penerapan Hash-Based Message Authentication Code (HMAC), lihat receive-webhooks di halaman Github aws-samples. Untuk informasi selengkapnya tentang penerapan otorisasi token, lihat contoh fungsi Lambda otorisasi TOKEN dari dokumentasi API Gateway.
- Solusinya menggunakan RateLimit, BurstLimit, dan Kuota di API Gateway untuk mengontrol volume permintaan. Alat-alat ini membatasi berapa banyak permintaan yang dapat diproses

dalam waktu yang ditentukan. Ini membantu mencegah kelebihan sistem dan menjaga layanan tetap stabil. Untuk informasi selengkapnya tentang pembatasan, lihat Panduan Pengembang API Gateway.

- Pertimbangkan untuk menggunakan AWS Web Application Firewall (WAF) untuk melindungi API Gateway dari alamat IP buruk yang diketahui. Ini mengurangi risiko penyerang membanjiri API dengan permintaan palsu yang dapat memblokir peristiwa log nyata.
- AWS Secrets Manager nilai token harus disimpan dalam alat Application Performance Monitoring (APM) Anda sebagai header HTTP. Pastikan untuk memutar token secara teratur sebagai praktik terbaik keamanan.
- Biaya tambahan akan dikeluarkan untuk sumber daya yang digunakan melalui CloudFormation template ini (misalnya: Lambda dan). EventBridge Untuk informasi selengkapnya tentang harga layanan ini, lihat AWS Harga.
- Setelah menguji integrasi, hapus pernyataan logger.info () dari (fungsi `TransformLambdaFunction` Lambda) untuk mencegah payload muncul di Amazon Logs. CloudWatch
- Terapkan CloudFormation template ini di setiap AWS akun dan Wilayah tempat Deteksi dan Respons Insiden AWS perlu menyerap alarm.

Mempersiapkan CloudFormation Template:

Catatan: Langkah integrasi menggunakan Dynatrace sebagai contoh, namun template ini dapat digunakan untuk APM apa pun yang dapat mengirim muatan ke API Gateway.

1. Unduh dan buka CloudFormation template.
2. Temukan `APIGWUsagePlan` di template. Tinjau nilai yang dikonfigurasi untuk `RateLimitBurstLimit`,, dan `Quota Limit` yang diatur ke 20, 50 & 2000 secara default. Sesuaikan nilai untuk memenuhi kebutuhan Anda.
3. Temukan `AuthorizerLambdaFunction` di template. Fungsi Lambda ini berfungsi sebagai contoh mekanisme otentikasi. Ini mengekstrak nilai token dari header yang disebut`authorizationToken`, yang diteruskan dari APM Anda. Anda dapat mengubah kode ini agar selaras dengan kebijakan keamanan organisasi dan persyaratan APM.
4. Temukan `TransformLambdaFunction` di template. Ganti jalur kamus`raw_json["detail"]["ProblemTitle"]`,, dengan jalur ke nama alarm Anda yang dikirim dalam payload JSON dari APM Anda. Biarkan ini seperti untuk Dynatrace.

Menyebarkan CloudFormation template:

1. Buka CloudFormation konsol di akun target Anda dan Wilayah AWS.
2. Pilih Buat tumpukan, Dengan sumber daya baru (standar).
   - Pilih Pilih templat yang ada, Unggah file templat, Pilih file, lalu unggah CloudFormation templat yang Anda simpan secara lokal.
3. Tentukan detail tumpukan:
   - Masukkan nama tumpukan (contoh, *`DynatraceIntegrationForIDR`*.)
   - APMNameParameter (contoh, *`Dynatrace`*.)
   - Pilih Berikutnya.
4. Konfigurasikan opsi tumpukan:
   - Gulir ke bagian bawah halaman dan centang kotak CloudFormation untuk memungkinkan membuat sumber daya IAM dengan nama khusus.
5. Tinjau dan buat:
   - Validasi nilai parameter dikonfigurasi dengan benar dan pilih Kirim.
6. CloudFormation Tumpukan menyebarkan sumber daya yang diperlukan untuk mengintegrasikan peristiwa APM Anda ke Deteksi dan Respons Insiden AWS. Tunggu hingga Status CloudFormation Stack CREATE_COMPLETE.
7. CloudFormation Tumpukan membuat sumber daya di bawah ini dengan `Dynatrace` asumsi nilai contoh dimasukkan ke dalam parameter dan dieksekusi di US-EAST-1 Wilayah.
   - Nama rahasia: DynatraceMySecretTokenName (nilai Rahasia acak akan dibuat terhadap kunci Rahasia APMSecureToken)
   - Sumber daya API Gateway:
     - Nama API: Dynatrace-AWSIncidentDetectionResponse-APIGW
     - Nama Panggung: Dynatrace-Stage-Prod
     - Pengotorisasi: Dynatrace-APIGW-Authorizer
     - Paket penggunaan: APIGW_ Throttling_Plan
   - Fungsi Lambda:
     - Fungsi untuk otorisasi: Dynatrace-AWSIncidentDetectionResponse-Lambda-Authorizer
     - Fungsi untuk transformasi: Dynatrace-AWSIncidentDetectionResponse-Lambda-Transform
   - EventBus Nama kustom: Dynatrace-AWSIncidentDetectionResponse-EventBus
   - Peran IAM:

- TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
- AuthorizerLambdaExecutionRole: IDR-AuthorizerLambdaExecutionRole-us-east-1

8. Catat URL Webhook dan nilai Token:
   - Buka konsol API Gateway dan pilih Nama API yang dibuat sebagai bagian dari CloudFormation tumpukan.
   - Pilih Tahapan dari navigasi sebelah kiri, perluas nama panggung menggunakan tanda +, lalu pilih POST. Rekam URL Panggil. Konfigurasikan URL ini di APM Anda sebagai tujuan untuk mengirim webhook untuk acara alarm.
   - Buka AWS Secrets Manager konsol dan pilih nama Rahasia yang dibuat sebagai bagian dari CloudFormation tumpukan. (Contoh: DynatraceMySecretTokenName.)
     - Di tab Nilai rahasia, pilih Ambil nilai rahasia. Anda akan melihat kunci Rahasia sebagai APMSecureToken. Catat nilai Rahasia. Jangan berbagi nilai rahasia ini dengan siapa pun.

Pengujian integrasi

Setelah menerapkan tumpukan, uji integrasi dengan mengirimkan payload pengujian dari APM Anda:

1. Arahkan ke Konsol Lambda dan pilih `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` fungsi. Pilih tab Pantau.
2. Cari pemanggilan yang berhasil dalam grafik metrik.
3. Pilih Lihat CloudWatch Log Amazon untuk memeriksa aliran Log untuk muatan pengujian Anda atau kesalahan apa pun.

Berbagi ARN Bus Acara Anda ke Deteksi dan Respons Insiden AWS

1. Buka EventBridge Konsol Amazon. Pilih bus acara.
2. Salin ARN dari bus acara Kustom yang dibuat sebagai bagian dari CloudFormation tumpukan, contoh:. `arn:aws:events:us-east-1:123456789123:event-bus/Dynatrace-AWSIncidentDetectionResponse-EventBus`
   - Tambahkan ARN ini ke bidang "EventBridge Event Bus ARN” di bagian "Third-Party Alarm APM” di bagian Anda. Kuesioner konsumsi alarm - Ikhtisar
3. Selama proses orientasi, AWS Incident Detection and Response akan membuat EventBridge aturan Terkelola pada bus acara khusus ini untuk menyerap alarm APM Anda.

Opsi 2: Integrasi manual

Gunakan langkah-langkah berikut untuk menyiapkan integrasi dengan AWS Incident Detection and Response.

1. Buat Amazon API Gateway untuk menerima payload dari APM Anda.
2. Tentukan fungsi Lambda untuk otorisasi menggunakan token otentikasi.
3. Lakukan salah satu hal berikut:
   - (Disarankan) Buat bus acara EventBridge khusus bernama`$YourApmName-AWSIncidentDetectionResponse-EventBus`.
   - (Alternatif) Gunakan bus EventBridge acara default alih-alih bus acara khusus.
4. Tentukan fungsi Transform Lambda untuk menambahkan AWS Incident Detection and Response identifier ke payload Anda. Anda juga dapat menggunakan fungsi ini untuk memfilter peristiwa yang ingin Anda kirim ke AWS Incident Detection and Response.
   - API Gateway harus menjalankan fungsi Transform Lambda yang akan mengubah payload yang diteruskan oleh API Gateway.
   - Fungsi Transform Lambda harus menulis peristiwa yang diubah dalam bus peristiwa yang ditentukan pada poin 3 di atas.
5. Siapkan APM Anda untuk mengirim notifikasi ke URL yang dihasilkan dari API Gateway.

Ingest Alarm dari APM dengan integrasi Amazon SNS langsung

Jika APM mendukung pengiriman alarm ke topik Amazon SNS, Anda dapat mengikuti panduan ini untuk menyerap alarm APM Anda ke AWS Incident Detection and Response.

Anda dapat menerapkan CloudFormation template yang disediakan atau mengatur integrasi ini secara manual. Sebelum menyiapkan integrasi, verifikasi bahwa peran AWS terkait layanan (SLR)`AWSServiceRoleForHealth_EventProcessor`, dibuat di akun Anda.

Opsi 1: Menggunakan CloudFormation

CloudFormation Template tersedia untuk menyederhanakan proses pembuatan infrastruktur integrasi yang diperlukan untuk menyerap alarm ke AWS Incident Detection and Response dari APM Anda dengan integrasi Amazon SNS.

> **Note**
>
> - Biaya tambahan akan dikeluarkan untuk sumber daya yang digunakan melalui CloudFormation template ini (misalnya: Lambda dan). EventBridge Untuk informasi selengkapnya tentang harga layanan ini, lihat AWS Harga.
> - CloudFormation Template ini harus digunakan di setiap AWS akun dan Wilayah tempat alarm harus dicerna oleh AWS Incident Detection and Response.
> - Contoh yang diberikan dalam dokumen ini adalah untuk Grafana, namun template ini dapat digunakan untuk APM apa pun yang memiliki integrasi langsung dengan Amazon Simple Notification Service.
> - Untuk alasan keamanan, AWS sarankan untuk menghapus `logger.info()` pernyataan dari `TransformLambdaFunction` untuk mencegah payload masuk ke Amazon CloudWatch Logs.

Prasyarat untuk menerapkan template ini: CloudFormation

- Topik Layanan Pemberitahuan Sederhana Amazon Standar harus dibuat untuk menerima peristiwa alarm dari APM Anda. Buat topik SNS di konsol Amazon Simple Notification Service.
- `TransformLambdaFunction`Dalam template harus dimodifikasi untuk mengatur `["detail"]["incident-detection-response-identifier"]` ke nilai yang diinginkan berdasarkan APM yang digunakan.

Penyelesaian prasyarat:

1. Buka Amazon SNS Console, lalu pilih Topik. Salin ARN dari topik Standar Amazon SNS yang dibuat untuk menerima acara alarm dari APM Anda.
   - Contoh: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
2. Unduh dan buka CloudFormation template
   - Temukan `TransformLambdaFunction` di template
     - Di bawah `def lambda_handler(event, context)` disetel `event["detail"]["incident-detection-response-identifier"]` ke jalur json di mana nama alarm muncul di payload JSON dari catatan SNS.

- Setiap peristiwa yang dikirim ke `TransformLambdaFunction` melalui SNS memiliki struktur muatan induk sebagai. `event["Records"][n]["Sns"]["Message"]` Asal muatan aktual dari sumber (APM) dibungkus di dalam struktur induk.
- Contoh untuk Grafana: `event["Records"][n]["Sns"]["Message"]["alerts"][n]["labels"]["alertname"]`

Menyebarkan CloudFormation Template:

1. Arahkan ke CloudFormation konsol di akun dan Wilayah tempat Anda perlu mengatur integrasi.
2. Arahkan ke CloudFormation.
   - Pilih Buat tumpukan, Dengan sumber daya baru (standar)
     - Pilih Pilih templat yang ada, Unggah file templat, Pilih file, lalu unggah CloudFormation templat yang Anda simpan secara lokal.
3. Tentukan detail tumpukan:
   - Masukkan contoh nama tumpukan: `<your-apm-name>IntegrationForIDR`
   - Tentukan nilai Parameter yang diperoleh selama penyelesaian Prasyarat
     - APMNameParameterContoh: `Grafana`
     - Contoh TriggersnSParameter: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
   - Pilih Berikutnya.
4. Konfigurasikan opsi tumpukan:
   - Gulir ke bagian bawah halaman dan akui kotak centang CloudFormation untuk memungkinkan membuat sumber daya IAM dengan nama khusus.
5. Tinjau dan buat:
   - Validasi nilai parameter dikonfigurasi dengan benar, lalu pilih Kirim.
6. CloudFormation Stack akan menerapkan sumber daya yang diperlukan untuk mengintegrasikan peristiwa APM Anda ke AWS Incident Detection and Response. Tunggu hingga Status CloudFormation Stack CREATE_COMPLETE.
7. CloudFormation Tumpukan membuat sumber daya di bawah ini dengan asumsi nilai contoh dimasukkan ke dalam parameter untuk Grafana dan dieksekusi di EU-WEST-1 Wilayah.
   - CustomEventBus: Grafana-AWSIncidentDetectionResponse-EventBus
   - SNSSubscription: arn:aws:sns:eu-west- 1:012345678912: grafana-sns: [random_string]

- TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-eu-west-1
- TransformLambdaFunction: Grafana-AWSIncidentDetectionResponse-Lambda-Transform
- TransformLambdaPermission: GrafanaIntegrationForIDR-TransformLambdaPermission - [random_string]

Pengujian integrasi

Setelah CloudFormation tumpukan berhasil diterapkan, Anda dapat memvalidasi integrasi dengan mengirimkan payload pengujian dari APM Anda. Setelah payload tes dikirim dari APM Anda:

1. Arahkan ke Konsol Lambda dan pilih fungsinya. `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` Kemudian, pilih tab Monitor.
2. Doa yang berhasil harus diamati dalam grafik metrik.
3. Pilih Lihat CloudWatch Log Amazon. Anda dapat memverifikasi dari peristiwa Log di aliran Log untuk mengonfirmasi bahwa muatan pengujian yang dikirim dari APM Anda ada, atau jika ada kesalahan yang ditemukan.

Berbagi ARN Bus Acara Anda ke Deteksi dan Respons Insiden AWS

1. Arahkan ke EventBridge Konsol Amazon. Pilih bus acara.
2. Rekam ARN dari bus peristiwa Kustom yang digunakan sebagai bagian dari CloudFormation tumpukan, misalnya:. `arn:aws:events:eu-west-1:012345678912:event-bus/Grafana-AWSIncidentDetectionResponse-EventBus`
   - Berikan ARN bus acara Kustom ini ke AWS Incident Detection and Response di bidang "EventBridge Event Bus ARN” pada bagian "Third-Party Alarm APM” pada. Kuesioner konsumsi alarm - Ikhtisar
3. Selama proses orientasi, AWS Incident Detection and Response akan membuat EventBridge aturan Terkelola pada bus acara khusus ini untuk menyerap alarm APM Anda.

Opsi 2: Integrasi manual

1. Buka Konsol Amazon SNS dan buat topik Standar Amazon SNS yang `[apm_name]-sns` diberi nama untuk menerima peristiwa alarm dari APM Anda. Pastikan Anda memilih Standar (bukan FIFO) sebagai jenis topik. Perhatikan ARN dari topik Amazon SNS yang dibuat.

2. Lakukan salah satu hal berikut:
   - (Disarankan) Buat bus acara EventBridge khusus bernama`[apm_name]-AWSIncidentDetectionResponse-EventBus`.
   - (Alternatif) Gunakan bus EventBridge acara default alih-alih bus acara khusus.

   AWS Incident Detection and Response akan menginstal aturan terkelola (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) pada bus peristiwa kustom atau default melalui `AWSServiceRoleForHealth_EventProcessor` SLR. Sumber aturan akan menjadi bus peristiwa khusus atau default, tujuan aturan adalah AWS Incident Detection and Response, dan aturan akan cocok dengan pola untuk menelan peristiwa APM pihak ke-3.
3. Buat fungsi Lambda bernama `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` untuk mengubah muatan SNS Anda.
   - Peristiwa yang diubah harus memenuhi persyaratan muatan sebagaimana diatur dalam Persyaratan Muatan Untuk Menelan Peringatan APM dengan EventBridge
   - Tetapkan target fungsi Lambda ke bus acara khusus (Disarankan) yang dibuat di Langkah 2 atau ke bus acara default Anda.
4. Tetapkan topik SNS sebagai pemicu fungsi `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` Lambda Anda.
   - Di halaman “Tambahkan Pemicu”, cari “SNS”.
   - Tambahkan ARN Topik SNS khusus Anda yang dibuat di Langkah 1.
   - Pilih “Tambah”.
5. Ikuti dokumentasi APM Anda untuk menyiapkan tujuan SNS untuk muatan APM Anda yang perlu dicerna oleh AWS Incident Detection and Response.

AWS Incident Detection and Response akan menginstal aturan terkelola (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) pada bus peristiwa kustom atau default melalui `AWSServiceRoleForHealth_EventProcessor` SLR. Sumber aturan akan menjadi bus peristiwa khusus atau default, tujuan aturan adalah AWS Incident Detection and Response, dan aturan akan cocok dengan pola untuk menelan peristiwa APM pihak ke-3.

Pengoptimalan alarm dan penyesuaian pemantauan

Untuk memastikan akurasi deteksi insiden yang optimal, Insinyur Manajemen Insiden kami terus mengevaluasi kinerja alarm terhadap beban kerja kritis Anda. Kami menyediakan perubahan

konfigurasi alarm yang disarankan, yang harus Anda lakukan, dan secara proaktif berkolaborasi dengan Anda dan Manajer Akun Teknis (TAM) Anda untuk menyempurnakan pengaturan ini.

Ketika data pemantauan menunjukkan bahwa alarm mungkin tidak selaras dengan operasi penting bisnis Anda, seperti ketika peringatan dipicu tanpa dampak pelanggan yang sesuai atau ketika status alarm sering berfluktuasi, kami sarankan untuk melepaskan alarm non-kritis dan alarm orientasi yang lebih mencerminkan dampak beban kerja yang kritis. Ini membantu menjaga efektivitas keseluruhan cakupan respons insiden Anda.

Ulasan alarm dan umpan balik

AWS Incident Detection and Response melakukan tinjauan komprehensif terhadap alarm Anda sebelum melakukan onboarding untuk pemantauan. Alarm dievaluasi berdasarkan kriteria penerimaan teknis termasuk parameter konfigurasi, kualitas data, dan efektivitas peringatan.

Berdasarkan ulasan ini, dua jenis umpan balik disediakan:

- Persyaratan konfigurasi wajib - perubahan ini harus diterapkan untuk penerimaan alarm.
- Rekomendasi perbaikan opsional - perubahan ini meningkatkan efektivitas alarm tetapi tidak wajib untuk penerimaan alarm.

Setelah menerima umpan balik ini, Anda dapat memutuskan untuk melanjutkan dengan hanya orientasi alarm yang diterima dan mereka yang membutuhkan perbaikan opsional, sambil mengerjakan perubahan konfigurasi untuk alarm dengan persyaratan konfigurasi wajib secara paralel.

Atau, Anda dapat menerapkan semua perubahan sebelum ditayangkan. Pendekatan ini memperluas timeline orientasi, berdasarkan jumlah alarm yang membutuhkan penyesuaian.

Alarm ditayangkan

Setelah alarm menelan selesai, AWS Incident Detection and Response memungkinkan pemantauan beban kerja Anda. Mulai saat ini, alarm onboard Anda dipantau secara aktif dan AWS Incident Detection and Response melibatkan Anda sesuai runbook beban kerja saat alarm onboard Anda memasuki status ALARM.

Output kunci

- Beban kerja Anda dikonfirmasi sebagai live dan dipantau oleh AWS Incident Detection and Response.

Langkah selanjutnya

- Untuk memvalidasi bahwa alarm onboard Anda menggunakan Deteksi dan Respons Insiden AWS seperti yang diharapkan, lihat. Uji beban kerja onboard di Deteksi dan Respons Insiden
- Untuk membuat perubahan pada alarm onboard, runbook, atau informasi beban kerja Anda, lihat. Meminta perubahan pada beban kerja onboard di Deteksi dan Respons Insiden

Kuesioner orientasi beban kerja dan konsumsi alarm di Deteksi dan Respons Insiden (jalur pengecualian)

> **Note**
>
> Jika Anda tidak dapat menggunakan IDR CLI untuk mengisi beban kerja Anda, gunakan kuesioner berikut untuk beban kerja dan orientasi alarm.

Topik ini menyediakan kuesioner yang perlu Anda lengkapi saat melakukan onboarding beban kerja ke AWS Incident Detection and Response dan saat mengonfigurasi alarm untuk masuk ke dalam layanan. Kuesioner orientasi beban kerja mencakup informasi umum tentang beban kerja Anda, detail arsitekturnya, dan kontak untuk respons insiden. Dalam kuesioner konsumsi alarm, Anda menentukan alarm kritis yang memicu pembuatan insiden di Deteksi dan Respons Insiden untuk beban kerja Anda, serta informasi buku runbook tentang siapa yang harus dihubungi dan tindakan apa yang harus diambil. Mengisi kuesioner ini dengan benar adalah langkah kunci dalam menyiapkan proses pemantauan dan respons insiden untuk beban kerja Anda AWS .

Unduh kuesioner orientasi Beban Kerja:

- Versi bahasa Inggris
- Versi Jepang

Unduh kuesioner konsumsi Alarm:

- Versi bahasa Inggris
- Versi Jepang

Kuesioner orientasi beban kerja - Pertanyaan umum

Pertanyaan umum

Pertanyaan	Contoh Respons
Nama Perusahaan	Amazon Inc.
Nama beban kerja ini (termasuk singkatan apa pun)	Operasi Ritel Amazon (ARO)
Pengguna akhir primer dan fungsi beban kerja ini.	Beban kerja ini adalah aplikasi e-commerce yang memungkinkan pengguna akhir untuk membeli berbagai item. Beban kerja ini adalah penghasil pendapatan utama untuk bisnis kami.

Kuesioner orientasi beban kerja - Pertanyaan arsitektur

Pertanyaan arsitektur

Pertanyaan	Contoh Respons
Daftar tag AWS sumber daya yang digunakan untuk menentukan sumber daya yang merupakan bagian dari beban kerja ini. AWS menggunakan tag ini untuk mengidentifikasi sumber daya beban kerja ini untuk mempercepat dukungan selama insiden. **Note** Tag peka terhadap huruf besar dan kecil. Jika Anda memberikan beberapa tag, semua sumber daya yang digunakan oleh beban kerja ini harus memiliki tag yang sama.	AppName: Optimax lingkungan: Produksi

Pertanyaan	Contoh Respons
Daftar Layanan AWS(s) yang digunakan oleh beban kerja ini, Akun AWS(s) dan Wilayah AWS(s) tempat mereka berada.	Layanan AWS: Rute 53, ALB, ECS,... Akun: 123456789101, 123456789102,... Wilayah: US-EAST-1, US-WEST-2,...

Kuesioner konsumsi alarm - Ikhtisar

Dalam kuesioner menelan alarm, Anda menentukan alarm penting untuk beban kerja yang ingin Anda gunakan untuk Deteksi dan Respons Insiden AWS, serta kontak yang ingin digunakan oleh Insinyur Manajemen Insiden saat alarm ini dipicu.

Kuesioner Alarm Ingestion dibagi menjadi beberapa bagian berikut:

- Bagian Kontak: Pertama, tentukan kontak utama yang akan disertakan pada Dukungan Kasus yang dibuat dengan Deteksi dan Respons Insiden AWS saat alarm dipicu, serta aplikasi konferensi pilihan Anda untuk jembatan insiden. Jika tidak ada preferensi bridge yang diberikan, AWS Incident Detection and Response akan membuat jembatan insiden selama insiden. Selanjutnya, tentukan kontak eskalasi dan interval waktu untuk melibatkan mereka ketika kontak utama tidak dapat dijangkau. Terakhir, daftarkan kontak apa pun yang harus menerima pembaruan status insiden reguler melalui kasus dukungan selama insiden terjadi.
- Matriks alarm: Buat daftar set alarm yang akan melibatkan Deteksi dan Respons Insiden AWS saat dipicu. Lihat “Kriteria Alarm Kritis” yang ditentukan oleh Deteksi dan Respons Insiden AWS saat memilih alarm untuk orientasi. Untuk informasi selengkapnya, lihat Definisi alarm.
  - CloudWatch Alarm Amazon (biarkan bagian ini kosong jika Anda tidak memiliki CloudWatch alarm Amazon)
  - Alarm APM pihak ketiga (biarkan bagian ini kosong jika Anda tidak memiliki alarm APM pihak ketiga)
    - EventBridge EventBus ARN: Ini adalah ARN dari ARN khusus yang Anda buat EventBus di atau. Ingest Alarm dari APM dengan integrasi langsung EventBridge Menelan alarm dari APM tanpa integrasi langsung dengan EventBridge
    - Pengidentifikasi Alarm: Bagikan nomor akun, wilayah, dan nama alarm APM.

Kuesioner konsumsi alarm - Pertanyaan buku runbook

Pertanyaan buku runbook

Pertanyaan	Contoh Respons
AWS melibatkan kontak beban kerja melalui kasus ini Dukungan . Siapa kontak utama ketika alarm memicu beban kerja ini? Tentukan aplikasi konferensi pilihan Anda dan AWS akan meminta rincian ini selama insiden. **Note** Jika aplikasi konferensi pilihan tidak disediakan, maka AWS akan menghubungi selama insiden dan menyediakan jembatan Chime bagi Anda untuk bergabung.	Tim Aplikasi app@example.com +61 2 3456 7890
Jika kontak utama tidak tersedia selama insiden, harap berikan kontak eskalasi dan garis waktu dalam urutan komunikasi pilihan.	1. Setelah 10 menit, jika tidak ada tanggapan dari Kontak Utama, libatkan: John Smith - Pengawas Aplikasi john.smith@example.com +61 2 3456 7890 2. Setelah 10 menit, jika tidak ada tanggapan dari John Smith, hubungi: Jane Smith - Manajer Operasi jane.smith@example.com +61 2 3456 7890

Matriks alarm

Berikan informasi berikut untuk mengidentifikasi kumpulan alarm yang akan melibatkan Deteksi dan Respons Insiden AWS untuk membuat insiden atas nama beban kerja Anda. Setelah teknisi dari AWS Incident Detection and Response meninjau alarm Anda, langkah orientasi tambahan akan dikirimkan.

Deteksi dan Respons Insiden AWS Kriteria alarm kritis:

- Alarm Deteksi dan Respons Insiden AWS hanya boleh memasukkan status “Alarm” setelah dampak bisnis yang signifikan terhadap beban kerja yang dipantau (hilangnya pengalaman revenue/degraded pelanggan) yang memerlukan perhatian operator segera.
- Alarm Deteksi dan Respons Insiden AWS juga harus melibatkan resolver Anda untuk beban kerja pada saat yang sama atau sebelum keterlibatan. AWS Manajer Insiden berkolaborasi dengan resolver Anda dalam proses mitigasi, dan tidak berfungsi sebagai responden lini pertama yang kemudian meningkat kepada Anda.
- Ambang batas alarm Deteksi Insiden dan Respons AWS harus disetel ke ambang batas dan durasi yang sesuai sehingga setiap kali alarm memicu investigasi harus dilakukan. Jika alarm bergerak di antara status “Alarm” dan “OK”, dampak yang cukup akan terjadi untuk menjamin respons dan perhatian operator.

Kebijakan Deteksi dan Respons Insiden AWS untuk pelanggaran kriteria:

Kriteria ini hanya dapat dievaluasi berdasarkan kasus per kasus saat peristiwa terjadi. Tim Manajemen Insiden bekerja dengan manajer akun teknis (TAM) Anda untuk menyesuaikan alarm dan dalam kasus yang jarang terjadi menonaktifkan pemantauan jika diduga alarm pelanggan tidak mematuhi kriteria ini dan melibatkan tim Manajemen Insiden secara tidak perlu dengan tarif reguler.

> **Important**
>
> Berikan alamat email distribusi grup saat memberikan alamat kontak, sehingga Anda dapat mengontrol penambahan dan penghapusan penerima tanpa pembaruan runbook.
> Berikan nomor telepon kontak untuk tim rekayasa keandalan situs (SRE) Anda jika Anda ingin tim Deteksi dan Respons Insiden AWS menelepon mereka setelah mengirim email keterlibatan awal.

Tabel matriks alarm untuk CloudWatch alarm

CloudWatch alarm ARN	Kontak utama untuk alarm ini. (Jika berbeda dari beban kerja kontak utama)	Tentukan yang paling relevan Layanan AWS untuk alarm ini untuk melibatkan insinyur yang tepat. Masukkan N/A jika tidak diperlukan.
Contoh: `arn:aws:cloudwatch:us-east-1:123456789012:alarm:ALB_5xx_Target_Response`	Contoh: Sam Smith - Manajer Aplikasi sam.smith@example.com +61 2 3456 7890	Contoh: ECS

Tabel matriks alarm untuk alarm APM pihak ketiga

EventBridge Bus Acara ARN
 	
(Ini dibuat sebagai bagian dari integrasi APM pihak ketiga untuk merutekan peringatan ke Deteksi dan Respons Insiden AWS.)
		Contoh: (Akan ada bus acara per Account/Region kombinasi)
		
		`arn:aws:events:us-east-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus`
		
		`arn:aws:events:us-west-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus`	

Pengidentifikasi Alarm	Apa yang diwakili oleh metrik ini? Mengapa alarm ini penting?	Kontak utama untuk alarm ini. (Jika berbeda dari beban kerja kontak utama)	Tentukan yang paling relevan Layanan AWS untuk alarm ini untuk melibatkan insinyur yang tepat. Masukkan N/A jika tidak diperlukan.

Contoh: Alb_5xx_ Target_Response ID Akun: 123456789012 Wilayah: us-east-1	Contoh: Metrik ini mewakili respons transaksi dari target di belakang ALB. Jika kesalahan 5XX melebihi ambang batas, ini merupakan kegagalan kritis untuk memproses transaksi bisnis.	Contoh: Sam Smith - Manajer Aplikasi sam.smith@example.com +61 2 3456 7890	Contoh: ECS

Kelola beban kerja di Deteksi dan Respons Insiden

Bagian penting dari manajemen insiden yang efektif adalah memiliki proses dan prosedur yang tepat untuk melakukan onboard, menguji, dan mempertahankan beban kerja Anda yang dipantau. Bagian ini mencakup langkah-langkah penting, termasuk mengembangkan runbook komprehensif dan rencana respons untuk memandu tim Anda melalui insiden, menguji dan memvalidasi beban kerja baru secara menyeluruh, meminta perubahan untuk memperbarui pemantauan beban kerja, dan melepaskan beban kerja dengan benar bila diperlukan.

Topik

Kembangkan runbook dan rencana respons untuk menanggapi insiden di Deteksi dan Respons Insiden

AWS Incident Detection and Response menggunakan informasi yang diambil dari orientasi IDR CLI Anda untuk mengembangkan runbook untuk pengelolaan insiden yang memengaruhi beban kerja Anda. Runbook mendokumentasikan langkah-langkah yang diambil Manajer Insiden saat menanggapi suatu insiden. Rencana respons dipetakan ke setidaknya satu dari beban kerja Anda. Tim manajemen insiden membuat template ini dari informasi yang Anda berikan selama orientasi beban kerja.

Output kunci:

- Penyelesaian definisi beban kerja Anda pada Deteksi dan Respons Insiden AWS.
- Penyelesaian alarm dan runbook di AWS Incident Detection and Response.

Anda juga dapat mengunduh contoh AWS Incident Detection and Response Runbook: aws-idr-runbook-example.zip.

Contoh runbook

Example Contoh runbook

Deskripsi

Dokumen ini ditujukan untuk [CustomerName] - [WorkloadName].

Langkah: Prioritas

Tindakan prioritas

1. Kirim korespondensi pertama tentang Dukungan kasus ini kepada pelanggan seperti di bawah ini.

```
Hello,

This is <<Engineer's name>> from AWS Incident Detection and Response. An alarm has
 triggered for your workload <<Application_Name>>. I am currently investigating and
 will update you in a few minutes once I have finished initial investigation.

Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
```

Langkah: Informasi

Rencana keterlibatan

Bagian ini menjelaskan rencana keterlibatan yang berlaku untuk buku runbook ini dan hanya berisi detail kontak. Rencana keterlibatan akan direferensikan dalam Rencana Komunikasi langkah demi langkah.

- Keterlibatan awal

  AWS Incident Detection and Response Team menambahkan alamat pemangku kepentingan pelanggan di bawah ini ke kasus ini. Dukungan AWS Pemangku kepentingan adalah untuk pemangku kepentingan tambahan yang mungkin perlu disadarkan akan masalah apa pun.

  - Pemangku Kepentingan Pelanggan: customeremail1; customeremail2; mobile1
  - AWS Pemangku kepentingan: aws-idr-oncall@amazon.com; tam-tim-email; dll.
  - One Time Only Contacts: [Ini adalah kontak email yang disertakan hanya pada komunikasi pertama. Hapus kontak ini setelah komunikasi pertama padam. Ini bisa berupa alamat email

paging pelanggan seperti pager-duty yang tidak boleh dipaged untuk setiap korespondensi. Secara eksplisit menambahkan instruksi di bagian “Prioritas”, “Rencana komunikasi” tentang cara menggunakannya hanya jika Kontak Satu Kali Saja tersedia.]

- Pengaturan panggilan insiden

  Tunjukkan jika pelanggan memerlukan Deteksi dan Respons Insiden AWS untuk membuat jembatan, jika pelanggan menggunakan jembatan statis atau jika pelanggan akan menyediakan jembatan saat insiden dibuka.

  (Pilih satu opsi berdasarkan preferensi pelanggan)

  - Deteksi dan Respons Insiden AWS membuat Chime/Zoom Jembatan Amazon
  - Jembatan statis yang disediakan pelanggan
    - Nomor Konferensi: **<** Insert Conference number **>**
  - Pelanggan memberikan rincian jembatan untuk setiap insiden dengan menanggapi komunikasi yang dikirim oleh AWS Incident Detection and Response Team.
  - Lainnya - Tentukan detail.
- Eskalasi Keterlibatan

  Deteksi dan Respons Insiden AWS akan menghubungi kontak berikut jika kontak dari paket keterlibatan Awal tidak merespons insiden.

  Untuk setiap Kontak Eskalasi menunjukkan apakah mereka harus ditambahkan ke Dukungan kasing, menelepon atau keduanya.

  - Pastikan bahwa Anda telah menelepon kontak Keterlibatan Awal, jika ada, sebelum meningkatkan.
  - Kontak Eskalasi Pertama: [eskalasi EmailAddress #1]/[PhoneNumber] - Tunggu XX Menit sebelum eskalasi ke kontak ini.
    - [Tambahkan kontak ke Kasus/Telepon] kontak ini.
  - Kontak Eskalasi Kedua: [eskalasi EmailAddress #2]/[PhoneNumber] - Tunggu XX Menit sebelum eskalasi ke kontak ini.
    - [Tambahkan Kontak ke Kasus/Telepon] kontak ini.
  - dll.

Rencana komunikasi

Bagian ini menjelaskan bagaimana Insinyur Manajemen Insiden berkomunikasi dengan pemangku kepentingan yang ditunjuk di luar panggilan insiden dan saluran komunikasi.

- Rencana Komunikasi Dampak

  Rencana ini dimulai ketika AWS Incident Detection and Response telah menentukan dari langkah Triage bahwa peringatan menunjukkan potensi dampak bagi pelanggan.

  Deteksi dan Respons Insiden AWS akan meminta pelanggan untuk bergabung dengan jembatan yang telah ditentukan seperti yang ditunjukkan dalam paket Keterlibatan - Penyiapan panggilan insiden.

  (Pilih satu tergantung pada apakah One Time Only Contacts tersedia atau tidak.)

  1. Pastikan Pemangku Kepentingan Pelanggan dari rencana Keterlibatan - Keterlibatan awal ditambahkan ke kasus CC.

  ATAU

  1. Pastikan Pemangku Kepentingan Pelanggan dan Kontak Satu Kali Saja dari rencana Keterlibatan - Keterlibatan awal ditambahkan ke CC kasus.
  2. Kirim notifikasi keterlibatan ke pelanggan berdasarkan template berikut:

     (Pilih salah satu)

     Templat Dampak - Jembatan Amazon Chime

     ```
     The following alarm has engaged AWS Incident Detection and Response to an Incident
      bridge:
         Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
         Alarm State Change Reason - <insert_state_change_reason>
         Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
     Please join the Amazon Chime Bridge below so we can start the steps outlined in
      your Runbook:
         Amazon Chime Meeting ID: <insert_Meeting_ID_here>
         Link to Amazon Chime Bridge: <insert_Link_here>
         International dial-in numbers: https://chime.aws/dialinnumbers/
     ```

     Template Dampak - Jembatan yang Disediakan Pelanggan

     ```
     The following alarm has engaged AWS Incident Detection and Response:
         Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
     ```

```
    Alarm State Change Reason - <insert_state_change_reason>
    Alarm Start Time - <Example: 1 January 2025 3:30 PM UTC>
Please respond with your internal bridge details so we can join and start the steps
 outlined in your Runbook.
```

Templat Dampak - Jembatan Statis Pelanggan

```
The following alarm has engaged AWS Incident Detection and Response to an Incident
 bridge:
    Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
    Alarm State Change Reason - <insert_state_change_reason>
    Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
Please join the Bridge below so we can start the steps outlined in your Runbook:
    Conference Number: <insert_conference_number>
    Conference URL: <insert_bridge_URL>
```

3. Atur Kasus ke Tindakan Pelanggan yang Tertunda.
4. HAPUS Satu Kali Saja Kontak dari kasing setelah mengirim Komunikasi Dampak di atas. (Jika Kontak Satu Kali Saja tersedia.)
5. Ikuti rencana Eskalasi Keterlibatan seperti yang disebutkan di atas.
6. Jika pelanggan tidak merespons dalam waktu 30 menit, lepaskan dan terus pantau hingga alarm pulih.

- Rencana Komunikasi Tanpa Dampak

  Rencana ini dimulai ketika alarm pulih sebelum Deteksi dan Respons Insiden menyelesaikan Triase awal.

  1. Sebelum mengirim notifikasi tanpa dampak, verifikasi, lalu hapus and/or tambahkan kontak pelanggan dari CC Dukungan Kasus berdasarkan kontak yang tercantum dalam Rencana Keterlibatan - Rencana Keterlibatan Awal.

     ["JANGAN tambahkan Kontak Satu Kali Saja."] (Berlaku jika Kontak Satu Kali Saja tersedia.)
  2. Kirim pemberitahuan tanpa keterlibatan kepada pelanggan berdasarkan templat di bawah ini:

     Template Tanpa Dampak

```
AWS Incident Detection and Response received an alarm that has recovered for your
 workload.
    Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
    Alarm State Change Reason - <insert_state_change_reason>
```

```
    Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
    Alarm End Time - <Example: 1 January 2025, 3:35 PM UTC>
This may indicate a brief customer impact that is currently not ongoing.
If there is an ongoing impact to your workload, please let us know and we will
 engage to assist.
```

3. Masukkan kasing ke dalam Tindakan Pelanggan yang Tertunda.
4. Jika pelanggan tidak merespons dalam waktu 30 menit, selesaikan kasusnya.

Ikhtisar arsitektur aplikasi

Bagian ini memberikan ikhtisar application/workload arsitektur untuk kesadaran Insinyur Manajemen Insiden dan Insinyur Operasi.

- AWS Akun dan Wilayah dengan layanan utama - daftar AWS akun dengan Wilayah yang mendukung aplikasi ini. Membantu Insinyur dalam menilai infrastruktur dasar yang mendukung aplikasi.
  - 123456789012
    - US-EAST-1 - desc singkat yang sesuai
      - Amazon EC2 - desc singkat yang sesuai
      - DynamoDB - desc singkat yang sesuai
      - dll.
    - US-WEST-1 - desc singkat yang sesuai
      - dll.
  - akun lain
    - dll.

Uji beban kerja onboard di Deteksi dan Respons Insiden

Setelah Alarm Tertelan selesai, AWS Incident Detection and Response memungkinkan pemantauan beban kerja Anda dan mengirimkan konfirmasi. Go-Live Beban kerja Anda dipantau secara aktif dari titik ini ke depan.

Pengujian alarm memvalidasi bahwa alarm onboard Anda menggunakan Deteksi dan Respons Insiden AWS seperti yang diharapkan, memicu runbook yang sesuai, dan tindakan lain yang diinginkan, seperti pembuatan casing otomatis jika Anda memilihnya selama penggunaan alarm.

Pengujian bersifat opsional tetapi sangat disarankan. Anda bertanggung jawab untuk memvalidasi pengaturan respons Anda sebelum insiden nyata terjadi.

Opsi pengujian

AWS Incident Detection and Response menawarkan dua opsi pengujian.

Opsi 1: Dijadwalkan GameDay (disarankan)

Terjadwal GameDay adalah simulasi end-to-end langsung dari apa yang mungkin terjadi selama insiden nyata. AWS Incident Detection and Response mengikuti langkah-langkah runbook yang ditentukan untuk memberi Anda wawasan tentang bagaimana insiden nyata dapat terjadi. GameDay Ini adalah kesempatan bagi Anda untuk mengajukan pertanyaan atau menyempurnakan instruksi untuk meningkatkan keterlibatan.

Untuk menjadwalkan a GameDay, selesaikan langkah-langkah berikut:

1. Beri tahu Deteksi dan Respons Insiden AWS dengan tanggal yang diinginkan dan jendela waktu 1 jam, termasuk zona waktu. Berikan setidaknya 48 jam lead time.
2. Rencanakan sumber daya untuk GameDay, termasuk SRE/Ops tim Anda dan kontak eskalasi.

GameDay jadwal:

1. Anda dan AWS Incident Detection and Response bergabung dalam panggilan.
2. Anda menonaktifkan tindakan alarm, jika berlaku.
3. Anda secara manual mengatur alarm Anda ke status ALARM menggunakan instruksi diCara menguji alarm Anda.
4. Deteksi dan Respons Insiden AWS mengonfirmasi penerimaan pemberitahuan alarm.
5. AWS Incident Detection and Response merespons alarm dan bergabung dengan bridge yang ditentukan dalam runbook Anda.
6. Anda dan AWS Incident Detection and Response mengonfirmasi GameDay hasilnya.

Opsi 2: Pengujian alarm offline

Anda dapat menguji alarm Anda secara independen kapan saja tanpa menjadwalkan panggilan. Memicu alarm melibatkan Deteksi dan Respons Insiden AWS sesuai dengan runbook Anda, seperti halnya selama insiden nyata.

Untuk melakukan pengujian alarm offline, selesaikan langkah-langkah berikut:

1. Untuk mencegah tindakan yang tidak diinginkan, nonaktifkan tindakan CloudWatch alarm Amazon apa pun.
2. Picu alarm Anda menggunakan instruksi diCara menguji alarm Anda.
3. Dalam 5 menit, kasus dukungan dibuat atas nama Anda dan AWS Incident Detection and Response melibatkan Anda sebagaimana ditentukan dalam runbook Anda.
4. Beri tahu Manajer Insiden bahwa Anda sedang melakukan pengujian alarm offline.
5. Manajer Insiden mengonfirmasi perubahan status alarm mana yang diterima dan memvalidasi pengaturan respons.

Jika kasus dukungan tidak dibuat dalam waktu 5 menit, kirimkan permintaan insiden untuk melibatkan Deteksi dan Respons Insiden AWS secara manual untuk pemecahan masalah.

Cara menguji alarm Anda

CloudWatch Alarm Amazon

> **Note**
>
> AWS Identity and Access Management Pengguna atau peran yang Anda gunakan untuk pengujian alarm harus memiliki `cloudwatch:SetAlarmState` izin.

Gunakan AWS Command Line Interface atau AWS CloudShelluntuk mengatur alarm Anda secara manual ke status ALARM. Perintah ini mengubah status alarm tanpa memengaruhi beban kerja Anda.

Untuk mencegah tindakan yang tidak diinginkan, misalnya instans Amazon EC2 dimulai ulang, nonaktifkan tindakan alarm CloudWatch apa pun sebelum Anda mengubah status alarm. Anda dapat mengaktifkan kembali tindakan CloudWatch alarm setelah pengujian selesai. Untuk mempelajari selengkapnya tentang menonaktifkan atau mengaktifkan tindakan alarm, lihat DisableAlarmActionsdan EnableAlarmActionsdi Referensi Amazon CloudWatch API.

Nonaktifkan tindakan alarm:

```
aws cloudwatch disable-alarm-actions --alarm-names "ExampleAlarm" --region us-east-1
```

Setel status alarm ke ALARM:

```
aws cloudwatch set-alarm-state --alarm-name "ExampleAlarm" --state-value ALARM --state-reason "Testing AWS Incident Detection and Response" --region us-east-1
```

Re-enable tindakan alarm setelah pengujian:

```
aws cloudwatch enable-alarm-actions --alarm-names "ExampleAlarm" --region us-east-1
```

Status alarm kembali ke OK secara otomatis dalam beberapa detik.

Alarm komposit

`set-alarm-state`Perintah tidak menjamin bahwa alarm komposit kembali ke status OK. Sebagai praktik terbaik, verifikasi status alarm komposit setelah pengujian. Untuk mengatur ulang alarm komposit secara manual, gunakan perintah berikut:

```
aws cloudwatch set-alarm-state --alarm-name "ExampleCompositeAlarm" --state-value OK --state-reason "Testing AWS Incident Detection and Response" --region us-east-1
```

Untuk mempelajari selengkapnya tentang mengubah status CloudWatch alarm secara manual, lihat SetAlarmStatedi Referensi Amazon CloudWatch API.

Untuk mempelajari lebih lanjut tentang izin yang diperlukan untuk operasi CloudWatch API, lihat referensi CloudWatch izin Amazon.

Third-party Alarm APM

Beban kerja yang menggunakan alat Application Performance Monitoring (APM) pihak ketiga, seperti Datadog, Splunk, New Relic, atau Dynatrace, memerlukan instruksi yang berbeda untuk mensimulasikan alarm.

1. Nonaktifkan tindakan alarm di APM Anda untuk mencegah tindakan yang tidak diinginkan.
2. Ubah ambang alarm atau operator perbandingan Anda untuk memaksa alarm ke status ALARM. Ini memicu payload ke AWS Incident Detection and Response.
3. Setelah pengujian selesai, putar kembali ambang batas atau perubahan operator perbandingan untuk mengembalikan alarm ke status OK.

Hasil utama

Setelah pengujian berhasil:

- Konsumsi alarm dikonfirmasi dan konfigurasi alarm Anda benar.
- Alarm diterima oleh AWS Incident Detection and Response.
- Kasus dukungan dibuat dan kontak yang Anda tentukan diberi tahu.
- Deteksi dan Respons Insiden AWS melibatkan Anda dengan cara konferensi yang ditentukan.
- Semua alarm dan kasus dukungan yang dihasilkan selama pengujian diselesaikan.

Pertanyaan umum

Apakah pengujian alarm wajib?

Tidak. Pengujian bersifat opsional tetapi sangat disarankan untuk memvalidasi pengaturan respons ujung ke ujung Anda sebelum insiden nyata terjadi.

Apakah beban kerja saya akan terpengaruh?

Tidak. Namun, selama pengujian tindakan alarm apa pun yang dikonfigurasi pada alarm Anda dipicu kecuali Anda menonaktifkannya. Nonaktifkan tindakan alarm sebelum pengujian untuk mencegah dampak yang tidak diinginkan.

Siapa yang diberitahu selama pengujian?

Selama jadwal GameDay, semua kontak dan jalur eskalasi di runbook Anda dihubungi untuk verifikasi. Selama pengujian alarm offline, hanya kontak awal yang ditentukan selama orientasi alarm yang diberitahukan.

Dapatkah saya membalas melalui email ke pembaruan kasus?

Tidak. Salinan email korespondensi Dukungan kasus dikirim dari alamat tanpa balasan. Untuk memperbarui kasus, gunakan file AWS Support Center Console.

Bagaimana cara meminta GameDay setelah go-live?

Balas kasus dukungan orientasi Anda yang ada, jika ada, atau buatMeminta perubahan pada beban kerja onboard di Deteksi dan Respons Insiden.

Meminta perubahan pada beban kerja onboard di Deteksi dan Respons Insiden

Untuk meminta perubahan pada beban kerja onboard, selesaikan langkah-langkah berikut untuk membuat kasus dukungan dengan AWS Incident Detection and Response.

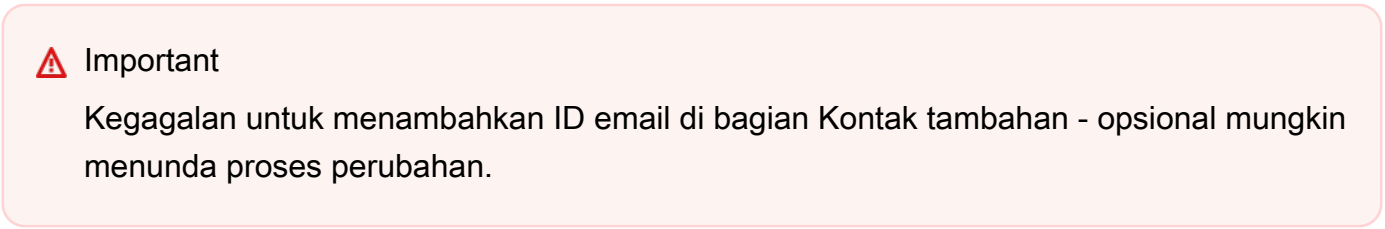
1. Pergi ke AWS Dukungan Pusat, lalu pilih Buat kasus, seperti yang ditunjukkan pada contoh berikut:

2. Pilih Teknis.
3. Untuk Layanan, pilih Deteksi dan Respons Insiden.
4. Untuk Kategori, pilih Permintaan perubahan beban kerja.
5. Untuk Keparahan, pilih Panduan Umum.
6. Masukkan Subjek untuk perubahan ini. Contoh:

   Deteksi dan Respons Insiden AWS - *`workload_name`*
7. Masukkan Deskripsi untuk perubahan ini. Misalnya, masukkan “Permintaan ini untuk perubahan pada beban kerja yang ada yang terhubung ke AWS Incident Detection and Response”. Pastikan Anda menyertakan informasi berikut dalam permintaan Anda:

   - Nama beban kerja: Nama beban kerja Anda.
   - ID Akun: ID1, ID2, ID3, dan sebagainya.
   - Rincian perubahan: Masukkan detail untuk perubahan yang Anda minta.
8. Di bagian Kontak tambahan - opsional, masukkan ID email apa pun yang ingin Anda terima korespondensi tentang perubahan ini.

   Berikut ini adalah contoh Kontak tambahan - bagian opsional.



> **Important**
>
> Kegagalan untuk menambahkan ID email di bagian Kontak tambahan - opsional mungkin menunda proses perubahan.

9. Pilih Kirim.

Setelah mengirimkan permintaan perubahan, Anda dapat menambahkan email tambahan dari organisasi Anda. Untuk menambahkan email, pilih Balas dalam detail Kasus, seperti yang ditunjukkan pada contoh berikut:

Kemudian, tambahkan ID email di bagian Kontak tambahan - opsional.

Berikut ini adalah contoh halaman Balas yang menunjukkan di mana Anda dapat memasukkan email tambahan.

Menekan alarm agar tidak melibatkan Deteksi dan Respons Insiden

Tentukan alarm beban kerja onboard mana yang terhubung dengan AWS Incident Detection and Response monitoring dengan menekannya sementara atau sesuai jadwal. Misalnya, Anda dapat menekan sementara alarm beban kerja selama pemeliharaan yang direncanakan untuk mencegah alarm terlibat Deteksi dan Respons Insiden. Atau, Anda dapat menekan alarm pada jadwal jika Anda memiliki aktivitas reboot harian. Anda dapat menekan alarm di sumber alarm, seperti Amazon CloudWatch, atau Anda dapat mengirimkan permintaan perubahan beban kerja.

Topik

- Menekan alarm di sumber alarm
- Kirim permintaan perubahan beban kerja untuk menekan alarm
- Tutorial: Gunakan fungsi matematika metrik untuk menekan alarm
- Tutorial: Hapus fungsi matematika metrik untuk menghapus alarm

Menekan alarm di sumber alarm

Tentukan alarm mana yang terlibat dengan Deteksi dan Respons Insiden dan kapan mereka melakukannya dengan menekan alarm di sumber alarm.

Topik

- Gunakan fungsi matematika metrik untuk menekan alarm CloudWatch
- Hapus fungsi matematika metrik untuk menghapus alarm CloudWatch
- Contoh fungsi matematika metrik dan kasus penggunaan terkait

- Menekan alarm dari APM pihak ketiga

Gunakan fungsi matematika metrik untuk menekan alarm CloudWatch

Untuk menekan Deteksi Insiden dan pemantauan Respons CloudWatch alarm Amazon, gunakan fungsi matematika metrik untuk menghentikan CloudWatch alarm memasuki `ALARM` status selama jendela yang ditentukan.

> **Note**
>
> Menonaktifkan tindakan Alarm pada CloudWatch alarm tidak menekan pemantauan alarm Anda dengan Deteksi dan Respons Insiden. Perubahan status alarm dicerna melalui Amazon EventBridge, bukan melalui tindakan CloudWatch alarm.

Untuk menggunakan fungsi matematika metrik untuk menekan CloudWatch alarm, selesaikan langkah-langkah berikut:

1. Masuk ke Konsol Manajemen AWS dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Alarm, lalu cari alarm yang ingin Anda tambahkan fungsi matematika metrik.
3. Pilih Tindakan, lalu pilih Edit untuk mengubah alarm.
4. Pilih Edit metrik untuk mengubah metrik alarm.
5. Pilih Tambahkan matematika, Mulai dengan ekspresi kosong.
6. Masukkan ekspresi matematika Anda, lalu pilih Terapkan.
7. Hapus pilihan metrik yang ada yang dipantau alarm.
8. Pilih ekspresi yang baru saja Anda buat, lalu pilih Pilih metrik.
9. Pilih Lewati ke Pratinjau dan buat.
10. Tinjau perubahan Anda untuk memastikan bahwa fungsi matematika metrik Anda diterapkan seperti yang diharapkan, lalu pilih Perbarui alarm.

Untuk contoh langkah demi langkah menekan CloudWatch alarm dengan fungsi matematika metrik, lihatTutorial: Gunakan fungsi matematika metrik untuk menekan alarm.

Untuk informasi selengkapnya tentang sintaks dan fungsi yang tersedia, lihat Sintaks dan fungsi matematika metrik di CloudWatch Panduan Pengguna Amazon.

Hapus fungsi matematika metrik untuk menghapus alarm CloudWatch

Hapus CloudWatch alarm dengan menghapus fungsi matematika metrik. Untuk menghapus fungsi matematika metrik dari alarm, selesaikan langkah-langkah berikut:

1. Masuk ke Konsol Manajemen AWS dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Alarm, lalu cari alarm atau alarm tempat Anda ingin menghapus ekspresi matematika metrik.
3. Di bagian matematika metrik, pilih Edit.
4. Untuk menghapus metrik dari alarm, pilih Edit pada metrik, lalu pilih tombol x di sebelah ekspresi matematika metrik.
5. Pilih metrik asli, lalu pilih Pilih metrik.
6. Pilih Lewati ke Pratinjau dan buat.
7. Tinjau perubahan Anda untuk memastikan bahwa fungsi matematika metrik Anda diterapkan seperti yang diharapkan, lalu pilih Perbarui alarm.

Contoh fungsi matematika metrik dan kasus penggunaan terkait

Tabel berikut berisi contoh fungsi matematika metrik, bersama dengan kasus penggunaan terkait dan penjelasan dari setiap komponen metrik.

Fungsi matematika metrik	Kasus penggunaan	Penjelasan
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	Menekan alarm antara 1:00 hingga 3:00 AM UTC setiap hari Selasa dengan mengganti titik data nyata dengan 0 selama jendela ini.	• HARI (m1) == 2: Memastikan hari Selasa (Senin = 1, Minggu = 7). • JAM (m1) >= 1 && JAM (m1) > 3: Menentukan rentang waktu dari 1 pagi sampai 3 pagi UTC. • IF (condition, value_if_true, value_if_false :Jika kondisi benar, maka ganti nilai

Fungsi matematika metrik	Kasus penggunaan	Penjelasan
		metrik dengan 0. Jika tidak, kembalikan nilai asli (m1)
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	Menekan alarm antara 11:00 PM hingga 4:00 AM UTC, setiap hari dengan mengganti titik data nyata dengan 0 selama jendela ini.	• JAM (m1) >= 23: Menangkap jam mulai pukul 23:00 UTC. • JAM (m1) < 4: Menangkap jam hingga (tetapi tidak termasuk) 04:00 UTC. • ||: Logis ATAU memastikan kondisi ini berlaku di dua rentang — jam larut malam dan dini hari. • IF (condition, value_if_true, value_if_false): Mengembalikan 0 selama rentang waktu yang ditentukan. Mempertahankan nilai metrik asli m1 di luar rentang itu.
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	Menekan alarm antara 11:00 AM hingga 1:00 PM UTC setiap hari dengan mengganti titik data nyata dengan 0 selama jendela ini.	• JAM (m1) >= 11 && JAM (m1) < 13: Menangkap rentang waktu dari 11:00 hingga 13:00 UTC. • IF (condition, value_if_true, value_if_false): Jika kondisi benar (misalnya, waktunya antara 11:00 dan 13:00 UTC), kembalikan 0, Jika kondisinya salah, pertahankan nilai metrik asli (m1).

Fungsi matematika metrik	Kasus penggunaan	Penjelasan
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	Menekan alarm antara 1:00 hingga 3:00 AM UTC setiap hari Selasa dengan mengganti titik data nyata dengan 99 selama jendela ini.	• HARI (m1) == 2:: Memastikan hari Selasa (Senin = 1, Minggu = 7). • JAM (m1) >= 1 && JAM (m1) < 3: Menentukan rentang waktu dari 1 AM sampai 3 AM UTC. • IF (condition, value_if_true, value_if_false): Jika kondisi benar, ganti nilai metrik dengan 99. Jika tidak, kembalikan nilai asli (m1).
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	Menekan alarm antara 11:00 PM hingga 4:00 AM UTC, setiap hari dengan mengganti titik data nyata dengan 100 selama jendela ini.	• JAM (m1) >= 23: Menangkap jam mulai pukul 23:00 UTC. • JAM (m1) < 4: Menangkap jam hingga (tetapi tidak termasuk) 04:00 UTC. • ||: Logis ATAU memastikan kondisi ini berlaku di dua rentang — jam larut malam dan dini hari. • IF (condition, value_if_true, value_if_false): Mengembalikan 100 selama rentang waktu yang ditentukan. Mempertahankan nilai metrik asli m1 di luar rentang itu.

Fungsi matematika metrik	Kasus penggunaan	Penjelasan
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	Menekan alarm antara 11:00 AM hingga 1:00 PM UTC setiap hari dengan mengganti titik data nyata dengan 99 selama jendela ini.	• JAM (m1) >= 11 && JAM (m1) < 13: Menangkap rentang waktu dari 11:00 hingga 13:00 UTC. • IF (condition, value_if_true, value_if_false): Jika kondisi benar (misalnya, waktunya antara 11:00 dan 13:00 UTC), kembalikan 99. Jika kondisinya salah, pertahankan nilai metrik asli (m1).

Menekan alarm dari APM pihak ketiga

Lihat dokumentasi vendor APM pihak ketiga Anda untuk petunjuk tentang cara menekan alarm. Contoh vendor APM pihak ketiga adalah New Relic, Splunk, Dynatrace, Datadog, dan. SumoLogic

Kirim permintaan perubahan beban kerja untuk menekan alarm

Jika Anda tidak dapat menekan alarm di sumber seperti yang dijelaskan di bagian sebelumnya, kirimkan Permintaan Perubahan Beban Kerja untuk menginstruksikan Deteksi dan Respons Insiden untuk secara manual menekan pemantauan sebagian atau semua alarm beban kerja Anda.

Untuk petunjuk mendetail tentang cara membuat Permintaan Perubahan Beban Kerja, lihat Meminta perubahan ke beban kerja onboard di Deteksi dan Respons Insiden. Saat menaikkan Permintaan Perubahan Beban Kerja untuk meminta penindasan alarm Anda, pastikan Anda memberikan informasi yang diperlukan berikut

- Nama beban kerja: Nama beban kerja Anda.
- ID Akun: ID1,, ID2 ID3, dan sebagainya.
- Ubah detail: Penindasan Alarm
- Waktu mulai penindasan: Tanggal, waktu, dan zona waktu.
- Waktu akhir penindasan: Tanggal, waktu, dan zona waktu.

- Alarm untuk ditekan: Daftar CloudWatch alarm ARNs atau pengidentifikasi acara APM pihak ketiga untuk ditekan.

Setelah membuat Permintaan Perubahan Beban Kerja penekanan alarm, Anda menerima pemberitahuan berikut dari Deteksi dan Respons Insiden:

- Pengakuan Permintaan Perubahan Beban Kerja Anda.
- Pemberitahuan saat alarm ditekan.
- Pemberitahuan saat alarm diaktifkan kembali untuk pemantauan.

Tutorial: Gunakan fungsi matematika metrik untuk menekan alarm

Tutorial berikut memandu Anda melalui cara menekan CloudWatch alarm menggunakan matematika metrik.

Contoh skenario

Ada kegiatan yang direncanakan yang berlangsung antara 1:00 hingga 3:00 AM UTC pada hari Selasa mendatang. Anda ingin membuat fungsi matematika CloudWatch metrik yang menggantikan titik data nyata selama waktu ini, dengan 0 (titik data yang berada di bawah ambang batas yang ditetapkan).

1. Nilai kriteria yang menyebabkan alarm Anda terpicu. Screenshot berikut memberikan contoh kriteria alarm:

   Alarm yang ditampilkan pada tangkapan layar sebelumnya memonitor `UnHealthyHostCount` metrik untuk grup target Application Load Balancer. Alarm ini memasuki `ALARM` keadaan ketika `UnHealthyHostCount` metrik lebih besar dari atau sama dengan 3 untuk 5 dari 5 titik data. Alarm memperlakukan data yang hilang sebagai hal yang buruk (melanggar ambang batas yang dikonfigurasi).
2. Buat fungsi matematika metrik.

   Dalam contoh ini, kegiatan yang direncanakan berlangsung antara pukul 1:00 hingga 3:00 UTC pada hari Selasa mendatang. Jadi, buat fungsi matematika CloudWatch metrik yang menggantikan titik data nyata selama waktu ini, dengan 0 (titik data yang berada di bawah ambang batas yang ditetapkan).

Perhatikan bahwa titik data pengganti yang harus Anda konfigurasikan berbeda tergantung pada konfigurasi alarm Anda. Misalnya, jika Anda memiliki alarm yang memantau tingkat keberhasilan HTTP, dengan ambang kurang dari 98, maka ganti titik data nyata Anda selama aktivitas yang direncanakan dengan nilai di atas ambang batas yang dikonfigurasi, 100. Berikut ini adalah contoh fungsi matematika metrik untuk skenario ini.

```
IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)
```

Fungsi matematika metrik sebelumnya berisi elemen-elemen berikut:

- HARI (m1) == 2: Memastikan hari Selasa (Senin = 1, Minggu = 7).
- JAM (m1) >= 1 && JAM (m1) < 3: Menentukan rentang waktu dari 1 AM sampai 3 AM UTC.
- IF (condition, value_if_true, value_if_false): Jika kondisi benar, fungsi menggantikan nilai metrik dengan 0. Jika tidak, nilai asli (m1) dikembalikan.

Untuk informasi tambahan tentang sintaks dan fungsi yang tersedia, lihat Sintaks dan fungsi matematika metrik di Panduan Pengguna Amazon CloudWatch

3. Masuk ke Konsol Manajemen AWS dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
4. Pilih Alarm, lalu cari alarm yang ingin Anda tambahkan fungsi matematika metrik.
5. Di bagian matematika metrik, pilih Edit.
6. Pilih Tambahkan matematika, Mulai dengan ekspresi kosong.
7. Masukkan ekspresi matematika Anda, lalu pilih Terapkan.

   Metrik yang ada yang dipantau alarm secara otomatis menjadi m1 dan ekspresi matematika Anda adalah e1, seperti yang ditunjukkan pada contoh berikut:

8. (Opsional) Edit label ekspresi matematika metrik untuk membantu orang lain memahami fungsinya dan mengapa itu dibuat, seperti yang ditunjukkan pada contoh berikut:

9. Hapus pilihan m1, pilih e1, lalu pilih Pilih metrik. Ini menyetel alarm untuk memantau ekspresi matematika alih-alih metrik yang mendasarinya secara langsung.
10. Pilih Lewati ke Pratinjau dan buat.

11. Validasi bahwa alarm dikonfigurasi seperti yang diharapkan, lalu pilih Perbarui alarm untuk menyimpan perubahan.

Dalam contoh sebelumnya, tanpa fungsi matematika metrik yang diterapkan, `UnHealthyHostCount` metrik sebenarnya akan dilaporkan selama aktivitas yang direncanakan. Ini akan mengakibatkan CloudWatch alarm memasuki `ALARM` status dan melibatkan Deteksi dan Respons Insiden, seperti yang ditunjukkan pada contoh berikut:

Dengan fungsi matematika metrik di tempat, titik data nyata diganti dengan 0 selama aktivitas, dan alarm tetap dalam `OK` status, menekan keterlibatan Deteksi Insiden dan Respons.

Tutorial: Hapus fungsi matematika metrik untuk menghapus alarm

Jika Anda menekan CloudWatch alarm untuk aktivitas satu kali, hapus fungsi matematika metrik dari alarm setelah aktivitas selesai untuk melanjutkan pemantauan alarm secara teratur. Untuk menekan alarm pada jadwal reguler, misalnya, jika Anda memiliki rutinitas penambalan mingguan terjadwal yang menghasilkan reboot instance pada hari dan waktu yang sama setiap minggu, maka biarkan fungsi matematika metrik di tempatnya.

Tutorial berikut memandu Anda melalui cara menghapus fungsi matematika metrik untuk menghapus alarm CloudWatch

1. Masuk ke Konsol Manajemen AWS dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Alarm, lalu cari alarm yang ingin Anda tambahkan fungsi matematika metrik.
3. Di bagian matematika metrik, pilih Edit.
4. Untuk menghapus penekanan dari alarm, pilih tombol x di sebelah ekspresi matematika metrik.
5. Pilih metrik untuk melanjutkan pemantauan metrik sebenarnya. lalu pilih Pilih metrik.
6. Pilih Lewati ke Pratinjau dan buat.
7. Validasi bahwa alarm dikonfigurasi seperti yang diharapkan, lalu pilih Perbarui alarm untuk menyimpan perubahan.

Lepas beban kerja dari Deteksi dan Respons Insiden

Untuk melepaskan beban kerja dari AWS Incident Detection and Response, buat kasus dukungan baru untuk setiap beban kerja. Saat Anda membuat kasus dukungan, ingatlah hal berikut:

- Untuk melepaskan beban kerja yang ada dalam satu AWS akun, buat kasus dukungan baik dari akun beban kerja atau dari akun pembayar Anda.
- Untuk melepaskan beban kerja yang mencakup beberapa AWS akun, buat kasus dukungan dari akun pembayar Anda. Di badan kasus dukungan, daftarkan semua ID akun ke offboard.

> **Important**
>
> Jika Anda membuat kasus dukungan untuk melepaskan beban kerja dari akun yang salah, Anda mungkin mengalami penundaan dan permintaan informasi tambahan sebelum beban kerja Anda dapat diturunkan.

Permintaan untuk melepaskan beban kerja

1. Pergi ke AWS Dukungan Pusat, lalu pilih Buat kasus.
2. Pilih Teknis.
3. Untuk Layanan, pilih Deteksi dan Respons Insiden.
4. Untuk Kategori, pilih Workload Offboarding.
5. Untuk Keparahan, pilih Panduan Umum.
6. Masukkan Subjek untuk perubahan ini. Contoh:

   [Offboard] Deteksi dan Respons Insiden AWS - *`workload_name`*
7. Masukkan Deskripsi untuk perubahan ini. Misalnya, masukkan “Permintaan ini untuk offboarding beban kerja yang ada yang terhubung ke AWS Incident Detection and Response”. Pastikan Anda menyertakan informasi berikut dalam permintaan Anda:

   - Nama beban kerja: Nama beban kerja Anda.
   - ID Akun: ID1, ID2, ID3, dan sebagainya.
   - Alasan offboarding: Berikan alasan untuk melepaskan beban kerja.
8. Di bagian Kontak tambahan - opsional, masukkan ID email apa pun yang ingin Anda terima korespondensi tentang permintaan offboarding ini.

9. Pilih Kirim.

Deteksi Insiden AWS dan pemantauan dan observabilitas Respons

AWS Incident Detection and Response menawarkan panduan ahli tentang menentukan observabilitas di seluruh beban kerja Anda mulai dari lapisan aplikasi hingga infrastruktur yang mendasarinya. Pemantauan memberi tahu Anda bahwa ada sesuatu yang salah. Observabilitas menggunakan pengumpulan data untuk memberi tahu Anda apa yang salah dan mengapa itu terjadi.

Sistem Deteksi dan Respons Insiden memantau AWS beban kerja Anda dari kegagalan dan penurunan kinerja dengan memanfaatkan AWS layanan asli seperti Amazon dan CloudWatch Amazon EventBridge untuk mendeteksi peristiwa yang dapat memengaruhi beban kerja Anda. Pemantauan memberi Anda pemberitahuan tentang kegagalan yang akan terjadi, sedang berlangsung, surut, atau potensi kegagalan atau penurunan kinerja. Saat Anda memasukkan akun Anda ke Deteksi dan Respons Insiden, Anda memilih alarm mana di akun Anda yang harus dipantau oleh sistem pemantauan Deteksi Insiden dan Respons dan Anda mengaitkan alarm tersebut dengan aplikasi dan buku runbook yang digunakan selama manajemen insiden.

Deteksi dan Respons Insiden menggunakan Amazon CloudWatch dan lainnya Layanan AWS untuk membangun solusi observabilitas Anda. AWS Incident Detection and Response membantu Anda dengan observabilitas dalam dua cara:

- Metrik Hasil Bisnis: Pengamatan pada Deteksi dan Respons Insiden AWS dimulai dengan menentukan metrik utama yang memantau hasil beban kerja atau pengalaman pengguna akhir Anda. AWS Para ahli bekerja sama dengan Anda untuk memahami tujuan beban kerja Anda, output utama atau faktor yang dapat memengaruhi pengalaman pengguna, dan untuk menentukan metrik dan peringatan yang menangkap degradasi apa pun dalam metrik utama tersebut. Misalnya metrik bisnis utama untuk aplikasi panggilan seluler adalah Tingkat Sukses Pengaturan Panggilan (memantau tingkat keberhasilan upaya panggilan pengguna), dan metrik kunci untuk situs web adalah kecepatan halaman. Keterlibatan insiden dipicu berdasarkan metrik hasil bisnis.
- Metrik tingkat infrastruktur: Pada tahap ini, kami mengidentifikasi dasar Layanan AWS dan infrastruktur yang mendukung aplikasi Anda dan menentukan metrik dan alarm untuk melacak kinerja layanan infrastruktur ini. Ini mungkin termasuk metrik seperti `ApplicationLoadBalancerErrorCount` untuk instance Application Load Balancer. Ini dimulai setelah beban kerja telah di-onboard dan pemantauan diatur.

Menerapkan observabilitas pada Deteksi dan Respons Insiden AWS

Karena observabilitas adalah proses berkelanjutan yang mungkin tidak diselesaikan dalam satu latihan atau kerangka waktu, AWS Incident Detection and Response mengimplementasikan observabilitas dalam dua fase:

- Fase orientasi: Observabilitas selama orientasi difokuskan pada pendeteksian kapan hasil bisnis aplikasi Anda terganggu. Untuk tujuan ini, observabilitas selama fase orientasi difokuskan pada mendefinisikan metrik hasil bisnis utama di lapisan aplikasi untuk memberi tahu AWS gangguan pada beban kerja Anda. Cara ini AWS dapat segera menanggapi gangguan ini dan memberi Anda bantuan menuju pemulihan. Untuk mempelajari selengkapnya tentang menggunakan AWS Incident Detection and Response Customer Command Line Interface untuk membantu mengotomatiskan langkah-langkah ini, lihat CLI for AWS Incident Detection and Response.
- Post-onboarding fase: AWS Incident Detection and Response menawarkan sejumlah layanan proaktif untuk observabilitas termasuk definisi metrik tingkat infrastruktur, penyetelan metrik, dan pengaturan jejak dan log tergantung, pada tingkat kematangan pelanggan. Implementasi layanan ini dapat berlangsung beberapa bulan dan melibatkan banyak tim. AWS Incident Detection and Response memberikan panduan tentang penyiapan observabilitas dan pelanggan diharuskan untuk menerapkan perubahan yang diperlukan di lingkungan beban kerja mereka. Untuk bantuan implementasi langsung fitur observabilitas, ajukan permintaan ke manajer akun teknis (TAM) Anda.

Manajemen insiden dengan Deteksi dan Respon Insiden

AWS Incident Detection and Response menawarkan Anda 24 jam sehari, 7 hari seminggu pemantauan proaktif dan manajemen insiden yang disampaikan oleh tim manajer insiden yang ditunjuk. Diagram berikut menguraikan proses manajemen insiden standar ketika alarm aplikasi memicu insiden, termasuk pembuatan alarm, keterlibatan Manajer AWS Insiden, resolusi insiden, dan tinjauan pasca-insiden.

1. Pembuatan alarm: Alarm yang dipicu pada beban kerja Anda didorong melalui Amazon ke Deteksi dan Respons Insiden EventBridge AWS. AWS Incident Detection and Response secara otomatis menarik runbook yang terkait dengan alarm Anda dan memberi tahu manajer insiden. Jika insiden kritis terjadi pada beban kerja Anda yang tidak terdeteksi oleh alarm yang dipantau oleh Deteksi dan Respons Insiden AWS, Anda dapat membuat kasus dukungan untuk meminta Respons Insiden. Untuk informasi lebih lanjut tentang meminta Respons Insiden, lihatMeminta Tanggapan Insiden.
2. AWS Keterlibatan Manajer Insiden: Manajer insiden merespons alarm dan melibatkan Anda pada panggilan konferensi atau sebagaimana ditentukan dalam buku runbook. Manajer insiden memverifikasi kesehatan Layanan AWS untuk menentukan apakah alarm terkait dengan masalah yang Layanan AWS digunakan oleh beban kerja dan memberi nasihat tentang status layanan yang mendasarinya. Jika diperlukan, manajer insiden kemudian membuat kasus atas nama Anda dan melibatkan AWS ahli yang tepat untuk mendapatkan dukungan. Karena Deteksi dan Respons Insiden AWS memantau Layanan AWS secara khusus untuk aplikasi Anda, Deteksi dan Respons Insiden AWS dapat menentukan bahwa insiden tersebut terkait dengan Layanan AWS masalah sebelum Layanan AWS peristiwa dideklarasikan. Dalam skenario ini, manajer insiden memberi tahu Anda tentang status Layanan AWS, memicu alur kerja manajemen insiden Layanan AWS peristiwa, dan menindaklanjuti dengan tim layanan tentang resolusi. Informasi yang diberikan memberi Anda kesempatan untuk mengimplementasikan rencana pemulihan atau solusi Anda lebih awal untuk mengurangi dampak acara. Layanan AWS

   Terkadang alarm memicu dan cepat pulih. Dalam skenario ini, manajer insiden mengirimkan korespondensi kasus yang menyatakan alarm telah pulih, tetapi tidak melibatkan Anda. Namun, jika alarm memicu lebih dari sekali dalam 15 menit, manajer insiden melibatkan Anda sesuai instruksi runbook Anda, bahkan jika alarm pulih.

3. Resolusi insiden: Manajer insiden mengoordinasikan insiden di seluruh AWS tim yang diperlukan dan memastikan bahwa Anda tetap terlibat dengan AWS ahli yang tepat sampai insiden tersebut dikurangi atau diselesaikan.
4. Peninjauan Pasca Insiden (jika diminta): Setelah insiden, Deteksi dan Respons Insiden AWS dapat melakukan peninjauan pasca insiden atas permintaan Anda dan menghasilkan Laporan Pasca Insiden. Laporan Post Incident mencakup deskripsi masalah, dampak, tim mana yang terlibat, dan solusi atau tindakan yang diambil untuk mengurangi atau menyelesaikan insiden tersebut. Post Incident Report mungkin berisi informasi yang dapat digunakan untuk mengurangi kemungkinan terulangnya insiden, atau untuk meningkatkan pengelolaan kejadian di masa depan dari insiden serupa. Post Incident Report bukanlah Root Cause Analysis (RCA). Anda dapat meminta RCA selain Laporan Insiden Pasca. Contoh Laporan Pasca Insiden disediakan di bagian berikut.

> **⚠ Important**
>
> Template laporan berikut adalah contoh saja.

```
Post ** Incident ** Report ** Template
Post Incident Report - 0000000123
Customer: Example Customer
AWS Dukungan case ID(s): 0000000000
Customer internal case ID (if provided): 1234567890
Incident start: 2023-02-04T03:25:00 UTC
Incident resolved: 2023-02-04T04:27:00 UTC
Total Incident time: 1:02:00 s
Source Alarm ARN: arn:aws:cloudwatch:us-east-1:000000000000:alarm:alarm-prod-workload-
impaired-useast1-P95

Problem Statement:
Outlines impact to end users and operational infrastructure impact.
 Starting at 2023-02-04T03:25:00 UTC, the customer experienced a large scale outage
 of their workload that lasted one hour and two minutes and spanning across all
 Availability Zones where the application is deployed. During impact, end users were
 unable to connect to the workload's Application Load Balancers (ALBs) which service
 inbound communications to the application.

Incident Summary:
```

```
Summary of the incident in chronological order and steps taken by AWS Incident Managers
 to direct the incident to a path to mitigation.
  At 2023-02-04T03:25:00 UTC, the workload impairments alarm triggered a critical
 incident for the workload. AWS Incident Detection and Response Managers responded to
 the alarm, checking AWS service health and steps outlined in the workload's runbook.
  At 2023-02-04T03:28:00 UTC, ** per the runbook, the alarm had not recovered and the
 Incident Management team sent the engagement email to the customer's Site Reliability
 Team (SRE) team, created a troubleshooting bridge, and an Dukungan support case on
 behalf of the customer.
  At 2023-02-04T03:32:00 UTC, ** the customer's SRE team, and Dukungan Engineering
 joined the bridge. The Incident Manager confirmed there was no on-going AWS impact to
 services the workload depends on. The investigation shifted to the specific resources
 in the customer account.
  At 2023-02-04T03:45:00 UTC, the Cloud Support Engineer discovered a sudden increase
 in traffic volume was causing a drop in connections. The customer confirmed this
 ALB was newly provisioned to handle an increase in workload traffic for an on-going
 promotional event.
  At 2023-02-04T03:56:00 UTC, the customer instituted back off and retry logic. The
 Incident Manager worked with the Cloud Support Engineer to raise an escalation a
 higher support level to quickly scale the ALB per the runbook.
  At 2023-02-04T04:05:00 UTC, ALB support team initiates scaling activities. The
 back-off/retry logic yields mild recovery but timeouts are still being seen for some
 clients.
 By 2023-02-04T04:15:00 UTC, scaling activities complete and metrics/alarms return to
 pre-incident levels. Connection timeouts subside.
  At 2023-02-04T04:27:00 UTC, per the runbook the call was spun down, after 10 minutes
 of recovery monitoring. Full mitigation is agreed upon between AWS and the customer.

Mitigation:
Describes what was done to mitigate the issue. NOTE: this is not a Root Cause Analysis
 (RCA).
  Back-off and retries yielded mild recovery. Full mitigation happened after escalation
 to ALB support team (per runbook) to scale the newly provisioned ALB.

Follow up action items (if any):
Action items to be reviewed with your Technical Account Manager (TAM), if required.
Review alarm thresholds to engage AWS Incident Detection and Response closer to the
 time of impact.
Work with AWS Dukungan and TAM team to ensure newly created ALBs are pre-scaled to
 accommodate expected spikes in workload traffic.
```

Topik

- Menyediakan akses ke AWS Support Center Console untuk tim aplikasi

- Meminta Tanggapan Insiden
- Kelola kasus dukungan Deteksi Insiden dan Respons dengan AWS Support App in Slack

Menyediakan akses ke AWS Support Center Console untuk tim aplikasi

AWS Incident Detection and Response berkomunikasi dengan Anda melalui Dukungan kasus selama siklus hidup insiden. Untuk berkorespondensi dengan Manajer Insiden, tim Anda harus memiliki akses ke Dukungan Pusat.

Untuk informasi selengkapnya tentang penyediaan akses, lihat Mengelola akses ke Dukungan Pusat di Dukungan Panduan Pengguna.

Meminta Tanggapan Insiden

Jika insiden kritis terjadi pada beban kerja Anda yang tidak terdeteksi oleh alarm yang dipantau oleh AWS Incident Detection and Response, Anda dapat membuat kasus dukungan untuk meminta Respons Insiden. Anda dapat meminta Respons Insiden untuk beban kerja apa pun yang berlangganan Deteksi dan Respons Insiden AWS, termasuk beban kerja dalam proses orientasi, menggunakan API, atau. AWS Support Center Console AWS Dukungan AWS Support App in Slack

Diagram berikut menggambarkan alur kerja ujung ke ujung untuk AWS pelanggan yang meminta bantuan insiden dari tim Deteksi dan Respons Insiden, merinci langkah-langkah dari permintaan awal melalui investigasi, mitigasi, dan resolusi.

Untuk meminta Respons Insiden atas insiden yang secara aktif memengaruhi beban kerja Anda, buat kasus. Dukungan Setelah kasus dukungan dinaikkan, AWS Incident Detection and Response melibatkan Anda di jembatan konferensi dengan AWS para ahli yang diperlukan untuk mempercepat pemulihan beban kerja Anda.

Meminta Respons Insiden menggunakan AWS Support Center Console

Untuk meminta tanggapan insiden, selesaikan langkah-langkah berikut:

1. Buka AWS Support Center Consoleuntuk membuat kasus dukungan baru.
2. Untuk Subjek, masukkan ringkasan singkat insiden tersebut. Misalnya, `AWS Incident Detection and Response - Active Incident - workload_name`.

3. Untuk Deskripsi, masukkan detail kejadian. Kami menyarankan Anda menyertakan detail berikut dalam kasus dukungan Anda:

   - ARN AWS sumber daya yang terpengaruh, nama beban kerja dan fungsinya
   - Deskripsi dampak terhadap bisnis
   - (Opsional) URL jembatan konferensi pilihan Anda. Jika Anda tidak memberikan detail bridge, AWS Incident Detection and Response akan membuat jembatan AWS konferensi dan mengirimi Anda undangan dengan URL bridge.
4. (Opsional) Lampirkan file yang dapat membantu menggambarkan kejadian, seperti tangkapan layar atau kutipan log.
5. Konfigurasikan bidang klasifikasi kasus berikut:

   - Jenis kasus: Teknis
   - Layanan: Deteksi dan Respon Insiden
   - Kategori: Insiden Aktif
   - Keparahan: Business-critical sistem turun
6. Berikan konteks tambahan untuk membantu AWS Incident Detection and Response melibatkan AWS para ahli dengan lebih cepat, seperti dampak Layanan AWS, dampak Wilayah AWS, dampak bisnis, waktu mulai dampak, dan sumber daya yang terpengaruh.
7. Pilih Kirim.
8. AWS Incident Detection and Response mengakui kasus Anda dalam waktu lima menit dan melibatkan Anda di jembatan konferensi dengan para ahli yang sesuai AWS .

Meminta Respons Insiden menggunakan AWS Dukungan API

Anda dapat menggunakan AWS Dukungan API untuk membuat kasus dukungan secara terprogram. Untuk informasi selengkapnya, lihat Tentang AWS Dukungan API di Panduan AWS Dukungan Pengguna.

Meminta Respons Insiden menggunakan AWS Support App in Slack

Untuk menggunakan aplikasi AWS Support App in Slack untuk meminta Respons Insiden, selesaikan langkah-langkah berikut:

1. Buka saluran Slack yang Anda AWS Support App in Slack konfigurasikan.
2. Masukkan perintah berikut:

```
/awssupport create
```

3. Masukkan Subjek untuk kejadian ini. Misalnya, masukkan AWS Incident Detection and Response - Active Incident - workload_name.
4. Masukkan Deskripsi Masalah untuk kejadian ini. Tambahkan detail berikut:

   Informasi Teknis:

   Layanan yang Terkena Dampak:

   Sumber Daya yang Terdampak:

   Wilayah yang Terdampak:

   Nama Beban Kerja:

   Informasi Bisnis:

   Deskripsi dampak terhadap bisnis:

   [Opsional] Detail Jembatan Pelanggan:
5. Pilih Berikutnya.

6. Untuk Jenis Masalah, pilih Dukungan teknis.
7. Untuk Layanan, pilih Deteksi dan Respons Insiden.
8. Untuk Kategori, pilih Insiden Aktif.
9. Untuk Keparahan, pilih Business-critical sistem ke bawah.

10. Secara opsional masukkan hingga 10 kontak tambahan di bidang Kontak tambahan untuk memberi tahu, dipisahkan dengan koma. Kontak tambahan ini menerima salinan korespondensi email tentang insiden ini.

11. Pilih Tinjau.
12. Pesan baru yang hanya terlihat oleh Anda muncul di saluran Slack. Tinjau detail kasus, lalu pilih Buat kasus.

13 ID Kasus Anda disediakan dalam pesan baru dari file AWS Support App in Slack.

14 Deteksi dan Respons Insiden mengakui kasus Anda dalam waktu 5 menit dan melibatkan Anda di jembatan konferensi dengan para ahli yang sesuai AWS .

15 Korespondensi dari Deteksi dan Respons Insiden diperbarui di utas kasus.

Kelola kasus dukungan Deteksi Insiden dan Respons dengan AWS Support App in Slack

Dengan itu AWS Support App in Slack, Anda dapat mengelola Dukungan kasus di Slack, menerima pemberitahuan tentang insiden baru yang dimulai alarm pada beban kerja Deteksi dan Respons Insiden AWS, dan membuat Permintaan Respons Insiden.

Untuk mengkonfigurasi AWS Support App in Slack, ikuti petunjuk yang disediakan dalam Panduan Dukungan Pengguna.

Important

- Untuk menerima pemberitahuan di Slack untuk semua insiden yang dimulai alarm pada beban kerja Anda, Anda harus mengonfigurasi AWS Support App in Slack untuk semua akun beban kerja Anda yang terhubung ke Deteksi dan Respons Insiden AWS. Kasus Support dibuat di akun tempat alarm beban kerja berasal.
- Beberapa kasus dukungan tingkat keparahan tinggi dapat dibuka atas nama Anda selama insiden untuk melibatkan Dukungan resolver. Anda menerima notifikasi di Slack untuk semua kasus dukungan yang dibuka selama insiden yang sesuai dengan konfigurasi notifikasi Anda untuk saluran Slack.
- Pemberitahuan yang Anda terima melalui AWS Support App in Slack tidak menggantikan kontak awal dan eskalasi beban kerja Anda yang terlibat melalui email atau panggilan telepon oleh Deteksi dan Respons Insiden selama AWS insiden terjadi.

Topik

- Pemberitahuan insiden yang diprakarsai alarm di Slack
- Buat Permintaan Respons Insiden di Slack

Pemberitahuan insiden yang diprakarsai alarm di Slack

Setelah mengonfigurasi saluran Slack, Anda menerima pemberitahuan tentang insiden yang dimulai alarm pada beban kerja yang dipantau Deteksi Insiden AWS dan Respons. AWS Support App in Slack

Contoh berikut menunjukkan bagaimana pemberitahuan untuk insiden yang dimulai alarm muncul di Slack.

Contoh pemberitahuan

Ketika insiden yang dimulai alarm Anda diakui oleh AWS Incident Detection and Response, pemberitahuan yang serupa dengan yang berikut akan dihasilkan di Slack:

Untuk melihat korespondensi lengkap yang ditambahkan oleh AWS Incident Detection and Response, pilih Lihat detail.

Pembaruan lebih lanjut dari AWS Incident Detection and Response muncul di thread case.

Pilih Lihat detail untuk melihat korespondensi lengkap yang ditambahkan oleh AWS Incident Detection and Response.

Buat Permintaan Respons Insiden di Slack

Untuk petunjuk tentang cara membuat Permintaan Respons Insiden melalui AWS Support App in Slack, lihatMeminta Tanggapan Insiden.

Pelaporan dalam Deteksi dan Respon Insiden

AWS Incident Detection and Response menyediakan data operasional dan kinerja untuk membantu Anda memahami cara layanan dikonfigurasi, riwayat insiden Anda, dan kinerja layanan Deteksi dan Respons Insiden. Halaman ini mencakup jenis data yang tersedia, termasuk data konfigurasi, data insiden, dan data kinerja.

Data konfigurasi

- Semua akun onboard
- Nama semua aplikasi
- Alarm, runbook, dan profil dukungan yang terkait dengan setiap aplikasi

Data insiden

- Tanggal, jumlah, dan durasi insiden untuk setiap aplikasi
- Tanggal, jumlah, dan durasi insiden yang terkait dengan alarm tertentu
- Laporan Pasca Insiden

Data kinerja

- Kinerja Tujuan Tingkat Layanan (SLO)

Hubungi Manajer Akun Teknis Anda untuk data operasional dan kinerja yang mungkin Anda perlukan.

Deteksi Insiden dan Keamanan Respon dan ketahanan

Model Tanggung Jawab AWS Bersama berlaku untuk perlindungan data di Dukungan. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Konten ini mencakup konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan.

Untuk informasi selengkapnya tentang privasi data, silakan lihat Pertanyaan Umum Privasi Data.

Untuk informasi tentang perlindungan data di Eropa, lihat Model Tanggung Jawab AWS Bersama dan posting blog GDPR di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi kredensyal AWS akun dan menyiapkan akun pengguna individu dengan AWS Identity and Access Management (IAM). Dengan cara ini, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut ini:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan sertifikat Secure SocketsLayer/Transport Layer Security (SSL/TLS) untuk berkomunikasi dengan AWS sumber daya. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru. Untuk selengkapnya, lihat Apa Itu Sertifikat SSL/TLS? .
- Siapkan API dan logging aktivitas pengguna dengan AWS CloudTrail. Untuk informasi, lihat AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data pribadi yang disimpan di Amazon S3. Untuk informasi tentang Amazon Macie, lihat Amazon Macie.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi tentang titik akhir FIPS yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti

bidang Nama. Ini termasuk ketika Anda bekerja dengan Dukungan atau lainnya Layanan AWS menggunakan konsol, API, AWS CLI, atau. AWS SDKs Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, sebaiknya Anda tidak menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Deteksi Insiden AWS dan Akses Respons ke akun Anda

AWS Identity and Access Management (IAM) adalah layanan web yang membantu Anda mengontrol akses ke AWS sumber daya dengan aman. Anda menggunakan IAM untuk mengontrol siapa yang diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya.

Deteksi dan Respons Insiden AWS serta data alarm Anda

Secara default, Deteksi dan Respons Insiden menerima nama sumber daya Amazon (ARN) dan status setiap CloudWatch alarm di akun Anda, lalu memulai proses deteksi dan respons insiden saat alarm yang terpasang berubah menjadi status ALARM. Jika Anda ingin menyesuaikan informasi yang diterima deteksi insiden dan respons tentang alarm dari akun Anda, hubungi Manajer Akun Teknis Anda.

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir panduan IDR.

Ubah	Deskripsi	Date
Topik Standar Amazon SNS yang diklarifikasi untuk integrasi APM	Mengklarifikasi bahwa pelanggan harus membuat topik Layanan Pemberitahuan Sederhana Amazon Standar (bukan FIFO) saat mengintegrasikan alarm APM pihak ketiga dengan AWS Incident Detection and Response. Untuk informasi selengkapnya, lihat Ingest Alarm dari APM dengan integrasi Amazon SNS langsung.	26 Mei 2026
GameDay sekarang opsional, kuesioner orientasi yang disederhanakan, dan pengembangan runbook yang diperbarui	Pengujian alarm yang diperbarui (GameDay) menjadi opsional setelahnya Go-Live, dengan dua opsi pengujian: pengujian alarm terjadwal GameDay atau offline. Menyederhanakan kuesioner orientasi beban kerja dan konsumsi alarm. Pengembangan runbook yang diperbaru i untuk menghapus referensi ke AWS Systems Manager dokumen. Lihat informasi selengkapnya di Uji beban kerja onboard di Deteksi dan Respons Insiden, Kuesioner orientasi beban kerja dan konsumsi alarm di Deteksi dan Respons Insiden (jalur pengecualian), dan Kembangkan runbook dan rencana respons untuk menanggapi insiden di Deteksi dan Respons Insiden.	26 Mei 2026
Prosedur Permintaan Tanggapan Insiden yang Diperbarui	Memperbarui prosedur Minta Respons Insiden agar sesuai dengan AWS Support Center Console UI saat ini, menambahkan panduan	12 Mei 2026

Ubah	Deskripsi	Date
	URL jembatan, dan menghapus tangkapan layar yang sudah ketinggalan zaman. Untuk informasi selengkapnya, lihat Meminta Respons Insiden menggunakan AWS Support Center Console.	
Orientasi yang diperbarui untuk didekati CLI-first	Memperbarui chapter Memulai untuk mempromosikan AWS Incident Detection and Response Customer Command Line Interface sebagai metode orientasi utama dan menghentikan Kuesioner Onboarding Beban Kerja dan Kuesioner Penyerapan Alarm sebagai jalur orientasi default. Kuesioner tetap tersedia sebagai opsi khusus pengecualian bagi pelanggan yang tidak dapat menggunakan IDR CLI. Untuk informasi selengkapnya, lihat Beban kerja onboard untuk Deteksi dan Respons Insiden dan Alarm Tertelan.	12 Mei 2026
Menambahkan tautan kuesioner Jepang	Menambahkan tautan Japanese-language unduhan untuk kuesioner orientasi Beban Kerja dan kuesioner konsumsi Alarm. Untuk informasi selengkapnya, lihat Kuesioner orientasi beban kerja dan konsumsi alarm di Deteksi dan Respons Insiden (jalur pengecualian).	April 20, 2026
Referensi arsitektur yang diperbarui	Menghapus referensi ke diagram arsitektur dan diganti dengan detail arsitektur. Untuk informasi selengkapnya, lihat Arsitektur Deteksi dan Respon Insiden dan Tentang beban kerja di Deteksi dan Respons Insiden.	Maret 31, 2026

Ubah	Deskripsi	Date
Beban kerja onboard Uji yang diperbarui dalam Deteksi dan Respons Insiden	Menambahkan informasi tentang menonakti fkan tindakan CloudWatch alarm sebelum mengubah status alarm selama pengujian. Untuk informasi selengkapnya, lihat Uji beban kerja onboard di Deteksi dan Respons Insiden.	Maret 2, 2026
Manajemen Insiden yang Diperbarui dengan Deteksi dan Respons Insiden	Menambahkan informasi tentang perilaku alarm berulang dan keterlibatan manajer insiden. Untuk informasi selengkapnya, lihat Manajemen insiden dengan Deteksi dan Respon Insiden.	Maret 2, 2026
Langkah-langkah yang diperbarui dalam fungsi Gunakan matematika metrik untuk menekan bagian CloudWatch alarm	Langkah-langkah yang diperbarui dalam fungsi Gunakan matematika metrik untuk menekan bagian CloudWatch alarm. Untuk informasi selengkapnya, lihat Menekan alarm di sumber alarm.	Februari 3, 2026
Menambahkan bahasa Korea sebagai bahasa yang didukung	Menambahkan bahasa Korea sebagai bahasa yang didukung. Untuk informasi selengkapnya, lihat Ketersedi aan wilayah untuk Deteksi dan Respons Insiden.	Januari 22 2026
Ditambahkan Mandarin sebagai bahasa yang didukung	Ditambahkan Mandarin sebagai bahasa yang didukung. Untuk informasi selengkapnya, lihat Ketersedi aan wilayah untuk Deteksi dan Respons Insiden.	Januari 13, 2026

Ubah	Deskripsi	Date
Menambahkan bagian baru: AWS Incident Detection and Response Customer Command Line Interface	Menambahkan bagian IDR CLI dan memperbarui chapter Memulai untuk menyertakan informasi tentang AWS Incident Detection and Response Customer Command Line Interface. Untuk informasi selengkapnya, lihat CLI untuk Deteksi dan Respons Insiden AWS.	Desember 8, 2025
Beberapa bagian yang diperbarui: Kuesioner orientasi beban kerja dan konsumsi alarm di Deteksi dan Respons Insiden dan Memulai Deteksi dan Respons Insiden	Proses penanganan Layanan AWS peristiwa tidak lagi menjadi bagian dari AWS Incident Detection and Response. Bagian dari panduan pengguna ini diperbarui untuk menghapus referensi ke proses ini. Anda akan terus menerima pemberitahuan acara layanan melalui AWS Service Health Dashboard . Pelanggan AWS Incident Detection and Response dapat menggunakan permintaan Respons Insiden untuk menerima bantuan selama peristiwa layanan sesuai kebutuhan. Untuk informasi selengkapnya, lihat Meminta Tanggapan Insiden.	Oktober 14, 2025
Bagian yang dihapus: Manajemen insiden untuk acara layanan	Proses penanganan Layanan AWS peristiwa tidak lagi menjadi bagian dari AWS Incident Detection and Response. Bagian panduan pengguna ini telah dihapus untuk mencermin kan perubahan ini. Anda akan terus menerima pemberitahuan acara layanan melalui AWS Service Health Dashboard. Pelanggan AWS Incident Detection and Response dapat menggunakan permintaan Respons Insiden untuk menerima bantuan selama peristiwa layanan sesuai kebutuhan. Untuk informasi selengkapnya, lihat Meminta Tanggapan Insiden.	Oktober 14, 2025

Ubah	Deskripsi	Date
Bagian yang diperbarui: Ketersediaan wilayah untuk Deteksi dan Respons Insiden	AWS Incident Detection and Response sekarang tersedia di AWS GovCloud (US-East) dan AWS GovCloud (US-West). Untuk informasi selengkapnya, lihat Ketersediaan wilayah untuk Deteksi dan Respons Insiden	Oktober 05, 2025
Bagian yang diperbarui: Kuesioner orientasi beban kerja dan konsumsi alarm di Deteksi dan Respons Insiden	Diperbarui contoh alamat email untuk tabel matriks Alarm.	Agustus 26, 2025
Bagian yang diperbarui: Berlangganan beban kerja ke Deteksi dan Respons Insiden AWS	Referensi yang dihapus ke bidang Tanggal mulai Berlangganan di bagian Deskripsi pada jendela Buat kasus. Bagian yang diperbarui: Berlangganan beban kerja ke Deteksi dan Respons Insiden AWS	Agustus 4, 2025
Fungsi baru: Menekan alarm agar tidak melibatkan Deteksi dan Respons Insiden	Menambahkan bagian baru ke Beban kerja terkelola yang memberikan informasi tentang cara menekan alarm sementara atau sesuai jadwal Bagian baru: Menekan alarm agar tidak melibatkan Deteksi dan Respons Insiden	April 9, 2025
Instruksi yang diperbarui untuk Meminta Tanggapan Insiden menggunakan AWS Support Center Console	Menambahkan detail tentang informasi apa yang harus dimasukkan di bidang Deskripsi masalah. Bagian yang diperbarui: Meminta Tanggapan Insiden	Februari 6, 2025

Ubah	Deskripsi	Date
Tambahan Wilayah AWS ditambahkan	Tambahan Wilayah AWS telah ditambahkan ke bagian Deteksi Insiden dan Ketersediaan Respons. Bagian yang diperbarui: Ketersediaan wilayah untuk Deteksi dan Respons Insiden	November 1, 2024
Pembaruan untuk Mengelola Deteksi Insiden dan kasus dukungan Respons dengan AWS Support App in Slack halaman	Memindahkan halaman di bawah Manajemen Insiden, teks yang direvisi, dan tangkapan layar yang diganti. Bagian yang diperbarui: Kelola kasus dukungan Deteksi Insiden dan Respons dengan AWS Support App in Slack	Oktober 10, 2024
Ditambahkan halaman baru AWS Support App in Slack Manajemen Insiden yang diperbarui dengan Deteksi dan Respons Insiden AWS	Ditambahkan halaman baru untuk AWS Support App in Slack Memperbarui manajemen Insiden dengan AWS Incident Detection and Response untuk menambahkan bagian baru, “Minta Respons Insiden menggunakan AWS Support App in Slack”.	September 10, 2024
Langganan Akun yang Diperbarui	Memperbarui bagian berlangganan Akun untuk menyertakan detail tentang tempat membuka kasus dukungan saat Anda meminta untuk berlangganan akun. Bagian yang diperbarui: Berlangganan beban kerja ke Deteksi dan Respons Insiden AWS	Juni 12, 2024

Ubah	Deskripsi	Date
Menambahkan bagian baru: Offboard beban kerja	Menambahkan bagian Offload a workload di Memulai untuk menyertakan informasi tentang beban kerja offboarding Untuk informasi selengkapnya, lihat Lepas beban kerja dari Deteksi dan Respons Insiden.	Maret 28, 2024
Langganan Akun yang Diperbarui	Memperbarui bagian langganan Akun untuk menyertakan informasi tentang beban kerja offboarding Untuk informasi selengkapnya, lihat Berlangga nan beban kerja ke Deteksi dan Respons Insiden AWS	Maret 28, 2024
Pengujian yang Diperbarui	Memperbarui bagian Pengujian untuk menyertakan informasi tentang pengujian gameday sebagai langkah terakhir dalam proses orientasi. Bagian yang diperbarui: Uji beban kerja onboard di Deteksi dan Respons Insiden	Februari 29, 2024
Memperbarui Apa itu Deteksi dan Respons Insiden AWS	Memperbarui bagian Apa itu Deteksi dan Respons Insiden AWS. Bagian yang diperbarui: Apa itu Deteksi dan Respons Insiden AWS?	Februari 19, 2024
Bagian Kuesioner yang Diperbarui	Memperbarui kuesioner orientasi Beban Kerja dan menambahkan kuesioner konsumsi Alarm. Mengganti nama bagian dari kuesioner Orientasi menjadi onboarding Beban Kerja dan kuesioner konsumsi Alarm.	Februari 2, 2024

Ubah	Deskripsi	Date
Acara AWS Layanan yang Diperbarui dan informasi orientasi	Memperbarui beberapa bagian dengan informasi baru untuk orientasi. Bagian yang diperbarui: • Beban kerja onboard untuk Deteksi dan Respons Insiden • Berlangganan beban kerja ke AWS Incident Detection and Response Bagian baru • Menyediakan akses ke AWS Support Center Console untuk tim aplikasi	Januari 31, 2024
Ditambahkan bagian informasi terkait	Menambahkan bagian informasi terkait dalam penyediaan Access. Bagian yang diperbarui: Menyediakan akses untuk menelan alarm ke Deteksi dan Respons Insiden	Januari 17, 2024
Langkah contoh yang diperbarui	Memperbarui prosedur untuk langkah 2,3, dan 4 di Contoh: Mengintegrasikan pemberitahuan dari Datadog dan Splunk. Bagian yang diperbarui: Contoh: Menginteg rasikan pemberitahuan dari Datadog dan Splunk	21 Desember 2023

Ubah	Deskripsi	Date
Grafik dan teks pengantar yang diperbarui	Grafik yang diperbarui di alarm Ingest dari APM yang memiliki integrasi langsung dengan Amazon. EventBridge Bagian yang diperbarui: Kembangkan runbook dan rencana respons untuk menanggapi insiden di Deteksi dan Respons Insiden	21 Desember 2023
Template runbook yang diperbarui	Memperbarui template runbook di Mengemban gkan runbook untuk AWS Incident Detection and Response. Bagian yang diperbarui: Kembangkan runbook dan rencana respons untuk menanggapi insiden di Deteksi dan Respons Insiden	Desember 4, 2023
Konfigurasi Alarm Diperbarui	Konfigurasi Alarm yang Diperbarui dengan informasi terperinci tentang konfigurasi CloudWatch alarm. Bagian baru: Buat CloudWatch alarm yang sesuai dengan kebutuhan bisnis Anda di Deteksi dan Respons Insiden Bagian baru: Bangun CloudWatch alarm di Deteksi Insiden dan Respons dengan template CloudFormation Bagian baru: Contoh kasus penggunaan untuk CloudWatch alarm di Deteksi dan Respons Insiden	28 September 2023

Ubah	Deskripsi	Date
Diperbarui Memulai	Memperbarui Memulai dengan informasi tentang permintaan perubahan Beban Kerja. Bagian baru: Meminta perubahan pada beban kerja onboard di Deteksi dan Respons Insiden Bagian yang diperbarui: Berlangganan beban kerja ke Deteksi dan Respons Insiden AWS	September 05, 2023
Bagian baru di Memulai	Menambahkan peringatan Ingesting ke AWS Incident Detection and Response.	Juni 30, 2023
Dokumen asli	Deteksi dan Respons Insiden AWS pertama kali diterbitkan	15 Maret 2023

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