AWS 보안 인시던트 대응 사용 설명서

버전 March 27, 2026

AWS 보안 인시던트 대응 사용 설명서:

Table of Contents

AWS 보안 인시던트 대응이란?

AWS 보안 인시던트 대응를 이용하면 보안 인시던트에 신속하게 대비 및 대응하고 인시던트로부터 복구하는 데 도움이 되는 지침을 받을 수 있습니다. 여기에는 계정 탈취, 데이터 침해, 랜섬웨어 공격과 같은 인시던트가 포함됩니다.

AWS 보안 인시던트 대응는 위협 조사 결과를 분류하고, 보안 이벤트를 에스컬레이션하며, 즉각적인 주의가 필요한 사례를 관리합니다. 또한 영향을 받는 리소스를 조사할 Security Incident Response 엔지니어에게 접근할 수 있습니다.

> **Note**
>
> 영향을 받는 리소스를 복구할 수 있다는 보장은 없습니다. 비즈니스 요구 사항에 영향을 줄 수 있는 리소스에 대한 백업을 설정하고 유지하는 것이 좋습니다.

AWS 보안 인시던트 대응는 다른 AWS의 탐지 및 대응 서비스와 연동하여 탐지부터 복구까지 인시던트 수명 주기 전체를 안내합니다.

내용

지원되는 구성

AWS 보안 인시던트 대응는 다음 언어와 리전 구성을 지원합니다.

- 언어: AWS 보안 인시던트 대응는 전용 영어 지원을 제공합니다. 일본어 지원은 일본 표준시 업무 시간에 한해 제공되며 다음과 같은 특정 제한 사항이 적용됩니다.
-
  > **Note**
  >
  > 일본어 지원은 업무 시간(월요일~금요일 9:00~17:00, 공휴일 제외) 동안 최선을 다해 제공됩니다.
- 지원되는 AWS 리전:

AWS 보안 인시던트 대응는 일부 AWS 리전에서 제공됩니다. 이러한 지원되는 리전에서 멤버십을 생성하고, 사례를 생성 및 조회하고, 대시보드에 액세스할 수 있습니다.

- 미국 동부(오하이오)
- 미국 서부(오리건)
- 미국 동부(버지니아)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(밀라노)
- 유럽(파리)
- 유럽(스페인)
- 유럽(스톡홀름)
- 유럽(취리히)
- 아시아 태평양(홍콩)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(자카르타)
- 아시아 태평양(멜버른)
- 아시아 태평양(뭄바이)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 캐나다(중부)
- 중동(바레인)
- 중동(UAE)
- 남아메리카(상파울루)
- 아프리카(케이프타운)

모니터링 및 조사 기능을 활성화하면 AWS 보안 인시던트 대응에서 모든 활성 상용 AWS 리전의 Amazon GuardDuty 조사 결과를 모니터링합니다. 보안 모범 사례에 따라 AWS에서는 지원되는 모든 AWS 리전에서 GuardDuty를 활성화할 것을 권장합니다. 이 구성을 사용하면 리소스를 전략적으로 배포하지 않는 AWS 리전에서도 GuardDuty가 승인되지 않은 활동이나 비정상적인 활동에 대한

결과를 생성할 수 있습니다. 이렇게 하면 전반적인 보안 태세를 강화하고 AWS 환경 전체에서 포괄적인 위협 탐지 범위를 유지할 수 있습니다.

> **Note**
>
> Amazon GuardDuty는 구성된 리전에 대한 조사 결과를 보고합니다. 특정 리전에서 서비스를 활성화하지 않도록 선택하면 알림을 사용할 수 없습니다.

기능 요약

모니터링 및 조사

AWS 보안 인시던트 대응는 Amazon GuardDuty 및 AWS Security Hub CSPM와 서드 파티 통합에서 생성된 보안 위협 알림을 신속하게 검토하여 팀에서 분석해야 하는 해당 알림 수를 줄입니다. 환경에 따라 억제 규칙을 구성하여 분류하고 조사해야 하는 위협 알림을 줄입니다.

인시던트 대응 간소화

관련 이해관계자, 타사 서비스 및 도구를 사용하여 몇 분 내에 인시던트 대응 규모를 조정하고 실행합니다.

셀프 서비스 보안 솔루션

AWS 보안 인시던트 대응는 API를 제공하여 통합하고 사용자가 사용자 지정 보안 솔루션을 직접 구축할 수 있도록 지원합니다.

가시성을 위한 대시보드

인시던트 대응 준비 상태를 모니터링하고 측정할 수 있습니다.

보안 태세

보안 평가 및 신속한 인시던트 대응 조사를 위한 AWS 모범 사례와 검증된 도구에 액세스할 수 있습니다.

신속 지원

Security Incident Response 엔지니어와 연계하여 보안 이벤트를 조사 및 격리하고 복구 방법에 대한 지침을 받을 수 있습니다.

사전 준비 및 즉각 대응 준비

미리 정의된 권한 정책을 사용하여 지정된 개인 또는 그룹에 알림을 트리거하는 인시던트 대응 팀을 설정하여 간소화된 알림을 구현할 수 있습니다.

개념 및 용어

다음은 AWS 보안 인시던트 대응 서비스 및 그 작동 방식을 이해하는 데 중요한 용어 및 개념입니다.

범위: AWS 보안 인시던트 대응는 NIST(국립표준기술연구소) 800-61 Computer Security Incident Handling Guide를 준수하여 업계 모범 사례와 관련된 보안 이벤트 관리에 대한 일관된 접근 방식을 제공합니다.

분석: 보안 이벤트의 범위, 영향 및 근본 원인을 파악하기 위한 자세한 조사 및 검사입니다.

AWS 보안 인시던트 대응 서비스 포털: 보안 이벤트 사례를 시작하고 관리할 수 있는 셀프 서비스 포털입니다. 티켓팅 시스템, 자동 알림, 서비스 팀과의 직접 참여를 통해 지속적인 커뮤니케이션과 보고가 용이해집니다.

커뮤니케이션: 인시던트 대응 프로세스 중 AWS Security Incident Response 팀과 고객 간의 지속적인 대화 및 정보 공유입니다.

방지, 근절 및 복구: 추가적인 무단 활동을 방지하고, 승인되지 않은 리소스와 원래 취약성을 제거(근절)하고, 리소스를 복구하여 정상적으로 비즈니스로 복귀합니다.

지속적 개선: AWS 보안 인시던트 대응는 이전 참여에서 얻은 피드백과 파악한 내용을 통합하여 탐지 기능, 조사 프로세스 및 문제 해결 작업을 개선합니다. 또한 AWS 보안 인시던트 대응는 최신 보안 위협 및 모범 사례를 지속적으로 업데이트하여 끊임없이 변화하는 보안 과제를 해결합니다.

사이버 보안 이벤트: 정보 시스템 또는 네트워크를 사용하여 시스템, 네트워크 또는 여기에 포함된 정보에 부정적인 영향을 미치는 작업입니다.

사이버 보안 인시던트: 컴퓨터 보안 정책, 허용 가능한 사용 정책 또는 표준 보안 관행의 위반 또는 임박한 위반 위협입니다.

Security Incident Response 엔지니어: 활성 보안 이벤트 중 지원을 제공하는 개인의 그룹. AWS 지원 사례의 경우 Security Incident Response 엔지니어가 이에 해당합니다.

인시던트 대응 워크플로: NIST 800-61 표준에 따른 보안 이벤트의 엔드 투 엔드 관리와 관련된 정의된 순서의 단계와 활동입니다.

조사 도구: 계정과 리소스의 운영 상태를 검토하는 데 사용되는 AWS 보안 인시던트 대응 도구 및 서비스 연결 역할입니다.

파악한 내용: 개선이 필요한 영역을 식별하고 향후 인시던트 대응 계획에 알리기 위한 보안 이벤트 대응 검토 및 문서화 작업입니다.

모니터링 및 조사: AWS 보안 인시던트 대응는 Amazon GuardDuty의 보안 알림을 신속하게 검토하여 팀에서 분석해야 할 가장 중요한 알림을 최우선으로 표시합니다. 불필요한 알림을 방지하기 위해 환경의 특성에 따라 억제 규칙을 구성합니다.

준비: 인시던트 대응 계획과 테스트 절차를 개발하는 등 조직이 보안 이벤트에 효과적으로 대응하고 관리할 수 있도록 준비하는 활동입니다.

보고 및 커뮤니케이션: 자동 알림, 통화 연결, 조사 아티팩트 전달 등 인시던트 대응 프로세스 전반에 걸쳐 정보를 제공하는 데 사용되는 프로세스입니다. AWS 보안 인시던트 대응는 AWS Management Console에서 단일 중앙 대시보드를 제공하여 모든 AWS 보안 인시던트 대응 작업을 관리합니다.

대응 담당자 생성 인텔리전스: 침해 지표, 전술, 기술 및 절차, AWS 조사에서 관찰된 관련 패턴입니다.

보안 이벤트 전문성: 특히 AWS 클라우드 환경에서 보안 이벤트에 효과적으로 대응하고 관리하는 데 필요한 전문 지식과 기술입니다.

공동 책임 모델: AWS와 고객 간의 보안 책임 분담으로, AWS는 클라우드 보안을 책임지고 고객은 클라우드 내 보안을 책임집니다.

위협 인텔리전스: 진화하는 보안 위협을 식별하고 대응하는 데 도움이 되는 무단 활동의 세부 정보가 포함된 내부 및 외부 데이터 피드입니다.

티켓팅 시스템: 보안 이벤트 사례를 온보딩 및 관리하고, 첨부 파일을 추가하고, 인시던트 대응 수명 주기를 추적할 수 있는 전용 사례 관리 플랫폼입니다.

분류: 적절한 대응과 다음 단계를 결정하기 위한 보안 이벤트의 초기 평가 및 우선순위 지정입니다.

워크플로: 보안 이벤트의 엔드 투 엔드 관리와 관련된 정의된 순서의 단계와 활동입니다.

시작하기

AWS 보안 인시던트 대응 시작하기

내용

온보딩 가이드

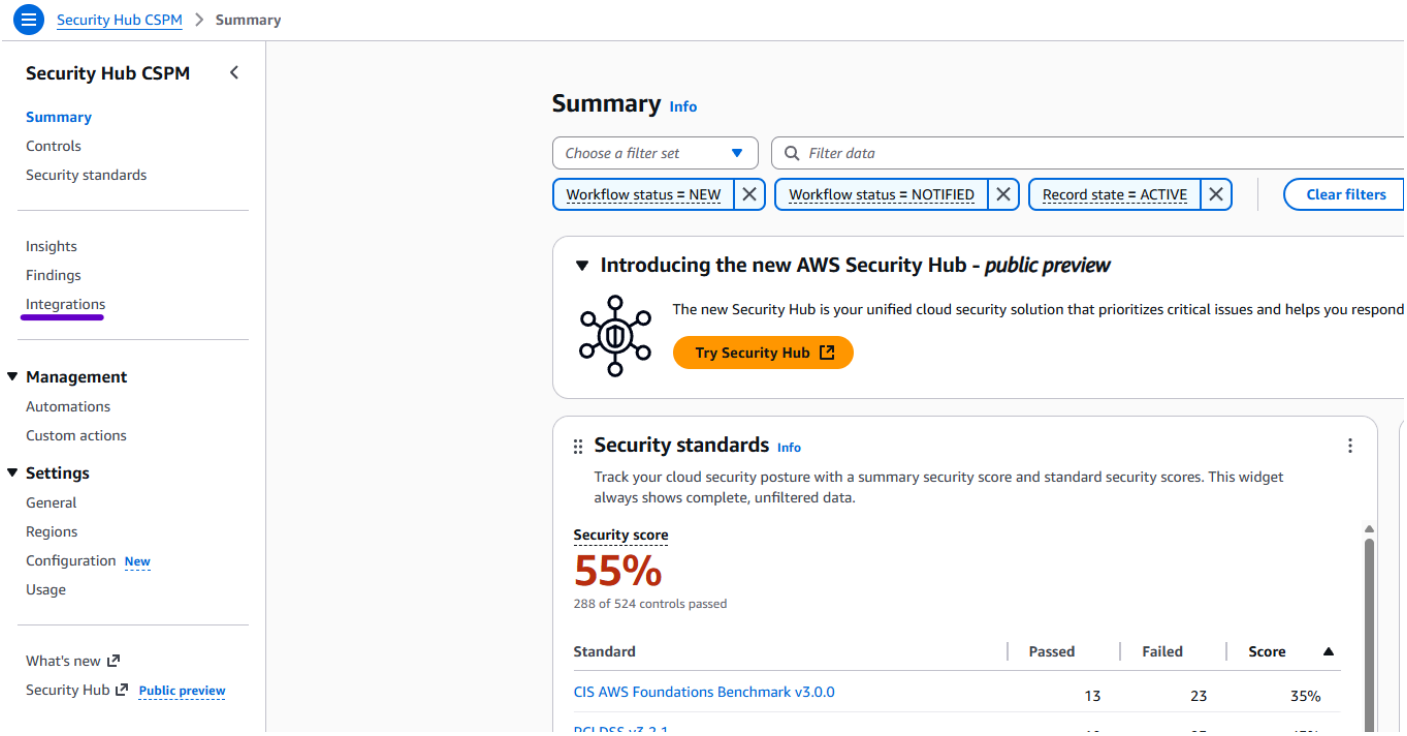
온보딩 가이드는 전제 조건과 AWS 보안 인시던트 대응 온보딩 및 격리 작업을 안내합니다.

> **Important**
>
> 사전 조건
>
> 1. 유일한 배포 사전 조건은 AWS Organizations를 활성화하는 것입니다.
> 2. 필수는 아니지만 모든 계정 및 활성 AWS 리전에서 Amazon GuardDuty와 AWS Security Hub CSPM를 활성화하여 Security Incident Response 이점을 극대화하는 것이 좋습니다.
> 3. GuardDuty 및 Security Incident Response를 검토합니다.
> 4. GuardDuty 모범 사례 가이드를 검토합니다.

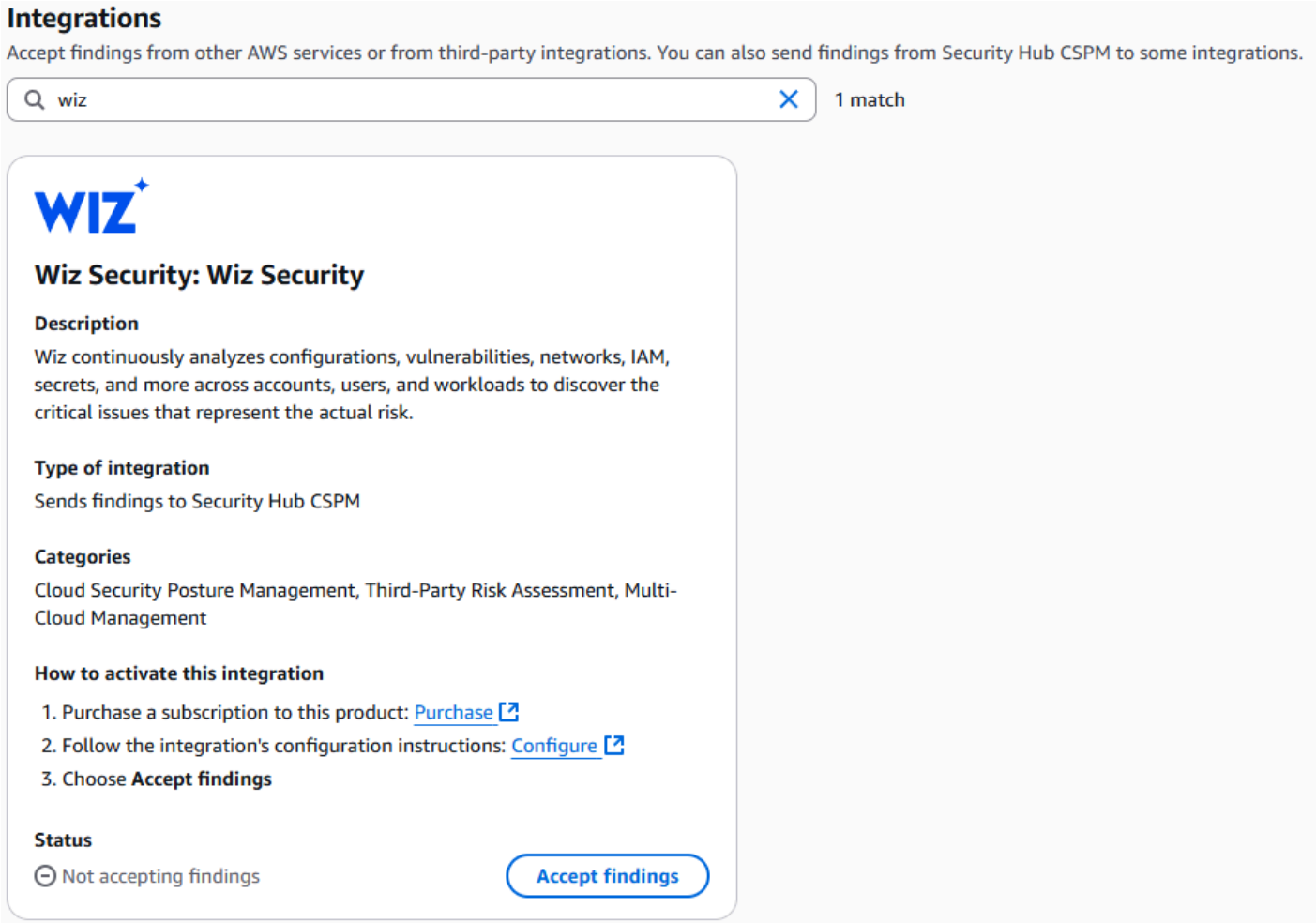
AWS Security Hub CSPM는 타사 엔드포인트 탐지 및 응답(EDR) 공급업체(CrowdStrike, FortinetCNAPP(Lacework), Trend Micro 등)에서 조사 결과를 수집합니다. 이러한 조사 결과가 Security Hub CSPM에 수집되는 경우 선제적 사례 생성을 위해 Security Incident Response에 의해 자동으로 분류됩니다. Security Hub CSPM을 사용하여 타사 EDR을 설정하려면 탐지 및 분석을 참조하세요.

Security Hub CSPM을 사용하여 타사 EDR을 설정하려면 다음을 수행합니다.

1. Security Hub CSPM 통합 페이지로 이동하여 타사 통합이 존재하는지 확인합니다.
2. 콘솔에서 Security Hub CSPM 서비스 페이지로 이동합니다.
3. 통합을 선택합니다(예: Wiz.IO 사용).



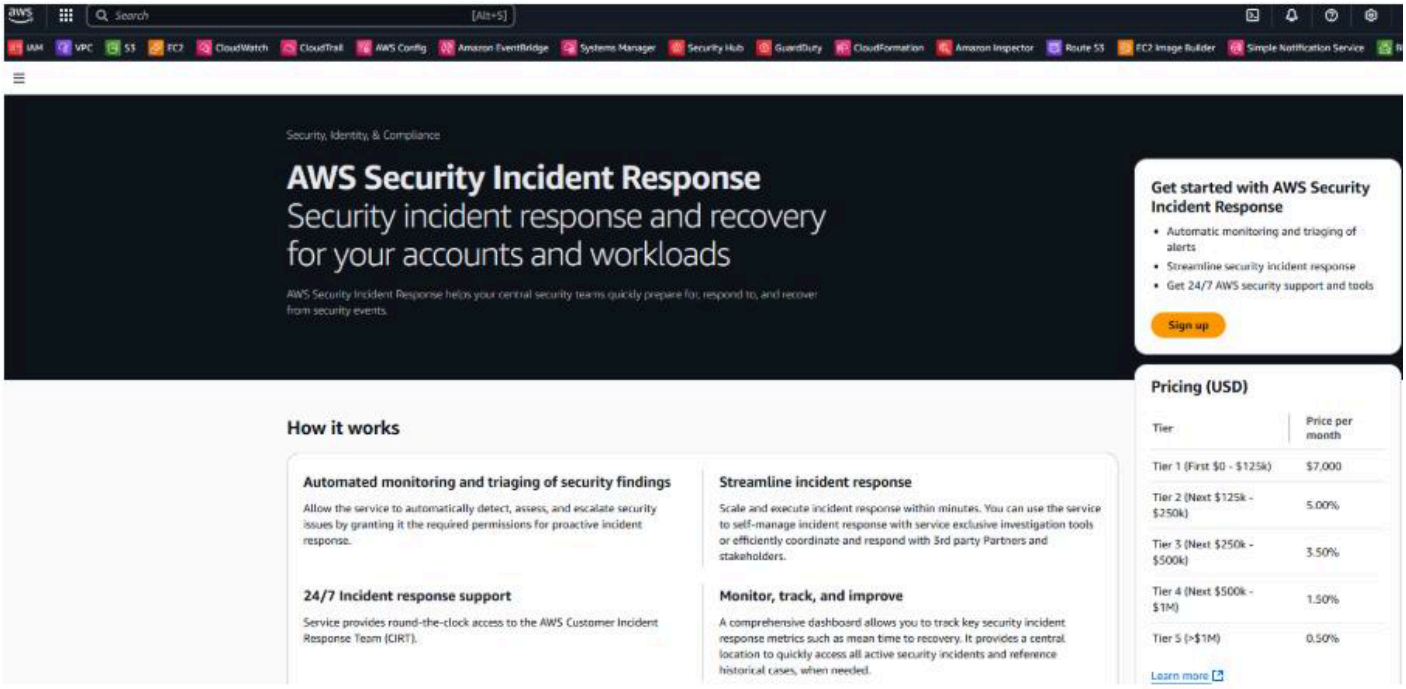
4. 통합하려는 공급업체를 검색합니다.



> **Note**
>
> 메시지가 나타나면 계정 또는 구독 정보를 제공합니다. 이 정보를 제공하면 Security Incident Response에서 타사 조사 결과를 수집합니다. 타사 조사 결과 수집에 대한 요금을 검토하려면 Security Hub CSPM의 통합 페이지에서 확인할 수 있습니다.

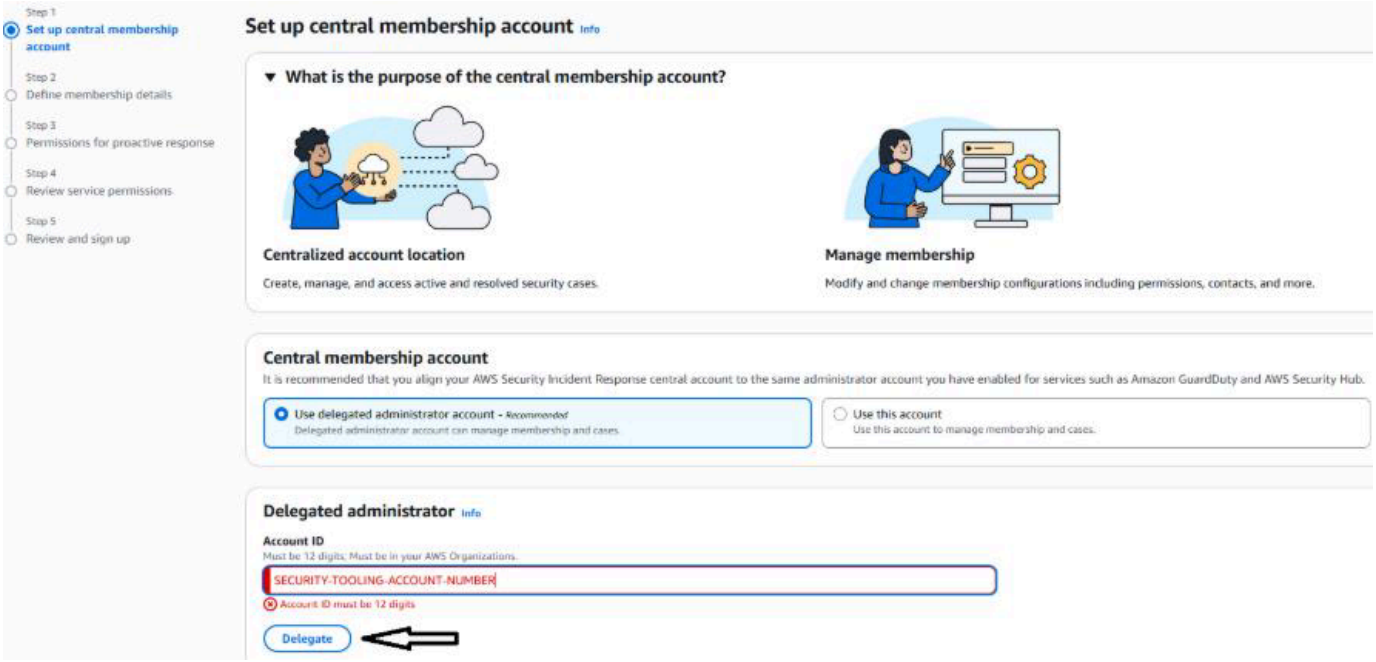
Security Incident Response 배포 및 구성

1. 가입을 선택합니다.

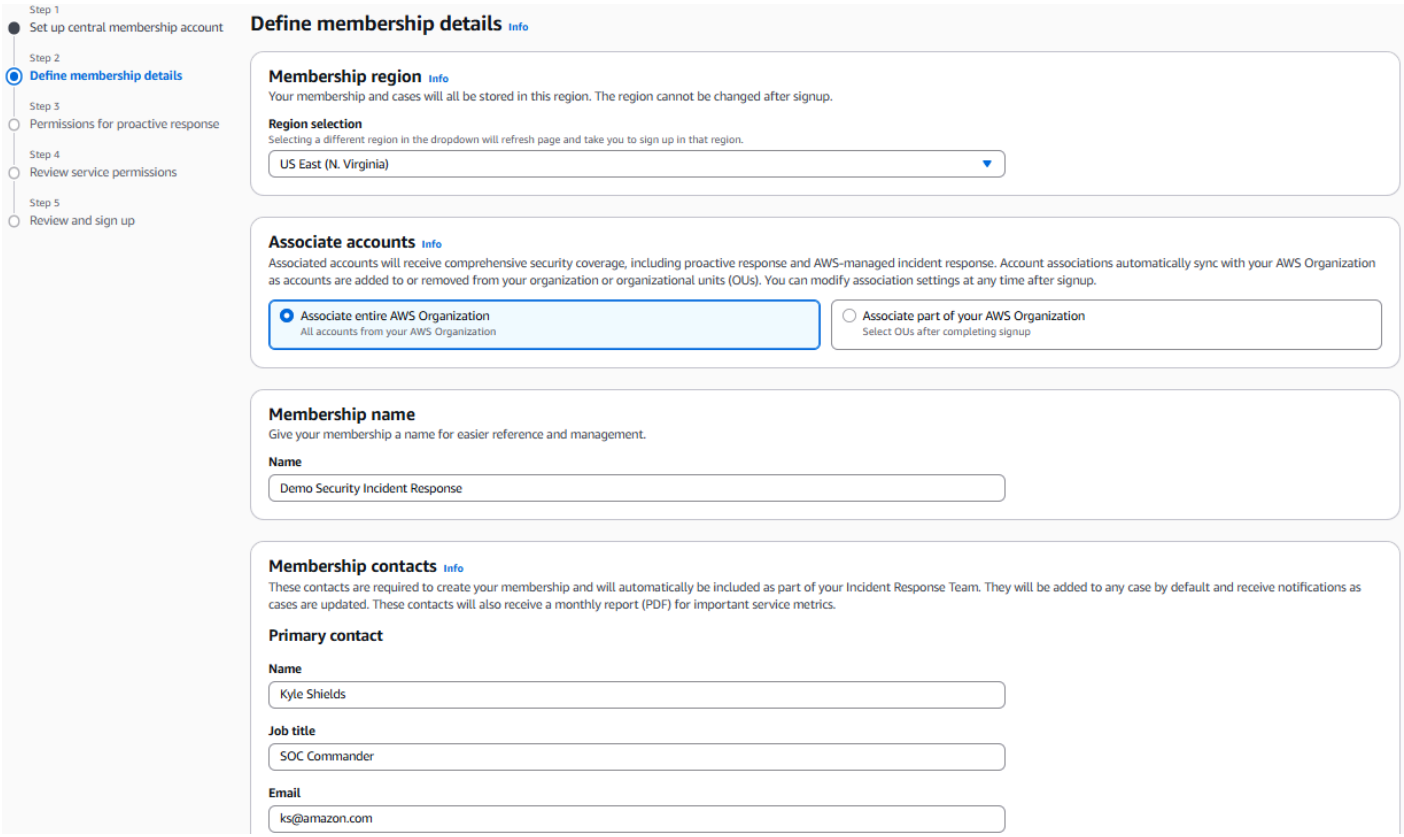


2. 관리 계정에서 위임된 관리자로 보안 도구 계정을 선택합니다.

   - Security Reference Architecture
   - 위임된 관리자 설명서



3. 위임된 관리자 계정에 로그인
4. 멤버십 세부 정보 입력 및 계정 연결



Security Incident Response에 작업 권한 부여

이 페이지에서는 AWS 환경에서 자동화된 모니터링 및 격리 작업을 수행하도록 Security Incident Response에 권한을 부여하는 방법을 설명합니다. 선테적 대응 모니터링 및 격리 작업 기본 설정이라는 두 가지 고유한 권한 부여 기능을 활성화할 수 있습니다. 이러한 기능은 서로 독립적이며 보안 요구 사항에 따라 별도로 활성화할 수 있습니다.

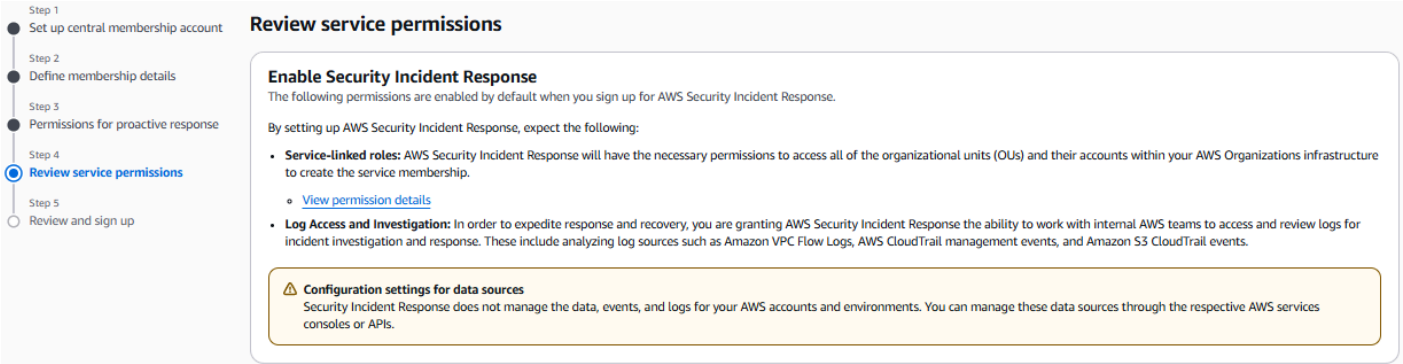
선제적 대응 활성화

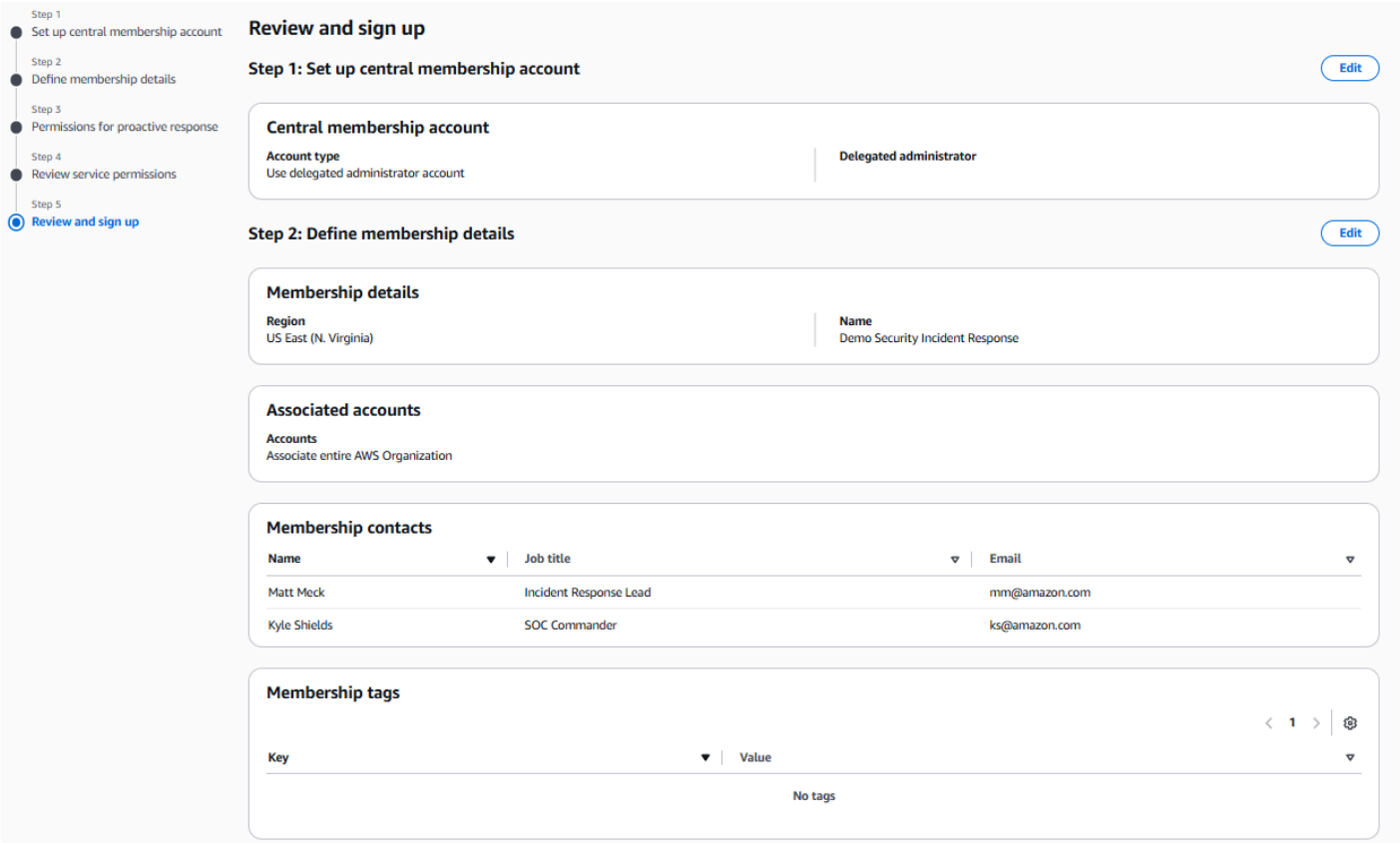
선제적 대응을 통해 Security Incident Response는 조직 전체에서 Amazon GuardDuty 및 AWS Security Hub CSPM 통합으로부터 생성된 알림을 모니터링하고 조사할 수 있습니다. 활성화된 경우 Security Incident Response는 서비스 자동화를 통해 우선순위가 낮은 알림을 분류하므로 팀이 가장 중요한 문제에 집중할 수 있습니다.

온보딩 중에 선제적 대응을 활성화하는 방법:

1. Security Incident Response 콘솔에서 온보딩 워크플로로 이동하세요.
2. Security Incident Response가 조직에서 해당되는 모든 계정 및 활성 지원 AWS 리전의 조사 결과를 모니터링하도록 허용하는 서비스 권한을 검토하세요.

3. 가입을 선택하여 기능을 활성화하세요.





이 기능은 AWS Organizations 내 해당되는 모든 멤버 계정에서 서비스 연결 역할을 자동으로 생성합니다. 그러나 관리 계정에서는 AWS CloudFormation 스택 세트를 통해 서비스 연결 역할을 수동으로 생성해야 합니다.

다음 단계: Security Incident Response가 Amazon GuardDuty 및 AWS Security Hub CSPM와 작동하는 방식에 대한 자세한 내용은 AWS 보안 인시던트 대응 사용 설명서의 탐지 및 분석을 참조하세요.

격리 작업 기본 설정 정의

격리 작업을 통해 AWS 보안 인시던트 대응는 활성 보안 인시던트 중에 신속한 대응 조치를 실행할 수 있습니다. 이러한 작업은 환경에서 보안 인시던트의 영향을 신속하게 완화하는 데 도움이 됩니다.

> **Important**
>
> Security Incident Response는 기본적으로 격리 기능을 활성화하지 않습니다. 격리 기본 설정을 통해 명시적으로 격리 작업에 권한을 부여해야 합니다.

AWS 보안 인시던트 대응 엔지니어가 사용자를 대신하여 격리 작업을 수행하도록 권한을 부여하려면 필요한 IAM 역할을 생성하는 AWS CloudFormation StackSet를 배포하는 것 외에도 조직 또는 계정 수준 격리 기본 설정을 정의해야 합니다. 계정 수준 기본 설정은 조직 수준 기본 설정을 대체합니다.

사전 조건: AWS Support 사례를 생성할 권한이 있어야 합니다.

격리 옵션:

- 승인 필요(기본값): 사례별로 명시적 권한 부여 없이 리소스를 선제적으로 격리하지 않습니다.
- 확인 항목 격리: 손상된 것으로 확인된 리소스에 대해 선제적 격리를 수행합니다.
- 의심 항목 격리: AWS 보안 인시던트 대응 엔지니어링에서 수행한 분석을 기반으로 손상 가능성이 큰 리소스를 선제적으로 격리합니다.

격리 기본 설정을 정의하는 방법:

1. Security Incident Response의 격리 작업 기본 설정을 구성하도록 요청하는AWS Support 사례를 생성하세요.
2. 지원 사례에서 다음을 지정하세요.
   - 격리 작업에 대한 권한을 부여해야 하는 AWS Organizations ID 또는 특정 계정 ID
   - 선호하는 격리 옵션(승인 필요, 확인 항목 격리, 의심 항목 격리).
   - 권한을 부여하려는 격리 작업 유형(예: EC2 인스턴스 격리, 자격 증명 교체 또는 보안 그룹 수정)
3. AWS Support는 사용자와 협력하여 격리 기본 설정을 구성합니다. 필요한 IAM 역할을 생성하는 AWS CloudFormation StackSet를 배포해야 합니다. 필요한 경우 AWS Support에서 도움을 받을 수 있습니다.

구성 후 AWS 보안 인시던트 대응는 환경 보호를 위해 활성 보안 인시던트 중 권한이 부여된 격리 작업을 실행합니다.

다음 단계: 격리 기본 설정을 구성한 후 Security Incident Response 콘솔에서 인시던트 중에 수행된 격리 작업을 모니터링할 수 있습니다.

Security Incident Response의 사후 배포

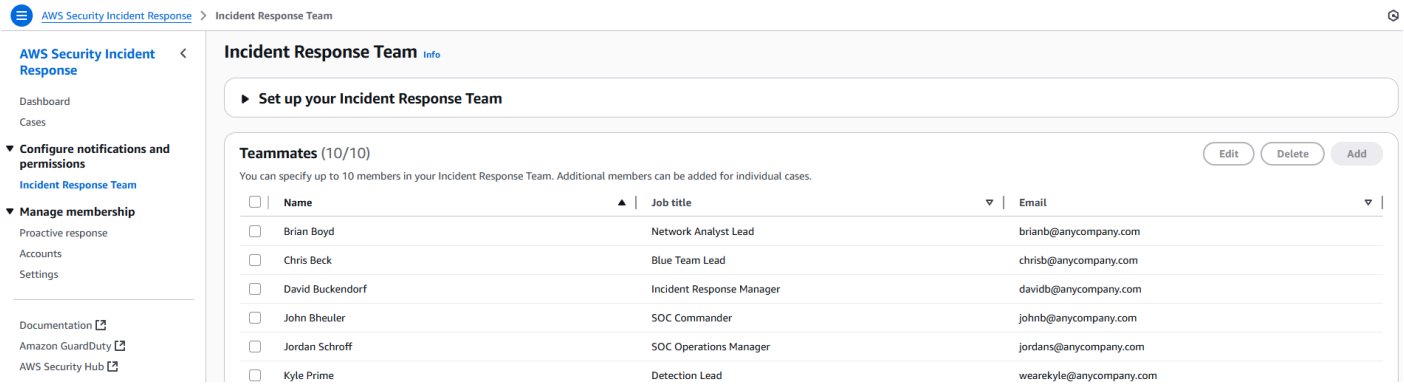
AWS는 교체하는 대신 기존 인시던트 대응 프레임워크와 통합됩니다.

1. 현재 방식을 개선하기 위해 당사의 운영 통합 기능을 검토해 보세요.
2. 보다 효율적인 보안 운영을 위해 OU 수준 멤버십 지원 데모, EventBridge 활용 및 Jira-ITSM 통합을 시청해 보세요.

   AWS 보안 인시던트 대응: 새로운 통합 및 OU 수준 구독

인시던트 대응 팀 업데이트

1. 구독을 완료하고 본 온보딩 가이드에 설명된 온보딩 단계를 모두 마쳤는지 확인하세요.
2. 왼쪽 탐색 창에서 인시던트 대응 팀을 선택합니다.
3. 팀에 추가할 팀원을 선택합니다.



> **Note**
>
> 팀에는 조직 리더십, 법률 고문, MDR 파트너, 클라우드 엔지니어 등이 포함될 수 있습니다. 최대 10명의 멤버를 추가할 수 있습니다. 각 멤버의 이름, 직함 및 이메일 주소만 포함합니다.

AWS 지원 사례

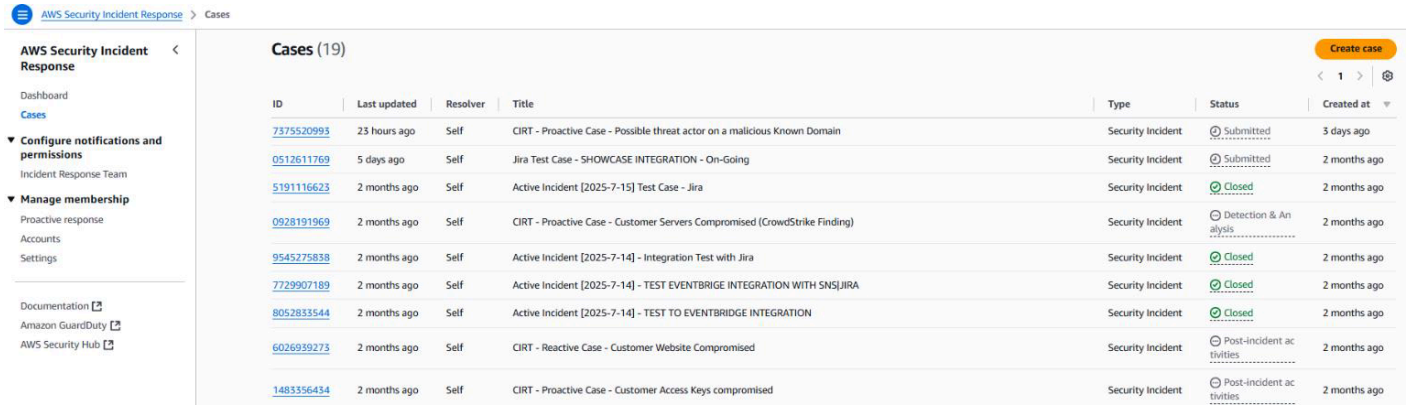
AWS 보안 인시던트 대응는 조직이 Security Incident Response 엔지니어와 직접 소통할 수 있는 구독 기반 사례 관리 포털을 제공합니다. 대응 사례에 대한 제한 없이 15분 SLO를 통해 보안 조사 및 활성 인시던트를 지원합니다. AWS 지원되는 사례 생성 설명서를 참조하세요.

조사 팀 확장

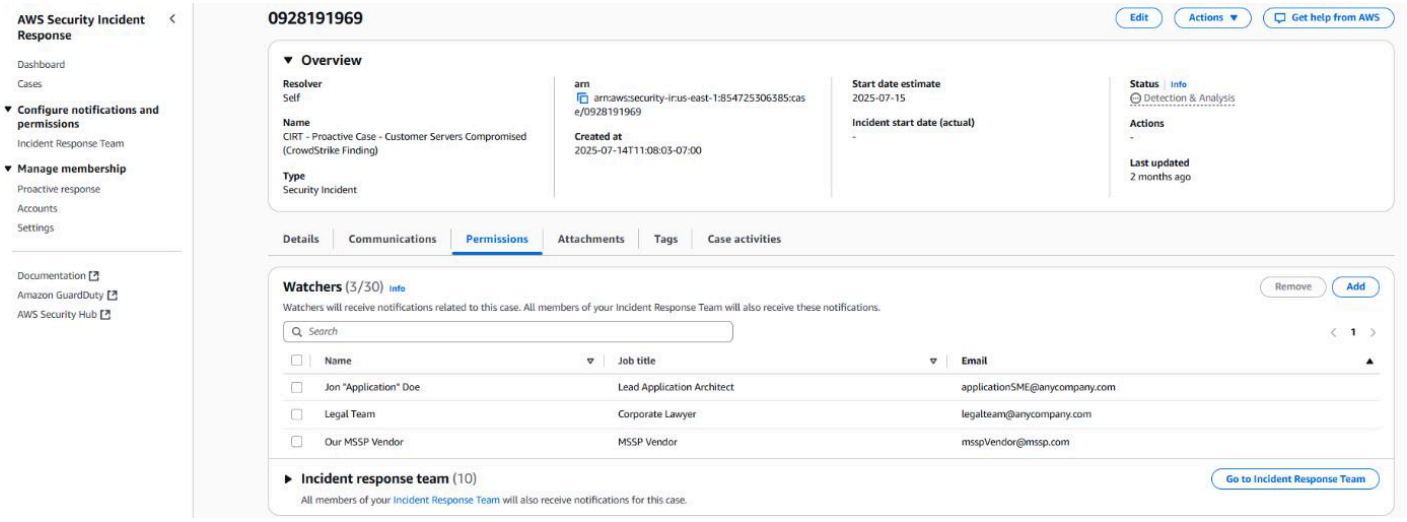
사례 관리 포털을 통해 감시자 및 IAM 정책을 추가하여 외부 당사자에게 사례 가시성을 부여할 수 있습니다. 파트너, 법률 팀 또는 주제 전문가에 대해 이러한 옵션을 사용합니다.

사례에 감시자를 추가하는 방법

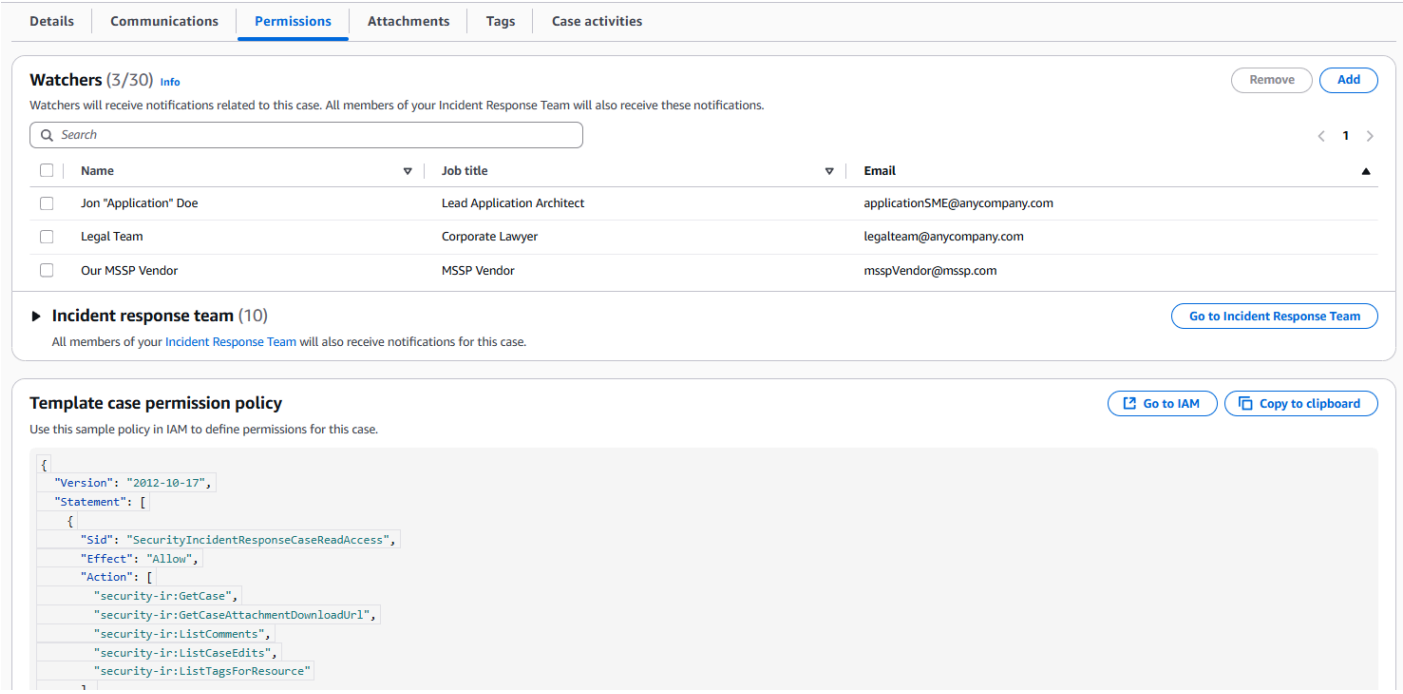
1. Security Incident Response 사례 포털에서 사례를 엽니다.



2. 권한 탭 선택



3. 추가 선택



> **Note**
>
> 각 사례에는 특정 사례에만 액세스 권한을 부여하여 최소 권한을 유지하는 미리 채워진 IAM 정책이 포함됩니다. 이 정책을 복사하여 타사 MDR 파트너 또는 특정 조사 팀의 IAM 역할 또는 사용자에게 직접 붙여 넣어 기여도를 높입니다.

GuardDuty 조사 결과 및 억제 규칙

AWS 보안 인시던트 대응는 CrowdStrike, FortinetCNAPP(Lacework), Trend Micro의 모든 Amazon GuardDuty 조사 결과와 AWS Security Hub CSPM 조사 결과를 사전에 수집 및 분류하고 이에 대응합니다. 자동 분류 기술은 내부 분석 요구 사항이 필요하지 않습니다. 이 서비스는 GuardDuty 및 Security Hub CSPM에서 양성 조사 결과에 대한 억제 및 자동 보관 규칙을 생성합니다. Amazon GuardDuty 콘솔의 '조사 결과'에서 이러한 규칙을 보거나 수정합니다.

활성화된 GuardDuty 억제 규칙을 검토하려면 다음 단계를 완료합니다.

1. Amazon GuardDuty 콘솔을 엽니다.
2. 조사 결과를 선택합니다.
3. 탐색 창에서 억제 규칙을 선택합니다. 억제 규칙 페이지에는 계정에 대한 모든 억제 규칙 목록이 표시됩니다.

4. 규칙 설정을 검토하거나 변경하려면 규칙을 선택한 다음 작업 메뉴에서 억제 규칙 업데이트를 선택합니다.

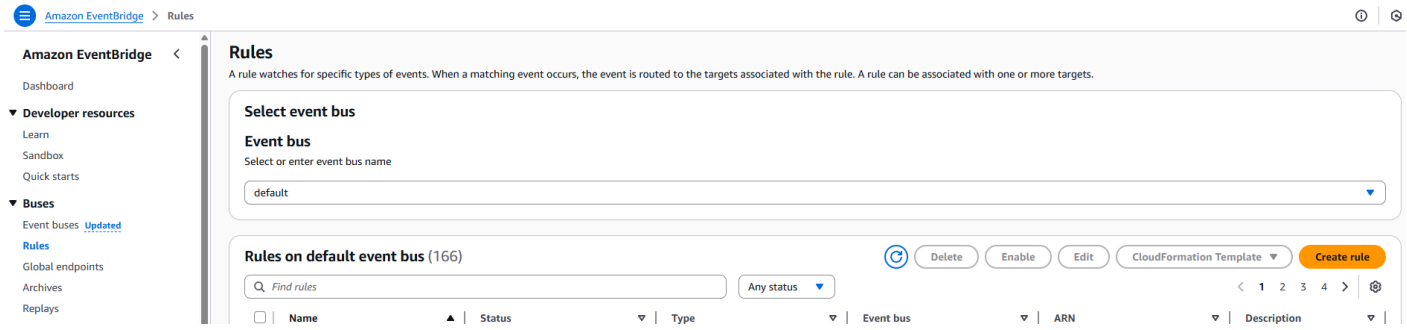
> **Note**
>
> SIEM 기술을 사용하는 조직은 시간이 지남에 따라 GuardDuty 조사 결과 볼륨이 크게 감소하여 Security Incident Response 서비스와 SIEM 효율성이 모두 개선됩니다.

Amazon EventBridge

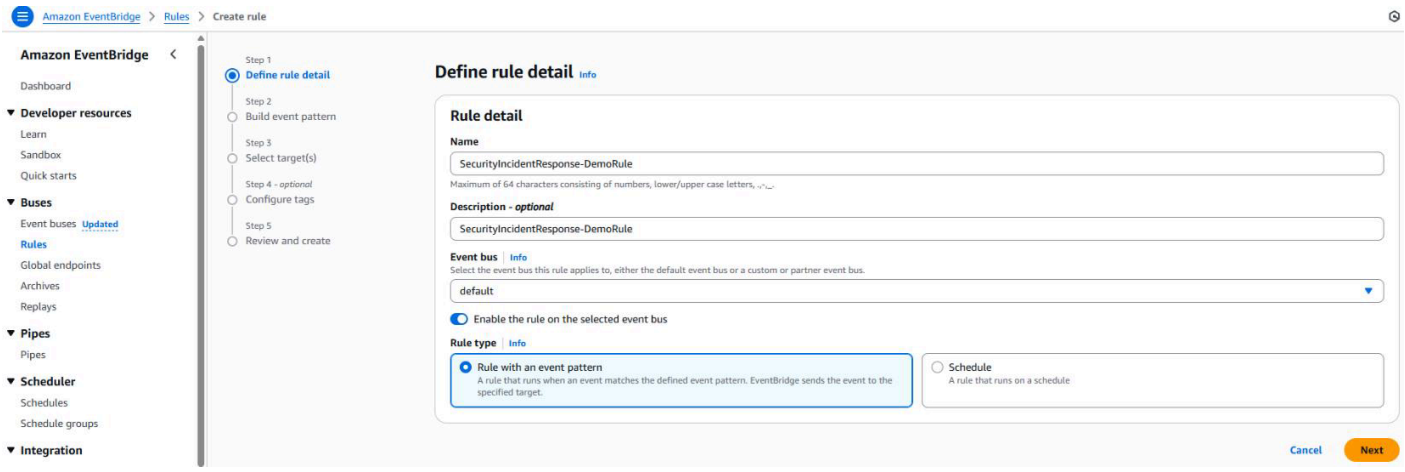
Amazon EventBridge는 보안 인시던트 대응을 위한 이벤트 기반 아키텍처를 지원하므로 사례 활동이 다운스트림 서비스(SNS, Lambda, SQS, Step-Functions) 또는 외부 도구(Jira, ServiceNow, Teams, Slack, PagerDuty)를 트리거할 수 있습니다.

EventBridge 규칙 구성 방법

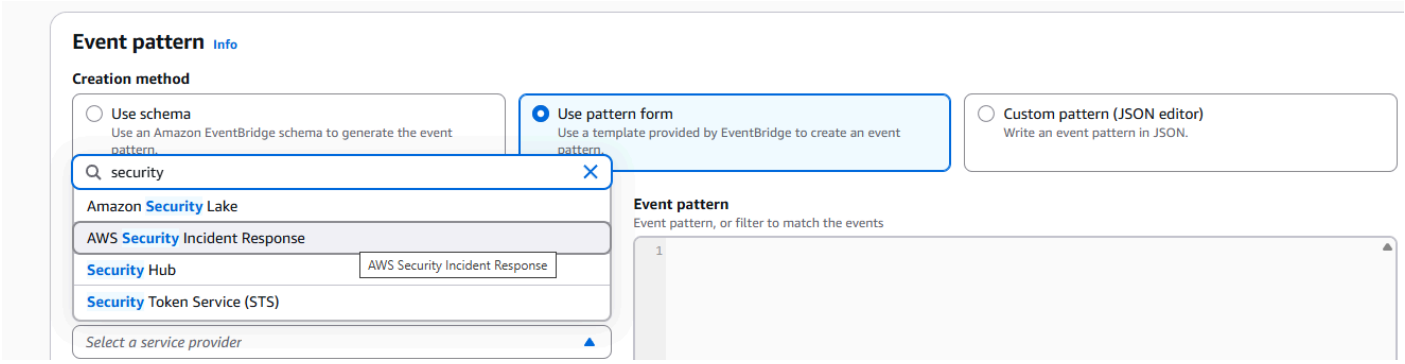
1. Amazon EventBridge에 액세스
2. 버스 드롭다운에서 규칙을 선택합니다.



3. [Create Rule]을 선택합니다.
4. 규칙 세부 정보를 입력합니다.
5. 다음을 선택합니다.



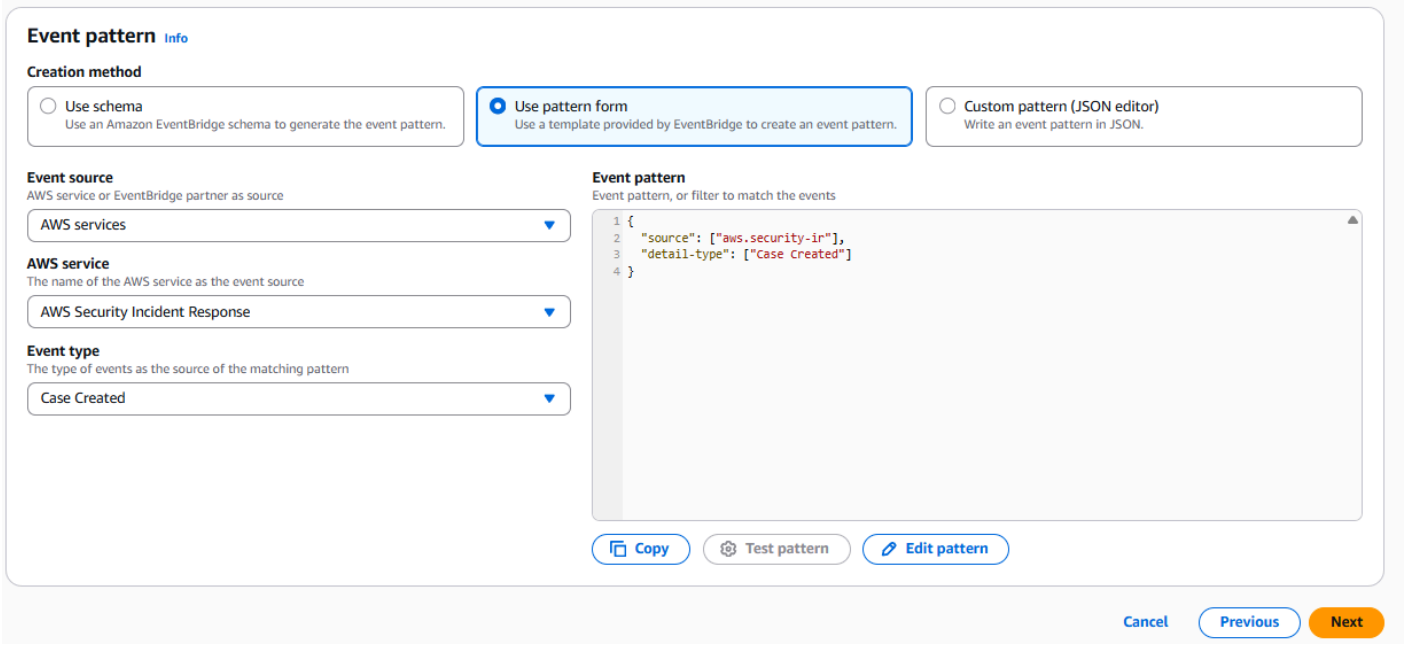
6. AWS 서비스로 스크롤하고 드롭다운 메뉴에서 AWS 보안 인시던트 대응를 선택합니다.



7. 이벤트 유형 드롭다운에서 패턴을 생성할 이벤트 또는 API 직접 호출을 선택합니다.

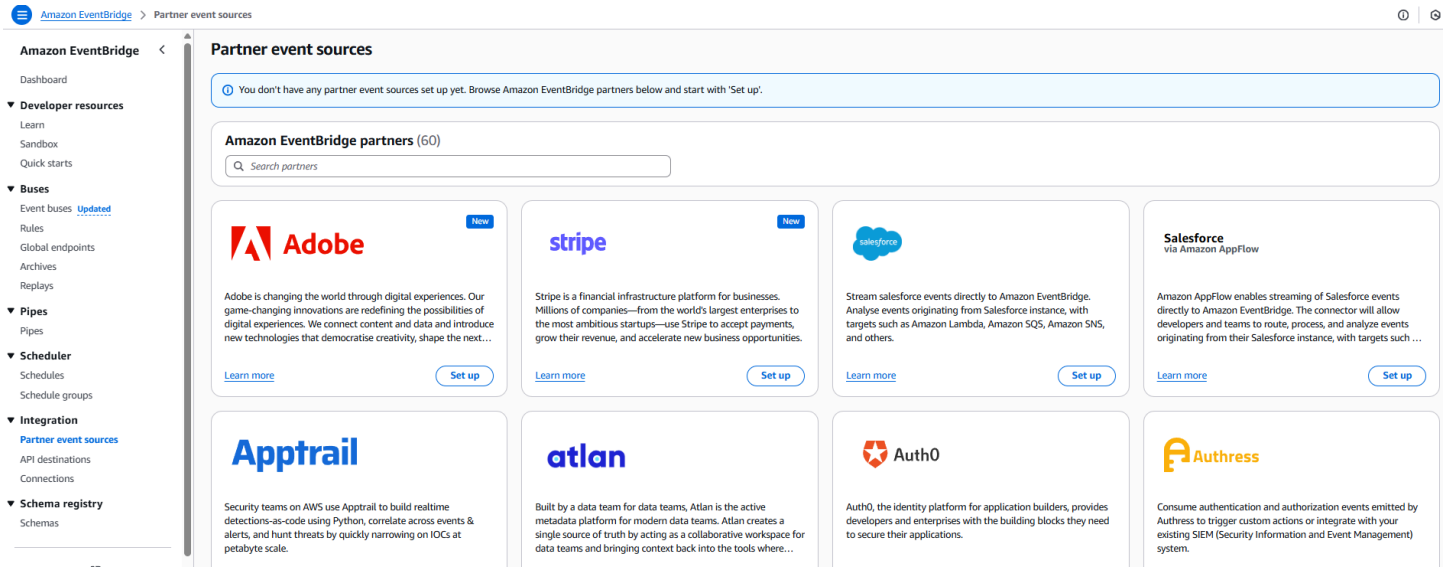
8. 둘 이상의 이벤트를 포함하도록 패턴을 수동으로 편집할 수 있습니다.

9. 다음을 선택합니다.



> **Note**
>
> 이벤트에 대해 하나 이상의 대상(Amazon Simple Notification Service, AWS Lambda, SSM 문서, Step-Function)을 선택합니다. 필요한 경우 교차 계정 대상을 구성합니다.

EventBridge 통합 메뉴의 파트너 이벤트 소스에서 파트너 통합 패턴을 확인할 수 있습니다. 사용 가능한 파트너로는 Atlassian(Jira), DataDog, New Relic, PagerDuty, Symantec, Zendesk 등이 있습니다.



통합 및 외부 도구 워크플로

JIRA 또는 ServiceNow를 Security Incident Response와 통합하는 AWS 솔루션

Jira 및 ServiceNow와의 양방향 통합을 위해 완전히 개발된 솔루션을 배포합니다. 이러한 통합을 통해 AWS 보안 인시던트 대응 사례와 ITSM 플랫폼 간의 양방향 통신이 가능하며, 사례 업데이트는 해당 Jira 작업에 자동으로 반영됩니다.

통합의 이점

AWS 보안 인시던트 대응를 기존 ITSM 플랫폼과 통합하면 인시던트 추적 및 대응 워크플로를 중앙 집중화하여 보안 운영을 간소화할 수 있습니다. 이러한 사전 빌드된 솔루션을 사용하면 사용자 지정 개발이 필요하지 않으므로 보안 팀이 AWS 네이티브 및 전사적 인시던트 관리 시스템 모두에서 가시성을 유지 관리할 수 있습니다. 이벤트 기반 자동화에 Amazon EventBridge를 활용하면 여러 플랫폼 사이에서 업데이트가 실시간으로 원활하게 전달되므로 보안 인시던트가 발생한 위치에 관계없이 일관되게 추적되도록 할 수 있습니다. 이 통합 접근 방식은 보안 분석가의 컨텍스트 전환을 줄이고, 대응 시간을 개선하며, 전체 인시던트 대응 수명 주기에서 포괄적인 감사 추적을 제공합니다.

EventBridge 규칙 구성 방법:

1. Amazon EventBridge에 액세스합니다.
2. 버스 드롭다운에서 규칙을 선택합니다.

외부 도구 워크플로

보안 인시던트 대응은 여러 가지 방법으로 외부 도구 및 파트너와 통합됩니다.

- SIEM 통합: Security Incident Response 엔지니어는 AWS 지원 사례를 제출할 때 팀과 함께 이러한 조사 결과를 분석하고 조사하는 데 도움을 줍니다. 하이브리드 및 멀티 클라우드 환경 간의 상관관계를 식별하여 공급자 간의 위협 행위자 이동 범위를 정하는 데 도움이 됩니다.
- 기존 보안 작업 개선: 기존 GuardDuty 대응 워크플로를 보다 효율적인 병렬 대응 모델로 대체합니다. 현재 많은 조직이 사례 관리를 통한 탐지 워크플로에 SIEM 기술을 활용하고 있습니다. 이 서비스는 GuardDuty와 일부 Security Hub CSPM 조사 결과에 대한 간소화된 대안을 제공합니다. 이 솔루션은 정교한 자동 분류 기술과 인적 감독을 활용하여 포털에서 선제적 사례를 생성하고, 동시에 대응 팀에 알리며, 조정된 문제 해결 작업을 위해 Security Incident Response 엔지니어를 참여시킵니다.
- 서드 파티 조사 팀: Security Incident Response 엔지니어가 파트너 및 MDR 공급자와 직접 협업합니다.

부록 A: 연락 담당자

메타데이터를 Security Incident Response 엔지니어에게 미리 제공하면 프로파일 생성 시간을 가속하여 게이트 외부에서 분류 기술에 대한 신뢰도를 높일 수 있습니다. 그러면 위협 조사 결과를 수집하고 '정상 환경'을 생성하기 시작할 때 발생하는 초기 오탐지를 줄일 수 있습니다.

IR 및 SOC 직원 연락처 정보

입력	IR | SOC 직원: 역할, 이름, 이메일	기본, 보조에스컬레이션연락처	내부, 알려진 CIDR 범위	외부, 알려진 CIDR 범위	추가 클라우드 서비스 제공업체	작업 AWS 리전	DNS 서버 IP(An Route Resol 가 아닌 경우)	VPN | 원격 액세스 솔루션 및 IP	중요 애플리케이션 이름 | 계정 번호	많이 사용되는 비일반 포트	ERD | AV | 사용된 취약성 관리 도구	IDP | 위치
1	SOC Comma , John Smith, jsmith@ ample.c	Prima	10.0.(16	5.5.6(20(Az	Azure	us-east-1 , us-east-2	해당 사항 없음	Direct Connect 퍼블릭 VIF 116.32.8 7	Nginx Webser (중요 예제) | 1234567 0	8080	CrowdSt ke Falcon	Entra, Azure

환경에 대한 메타데이터 정보를 제출하려면 AWS Support 사례를 생성합니다.

메타데이터를 제출하려면

1. 환경 정보를 사용하여 메타데이터 테이블을 작성합니다.
2. 다음 세부 정보를 사용하여 AWS Support 사례를 생성합니다.
   - 사례 유형: 기술
   - 서비스: Security Incident Response 서비스

- 범주: 기타

3. 작성된 메타데이터 테이블을 사례에 연결합니다.

RACI 매트릭스

다음과 같은 RACI 매트릭스는 Security Incident Response 구현 프로세스 전반에서 역할과 담당 업무를 정의합니다. RACI는 담당(Responsible), 책임(Accountable), 상담(Consulted), 정보 지원(Informed)의 약자입니다.

활동	Customer	AWS 계정 팀	SIR 팀
사전 온보딩			
주요 이해관계자 식별	R		I
조사 결과 소스 검증	R	C	I
[서드 파티 EDR 통합] Security Hub CSPM	R	C	I
GuardDuty 검증/상태 확인	C	R	I
계정 범위 결정	R		
에스컬레이션 프로토콜 설정	R	I	C
AWS Organizations 활성화	R	C	
AWS Organizations와 계정 연결	R	I	
위임된 관리자/보안 도구 계정 선택	R	I	
온보딩			
멤버십 세부 정보 설정	R	I	
연습(선제적 대응 및 알림 분류 워크플로 설정, 관리 계정에 서비스 연결 역할 배포, 격리 작업 권한 부여)	R	C	I

활동	Customer	AWS 계정 팀	SIR 팀
사후 배포 구성			
운영 통합 기능 검토	R	C	I
Security Incident Response 대응 사례 제출	R		
Amazon EventBridge 통합 구성	R	C	C
서드 파티 도구(Jira, ServiceNow, PagerDuty, Teams 등) 연결	R	I	C
서비스 심층 분석 및 데모	A	R	C

RACI 정의:

- 담당(Responsible) - 작업을 수행하여 태스크를 완료하는 당사자
- 책임(Accountable) - 최종적으로 태스크의 올바른 완료에 대한 책임이 있는 당사자
- 상담(Consulted) - 조언을 제공하고 양방향 커뮤니케이션을 하는 당사자
- 정보 지원(Informed) - 진행 상황을 최신 상태로 유지하고 단방향 커뮤니케이션을 하는 당사자

멤버 계정 선택

멤버십 계정은 계정 세부 정보를 구성하고, 인시던트 대응 팀에 대한 세부 정보를 추가 및 제거하며, 모든 활성 및 기록 보안 이벤트를 생성하고 관리할 수 있는 데 사용되는 AWS 계정입니다. Amazon GuardDuty 및 AWS Security Hub CSPM와 같은 서비스에 대해 활성화한 것과 동일한 계정에 AWS 보안 인시던트 대응 멤버십 계정을 정렬하는 것이 좋습니다.

AWS Organizations를 사용하여 AWS 보안 인시던트 대응 멤버십 계정을 선택하는 두 가지 옵션이 있습니다. 조직 관리 계정 또는 조직 위임 관리자 계정에서 멤버십을 생성할 수 있습니다.

위임 관리자 계정 사용: AWS 보안 인시던트 대응 관리 태스크 및 사례 관리는 위임 관리자 계정에 있습니다. 다른 AWS 보안 및 규정 준수 서비스에 설정한 것과 동일한 위임 관리자를 사용하는 것이 좋습니다. 12자리 위임 관리자 계정 ID를 입력한 다음 해당 계정에 로그인하여 계속 진행합니다.

> **Important**
>
> 위임 관리자 계정을 설정의 일부로 사용하는 경우 AWS 보안 인시던트 대응는 AWS Organizations 관리 계정에서 필요한 분류 서비스 연결 역할을 자동으로 생성할 수 없습니다. IAM을 사용하여 AWS Organizations 관리 계정에서 이 역할을 생성할 수 있습니다.
>
> 서비스 연결 역할을 만드는 방법(콘솔)
>
> 1. AWS Organizations 관리 계정에 로그인합니다.
> 2. AWS CloudShell 창에 액세스하거나 원하는 방법으로 CLI를 통해 계정에 액세스합니다.
> 3. CLI 명령 `aws iam create-service-linked-role --aws-service-name "triage.security-ir.amazonaws.com" --no-cli-pager`을 사용합니다.
> 4. (선택 사항) 명령이 작동하는지 확인하려면 명령 `aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage`을 실행합니다.

현재 로그인한 계정 사용: 이 계정을 선택하면 현재 계정이 멤버십의 중앙 AWS 보안 인시던트 대응 멤버십 계정으로 지정됩니다. 조직 내 개인은 이 계정을 통해 서비스에 액세스하여 활성 및 해결된 사례를 생성, 액세스 및 관리해야 합니다.

AWS 보안 인시던트 대응를 관리할 수 있는 충분한 권한이 있는지 확인합니다.

권한을 추가하는 특정 단계는 IAM ID 권한 추가 및 제거를 참조하세요.

AWS 보안 인시던트 대응 관리형 정책을 참조하세요.

IAM 권한을 확인하려면 다음 단계를 따르세요.

- IAM 정책 확인: 사용자, 그룹 또는 역할에 연결된 IAM 정책을 검토하여 필요한 권한을 부여하는지 확인합니다. https://console.aws.amazon.com/iam/으로 이동하여 `Users` 옵션을 선택하고 특정 사용자를 선택한 다음 요약 페이지에서 연결된 모든 정책 목록을 볼 수 있는 `Permissions` 탭으로 이동하여 각 정책 행을 확장하여 세부 정보를 볼 수 있습니다.
- 권한 테스트: 권한을 확인하는 데 필요한 작업을 수행해 봅니다. 예를 들어 사례에 액세스해야 하는 경우 `ListCases`를 시도합니다. 필요한 권한이 없는 경우 오류 메시지가 표시됩니다.
- AWS CLI 또는 SDK 사용: 원하는 프로그래밍 언어로 AWS Command Line Interface 또는 AWS SDK를 사용하여 권한을 테스트할 수 있습니다. 예를 들어 AWS Command Line Interface를 사용하여 `aws sts get-caller-identity` 명령을 실행하여 현재 사용자 권한을 확인할 수 있습니다.
- AWS CloudTrail 로그 확인: CloudTrail 로그를 검토하여 수행하려는 작업이 로깅되고 있는지 확인합니다. 이렇게 하면 권한 문제를 식별하는 데 도움이 될 수 있습니다.

- IAM 정책 시뮬레이터 사용: IAM 정책 시뮬레이터는 IAM 정책을 테스트하고 권한이 미치는 영향을 확인할 수 있는 도구입니다.

> **Note**
>
> 특정 단계는 AWS 서비스와 수행하려는 작업에 따라 달라질 수 있습니다.

멤버십 세부 정보 설정

- 멤버십과 사례가 저장될 AWS 리전을 선택합니다.

> **Warning**
>
> 초기 멤버십 등록 후에는 기본 AWS 리전을 변경할 수 없습니다.

- 조직 단위(OU)를 통해 전체 AWS Organizations 또는 AWS Organizations의 일부에 대해 전체 멤버십 적용 범위를 제공할지 여부를 선택합니다.
- 선택적으로 이 멤버십의 이름을 선택할 수 있습니다.
- 멤버십 생성 워크플로의 일부로 기본 및 보조 연락처를 제공해야 합니다. 이러한 연락처는 인시던트 대응 팀의 일부로 자동으로 포함됩니다. 단일 멤버십에 대해 최소 2개의 연락처가 있어야 하며, 이를 통해 인시던트 대응 팀에 최소 2개의 연락처가 포함됩니다.
- 멤버십에 대한 선택적 태그를 정의합니다. 태그를 사용하면 AWS 비용을 추적하고 리소스를 검색할 수 있습니다.

AWS Organizations와 계정 연결

설정 중에 전체 AWS Organizations를 연결하도록 선택한 경우 멤버십은 조직의 모든 멤버 계정에 대한 적용 권한을 부여합니다. 연결된 계정은 조직에서 계정이 추가되거나 제거될 때 자동으로 업데이트됩니다.

설정 중에 AWS Organizations의 일부를 연결하도록 선택하고 멤버십을 특정 조직 단위(OU)로 제한한 경우 멤버십은 선택한 OU의 모든 계정에 대한 적용 권한을 부여합니다. 여기에는 선택한 OU의 하위 OU에 있는 계정이 포함됩니다. 연결된 계정은 이러한 OU에서 추가되거나 제거될 때 자동으로 업데이트됩니다.

조직 단위와 관련된 모범 사례에 대한 자세한 내용은 여러 계정을 사용하여 AWS 환경 구성을 참조하세요.

선제적 대응 및 알림 분류 워크플로 설정

AWS 보안 인시던트 대응는 Amazon GuardDuty 및 Security Hub CSPM 통합으로부터 생성된 알림을 모니터링하고 조사합니다. 이 기능을 사용하려면 Amazon GuardDuty를 활성화해야 합니다. AWS 보안 인시던트 대응는 팀이 가장 중요한 문제에 집중할 수 있도록 서비스 자동화를 통해 우선순위가 낮은 알림을 분류합니다. AWS 보안 인시던트 대응가 Amazon GuardDuty 및 AWS Security Hub CSPM와 함께 작동하는 방식에 대한 추가 정보는 사용 설명서의 탐지 및 분석 섹션을 참조하세요.

온보딩 문제가 발생하는 경우 추가 지원을 위한 AWS Support 사례를 생성하세요. 설정 프로세스 중 발생할 수 있는 AWS 계정 ID 및 오류를 포함한 세부 정보를 포함해야 합니다.

> **Note**
>
> Amazon GuardDuty 격리 규칙, 알림 분류 구성 또는 선제적 대응 워크플로에 대한 질문이 있는 경우 AWS 지원 사례(사례 유형 조사 및 문의)를 생성하여 AWS Security Incident Response 팀과 상담할 수 있습니다. 자세한 내용은 AWS 지원 사례 생성 섹션을 참조하세요.

이 기능을 사용하면 AWS 보안 인시던트 대응가 조직 내 적용되는 모든 계정과 활성 상태의 지원되는 AWS 리전에서 발견 사항을 모니터링하고 조사할 수 있습니다. 이 기능을 용이하게 하기 위해 AWS 보안 인시던트 대응는 AWS Organizations 내 적용되는 모든 멤버 계정에서 서비스 연결 역할을 자동으로 생성합니다. 그러나 관리 계정의 경우 모니터링을 활성화하려면 서비스 연결 역할을 수동으로 생성해야 합니다.

서비스가 관리 계정에서 서비스 연결 역할을 생성할 수 없습니다. AWS CloudFormation 스택 세트로 작업하여 관리 계정에서 이 역할을 수동으로 생성해야 합니다.

선테적 대응을 통한 자동 아카이브 이해

선제적 대응 및 알림 분류를 활성화하면 AWS 보안 인시던트 대응는 Amazon GuardDuty 및 Security Hub CSPM의 보안 조사 결과를 자동으로 모니터링하고 분류합니다. 이 자동 분류 워크플로의 일부로 조사 결과는 다음 기준에 따라 자동으로 아카이브됩니다.

자동 아카이브 동작:

- 양성 조사 결과: 자동 분류 프로세스에서 결과가 양성(실제 보안 위협이 아님)으로 판단되면 AWS 보안 인시던트 대응는 Amazon GuardDuty에 조사 결과를 자동으로 아카이브하고 억제 규칙을 생성하여 유사한 조사 결과로 인해 향후 알림을 생성하지 않도록 합니다.
- 억제 규칙: 서비스는 Amazon GuardDuty 및 Security Hub CSPM 모두에서 환경의 알려진 양호한 패턴(예: 예상 IP 주소, IAM 엔터티 및 정상 작동 동작)과 일치하는 조사 결과에 대한 억제 및 자동 아카이브 규칙을 생성합니다.
- 알림 볼륨 감소: SIEM 기술을 사용하는 조직에서는 서비스가 환경을 학습하고 양성 조사 결과를 자동으로 아카이브함에 따라 시간이 경과하면 Amazon GuardDuty 조사 결과 볼륨이 크게 감소합니다. 이를 통해 AWS 보안 인시던트 대응 서비스와 SIEM의 효율성이 모두 향상됩니다.

아카이브된 조사 결과 보기:

자동으로 아카이브된 조사 결과와 AWS 보안 인시던트 대응에서 생성한 억제 규칙을 검토할 수 있습니다.

1. Amazon GuardDuty 콘솔로 이동
2. 조사 결과 선택
3. 조사 결과 필터에서 아카이브됨 선택
4. 각 규칙 옆에 있는 아래쪽 화살표를 선택하여 억제 규칙 검토

중요 고려 사항:

- 아카이브된 조사 결과는 90일 동안 Amazon GuardDuty에서 유지되며 해당 기간에 언제든지 볼 수 있음
- Amazon GuardDuty 콘솔을 통해 언제든지 억제 규칙을 수정하거나 삭제할 수 있음
- 자동 분류 프로세스는 환경에 지속적으로 적응하여 시간 경과에 따른 정확도를 개선하고 오탐을 줄임

격리: 보안 인시던트가 발생하는 경우 AWS 보안 인시던트 대응는 격리 조치를 실행하여 손상된 호스트 격리 또는 자격 증명 교체와 같은 영향을 신속하게 완화할 수 있습니다. Security Incident Response는 기본적으로 격리 기능을 활성화하지 않습니다. 이러한 격리 조치를 실행하려면 먼저 서비스에 필요한 권한을 부여해야 합니다. 이는 필요한 역할을 생성하는 AWS CloudFormation StackSet를 배포하여 수행할 수 있습니다.

사용자 태스크

내용

대시보드

AWS 보안 인시던트 대응 콘솔의 대시보드에서는 인시던트 대응 팀의 개요, 선제적 대응 상태 및 4주간의 롤링 사례 수를 제공합니다.

인시던트 대응 팀

인시던트 대응 팀원의 세부 정보에 액세스하려면 인시던트 대응 팀 보기를 선택합니다.

내 사례

대시보드의 내 사례 섹션에는 정의된 기간 내에 할당된 자체 관리형 사례와 함께 AWS 지원 사례의 열림 및 종결 건수가 표시됩니다. 또한 종결된 사례를 해결하는 데 걸린 평균 시간을 시간 단위로 보여줍니다.

인시던트 대응 팀 관리

인시던트 대응 팀에는 인시던트 대응 프로세스에 대한 이해관계자가 포함되어 있습니다. 멤버십의 일부로 최대 10명의 이해관계자를 구성할 수 있습니다.

내부 이해관계자의 예로는 인시던트 대응 팀의 멤버, 보안 분석가, 애플리케이션 소유자 및 보안 리더십 팀이 있습니다.

외부 이해관계자의 예로는 인시던트 대응 프로세스에 포함하려는 독립 소프트웨어 개발 판매 회사(ISV) 및 관리형 서비스 제공업체(MSP)의 개인이 있습니다.

> **Note**
>
> 인시던트 대응 팀을 설정해도 멤버십, 사례 등의 서비스 리소스에 대한 액세스 권한이 팀원에게 자동으로 부여되지는 않습니다. AWS 보안 인시던트 대응를 위한 AWS 관리 정책을 사용하

여 리소스에 대한 읽기 및 쓰기 액세스 권한을 부여할 수 있습니다. 자세히 알아보려면 여기를 클릭하세요.

멤버십 수준에 지정된 인시던트 대응 팀원이 모든 사례에 자동으로 추가됩니다. 사례가 생성된 후 언제든지 개별 팀원을 추가하거나 제거할 수 있습니다.

인시던트 대응 팀은 커뮤니케이션 기본 설정에 나열된 이벤트에 대한 이메일 알림을 수신합니다.

통신 기본 설정

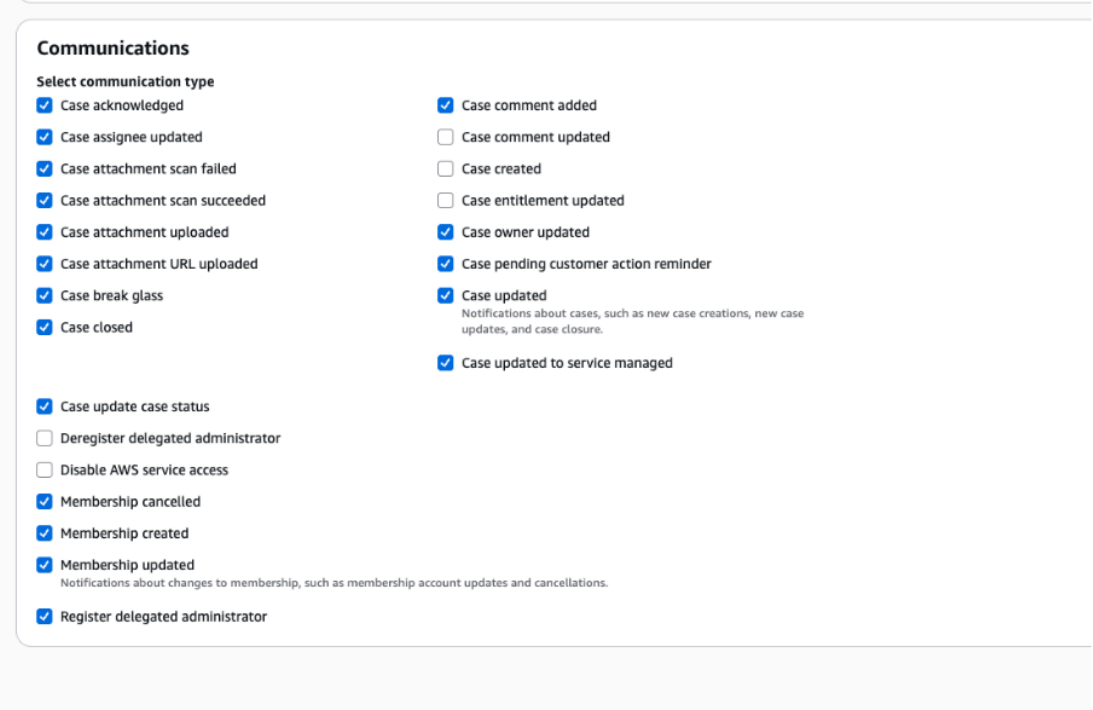
보안 인시던트 발생 시 알림을 수신하고 인시던트 대응 시스템과 상호 작용하는 방법을 제어하도록 통신 기본 설정을 구성합니다.

팀 통신 기본 설정 관리

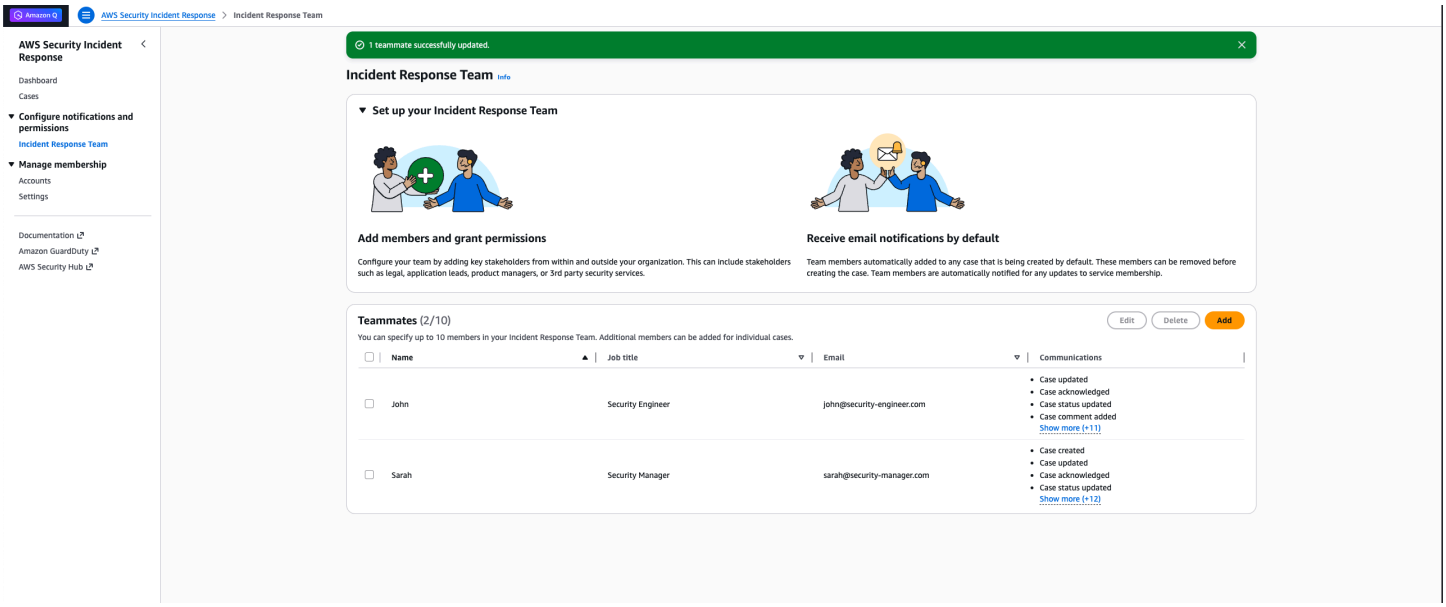
대시보드 페이지에서 인시던트 대응 팀의 개인별 통신 기본 설정을 구성할 수 있습니다.

다음 단계에 따라 멤버 통신 설정을 관리합니다.

1. 대시보드에서 인시던트 대응 팀 페이지로 이동합니다.
2. 다음 중 하나를 수행하세요.
   - 기존 팀원을 업데이트하는 방법: 커뮤니케이션 기본 설정을 수정하려는 팀원을 선택하고 편집 선택
   - 새 팀원을 추가하는 방법: 추가 선택
3. 양식 하단에 통신이 표시됩니다.
   a. 수신하려는 통신의 확인란을 선택합니다.
   b. 수신하지 않으려는 통신의 확인란을 선택 취소합니다.



4. 변경 내용을 저장합니다.



기본 통신 설정

기본적으로 인시던트 대응 팀원은 모든 커뮤니케이션을 활성화합니다. 위의 단계에 따라 언제든지 이러한 설정을 수정할 수 있습니다.

통신 옵션

통신 기본 설정은 인시던트 대응 시스템과 상호 작용하는 방식과 보안 인시던트 중에 알림이 전달되는 방식을 제어합니다.

> **Note**
>
> 이러한 기본 설정은 보안 인시던트 대응 시스템 내의 향후 모든 통신에 적용됩니다. 위의 단계를 반복하여 언제든지 이러한 설정을 수정할 수 있습니다.

AWS Organizations에 대한 계정 연결

AWS 보안 인시던트 대응을(를) 활성화하면 전체 조직 또는 특정 조직 단위(OU)를 선택할 수 있는 옵션이 제공됩니다. 특정 OU를 선택한 경우 멤버십은 선택한 OU에 속하는 계정만 적용 범위에 포함합니다. 전체 조직을 선택하면 멤버십이 조직 내 모든 계정을 적용 범위에 포함합니다.

자세한 내용은 AWS Organizations를 사용하여 AWS 보안 인시던트 대응 계정 관리를 참조하세요.

멤버십 적용 범위 관리

조직 전체 적용 범위에서 특정 OU로 전환을 포함하여 언제든지 멤버십 적용 범위 옵션을 변경할 수 있습니다.

OU 연결 업데이트

멤버십 적용 범위를 관리하는 방법:

1. 계정 연결 설정 페이지로 이동
2. OU 추가를 선택하여 멤버십에 연결하려는 OU 선택
3. 멤버십에 연결하려는 OU 선택
4. 연결 업데이트를 클릭하여 멤버십에서 OU 연결 저장

연결을 업데이트한 후 동일한 페이지로 돌아가 멤버십에서 연결 해제하려는 OU를 모두 제거할 수 있습니다. 이러한 유연성은 처음에 전체 조직을 선택했더라도 적용됩니다. 서비스를 취소하고 다시 활성화하지 않고도 특정 OU만 포함하도록 나중에 멤버십을 업데이트할 수 있습니다.

자세한 내용은 조직 단위(OU)를 통해 멤버십 관리를 참조하세요.

중요 고려 사항

루트 바로 아래 계정: 멤버십에 대한 특정 OU를 선택할 때 조직 루트 바로 아래에 있는 계정(OU의 일부가 아님)은 멤버십에 연결되지 않습니다. 멤버십 적용 범위에 이러한 계정을 포함하려면 먼저 OU에 추가한 다음 해당 OU를 멤버십에 연결해야 합니다.

> **Note**
>
> 보다 직관적이면서 자체적 설명을 포함하는 프로세스를 구성하기 위해 OU 연결 사용자 환경을 지속적으로 개선하고 있습니다.

모니터링 및 조사

AWS Security Incident Response는 Amazon GuardDuty 및 AWS Security Hub CSPM에서 보안 알림을 검토하고 분류한 다음, 환경에 따라 억제 규칙을 구성하여 불필요한 알림을 차단합니다. AWS 보안 인시던트 대응 엔지니어링(SIRE) 팀은 조사 결과를 조사하고 잠재적 문제를 빠르게 격리하도록 팀을 신속하게 에스컬레이션하고 안내합니다. 원하는 경우 AWS 보안 인시던트 대응에 사용자를 대신하여 격리 조치를 구현할 수 있는 권한을 부여할 수 있습니다.

AWS 보안 인시던트 대응는 보안 이벤트 대응을 위한 NIST 800-61r2 Computer Security event Handling Guide를 따릅니다. AWS 보안 인시던트 대응는 이러한 업계 표준을 준수함으로써 보안 이벤트 관리에 대한 일관된 접근 방식을 제공하고 AWS 환경에서 보안 이벤트를 보호하고 대응하는 모범 사례를 준수합니다.

AWS 보안 인시던트 대응에서 보안 알림을 식별하거나 사용자가 보안 지원을 요청하면 AWS SIRE에서 조사합니다. 팀은 GuardDuty 알림과 같은 로그 이벤트와 서비스 데이터를 수집하고, 해당 데이터를 분류 및 분석하고, 문제 해결 및 격리 활동을 수행하고, 인시던트 사후 보고를 제공합니다.

내용

준비

AWS 보안 인시던트 대응 팀은 보안 이벤트 대응 수명 주기 전반에 걸쳐 조사를 실시하고 사용자와 협력합니다. 보안 이벤트가 발생하기 전에 이 팀을 설정하고 필요한 권한을 할당하는 것이 좋습니다.

탐지 및 분석

이벤트 보고

AWS 보안 인시던트 대응 포털을 통해 보안 이벤트를 제기할 수 있습니다. 보안 이벤트 중에 기다리지 않는 것이 중요합니다. AWS 보안 인시던트 대응는 자동 및 수동 기술을 사용하여 보안 이벤트를 조사하고, 로그를 분석하고, 비정상적인 패턴을 찾습니다. 파트너십과 환경에 대한 이해가 이 분석을 가속화합니다.

지원되는 탐지 소스 활성화

> **Note**
>
> AWS 보안 인시던트 대응 서비스 비용에는 지원되는 탐지 소스나 다른 AWS 서비스 사용과 관련된 사용료 및 기타 비용과 수수료가 포함되지 않습니다. 비용 세부 정보는 개별 기능 또는 서비스 페이지를 참조하세요.

Amazon GuardDuty

조직 전체에서 GuardDuty를 활성화하려면 Amazon GuardDuty 사용 설명서의 `Setting up GuardDuty` 섹션을 참조하세요.

지원되는 모든 AWS 리전에서 GuardDuty를 활성화하는 것이 좋습니다. 이렇게 하면 현재 활발히 사용하고 있지 않은 리전에서도 비정상적인 활동이나 허가되지 않은 활동에 대한 결과를 GuardDuty를 통해 작성할 수 있습니다. 자세한 내용은 Amazon GuardDuty Regions and endpoints를 참조하세요.

GuardDuty를 활성화하면 AWS 보안 인시던트 대응에서 중요한 위협 탐지 데이터에 액세스할 수 있으므로 AWS 환경에서 잠재적인 보안 문제를 식별하고 대응하는 능력이 향상됩니다.

AWS Security Hub CSPM

Security Hub CSPM은 여러 AWS 서비스와 지원되는 타사 보안 솔루션에서 보안 조사 결과를 수집할 수 있습니다. 이러한 통합은 AWS 보안 인시던트 대응가 다른 탐지 도구에서 얻은 조사 결과를 모니터링하고 조사하는 데 도움이 될 수 있습니다.

Security Hub CSPM with Organizations 통합을 활성화하려면 AWS Security Hub CSPM 사용 설명서를 참조하세요.

Security Hub CSPM에서 통합을 활성화하는 방법에는 여러 가지가 있습니다. 타사 제품 통합의 경우, AWS Marketplace에서 통합을 구입한 다음 통합을 구성해야 할 수 있습니다. 통합 정보는 이러한 작업을 수행할 수 있는 링크를 제공합니다. AWS Security Hub CSPM 통합을 활성화하는 방법에 대해 자세히 알아봅니다.

AWS 보안 인시던트 대응는 다음 도구가 AWS Security Hub CSPM와 통합되는 경우 해당 도구의 조사 결과를 모니터링하고 조사할 수 있습니다.

- CrowdStrike – CrowdStrike Falcon
- Lacework – Lacework
- Trend Micro – Cloud One

이러한 통합을 활성화하면 AWS 보안 인시던트 대응의 모니터링 및 조사 기능의 범위와 효과를 크게 향상시킬 수 있습니다.

탐지

'선제적 응답'이 활성화된 경우(https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html) AWS 보안 인시던트 대응는 온보딩 중에 계정에 배포된 Amazon EventBridge 규칙을 통해 AWS Security Hub CSPM 및 Amazon GuardDuty에서 조사 결과를 수집합니다.

AWS 보안 인시던트 대응는 자동화된 분류 중에 양성으로 확인되거나 예상되는 활동에 연결된 Amazon GuardDuty 조사 결과를 자동으로 아카이브합니다. 조사 결과 상태 필터에서 아카이브됨을 선택하여 Amazon GuardDuty 콘솔에서 아카이브된 조사 결과를 볼 수 있습니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 Viewing generated findings in GuardDuty console을 참조하세요.

AWS 보안 인시던트 대응는 자동화된 분류 중에 양성으로 확인되거나 예상되는 활동에 연결된 Amazon GuardDuty 조사 결과를 자동으로 아카이브합니다. 이 아카이브는 분류되고 결과가 '아카이브'로 지정된 조사 결과에 대해서만 수행됩니다. 조사가 진행 중인 조사 결과는 조사가 완료된 후에도 Amazon GuardDuty 콘솔에서 계속 볼 수 있습니다. 조사 결과 필터에서 아카이브됨을 선택하여 Amazon GuardDuty 콘솔에서 아카이브된 조사 결과를 볼 수 있습니다. 아카이브된 조사 결과 작업에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 Working with findings를 참조하세요.

AWS Security Hub CSPM에서 보안 조사 결과를 수집하면 시스템은 자동화된 분류가 시작되었음을 나타내는 메모와 함께 각 조사 결과를 업데이트합니다. 워크플로 상태가 NEW에서 NOTIFIED로 변경되

고, 이때 기본 AWS Security Hub CSPM 조사 결과 보기에서 조사 결과가 제거됩니다. 분류에서 조사 결과가 양성이거나 예상되는 활동과 관련이 있다고 판단되면 시스템은 조사 결과에 메모를 추가하고 워크플로 상태를 SUPPRESSED로 업데이트합니다.

분석: 자동화된 분류

AWS 보안 인시던트 대응는 보안 조사 결과를 자동으로 분류합니다. 분류 프로세스에서는 조사 결과 페이로드, AWS 서비스 메타데이터, AWS 로깅 및 모니터링 데이터(예: AWS CloudTrail 및 VPC 흐름 로그), AWS 위협 인텔리전스 그리고 AWS 및 온프레미스 환경에 대한 컨텍스트를 제공하기 위해 사용자가 초대된 해당 컨텍스트를 포함한 여러 소스의 데이터를 분석하여 탐지된 활동이 예상되는 동작을 나타내는지를 결정합니다.

자동화된 분류에서 탐지된 활동이 예상되는 것으로 확인되면 시스템은 추가 조사 작업을 수행하지 않습니다.

분석: 인시던트 대응 보안 조사

AWS 보안 인시던트 대응 엔지니어링은 AWS 및 보안 인시던트 대응에 대한 전문 지식을 갖추고 상시 운영되는 글로벌 보안 전문가 팀입니다. 자동화된 분류를 통해 활동이 예상되는지 확인할 수 없는 경우 AWS 보안 인시던트 대응 엔지니어링이 참여하여 보안 조사를 수행합니다. Security Hub에서 이벤트가 수집되는 경우 AWS 보안 인시던트 대응 엔지니어링의 조사가 진행 중이라는 메모가 관련 조사 결과에 게시됩니다.

AWS 보안 인시던트 대응 엔지니어링은 추가 서비스 메타데이터 및 위협 인텔리전스를 분석하고, 환경의 과거 조사 결과 및 조사에서 얻은 인사이트를 검토하며, 인시던트 대응 전문 지식을 적용하여 실제 보안 조사를 수행합니다. 격리 기본 설정(격리 참조)에 따라 AWS Security Incident Response 엔지니어링은 AWS 보안 인시던트 대응 콘솔의 Security Incident Response 사례를 통해 조직의 인시던트 대응 팀을 참여시켜 탐지된 활동이 예상되고 해당 활동에 AWS에서 생성된 사례에 대한 대응 권한이 있는지 확인할 수 있습니다.

커뮤니케이션

AWS Security Incident Response는 Security Incident Response 사례를 통해 인시던트 대응 팀과 협력하여 보안 조사 중에 정보를 제공합니다. 여러 AWS 보안 인시던트 대응 엔지니어링 구성원이 조사를 지원할 수 있습니다. 커뮤니케이션에는 보안 조사 생성에 대한 확인 또는 알림, 통화 브리지 설정, 로그 파일과 같은 아티팩트 분석, 예상되는 활동 확인 요청, 조사 결과 공유가 포함될 수 있습니다.

AWS 보안 인시던트 대응가 선제적으로 인시던트 대응 팀을 참여시키면 AWS 보안 인시던트 대응 멤버십 계정에서 사례가 생성되고 이를 통해 모든 조직 계정에 대한 커뮤니케이션을 한 곳에서 중앙 집중화합니다. 이러한 사례에는 제목에 '[선제적 사례]'와 같은 접두사가 포함되며, 이 접두사는 AWS 보안 인시던트 대응에 의해 시작된 항목임을 식별합니다. 인시던트 대응 팀은 이러한 커뮤니케이션에 적극

적으로 참여하고 적시에 대응함으로써 다음을 수행할 수 있도록 AWS 보안 인시던트 대응를 지원할 수 있습니다.

- 실제 보안 인시던트에 신속하게 대응합니다.
- 환경과 예상 동작을 이해합니다.
- 시간 경과에 따라 거짓 양성 탐지를 줄입니다.

AWS 보안 인시던트 대응의 효과는 사용자와의 협업을 통해 향상되고 더욱 효율적으로 모니터링되는 보안 AWS 환경으로 이어집니다.

조사 결과 업데이트

AWS 보안 인시던트 대응는 소스 및 분류 결과에 따라 조사 결과를 다른 방식으로 관리합니다.

서비스 조정

계정 서비스 할당량이 허용되면 AWS 보안 인시던트 대응는 Amazon GuardDuty 억제 규칙 또는 AWS Security Hub CSPM 자동화 규칙을 배포하려고 시도합니다. 이러한 규칙은 알려진 권한 있는 활동의 유형 및 소스(예: 소스 IP 주소, ASN, ID 위탁자 또는 리소스)와 일치하는 향후 조사 결과를 억제합니다. AWS Security Hub CSPM 규칙은 10개의 우선순위로 배포되므로 필요한 경우 자체 정의되는 규칙으로 이러한 자동화를 재정의할 수 있습니다.

이러한 방식으로 AWS 보안 인시던트 대응는 AWS 환경에서 예상되는 동작을 기반으로 탐지 소스를 조정합니다. 인시던트 대응 팀은 이러한 규칙 세트의 수정에 대한 알림을 받으며, 변경 사항은 요청 시 롤백됩니다.

AI 조사 에이전트

개요

AI 기반 조사 에이전트는 고객 및 AWS 보안 인시던트 대응 엔지니어와 협력하여 보안 조사를 신속하게 처리합니다. 고객이 AWS 지원 사례를 생성하면 Security Incident Response 참여와 동시에 에이전트가 자동으로 활성화되어 해결 시간을 며칠에서 몇 시간으로 단축합니다.

고객 에스컬레이션 중에 AWS 보안 인시던트 대응에 의해 선제적으로 또는 사용자에 의해 Security Incident Response 사례가 생성될 수 있습니다. 새로운 AWS 지원 사례가 생성되면 조사 에이전트가 자동으로 트리거됩니다. 콘솔, API 또는 Amazon EventBridge 통합을 통해 모든 사례를 관리할 수 있습니다.

주요 이점

- 병렬 조사 - 대응 담당자가 함께 에이전트가 작동하여 AI 기반 자동화와 인적 전문 지식을 모두 제공합니다.
- 자동 증거 수집 - AWS CloudTrail, IAM, Amazon EC2, Cost Explorer를 자동으로 쿼리하여 수동 로그 분석을 제거합니다.
- 자연어 인터페이스 - AWS 로그 형식에 대한 전문 지식이 필요 없도록 일상 언어로 보안 문제를 설명합니다.
- 응답 속도 개선 - 조사 탭에서 몇 분 이내에 조사 요약이 제공됩니다.
- 전체 감사 가능성 - 모든 에이전트 작업이 `AWSServiceRoleForSupport` 역할의 AWS CloudTrail에 로깅됩니다.

> **Important**
>
> 이 기능은 AWS 지원 사례에만 제공됩니다. 자체 관리형 사례에는 AI 조사 기능이 포함되지 않습니다.

작동 방식

AI 조사 에이전트는 AWS 지원 보안 사례를 분석할 때 구조화된 워크플로를 따릅니다.

조사 워크플로

1. 사례 생성 - 고객이 Security Incident Response 콘솔에서 보안 관련 문제를 설명하는 AWS 지원 사례를 생성합니다.
2. 병렬 활성화
   - Security Incident Response 엔지니어가 사례에 참여합니다.
   - 이와 동시에 AI 에이전트가 조사 워크플로를 시작합니다.
3. 컨텍스트에 맞는 질문(선택 사항) - 에이전트가 다음의 특정 세부 정보를 수집하기 위해 구체화하는 질문을 할 수 있습니다.
   - 영향을 받는 AWS 계정 ID
   - 관련된 IAM 위탁자(사용자, 역할, 액세스 키)
   - 특정 리소스 식별자(S3 버킷, EC2 인스턴스, ARN)
   - 의심스러운 활동의 기간
4. 증거 수집 - 에이전트가 AWS 데이터 소스를 자동으로 쿼리합니다.
   - AWS CloudTrail - 인시던트와 연결된 API 직접 호출 및 활동

- IAM - 사용자 및 역할 권한, 정책 변경 및 새 자격 증명 생성
- Amazon EC2 인스턴스 API - 관련된 경우 컴퓨팅 리소스에 대한 정보
- Cost Explorer - 비정상적인 리소스 소비에 대한 비용 및 사용량 지표

5. 분석 및 상관관계 파악 - 에이전트가 여러 서비스에서 수집한 증거의 상관관계를 파악하고, 패턴을 식별하고, 이벤트의 타임라인을 구성합니다.
6. 요약 생성 - 몇 분 안에 에이전트가 조사 탭에 포괄적인 조사 요약을 제공합니다.

> **Note**
>
> 모든 필드는 선택 사항입니다. 10분 이내에 답변이 제공되지 않으면 자동으로 조사가 시작됩니다. 경우에 따라 충분한 정보가 이미 제공되어 있다면 에이전트가 선택 사항 질문을 완전히 건너뛸 수 있습니다.

조사 결과 액세스

AI 분석을 보는 방법은 다음과 같습니다.

1. Security Incident Response 콘솔에서 해당 사례로 이동합니다.
2. 조사 탭을 선택합니다.
3. 조사 결과, 타임라인, 컨텍스트가 포함된 조사 요약을 검토합니다.

AI 조사 에이전트 요약이 자동으로 사례의 커뮤니케이션 섹션에 설명으로 게시되므로 다른 사례 업데이트와 함께 쉽게 검토할 수 있습니다.

데이터 액세스 및 권한

AI 조사 에이전트는 `AWSServiceRoleForSupport` 서비스 연결 역할을 사용하여 AWS 리소스에 액세스합니다. 이 역할에서는 증거 수집에 필요한 읽기 전용 권한을 제공합니다.

에이전트가 수행하는 모든 작업이 AWS CloudTrail에 로깅되므로 조사 중에 액세스한 데이터를 고객이 정확하게 감사할 수 있습니다. AWS CloudTrail 로그에서 이러한 작업은 `AWSServiceRoleForSupport`에 귀속됩니다.

사전 조건

AI 기반 조사 기능을 사용하기 전에 다음을 확인하세요.

필수 설정

- AWS 보안 인시던트 대응 활성화됨 - AWS Organizations 관리 계정을 통해 서비스를 활성화해야 합니다.
- AWS 지원 사례 유형 - AI 조사는 AWS 지원 사례(자체 관리형 사례 제외)에만 사용할 수 있습니다.
- AWSServiceRoleForSupport - 이 서비스 연결 역할은 자동으로 생성되며 조사 에이전트에 필요한 권한을 제공합니다.

필요한 권한

AWS 지원 사례를 생성하고 조사 결과에 액세스하려면 IAM 위탁자에게 다음과 같은 권한이 필요합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "security-ir:CreateCase",
                "security-ir:GetCase",
                "security-ir:ListCases",
                "security-ir:UpdateCase"
            ],
            "Resource": "*"
        }
    ]
}
```

조사 에이전트 사용

AI 조사 에이전트는 AWS 지원 사례를 생성할 때 자동으로 활성화됩니다.

AI 조사 진행 상황을 모니터링하는 방법

1. AWS 보안 인시던트 대응 콘솔에서 사례를 엽니다.
2. 조사 탭을 선택합니다.
3. 조사 상태(진행 중 또는 완료됨)를 봅니다.
4. 조사 완료되면 조사 결과, 타임라인, 권장 사항이 포함된 종합적인 조사 요약을 검토합니다.

책임 있는 AI 공개

조사 요약은 AWS 생성형 AI 기능을 사용하여 생성됩니다. 사용자는 특정 컨텍스트에서 AI 생성 권장 사항을 평가하고, 적절한 감독 메커니즘을 구현하고, 조사 결과를 독립적으로 검증하고, 모든 보안 결정에 대한 인적 감독을 유지 관리할 책임이 있습니다.

고객 데이터 사용

AI 조사 에이전트는 모델 훈련에 고객 데이터를 사용하지 않으며 고객 데이터를 서드 파티와 공유하지 않습니다.

격리

AWS Security Incident Response는 이벤트를 포함하기 위해 사용자와 협력합니다. 보안 조사 결과에 대응하여 계정에서 선제적 격리 작업을 수행하도록 서비스를 구성할 수 있습니다. 또한 지원되는 격리 작업에서 설명한 대로 SSM 문서를 사용하여 직접 또는 서드 파티 관계자와 협력하여 격리를 수행할 수도 있습니다.

> **Important**
>
> AWS Security Incident Response는 기본적으로 격리 기능을 활성화하지 않습니다. 선제적 격리 기능을 활성화하려면 다음 두 단계가 필요합니다.
>
> 1. IAM 역할을 사용하여 서비스에 필요한 권한을 부여합니다. 필요한 역할을 생성하는 AWS CloudFormation StackSets 작업을 통해 계정당 또는 조직 전체에서 이러한 역할을 개별적으로 생성할 수 있습니다.
> 2. 계정별 또는 조직 전체에서 격리 기본 설정을 정의하여 선제적 격리 작업에 권한을 부여합니다. 계정 수준 기본 설정은 조직 수준 기본 설정을 대체합니다. 이 작업은 AWS 지원 사례(기술: Security Incident Response 서비스/기타)를 생성하여 수행할 수 있습니다. 사용 가능한 격리 기본 설정은 다음과 같습니다.
>   - 승인 필요(기본값): 사례별로 명시적 권한 부여 없이 리소스를 선제적으로 격리하지 않습니다.
>   - 확인 항목 격리: 손상된 것으로 확인된 리소스에 대해 선제적 격리를 수행합니다.
>   - 의심 항목 격리: AWS Security Incident Response 엔지니어링에서 수행한 분석을 기반으로 손상 가능성이 큰 리소스를 선제적으로 격리합니다.

격리 의사 결정

격리의 필수적인 부분은 시스템 종료, 네트워크에서 리소스 격리, 액세스 차단 또는 세션 종료 여부와 같은 의사 결정입니다. 이러한 결정은 이벤트를 격리하려는 미리 결정된 전략과 절차가 있을 때 더 쉬

워집니다. AWS Security Incident Response는 격리 전략을 제공하고, 잠재적 영향을 알리며, 관련된 위험을 고려하고 동의한 후에만 솔루션을 구현하는 방법을 안내합니다.

지원되는 격리 작업

AWS 보안 인시던트 대응는 지원되는 격리 조치를 사용자를 대신하여 실행하여 대응을 신속하게 진행하고 위협 행위자가 사용자 환경에 잠재적으로 피해를 입힐 수 있는 시간을 줄여줍니다. 이 기능을 사용하면 식별된 위협을 더 빠르게 완화하고 잠재적 영향을 최소화하며 전반적인 보안 태세를 강화할 수 있습니다. 분석 중인 리소스에 따라 다양한 격리 옵션이 있습니다. 지원되는 격리 작업은 아래 하위 섹션에 설명되어 있습니다.

EC2 격리

`AWSSupport-ContainEC2Instance` 격리 자동화는 EC2 인스턴스의 가역 네트워크 격리를 수행하여 인스턴스를 그대로 실행 상태로 유지하지만 새로운 네트워크 활동으로부터 격리하고 VPC 내부 및 외부 리소스와 통신하지 못하도록 합니다.

> **Important**
>
> 보안 그룹 변경으로 인해 기존의 추적된 연결은 종료되지 않으며, 새로운 보안 그룹과 이 SSM 문서에 의해 향후 트래픽만 효과적으로 차단된다는 점에 유의하세요. 자세한 내용은 서비스 기술 가이드의 source containment 섹션에서 확인할 수 있습니다.

IAM 격리

`AWSSupport-ContainIAMPrincipal` 격리 자동화는 IAM 사용자 또는 역할에 대한 가역적 네트워크 격리를 수행하여 사용자 또는 역할을 IAM에 그대로 두지만 계정 내의 리소스와 통신하지 못하도록 격리합니다.

S3 격리

`AWSSupport-ContainS3Resource` 격리 자동화는 S3 버킷의 가역적 격리를 수행하여 객체를 버킷에 그대로 두고 액세스 정책을 수정하여 Amazon S3 버킷 또는 객체를 격리합니다.

격리 전략 개발

AWS 보안 인시던트 대응는 위험 수용 범위에 맞는 각 주요 이벤트 유형에 대한 격리 전략을 고려하도록 권장합니다. 이벤트 중 의사 결정에 도움이 되는 명확한 기준을 문서화하세요. 고려해야 할 기준은 다음과 같습니다.

- 리소스의 잠재적 손상

- 증거 및 규제 요구 사항 보존
- 서비스 사용 불가(예: 네트워크 연결, 외부 당사자에게 제공되는 서비스)
- 전략을 구현하는 데 필요한 시간 및 리소스
- 전략의 효율성(예: 부분 격리 및 전체 격리)
- 솔루션의 영구성(예: 가역적 및 비가역적)
- 솔루션 기간(예: 긴급 해결 방법, 임시 해결 방법, 영구 솔루션)

보안 제어를 적용합니다. 그러면 위험을 낮추고 보다 효과적인 격리 전략을 정의하고 구현할 시간을 확보할 수 있습니다.

단계적 격리 접근 방식

AWS 보안 인시던트 대응는 리소스 유형에 따라 단기 및 장기 전략을 포함하는 단계적 접근 방식을 통해 효율적이고 효과적인 격리를 달성할 것을 권장합니다.

격리 전략

AWS 보안 인시던트 대응는 보안 이벤트의 범위를 파악할 수 있나요?

- 그렇다면 모든 리소스(사용자, 시스템, 리소스)를 식별합니다.
- 그렇지 않으면 식별된 리소스에 대해 다음 단계를 실행하는 것과 병행하여 조사합니다.

리소스를 격리할 수 있나요?

- 그렇다면 영향을 받는 리소스를 격리합니다.
- 그렇지 않은 경우 시스템 소유자 및 관리자와 협력하여 문제를 격리하는 데 필요한 추가 조치를 결정합니다.

영향을 받는 모든 리소스가 영향을 받지 않는 리소스로부터 격리되어 있나요?

- 그렇다면 다음 단계로 계속 진행합니다.
- 그렇지 않으면 영향을 받는 리소스를 계속 격리하여 단기 격리를 완료하고 이벤트가 더 이상 에스컬레이션되지 않도록 합니다.

시스템 백업

추가 분석을 위해 영향을 받는 시스템의 백업 사본이 생성되었나요?

포렌식 사본은 암호화되어 안전한 위치에 저장되나요?

- 그렇다면 다음 단계로 계속 진행합니다.
- 그렇지 않으면 포렌식 이미지를 암호화한 다음 안전한 위치에 저장하여 우발적인 사용, 손상 및 변조를 방지합니다.

격리 기본 설정 제출

계정 또는 조직의 격리 기본 설정을 구성하려면 AWS Support 사례를 생성합니다.

지원 사례에서 다음 정보를 지정합니다.

구성 후 AWS 보안 인시던트 대응는 환경 보호를 위해 활성 보안 인시던트 중 권한이 부여된 격리 작업을 실행합니다.

- 격리 작업에 대한 권한을 부여해야 하는 AWS Organizations ID 또는 특정 계정 ID.
- 선호하는 격리 옵션.

> **Note**
>
> AWS 보안 인시던트 대응는 적절한 기본 설정으로 구성된 경우에만 필요한 권한을 부여하기 위해 필수 AWS CloudFormation StackSet가 배포된 후에 격리 작업을 실행합니다.

근절

근절 단계에서는 맬웨어 삭제, 손상된 사용자 계정 제거, 발견된 취약성 완화 등 영향을 받는 모든 계정, 리소스 및 인스턴스를 식별하고 해결하여 환경 전체에 균일한 해결 방법을 적용하는 것이 중요합니다.

근절 및 복구에 단계적 접근 방식을 사용하고 문제 해결 단계의 우선순위를 지정하는 것이 가장 좋습니다. 초기 단계의 목적은 향후 이벤트를 방지하기 위해 가치가 높은 변경 사항을 적용하여 전반적인 보안을 빠르게(며칠에서 몇 주) 강화하는 것입니다. 이후 단계에서는 인프라 변경 등의 장기적인 변화와 엔터프라이즈의 보안을 최대한 유지하기 위한 지속적인 작업에 집중할 수 있습니다. 각 사례는 고유하며 AWS Security Incident Response 엔지니어는 는 고객과 협력하여 필요한 조치를 평가합니다.

다음을 고려하세요.

- 시스템을 다시 이미지화하고 패치나 기타 대응책으로 시스템을 강화하여 공격의 위험을 방지하거나 줄일 수 있나요?

- 감염된 시스템을 새로운 인스턴스나 리소스로 교체하여 감염된 항목을 종료하는 동시에 깨끗한 기준선을 유지할 수 있나요?
- 무단 사용으로 인해 남아 있는 모든 맬웨어와 기타 아티팩트를 제거하고 영향을 받는 시스템을 추가 공격으로부터 강화했나요?
- 영향을 받는 리소스에 대한 포렌식 요구 사항이 있나요?

복구

AWS 보안 인시던트 대응는 시스템을 정상 작동으로 복원하고, 시스템이 제대로 작동하는지 확인하고, 향후 유사한 이벤트를 방지하기 위해 취약성을 해결하는 데 도움이 되는 지침을 제공합니다. AWS 보안 인시던트 대응는 시스템 복구에 직접적인 도움이 되지 않습니다. 주요 고려 사항은 다음과 같습니다.

- 영향을 받는 시스템이 최근 공격에 대비해 패치가 적용되고 강화되었나요?
- 시스템을 프로덕션으로 복원하는 데 가능한 타임라인은 어떻게 되나요?
- 복구된 시스템을 테스트, 모니터링, 확인하는 데 어떤 도구를 사용할 예정인가요?

인시던트 사후 보고서

AWS 보안 인시던트 대응는 고객 팀과 당사 팀 간의 보안 활동이 종료된 후 이벤트 요약을 제공합니다.

매월 말에 AWS 보안 인시던트 대응 서비스는 이메일을 통해 각 고객의 기본 연락 창구로 월별 보고서를 전송합니다. 보고서는 아래 설명된 지표를 사용하여 PDF 형식으로 전달됩니다. 고객은 AWS Organizations당 하나의 보고서를 받게 됩니다.

사례 지표

- 생성된 사례
  - 차원 이름: 입력
  - 차원 값: AWS 지원, 자체 지원
  - 단위: 수
  - 설명: 생성된 사례 수입니다.
- 종결된 사례
  - 차원 이름: 입력
  - 차원 값: AWS 지원, 자체 관리형

- 단위: 수
- 설명: 종결된 총 사례 수를 측정한 값입니다.

- 열린 사례
  - 차원 이름: 입력
  - 차원 값: AWS 지원, 자체 지원
  - 단위: 수
  - 설명: 미해결 사례 수입니다.

지표 분류

- 수신된 조사 결과
  - 단위: 수
  - 설명: 분류를 위해 보낸 조사 결과 수입니다.
- 아카이브된 조사 결과
  - 단위: 수
  - 설명: 수동 조사 없이 처리된 후 보관된 조사 결과 수입니다.
- 수동으로 조사된 조사 결과
  - 단위: 수
  - 설명: 수동 조사가 수행된 결과 수입니다.
- 아카이브된 조사
  - 단위: 수
  - 설명: 오탐이 발생하고 아카이빙을 위해 보낸 수동 조사 수입니다.
- 에스컬레이션된 조사
  - 단위: 수
  - 설명: 보안 인시던트로 이어지는 수동 조사 수입니다.

Cases

AWS 보안 인시던트 대응를 사용하면 AWS 지원 사례 또는 자체 관리형 사례라는 두 가지 유형의 사례를 생성할 수 있습니다.

AWS 지원 사례 생성

콘솔, API 또는 AWS Command Line Interface를 통해 AWS 보안 인시던트 대응에 대한 AWS 지원 사례를 생성할 수 있습니다. AWS 지원 사례를 사용하면 Security Incident Response 엔지니어의 지원을 받을 수 있습니다.

Important

데모/시뮬레이션 사례는 90일 후에 종료됩니다.

Note

AWS Security Incident Response 엔지니어는 15분 이내에 사례에 응답합니다. 대응 시간은 AWS Security Incident Response 엔지니어의 첫 번째 대응 시간입니다. 이 기간 내에 초기 요청에 대응하기 위해 최선을 다하겠습니다. 이 대응 시간은 후속 대응에는 적용되지 않습니다.

Note

활성 보안 인시던트 및 조사뿐만 아니라 AWS Security Incident Response 기능에 대한 문의를 위해서도 AWS 지원 사례를 생성할 수 있습니다. 여기에는 GuardDuty 억제 규칙, 알림 분류 구성, 선제적 대응 워크플로 및 보안 태세에 대한 일반적인 지침에 대한 질문이 포함됩니다. 이러한 목적에 대해서는 조사 및 문의 사례 유형을 선택합니다.

AWS 보안 인시던트 대응에 문의해야 하는 경우

필요에 따라 다양한 목적으로 AWS Security Incident Response에 문의할 수 있습니다. 다음 표에서는 다양한 시나리오와 각 시나리오에 적합한 문의 방법을 설명합니다.

시나리오	사용해야 하는 경우	응답 시간	사례 유형
활성 보안 인시던트	즉각적인 인시던트 대응 지원 및 서비스가 필요한 긴급 보안 인시던트가 발생하는 경우	15분(첫 번째 응답)	활성 보안 인시던트
조사	인지된 보안 인시던트가 있으며 인시던트 대응 조사의 로그	15분(첫 번째 응답)	조사 및 문의

시나리오	사용해야 하는 경우	응답 시간	사례 유형
	분석 및 2차 확인에 대한 지원이 필요한 경우		
문의 및 안내	Amazon GuardDuty 조사 결과, 억제 규칙, 알림 분류 구성, 선제적 대응 워크플로 또는 AWS 보안 인시던트 대응 기능과 관련된 일반적인 보안 태세에 대한 질문이 있는 경우	15분(첫 번째 응답)	조사 및 문의
온보딩 문제	AWS Security Incident Response에 대한 온보딩 프로세스 중에 기술 문제가 발생한 경우	지원 계획에 따라 다름	AWS Support 사례

모든 AWS 지원 사례(활성 보안 인시던트와 조사 및 문의)에 대해 AWS Security Incident Response 엔지니어는 첫 번째 대응 시 15분 이내에 대응합니다. 이 응답 시간은 초기 문의에만 적용되며 후속 대응에는 적용되지 않습니다.

다음 예시에서는 콘솔 사용을 다룹니다.

1. AWS Management Console을 AWS 보안 인시던트 대응에 로그인하세요.
2. 사례 생성을 선택합니다.
3. AWS를 통한 사례 해결을 선택합니다.
4. 요청의 유형을 선택합니다.
   a. 활성 보안 인시던트: 이 유형은 긴급 인시던트 대응 지원 및 서비스를 위한 것입니다.
   b. 조사 및 문의: Security Incident Response 엔지니어가 인시던트 대응 조사의 로그 분석 및 2차 확인에서 지원할 수 있는 인지된 AWS 보안 인시던트에 이 유형을 사용합니다. 또한 이 유형을 사용하여 GuardDuty 조사 결과, 억제 규칙, 알림 분류 구성, 선제적 대응 워크플로 및 AWS Security Incident Response 기능과 관련된 일반적인 보안 태세 질문에 대한 문의를 할 수 있습니다.
5. 예상 시작 날짜를 인시던트의 가장 초기 지표 날짜로 설정합니다. 예를 들어, 비정상적인 동작을 처음 경험했거나 관련 보안 알림을 처음 받았을 때입니다.
6. 사례에 대한 제목 정의

7. 사례에 대한 자세한 설명을 제공합니다. 인시던트 대응 담당자가 사례 해결에 도움이 될 수 있는 다음 측면을 고려하세요.
   a. 어떻게 된 걸까요?
   b. 누가 인시던트를 발견하고 보고했나요?
   c. 누가 사례의 영향을 받나요?
   d. 알려진 영향은 무엇인가요?
   e. 이 사례의 긴급성은 무엇인가요?
   f. 사례 범위에 속하는 AWS 계정 ID를 하나 이상 추가합니다.
8. 선택적 사례 세부 정보를 추가합니다.
   a. 드롭다운 목록에서 영향을 받는 기본 서비스를 선택합니다.
   b. 드롭다운 목록에서 영향을 받는 기본 리전을 선택합니다.
   c. 이 사례의 일부로 식별한 위협 행위자 IP 주소를 하나 이상 추가합니다.
9. 알림을 받을 사례에 선택적 추가 인시던트 대응 담당자를 추가합니다. 개인을 추가하려면 다음을 수행합니다.
   a. 이메일 주소를 추가합니다.
   b. 선택적 이름과 성을 추가합니다.
   c. 새 항목 추가를 선택하여 다른 개인을 추가합니다.
   d. 개인을 제거하려면 해당 개인에 대한 제거 옵션을 선택합니다.
   e. 추가를 선택하여 나열된 모든 개인을 사례에 추가합니다.
      i. 여러 개인을 선택하고 제거를 선택하여 목록에서 삭제할 수 있습니다.
10사례에 선택적 태그를 추가합니다.
   a. 태그를 추가하려면 다음을 수행합니다.
   b. 새로운 태그 추가를 선택합니다.
   c. 키에는 태그의 이름을 입력합니다.
   d. 값에는 태그 값을 입력합니다.
   e. 태그를 제거하려면 태그의 제거 옵션을 선택합니다.

AWS 지원 사례가 생성되면 AWS Security Incident Response 엔지니어와 인시던트 대응 팀에 즉시 알림이 전달됩니다.

AI 조사로 AWS 지원 사례를 생성하는 방법

1. console.aws.amazon.com/에서 AWS 보안 인시던트 대응 콘솔을 여세요.

2. 탐색 창에서 사례를 선택합니다.
3. 사례 생성을 선택합니다.
4. 사례 유형에서 AWS 지원 사례를 선택합니다.
5. 제목, 인시던트 시작 날짜, 영향을 받는 AWS 계정 ID를 포함한 사례 세부 정보를 제공합니다.
6. 보안 이벤트 설명 섹션에서 인시던트에 대한 상세한 설명을 제공합니다.
7. 영향을 받는 AWS 서비스, 리전 및 기타 관련 세부 정보에 대한 추가 정보를 제공합니다.
8. 사례 생성을 선택합니다.

사례 생성 후 Security Incident Response 엔지니어와 AI 에이전트 모두 동시에 작업을 시작합니다.

AI의 구체화 질문에 응답하는 방법(선택 사항)

1. 사례의 조사 탭으로 이동합니다.
2. AI 에이전트가 제시한 구체화 질문을 검토합니다.
3. 질문에 응답하거나, 답변하지 않으려면 건너뛰기를 선택합니다.
4. 제출을 선택하여 계속합니다. 모든 필드는 선택 사항입니다.

책임 있는 AI 공개

조사 요약은 AWS 생성형 AI 기능을 사용하여 생성됩니다. 사용자는 특정 컨텍스트에서 AI 생성 권장 사항을 평가하고, 적절한 감독 메커니즘을 구현하고, 조사 결과를 독립적으로 검증하고, 모든 보안 결정에 대한 인적 감독을 유지 관리할 책임이 있습니다.

자체 관리형 사례 생성

콘솔, API 또는 AWS Command Line Interface를 통해 AWS 보안 인시던트 대응에 대한 자체 관리형을 생성할 수 있습니다. 이 유형의 사례는 AWS Security Incident Response 엔지니어를 참여시키지 않습니다. 다음 예시에서는 콘솔 사용을 다룹니다.

1. https://console.aws.amazon.com/security-ir/를 AWS 보안 인시던트 대응 통해 AWS Management Console에 로그인합니다.
2. Create Case(사례 생성)을 선택합니다.
3. 자체 인시던트 대응 팀과 함께 사례 해결을 선택합니다.
4. 예상 시작 날짜를 인시던트의 가장 초기 지표 날짜로 설정합니다. 예를 들어, 비정상적인 동작을 처음 경험했거나 관련 보안 알림을 처음 받았을 때입니다.

5. 사례의 제목을 정의합니다. 제목 생성 옵션을 선택할 때 제안된 대로 사례 제목에 데이터를 포함하는 것이 좋습니다.
6. 사례의 일부인 AWS 계정 ID를 입력합니다. 계정 ID를 추가하려면 다음을 수행합니다.
   a. 12자리 계정 ID를 입력하고 계정 추가를 선택합니다.
   b. 계정을 제거하려면 사례에서 제거하려는 계정 옆의 제거를 선택합니다.
7. 사례에 대한 자세한 설명을 제공합니다.
   a. 인시던트 대응 담당자가 사례 해결에 도움이 될 수 있는 다음 측면을 고려하세요.
      i. 어떻게 된 걸까요?
      ii. 누가 인시던트를 발견하고 보고했나요?
      iii. 누가 사례의 영향을 받나요?
      iv. 알려진 영향은 무엇인가요?
      v. 이 사례의 긴급성은 무엇인가요?
8. 선택적 사례 세부 정보를 추가합니다.
   a. 드롭다운 목록에서 영향을 받는 기본 서비스를 선택합니다.
   b. 드롭다운 목록에서 영향을 받는 기본 리전을 선택합니다.
   c. 이 사례의 일부로 식별한 위협 행위자 IP 주소를 하나 이상 추가합니다.
9. 알림을 받을 사례에 선택적 추가 인시던트 대응 담당자를 추가합니다. 개인을 추가하려면 다음을 수행합니다.
   a. 이메일 주소를 추가합니다.
   b. 선택적 이름과 성을 추가합니다.
   c. 새 항목 추가를 선택하여 다른 개인을 추가합니다.
   d. 개인을 제거하려면 해당 개인에 대한 제거 옵션을 선택합니다.
   e. 추가를 선택하여 나열된 모든 개인을 사례에 추가합니다. 여러 개인을 선택하고 제거를 선택하여 목록에서 삭제할 수 있습니다.
10. 사례에 선택적 태그를 추가합니다. 태그를 추가하려면 다음을 수행합니다.
   a. 새로운 태그 추가를 선택합니다.
   b. 키에는 태그의 이름을 입력합니다.
   c. 값에는 태그 값을 입력합니다.
   d. 태그를 제거하려면 태그의 제거 옵션을 선택합니다.

사례가 생성되면 인시던트 대응 팀에 이메일로 알림이 전송됩니다.

AWS Security Incident Response 엔지니어와의 작업

보안 인시던트 사례를 연 후 AWS Security Incident Response 엔지니어가 인시던트 작업을 시작합니다. 이 섹션에서는 조사 중에 예상되는 사항과 팀과 효과적으로 협업하는 방법을 설명합니다.

AWS Security Incident Response 엔지니어에게 예상되는 사항

AWS 지원 사례를 열면 Security Incident Response 엔지니어가 인시던트에 할당됩니다. 할당된 대응 응답자는 다음을 수행합니다.

- 사례에서 제공한 초기 정보 검토
- 관련 AWS 서비스 로그 및 보안 조사 결과 분석
- 보안 인시던트의 범위 및 영향 식별
- 상황에 맞는 조사 및 대응 계획 개발

응답 타임라인: AWS 보안 인시던트 대응 엔지니어의 신규 사례 승인에 대한 서비스 수준 목표(SLO)는 15분 이내입니다. 초기 평가 타임라인은 사례 심각도와 복잡도에 따라 다를 수 있습니다. AWS 보안 인시던트 대응 엔지니어가 영업일 기준 5일 이내에 응답이나 중요한 정보를 받지 못하면 사례가 종결됩니다.

조사 워크플로

AWS Security Incident Response 엔지니어는 NIST 800-61r2 프레임워크에 부합하는 구조화된 인시던트 대응 프로세스를 따릅니다. 조사 중에 다음과 같은 단계를 예상할 수 있습니다.

1. 초기 분류 - Security Incident Response 엔지니어가 사례 세부 정보를 검토하고 인시던트 범위를 확인함
2. 조사 - Security Incident Response 엔지니어가 로그를 분석하고, 위협 지표를 식별하며, 근본 원인을 파악함
3. 격리 - Security Incident Response 엔지니어가 인시던트의 영향을 제한하는 작업을 권장함
4. 제거 및 복구 - Security Incident Response 엔지니어가 위협을 제거하고 정상 운영을 복원하는 데 도움을 줌
5. 인시던트 사후 검토 - Security Incident Response 엔지니어가 향후 인시던트를 방지하기 위해 조사 결과 및 권장 사항을 제공함

이러한 단계 전체에서 Security Incident Response 엔지니어는 사례 업데이트를 통해 사용자에게 최신 정보를 제공하고 추가 정보 또는 조치를 요청할 수 있습니다.

Security Incident Response 엔지니어가 요청할 수 있는 정보

인시던트를 효과적으로 조사하기 위해 AWS Security Incident Response 엔지니어는 다음을 제공하도록 요청할 수 있습니다.

- 타임라인 세부 정보 - 인시던트 및 인시던트로 이어지는 관련 이벤트를 처음 탐지한 시점
- 영향을 받는 리소스 - 관련된 특정 AWS 계정 ID, 서비스, 리전 및 리소스 ARN
- 액세스 정보 - 영향을 받는 리소스에 대한 액세스 권한을 가진 사람에 대한 세부 정보 및 최근 모든 액세스 변경 사항
- 비즈니스 컨텍스트 - 영향을 받는 리소스의 사용 방식 및 잠재적 비즈니스 영향
- 로그 및 증거 - 조사에 도움이 될 수 있는 추가적인 로그, 스크린샷 또는 아티팩트
- 권한 부여 - 사용자를 대신하여 특정 격리 또는 수정 작업을 수행하기 위한 승인

Security Incident Response 엔지니어는 각 정보가 필요한 이유와 이 정보가 조사에 어떻게 도움이 되는지 설명합니다.

커뮤니케이션 모범 사례

효과적인 커뮤니케이션은 인시던트 해결을 가속합니다. AWS Security Incident Response 엔지니어와 협력할 때는 다음과 같은 사례를 따릅니다.

- 즉각적 대응: Security Incident Response 엔지니어의 정보 요청에 즉시 대응
- 전체 정보 제공: 관련성이 확실하지 않은 경우에도 전체 정보 제공
- 질문: 권장 사항을 이해하지 못하거나 자세한 설명이 필요한 경우 질문
- 사례 업데이트: 인시던트에 대한 새로운 진전 사항 또는 변경 사항으로 사례 업데이트
- 기본 담당자 지정: Security Incident Response 엔지니어와 조율할 팀의 기본 담당자 지정

> **Important**
>
> AWS 보안 인시던트 대응 엔지니어가 영업일 기준 5일 이내에 중요한 정보 요청에 대한 응답을 받지 못하면 사례 종결이 진행됩니다. 사용 가능한 새 정보가 있으면 사례를 다시 열 수 있습니다.

조사 중 역할

AWS 보안 인시던트 대응 엔지니어가 조사를 주도하지만 여러분의 참여는 중요합니다. 사용자는 다음을 수행할 책임이 있습니다.

- 정보 요청에 대해 적시에 대응
- AWS 환경에서 권장되는 격리 및 문제 해결 작업 구현
- Security Incident Response 엔지니어가 사용자를 대신하여 조치를 취하도록 권한 부여(선제적 대응을 활성화한 경우)
- 필요에 따라 내부 팀(보안, 법률, 규정 준수)과 조율
- 인시던트 대응 우선순위 및 장단점에 대한 비즈니스 의사 결정 수립

AWS 보안 인시던트 대응 엔지니어는 전문 지식과 권장 사항을 제공하지만, AWS 리소스에 대한 제어를 유지 관리하고 대응 조치에 대한 최종 결정을 내리는 것은 사용자입니다.

사례 종료

다음과 같은 경우 AWS 보안 인시던트 대응 엔지니어가 사례를 종결합니다.

- 인시던트가 격리 및 해결됨
- 모든 조사 결과가 사용자와 공유됨
- 추가 Security Incident Response 엔지니어 지원이 필요하지 않음
- 사례 종료를 요청함

사례를 종료하기 전에 Security Incident Response 엔지니어는 조사 결과, 수행한 조치 및 보안 태세를 개선하기 위한 권장 사항을 요약하여 제공합니다.

사례 종결 후 추가 지원이 필요한 경우 새 사례를 열거나 AWS Support에 문의할 수 있습니다.

AWS에서 생성한 사례에 대응

AWS 보안 인시던트 대응는 계정이나 리소스에 영향을 줄 수 있는 사항에 대해 조치를 취하거나 알아야 할 때 아웃바운드 알림이나 사례를 생성할 수 있습니다. 이는 구독의 일부로 선제적 대응 및 알림 분류 워크플로를 활성화한 경우에만 발생합니다.

이러한 알림은 AWS 보안 인시던트 대응 콘솔에 접두사 '[선제적 사례]'가 붙은 Security Incident Response 사례로 표시됩니다. 이러한 사례를 보고 관리하려면 다음 단계를 완료하세요.

- Security Incident Response 콘솔(https://console.aws.amazon.com/security-ir/)을 엽니다.

- 사례를 선택합니다.
- '[선제적 사례]' 접두사가 붙은 사례를 포함하여 모든 사례가 보입니다.

필요에 따라 이러한 사례를 업데이트하고, 해결하고, 다시 열 수 있습니다. 이러한 사례를 통해 AWS 보안 인시던트 대응 팀과 직접 소통하여 잠재적 보안 문제를 효율적으로 처리할 수 있습니다.

사례 관리

내용

사례 상태 변경

사례는 다음 상태 중 하나입니다.

- 제출됨: 사례의 초기 상태입니다. 이 상태의 사례는 요청자가 제출했지만 아직 작업 중이 아닙니다.
- 탐지 및 분석: 이 상태는 인시던트 대응 담당자가 사례에 대한 작업을 시작했음을 나타냅니다. 이 단계에는 데이터 수집, 이벤트 분류, 데이터 기반 결론 생성을 위한 분석 수행이 포함됩니다.
- 방지, 근절, 복구: 이 상태에서 인시던트 대응 담당자가 제거를 위해 추가적인 노력이 필요한 의심스러운 활동을 식별했습니다. 인시던트 대응 담당자가 비즈니스 위험 분석 및 추가 조치에 대한 권장 사항을 제공합니다. 서비스에 대한 옵트인 기능을 활성화한 경우 AWS 인시던트 대응 담당자는 영향을 받는 계정의 SSM 문서로 격리 조치를 수행하는 데 동의를 구합니다.
- 인시던트 사후 활동: 이 상태에서 기본 보안 이벤트가 격리되었습니다. 이제 핵심은 비즈니스 운영을 복구하고 정상으로 되돌리는 것입니다. 사례에 대한 해석기가 AWS에서 지원되는 경우 요약 및 근본 원인 분석이 제공됩니다.

- 종결됨: 워크플로의 최종 상태입니다. 종결됨 상태의 사례는 작업이 완료되었음을 나타냅니다. 종결된 사례는 다시 열 수 없으므로 이 상태로 전환하기 전에 모든 작업이 완료되었는지 확인하세요.

작업/상태 업데이트를 선택하여 자체 관리형 사례의 사례 상태를 변경합니다. AWS 지원 사례의 경우 AWS Security Incident Response 엔지니어가 이 상태를 설정합니다.

해석기 변경

자체 관리형 사례의 경우 인시던트 대응 팀이 AWS에 도움을 요청할 수 있습니다. AWS의 지원 받기를 선택하여 이 사례에 대한 해결자를 AWS로 변경합니다. 사례가 AWS 지원으로 업데이트되면 상태가 제출됨으로 변경됩니다. AWS Security Incident Response 엔지니어는 기존 사례 기록을 사용할 수 있습니다. AWS의 지원을 요청하면 다시 자체 관리형으로 변경할 수 없습니다.

작업 항목

사례를 처리하는 AWS Security Incident Response 엔지니어가 내부 팀으로부터 조치를 요청할 수 있습니다.

사례가 생성된 후 표시되는 작업 항목은 다음과 같습니다.

- 인시던트 대응 담당자가 사례에 액세스할 수 있는 권한 제공 요청
- 사례에 대한 추가 정보 제공 요청

사례를 종결할 준비가 되었을 때의 작업 항목:

- 사례 보고서 검토 요청
- 사례 종결 요청

사례 편집

사례 세부 정보를 변경하려면 편집을 선택합니다.

AWS 지원 사례 및 자체 관리형 사례의 경우:

사례가 생성된 후 다음 사례 세부 정보를 변경할 수 있습니다.

- Title
- 설명

AWS 지원 사례의 경우에만:

추가 필드를 변경할 수 있습니다.

- 요청 유형:
  - 활성 보안 인시던트: 이 유형은 긴급 인시던트 대응 지원 및 서비스를 위한 것입니다.
  - 조사: 조사를 통해 AWS Security Incident Response 엔지니어가 및 보안 이벤트의 로그 분석 및 2차 확인에서 지원할 수 있는 인지된 보안 인시던트에 대한 지원을 받을 수 있습니다.
- 추정 시작일: 이 사례에 대해 처음 제공된 시작 날짜보다 앞선 지표를 받은 경우 이 필드를 변경합니다. 설명 필드에 새로 탐지된 지표와 관련된 추가 세부 정보를 입력하거나 커뮤니케이션 탭에 설명을 추가하는 것을 고려하세요.

통신

AWS Security Incident Response 엔지니어는 사례 작업 시 활동을 문서화하기 위해 설명을 추가할 수 있습니다. 여러 AWS Security Incident Response 엔지니어가 동시에 사례에 대해 작업할 수 있습니다. 이들은 커뮤니케이션 로그 내에서 AWS 대응 담당자로 표시됩니다.

권한

권한 탭에는 사례 변경에 대해 알림을 받을 모든 개인이 나열됩니다. 사례가 종결될 때까지 목록에서 개인을 추가하고 제거할 수 있습니다.

> **Note**
>
> 개별 사례에서는 최대 30명의 이해관계자를 포함할 수 있습니다. 이러한 이해관계자에게 사례 수준 액세스 권한을 부여하려면 추가 권한 구성이 필요합니다.

콘솔에서 사례에 대한 액세스 권한 제공

AWS Management Console에서 사례에 대한 액세스를 제공하기 위해 IAM 권한 정책 템플릿을 복사하고 이 권한을 사용자 또는 역할에 추가할 수 있습니다.

사용자 또는 역할에 IAM 정책 추가:

1. IAM 권한 정책을 복사합니다.
2. IAM(https://console.aws.amazon.com/iam/)을 엽니다.
3. 탐색 창에서 사용자 또는 역할을 선택합니다.

4. 사용자나 역할을 선택하여 세부 정보 페이지를 엽니다.
5. 권한 탭에서 권한 추가를 선택합니다.
6. 정책 연결을 선택합니다.
7. 적절한 AWS 보안 인시던트 대응 관리형 정책을 선택합니다.
8. 정책 추가를 선택합니다.

첨부 파일

인시던트 대응 담당자는 다른 인시던트 대응 담당자가 자체 관리형 사례를 조사하는 데 도움이 되는 첨부 파일을 사례에 추가할 수 있습니다.

> **Note**
>
> AWS 지원 사례를 선택하면 AWS에서 첨부 파일을 볼 수 없습니다. 선호하는 커뮤니케이션 기술을 사용한 화면 공유나 사례 설명을 통해 AWS 지원 사례에 대한 모든 세부 정보를 공유해야 합니다.

컴퓨터에서 사례에 추가할 파일을 선택하려면 업로드를 선택합니다.

> **Note**
>
> 업로드된 모든 첨부 파일은 케이스가 `Closed`된 후 7일이 지나면 삭제됩니다.

Tags

태그는 해당 리소스에 대한 메타데이터를 보관하기 위해 사례에 할당할 수 있는 선택적 레이블입니다. 각 태그는 키와 값(선택 사항)으로 구성됩니다. 태그를 사용하여 리소스에 대한 권한을 검색 및 인증하고 비용을 할당할 수 있습니다.

태그를 추가하려면 다음을 수행합니다.

1. 새로운 태그 추가를 선택합니다.
2. 키에는 태그의 이름을 입력합니다.
3. 값에는 태그 값을 입력합니다.

태그를 제거하려면 태그의 제거 옵션을 선택합니다.

사례 활동

감사 추적은 모든 사례 활동에 대한 상세한 시간순 레코드를 제공합니다. 또한 이벤트 후 활동에서 중요한 정보를 제공하고 잠재적인 개선 사항을 파악하는 데 도움이 됩니다. 사례 변경의 시간, 사용자, 작업 및 세부 정보는 사례 감사 추적에 로깅됩니다.

사례 닫기

AWS 지원 사례의 경우 케이스 세부 정보 페이지에서 사례 종결을 선택하여 어떤 상태에서도 사례를 영구히 종결할 수 있습니다. 일반적으로 사례는 영구히 종결되기 전에 종결 준비 완료 상태가 됩니다. 종결 준비 완료가 아닌 다른 상태에서 사례를 중간에 종결하는 경우 AWS Security Incident Response 엔지니어가 이 AWS 지원 사례에 대한 작업을 중단하도록 요청합니다.

인시던트 대응 팀이 대응 담당자인 경우 사례 세부 정보 페이지에서 작업/사례 종결을 선택합니다.

> **Note**
>
> '종결 준비 완료' 상태는 사례가 영구히 종결될 수 있고 사례에 대해 수행할 추가 작업이 없음을 나타냅니다.

사례가 영구히 종결된 후에는 다시 열 수 없습니다. 모든 정보는 읽기 전용으로 제공됩니다. 실수로 종료되지 않도록 사례를 종료할 것인지 확인하라는 메시지가 표시됩니다.

CloudFormation StackSets 작업

> **Important**
>
> AWS 보안 인시던트 대응는 기본적으로 격리 기능을 활성화하지 않습니다. 이러한 격리 조치를 실행하려면 AWS Identity and Access Management 역할을 사용하여 서비스에 필요한 권한을 부여해야 합니다. CloudFormation StackSets를 배포하여 계정당 또는 조직 전체에 걸쳐 이러한 역할을 개별적으로 생성할 수 있습니다. StackSets가 필요한 역할을 생성합니다.

서비스 관리형 권한으로 StackSet를 생성하는 방법에 대한 구체적인 지침은 AWS CloudFormation 사용 설명서의 서비스 관리형 권한으로 CloudFormation StackSet 생성을 참조하세요.

다음은 AWSSecurityIncidentResponseContainment 및 AWSSecurityIncidentResponseContainmentExecution 역할을 생성하기 위한 템플릿입니다.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for production SIR containment roles'

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

```
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainIAMPrincipal:$DEFAULT',
                      ],
                  },
                  {
                    'Effect': 'Allow',
                    'Action':
                      ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
                    'Resource': '*',
                  },
                  {
                    'Effect': 'Allow',
                    'Action': ['iam:PassRole'],
                    'Resource': !GetAtt
 AWSSecurityIncidentResponseContainmentExecution.Arn,
                    'Condition': { 'StringEquals': { 'iam:PassedToService':
 'ssm.amazonaws.com' } },
                  },
                ],
            }
  AWSSecurityIncidentResponseContainmentExecution:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainmentExecution
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
 'Action': 'sts:AssumeRole' }],
        }
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Sid': 'AllowIAMContainment',
                    'Effect': 'Allow',
```

```
                    'Action':
                      [
                        'iam:AttachRolePolicy',
                        'iam:AttachUserPolicy',
                        'iam:DeactivateMFADevice',
                        'iam:DeleteLoginProfile',
                        'iam:DeleteRolePolicy',
                        'iam:DeleteUserPolicy',
                        'iam:GetLoginProfile',
                        'iam:GetPolicy',
                        'iam:GetRole',
                        'iam:GetRolePolicy',
                        'iam:GetUser',
                        'iam:GetUserPolicy',
                        'iam:ListAccessKeys',
                        'iam:ListAttachedRolePolicies',
                        'iam:ListAttachedUserPolicies',
                        'iam:ListMfaDevices',
                        'iam:ListPolicies',
                        'iam:ListRolePolicies',
                        'iam:ListUserPolicies',
                        'iam:ListVirtualMFADevices',
                        'iam:PutRolePolicy',
                        'iam:PutUserPolicy',
                        'iam:TagMFADevice',
                        'iam:TagPolicy',
                        'iam:TagRole',
                        'iam:TagUser',
                        'iam:UntagMFADevice',
                        'iam:UntagPolicy',
                        'iam:UntagRole',
                        'iam:UntagUser',
                        'iam:UpdateAccessKey',
                        'identitystore:CreateGroupMembership',
                        'identitystore:DeleteGroupMembership',
                        'identitystore:IsMemberInGroups',
                        'identitystore:ListUsers',
                        'identitystore:ListGroups',
                        'identitystore:ListGroupMemberships',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowOrgListAccounts',
```

```
                    'Effect': 'Allow',
                    'Action': 'organizations:ListAccounts',
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSOContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'sso:CreateAccountAssignment',
                        'sso:DeleteAccountAssignment',
                        'sso:DeleteInlinePolicyFromPermissionSet',
                        'sso:GetInlinePolicyForPermissionSet',
                        'sso:ListAccountAssignments',
                        'sso:ListInstances',
                        'sso:ListPermissionSets',
                        'sso:ListPermissionSetsProvisionedToAccount',
                        'sso:PutInlinePolicyToPermissionSet',
                        'sso:TagResource',
                        'sso:UntagResource',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSORead',
                    'Effect': 'Allow',
                    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Read',
                    'Effect': 'Allow',
                    'Action':
                      [
                        's3:GetAccountPublicAccessBlock',
                        's3:GetBucketAcl',
                        's3:GetBucketLocation',
                        's3:GetBucketOwnershipControls',
                        's3:GetBucketPolicy',
                        's3:GetBucketPolicyStatus',
                        's3:GetBucketPublicAccessBlock',
                        's3:GetBucketTagging',
                        's3:GetEncryptionConfiguration',
```

```
                'Sid': 'AllowS3Write',
                'Effect': 'Allow',
                'Action':
                  [
                    's3:CreateBucket',
                    's3:DeleteBucketPolicy',
                    's3:DeleteObjectTagging',
                    's3:PutAccountPublicAccessBlock',
                    's3:PutBucketACL',
                    's3:PutBucketOwnershipControls',
                    's3:PutBucketPolicy',
                    's3:PutBucketPublicAccessBlock',
                    's3:PutBucketTagging',
                    's3:PutBucketVersioning',
                    's3:PutObject',
                    's3:PutObjectAcl',
                    's3express:CreateSession',
                    's3express:DeleteBucketPolicy',
                    's3express:PutBucketPolicy',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowAutoScalingWrite',
                'Effect': 'Allow',
                'Action':
                  [
                    'autoscaling:CreateOrUpdateTags',
                    'autoscaling:DeleteTags',
                    'autoscaling:DescribeAutoScalingGroups',
                    'autoscaling:DescribeAutoScalingInstances',
                    'autoscaling:DescribeTags',
                    'autoscaling:EnterStandby',
                    'autoscaling:ExitStandby',
```

```
                'autoscaling:UpdateAutoScalingGroup',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowEC2Containment',
            'Effect': 'Allow',
            'Action':
              [
                'ec2:AuthorizeSecurityGroupEgress',
                'ec2:AuthorizeSecurityGroupIngress',
                'ec2:CopyImage',
                'ec2:CreateImage',
                'ec2:CreateSecurityGroup',
                'ec2:CreateSnapshot',
                'ec2:CreateTags',
                'ec2:DeleteSecurityGroup',
                'ec2:DeleteTags',
                'ec2:DescribeImages',
                'ec2:DescribeInstances',
                'ec2:DescribeSecurityGroups',
                'ec2:DescribeSnapshots',
                'ec2:DescribeTags',
                'ec2:ModifyNetworkInterfaceAttribute',
                'ec2:RevokeSecurityGroupEgress',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowKMSActions',
            'Effect': 'Allow',
            'Action':
              [
                'kms:CreateGrant',
                'kms:DescribeKey',
                'kms:GenerateDataKeyWithoutPlaintext',
                'kms:ReEncryptFrom',
                'kms:ReEncryptTo',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowSSMActions',
            'Effect': 'Allow',
```

```
                'Action': ['ssm:DescribeAutomationExecutions'],
                'Resource': '*',
            },
        ],
    }
```

멤버십 취소

AWS 보안 인시던트 대응에 대한 CancelMembership 권한이 있는 역할은 콘솔, API 또는 AWS Command Line Interface에서 멤버십을 취소할 수 있습니다.

> **Important**
>
> 멤버십이 취소되면 과거 사례 데이터를 볼 수 없습니다. 멤버십을 취소하면 멤버십이 즉시 삭제되며 멤버십의 사례에 더는 액세스할 수 없습니다. 멤버십이 취소되면 `Active` 또는 `ready to close` 상태의 모든 리소스나 조사가 종료됩니다.

멤버십을 취소하는 경우:

멤버십이 삭제되며 멤버십의 사례에 더는 액세스할 수 없습니다.

> **Important**
>
> 서비스를 구독하면 새 멤버십이 생성되며, 이전 멤버십에 속했던 사례 자료는 취소 전에 다운로드한 경우에만 액세스할 수 있습니다.

멤버십이 취소된 후에는 멤버십 인시던트 대응 팀의 모든 구성원에게 이메일로 알림이 전송됩니다.

> **Important**
>
> 위임 관리자 계정을 사용하여 멤버십을 생성한 후 AWS Organizations API를 사용하여 계정에서 위임 관리자 지정을 제거하면 멤버십이 즉시 종료됩니다.

AWS 보안 인시던트 대응 리소스에 태그 지정

태그는 사용자 또는 AWS가 AWS 리소스에 할당하는 메타데이터 레이블입니다. 각 태그는 키와 값으로 구성됩니다. 사용자가 할당하는 태그에 대해 키와 값을 정의합니다. 예를 들어 키를 `stage`로 정의하고 리소스 하나의 값을 `test`로 정의할 수 있습니다.

태그는 다음을 지원합니다.

- AWS 리소스를 식별하고 정리합니다. 많은 AWS 서비스가 태그 지정을 지원하므로 다른 서비스의 리소스에 동일한 태그를 할당하여 해당 리소스의 관련 여부를 나타낼 수 있습니다.
- AWS 비용을 추적합니다. AWS Billing 대시보드에서 이러한 태그를 활성화합니다. AWS는 태그를 사용하여 비용을 분류하고 월별 비용 할당 보고서를 전달합니다. 자세한 내용은 AWS 사용자 가이드의 Use cost allocation tags를 참조하세요.
- AWS 리소스에 대한 액세스를 제어합니다. 자세한 내용은 IAM 사용 설명서의 태그를 사용한 액세스 제어를 참조하십시오.

태깅은 AWS 보안 인시던트 대응 API Reference를 참조하세요.

AWS CloudShell을 사용하여 AWS Security Incident Response 작업 수행

AWS CloudShell은 브라우저 기반의 사전 인증된 쉘로, AWS Management Console에서 바로 시작할 수 있습니다. 원하는 쉘(Bash, PowerShell 또는 Z 쉘)을 사용하여 AWS 서비스(AWS Security Incident Response 포함)에 대해 AWS CLI 명령을 실행할 수 있습니다. 또한 명령줄 도구를 다운로드하거나 설치할 필요 없이 이 작업을 수행할 수 있습니다.

AWS Management Console에서 AWS CloudShell을 실행합니다. 그러면 콘솔에 로그인할 때 사용한 AWS 보안 인증을 새 셸 세션에서 자동으로 사용할 수 있습니다. 이러한 AWS CloudShell 사용자 사전 인증을 통해 AWS CLI 버전 2(셸의 컴퓨팅 환경에 사전 설치됨)를 사용하여 Security Incident Response와 같은 AWS 서비스와 상호 작용할 때 자격 증명 구성을 건너뛸 수 있습니다.

내용

- AWS CloudShell에 대한 IAM 권한 획득
- AWS CloudShell을 사용하여 Security Incident Response와 상호 작용

AWS CloudShell에 대한 IAM 권한 획득

관리자는 AWS Identity and Access Management에서 제공하는 액세스 관리 리소스를 사용하여 IAM 사용자에게 AWS CloudShell에 액세스하고 환경 기능을 사용할 수 있는 권한을 부여할 수 있습니다.

관리자가 사용자에게 액세스 권한을 부여하는 가장 빠른 방법은 AWS 관리형 정책을 사용하는 것입니다. AWS 관리형 정책은 AWS에서 생성 및 관리하는 독립 실행형 정책입니다. 다음과 같은 CloudShell에 대한 AWS 관리형 정책을 IAM ID에 연결할 수 있습니다.

- `AWSCloudShellFullAccess`: 모든 기능에 대한 전체 액세스 권한과 함께 AWS CloudShell을 사용할 수 있는 권한을 부여합니다.

IAM 사용자가 AWS CloudShell에서 수행할 수 있는 작업의 범위를 제한하려면 `AWSCloudShellFullAccess` 관리형 정책을 템플릿으로 사용하는 사용자 지정 정책을 생성할 수 있습니다. CloudShell에서 사용자가 사용할 수 있는 작업을 제한하는 방법에 대한 자세한 내용은 AWS CloudShell 사용 설명서의 Managing AWS CloudShell access and usage with IAM policies를 참조하세요.

> **Note**
>
> IAM ID에는 Security Incident Response에 대한 직접 호출 권한을 부여하는 정책도 필요합니다.

AWS CloudShell을 사용하여 Security Incident Response와 상호 작용

AWS Management Console에서 AWS CloudShell을 시작한 후에 명령줄 인터페이스를 사용하여 즉시 Security Incident Response와 상호 작용을 시작할 수 있습니다.

> **Note**
>
> AWS CloudShell에서 AWS Command Line Interface을 사용하는 경우 추가 리소스를 다운로드하거나 설치할 필요가 없습니다. 또한 셸 내에서 이미 인증되었기 때문에 직접 호출을 하기 전에 보안 인증을 구성하지 않아도 됩니다.

AWS CloudShell 및 Security Incident Response 작업

1. AWS Management Console에서는 탐색 표시줄에 제공되는 다음 옵션을 선택하여 CloudShell을 시작합니다.
   - CloudShell 아이콘을 선택합니다.
   - 검색 상자에 'cloudshell'을 입력하고 CloudShell 옵션을 선택합니다.
2. 표준 AWS를 사용하여 AWS Command Line Interface Security Incident Response와 상호 작용합니다. 사용 가능한 CLI 명령의 전체 참조는 AWS Security Incident Response용 AWS CLI 명령 참조를 확인하세요.

AWS CloudTrail을 사용하여 AWS Security Incident Response API 직접 호출 로깅

AWS Security Incident Response는 Security Incident Response에서 사용자, 역할 또는 AWS 서비스가 수행한 작업 기록을 제공하는 서비스인 AWS CloudTrail과 통합되어 있습니다. CloudTrail은 Security Incident Response에 대한 모든 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 직접 호출에는 Security Incident Response 콘솔에서의 직접 호출과 Security Incident Response API 작업에 대한 코드 직접 호출이 포함됩니다. 추적을 생성하면 Security Incident Response에 대한 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Security Incident Response에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Security Incident Response 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. Security Incident Response에서 활동이 발생하면, 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트 로그에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

지난 90일 동안 AWS 계정에서 진행 중인 이벤트 기록을 보려면 추적 또는 CloudTrail Lake 이벤트 데이터 스토어를 생성합니다.

CloudTrail 추적

CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. AWS Management Console을 사용하여 만든 추적은 모두 다중 리전입니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 추적을 생성할 수 있습니다. 계정의 모든 AWS 리전에서 활동을 캡처하므로, 다중 리전 추적 생성이 권장됩니다. 단일 리전 추적을 생성하는 경우 추적의 AWS 리전에 로깅된 이벤트만 볼 수 있습니다. 추적에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 Creating a trail for your AWS 계정 및 Creating a trail for an organization을 참조하세요.

CloudTrail에서 추적을 생성하여 진행 중인 관리 이벤트의 사본 하나를 Amazon S3 버킷으로 무료로 전송할 수는 있지만, Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요. Amazon S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어

CloudTrail Lake를 사용하면 이벤트에 대해 SQL 기반 쿼리를 실행할 수 있습니다. CloudTrail Lake는 행 기반 JSON 형식의 기존 이벤트를 Apache ORC 형식으로 변환합니다. ORC는 빠른 데이터 검색에 최적화된 열 기반 스토리지 형식입니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 고급 이벤트 선택기를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 이벤트 데이터 스토어에 적용하는 선택기는 어떤 이벤트가 지속되고 쿼리할 수 있는지 제어합니다. CloudTrail Lake에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 Working with AWS CloudTrail Lake를 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 비용이 발생합니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

Security Incident Response 작업은 CloudTrail에서 로깅되고 AWS Security Incident Response API 참조에 기록됩니다. 예를 들어 `CreateMembership`, `CreateCase`, `UpdateCase` 작업을 직접 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 보안 인증으로 했는지 여부입니다.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Security Incident Response 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예시에서는 CreateCase 작업이 시연되는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA00000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA00000000000000000",
                "arn": "arn:aws:iam::123412341234:role/Admin",
                "accountId": "123412341234",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-10-13T06:32:53Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-10-13T06:40:45Z",
    "eventSource": "security-ir.amazonaws.com",
    "eventName": "CreateCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/
arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#security-ir.create-case",
    "requestParameters": {
        "impactedServices": [
            "Amazon GuardDuty"
        ],
        "impactedAccounts": [],
        "clientToken": "testToken112345679",
        "resolverType": "Self",
        "description": "***",
        "engagementType": "Investigation",
        "watchers": [
            {
                "email": "***",
                "name": "***",
                "jobTitle": "***"
```

```
            }
        ],
        "membershipId": "m-r1abcdabcd",
        "title": "***",
        "impactedAwsRegions": [
            {
                "region": "ap-southeast-1"
            }
        ],
        "reportedIncidentStartDate": 1711553521,
        "threatActorIpAddresses": [
            {
                "ipAddress": "***",
                "userAgent": "browser"
            }
        ]
    },
    "responseElements": {
        "caseId": "0000000001"
    },
    "requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
    "eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123412341234",
            "type": "AWS::SecurityResponder::Case",
            "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123412341234",
    "eventCategory": "Management"
}
```

AWS Organizations를 사용하여 AWS 보안 인시던트 대응 계정 관리

AWS 보안 인시던트 대응는 AWS Organizations에 통합됩니다. 조직의 AWS Organizations 관리 계정은 AWS 보안 인시던트 대응의 위임 관리자로 계정을 지정할 수 있습니다. 이 작업을 통해 AWS Organizations에서 AWS 보안 인시던트 대응를 신뢰할 수 있는 서비스로 사용할 수 있습니다. 이러한 권한이 부여되는 방식에 대한 자세한 내용은 다른 AWS 서비스와 함께 AWS Organizations 사용을 참조하세요.

다음 섹션에서는 위임된 Security Incident Response 관리자 계정으로 수행할 수 있는 다양한 태스크를 안내합니다.

내용

AWS Organizations와 함께 AWS 보안 인시던트 대응를 사용할 때 고려 사항 및 권장 사항

다음 고려 사항 및 권장 사항은 위임된 Security Incident Response 관리자 계정이 AWS 보안 인시던트 대응에서 작동하는 방식을 이해하는 데 도움이 될 수 있습니다.

AWS 보안 인시던트 대응를 위한 위임 관리자 계정.

> 멤버 계정 하나를 위임된 Security Incident Response 관리자 계정으로 지정할 수 있습니다. 예를 들어 *##(####)*에서 멤버 계정 *111122223333*을 지정하는 경우 *###(##)*에서 다른 멤버 계정 *555555555555*을 지정할 수 없습니다. 다른 모든 리전에서는 위임된 Security Incident Response 관리자 계정과 동일한 계정을 사용해야 합니다.

특정 AWS 리전에서 위임된 Security Incident Response 관리자 계정을 설정합니다.

초기 설정 중에 하나의 AWS 리전에서 위임된 Security Incident Response 관리자 계정을 지정합니다. 설정은 리전별로 이루어지지만 AWS 보안 인시던트 대응는 지원되는 모든 AWS 리전에서 조직 전체 범위를 지원합니다. Amazon GuardDuty 및 AWS Security Hub CSPM의 보안 조사 결과는 지원되는 모든 AWS 리전에서 수집되며, 사례는 구독을 활성화한 리전에서 중앙 집중식으로 관리됩니다. 위임된 Security Incident Response 관리자 계정과 멤버 계정은 AWS Organizations를 통해 추가해야 합니다.

조직의 관리 계정을 위임된 Security Incident Response 관리자 계정으로 설정하는 것은 권장되지 않습니다.

조직의 관리 계정은 위임된 Security Incident Response 관리자 계정이 될 수 있습니다. 하지만 AWS 보안 모범 사례는 최소 권한 원칙을 따르므로 이 구성을 권장하지 않습니다.

라이브 구독에서 위임된 Security Incident Response 관리자 계정을 제거하면 구독이 즉시 취소됩니다.

위임된 Security Incident Response 관리자 계정을 제거하면 AWS 보안 인시던트 대응는 이 위임된 Security Incident Response 관리자 계정과 연결된 모든 멤버 계정을 제거합니다. AWS 보안 인시던트 대응는 모든 멤버 계정에 대해 더 이상 활성화되지 않습니다.

AWS Account Management에 대한 신뢰할 수 있는 액세스 활성화

AWS 보안 인시던트 대응에 대한 신뢰할 수 있는 액세스를 활성화하면 관리 계정의 위임 관리자가 AWS Organizations의 각 멤버 계정과 관련된 정보 및 메타데이터(예: 기본 또는 대체 연락처 세부 정보)를 수정할 수 있습니다.

다음 절차에 따라 조직의 AWS 보안 인시던트 대응에 대한 신뢰할 수 있는 액세스를 활성화합니다.

최소 권한

이 작업을 수행하려면 다음 요구 사항을 충족해야 합니다.

- 이 작업은 조직의 관리 계정에서만 수행할 수 있습니다.
- 조직의 모든 기능을 활성화해야 합니다.

Console

AWS 보안 인시던트 대응에 대한 신뢰할 수 있는 액세스를 활성화하려면 다음을 수행하세요.

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS 보안 인시던트 대응를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS 보안 인시던트 대응에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.

API/CLI

AWS Account Management에 대한 신뢰할 수 있는 액세스를 활성화하려면 다음을 수행하세요.

다음 명령을 실행한 후 조직의 관리 계정에서 자격 증명을 사용하여 `--accountId` 파라미터로 조직의 멤버 계정을 참조하는 계정 관리 API 작업을 호출할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 예에서는 직접 호출 계정의 조직에서 AWS 보안 인시던트 대응에 대한 신뢰할 수 있는 액세스를 활성화합니다.

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

  성공 시 이 명령은 출력을 생성하지 않습니다.

위임된 Security Incident Response 관리자 계정을 지정하는 데 필요한 권한

AWS Organizations에 대해 위임 관리자를 사용하여 AWS 보안 인시던트 대응 멤버십을 설정하도록 선택할 수 있습니다. 이러한 권한이 부여되는 방식에 대한 자세한 내용은 다른 AWS 서비스와 함께 AWS Organizations 사용을 참조하세요.

> **Note**
>
> AWS 보안 인시던트 대응는 설정 및 관리를 위해 콘솔을 사용할 때 AWS Organizations의 신뢰 관계를 자동으로 활성화합니다. CLI/SDK를 사용하는 경우 EnableAWSServiceAccess API를 사용하여 `security-ir.amazonaws.com`을 신뢰하도록 이를 수동으로 활성화해야 합니다.

AWS Organizations 관리자로서 조직에 대해 위임된 Security Incident Response 관리자 계정을 지정하기 전에 AWS 보안 인시던트 대응 작업인 `security-ir:CreateMembership` 및 `security-ir:UpdateMembership`을 수행할 수 있는지 확인하세요. 이러한 작업을 통해 AWS 보안 인시던트 대응를 사용하여 조직의 위임된 Security Incident Response 관리자 계정을 지정할 수 있습니다. 또한 조직에 대한 정보를 검색하는 데 도움이 되는 AWS Organizations 작업을 수행할 수 있도록 허용해야 합니다.

이러한 권한을 부여하려면 계정의 AWS Identity and Access Management(IAM) 정책에 다음 내용을 포함하세요.

```
{
    "Sid": "PermissionsForSIRAdmin",
    "Effect": "Allow",
    "Action": [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

AWS Organizations 관리 계정을 위임된 Security Incident Response 관리자 계정으로 지정하려면 계정에도 IAM 작업 `CreateServiceLinkedRole`이 필요합니다. 권한 추가를 진행하기 전에 AWS Organizations와 함께 AWS 보안 인시던트 대응를 사용할 때 고려 사항 및 권장 사항을 검토합니다.

AWS Organizations 관리 계정을 위임된 Security Incident Response 관리자 계정으로 지정하려면 IAM 정책에 다음 문을 추가하고 *111122223333*을 AWS Organizations 관리 계정의 AWS 계정 ID로 바꿉니다.

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

AWS 보안 인시던트 대응를 위한 위임 관리자 지정

이 섹션에서는 AWS 보안 인시던트 대응 조직에서 위임 관리자를 지정하는 단계를 설명합니다.

AWS 조직의 관리자로서 위임된 Security Incident Response 관리자 계정의 작동 방식에 대해 사용 고려 사항 및 권장 사항을 읽어야 합니다. 계속하기 전에 위임된 Security Incident Response 관리자 계정을 지정하는 데 필요한 권한가 있는지 확인하세요.

선호하는 액세스 방법을 선택하여 조직에 대한 위임된 Security Incident Response 관리자 계정을 지정하세요. 관리만 이 단계를 수행할 수 있습니다.

Console

1. Security Incident Response 콘솔(https://console.aws.amazon.com/security-ir/)을 엽니다.

   로그인하려면 AWS Organizations 조직의 관리 자격 증명을 사용합니다.
2. 페이지 오른쪽 상단 모서리에 있는 AWS 리전 선택기를 사용하여 조직의 위임된 Security Incident Response 관리자 계정을 지정하려는 리전을 선택합니다.
3. 설정 마법사를 따라 위임된 관리자 계정을 포함한 멤버십을 생성하세요.

API/CLI

- 조직 관리의 AWS 계정의 자격 증명을 사용하여 CreateMembership을 실행합니다.
  - 또는 AWS Command Line Interface를 사용할 수 있습니다. 다음 AWS CLI 명령은 위임된 Security Incident Response 관리자 계정을 지정합니다. 다음은 멤버십을 구성하는 데 사용할 수 있는 문자열 옵션입니다.

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

위임된 Security Incident Response 관리자 계정에서 AWS 보안 인시던트 대응가 활성화되지 않으면 어떤 작업도 할 수 없습니다. 아직 활성화하지 않았다면 새로 지정된 위임된 Security Incident Response 관리자 계정에서 AWS 보안 인시던트 대응를 활성화해야 합니다.

AWS 보안 인시던트 대응에 대한 조직 단위(OU)의 멤버십 관리

AWS 보안 인시던트 대응은(는) 개별 조직 단위(OU)에 대한 멤버십 적용 범위를 지원합니다. 언제든지 특정 OU를 포함하도록 멤버십을 업데이트할 수 있습니다. 하위 OU의 계정을 포함하여 선택한 OU 내의 모든 계정에는 멤버십이 적용됩니다.

멤버십 연결을 업데이트할 때 한 번에 최대 5개의 OU에 업데이트를 적용할 수 있습니다. 5개 이상의 OU를 변경하려면 모든 업데이트가 완료될 때까지 5개 OU의 배치로 연결 변경을 완료합니다.

Console

1. Security Incident Response 콘솔(https://console.aws.amazon.com/security-ir/)을 엽니다.

   로그인하려면 AWS Organizations 조직의 관리 자격 증명을 사용합니다.
2. 멤버십 관리 > 계정으로 이동합니다.
3. 연결 업데이트를 클릭합니다.
4. 조직 단위(OU) 선택을 선택합니다.
5. OU 추가 또는 OU 제거를 선택합니다.
6. 업데이트하려는 OU를 최대 5개 선택합니다. OU를 동시에 추가하거나 제거할 수 없습니다.

   > **Note**
   >
   > 선택한 OU 아래 모든 계정과 하위 OU가 연결됩니다.
7. 연결 업데이트를 클릭합니다.
8.

   > **Note**
   >
   > OU를 5개 이상 변경하려면 모든 OU가 연결될 때까지 5단계와 6단계를 반복합니다.

AWS 조직 내에서 OU를 변경하는 방법에 대한 자세한 내용은 AWS Organizations을(를) 사용하여 조직 단위(OU) 관리를 참조하세요.

AWS 보안 인시던트 대응에 멤버 추가

AWS Organizations와 AWS 보안 인시던트 대응 멤버십은 일대일 관계입니다. 조직 또는 조직 단위(OU)에 계정이 추가되거나 제거되면 이러한 변경 내용이 AWS 보안 인시던트 대응 멤버십의 적용 대상 계정에 반영됩니다.

멤버십에 계정을 추가하려면 AWS Organizations로 조직 내 계정 관리 옵션 중 하나를 따르세요.

언제든지 멤버십에 OU를 추가할 수도 있습니다. 조직 단위(OU)의 멤버십 관리를 참조하세요.

AWS 보안 인시던트 대응에서 멤버 제거

멤버십에서 계정을 제거하려면 조직에서 멤버 계정을 제거하거나, 선택한 OU 외부로 계정을 이동하거나, 멤버십에서 OU를 제거하면 됩니다.

멤버십에서 계정을 제거하려면 조직에서 멤버 계정 제거 절차를 따르세요.

계정을 OU 외부로 이동하려면 AWS Organizations을(를) 사용하여 계정을 조직 단위(OU)로 이동 또는 루트와 OU 간에 이동 절차를 따릅니다.

멤버십에서 OU를 제거하려면 조직 단위(OU)로 멤버십 관리 절차를 따릅니다.

Amazon EventBridge

Amazon EventBridge를 사용하면 AWS 보안 인시던트 대응 사례 및 멤버십과 관련된 이벤트에 대응하고, 모니터링하고, 오케스트레이션할 수 있습니다. 이러한 이벤트를 규칙(하나 이상의 대상에 대한 팬아웃 시나리오의 경우)을 통해 라우팅하거나 파이프(향상된 필터링, 강화 및 변환 기능을 갖춘 포인트 투 포인트 통합의 경우)를 통해 라우팅할 수 있습니다.

Security Incident Response와 타사 도구 간의 통합을 생성하거나 생성형 AI와 기타 AWS 도구를 사용하여 분석할 데이터를 집계할 수 있습니다. 예를 들어 Security Incident Response에서 사전에 사례를 생성하는 경우 EventBridge 자동화를 사용하여 이해관계자에게 알리도록 시스템을 트리거할 수 있습니다. 또한 여러 AWS 환경을 관리하는 경우 Amazon EventBridge 통합을 사용해서 AWS 보안 인시던트 대응 멤버십을 모니터링하여 모든 환경이 강력한 보안 태세를 유지하도록 할 수 있습니다.

자세한 내용은 What is Amazon EventBridge?를 참조하세요.

> **Note**
>
> ITSM 통합을 포함하여 AWS 보안 인시던트 대응와의 Amazon EventBridge 통합에 대한 최신 업데이트는 AWS의 새로운 기능 페이지에서 AWS Security Incident Response, ITSM과의 통합 기능 도입 섹션을 참조하세요.

내용

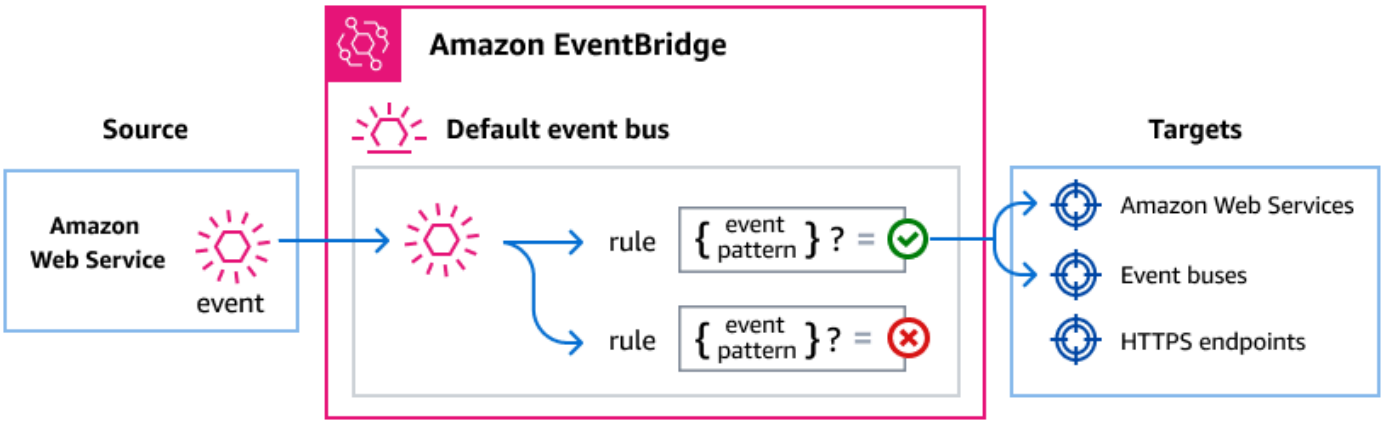
- Amazon EventBridge를 사용하여 Security Incident Response 이벤트 관리
- AWS 보안 인시던트 대응 이벤트 사용
- 자습서: Membership Updated 이벤트에 대한 Amazon Simple Notification Service 알림 전송

Amazon EventBridge를 사용하여 Security Incident Response 이벤트 관리

Amazon EventBridge는 이벤트를 사용하여 애플리케이션 구성 요소를 서로 연결하는 서버리스 서비스로, 확장 가능한 이벤트 기반 애플리케이션을 더 쉽게 구축할 수 있습니다. 이벤트 기반 아키텍처는 이벤트를 내보내고 이에 응답하여 함께 작동하는 느슨하게 결합된 소프트웨어 시스템을 구축하는 스타일입니다. 이벤트는 리소스나 환경의 변화를 나타냅니다.

작동 방식은 다음과 같습니다.

많은 AWS 서비스와 마찬가지로 Security Incident Response는 이벤트를 생성하여 EventBridge 기본 이벤트 버스로 전송합니다. (AWS 계정에서 기본 이벤트 버스는 자동으로 프로비저닝됩니다.) 이벤트 버스는 이벤트를 수신하여 0개 이상의 목적지 또는 대상에 전달하는 라우터입니다. 이벤트 버스에 대해 지정한 규칙은 이벤트가 도착할 때 이벤트를 평가합니다. 각 규칙은 이벤트가 규칙의 이벤트 패턴과 일치하는지 여부를 확인합니다. 이벤트가 일치하면 이벤트 버스는 이벤트를 지정된 대상에게 전송합니다.



EventBridge 규칙을 사용하여 Security Incident Response 이벤트 제공

EventBridge 기본 이벤트 버스가 Security Incident Response 이벤트를 대상으로 전송하도록 하려면 규칙을 생성해야 합니다. 각 규칙에는 이벤트 버스에서 수신된 각 이벤트와 일치하는 EventBridge 패턴이 포함되어 있습니다. 이벤트 데이터가 지정된 이벤트 패턴과 일치하면 EventBridge는 해당 이벤트를 규칙의 대상으로 보냅니다.

이벤트 버스 규칙 생성에 대한 포괄적인 지침은 Amazon EventBridge 사용 설명서의 Creating rules that react to events를 참조하세요.

Security Incident Response 이벤트와 일치하는 이벤트 패턴 생성

각 이벤트 패턴은 다음을 포함하는 JSON 객체입니다.

- 이벤트를 전송하는 서비스를 식별하는 `source` 속성입니다. Security Incident Response 이벤트의 경우 소스는 `"aws.security-ir"`입니다.
- (선택 사항): 일치시킬 이벤트 유형의 배열을 포함하는 `detail-type` 속성입니다.
- (선택 사항): 일치시킬 다른 이벤트 데이터를 포함하는 `detail` 속성입니다.

예를 들어, 다음 이벤트 패턴은 지정된 AWS 계정에 대한 모든 `Case Updated by AWS ## #### ## Service` 이벤트와 일치합니다.

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

이벤트 작성에 대한 자세한 내용은 EventBridge 사용 설명서의 이벤트 패턴을 참조하세요.

Security Incident Response 이벤트 세부 정보 참조

AWS 서비스의 모든 이벤트에는 이벤트의 소스인 AWS 서비스, 이벤트가 생성된 시간, 이벤트가 발생한 계정 및 리전 등과 같은 이벤트에 대한 메타데이터를 포함하는 공통 필드 집합이 있습니다. 이러한 일반 필드에 대한 정의는 Amazon EventBridge 사용 설명서의 이벤트 구조 참조를 참조하세요.

또한 각 이벤트에는 해당 특정 이벤트와 관련된 데이터를 포함하는 `detail` 필드가 있습니다. 다음 참조는 다양한 Security Incident Response 이벤트에 대한 세부 정보 필드를 정의합니다.

EventBridge를 사용하여 Security Incident Response 이벤트를 선택하고 관리할 때는 다음 사항을 염두에 두는 것이 유용합니다.

- Security Incident Response의 모든 이벤트에 대한 `source` 필드는 `"aws.security-ir"`로 설정됩니다.
- `detail-type` 필드는 이벤트 유형을 지정합니다.

  예를 들어 `"Case Updated"`입니다.

- `detail` 필드는 해당 특정 이벤트와 관련된 데이터를 포함합니다.

Security Incident Response 이벤트와 일치하는 규칙을 활성화하는 이벤트 패턴을 구성하는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 Event patterns를 참조하세요.

이벤트 및 EventBridge가 이벤트를 처리하는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 EventBridge 이벤트를 참조하세요.

공통 필드: 모든 AWS 보안 인시던트 대응 이벤트에는 이러한 표준 Amazon EventBridge 필드가 포함됩니다.

- version: EventBridge 이벤트 형식 버전
- id: 이벤트의 고유 식별자
- detail-type: 사람이 읽을 수 있는 이벤트 유형 설명
- source: Security Incident Response 이벤트의 경우 항상 'aws.security-ir'
- 계정: 이벤트가 발생한 AWS 계정 ID입니다.
- 타임 – 이벤트가 발생한 시점의 ISO 8601 타임스탬프입니다.
- 리소스: 리소스가 존재하는 AWS 리전입니다.
- resources: 영향을 받는 리소스의 ARN이 포함된 배열

세부 정보 필드: `detail` 객체에는 Security Incident Response 관련 정보가 포함됩니다.

- caseId: 사례의 고유 식별자(사례 이벤트만 해당)
- membershipId: 멤버십의 고유 식별자(멤버십 이벤트만 해당)
- updatedBy: 업데이트를 수행한 사람(사례 및 설명 업데이트 이벤트만 해당)
- createdBy: 엔터티를 생성한 사람(사례 및 설명 생성 이벤트만 해당)

행위자 값: `updatedBy` 및 `createdBy` 필드에는 다음이 포함될 수 있습니다.

- AWS Responder: AWS 보안 대응 담당자가 수행하는 작업
- *`security-ir.amazonaws.com`*: 서비스에서 자동으로 수행하는 작업
- Account ID: 고객이 수행하는 작업(예: '111122223333')

리소스 ARN 값: AWS 보안 인시던트 대응 리소스는 다음 ARN 형식을 사용합니다.

- 사례: `arn:aws:security-ir:{region}:{account-id}:case/{case-id}`
- 멤버십: `arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`

사례 이벤트

AWS 대응 담당자가 생성한 사례

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

서비스가 생성한 사례

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

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

고객이 생성한 사례

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

AWS 대응 담당자가 업데이트한 사례

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

```
    "updatedBy": "AWS Responder"
  }
}
```

AWS 고객이 업데이트한 사례

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

AWS 보안 인시던트 대응 서비스가 업데이트한 사례

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

```
  }
}
```

종결된 사례

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

사례 설명 이벤트

AWS 대응 담당자가 생성한 사례 설명

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

```
  }
}
```

고객이 생성한 사례 설명

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

AWS 보안 인시던트 대응 서비스가 생성한 사례 설명

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

```
}
```

고객이 업데이트한 사례 설명

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

AWS 보안 인시던트 대응 서비스가 업데이트한 사례 설명

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

AWS 대응 담당자가 생성한 사례 설명

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

멤버십 이벤트

멤버십 생성됨

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

```
            }
```

멤버십 업데이트됨

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

취소된 멤버십

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

종료된 멤버십

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Terminated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-07-01T00:00:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-123456s7890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

AWS 보안 인시던트 대응 이벤트 사용

이러한 이벤트와 일치시키고 자동화된 작업을 트리거하는 EventBridge 규칙을 생성할 수 있습니다. 몇 가지 사용 사례가 아래에 예시되어 있습니다.

모든 AWS 보안 인시던트 대응 이벤트와 일치:

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

사례 이벤트만 일치:

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

```
            "Case Created",
            "Case Updated",
            "Case Closed",
            "Case Comment Added",
            "Case Comment Updated"
        ]
    }
```

AWS 대응 담당자가 업데이트한 사례 일치:

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

특정 사례에 대한 이벤트 일치:

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

자습서: **Membership Updated** 이벤트에 대한 Amazon Simple Notification Service 알림 전송

이 자습서에서는 구독이 `Membership Updated` 상태가 되는 이벤트만 캡처하는 Amazon EventBridge 이벤트 규칙을 구성합니다.

사전 조건

이 자습서에서는 멤버십에 유효한 구독과 활성 AWS 계정이 있다고 가정합니다.

주제

자습서: Amazon SNS 주제 생성 및 구독

본 자습서를 위해 새 이벤트 규칙의 이벤트 대상으로 사용할 Amazon SNS 주제를 구성합니다.

Amazon SNS 주제를 생성하려면

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 주제(Topics), 주제 생성(Create topic)을 차례로 선택합니다.
3. 유형에서 표준을 선택합니다.
4. 주제 이름에 **`MembershipUpdated`**(을)를 입력하고 주제 생성을 선택합니다.
5. MembershipUpdated 화면에서 구독 생성을 선택합니다.
6. 프로토콜(Protocol)에서 이메일(Email)을 선택합니다.
7. 엔드포인트(Endpoint)에 현재 액세스 권한이 있는 이메일 주소를 입력하고 구독 생성(Create subscription)을 선택합니다.
8. 이메일 계정을 확인하고 구독 확인 이메일 메시지를 기다립니다. 메시지를 수신하면 구독 확인(Confirm subscription)을 선택합니다.

자습서: 이벤트 규칙 등록

다음으로 `Membership Updated` 이벤트만 캡처하는 이벤트 규칙을 등록합니다.

EventBridge 규칙을 등록하려면

1. https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택합니다.
3. 규칙 생성을 선택합니다.
4. 규칙에 대해 이름과 설명을 입력하세요.

> **Note**
>
> 규칙은 동일한 리전과 동일한 이벤트 버스의 다른 규칙과 동일한 이름을 가질 수 없습니다.

5. 이벤트 버스에서 이 규칙과 연결할 이벤트 버스를 선택합니다. 이 규칙이 자신의 계정에서 발생하는 이벤트와 일치하도록 하려면 AWS 기본 이벤트 버스(default event bus)를 선택합니다. 계정의 AWS 서비스가 이벤트를 출력하면 항상 계정의 기본 이벤트 버스로 이동합니다.

> **Note**
>
> AWS Organizations 멤버십을 생성한 AWS 보안 인시던트 대응 또는 위임 관리자 계정에서 이를 설정해야 합니다.

6. 규칙 유형(Rule type)에서 이벤트 패턴이 있는 규칙(Rule with an event pattern)을 생성합니다.
7. 다음을 선택합니다.
8. 이벤트 소스에서 기타를 선택합니다.
9. 이벤트 패턴에서 사용자 지정 패턴(JSON 편집기)을 선택합니다.
10. 다음 이벤트 패턴을 텍스트 영역에 붙여 넣습니다.

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

이 코드는 서비스 멤버십이 업데이트되거나 수정된 모든 이벤트와 일치하는 EventBridge 규칙을 정의합니다. 이벤트 패턴에 대한 자세한 내용은 Amazon EventBridge 사용 설명서에서 이벤트 및 이벤트 패턴을 참조하세요.

11. 다음을 선택합니다.
12. 대상 유형에서 AWS서비스를 선택합니다.
13. 대상 선택에서 SNS 주제를 선택하고, 주제에 대해 MembershipUpdated를 선택합니다.
14. (선택 사항)추가 설정에서 다음을 수행합니다.

a. 최대 이벤트 기간(Maximum age of event)에 1분(00:01)에서 24시간(24:00) 사이의 값을 입력합니다.

b. 재시도(Retry attempts)에 0에서 185 사이의 숫자를 입력합니다.

c. 배달 못한 편지 대기열(Dead-letter queue)에서 표준 Amazon SQS 대기열을 배달 못한 편지 대기열로 사용할지를 선택합니다. 이벤트가 대상에 성공적으로 전달되지 않은 경우 EventBridge는 이 규칙과 일치하는 이벤트를 배달 못한 편지 대기열로 보냅니다. 다음 중 하나를 수행합니다.

- 배달 못한 편지 대기열을 사용하지 않으려면 없음(None)을 선택합니다.
- 현재 AWS 계정에서 DLQ(Dead Letter Queue)로 사용할 Amazon SQS 대기열 선택(Select an Amazon SQS queue in the current account to use as the dead-letter queue)을 선택하고 드롭다운에서 사용할 대기열을 선택합니다.
- 다른 AWS 계정에서 배달 못한 편지 대기열로 사용할 Amazon SQS 대기열 선택을 선택한 다음, 사용할 대기열의 ARN을 입력합니다. 메시지를 보낼 수 있는 EventBridge 권한을 부여하는 리소스 기반 정책을 대기열에 연결해야 합니다. 자세한 정보는 Amazon EventBridge 사용 설명서의 DLQ(Dead Letter Queue)에 대한 권한 부여를 참조하세요.

15. 다음을 선택합니다.
16. (선택 사항)규칙에 대해 하나 이상의 태그를 입력하세요. 자세한 정보는 Amazon EventBridge 사용 설명서의 Amazon EventBridge 태그를 참조하세요.
17. 다음을 선택합니다.
18. 규칙의 세부 정보를 검토하고 규칙 생성을 선택합니다.

자습서: 규칙 테스트

규칙을 테스트하려면 AWS 보안 인시던트 대응 멤버십에 대한 업데이트를 제출하세요. 규칙이 올바로 구성되었다면 몇 분 후에 이벤트 텍스트가 포함된 이메일 메시지를 수신할 것입니다.

대체 규칙: Security Incident Response 사례 업데이트

모든 사례 업데이트를 모니터링하는 이벤트 규칙을 생성하려면 다음과 같이 변경하여 이 자습서를 반복합니다.

1. 자습서: Amazon SNS 주제 생성 및 구독에서 *CaseUpdates*를 주제 이름으로 사용합니다.
2. 자습서: 이벤트 규칙 등록에서 JSON 편집기에서 다음 패턴을 사용합니다.

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

문제 해결

AWS 보안 인시던트 대응과 관련된 작업을 수행하는 데 문제가 있는 경우 이 섹션의 주제를 참조하세요.

ERROR는 일부 또는 모든 작업에 결함이 있음을 나타내는 작업 상태입니다. 또는 문제가 발생해도 태스크가 완료되는 경우 경고를 받습니다.

내용

문제

올바른 컨텍스트에서 요청을 전송하지 않음

AWS 보안 인시던트 대응 API에 대한 모든 직접 호출은 서비스 위임 관리자 또는 멤버십 계정의 IAM 위탁자가 시작해야 합니다. 조직의 AWS 보안 인시던트 대응 위임 관리자 또는 멤버십 계정인 AWS 계정에서 올바른 IAM 위탁자로 운영하고 있는지 확인하세요.

오류

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

AWS 관리자와 협력하여 AWS 보안 인시던트 대응 위임 관리자 또는 멤버십 계정에서 IAM 역할을 수임할 수 있는 권한이 있는지 확인하세요. 또한 역할에 요청된 작업을 허용하는 IAM 정책이 있는지도 확인하세요. 자세한 내용은 AWS 보안 인시던트 대응 IAM을 참조하세요.

ConflictException

요청으로 인해 일관되지 않은 상태가 발생합니다.

지정한 사례 첨부 파일 이름이나 기본 대응 팀원이 고유한지 확인하세요. AWS 보안 인시던트 대응 서비스 멤버십이 아직 구성되지 않았는지도 확인하세요. https://console.aws.amazon.com/security-ir/에서 Security Incident Response 콘솔을 열고 `Membership Details`로 이동합니다.

InternalServerException

요청을 처리하는 동안 예상치 못한 오류가 발생했습니다. 몇 분 후에 다시 시도하세요. 문제가 지속되면 지원에 사례를 제출합니다.

ResourceNotFoundException

요청이 존재하지 않는 리소스를 참조합니다.

요청에 지정된 하나 이상의 리소스가 존재하지 않습니다. 제공된 모든 리소스 ARN 또는 ID가 올바른지 확인하세요. 이는 AWS Organizations ID, 계정 ID, IAM 역할, 멤버십, 사례, 대응 팀원, 사례, 사례 대응 담당자, 사례 첨부 파일 및 사례 설명에 적용됩니다.

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

지정된 기간 동안 IAM 위탁자가 해당 API 함수에 너무 많은 요청을 했습니다. 잠시 기다렸다가 다시 시도하세요. 문제가 지속되면 지수 백오프 및 재시도 알고리즘 구현을 고려하세요.

ValidationException

입력이 AWS 서비스에서 지정한 제약 조건을 충족하지 못합니다.

요청의 하나 이상의 데이터 필드가 검증 및/또는 논리적 조합 요구 사항을 충족하지 않았습니다. 모든 리소스 ARN이 완전한지, 텍스트 값이 AWS 보안 인시던트 대응 API Reference 가이드의 크기 및 형식 제약 조건을 충족하는지 확인하세요. 또한 값 업데이트가 허용되는지 확인합니다. 예를 들어AWS 지원에서 자체 관리형으로 사례를 변경하는 것은 불가능합니다.

지원

추가 지원이 필요하면 문제 해결을 위해 지원 센터에 문의하세요. 다음 정보를 준비하세요.

- 사용한 AWS 리전
- 멤버십의 AWS 계정 ID
- 소스 콘텐츠(해당 시 및 가용할 경우)
- 문제 해결에 도움이 될 수 있는 문제에 대한 기타 세부 정보

보안

내용

AWS 보안 인시던트 대응의 데이터 보호

내용

AWS 공동 책임 모델은 AWS Security Incident Response 서비스의 데이터 보호에 적용됩니다. 이 모델에서 설명하는 것처럼 AWS는 AWS 클라우드에서 제공되는 서비스를 실행하는 인프라를 보호할 책임이 있습니다. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS Security Blog의 AWS Shared Responsibility Model and GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 보안 모범 사례에서는 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center 또는 AWS Identity and Access Management(IAM)를 사용하여 개별 사용자를 설정해야 한다고

명시되어 있습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS리소스와 통신하세요. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- AWS CloudTrail로 API 및 사용자 활동 로깅을 설정합니다.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용합니다.
- FIPS 140-3은 현재 서비스에서 지원되지 않습니다.

이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하면 안 됩니다. 여기에는 AWS Support 또는 기타 AWS 서비스에서 콘솔, API, AWS CLI 또는 AWS SDK를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드를 입력하는 모든 데이터는 결제 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

데이터 암호화

내용

저장 시 암호화

저장 데이터는 투명 서버 측 암호화를 사용하여 암호화됩니다. 이를 사용하면 중요한 데이터 보호와 관련된 운영 부담 및 복잡성을 줄일 수 있습니다. 유휴 시 암호화를 사용하면 암호화 규정 준수 및 규제 요구 사항이 필요한, 보안에 민감한 애플리케이션을 구축할 수 있습니다.

전송 중 암호화

AWS 보안 인시던트 대응가 수집 및 액세스하는 데이터는 Transport Layer Security(TLS) 보호 채널을 통해서만 수집 및 액세스됩니다.

키 관리

AWS 보안 인시던트 대응는 AWS KMS와의 통합을 구현하여 사례와 첨부 파일 데이터에 대한 저장 암호화를 제공합니다.

AWS 보안 인시던트 대응는 고객 관리형 키를 지원하지 않습니다.

인터네트워크 트래픽 개인 정보 보호

서비스와 온프레미스 클라이언트 및 애플리케이션 간의 트래픽

프라이빗 네트워크와 AWS 사이에 두 연결 옵션이 있습니다.

- AWS Site-to-Site VPN 연결. 자세한 정보는 AWS Site-to-Site VPN 사용 설명서의 AWS Site-to-Site VPN란 무엇입니까? 단원을 참조하세요.
- Direct Connect 연결. 자세한 내용은 Direct Connect 사용 설명서의 Direct Connect란 무엇입니까?를 참조하세요.

네트워크를 통한 AWS 보안 인시던트 대응 액세스는 AWS에서 게시한 API를 통해 이루어집니다. 클라이언트가 Transport Layer Security(TLS) 1.2를 지원해야 합니다. TLS 1.3을 권장합니다. 클라이언트는 DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Diffie-Hellman Ephemeral)와 같은 PFS(전달 완전 보안)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다. 또한, 액세스 키 ID와 IAM 보안 주체와 관련된 비밀 액세스 키를 사용하여 요청에 서명하거나 AWS Security Token Service(STS)를 사용하여 요청에 서명할 수 있는 임시 보안 자격 증명을 생성할 수 있습니다.

같은 리전에 있는 AWS 리소스 사이의 트래픽

AWS 보안 인시던트 대응용 Amazon Virtual Private Cloud(Amazon VPC) 엔드포인트는 VPC 내의 논리적 엔터티로서, AWS 보안 인시던트 대응에만 연결을 허용합니다. Amazon VPC는 AWS 보안 인시던트 대응로 요청을 라우팅하고, 대응을 다시 VPC로 라우팅합니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 참조하세요. VPC 엔드포인트의 액세스 제어에 사용할 수 있는 정책의 예는 IAM 정책을 사용하여 DynamoDB에 대한 액세스 제어를 참조하세요.

> **Note**
>
> Amazon VPC 엔드포인트는 AWS Site-to-Site VPN 또는 Direct Connect를 통해 액세스할 수 없습니다.

자격 증명 및 액세스 관리

AWS Identity and Access Management(IAM)는 AWS 리소스에 대한 관리자의 액세스를 제어하는 데 도움이 되는 AWS 서비스입니다. IAM 관리자는 인증(로그인)된 위탁자와 승인(권한 있음)된 위탁자가 AWS 보안 인시던트 대응 리소스를 사용하도록 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

내용

대상

AWS Identity and Access Management(IAM)을 사용하는 방법은 AWS 보안 인시던트 대응에서 수행하는 작업에 따라 달라집니다.

보안 관리자

이러한 사용자에게 멤버십 및 사례 리소스에 대한 읽기 및 쓰기 액세스 권한이 있는지 확인하기 위해 AWSSecurityIncidentResponseFullAccess 관리형 정책을 사용하는 것이 좋습니다.

사례 감시자

이러한 개인은 사용자가 명시적으로 권한을 부여한 개별 사례를 제외한 모든 사례에 액세스할 수 있는 권한이 없습니다.

인시던트 대응 팀원

팀원에게 전체 멤버십과 사례 액세스 권한을 모두 부여할 수 있습니다. 모든 개인이 서비스 멤버십에 대한 권한 있는 조치를 취할 필요는 없지만 서비스를 통해 생성되고 관리되는 모든 사례에 대한 액세스 권한이 있어야 합니다. 자세한 내용은 AWS 보안 인시던트 대응 관리형 정책을 참조하세요.

ID를 통한 인증

인증은 ID 자격 증명을 사용하여 AWS에 로그인하는 방식입니다. AWS 계정 루트 사용자나 IAM 사용자로 또는 IAM 역할을 수임하여 인증(AWS에 로그인)되어야 합니다.

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 AWS에 로그인할 수 있습니다. AWS IAM Identity Center 사용자, 회사의 통합 인증, Google 또는 Facebook 자격 증명은 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS에 액세스하면 간접적으로 역할을 수임합니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. AWS 로그인에 대한 자세한 내용은 AWS 로그인 사용자 가이드의 AWS 계정에 로그인하는 방법을 참조하세요.

AWS에 프로그래밍 방식으로 액세스하는 경우, AWS에서는 보안 인증 정보를 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK) 및 명령줄 인터페이스(CLI)를 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청에 서명을 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS는 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용자 가이드의 다중 인증과 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

AWS 계정을 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 ID로 시작합니다. 이 ID는 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 태스크에 루트 사용자를 사용하지 말고 루트 사용자 자격 증명을 보호하기 위한 조치를 취하세요. 루트 사용자만 수행할 수 있는 태스크를 수행하는 데만 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 ID

임시 자격 증명을 사용하여 ID 제공업체와 페더레이션을 통해 AWS 서비스에 액세스하도록 관리자 액세스 권한이 필요한 사용자를 포함한 인간 사용자에게 요구하는 것이 가장 좋습니다.

페더레이션 ID는 엔터프라이즈 사용자 디렉터리, 웹 ID 제공업체, AWS Directory Service, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스에 액세스하는 모든 사용자입니다. 페더레이션 ID는 AWS 계정에 액세스할 때 역할을 수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 AWS 계정 및 애플리케이션에서 사용하기 위해 고유한 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가지고 있는 AWS 계정 내 ID입니다. 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용

하는 것이 좋습니다. IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 자격 증명이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 ID입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가지고 있는 AWS 계정 내 ID입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 전환하여 AWS Management Console에서 IAM 역할을 임시로 수임할 수 있습니다. AWS CLI 또는 AWS API 작업을 직접 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 만들기를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 교차 계정 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스를 사용하면 역할을 (프록시로 사용하는 대신) 리소스에 정책을 직접 연결할 수 있습니다. 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 – 일부 AWS 서비스는 다른 AWS 서비스의 기능을 사용합니다. 예를 들어 서비스에서 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나

Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.

  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할 – 서비스 연결 역할은 AWS 서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 태스크를 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행 중인 애플리케이션 – IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 해당 역할을 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

AWS 보안 인시던트 대응에서 IAM을 사용하는 방식

AWS Identity and Access Management(IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 지원하는 AWS 서비스입니다. IAM 관리자는 어떤 사용자가 AWS 보안 인시던트 대응 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

AWS 보안 인시던트 대응에서 사용할 수 있는 IAM 기능	
IAM 기능	서비스 정렬
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예

AWS 보안 인시던트 대응에서 사용할 수 있는 IAM 기능	
정책 조건 키	예(글로벌)
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	아니요
서비스 연결 역할	예

내용

- AWS 보안 인시던트 대응에 대한 ID 기반 정책
- AWS 보안 인시던트 대응 정책 조건 키
- AWS 보안 인시던트 대응의 ACL(액세스 제어 목록)

AWS 보안 인시던트 대응에 대한 ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

내용

- ID 기반 정책 예시
- 정책 모범 사례
- AWS 보안 인시던트 대응 콘솔 사용

- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 리소스 기반 정책
- 정책 작업

ID 기반 정책 예시

기본적으로 사용자 및 역할에는 AWS 보안 인시던트 대응 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface(AWS CLI) 또는 AWS API를 사용해 태스크를 수행할 수 없습니다. IAM 관리자는 사용자에게 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하는 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 AWS Security Incident Response에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS 보안 인시던트 대응에 대한 작업, 리소스 및 조건 키를 참조하세요.

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 AWS 보안 인시던트 대응 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

AWS 관리형 정책으로 시작하고 최소 권한을 향해 나아가기 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS관리형 정책을 사용합니다. AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS직무에 대한 관리형 정책을 참조하세요.

최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.

IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS CloudFormation와 같이, 특정 AWS 서비스를 통해 사용되는 경우에

만 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.

다중 인증(MFA) 필요 – AWS 계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우, 추가 보안을 위해 MFA를 설정합니다. API 작업을 직접적으로 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

AWS 보안 인시던트 대응 콘솔 사용

https://console.aws.amazon.com/security-ir/에 액세스하려면 최소한의 권한 집합이 있어야 합니다. 이러한 권한은 AWS 계정에서 AWS 보안 인시던트 대응 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

AWS 보안 인시던트 대응 액세스 또는 읽기 전용 AWS 관리형 정책을 연결하여 사용자와 역할이 서비스 콘솔을 사용할 수 있도록 합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI나 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

리소스 기반 정책

AWS Security Incident Response 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자

는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연합된 사용자 또는 AWS 서비스가 포함될 수 있습니다.

자세한 내용은 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

정책 작업

AWS 보안 인시던트 대응를 위한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 일반적으로 정책 작업의 이름은 연결된 AWSAPI 작업의 이름과 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AWS 보안 인시던트 대응 작업 목록을 보려면 서비스 권한 부여 참조의 AWS 보안 인시던트 대응에서 정의한 작업을 참조하세요.

AWS 보안 인시던트 대응의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

AWS 보안 인시던트 대응 -ID

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

"Action": ["AWS 보안 인시던트 대응 -identity:action1", "AWS 보안 인시던트 대응 -identity:action2"]

Amazon AWS Security Incident Response를 위한 정책 리소스

정책 리소스 지원: 예 관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 명령문에는 Resource 또는 NotResource 요소가 포함되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하

여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

"Resource": "*"

AWS 보안 인시던트 대응 정책 조건 키

서비스별 정책 조건 키 지원: 아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소(또는 Condition 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. Condition 요소는 선택 사항입니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 조건 요소를 지정하거나 단일 조건 요소에서 여러 키를 지정하는 경우, AWS는 논리적 AND 태스크를 사용함으로써 평가합니다. 단일 조건 키의 여러 값을 지정하는 경우 AWS는 논리적 OR 태스크를 사용함으로써 조건을 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

AWS 보안 인시던트 대응의 ACL(액세스 제어 목록)

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

AWS Security Incident Response의 속성 기반 액세스 제어(ABAC)

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 엔티티(사용자 또는 역할) 및 많은 AWS리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다. ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 AWS:ResourceTag/key-name, AWS:RequestTag/key-name 또는 AWS:TagKeys 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다. 서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다. ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇입니까?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

AWS 보안 인시던트 대응의 임시 자격 증명

임시 자격 증명 지원: 예

AWS 서비스는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 작동하는 AWS 서비스를 비롯한 추가 정보는 IAM 사용 설명서의 IAM으로 작업하는 AWS 서비스를 참조하세요. 사용자 이름과 암호를 제외한 다른 방법을 사용하여 AWS에 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어, 회사의 Single Sign-On(SSO) 링크를 사용하여 AWS에 액세스하면 해당 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 AWS에 액세스할 수 있습니다. AWS에서는 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

AWS 보안 인시던트 대응에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 위탁자로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 주체의 권한을 요청하는 AWS 서비스와 결합하여 다운스트림 서비스에 요청합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 경우에만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS 보안 인시던트 대응 ID 및 액세스 문제 해결

다음 정보를 사용하여 AWS Security Incident Response 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음
- 내 AWS 계정 외부의 사람이 내 AWS 보안 인시던트 대응 리소스에 액세스할 수 있게 허용하려고 함

작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예시 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상의 my-example-widget 리소스에 대한 세부 정보를 보려고 하지만 가상의 AWS Security Incident Response :GetWidget 권한이 없는 경우 발생합니다.

리소스 my-example-widget에 대해 AWS 보안 인시던트 대응 :GetWidget을 수행할 권한이 사용자 arn:AWS:iam::123456789012:user/mateojackson에 없습니다.

이 경우 AWS 보안 인시던트 대응 :GetWidget 작업을 사용하여 my-example-widget 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행할 권한이 없음 iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS 보안 인시던트 대응에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신, 해당 서비스에 기존 역할을 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예시 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 AWS Security Incident Response에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

iam:PassRole을 수행할 권한이 사용자 AWS:iam::123456789012:user/marymajor에 없습니다.

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다. 도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사람이 내 AWS 보안 인시던트 대응 리소스에 액세스할 수 있게 허용하기를 원합니다

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- Amazon AWS 보안 인시던트 대응에서 이러한 기능을 지원하는지 알아보려면 AWS Security Incident Response가 IAM과 함께 작동하는 방식을 참조하세요.
- 소유하고 있는 AWS 계정의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공을 참조하세요.
- 리소스에 대한 액세스 권한을 서드 파티 AWS 계정에게 제공하는 방법을 알아보려면 IAM 사용 설명서의 서드 파티가 소유한 AWS 계정에 대한 액세스 제공을참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

서비스 역할 사용

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS서비스에 대한 권한을 위임할 역할 생성을 참조하세요.

서비스 연결 역할 사용

AWS 보안 인시던트 대응에 대한 서비스 연결 역할

내용

- AWS SLR: AWSServiceRoleForSecurityIncidentResponse
- AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage

- AWS 보안 인시던트 대응 서비스 연결 역할이 지원되는 리전

서비스 연결 역할 지원: 예

서비스 연결 역할은 AWS서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS계정에 나타나고, 서비스가 소유합니다. AWS Identity and Access Management 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할을 통해 AWS 보안 인시던트 대응 설정이 쉬워지는데 필요한 권한을 수동으로 추가할 필요가 없기 때문입니다. AWS 보안 인시던트 대응에서 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 AWS 보안 인시던트 대응에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse

AWS 보안 인시던트 대응는 AWSServiceRoleForSecurityIncidentResponse라는 서비스 연결 역할(SLR) - AWS 보안 인시던트 대응 정책을 사용하여 가입된 계정을 식별하고, 사례를 생성하고, 관련 리소스에 태그를 지정합니다.

권한

AWSServiceRoleForNetworkFlowMonitor 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

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

이 역할에는 AWSSecurityIncidentResponseServiceRolePolicy라는 AWS 관리형 정책이 연결됩니다. 서비스는 역할을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- AWS Organizations: 서비스에서 사용할 멤버십 계정을 조회할 수 있도록 허용합니다.
- CreateCase: 서비스가 멤버십 계정을 대신하여 서비스 사례를 생성할 수 있도록 허용합니다.
- ListCases: 서비스의 AI 에이전트에 보안 조사 목적의 사례 보기를 허용합니다.
- UpdateCase: 서비스의 AI 에이전트에 사례 메타데이터 업데이트를 허용합니다.

- CreateCaseComment: 서비스의 AI 에이전트에 사례 설명으로 결과 게시를 허용합니다.
- ListComments: 서비스의 AI 에이전트에 자동 조사 수행에 필요한 사례 설명 보기를 허용합니다.
- TagResource: 서비스의 일부로 구성된 서비스 태그 리소스를 허용합니다.

역할 관리

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI 또는 AWS API에서 AWS 보안 인시던트 대응에 온보딩하면 서비스가 사용자를 대신하여 서비스 연결 역할을 생성합니다.

> **Note**
>
> 위임 관리자 계정을 사용하여 멤버십을 생성한 경우 AWS Organizations 관리 계정에서 서비스 연결 역할을 수동으로 생성해야 합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 서비스에 온보딩하면 서비스가 서비스 연결 역할을 다시 생성합니다.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage

AWS 보안 인시던트 대응는 AWSServiceRoleForSecurityIncidentResponse_Triage라는 서비스 연결 역할(SLR) - AWS 보안 인시던트 대응 정책을 사용하여 보안 위협에 대해 지속적으로 환경을 모니터링하고, 보안 서비스를 조정하여 알림 노이즈를 줄이고, 잠재적인 인시던트를 조사하기 위한 정보를 수집합니다.

권한

AWSServiceRoleForSecurityIncidentResponse_Triage 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

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

이 역할에는 AWS 관리형 정책 AWSSecurityIncidentResponseTriageServiceRolePolicy가 연결됩니다. 서비스는 역할을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- 이벤트: 서비스가 Amazon EventBridge 관리형 규칙을 생성할 수 있도록 허용합니다. 이 규칙은 AWS 계정에서 서비스로 이벤트를 전달하는 데 필요한 인프라입니다. 이 작업은 `triage.security-ir.amazonaws.com`에서 관리하는 모든 AWS 리소스에서 수행됩니다.
- Amazon GuardDuty: 서비스가 보안 서비스를 조정하여 알림 노이즈를 줄이고, 잠재적 인시던트를 조사하기 위한 정보를 수집하고, GuardDuty 맬웨어 스캔을 시작할 수 있도록 허용합니다.
- AWS Security Hub CSPM: 서비스가 활성화된 표준 및 제품 통합을 나열하고, 조직의 멤버 및 관리자 계정을 나열하고, 보안 서비스를 조정하여 알림 노이즈를 줄이고, 잠재적 인시던트를 조사하기 위한 정보를 수집할 수 있도록 허용합니다.
- AWS Identity and Access Management: 서비스가 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 서비스 연결 역할에 대한 역할 정보를 검색하여 GuardDuty MalwareProtection이 구성되어 있는지 확인하도록 허용합니다.
- AWS 보안 인시던트 대응: 서비스가 `SecurityIncidentResponseManaged=true` 태그가 지정된 리소스로 제한된 사례 및 태그 리소스를 생성 및 업데이트하도록 허용합니다. 서비스가 멤버십 정보(GetMembership, ListMemberships)를 읽을 수 있도록 허용합니다.

역할 관리

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI 또는 AWS API에서 AWS 보안 인시던트 대응에 온보딩하면 서비스가 사용자를 대신하여 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 서비스에 온보딩하면 서비스가 서비스 연결 역할을 다시 생성합니다.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS 보안 인시던트 대응 서비스 연결 역할이 지원되는 리전

AWS 보안 인시던트 대응는 서비스가 제공되는 모든 리전에서 서비스 연결 역할을 사용하도록 지원합니다.

- 미국 동부(오하이오)
- 미국 서부(오리건)
- 미국 동부(버지니아)
- 유럽(프랑크푸르트)

- 유럽(아일랜드)
- 유럽(런던)
- 유럽(밀라노)
- 유럽(파리)
- 유럽(스페인)
- 유럽(스톡홀름)
- 유럽(취리히)
- 아시아 태평양(홍콩)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(자카르타)
- 아시아 태평양(멜버른)
- 아시아 태평양(뭄바이)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 캐나다(중부)
- 중동(바레인)
- 중동(UAE)
- 남아메리카(상파울루)
- 아프리카(케이프타운)

AWS 관리형 정책

AWS 관리형 정책은 AWS에서 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

사용자, 그룹 또는 역할에 권한을 추가할 때 정책을 직접 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더욱 편리합니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하려면 시간과 전문 지식이 필요합니다. 빨리 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이러한 정책은 일반

적인 사용 사례에 적용되며 AWS계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 정보는 IAM 사용 설명서에서 AWS 관리형 정책을 참조하세요.

AWS 서비스가 연결된 AWS 관리형 정책을 유지하고 업데이트입니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 태스크를 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS관리형 정책에서 권한을 제거하지 않기 때문에 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 AWS는 여러 서비스의 직무에 대한 관리형 정책을 지원합니다. 예를 들어 ReadOnlyAccess라는 이름의 AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스 권한을 제공합니다. 서비스에서 새 기능을 시작하면 AWS가 새 작업 및 리소스에 대한 읽기 전용 권한을 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한 AWS 관리형 정책을 참조하세요.

내용

AWS 관리형 정책: AWSSecurityIncidentResponseServiceRolePolicy

AWS 보안 인시던트 대응는 AWSSecurityIncidentResponseServiceRolePolicy AWS 관리형 정책을 사용합니다. AWSServiceRoleForSecurityIncidentResponse 서비스 연결 역할에는 AWS 관리형 정책이 연결됩니다. 정책은 구독된 계정을 식별하고, 사례를 생성하고, 사례를 업데이트하고, 사례 설명을 생성하고, 사례를 나열하고, 사례 설명을 나열하고, 관련 리소스에 태그를 지정하는 AWS 보안 인시던트 대응대한 액세스 권한을 제공합니다.

> **Important**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. AWS 보안 인시던트 대응는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 개인 데이터나 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는 이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- AWS Organizations: 서비스에서 사용할 멤버십 계정을 조회할 수 있도록 허용합니다.
- CreateCase: 서비스가 멤버십 계정을 대신하여 서비스 사례를 생성할 수 있도록 허용합니다.
- ListCases: 서비스의 AI 에이전트에 보안 조사 목적의 사례 보기를 허용합니다.
- UpdateCase: 서비스의 AI 에이전트에 사례 메타데이터 업데이트를 허용합니다.
- CreateCaseComment: 서비스의 AI 에이전트에 사례 설명으로 결과 게시를 허용합니다.
- ListComments: 서비스의 AI 에이전트에 자동 조사 수행에 필요한 사례 설명 보기를 허용합니다.
- TagResource: 서비스의 일부로 구성된 서비스 태그 리소스를 허용합니다.

AWSSecurityIncidentResponseServiceRolePolicy에 대한 AWS 관리형 정책에서 이 정책과 연결된 권한을 볼 수 있습니다.

AWS 관리형 정책: AWSSecurityIncidentResponseFullAccess

AWS 보안 인시던트 대응는 AWSSecurityIncidentResponseAdmin AWS 관리형 정책을 사용합니다. 이 정책은 서비스 리소스에 대한 전체 액세스 권한과 관련 AWS 서비스에 대한 액세스 권한을 부여합니다. 이 정책을 IAM 위탁자와 함께 사용하여 AWS 보안 인시던트 대응에 대한 권한을 빠르게 추가할 수 있습니다.

> **Important**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. AWS 보안 인시던트 대응는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 개인 데이터나 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는 이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- IAM 위탁자 읽기 전용 액세스: 서비스 사용자에게 기존 AWS 보안 인시던트 대응 리소스에 대해 읽기 전용 작업을 수행할 수 있는 권한을 부여합니다.
- IAM 위탁자 쓰기 액세스: 서비스 사용자에게 AWS 보안 인시던트 대응 리소스를 업데이트, 수정, 삭제 및 생성할 수 있는 권한을 부여합니다.

AWSSecurityIncidentResponseFullAccess에 대한 AWS 관리형 정책에서 이 정책과 연결된 권한을 볼 수 있습니다.

AWS 관리형 정책: AWSSecurityIncidentResponseReadOnlyAccess

AWS 보안 인시던트 대응는 AWSSecurityIncidentResponseReadOnlyAccess AWS 관리형 정책을 사용합니다. 이 정책은 서비스 사례 리소스에 대한 읽기 전용 액세스 권한을 부여합니다. 이 정책을 IAM 위탁자와 함께 사용하여 AWS 보안 인시던트 대응에 대한 권한을 빠르게 추가할 수 있습니다.

> **Important**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. AWS 보안 인시던트 대응는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 개인 데이터나 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는 이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- IAM 위탁자 읽기 전용 액세스: 서비스 사용자에게 기존 AWS 보안 인시던트 대응 리소스에 대해 읽기 전용 작업을 수행할 수 있는 권한을 부여합니다.

AWSSecurityIncidentResponseReadOnlyAccess에 대한 AWS 관리형 정책에서 이 정책과 연결된 권한을 볼 수 있습니다.

AWS 관리형 정책: AWSSecurityIncidentResponseCaseFullAccess

AWS 보안 인시던트 대응는 AWSSecurityIncidentResponseCaseFullAccess AWS 관리형 정책을 사용합니다. 이 정책은 서비스 사례 리소스에 대한 전체 액세스 권한을 부여합니다. 이 정책을 IAM 위탁자와 함께 사용하여 AWS 보안 인시던트 대응에 대한 권한을 빠르게 추가할 수 있습니다.

> **Important**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. AWS 보안 인시던트 대응는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 개인 데이터나 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는 이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- IAM 위탁자 사례 읽기 전용 액세스: 서비스 사용자에게 기존 AWS 보안 인시던트 대응 사례에 대해 읽기 전용 작업을 수행할 수 있는 권한을 부여합니다.
- IAM 위탁자 사례 쓰기 액세스: 서비스 사용자에게 AWS 보안 인시던트 대응 사례를 업데이트, 수정, 삭제 및 생성할 수 있는 권한을 부여합니다.

AWSSecurityIncidentResponseCaseFullAccess에 대한 AWS 관리형 정책에서 이 정책과 연결된 권한을 볼 수 있습니다.

AWS 관리형 정책: AWSSecurityIncidentResponseTriageServiceRolePolicy

AWS 보안 인시던트 대응는 AWSSecurityIncidentResponseTriageServiceRolePolicy AWS 관리형 정책을 사용합니다. 이 AWS 관리형 정책은 AWSServiceRoleForSecurityIncidentResponse_Triage 서비스 연결 역할에 연결됩니다.

이 정책은 AWS 보안 인시던트 대응에 대한 액세스를 제공하여 환경에 보안 위협이 있는지 지속적으로 모니터링하고, 보안 서비스를 튜닝하여 알림 노이즈를 줄이고, 잠재적 인시던트를 조사하기 위한 정보를 수집합니다. IAM 엔터티에 이 정책을 연결할 수 없습니다.

> **Important**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. AWS 보안 인시던트 대응는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 개인 데이터나 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는 이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- 이벤트: 서비스가 Amazon EventBridge 관리형 규칙을 생성할 수 있도록 허용합니다. 이 규칙은 AWS 계정에서 서비스로 이벤트를 전달하는 데 필요한 인프라입니다. 이 작업은 `triage.security-ir.amazonaws.com`에서 관리하는 모든 AWS 리소스에서 수행됩니다.
- Amazon GuardDuty: 서비스가 보안 서비스를 조정하여 알림 노이즈를 줄이고, 잠재적 인시던트를 조사하기 위한 정보를 수집하고, GuardDuty 맬웨어 스캔을 시작할 수 있도록 허용합니다.
- AWS Security Hub CSPM: 서비스가 활성화된 표준 및 제품 통합을 나열하고, 조직의 멤버 및 관리자 계정을 나열하고, 보안 서비스를 조정하여 알림 노이즈를 줄이고, 잠재적 인시던트를 조사하기 위한 정보를 수집할 수 있도록 허용합니다.

- AWS Identity and Access Management: 서비스가 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 서비스 연결 역할에 대한 역할 정보를 검색하여 GuardDuty MalwareProtection이 구성되어 있는지 확인하도록 허용합니다.
- AWS 보안 인시던트 대응: 서비스가 `SecurityIncidentResponseManaged=true` 태그가 지정된 리소스로 제한된 사례 및 태그 리소스를 생성 및 업데이트하도록 허용합니다. 서비스가 멤버십 정보(GetMembership, ListMemberships)를 읽을 수 있도록 허용합니다.

AWSSecurityIncidentResponseTriageServiceRolePolicy에 대한 AWS 관리형 정책에서 이 정책과 연결된 권한을 볼 수 있습니다.

SLR 및 관리형 정책에 대한 AWS 보안 인시던트 대응 업데이트

이 서비스에서 이러한 변경 사항을 추적하기 시작한 이후부터 AWS 보안 인시던트 대응 SLR 및 관리 정책 역할에 대한 업데이트 세부 정보를 봅니다.

변경	설명	날짜
업데이트됨 - AWSSecurityIncidentResponseTriageServiceRolePolicy	이제 정책은 서비스가 `SecurityIncidentResponseManaged=true` 태그가 지정된 GuardDuty 필터를 수정하고, 감지기 구성을 업데이트하고, GuardDuty 맬웨어 스캔을 시작하도록 허용합니다. 이를 통해 서비스는 Security Hub CSPM 조사 결과에 자동으로 적용되는 규칙을 생성 및 관리하고 조직의 구조를 파악할 수 있습니다.	2026년 3월 27일
업데이트됨 - AWSSecurityIncidentResponseServiceRolePolicy	이제 정책에서 다음 리소스에 대한 작업을 수행합니다. ListCases: 서비스의 AI 에이전트에 보안 조사 목적의 사례 보기를 허용합니다. UpdateCase: 서비스의 AI 에이전트에 사례 메타데이터 업데이트를 허용합니다. CreateCaseComment: 서비스의 AI 에이전트에 사례 설명으로 결과 게시를 허용합니다. ListComments: 서비스의 AI 에이전트에 자동 조사 수행에 필요한 사례 설명 보기를 허용합니다.	2025년 11월

변경	설명	날짜
업데이트됨 - AWSSecurityIncidentResponseServiceRolePolicy	이제 정책에 `"organizations:DescribeAccount"` , `"organizations:ListDelegatedAdministrators"` 에 대한 두 가지 새 작업과 새 조건이 포함됩니다. `"Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } }`	2025년 11월
서비스 자격을 지원하기 위한 권한을 추가하는 SLR 업데이트	AWSSecurityIncidentResponseTriageServiceRolePolicy가 업데이트되어 security-ir:GetMembership, security-ir:ListMemberships, security-ir:UpdateCase, guardduty:ListFilters, guardduty:UpdateFilter, guardduty:DeleteFilter 및 guardduty:GetAdministratorAccount 권한이 추가되었습니다. guardduty:GetAdministratorAccount가 추가되어 위임 계정에서 GuardDuty 자동 아카이브 필터를 쉽게 관리할 수 있습니다.	2025년 6월 2일
새 SLR - AWSServiceRoleForSecurityIncidentResponse 새 관리형 정책 - AWSSecurityIncidentResponseServiceRolePolicy.	새로운 서비스 연결 역할과 연결된 정책을 통해 AWS Organizations 계정에 서비스 액세스를 허용하여 멤버십을 식별할 수 있습니다.	2024년 12월 1일

변경	설명	날짜
새 SLR - AWSServiceRoleForSecurityIncidentResponse_Triage 새 관리형 정책 - AWSSecurityIncidentResponseTriageServiceRolePolicy	새로운 서비스 연결 역할과 연결된 정책을 통해 AWS Organizations 계정에 서비스 액세스를 허용하여 보안 이벤트 분류를 수행할 수 있습니다.	2024년 12월 1일
새 관리형 정책 - AWSSecurityIncidentResponseFullAccess	AWS 보안 인시던트 대응는 서비스에 대한 읽기 및 쓰기 작업을 위해 IAM 위탁자에게 연결할 새 SLR을 추가합니다.	2024년 12월 1일
새 관리형 정책 역할 - AWSSecurityIncidentResponseReadOnlyAccess	AWS 보안 인시던트 대응는 읽기 작업을 위해 IAM 위탁자에게 연결할 새 SLR을 추가합니다.	2024년 12월 1일
새 관리형 정책 역할 - AWSSecurityIncidentResponseCaseFullAccess	AWS 보안 인시던트 대응는 서비스 사례에 대한 읽기 및 쓰기 작업을 위해 IAM 위탁자에게 연결할 새 SLR을 추가합니다.	2024년 12월 1일
변경 내용 추적 시작	AWS 보안 인시던트 대응 SLR과 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2024년 12월 1일

인시던트 대응

보안과 규정 준수는 AWS와 고객의 공동 책임입니다. 이 공동 모델은 고객의 운영 부담을 더는 데 도움이 될 수 있습니다. 호스트 운영 체제 및 가상화 계층부터 서비스 운영 시설의 물리적 보안에 이르는 구성 요소를 AWS에서 운영, 관리 및 제어하기 때문입니다. 고객의 책임 및 관리 범위에는 AWS가 제공하는 보안 그룹 방화벽의 구성과 게스트 운영 체제(업데이트 및 보안 패치 포함), 기타 관련 애플리케이션 소프트웨어가 포함됩니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

클라우드에서 실행되는 애플리케이션의 목표를 충족하는 보안 기준을 설정하면 대응할 수 있는 편차를 감지할 수 있습니다. 보안 인시던트 대응은 복잡한 항목일 수 있으므로, 인시던트 대응(IR)과 선택이 기업 목표에 미치는 영향을 더 잘 이해할 수 있도록 AWS 보안 모범 사례 백서, AWS Cloud Adoption Framework Security Perspective 백서 등의 리소스를 검토하는 것이 좋습니다.

규정 준수 확인

서드 파티 감사자는 여러 AWS 규정 준수 프로그램의 일환으로 AWS 서비스의 보안 및 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램 범위에 속하는 AWS 서비스의 목록은 규정 준수 프로그램 제공 AWS 범위 내 서비스를 참조하세요. 일반 정보는 AWS 규정 준수 프로그램을 참조하세요.

AWS Artifact를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact의 보고서 다운로드를 참조하세요.

AWS 서비스를 사용할 때 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS는 규정 준수를 지원하기 위해 다음과 같은 리소스를 제공합니다.

- 보안 및 규정 준수 빠른 시작 가이드 – 이 배포 가이드에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔 기본 AWS 환경을 배포하기 위한 단계를 제공합니다.
- HIPAA 보안 및 규정 준수 백서 설계 - 이 백서에서는 기업에서 AWS를 사용하여 HIPAA를 준수하는 애플리케이션을 생성하는 방법을 설명합니다.
- AWS 규정 준수 리소스 - 업계 및/또는 지역별로 적용되는 워크북과 안내서 모음입니다.
- AWS Config 개발자 안내서의 AWS Config 규칙을 사용하여 리소스 평가 - AWS Config는 리소스 구성이 내부 사례, 업계 지침, 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS 보안 허브- 이 AWS 서비스는 AWS 내의 보안 상태에 대한 포괄적인 보기를 제공합니다. Security Hub는 보안 컨트롤을 사용하여 AWS리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.

- Amazon GuardDuty - 이 AWS 서비스는 의심스럽고 악의적인 활동이 있는지 환경을 모니터링하여 AWS 계정, 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager – 이 AWS 서비스는 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 산업 표준의 준수를 관리하는 방법을 간소화하는 데 도움이 됩니다.

AWS Security Incident Response의 로깅 및 모니터링

모니터링은 AWS 보안 인시던트 대응 및 다른 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWS 보안 인시던트 대응는 현재 조직 및 조직 내에서 발생하는 활동을 모니터링할 수 있는 다음과 같은 AWS 서비스를 지원합니다.

AWS CloudTrail - CloudTrail을 사용하면 AWS Security Incident Response 콘솔에서 API 직접 호출을 캡처할 수 있습니다. 예를 들어 사용자가 인증할 때 CloudTrail은 요청의 IP 주소, 요청한 사람, 요청한 시기와 같은 세부 정보를 기록할 수 있습니다.

Amazon CloudWatch 지표 – CloudWatch 지표를 사용하면 이벤트 발생 시 거의 실시간으로 모니터링 및 보고하고 자동 조치를 취할 수 있습니다. 예를 들어 제공된 지표에 대한 CloudWatch 대시보드를 만들어 AWS 보안 인시던트 대응 사용량을 모니터링하거나 제공된 지표에 대한 CloudWatch 경보를 생성하여, 설정 임곗값 위반이 발생할 경우 알림을 받을 수 있습니다.

서비스의 네임스페이스는 AWS/Usage/ServiceName입니다. 사용 가능한 지표 이름은 ActiveManagedCases와 SelfManagedCases입니다.

AWS 서비스 약관에 따라 AWS 보안 인시던트 대응 대응 담당자 팀은 CloudTrail, VPC, DNS 및 S3 로그 데이터 기록에 액세스할 수 있습니다. AWS Security Incident Response 서비스 포털에서 사례가 열려 있을 때 활성 보안 인시던트 중 이 데이터를 사용할 수 있습니다.

복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며, 이러한 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

인프라 보안

AWS 보안 인시던트 대응는 AWS 글로벌 네트워크 보안에 의해 보호됩니다. AWS 보안 서비스와 AWS의 인프라 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안에 대한 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS에서 게시한 API 직접 호출을 사용하여 네트워크를 통해 AWS 보안 인시던트 대응에 액세스합니다. 클라이언트는 다음을 지원해야 합니다.

- Transport Layer Security(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 시크릿 액세스 키를 사용하여 서명해야 합니다. AWS 보안 토큰 서비스(AWS STS)를 사용하여 요청에 서명하기 위한 임시 보안 자격 증명을 생성할 수도 있습니다.

구성 및 취약성 분석

서비스 격리 역할과 관련 CloudFormation 스택 세트를 관리할 책임은 사용자에게 있습니다.

AWS는 게스트 운영 체제(OS) 및 데이터베이스 패치, 방화벽 구성, 재해 복구 등의 기본 보안 태스크를 처리합니다. 적합한 제3자가 이 절차를 검토하고 인증하였습니다. 자세한 내용은 다음 AWS 리소스를 참조하세요.

- 공동 책임 모델
- 보안, 자격 증명 및 규정 준수를 위한 모범 사례

교차 서비스 혼동된 대리자 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. AWS에서는 교차 서비스 가장으로 인해 혼동된 대리자 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(직접 호출하는 서비스)가 다른 서비스(직접 호출되는 서비스)를 직접 호출할 때 발생할 수 있습니다. 직접 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해

AWS에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 위탁자를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

Amazon Connect가 리소스에 다른 서비스를 제공하는 권한을 제한하려면 리소스 정책에서 AWS:SourceArn 및 AWS:SourceAccount 글로벌 조건 컨텍스트 키를 사용하는 것이 좋습니다. 두 전역 조건 컨텍스트 키를 모두 사용하는 경우 AWS:SourceAccount 값과 AWS:SourceArn 값의 계정은 동일한 정책 문에서 사용할 경우 동일한 계정 ID를 사용해야 합니다.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 허용하려는 리소스와 동일한 Amazon 리소스 이름(ARN)을 사용하는 것입니다. 리소스의 전체 ARN을 모르거나 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드(*)를 포함한 AWS:SourceArn 글로벌 조건 컨텍스트 키를 사용합니다. arn:AWS:servicename::region-name::your AWS account ID:*를 예로 들 수 있습니다.

혼동된 대리자 문제를 예방하는 방법을 보여주는 수임 역할 정책의 예는 Confused deputy prevention policy를 참조하세요.

Service Quotas

AWS 보안 인시던트 대응

AWS 일반 참조 가이드에는 최신 AWS 보안 인시던트 대응 엔드포인트 및 할당량이 포함되어 있습니다.

AWS 보안 인시던트 대응 기술 지침

내용

요약

이 가이드에서는 고객의 Amazon Web Services(AWS) 클라우드 환경 내 보안 인시던트 대응의 기본 사항에 대한 개요를 제공합니다. 클라우드 보안 및 인시던트 대응 개념의 개요를 제공하고 보안 문제에 대응하는 고객이 사용할 수 있는 클라우드 기능, 서비스 및 메커니즘을 파악합니다.

이 가이드는 기술 담당자를 대상으로 하며, 정보 보안의 일반 원칙을 잘 알고 있고, 현재 온프레미스 환경 내 보안 인시던트 대응에 대한 기본적인 이해가 있으며, 클라우드 서비스에 어느 정도 익숙하다는 가정하에 작성되었습니다.

귀사는 Well-Architected입니까?

AWS Well-Architected 프레임워크는 클라우드에서 시스템을 구축할 때 내리는 결정의 장단점을 이해하는 데 도움이 됩니다. 이 프레임워크를 사용하여 클라우드에서 안정적이고 안전하며 효율적이고 비용 효율적인 시스템을 설계하고 운영하기 위한 아키텍처 모범 사례를 살펴볼 수 있습니다. AWS Well-Architected Tool 콘솔에서 무료로 제공되는 AWS Well-Architected Tool 사용하면 각 요소에 대한 일련의 질문에 답하여, 이러한 모범 사례와 비교하여 워크로드를 검토할 수 있습니다.

참조 아키텍처 배포, 다이어그램, 백서 등 클라우드 아키텍처에 대한 더 많은 전문가 지침과 모범 사례를 보려면 AWS 아키텍처 센터를 참조하세요.

소개

AWS는 보안을 최우선으로 생각합니다. AWS 고객은 보안에 가장 민감한 조직의 요구를 지원하도록 구축된 데이터 센터와 네트워크 아키텍처의 이점을 누릴 수 있습니다. AWS는 공동 책임 모델을 채택하고 있습니다. 즉, AWS가 클라우드의 보안을 관리하고, 고객이 클라우드 내 보안을 책임집니다. 이는 보안 목표 달성에 도움이 되는 다양한 도구와 서비스에 대한 액세스를 포함하여 보안 구현을 완벽하게 제어할 수 있음을 의미합니다. 이러한 기능은 AWS 클라우드에서 실행되는 애플리케이션의 보안 기준을 설정하는 데 도움이 됩니다.

잘못된 구성이나 외부 요인 변경 등으로 인해 기준에서 벗어나는 경우 대응하고 조사해야 합니다. 이를 성공적으로 수행하려면 AWS 환경 내 보안 인시던트 대응의 기본 개념과 보안 문제가 발생하기 전에 클라우드 팀을 준비, 교육 및 훈련하기 위한 요구 사항을 파악해야 합니다. 사용할 수 있는 제어와 기능을 파악하고, 잠재적 문제를 해결하기 위한 주제 예시를 검토하고, 자동화를 사용하여 대응 속도와 일관성을 개선하는 해결 방법을 식별하는 것이 중요합니다. 또한 이러한 요구 사항을 충족하기 위해 보안 인시던트 대응 프로그램 구축과 관련된 규정 준수 및 규제 요구 사항을 이해해야 합니다.

보안 인시던트 대응은 복잡할 수 있으므로 핵심 보안 서비스부터 시작하여 기본 탐지 및 대응 기능을 구축한 다음 플레이북을 개발하여 반복 및 개선을 위한 인시던트 대응 메커니즘의 초기 라이브러리를 생성하는 등 반복적인 접근 방식을 구현하는 것이 좋습니다.

시작하기 전에

AWS에서 보안 이벤트에 대한 인시던트 대응에 대해 알아보기 전에 AWS 보안 및 인시던트 대응을 위한 관련 표준 및 프레임워크를 숙지하세요. 이러한 기반은 이 가이드에 제시된 개념과 모범 사례를 이해하는 데 도움이 됩니다.

AWS 보안 표준 및 프레임워크

먼저 보안, 자격 증명 및 규정 준수 모범 사례, 보안 요소 - AWS Well-Architected Framework 및 보안 관점: AWS Cloud Adoption Framework(AWS CAF)의 개요 백서를 검토하는 것이 좋습니다.

AWS CAF는 클라우드로 전환하는 조직의 여러 부서 간 조정을 지원하는 지침을 제공합니다. AWS 클라우드 기반 IT 시스템 구축과 관련된 몇 가지 중점 영역(관점)으로 나뉩니다. 보안 관점에서는 워크스트림 전반에서 보안 프로그램을 구현하는 방법을 설명하며, 그 중 하나가 인시던트 대응입니다. 이 문서는 고객이 효과적이고 효율적인 보안 인시던트 대응 프로그램과 역량을 구축할 수 있도록 지원하기 위해 고객과 협력한 경험의 산물입니다.

산업 인시던트 대응 표준 및 프레임워크

이 백서는 NIST(국립표준기술연구소)에서 만든 Computer Security Incident Handling Guide SP 800-61 r3의 인시던트 대응 표준 및 모범 사례를 따릅니다. NIST에서 소개하는 개념을 읽고 이해하는 것은 유용한 전제 조건입니다. 이 NIST 가이드의 개념과 모범 사례는 이 백서의 AWS 기술에 적용됩니다. 그러나 온프레미스 인시던트 시나리오는 이 가이드의 범위를 벗어납니다.

AWS 인시던트 대응 개요

먼저 클라우드에서 보안 운영과 인시던트 대응이 어떻게 다른지 이해하는 것이 중요합니다. AWS에서 효과적인 대응 기능을 구축하려면 기존 온프레미스 대응과의 편차와 이러한 편차가 인시던트 대응 프로그램에 미치는 영향을 이해해야 합니다. 이러한 각 차이점과 핵심 AWS 인시던트 대응 설계 원칙은 이 섹션에 자세히 설명되어 있습니다.

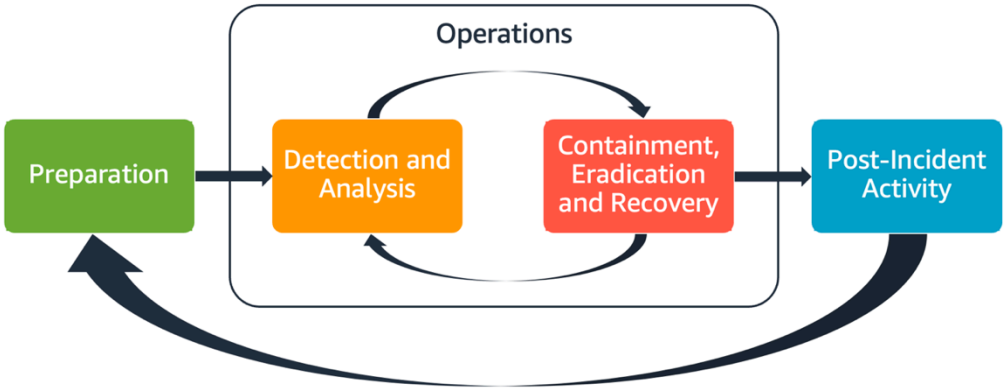
AWS 인시던트 대응 측면

조직 내 모든 AWS 사용자는 보안 인시던트 대응 프로세스에 대한 기본적인 이해가 있어야 하며 보안 직원은 보안 문제에 대응하는 방법을 이해해야 합니다. 교육, 훈련 및 경험은 성공적인 클라우드 인시던트 대응 프로그램에 필수적이며 발생 가능한 보안 인시던트를 처리하기 전에 미리 구현하는 것이 이상적입니다. 클라우드에서의 성공적인 인시던트 대응 프로그램은 준비, 운영, 인시던트 사후 활동에 기반합니다.

이러한 각 측면을 이해하려면 다음 설명을 고려하세요.

- 준비 - 탐지 제어를 활성화하고 필요한 도구 및 클라우드 서비스에 대한 적절한 액세스를 확인하여 인시던트 대응 팀이 AWS 내부 인시던트를 탐지하고 이에 대응할 수 있도록 준비합니다. 또한 신뢰할 수 있는 일관된 응답을 보장하는 데 필요한 수동 및 자동 런북을 준비합니다.
- 운영 - 탐지, 분석, 방지, 근절 및 복구와 같은 NIST의 인시던트 대응 단계에 따라 보안 이벤트 및 잠재적 인시던트를 해결합니다.
- 인시던트 사후 활동 - 보안 이벤트 및 시뮬레이션의 결과를 반복하여 대응의 효율성을 높이고, 대응 및 조사를 통해 도출된 가치를 높이며, 위험을 더욱 줄입니다. 인시던트를 통해 배우고 개선 활동에 대한 강한 주인의식을 가져야 합니다.

이 가이드에서 이러한 각 측면을 살펴보고 자세히 설명합니다. 다음 다이어그램에서는 이러한 측면의 흐름을 보여줍니다. 흐름은 앞서 언급한 NIST 인시던트 대응 수명 주기와 일치하지만 탐지 및 분석, 방지, 근절 및 복구를 포함하는 작업을 수행합니다.



AWS 인시던트 대응 측면

AWS 인시던트 대응 원칙 및 설계 목표

NIST SP 800-61 Computer Security Incident Handling Guide에 정의된 일반적인 인시던트 대응 프로세스와 메커니즘은 타당하지만, 클라우드 환경에서 보안 인시던트에 대응하는 것과 관련된 구체적인 설계 목표를 고려하는 것이 좋습니다.

- 대응 목표 수립 - 이해관계자, 법률 자문, 조직 리더십과 협력하여 인시던트 대응 목표를 결정합니다. 몇 가지 공통 목표로, 문제 격리 및 완화, 영향을 받는 리소스 복구, 포렌식을 위한 데이터 보존, 알려진 안전한 운영 환경으로 복구, 궁극적으로 인시던트를 통한 학습 등이 포함됩니다.
- 클라우드를 사용하여 대응 - 이벤트와 데이터가 존재하는 곳에 대응 패턴을 구현합니다.
- 무엇을 가지고 있고 무엇이 필요한지 파악 - 로그, 리소스, 스냅샷 및 기타 증거를 대응 전용 중앙 집중식 클라우드 계정에 복사 및 저장하여 보존합니다. 태그, 메타데이터, 보존 정책을 적용하는 메커니즘을 사용합니다. 어떤 서비스를 사용하고 있는지 파악한 다음 해당 서비스를 조사하기 위한 요구 사항을 파악해야 합니다. 환경을 이해하는 데 도움이 되도록 이 문서 뒷부분의 the section called “태그 지정 전략 개발 및 구현” 섹션에서 다루는 태깅을 사용할 수도 있습니다.
- 재배포 메커니즘 사용: 잘못된 구성으로 인해 보안 이상이 발생한 경우 올바른 구성으로 리소스를 재배포하여 변형을 제거하는 것만으로 간단하게 문제를 해결할 수 있습니다. 손상 가능성이 확인되면 재배포에 성공적이고 검증된 근본 원인 완화 조치가 포함되어 있는지 확인하세요.
- 가능한 경우 자동화 - 문제가 발생하거나 인시던트가 반복되면 프로그래밍 방식으로 분류하고 일반적인 이벤트에 대응하는 메커니즘을 구축하세요. 자동화가 불가능한 고유하거나 복잡하거나 민감한 인시던트에는 사람의 대응을 활용하세요.
- 확장 가능한 솔루션 선택 - 클라우드 컴퓨팅에 대한 조직의 접근 방식의 확장성과 일치하도록 노력하세요. 환경 전반으로 규모가 조정되는 탐지 및 대응 메커니즘을 구현하여 탐지와 대응 사이의 시간을 효과적으로 줄이세요.

- 프로세스 교육 및 개선 - 프로세스, 도구 또는 인력의 격차를 사전에 파악하고 이를 해결하기 위한 계획을 실행하세요. 시뮬레이션은 격차를 찾고 프로세스를 개선할 수 있는 안전한 방법입니다. 프로세스를 반복하는 방법에 대한 자세한 내용은 이 문서의 the section called “인시던트 사후 활동” 섹션을 참조하세요.

이러한 설계 목표는 인시던트 대응과 위협 탐지를 모두 수행할 수 있는지 아키텍처 구현을 검토하도록 상기시켜줍니다. 클라우드 구현을 계획할 때는 포렌식에 기반하여 타당한 대응 방법론을 사용하여 인시던트에 대응하는 방안을 생각해 보세요. 경우에 따라 이러한 대응 태스크를 위해 특별히 설정된 조직, 계정 및 도구가 여러 개 있을 수 있습니다. 이러한 도구와 기능은 배포 파이프라인을 통해 인시던트 대응 담당자가 사용할 수 있도록 해야 합니다. 더 큰 위험을 초래할 수 있으므로 정적이어서는 안 됩니다.

클라우드 보안 인시던트 영역

AWS 환경에서 보안 이벤트에 효과적으로 대비하고 대응하려면 일반적인 클라우드 보안 인시던트 유형을 이해해야 합니다. 고객의 책임하에 보안 인시던트가 발생할 수 있는 세 가지 영역은 서비스, 인프라, 애플리케이션입니다. 영역마다 다른 지식, 도구 및 대응 프로세스가 필요합니다. 다음 영역을 고려하세요.

- 서비스 영역 - 서비스 영역의 인시던트는 AWS 계정, AWS Identity and Access Management(IAM) 권한, 리소스 메타데이터, 결제 또는 기타 영역에 영향을 줄 수 있습니다. 서비스 영역 이벤트는 AWS API 메커니즘으로만 대응하거나 구성 또는 리소스 권한과 관련된 근본 원인이 있는 이벤트이며 관련 서비스 지향 로깅이 있을 수 있습니다.
- 인프라 영역 - 인프라 영역의 인시던트에는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 프로세스 및 데이터, 가상 프라이빗 클라우드(VPC) 내의 Amazon EC2 인스턴스로의 트래픽, 컨테이너 또는 기타 향후 서비스와 같은 기타 영역 등의 데이터 또는 네트워크 관련 활동이 포함됩니다. 인프라 영역 이벤트에 대한 대응에는 포렌식 분석을 위한 인시던트 관련 데이터 획득이 포함되는 경우가 많습니다. 여기에는 인스턴스 운영 체제와의 상호 작용이 포함될 가능성이 높으며, 경우에 따라 AWS 메커니즘이 관련될 수도 있습니다. 인프라 영역에서는 포렌식 분석 및 조사 수행 전용 Amazon EC2 인스턴스와 같은 게스트 운영 체제 내에서 AWS API와 디지털 포렌식/인시던트 대응(DFIR) 도구를 조합하여 사용할 수 있습니다. 인프라 영역 인시던트에는 네트워크 패킷 캡처, Amazon Elastic Block Store(Amazon EBS) 볼륨의 디스크 블록 또는 인스턴스에서 획득한 휘발성 메모리 분석이 포함될 수 있습니다.
- 애플리케이션 영역 - 애플리케이션 영역의 인시던트는 애플리케이션 코드나 서비스 또는 인프라에 배포된 소프트웨어에서 발생합니다. 이 영역은 클라우드 위협 탐지 및 대응 플레이북에 포함되어야 하며 인프라 영역의 대응과 유사한 대응을 통합할 수 있습니다. 적절하고 사려 깊은 애플리케이션 아

키텍처를 사용하면 자동 획득, 복구 및 배포를 사용하여 클라우드 도구를 통해 이 영역을 관리할 수 있습니다.

이러한 영역에서는 AWS 계정, 리소스 또는 데이터에 대해 조치를 취할 수 있는 행위자를 고려하세요. 내부 또는 외부에 관계없이 위험 프레임워크를 사용하여 조직에 대한 구체적인 위험을 파악하고 그에 따라 대비하세요. 또한 인시던트 대응 계획과 신중한 아키텍처 구축에 도움이 될 수 있는 위협 모델을 개발해야 합니다.

AWS에서 인시던트 대응의 주요 차이점

인시던트 대응은 온프레미스 또는 클라우드에서 사이버 보안 전략의 필수적인 부분입니다. 최소 권한, 심층 방어 등의 보안 원칙은 온프레미스와 클라우드 모두에서 데이터의 기밀성, 무결성 및 가용성을 보호하기 위한 것입니다. 로그 보존, 위협 모델링에서 파생된 알림 선택, 플레이북 개발, 보안 정보 및 이벤트 관리(SIEM) 통합 등 이러한 보안 원칙을 뒷받침하는 여러 인시던 대응 패턴도 마찬가지입니다. 고객이 클라우드에서 이러한 패턴을 설계하고 엔지니어링하기 시작할 때부터 차이가 시작됩니다. 다음은 AWS에서 인시던트 대응의 주요 차이입니다.

차이 1: 공동 책임으로서의 보안

보안과 규정 준수에 대한 책임은 AWS와 고객이 공유합니다. 이 공동 책임 모델은 고객의 운영 부담을 덜어줍니다. 호스트 운영 체제 및 가상화 계층부터 서비스 운영 시설의 물리적 보안에 이르는 구성 요소를 AWS에서 운영, 관리 및 제어하기 때문입니다. 공동 책임 모델에 대한 자세한 내용은 공동 책임 모델 설명서를 참조하세요.

클라우드에서 공동 책임이 변경되면 인시던트 대응 옵션도 변경됩니다. 이러한 상충 관계를 계획 및 이해하고 거버넌스 요구 사항에 맞추는 것은 인시던트 대응의 중요한 단계입니다.

AWS와의 직접적인 관계 외에도 특정 책임 모델에서 책임을 지는 다른 엔터티가 있을 수 있습니다. 예를 들어 운영의 일부 측면을 책임지는 내부 조직 단위가 있을 수 있습니다. 일부 클라우드 기술을 개발, 관리 또는 운영하는 다른 당사자와 관계를 맺고 있을 수도 있습니다.

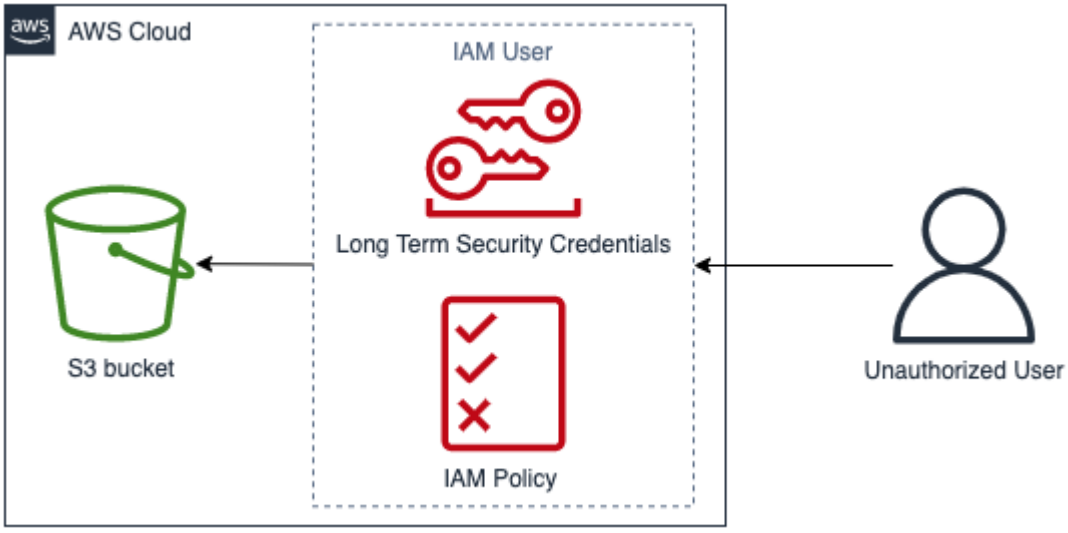
운영 모델에 맞는 적절한 인시던트 대응 계획과 적절한 플레이북을 생성하고 테스트하는 것이 매우 중요합니다.

차이 2: 클라우드 서비스 영역

클라우드 서비스에 존재하는 보안 책임의 차이로 인해 보안 인시던트에 대한 새로운 영역인 서비스 영역이 도입되었습니다.이는 앞서 인시던트 영역 섹션에서 설명했습니다. 서비스 영역은 고객의 AWS 계정, IAM 권한, 리소스 메타데이터, 결제 및 기타 영역을 포괄합니다. 이 영역은 대응 방식에 따라 인시

던트 대응이 달라집니다. 서비스 영역 내의 대응은 일반적으로 기존 호스트 기반 및 네트워크 기반 대응이 아닌 API 직접 호출을 검토하고 실행하는 방식으로 이루어집니다. 서비스 영역에서는 영향을 받는 리소스의 운영 체제와 상호 작용하지 않습니다.

다음 다이어그램은 아키텍처 안티 패턴을 기반으로 하는 서비스 영역의 보안 이벤트 예를 보여줍니다. 이 경우 권한이 없는 사용자는 IAM 사용자의 장기 보안 자격 증명을 얻습니다. IAM 사용자는 Amazon Simple Storage Service(Amazon S3) 버킷에서 객체를 검색할 수 있는 IAM 정책을 가지고 있습니다. 이 보안 이벤트에 대응하려면 AWS API를 사용하여 AWS CloudTrail 및 Amazon S3 액세스 로그와 같은 AWS 로그를 분석합니다. 또한 AWS API를 사용하여 인시던트를 격리하고 복구합니다.



서비스 영역 예시

차이 3: 인프라 프로비저닝을 위한 API

또 다른 차이는 온디맨드 셀프 서비스의 클라우드 특성에서 비롯됩니다. 주요 시설 고객은 전 세계 여러 지역에서 제공되는 퍼블릭 및 프라이빗 엔드포인트를 통해 RESTful API를 사용하여 AWS 클라우드와 상호 작용합니다. 고객은 AWS 자격 증명을 사용하여 이러한 API에 액세스할 수 있습니다. 온프레미스 액세스 제어와 달리, 이러한 자격 증명은 네트워크 또는 Microsoft Active Directory 도메인에 반드시 구속되지 않습니다. 자격 증명은 대신 AWS 계정 내의 IAM 위탁자와 연결됩니다. 이러한 API 엔드포인트는 회사 네트워크 외부에서 액세스할 수 있으므로 예상 네트워크 또는 지역 외부에서 자격 증명이 사용되는 인시던트에 대응할 때 이해해야 할 중요한 사항입니다.

AWS의 API 기반 특성으로 인해 보안 이벤트에 대응하는 데 중요한 로그 소스는 AWS 계정에서 이루어진 관리 API 직접 호출을 추적하고 API 직접 호출의 소스 위치에 대한 정보를 찾을 수 있는 AWS CloudTrail입니다.

차이 4: 클라우드의 동적 특성

클라우드는 동적이므로 리소스를 빠르게 생성하고 삭제할 수 있습니다. 오토 스케일링을 사용하면 트래픽 증가에 따라 리소스를 스핀 업하고 스핀 다운할 수 있습니다. 수명이 짧은 인프라와 빠른 변경으로 인해 조사 중인 리소스가 더 이상 존재하지 않거나 수정되었을 수 있습니다. AWS 리소스의 임시 특성과 AWS 리소스 생성 및 삭제를 추적하는 방법을 이해하는 것이 인시던트 분석에 중요합니다. AWS Config를 사용하여 AWS 리소스의 구성 기록을 추적할 수 있습니다.

차이 5: 데이터 액세스

클라우드에서는 데이터 액세스도 다릅니다. 보안 조사에 필요한 데이터를 수집하기 위해 서버에 연결할 수 없습니다. 데이터는 유선 및 API 직접 호출을 통해 수집됩니다. 이러한 변화에 대비하려면 API를 통해 데이터를 수집하는 방법을 연습하고 이해해야 하며, 효과적인 수집 및 액세스를 위해 적절한 스토리지를 확인해야 합니다.

차이 6: 자동화의 중요성

고객이 클라우드 채택의 이점을 완전히 실현하려면 운영 전략에 자동화가 포함되어야 합니다. 코드형 인프라(IaC)는 AWS CloudFormation이나 타사 솔루션과 같은 기본 IaC 서비스에서 지원하는 코드를 사용하여 AWS 서비스를 배포, 구성, 재구성 및 폐기하는 매우 효율적인 자동화 환경의 패턴입니다. 이를 통해 인시던트 대응 구현이 고도로 자동화되며, 특히 증거를 처리할 때 인적 실수를 방지하는 데 유리합니다. 자동화는 온프레미스에서 사용되지만 AWS 클라우드에서는 더 간단하고 필수적입니다.

이러한 차이 해소

이러한 차이를 해소하려면 다음 섹션에 설명된 단계에 따라 사람, 프로세스 및 기술 전반의 인시던트 대응 프로그램이 잘 준비되었는지 확인합니다.

준비

인시던트 대비는 시기적절하고 효과적인 인시던트 대응을 위해 매우 중요합니다. 준비는 세 가지 영역에서 이루어집니다.

- 사람 - 보안 인시던트에 대비하려면 인시던트 대응을 위한 관련 이해관계자를 식별하고 인시던트 대응 및 클라우드 기술에 대해 교육해야 합니다.
- 프로세스 - 보안 인시던트에 대비하여 프로세스를 준비하려면 아키텍처 문서화, 철저한 인시던트 대응 계획 개발, 보안 이벤트에 대한 일관된 대응을 위한 플레이북 작성이 포함됩니다.
- 기술 - 보안 인시던트에 대비한 기술 준비에는 액세스 설정, 필요한 로그 집계 및 모니터링, 효과적인 알림 메커니즘 구현, 대응 및 조사 기능 개발이 포함됩니다.

이러한 각 영역은 효과적인 인시던트 대응을 위해 동일하게 중요합니다. 이 세 가지가 모두 없으면 인시던트 대응 프로그램이 완전하거나 효과적이지 않습니다. 인시던트에 대비하려면 긴밀한 통합을 통해 직원, 프로세스 및 기술을 준비해야 합니다.

사람

보안 이벤트에 대응하려면 보안 이벤트에 대한 대응을 지원할 이해관계자를 식별해야 합니다. 또한 효과적인 대응을 위해서는 이해관계자를 대상으로 AWS 기술과 AWS 환경에 대한 교육을 실시하는 것이 중요합니다.

역할과 책임 정의

보안 이벤트를 처리하려면 조직 간 규율과 행동 성향이 필요합니다. 조직 구조 내에는 인사(HR) 담당자, 경영진, 법무 담당자와 같이 인시던트 발생 시 책임이 있거나(Responsible) 책임을 지거나(Accountable) 자문을 받거나(Consulted) 최신 정보를 제공받는(Informed) 사람들이 많이 있어야 합니다. 이러한 역할 및 책임과 제3자가 개입해야 하는지 여부를 고려합니다. 많은 지역에 해야 할 일과 하지 말아야 할 일을 규정하는 현지 법률이 있습니다. 보안 대응 계획을 위해 RACI(Responsible, Accountable, Consulted, Informed) 차트를 작성하는 것이 불필요해 보일 수 있지만, 그렇게 하면 신속하고 직접적인 커뮤니케이션이 가능하고 이벤트의 여러 단계에서 리더십의 윤곽을 명확하게 파악할 수 있습니다.

인시던트 발생 시 영향을 받는 애플리케이션 및 리소스의 소유자/개발자를 포함하는 것이 중요합니다. 이들은 영향을 측정하는 데 도움이 되는 정보와 컨텍스트를 제공할 수 있는 분야별 전문가(SME)이기 때문입니다. 개발자 및 애플리케이션 소유자의 인시던트 대응 전문 지식에 의존하기 전에 이들과 함께 연습하고 관계를 구축해야 합니다. 클라우드 관리자 또는 엔지니어와 같은 애플리케이션 소유자 또는 SME는 환경이 익숙하지 않거나 복잡하거나 대응자가 액세스할 수 없는 상황에서 조치를 취해야 할 수 있습니다.

마지막으로 신뢰할 수 있는 관계는 추가적인 전문 지식과 가치 있는 조사를 제공할 수 있으므로 조사 또는 대응에 참여할 수 있습니다. 팀에 이러한 기술이 없다면 외부 담당자를 고용하여 도움을 받는 것이 좋습니다.

인시던트 대응 직원 교육

인시던트 대응 직원을 대상으로 조직에서 사용하는 기술에 대한 교육을 실시하는 것은 보안 이벤트에 적절하게 대응하는 데 매우 중요합니다. 직원이 기본 기술을 이해하지 못하면 대응이 늦어질 수 있습니다. 기존의 인시던트 대응 개념 외에도 AWS 서비스와 AWS 환경을 이해하는 것도 중요합니다. 온라인 교육 및 강의실 교육 등 인시던트 직원을 교육하는 데는 여러 가지 전통적인 메커니즘이 있습니다. 또한 교육 메커니즘으로 게임데이 또는 시뮬레이션을 실행하는 것도 고려해야 합니다. 시뮬레이션을 실

행하는 방법에 대한 자세한 내용은 이 문서의 the section called “정기 시뮬레이션 실행” 섹션을 참조하세요.

AWS 클라우드 기술 이해

종속성을 줄이고 대응 시간을 줄이려면 보안 팀과 대응 담당자가 클라우드 서비스에 대한 교육을 받고 조직에서 사용하는 특정 클라우드 환경에서 실습할 기회를 얻어야 합니다. 인시던트 대응 담당자가 효과적으로 대응하려면 AWS 파운데이션, IAM, AWS Organizations, AWS 로깅 및 모니터링 서비스, AWS 보안 서비스를 이해하는 것이 중요합니다.

AWS는 AWS 보안 및 모니터링 서비스에 대한 실습 경험을 얻을 수 있는 온라인 보안 워크숍(AWS 보안 워크숍 참조)을 제공합니다. 또한 AWS는 디지털 교육, 강의실 교육, AWS 교육 파트너 및 인증을 통해 다양한 교육 옵션과 학습 경로를 제공합니다. 자세한 내용은 AWS 교육 및 자격증을 참조하세요.

AWS는 여러 페르소나와 중점 영역을 지원하는 무료 교육과 구독 기반 교육을 모두 제공합니다. 자세한 내용은 AWS Skillbuilder를 참조하세요.

AWS 환경 이해

AWS 서비스와 그 사용 사례, 그리고 서비스 간의 통합 방식을 이해하는 것 외에도, 조직의 AWS 환경이 실제로 어떻게 설계되었는지, 어떤 운영 프로세스가 마련되어 있는지 이해하는 것도 마찬가지로 중요합니다. 이러한 내부 지식은 문서화되지 않고 소수의 영역 전문가만 이해하는 경우가 많기 때문에 종속성이 발생하고 혁신을 저해하며 대응 시간이 느려질 수 있습니다.

이러한 종속성을 방지하고 대응 시간을 단축하려면 보안 분석가가 AWS 환경에 대한 내부 지식을 문서화하고, 액세스하고, 이해할 수 있어야 합니다. 클라우드의 전체 현황을 파악하려면 관련 보안 이해 관계자와 클라우드 관리자 간 협업이 필요합니다. 인시던트 대응을 위한 프로세스를 준비하는 작업에는 아키텍처 다이어그램 문서화와 중앙 중앙화가 포함되는데, 이에 대한 내용은 이 백서 뒷부분의 the section called “아키텍처 다이어그램 문서화 및 중앙 집중화”에 나와 있습니다. 하지만 사람의 관점에서 보면 분석가가 AWS 환경과 관련된 다이어그램과 운영 프로세스에 액세스하고 이해할 수 있는 것이 중요합니다.

AWS 대응 팀 및 지원 이해

지원

지원는 다양한 플랜을 제공합니다. 이러한 플랜을 통해 AWS 솔루션의 성공과 운영 상태를 지원하는 도구 및 전문 지식에 액세스할 수 있습니다. AWS 환경을 계획, 배포, 최적화하는 데 도움이 되는 기술 지원 및 추가 리소스가 필요한 경우 AWS 사용 사례에 가장 적합한 지원 플랜을 선택할 수 있습니다.

AWS Management Console의 지원 센터(로그인이 필요함)를 AWS 리소스에 영향을 미치는 문제에 대한 지원을 받을 수 있는 중앙 연락 창구로 고려하세요. 지원에 대한 액세스는 IAM으로 제어됩니다. AWS Support 기능에 액세스하는 방법에 대한 자세한 내용은 Getting started with 지원를 참조하세요.

또한 침해를 보고해야 하는 경우 AWS 신뢰 안전 팀에 문의하세요.

Security Incident Response 엔지니어

Security Incident Response 엔지니어는 상시 운영되는 전문 글로벌 AWS 팀으로, AWS 공동 책임 모델의 고객 측에서 활성 보안 이벤트가 진행되는 동안 고객에게 지원을 제공합니다.

Security Incident Response 엔지니어의 지원을 받으면 AWS에서 활성 보안 이벤트에 대한 분류 및 복구에 대한 지원을 받게 됩니다. 팀은 AWS 서비스 로그를 사용하여 근본 원인 분석을 지원하고 복구를 위한 권장 사항을 제공할 수 있습니다. 또한 향후 보안 이벤트를 방지하는 데 도움이 되는 보안 권장 사항 및 모범 사례를 제공합니다.

AWS 고객은 AWS 지원 사례를 통해 Security Incident Response 엔지니어를 참여시킬 수 있습니다.

- 모든 고객:
  1. 계정 및 청구(Account and billing)
  2. 서비스: 계정
  3. 범주: 보안
  4. 심각도: 일반 질문

- Developer 지원 플랜을 사용하는 고객:
  1. 계정 및 청구(Account and billing)
  2. 서비스: 계정
  3. 범주: 보안
  4. 심각도: 중요 질문

- Business 지원 플랜을 사용하는 고객:
  1. 계정 및 청구(Account and billing)
  2. 서비스: 계정
  3. 범주: 보안
  4. 심각도: 비즈니스에 영향을 미치는 긴급한 질문

- Enterprise 지원 플랜을 사용하는 고객:
  1. 계정 및 청구(Account and billing)
  2. 서비스: 계정
  3. 범주: 보안
  4. 심각도: 중요한 비즈니스 위험 질문

- AWS 보안 인시던트 대응 구독을 사용하는 고객: https://console.aws.amazon.com/security-ir/에서 Security Incident Response 콘솔을 엽니다.

DDoS 대응 지원

AWS는 AWS Shield를 제공합니다. 이 서비스는 AWS에서 실행되는 웹 애플리케이션을 보호하는 관리형 분산 서비스 거부(DDoS) 보호 서비스입니다. AWS Shield는 상시 탐지 및 자동 인라인 완화 기능을 제공하여 애플리케이션 가동 중지 시간과 지연 시간을 최소화하므로, DDoS 보호 혜택을 받기 위해 지원에 문의할 필요가 없습니다. AWS Shield에는 Shield Standard와 Shield Advanced, 두 가지 계층이 있습니다. 이 두 티어의 차이점에 대해 알아보려면 Shield 기능 설명서를 참조하세요.

AWS Managed Services(AMS)

AWS Managed Services(AMS)에서는 AWS 인프라를 지속적으로 관리하므로 사용자는 애플리케이션에 집중할 수 있습니다. 인프라를 유지 관리하기 위한 모범 사례를 구현함으로써 AMS는 운영 오버헤드와 위험을 줄이도록 지원합니다. AMS는 변경 요청, 모니터링, 패치 관리, 보안, 백업 서비스 등과 같은 일반적인 활동을 자동화하고 인프라를 프로비저닝, 운영 및 지원하기 위한 전체 수명 주기 서비스를 제공합니다.

AMS는 일련의 보안 탐지 제어를 배포하고 알림에 대한 일차 대응을 상시 제공합니다. 경고가 시작되면 AMS는 일련의 표준 자동 및 수동 플레이북에 따라 일관된 응답을 확인합니다. 이러한 플레이북은 온보딩 중에 AMS 고객과 공유되므로 고객이 AMS를 통해 대응 방안을 개발하고 조정할 수 있습니다.

프로세스

철저하고 명확하게 정의된 인시던트 대응 프로세스를 개발하는 것은 성공적이고 확장 가능한 인시던트 대응 프로그램의 핵심입니다. 보안 이벤트가 발생하면 명확한 단계 및 워크플로가 적시에 대응하는 데 도움이 됩니다. 기존 인시던트 대응 프로세스가 이미 있을 수 있습니다. 현재 상태에 관계없이 인시던트 대응 프로세스를 정기적으로 업데이트, 반복, 테스트하는 것이 중요합니다.

인시던트 대응 계획 개발 및 테스트

인시던트 대응을 위해 작성해야 할 첫 번째 문서는 인시던트 대응 계획입니다. 인시던트 대응 계획은 인시던트 대응 프로그램 및 전략의 기초가 되도록 설계되었습니다. 인시던트 대응 계획은 일반적으로 다음 섹션을 포함하는 개요 수준의 문서입니다.

- 인시던트 대응 팀 개요 - 인시던트 대응 팀의 목표와 기능을 간략하게 설명합니다.
- 역할 및 책임 - 인시던트 대응 이해관계자를 나열하고 인시던트 발생 시 해당 이해관계자의 역할을 자세히 설명합니다.
- 커뮤니케이션 계획 - 연락처 정보 및 인시던트 발생 시 커뮤니케이션 방법을 자세히 설명합니다.

  인시던트 커뮤니케이션의 백업으로 대역 외 통신을 사용하는 것이 모범 사례입니다. 안전한 대역 외 통신 채널을 제공하는 애플리케이션의 예는 AWS Wickr입니다.
- 인시던트 대응 단계 및 수행할 조치 - 인시던트 대응의 단계(예: 탐지, 분석, 근절, 방지, 복구)를 열거합니다. 여기에는 해당 단계 내에서 취해야 할 상위 수준 조치가 포함됩니다.
- 인시던트 심각도 및 우선순위 정의 - 인시던트의 심각도를 분류하는 방법, 인시던트의 우선순위를 지정하는 방법, 심각도 정의가 에스컬레이션 절차에 미치는 영향을 자세히 설명합니다.

이러한 섹션은 규모 및 업종이 다른 회사 간에 공통적으로 사용되지만 각 조직의 인시던트 대응 계획은 고유합니다. 조직에 가장 적합한 인시던트 대응 계획을 수립해야 합니다.

아키텍처 다이어그램 문서화 및 중앙 집중화

보안 이벤트에 빠르고 정확하게 대응하려면 시스템과 네트워크가 어떻게 설계되는지 이해해야 합니다. 이러한 내부 패턴을 이해하는 것은 인시던트 대응뿐만 아니라 모범 사례에 따라 패턴이 설계된 애플리케이션 전반의 일관성을 확인하는 데에도 중요합니다. 또한 이 설명서가 최신 상태이고 새 아키텍처 패턴에 따라 정기적으로 업데이트되는지 확인해야 합니다. 다음과 같은 항목을 자세히 설명하는 설명서와 내부 리포지토리를 개발해야 합니다.

- AWS 계정 구조 - 다음을 알아야 합니다.
  - AWS 계정이 몇 개 있나요?
  - 이러한 AWS 계정은 어떻게 구성되나요?
  - AWS 계정의 비즈니스 소유자는 누구인가요?
  - 서비스 제어 정책(SCP)을 사용하시나요? 그렇다면 SCP를 사용하여 구현되는 조직 가드레일은 무엇인가요?
  - 사용할 수 있는 리전과 서비스를 제한하나요?
  - 사업부와 환경(개발/테스트/프로덕션) 간에는 어떤 차이가 있나요?

- AWS 서비스 패턴
  - 어떤 AWS 서비스를 사용하나요?
  - 가장 널리 사용되는 AWS 서비스는 무엇인가요?
- 아키텍처 패턴
  - 어떤 클라우드 아키텍처를 사용하나요?
- AWS 인증 패턴
  - 개발자는 일반적으로 AWS에 어떻게 인증하나요?
  - IAM 역할, 사용자 또는 둘 다 사용하나요? AWS에 대한 인증이 ID 제공업체(idP)에 연결되어 있나요?
  - IAM 역할 또는 사용자를 직원 또는 시스템에 어떻게 매핑하나요?
  - 더 이상 권한이 없는 경우 어떻게 액세스 권한이 취소되나요?
- AWS 권한 부여 패턴
  - 개발자는 어떤 IAM 정책을 사용하나요?
  - 리소스 기반 정책을 사용하시나요?
- 로깅 및 모니터링
  - 어떤 로깅 소스를 사용하며 어디에 저장되나요?
  - AWS CloudTrail 로그를 집계하나요? 그렇다면 어디에 저장되나요?
  - CloudTrail 로그를 쿼리하려면 어떻게 해야 하나요?
  - Amazon GuardDuty를 활성화했나요?
  - GuardDuty 조사 결과(예: 콘솔, 티켓팅 시스템, SIEM)에 액세스하려면 어떻게 해야 하나요?
  - 조사 결과 또는 이벤트가 SIEM에서 집계되나요?
  - 티켓이 자동으로 생성되나요?
  - 조사를 위해 로그를 분석하기 위한 도구에는 어떤 것이 있나요?
- 네트워크 토폴로지
  - 네트워크의 디바이스, 엔드포인트 및 연결은 물리적 또는 논리적으로 어떻게 배열되나요?
  - 네트워크는 AWS와 어떻게 연결되나요?
  - 환경 간에 네트워크 트래픽은 어떻게 필터링되나요?
- 외부 인프라
  - 외부용 애플리케이션은 어떻게 배포되나요?
  - 공개적으로 액세스할 수 있는 AWS 리소스에는 어떤 것이 있나요?
  - 외부로 향하는 인프라가 포함된 AWS 계정에는 어떤 것이 있나요?

- 어떤 DDoS 또는 외부 필터링이 있나요?

내부 기술 다이어그램과 프로세스를 문서화하면 인시던트 대응 분석가의 작업이 쉬워지므로 보안 이벤트에 대응할 수 있는 제도적 지식을 빠르게 얻을 수 있습니다. 내부 기술 프로세스를 철저히 문서화하면 보안 조사가 간소화될 뿐만 아니라 프로세스의 합리화 및 평가에도 도움이 됩니다.

인시던트 대응 개발 플레이북

인시던트 대응 프로세스를 준비하는 데 있어 가장 중요한 부분은 플레이북을 개발하는 것입니다. 인시던트 대응 플레이북은 보안 이벤트가 발생했을 때 따라야 할 일련의 권장 가이드와 단계를 제공합니다. 명확한 구조와 단계를 갖추면 대응 프로세스가 간소화되고 인적 오류의 가능성이 줄어듭니다.

플레이북 작성 대상

다음과 같은 인시던트 시나리오에 대한 플레이북을 만들어야 합니다.

- 예상되는 인시던트 - 예상되는 인시던트에 대한 플레이북을 만들어야 합니다. 여기에는 서비스 거부(DoS), 랜섬웨어, 자격 증명 유출과 같은 위협이 포함됩니다.
- 알려진 보안 조사 결과 또는 알림 - 알려진 보안 조사 결과 및 알림(예: GuardDuty 조사 결과)에 대한 플레이북을 만들어야 합니다. GuardDuty 조사 결과를 받고 '이제 어떡하지?'라고 생각할 수 있습니다. GuardDuty 조사 결과를 잘못 처리하거나 무시하는 것을 방지하려면 잠재적인 GuardDuty 조사 결과에 대한 플레이북을 만드세요. 일부 수정 세부 사항과 지침은 GuardDuty 설명서에 나와 있습니다. GuardDuty는 기본적으로 활성화되어 있지 않으며 사용 시 별도의 비용이 발생한다는 점에 유의하세요. GuardDuty에 대한 자세한 내용은 부록 A: 클라우드 기능 정의 - the section called “가시성 및 알림”에서 확인할 수 있습니다.

플레이북 포함 대상

플레이북에는 보안 분석가가 잠재적인 보안 인시던트를 적절히 조사하고 대응하기 위해 완료해야 할 기술 단계가 포함되어야 합니다.

플레이북에 포함할 항목은 다음과 같습니다.

- 플레이북 개요 - 이 플레이북은 어떤 위험 또는 인시던트 시나리오를 다루고 있나요? 플레이북의 목표는 무엇인가요?
- 사전 조건 - 이 인시던트 시나리오에 어떤 로그 및 탐지 메커니즘이 필요한가요? 예상되는 알림은 무엇인가요?
- 이해관계자 정보 - 관련자는 누구이며 연락처 정보는 어떻게 되나요? 관련된 각 이해관계자의 책임은 무엇인가요?

- 대응 단계 - 인시던트 대응 단계 전반에서 어떤 전술적 단계를 수행해야 하나요? 분석가는 어떤 쿼리를 실행해야 하나요? 원하는 결과를 얻으려면 어떤 코드를 실행해야 하나요?
  - 탐지 - 어떻게 인시던트를 탐지하나요?
  - 분석 - 어떻게 영향 범위를 결정하나요?
  - 격리 - 범위를 제한하기 위해 어떻게 인시던트를 격리하나요?
  - 근절 - 환경에서 위협을 어떻게 제거하나요?
  - 복구 - 영향을 받은 시스템이나 리소스를 어떻게 프로덕션 환경으로 복구하나요?
- 예상 결과 - 쿼리와 코드가 실행된 후 플레이북의 예상 결과는 무엇인가요?

각 플레이북에서 일관된 정보를 확인하려면 다른 보안 플레이북에서 사용할 플레이북 템플릿을 생성하는 것이 유용할 수 있습니다. 이해관계자 정보와 같이 이전에 나열된 항목 중 일부를 여러 플레이북에서 공유할 수 있습니다. 그렇다면 해당 정보에 대한 중앙 집중식 문서를 만들고 플레이북에서 참조한 다음 플레이북에 명확한 차이점을 열거할 수 있습니다. 이렇게 하면 모든 개별 플레이북에서 동일한 정보를 업데이트할 필요가 없습니다. 플레이북에서 템플릿을 만들고 공통적이거나 공유되는 정보를 식별하면 플레이북 개발을 간소화하고 가속화할 수 있습니다. 마지막으로, 플레이북은 시간이 지남에 따라 진화할 가능성이 높으며, 단계가 일관성이 있음이 확인되면 자동화를 위한 요구 사항이 형성됩니다.

샘플 플레이북

부록 B의 the section called “플레이북 리소스”에서 여러 가지 샘플 플레이북을 찾을 수 있습니다. 여기의 예시는 어떤 플레이북을 만들어야 하는지, 플레이북에 무엇을 포함해야 하는지에 대한 지침을 제공하는 데 도움이 될 수 있습니다. 그러나 비즈니스와 가장 관련성 있는 위험을 통합한 플레이북을 만드는 것이 중요합니다. 플레이북 내의 단계와 워크플로에 기술과 프로세스가 포함되어 있는지 확인해야 합니다.

정기 시뮬레이션 실행

조직은 시간이 지남에 따라 성장하고 진화하며, 위협 환경도 마찬가지입니다. 이러한 이유로 인시던트 대응 역량을 지속적으로 검토하는 것이 중요합니다. 이 평가를 수행하는 데 사용할 수 있는 한 가지 방법은 시뮬레이션입니다. 시뮬레이션은 위협 행위자의 전술, 기술 및 절차(TTP)를 모방하도록 설계된 실제 보안 이벤트 시나리오를 사용하며, 이를 통해 조직은 이러한 모의 사이버 이벤트에 실제 상황과 같이 대응하여 인시던트 대응 능력을 발휘하고 평가할 수 있습니다.

시뮬레이션에는 다음과 같은 다양한 이점이 있습니다.

- 사이버 대비 상태를 검증하고 인시던트 대응자의 자신감을 높입니다.
- 도구 및 워크플로의 정확성과 효율성을 테스트합니다.

- 인시던트 대응 계획에 맞춰 커뮤니케이션 및 에스컬레이션 방법을 개선합니다.
- 덜 일반적인 벡터에 대응할 수 있는 기회를 제공합니다.

시뮬레이션 유형

시뮬레이션에는 다음과 같은 세 가지 주요 유형이 있습니다.

- 탁상 연습 - 시뮬레이션에 대한 탁상 접근 방식은 다양한 인시던트 대응 이해관계자가 참여하여 책임진 역할을 연습하고 확립된 커뮤니케이션 도구와 플레이북을 사용하는 토론 기반 세션입니다. 연습은 일반적으로 가상 장소, 실제 장소 또는 이들 장소의 조합에서 하루 종일 수행할 수 있어 언제든 촉진시킬 수 있습니다. 토론을 기반으로 하는 특성상 탁상 연습은 프로세스, 사람, 협업에 중점을 둡니다. 기술은 토론의 핵심 부분이지만 인시던트 대응 도구 또는 스크립트의 실제 사용은 일반적으로 탁상 연습의 일부가 아닙니다.
- 퍼플 팀 연습 - 퍼플 팀 연습은 인시던트 대응 담당자(블루 팀)와 시뮬레이션된 위협 행위자(레드 팀) 간의 협업 수준을 높입니다. 블루 팀은 보안 운영 센터(SOC)의 직원으로 구성되지만 실제 사이버 이벤트 중에 관여하게 될 다른 이해관계자들도 포함될 수 있습니다. 레드 팀은 대개 보안 공격 교육을 받은 침투 테스트 팀 또는 주요 이해관계자로 구성됩니다. 레드 팀은 시나리오를 설계할 때 연습 진행자와 협력하여 시나리오가 정확하고 실현 가능한지 확인합니다. 퍼플 팀 연습에서는 인시던트 대응 작업을 지원하는 탐지 메커니즘, 도구 및 표준 운영 절차(SOP)에 주로 초점을 맞춥니다.
- 레드 팀 연습 - 레드 팀 연습 중에 공격 팀(레드 팀)은 미리 정해진 범위에서 특정 목표 또는 일련의 목표를 달성하기 위해 시뮬레이션을 수행합니다. 방어 팀(블루 팀)은 훈련의 범위와 기간을 꼭 알 필요가 없습니다. 이를 모르면 실제 인시던트에 어떻게 대응하는지에 대한 더 현실적인 평가를 받을 수 있습니다. 레드 팀 연습은 침습적 테스트일 수 있으므로 주의가 필요하고 해당 연습이 환경에 실제로 해를 끼치지 않는지 확인하기 위한 관리 조치를 취해야 합니다.

> **Note**
>
> AWS에서는 고객이 퍼플 팀이나 레드 팀 훈련을 실시하기 전에 침투 테스트 웹 사이트에서 제공하는 침투 테스트 정책을 검토하도록 요구합니다.

표 1에는 이러한 유형의 시뮬레이션의 몇 가지 주요 차이점이 요약되어 있습니다. 일반적으로 이러한 정의는 포괄적인 정의로 간주되며 조직의 요구 사항에 맞게 사용자 지정할 수 있다는 점에 유의해야 합니다.

표 1 - 시뮬레이션 유형

	테이블탑 연습	퍼플 팀 연습	레드 팀 연습
요약	특정 보안 인시던트 시나리오 하나에 초점을 맞춘 종이 기반 연습. 이는 개괄적 또는 기술적일 수 있으며 일련의 종이 주입을 통해 구동됩니다.	테이블탑 연습에 비해 더 사실적인 오퍼링. 퍼플 팀 연습 중 진행자는 참가자와 협력하여 연습 참여를 높이고 필요한 경우 훈련을 제공합니다.	일반적으로 보다 진보된 시뮬레이션 오퍼링. 일반적으로 비밀 유지 수준이 높아서 참가자들이 연습의 모든 세부 사항을 알지 못할 수도 있습니다.
필요 리소스	제한된 기술 리소스 필요	다양한 이해관계자와 높은 수준의 기술 리소스 필요	다양한 이해관계자와 높은 수준의 기술 리소스 필요
복잡성	낮음	중간	높음

정기적으로 사이버 시뮬레이션을 진행하는 것이 좋습니다. 각 연습 유형에는 참가자와 조직 전체에 대한 고유한 이점이 있으므로 덜 복잡한 시뮬레이션 유형(예: 탁상 연습)에서 시작하여 더 복잡한 시뮬레이션 유형(레드 팀 연습)으로 진행할 수 있습니다. 보안 성숙도, 리소스, 원하는 성과에 따라 시뮬레이션 유형을 선택해야 합니다. 일부 고객은 복잡성과 비용 때문에 레드 팀 연습을 선택하지 않을 수 있습니다.

연습 수명 주기

선택한 유형에 관계없이 시뮬레이션은 일반적으로 다음 단계를 따릅니다.

1. 핵심 연습 요소 정의 - 시뮬레이션의 시나리오와 목표를 정의합니다. 이 두 가지 모두 리더의 승인을 받아야 합니다.
2. 주요 이해관계자 식별 - 연습에는 최소한 연습 진행자와 참가자가 필요합니다. 시나리오에 따라 법무, 커뮤니케이션 또는 경영진과 같은 추가 이해관계자가 참여할 수 있습니다.
3. 시나리오 구축 및 테스트 - 특정 요소가 실현 가능하지 않은 경우 구축 중인 시나리오를 재정의해야 할 수 있습니다. 이 단계의 결과로 최종 시나리오가 도출될 것으로 예상됩니다.
4. 시뮬레이션 촉진 - 시뮬레이션 유형에 따라 어떤 방법으로 촉진시킬지 결정됩니다(종이를 사용한 시나리오 또는 고도로 기술적인 시뮬레이션 시나리오). 진행자는 연습 목표에 맞게 촉진 전략을 조정해야 하며 가능한 한 모든 연습 참가자를 참여시켜 최대한의 이점을 확보해야 합니다.

5. 사후 조치 보고서(AAR) 개발 - 잘 운영된 영역, 개선이 필요한 영역, 잠재적인 격차를 식별합니다. AAR은 시뮬레이션의 효과와 시뮬레이션된 이벤트에 대한 팀의 반응을 측정하여 향후 시뮬레이션을 통해 시간의 흐름에 따른 진행 상황을 추적할 수 있도록 해야 합니다.

기술

보안 인시던트 전에 적절한 기술을 개발하고 구현하면 인시던트 대응 직원이 조사하고, 범위를 이해하고, 적시에 조치를 취할 수 있습니다.

AWS 계정 구조 개발

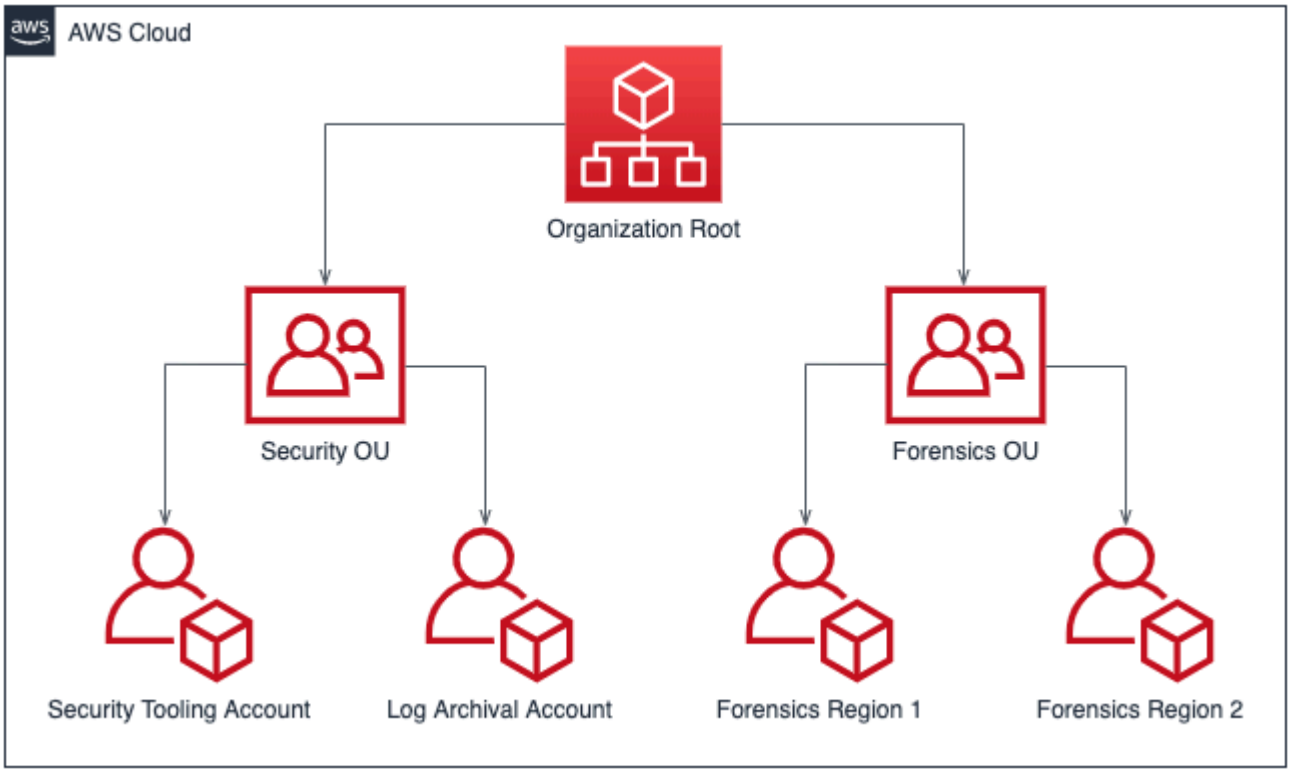
AWS Organizations는 AWS 리소스의 성장과 규모 조정에 따라 AWS 환경을 중앙에서 관리하고 제어할 수 있도록 도와줍니다. AWS 조직은 AWS 계정을 통합하여 단일 단위로 관리할 수 있도록 합니다. 조직 단위(OU)를 사용하면 계정을 그룹으로 만들어 단일 유닛으로 관리할 수 있습니다.

인시던트 대응에는 보안 OU 및 포렌식 OU를 포함하는 인시던트 대응 기능을 지원하는 AWS 계정 구조를 갖는 것이 도움이 됩니다. 보안 OU 내에는 다음에 대한 계정이 있어야 합니다.

- 로그 아카이브 - 로그 아카이브 AWS 계정의 로그를 집계합니다.
- 보안 도구 - 보안 도구 AWS 계정에서 보안 서비스를 중앙 집중화합니다. 이 계정은 보안 서비스에 대한 위임된 관리자 역할을 합니다.

포렌식 OU 내에서, 비즈니스와 운영 모델에 가장 적합한 것에 따라 운영하는 각 리전에 대해 단일 포렌식 계정 또는 여러 개의 계정을 구현할 수 있는 옵션이 있습니다. 리전별 계정 접근 방식의 예로 미국 동부(버지니아 북부)(us-east-1)와 미국 서부(오리건)(us-west-2)에서만 운영하는 경우 포렌식 OU에는 us-east-1용 계정과 us-west-2용 계정의 두 계정이 있습니다. 새 계정을 프로비저닝하는 데는 시간이 걸리므로, 인시던트 발생 훨씬 전에 포렌식 계정을 생성하고 계측하여 대응 담당자가 대응에 효과적으로 사용할 수 있도록 준비하는 것이 필수적입니다.

다음 다이어그램은 리전별 포렌식 계정이 있는 포렌식 OU를 포함한 샘플 계정 구조를 보여줍니다.



인시던트 대응을 위한 리전별 계정 구조

태그 지정 전략 개발 및 구현

AWS 리소스를 사용하는 비즈니스 사용 사례와 관련 내부 이해관계자에 대한 컨텍스트 정보를 얻는 것은 어려울 수 있습니다. 한 가지 방법은 AWS 리소스에 메타데이터를 할당하고 사용자 정의 키와 값으로 구성되는 태그의 형태를 사용하는 것입니다. 태그를 생성하여 리소스를 목적, 소유자, 환경, 처리되는 데이터 유형 및 기타 원하는 기준에 따라 분류할 수 있습니다.

일관된 태그 전략을 사용하면 AWS 리소스에 대한 컨텍스트 정보를 신속하게 식별할 수 있으므로 대응 시간을 단축할 수 있습니다. 태그는 응답 자동화를 시작하는 메커니즘으로도 사용할 수 있습니다. 태그를 지정할 항목에 대한 자세한 내용은 AWS 리소스 태깅에 대한 설명서를 참조하세요. 먼저 조직 전체에 구현할 태그를 정의하는 것이 좋습니다. 그런 다음 이 태그 지정 전략을 구현하고 적용합니다. 구현 및 시행에 대한 자세한 내용은 AWS 블로그 Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs)를 참조하세요.

AWS 계정 연락처 정보 업데이트

각 AWS 계정에는 정확하고 최신 연락처 정보가 있어야 합니다. 그래야 해당 이해관계자가 보안, 결제, 운영 등의 주제에 대한 AWS의 중요한 알림을 받을 수 있습니다. 각 AWS 계정에는 보안, 결제, 운영을

담당하는 기본 연락처와 대체 연락처가 있습니다. 이러한 연락처 간의 차이점은 AWS 계정 관리 참조 안내서에서 확인할 수 있습니다.

대체 연락처 관리에 대한 자세한 내용은 대체 연락처 추가, 변경 또는 제거에 대한 AWS 설명서를 참조하세요. 팀에서 결제, 운영 및 보안 관련 문제를 관리하는 경우 이메일 배포 목록을 사용하는 것이 가장 좋습니다. 이메일 배포 목록은 부재 또는 퇴사 시 막힘을 유발할 수 있는 한 사람에 대한 종속성을 없앱니다. 또한 전화번호를 포함한 이메일 및 계정 연락처 정보가 루트 계정 암호 재설정 및 다중 인증(MFA) 재설정으로부터 안전하게 보호되는지 확인해야 합니다.

AWS Organizations를 사용하는 고객의 경우 조직 관리자는 각 AWS 계정에 대한 자격 증명 없이 관리 계정 또는 위임 관리자 계정을 사용하여 멤버 계정의 대체 연락처를 중앙에서 관리할 수 있습니다. 또한 새로 생성된 계정에 정확한 연락처 정보가 있는지 확인해야 합니다. Automatically update alternate contacts for newly created AWS 계정 블로그 게시물을 참조하세요.

AWS 계정에 대한 액세스 준비

인시던트 중 인시던트 대응 팀은 인시던트와 관련된 환경과 리소스에 액세스할 수 있어야 합니다. 이벤트가 발생하기 전에 팀이 업무를 수행할 수 있는 적절한 액세스 권한을 가지고 있는지 확인합니다. 이를 위해서는 팀원에게 필요한 액세스 권한 수준(예: 어떤 종류의 작업을 수행할 가능성이 높은지)을 파악하고 최소 권한 액세스 권한을 미리 프로비저닝해야 합니다.

이 액세스를 구현하고 프로비저닝하려면 조직의 클라우드 아키텍트와 함께 AWS 계정 전략 및 클라우드 ID 전략을 식별하고 논의하여 구성된 인증 및 권한 부여 방법을 이해해야 합니다. 이러한 자격 증명의 권한 있는 특성으로 인해 구현의 일부로 승인 흐름을 사용하거나 저장소에서 자격 증명을 검색하는 것을 고려해야 합니다. 구현 후에는 이벤트가 발생하기 전에 팀원의 액세스를 문서화하고 테스트하여 지연 없이 대응할 수 있는지 확인해야 합니다.

마지막으로 보안 인시던트에 대응하기 위해 특별히 생성된 사용자는 충분한 액세스를 제공하기 위해 권한이 부여되는 경우가 많습니다. 따라서 이러한 자격 증명의 사용을 제한 및 모니터링하고, 일상적인 활동에는 사용하지 않아야 합니다.

위협 환경 이해

위협 모델 개발

위협 모델을 개발함으로써 조직은 권한이 없는 사용자보다 먼저 위협을 식별하고 완화책을 마련할 수 있습니다. 위협 모델링에는 다양한 전략과 접근 방식이 있습니다. How to approach threat modeling 블로그 게시물을 참조하세요. 인시던트 대응의 경우 위협 모델은 위협 행위자가 인시던트 중 사용했을 수 있는 공격 벡터를 식별하는 데 도움이 될 수 있습니다. 적시에 대응하기 위해서는 방어 대상을 파악하는 것이 중요합니다. 위협 모델링에 AWS Partner를 사용할 수도 있습니다. AWS 파트너를 검색하려면 AWS Partner Network를 사용합니다.

사이버 위협 인텔리전스 통합 및 사용

사이버 위협 인텔리전스는 위협 행위자의 의도, 기회 및 역량에 대한 데이터와 분석입니다. 위협 인텔리전스를 확보하고 사용하는 것은 인시던트를 조기에 탐지하고 위협 행위자 행동을 더 잘 이해하는 데 유용합니다. 사이버 위협 인텔리전스에는 IP 주소 또는 맬웨어의 파일 해시와 같은 정적 지표가 포함됩니다. 여기에는 행동 패턴, 의도 등의 개요 수준 정보도 포함됩니다. 많은 사이버 보안 벤더와 오픈 소스 리포지토리에서 위협 인텔리전스를 수집할 수 있습니다.

AWS 환경에 대한 위협 인텔리전스를 통합하고 극대화하려면 기본 제공 기능을 사용하고 자체 위협 인텔리전스 목록을 통합합니다. Amazon GuardDuty는 AWS 내부 및 타사 위협 인텔리전스 소스를 사용합니다. DNS 방화벽, AWS WAF 규칙 등의 다른 AWS 서비스도 AWS의 지능형 위협 인텔리전스 그룹으로부터 입력을 받습니다. 일부 GuardDuty 조사 결과는 적의 전술과 기법에 대한 실제 관찰 정보를 제공하는 MITRE ATT&CK 프레임워크에 매핑됩니다.

분석 및 알림을 위한 로그 선택 및 설정

보안 조사 중에 관련 로그를 검토하여 인시던트의 전체 범위와 타임라인을 기록하고 이해할 수 있어야 합니다. 관심 있는 특정 작업이 발생했음을 나타내는 알림 생성에도 로그가 필요합니다. 쿼리 및 검색 메커니즘을 선택, 활성화, 저장 및 설정하고 경보를 설정하는 것이 중요합니다. 이 섹션에서는 이러한 각 작업을 검토합니다. 자세한 내용은 Logging strategies for security incident response AWS 블로그 게시물을 참조하세요.

로그 소스 선택 및 활성화

보안 조사에 앞서 관련 로그를 캡처하여 AWS 계정의 활동을 소급하여 재구성해야 합니다. AWS 계정 워크로드와 관련된 로그 소스를 선택하고 활성화합니다.

AWS CloudTrail은 AWS 서비스 활동을 캡처하는 AWS 계정에 대해 수행된 API 직접 호출을 추적하는 로깅 서비스입니다. AWS Management Console, AWS CLI 또는 AWS SDK를 사용하여 CloudTrail의 이벤트 기록 기능을 통해 검색할 수 있는 관리 이벤트의 90일 보존 기능이 기본적으로 활성화되어 있습니다. 데이터 이벤트를 더 오래 보존하고 가시성을 확보하려면 CloudTrail 트레일을 생성하고 이를 Amazon S3 버킷과 연결하고 선택적으로 Amazon CloudWatch 로그 그룹과 연결해야 합니다. 또는 최대 7년 동안 CloudTrail 로그를 유지하고 SQL 기반 쿼리 기능을 제공하는 CloudTrail Lake를 생성할 수 있습니다.

AWS는 VPC를 사용하는 고객이 각각 VPC 흐름 로그 및 Amazon Route 53 Resolver 쿼리 로그를 사용하여 네트워크 트래픽 및 DNS 로그를 활성화하고 Amazon S3 버킷 또는 CloudWatch 로그 그룹으로 스트리밍할 것을 권장합니다. VPC, 서브넷 또는 네트워크 인터페이스에 대한 VPC 흐름 로그를 생성할 수 있습니다. VPC 흐름 로그의 경우 흐름 로그를 활성화하는 방법과 위치를 선택적으로 지정하여 비용을 절감할 수 있습니다.

AWS CloudTrail 로그, VPC 흐름 로그 및 Route 53 Resolver 쿼리 로그는 AWS에서 보안 조사를 지원하는 기본 로깅 트라이펙터입니다.

AWS 서비스는 Elastic Load Balancing 로그, AWS WAF 로그, AWS Config 레코더 로그, Amazon GuardDuty 조사 결과, Amazon Elastic Kubernetes Service(Amazon EKS) 감사 로그, Amazon EC2 인스턴스 운영 체제 및 애플리케이션 로그와 같은 기본 로그 트라이펙터에서 캡처하지 않는 로그를 생성할 수 있습니다. 로깅 및 모니터링 옵션의 전체 목록은 the section called “부록 A: 클라우드 기능 정의” 섹션을 참조하세요.

로그 스토리지 선택

로그 스토리지의 선택은 일반적으로 사용하는 쿼리 도구, 보존 기능, 친숙도 및 비용과 관련이 있습니다. AWS 서비스 로그를 활성화할 때 스토리지 시설, 일반적으로 Amazon S3 버킷 또는 CloudWatch 로그 그룹을 제공합니다.

Amazon S3 버킷은 선택적 수명 주기 정책을 통해 비용 효과적이고 내구성이 뛰어난 스토리지를 제공합니다. Amazon S3 버킷에 저장된 로그는 Amazon Athena와 같은 서비스를 사용하여 기본적으로 쿼리할 수 있습니다. CloudWatch 로그 그룹은 CloudWatch 로그 인사이트를 통해 내구성이 뛰어난 스토리지와 기본 제공 쿼리 기능을 제공합니다.

적절한 로그 보존 식별

S3 버킷 또는 CloudWatch 로그 그룹을 사용하여 로그를 저장하는 경우 각 로그 소스에 적절한 수명 주기를 설정하여 저장 및 검색 비용을 최적화해야 합니다. 고객은 일반적으로 3개월에서 12개월 사이의 로그를 쉽게 쿼리할 수 있으며 최대 7년 동안 보존할 수 있습니다. 가용성 및 보존에 대한 선택은 보안 요구 사항과 법적, 규제 및 비즈니스 의무의 조합과 일치해야 합니다.

로그에 대한 쿼리 메커니즘 선택 및 구현

AWS에서 로그를 쿼리하는 데 사용할 수 있는 주요 서비스는 CloudWatch 로그 그룹에 저장된 데이터의 경우 CloudWatch Logs Insights, Amazon S3에 저장된 데이터의 경우 Amazon Athena와 Amazon OpenSearch Service입니다. 보안 정보 및 이벤트 관리(SIEM)와 같은 타사 쿼리 도구를 사용할 수도 있습니다.

로그 쿼리 도구를 선택하는 프로세스는 보안 작업의 인력, 프로세스 및 기술 측면을 고려해야 합니다. 운영, 비즈니스 및 보안 요구 사항을 충족하고 장기적으로 액세스 및 유지 관리 가능한 도구를 선택합니다. 로그 쿼리 도구는 스캔할 로그 수가 도구의 한도 내에서 유지될 때 최적으로 작동합니다. 비용이나 기술적 제약으로 인해 고객이 여러 개의 쿼리 도구를 사용하는 경우는 드물지 않습니다. 예를 들어 지난 90일 데이터에 대한 쿼리를 수행할 때는 타사 SIEM을 사용하고, SIEM의 로그 수집 비용으로 인해 90일 이후 데이터에 대한 쿼리를 수행할 때는 Athena를 사용합니다. 구현에 관계없이, 특히 보안 이

벤트 조사 중에 운영 효율성을 극대화하는 데 필요한 도구의 수를 최소화하는 접근 방식인지 확인합니다.

알림에 로그 사용

AWS는 기본적으로 Amazon GuardDuty, AWS Security Hub CSPM, AWS Config와 같은 보안 서비스를 통해 알림을 제공합니다. 이러한 서비스에서 다루지 않는 보안 알림 또는 환경과 관련된 특정 알림에 대해 사용자 지정 알림 생성 엔진을 사용할 수도 있습니다. 이러한 알림과 탐지를 빌드하는 방법은 이 문서의 the section called “탐지” 섹션에서 다룹니다.

포렌식 기능 개발

보안 인시던트에 앞서 보안 이벤트 조사를 지원하기 위한 포렌식 기능을 개발하는 것이 좋습니다. NIST의 Guide to Integrating Forensic Techniques into Incident Response에서 이러한 지침을 제공합니다.

AWS 기반 포렌식

기존 온프레미스 포렌식의 개념이 AWS에 적용됩니다. Forensic investigation environment strategies in the AWS 클라우드 블로그 게시물은 법의학 전문 지식을 AWS로 마이그레이션하는 데 필요한 핵심 정보를 제공합니다.

포렌식을 위한 환경과 AWS 계정 구조를 설정한 후에는 네 단계에 걸쳐 포렌식 방법론을 효과적으로 수행하는 데 필요한 기술을 정의해야 합니다.

- 수집 - AWS CloudTrail, AWS Config, VPC 흐름 로그, 호스트 수준 로그 등 관련 AWS 로그를 수집합니다. 영향을 받은 AWS 리소스의 스냅샷, 백업, 메모리 덤프를 수집합니다.
- 검사 - 관련 정보를 추출하고 평가하여 수집한 데이터를 검사합니다.
- 분석 - 수집된 데이터를 분석하여 인시던트를 이해하고 결론을 도출합니다.
- 보고 - 분석 단계의 결과 정보를 제시합니다.

백업 및 스냅샷 캡처

주요 시스템과 데이터베이스의 백업을 설정하는 것은 보안 인시던트 복구 및 포렌식 용도로 매우 중요합니다. 백업을 설정하면 시스템을 이전의 안전한 상태로 복원할 수 있습니다. AWS에서는 다양한 리소스의 스냅샷을 생성할 수 있습니다. 스냅샷은 해당 리소스의 특정 시점 백업을 제공합니다. 백업 및 복구를 지원할 수 있는 많은 AWS 서비스가 있습니다. 백업 및 복구를 위한 이러한 서비스와 접근 방식에 대한 자세한 내용은 Backup and Recovery Prescriptive Guidance를 참조하세요. 자세한 내용은 Use backups to recover from security incidents 블로그 게시물을 참조하세요.

특히 랜섬웨어와 같은 상황에서는 백업의 보안을 잘 유지하는 것이 중요합니다. 백업 보안을 위한 지침은 Top 10 security best practices for securing backups in AWS 블로그 게시물을 참조하세요. 백업의 보안을 유지하는 것 외에도 정기적으로 백업 및 복원 프로세스를 테스트하여 보유한 기술과 프로세스가 정상적으로 작동하는지 확인해야 합니다.

AWS 기반 포렌식 자동화

보안 이벤트가 발생하는 동안 인시던트 대응 팀은 이벤트와 관련된 기간에 정확성을 유지하면서 증거를 신속하게 수집하고 분석할 수 있어야 합니다. 클라우드 환경, 특히 많은 인스턴스와 계정에서 관련 증거를 수동으로 수집하는 작업은 인시던트 대응 팀에 어렵고 시간이 많이 소요되는 업무입니다. 또한 수작업으로 수집하는 경우 인적 오류가 발생하기 쉽습니다. 이러한 이유로 고객은 포렌식을 위한 자동화를 개발하고 구현해야 합니다.

AWS는 포렌식을 위한 다양한 자동화 리소스를 제공하며, 이는 the section called “포렌식 리소스” 아래 부록에 통합되어 있습니다. 다음은 저희가 개발하고 고객이 구현한 포렌식 패턴의 리소스 예제입니다. 시작하기에 유용한 참조 아키텍처가 될 수 있지만, 환경, 요구 사항, 도구, 포렌식 프로세스에 따라 이를 수정하거나 새로운 포렌식 자동화 패턴을 생성하는 것을 고려하세요.

준비 항목 요약

보안 인시던트에 대응하기 위한 철저한 준비는 시기적절하고 효과적인 인시던트 대응에 매우 중요합니다. 인시던트 대응 준비에는 사람, 프로세스, 기술이 필요합니다. 이 세 가지 영역 모두 인시던트 대응 준비에 있어 똑같이 중요합니다. 세 가지 영역 모두에 걸쳐 인시던트 대응 프로그램을 준비하고 발전시켜야 합니다.

표 2에 이 섹션에서 자세히 설명하는 준비 항목이 요약되어 있습니다.

표 2 - 인시던트 대응 준비 항목

도메인	준비 항목	작업 항목
사람	역할과 책임을 정의합니다.	• 관련 인시던트 대응 이해관계자를 식별합니다. • 인시던트에 대한 RACI(Responsible, Accountable, Consulted, Informed) 차트를 작성합니다.

도메인	준비 항목	작업 항목
사람	인시던트 대응 직원에게 AWS에 대해 교육합니다.	• 인시던트 대응 이해관계자를 대상으로 AWS 파운데이션에 대한 교육을 실시합니다. • 인시던트 대응 이해관계자를 대상으로 AWS 보안 및 모니터링 서비스에 대한 교육을 실시합니다. • 인시던트 대응 이해관계자를 대상으로 AWS 환경과 그 설계 방식에 대한 교육을 실시합니다.
사람	AWS 지원 옵션을 이해합니다.	• AWS Support, Security Incident Response 엔지니어, DDoS 대응 팀(DRT) 및 AMS의 차이를 이해합니다. • 필요한 경우 활성 보안 이벤트 중 Security Incident Response 엔지니어에게 도달하기 위한 분류 및 에스컬레이션 경로를 이해합니다.
프로세스	인시던트 대응 계획을 개발합니다.	• 인시던트 대응 프로그램 및 전략을 정의하는 개요 수준 문서를 생성합니다. • RACI, 커뮤니케이션 계획, 인시던트 정의 및 인시던트 대응 계획에 대한 인시던트 대응 단계를 포함합니다.

도메인	준비 항목	작업 항목
프로세스	아키텍처 다이어그램을 문서화하고 중앙 집중화합니다.	• AWS 환경이 계정 구조, 서비스 사용, IAM 패턴 및 AWS 구성의 기타 핵심 기능에 걸쳐 어떻게 구성되는지에 대한 세부 정보를 문서화합니다. • 클라우드 아키텍처의 아키텍처 다이어그램을 개발합니다.
프로세스	인시던트 대응 플레이북을 개발합니다.	• 플레이북 구조에 대한 템플릿을 만듭니다. • 예상되는 보안 이벤트에 대한 플레이북을 작성합니다. • GuardDuty 조사 결과와 같은 알려진 보안 알림을 위한 플레이북을 작성합니다.
프로세스	정기 시뮬레이션을 실행합니다.	• 인시던트 시뮬레이션을 실행하기 위한 정기적인 주기를 개발합니다. • 얻은 결과와 파악한 내용을 사용하여 인시던트 대응 프로그램을 반복합니다.
기술	AWS 계정 구조를 개발합니다.	• 워크로드를 계정별로 분리하는 방법에 대한 AWS 계정 구조를 계획합니다. • 보안 도구 및 로그 아카이브 계정으로 보안 OU를 생성합니다. • 운영하는 각 리전의 포렌식 계정으로 포렌식 OU를 생성합니다.

도메인	준비 항목	작업 항목
기술	대응 담당자가 조사 결과에 대한 소유권과 컨텍스트를 식별하는 데 도움이 되는 태깅 전략을 개발하고 구현합니다.	• 태깅 전략과 AWS 리소스와 연결할 태그를 계획합니다. • 태깅 전략을 구현하고 적용합니다.
기술	AWS 계정 연락처 정보를 업데이트합니다.	• AWS 계정에 연락처 정보가 나열되어 있는지 확인합니다. • 연락처 정보에 대한 이메일 배포 목록을 생성하여 단일 장애 지점을 제거합니다. • AWS 계정 정보와 연결된 이메일 계정을 보호합니다.
기술	AWS 계정에 대한 액세스를 준비합니다.	• 인시던트 대응에 필요한 액세스 인시던트 대응 담당자를 정의합니다. • 액세스를 구현, 테스트 및 모니터링합니다.
기술	위협 환경을 이해합니다.	• 환경 및 애플리케이션의 위협 모델을 개발합니다. • 사이버 위협 인텔리전스를 통합하고 사용합니다.

도메인	준비 항목	작업 항목
기술	로그를 선택하고 설정합니다.	• 조사를 위한 로그를 식별하고 활성화합니다. • 로그 스토리지를 선택합니다. • 로그 보존을 식별하고 구현합니다. • 로그와 아티팩트를 검색하고 쿼리하는 메커니즘을 개발합니다. • 알림에 로그를 사용합니다.
기술	포렌식 기능을 개발합니다.	• 포렌식 수집에 필요한 아티팩트를 식별합니다. • 주요 시스템의 백업을 캡처하고 보호합니다. • 식별된 로그와 아티팩트 분석을 위한 메커니즘을 정의합니다. • 포렌식 분석을 위한 자동화를 구현합니다.

인시던트 대응 준비에는 반복적인 접근 방식이 권장됩니다. 이러한 모든 준비 항목은 하루아침에 이루어질 수 없으므로 작은 것부터 시작하여 시간이 지나면서 지속적으로 인시던트 대응 능력을 향상시킬 수 있는 계획을 세워야 합니다.

운영

운영은 인시던트 대응 수행의 핵심입니다. 여기서 보안 인시던트 대응 및 해결 조치가 이루어집니다. 운영에는 탐지, 분석, 격리, 근절, 복구와 같은 다섯 가지 단계가 포함됩니다. 이러한 단계 및 목표에 대한 설명은 표 3에 나와 있습니다.

표 3 - 운영 단계

Phase(단계)	목표
탐지	잠재적 보안 이벤트를 파악합니다.
분석	보안 이벤트가 인시던트인지 판단하고 인시던트 범위를 평가합니다.
격리	보안 이벤트의 범위를 최소화하고 제한합니다.
근절	보안 이벤트와 관련된 승인되지 않은 리소스 또는 아티팩트를 제거합니다. 보안 인시던트를 일으킨 완화 조치를 구현합니다.
복구	시스템을 알려진 안전 상태로 복원하고 이러한 시스템을 모니터링하여 위협이 다시 발생하지 않는지 확인합니다.

이 단계는 효과적이고 강력한 방식으로 대응하기 위해 보안 인시던트에 대응하고 이를 운영할 때 지침으로 활용해야 합니다. 실제로 취하는 조치는 인시던트에 따라 달라집니다. 예를 들어 랜섬웨어와 관련된 인시던트는 퍼블릭 Amazon S3 버킷과 관련된 인시던트와는 다른 대응 단계를 따라야 합니다. 또한 이러한 단계가 반드시 순차적으로 발생하는 것은 아닙니다. 격리 및 근절 후에는 분석 작업으로 돌아가 자신의 행동이 효과적이었는지 파악해야 할 수도 있습니다.

탐지

알림은 탐지 단계의 주요 구성 요소로서, 관심 있는 AWS 계정 위협 활동을 기반으로 인시던트 대응 프로세스를 시작하는 알림을 생성합니다.

알림 정확도는 까다롭습니다. 인시던트가 발생했는지, 진행 중인지 또는 향후 발생할지 항상 확실하게 확인할 수 있는 것은 아닙니다. 다음은 몇 가지 이유입니다.

- 탐지 메커니즘은 기준 편차, 알려진 패턴 및 내부 또는 외부 엔터티의 알림을 기반으로 합니다.
- 기술과 사람의 예측할 수 없는 특성, 즉 보안 인시던트의 수단과 행위자 때문에 기준은 시간 경과에 따라 달라집니다. 로그 패턴은 참신하거나 수정된 위협 행위자 전술, 기법 및 절차(TTP)를 통해 나타납니다.
- 사람, 기술 및 프로세스에 대한 변경 사항은 인시던트 대응 프로세스에 즉시 통합되지 않습니다. 일부는 조사 진행 중 발견됩니다.

알림 소스

다음 소스를 사용하여 알림을 정의하는 것을 고려해야 합니다.

- 조사 결과 - Amazon GuardDuty, AWS Security Hub CSPM, Amazon Macie, Amazon Inspector, AWS Config, IAM Access Analyzer, Network Access Analyzer 등의 AWS 서비스는 알림을 생성하는 데 사용할 수 있는 조사 결과를 생성합니다.
- 로그 - Amazon S3 버킷과 CloudWatch 로그 그룹에 저장된 AWS 서비스, 인프라 및 애플리케이션 로그를 구문 분석하고 상호 연관시켜 알림을 생성할 수 있습니다.
- 결제 활동 - 결제 활동이 갑자기 변경되면 보안 이벤트가 발생할 수 있습니다. 이를 모니터링하려면 결제 경보를 생성하여 예상 AWS 요금 모니터링에 대한 설명서를 참조하세요.
- 사이버 위협 인텔리전스 - 타사 사이버 위협 인텔리전스 피드를 구독하는 경우 해당 정보를 다른 로깅 및 모니터링 도구와 상호 연관시켜 이벤트의 잠재적 지표를 식별할 수 있습니다.
- 파트너 도구 - AWS Partner Network(APN)의 파트너는 보안 목표를 달성하는 데 도움이 되는 최상위 제품을 제공합니다. 인시던트 대응의 경우 엔드포인트 탐지 및 대응(EDR) 또는 SIEM이 있는 파트너 제품은 인시던트 대응 목표를 지원하는 데 도움이 될 수 있습니다. 자세한 내용은 보안 파트너 솔루션과 Security Solutions in the AWS Marketplace를 참조하세요.
- AWS 신뢰 및 안전 - 부적절하거나 악의적인 활동을 발견할 경우 지원에서 고객에게 연락할 수 있습니다.
- 일회성 연락 - 조직 내의 고객, 개발자 또는 기타 직원이 비정상적인 상황을 발견할 수 있으므로 보안 팀에 연락할 수 있는 잘 알려져 있고 널리 알려진 방법을 마련하는 것이 중요합니다. 인기 있는 선택 사항에는 티켓팅 시스템, 담당자 이메일 주소 및 웹 양식이 포함됩니다. 조직에서 일반 대중과 함께 일하는 경우에는 대민 보안 연락 메커니즘이 필요할 수도 있습니다.

조사 중 사용할 수 있는 클라우드 기능에 대한 자세한 내용은 이 설명서의 the section called “부록 A: 클라우드 기능 정의” 섹션을 참조하세요.

보안 제어 엔지니어링의 일부인 탐지

탐지 메커니즘은 보안 제어 개발의 중요한 부분입니다. 지시적 및 예방적 제어가 정의되면 관련 탐지 및 대응 제어를 구성해야 합니다. 예를 들어 조직에서 AWS 계정의 루트 사용자와 관련된 지시어 제어를 설정하는 경우, 이 지시어는 매우 잘 정의된 특정 활동에 대해서만 사용해야 합니다. 이를 조직의 AWS 서비스 제어 정책(SCP)을 사용하여 구현된 예방 제어와 연결합니다. 예상 기준을 초과하는 루트 사용자 활동이 발생하면 EventBridge 규칙 및 SNS 주제로 구현된 탐지 제어가 보안 운영 센터(SOC)에 알립니다. 대응 제어는 SOC가 적절한 플레이북을 선택하고, 분석을 수행하고, 인시던트가 해결될 때까지 작업하는 것을 의미합니다.

보안 제어는 AWS에서 실행되는 워크로드의 위협 모델링을 통해 가장 잘 정의됩니다. 탐지 제어의 중요도는 특정 워크로드에 대한 비즈니스 영향 분석(BIA)을 검토하여 설정됩니다. 탐지 제어에 의해 생성된 알림은 들어오는 대로 처리되지 않고 초기 중요도에 따라 분석 중 조정됩니다. 초기 중요도 세트는 우선순위를 정하는 데 도움이 됩니다. 알림이 발생한 상황에 따라 실제 중요도가 결정됩니다. 예를 들어 조직은 워크로드의 일부인 EC2 인스턴스에 사용되는 탐지 제어의 구성 요소로 Amazon GuardDuty를 사용합니다. 조사 결과 `Impact:EC2/SuspiciousDomainRequest.Reputation`이 생성되어 워크로드 내에 나열된 Amazon EC2 인스턴스가 악성으로 의심되는 도메인 이름을 쿼리하고 있음을 알려줍니다. 이 알림은 기본적으로 낮은 심각도로 설정되며, 분석 단계가 진행됨에 따라 권한이 없는 행위자가 `p4d.24xlarge` 유형의 EC2 인스턴스를 수백 개 배포하여 조직의 운영 비용을 크게 높인 것으로 확인되었습니다. 이 시점에서 인시던트 대응 팀은 이 알림의 중요도를 높음으로 조정하여 긴급성을 높이고 추가 조치를 신속하게 진행하기로 결정합니다. GuardDuty 조사 결과 심각도는 변경할 수 없습니다.

탐지 제어 구현

탐지 제어는 특정 이벤트에 대해 알림이 사용되는 방식을 결정하는 데 도움이 되므로 그 구현 방식을 이해하는 것이 중요합니다. 기술적 탐지 제어에는 두 가지 주요 구현이 있습니다.

- 동작 탐지는 일반적으로 기계 학습(ML) 또는 인공 지능(AI)이라고 하는 수학적 모델에 의존합니다. 탐지는 추론을 통해 이루어지므로 알림에 실제 이벤트가 반드시 반영되지는 않을 수 있습니다.
- 규칙 기반 탐지는 결정적입니다. 고객은 알림을 받을 활동의 정확한 파라미터를 설정할 수 있으며, 이는 확실합니다.

침입 탐지 시스템(IDS)과 같은 탐지 시스템의 최신 구현에는 일반적으로 두 메커니즘이 모두 함께 제공됩니다. 다음은 GuardDuty를 사용한 규칙 기반 및 동작 탐지의 몇 가지 예입니다.

- `Exfiltration:IAMUser/AnomalousBehavior`라는 조사 결과가 생성될 때 이는 '계정에서 변칙적인 API 요청이 관찰되었음'을 알려줍니다. 설명서를 자세히 살펴보면 "ML 모델은 계정의 모든 API 요청을 평가하고 공격자가 사용하는 기법과 관련된 이상 이벤트를 식별합니다."라는 내용이 있는데, 이는 이 조사 결과가 행동 특성을 가지고 있을 나타냅니다.
- 조사 결과 `Impact:S3/MaliciousIPCaller`의 경우 GuardDuty는 CloudTrail의 Amazon S3 서비스에서 API 직접 호출을 분석하여 `SourceIPAddress` 로그 요소를 위협 인텔리전스 피드가 포함된 퍼블릭 IP 주소 테이블과 비교합니다. 항목과 직접 일치하는 항목을 찾으면 조사 결과가 생성됩니다.

위협 모델 내의 모든 활동에 대해 규칙 기반 알림을 구현하는 것이 항상 가능한 것은 아니므로 동작 기반 알림과 규칙 기반 알림을 모두 혼합하여 구현하는 것이 좋습니다.

사람 기반 탐지

지금까지 기술 기반 탐지에 대해 설명했습니다. 다른 중요한 탐지 소스는 고객 조직 내부 또는 외부의 사람들로부터 비롯됩니다. 내부자는 직원 또는 계약자로 정의할 수 있으며, 외부자는 보안 연구원, 법 집행 기관, 뉴스, 소셜 미디어와 같은 엔터티입니다.

기술 기반 탐지는 체계적으로 구성할 수 있지만 사람 기반 탐지는 이메일, 티켓, 메일, 뉴스 게시물, 전화 통화, 대면 상호 작용과 같은 다양한 형태로 제공됩니다. 기술 기반 탐지 알림은 거의 실시간으로 전달될 것으로 예상할 수 있지만 사람 기반 탐지에 대한 타임라인 기대치는 없습니다. 보안 문화에서는 보안에 대한 심층적 방어 접근 방식을 위해 사람 기반의 탐지 메커니즘을 통합하고, 촉진하고, 강화하는 것이 필수적입니다.

요약

탐지를 통해 규칙 기반 알림과 동작 기반 알림을 혼합하는 것이 중요합니다. 또한 내부와 외부 모두에서 보안 문제에 대한 티켓을 제출할 수 있는 메커니즘이 있어야 합니다. 인간은 보안 이벤트의 가장 중요한 소스 중 하나일 수 있으므로 사람들이 우려 사항을 에스컬레이션할 수 있도록 프로세스를 마련하는 것이 중요합니다. 환경의 위협 모델을 사용하여 탐지 구축을 시작해야 합니다. 위협 모델은 환경과 가장 관련성이 높은 위협을 기반으로 알림을 구축하는 데 도움이 됩니다. 마지막으로, 위협 행위자의 전술, 기법 및 절차(TTP)를 이해하기 위해 MITRE ATT&CK와 같은 프레임워크를 사용할 수 있습니다. MITRE ATT&CK 프레임워크는 다양한 탐지 메커니즘에서 공통 언어로 사용하는 데 유용할 수 있습니다.

분석

로그, 쿼리 기능 및 위협 인텔리전스는 분석 단계에 필요한 몇 가지 지원 구성 요소입니다. 탐지에 사용되는 것과 동일한 많은 로그가 분석에도 사용되며 쿼리 도구의 온보딩 및 구성이 필요합니다.

알림의 영향 검증, 범위 지정 및 평가

분석 단계에서는 알림을 검증하고, 범위를 정의하고, 가능한 침해의 영향을 평가하기 위해 포괄적인 로그 분석을 수행합니다.

- 알림 검증은 분석 단계의 진입점입니다. 인시던트 대응 담당자는 다양한 소스에서 로그 항목을 찾고 영향을 받는 워크로드의 소유자와 직접 소통합니다.
- 범위 지정은 이해관계자가 오탐 가능성이 낮다는 데 동의한 후 관련된 모든 리소스를 목록화하고 알림의 중요도를 조정하는 다음 단계입니다.
- 마지막으로 영향 분석은 실제 비즈니스 중단을 자세히 설명합니다.

영향을 받는 워크로드 구성 요소를 식별한 후 범위 지정 결과를 관련 워크로드의 목표 복구 시점(RPO) 및 목표 복구 시간(RTO)과 연관시켜 알림의 중요도에 맞게 조정하면 리소스 할당과 다음에 발생하는 모든 활동이 시작됩니다. 모든 인시던트가 비즈니스 프로세스를 지원하는 워크로드의 운영을 직접 방해하는 것은 아닙니다. 민감한 데이터 공개, 지적 재산 도용 또는 리소스 하이재킹(암호화 화폐 채굴 등)과 같은 인시던트는 비즈니스 프로세스를 즉시 중단하거나 약화시키지는 않지만, 나중에 결과를 초래할 수 있습니다.

보안 로그 및 조사 결과 강화

위협 인텔리전스 및 조직 컨텍스트 강화

분석 과정에서 관심 있는 관찰 항목은 알림의 컨텍스트화를 강화하기 위해 보강이 필요합니다. 준비 섹션에 설명된 대로 사이버 위협 인텔리전스를 통합하고 활용하면 보안 조사 결과를 자세히 이해하는 데 도움이 될 수 있습니다. 위협 인텔리전스 서비스는 퍼블릭 IP 주소, 도메인 이름 및 파일 해시에 평판과 속성 소유권을 할당하는 데 사용됩니다. 이러한 도구는 유료 및 무료 서비스로 제공됩니다.

Amazon Athena를 로그 쿼리 도구로 채택한 고객은 AWS Glue 작업을 활용하여 위협 인텔리전스 정보를 테이블로 로드할 수 있습니다. SQL 쿼리에서 위협 인텔리전스 테이블을 사용하여 IP 주소 및 도메인 이름과 같은 로그 요소를 상호 연관시켜 분석할 데이터를 자세히 볼 수 있습니다.

AWS는 위협 인텔리전스를 고객에게 직접 제공하지 않지만 Amazon GuardDuty와 같은 서비스는 강화 및 결과 생성을 위해 위협 인텔리전스를 사용합니다. 자체 위협 인텔리전스를 기반으로 사용자 지정 위협 목록을 GuardDuty에 업로드할 수도 있습니다.

자동화를 통한 강화

자동화는 AWS 클라우드 거버넌스의 필수적인 부분으로, 인시던트 대응 수명 주기의 다양한 단계에서 사용할 수 있습니다.

탐지 단계의 경우 규칙 기반 자동화는 로그에서 위협 모델의 관심 패턴을 일치시키고 알림 전송과 같은 적절한 조치를 취합니다. 분석 단계에서는 탐지 메커니즘을 활용하여 로그를 쿼리하고 이벤트 컨텍스트화를 위해 관찰 가능한 항목을 보강할 수 있는 엔진에 알림 본문을 전달할 수 있습니다.

기본 형식의 알림 본문은 리소스와 ID로 구성됩니다. 예를 들어, 알림 시점을 기준으로 알림 본문의 ID 또는 리소스가 수행한 AWS API 활동에 대해 CloudTrail을 쿼리하는 자동화를 구현하여 식별된 API 활동의 `eventSource`, `eventName`, `SourceIPAddress` 및 `userAgent`를 포함한 추가 인사이트를 제공할 수 있습니다. 이러한 쿼리를 자동화된 방식으로 수행하면 대응 담당자가 분류 중 시간을 절약하고 추가 컨텍스트를 얻어 정보에 입각한 더 나은 결정을 내릴 수 있습니다.

자동화를 사용하여 보안 조사 결과를 풍부하게 하고 분석을 단순화하는 방법에 대한 예는 How to enrich AWS Security Hub findings with account metadata 블로그 게시물을 참조하세요.

포렌식 증거 수집 및 분석

이 문서의 the section called “준비” 섹션에 언급된 포렌식은 인시던트 대응 중 아티팩트를 수집하고 분석하는 프로세스입니다. AWS에서는 네트워크 트래픽 패킷 캡처, 운영 체제 메모리 덤프 등의 인프라 영역 리소스와 AWS CloudTrail 로그 등의 서비스 영역 리소스에 적용됩니다.

포렌식 프로세스는 다음과 같은 기본적인 특징을 가지고 있습니다.

- 일관성 - 편차 없이 문서화된 정확한 단계를 따릅니다.
- 반복 가능성 - 동일한 아티팩트에 대해 반복할 때 정확히 동일한 결과를 생성합니다.
- 관례성 - 공개적으로 문서화되고 널리 채택됩니다.

인시던트 대응 중 수집된 아티팩트에 대한 관리 연속성을 유지하는 것이 중요합니다. 자동화를 사용하고 이 컬렉션의 문서를 자동으로 생성하면 도움이 될 수 있으며, 아티팩트를 읽기 전용 리포지토리에 저장하는 것도 도움이 됩니다. 무결성을 유지하기 위해 수집된 아티팩트의 정확한 복제본에 대해서만 분석을 수행해야 합니다.

관련 아티팩트 수집

이러한 특성을 염두에 두고 영향과 범위에 대한 관련 알림과 평가를 기반으로 추가 조사 및 분석과 관련된 데이터를 수집해야 합니다. 서비스/컨트롤 플레인 로그(CloudTrail, Amazon S3 데이터 이벤트, VPC 흐름 로그), 데이터(Amazon S3 메타데이터 및 객체), 리소스(데이터베이스, Amazon EC2 인스턴스)를 포함하여 조사와 관련이 있을 수 있는 다양한 유형의 데이터와 소스입니다.

서비스/컨트롤 플레인 로그는 로컬 분석을 위해 수집하거나, 이상적으로는 기본 AWS 서비스(해당하는 경우)를 사용하여 직접 쿼리할 수 있습니다. 데이터(메타데이터 포함)를 직접 쿼리하여 관련 정보를 얻거나 소스 객체를 획득할 수 있습니다. 예를 들어 AWS CLI를 사용하여 Amazon S3 버킷 및 객체 메타데이터를 획득하고 소스 객체를 직접 획득합니다. 리소스는 리소스 유형 및 의도된 분석 방법과 일치하는 방식으로 수집해야 합니다. 예를 들어 데이터베이스를 실행하는 시스템의 복사본/스냅샷을 생성하거나, 전체 데이터베이스 자체의 복사본/스냅샷을 생성하거나, 조사와 관련된 데이터베이스에서 특정 데이터와 로그를 쿼리하고 추출하여 데이터베이스를 수집할 수 있습니다.

Amazon EC2 인스턴스의 경우 수집해야 하는 특정 데이터 세트와 분석 및 조사를 위해 가장 많은 양의 데이터를 획득하고 보존하기 위해 수행해야 하는 특정 수집 순서가 있습니다.

특히 Amazon EC2 인스턴스에서 가장 많은 양의 데이터를 획득하고 보존하기 위한 대응 순서는 다음과 같습니다.

1. 인스턴스 메타데이터 획득 - 조사 및 데이터 쿼리와 관련된 인스턴스 메타데이터(인스턴스 ID, 유형, IP 주소, VPC/서브넷 ID, 리전, Amazon Machine Image(AMI) ID, 연결된 보안 그룹, 시작 시간)를 획득합니다.
2. 인스턴스 보호 및 태그 활성화 - 종료 방지, 종료 동작을 중지(종료로 설정된 경우)로 설정, 연결된 EBS 볼륨에 대한 종료 시 삭제 속성 비활성화, 시각적 표시 및 가능한 대응 자동화에 사용하기에 적절한 태그 적용(예: 이름이 `Status`이고 값이 `Quarantine`인 태그를 적용할 때 데이터의 포렌식 획득 수행 및 인스턴스 격리)과 같은 인스턴스 보호를 활성화합니다.
3. 디스크 획득(EBS 스냅샷) - 연결된 EBS 볼륨의 EBS 스냅샷을 획득합니다. 각 스냅샷에는 (스냅샷을 만든 시점의) 데이터를 새 EBS 볼륨에 복원하는 데 필요한 정보가 들어 있습니다. 인스턴스 저장소 볼륨을 사용하는 경우 라이브 대응/아티팩트 수집을 수행하는 단계를 참조하세요.
4. 메모리 획득 - EBS 스냅샷은 애플리케이션 또는 OS가 메모리에 저장하거나 캐시하는 데이터를 제외할 수 있는 Amazon EBS 볼륨에 기록된 데이터만 캡처하므로 시스템에서 사용 가능한 데이터를 획득하려면 적절한 타사 오픈 소스나 상용 도구를 사용하여 시스템 메모리 이미지를 획득해야 합니다.
5. (선택 사항) 라이브 대응/아티팩트 수집 수행 - 디스크나 메모리를 다른 방법으로 확보할 수 없는 경우나 타당한 사업적 또는 운영적 이유가 있는 경우에만 시스템에서 라이브 대응을 통해 대상 데이터(디스크/메모리/로그)를 수집합니다. 이렇게 하면 중요한 시스템 데이터와 아티팩트가 수정됩니다.
6. 인스턴스 사용 중지 - Auto Scaling 그룹에서 인스턴스를 분리하고, 로드 밸런서에서 인스턴스를 등록 취소하고, 권한이 최소화되거나 없는 사전 빌드된 인스턴스 프로파일을 조정하거나 적용합니다.
7. 인스턴스 격리 - 인스턴스와의 현재 및 향후 연결을 종료하고 방지하여 환경 내 다른 시스템 및 리소스에서 인스턴스가 효과적으로 격리되었는지 확인합니다. 자세한 내용은 본 문서의 the section called “격리” 섹션을 참조하세요.
8. 대응 담당자의 선택 - 상황과 목표에 따라 다음 중 하나를 선택합니다.
   - 시스템을 사용 중지하고 종료합니다(권장).

     사용 가능한 증거가 확보되면 시스템을 종료하여 인스턴스가 환경에 미칠 수 있는 향후 영향에 대한 가장 효과적인 완화 조치를 확인합니다.
   - 모니터링을 위해 구성된 격리된 환경 내에서 인스턴스를 계속 실행합니다.

     표준적인 접근 방식으로 권장되지는 않지만, 상황에 따라 인스턴스를 지속적으로 관찰해야 하는 경우(인스턴스에 대한 포괄적인 조사 및 분석을 수행하기 위해 추가 데이터나 지표가 필요한 경우) 인스턴스를 종료하고 인스턴스의 AMI를 생성한 다음, 인스턴스에 대한 거의 연속적인 모니터링을 용이하게 하기 위해 완전히 격리되고 계측이 구성된 샌드박스 환경 내의 전용 포렌식 계정에서 인스턴스를 다시 시작하는 것을 고려할 수 있습니다(예: VPC 흐름 로그 또는 VPC 트래픽 미러링).

> **Note**
>
> 사용 가능한 휘발성(및 가치 있는) 데이터를 캡처하려면 라이브 대응 활동 또는 시스템 격리 또는 종료 전에 메모리를 캡처해야 합니다.

서술 개발

분석 및 조사 중 후속 단계와 최종 보고서에서 사용할 수 있도록 수행된 작업, 수행된 분석 및 식별된 정보를 문서화합니다. 이러한 서술은 간결하고 정확해야 하며, 인시던트에 대한 효과적인 이해를 확인하고 정확한 타임라인을 유지하기 위해 관련 정보가 포함되어 있는지 확인해야 합니다. 또한 핵심 인시던트 대응 팀 외부의 사람들을 참여시킬 때도 유용합니다. 다음 예를 참고하세요

> 마케팅 및 영업 부서는 2022년 3월 15일에 민감한 데이터가 공개적으로 게시되는 것을 피하려면 암호화폐를 지불하라는 랜섬웨어 공격을 받았습니다. SOC는 2022년 2월 20일 마케팅 및 영업 부서의 Amazon RDS 데이터베이스가 공개 접근이 가능했다고 판단했습니다. SOC는 RDS 액세스 로그를 쿼리하고 웹 개발자 중 한 명인 Major Mary에게 속한 자격 증명 *mm03434*와 함께 2022년 2월 20일에 IP 주소 198.51.100.23이 사용되었다고 판단했습니다. SOC는 VPC 흐름 로그를 쿼리하고 동일한 날짜에 약 256MB의 데이터가 동일한 IP 주소로 송신되었다고 판단했습니다(타임스탬프 2022-02-20T15:50+00Z). SOC는 오픈 소스 위협 인텔리전스를 통해 자격 증명이 현재 퍼블릭 리포지토리 *https[:]//example[.]com/majormary/rds-utils*에서 일반 텍스트로 사용 가능함을 확인했습니다.

격리

인시던트 대응과 관련된 격리의 한 가지 정의는 보안 이벤트의 범위를 최소화하고 환경 내 무단 사용의 영향을 포함하는 보안 이벤트를 처리하는 동안 전략의 프로세스 또는 구현입니다.

격리 전략은 다양한 요인에 따라 달라지며 격리 전략, 타이밍 및 목적의 적용 측면에서 조직마다 다를 수 있습니다. NIST SP 800-61 Computer Security Incident Handling Guide에는 다음을 포함하여 적절한 격리 전략을 결정하기 위한 몇 가지 기준이 요약되어 있습니다.

- 리소스의 잠재적 손상 및 도난
- 증거 보존 필요
- 서비스 가용성(네트워크 연결, 외부 당사자에게 제공되는 서비스)
- 전략을 구현하는 데 필요한 시간 및 리소스

- 전략의 효율성(부분 격리 또는 전체 격리)
- 솔루션 기간(4시간 내에 긴급 해결 방법 제거, 2주 내에 임시 해결 방법 제거, 영구 솔루션)

그러나 AWS의 서비스와 관련하여 기본 격리 단계는 다음 세 가지 범주로 나눌 수 있습니다.

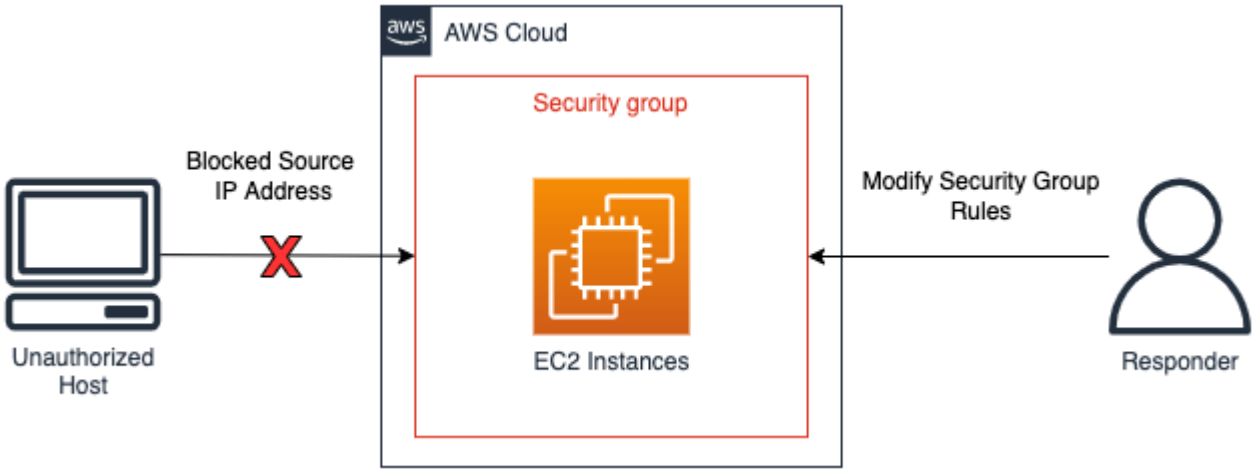
- 소스 격리 - 필터링 및 라우팅을 사용하여 특정 소스의 액세스를 방지합니다.
- 기법 및 액세스 격리 - 영향을 받는 리소스에 대한 무단 액세스를 방지하기 위해 액세스를 제거합니다.
- 대상 격리 - 필터링과 라우팅을 사용하여 대상 리소스에 대한 액세스를 방지합니다.

소스 격리

소스 격리는 특정 소스 IP 주소 또는 네트워크 범위의 리소스에 대한 액세스를 방지하기 위해 환경 내에서 필터링 또는 라우팅을 사용하고 적용하는 것입니다. AWS 서비스를 사용한 소스 격리의 예는 다음과 같습니다.

- 보안 그룹 - Amazon EC2 인스턴스에 격리 보안 그룹을 생성하고 적용하거나 기존 보안 그룹에서 규칙을 제거하면 Amazon EC2 인스턴스 또는 AWS 리소스에 대한 무단 트래픽을 격리하는 데 도움이 될 수 있습니다. 기존 추적 연결은 보안 그룹 변경으로 인해 종료되지 않습니다. 향후 트래픽만 새 보안 그룹에 의해 효과적으로 차단됩니다. 추적한 연결과 추적하지 않은 연결에 대한 자세한 내용은 이 Incident Response Playbook 및 보안 그룹 연결 추적을 참조하세요.
- 정책 - IP 주소, 네트워크 범위 또는 VPC 엔드포인트로부터의 트래픽을 차단하거나 허용하도록 Amazon S3 버킷 정책을 구성할 수 있습니다. 정책을 통해 의심스러운 주소와 Amazon S3 버킷에 대한 액세스를 차단할 수 있습니다. 버킷 정책에 대한 추가 정보는 Amazon S3 콘솔을 사용하여 버킷 정책 추가에서 확인할 수 있습니다.
- AWS WAF - AWS WAF에서 웹 액세스 제어 목록(웹 ACL)을 구성하여 리소스가 대응하는 웹 요청을 세밀하게 제어할 수 있습니다. AWS WAF에 구성된 IP 세트에 IP 주소 또는 네트워크 범위를 추가하고, IP 세트에 블록과 같은 일치 조건을 적용할 수 있습니다. 이렇게 하면 발신 트래픽의 IP 주소 또는 네트워크 범위가 IP 세트 규칙에 구성된 트래픽과 일치하는 경우 리소스에 대한 웹 요청이 차단됩니다.

다음 다이어그램에서는 인시던트 대응 분석가가 Amazon EC2 인스턴스의 보안 그룹을 수정하여 특정 IP 주소로만 새 연결을 제한하는 소스 격리의 예를 볼 수 있습니다. 보안 그룹 항목에서 언급했듯이, 보안 그룹을 변경해도 기존에 추적된 연결은 종료되지 않습니다.



소스 격리 예시

> **Note**
>
> 보안 그룹과 네트워크 ACL은 Amazon Route 53에 대한 트래픽을 필터링하지 않습니다. EC2 인스턴스를 격리할 때 외부 호스트와 접촉하지 않도록 하려면 DNS 통신도 명시적으로 차단해야 합니다.

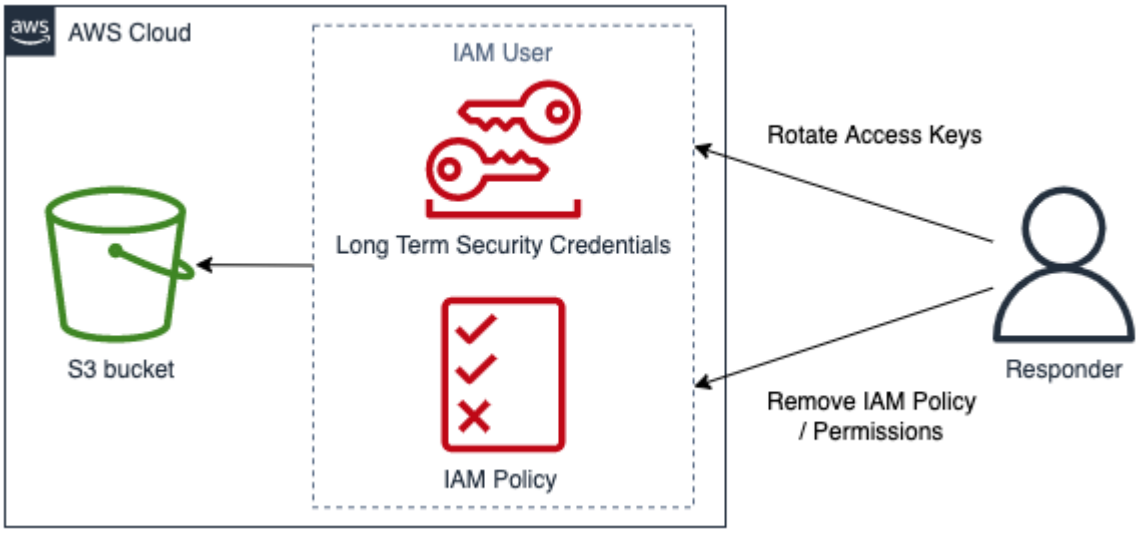
기법 및 액세스 격리

리소스에 액세스할 수 있는 기능과 IAM 위탁자를 제한하여 리소스의 무단 사용을 방지합니다. 여기에는 리소스에 액세스할 수 있는 IAM 위탁자의 권한 제한과 임시 보안 자격 증명 취소도 포함됩니다. AWS 서비스를 사용한 기법 및 액세스 격리의 예는 다음과 같습니다.

- 권한 제한 - IAM 위탁자에게 할당된 권한은 최소 권한 원칙을 따라야 합니다. 그러나 활성 보안 이벤트 중에는 특정 IAM 위탁자의 대상 리소스에 대한 액세스를 더 제한해야 할 수 있습니다. 이 경우 격리될 IAM 위탁자에서 권한을 제거하여 리소스에 대한 액세스를 격리할 수 있습니다. 이 작업은 IAM 서비스를 통해 수행되며 AWS Management Console, AWS CLI 또는 AWS SDK를 사용하여 적용할 수 있습니다.
- 키 취소 - IAM 위탁자는 IAM 액세스 키를 사용하여 리소스에 액세스하거나 관리합니다. 이 키는 AWS CLI 또는 AWS API에 대한 프로그래밍 방식 요청에 서명하는 데 사용되는 장기 정적 자격 증명이며, 접두사 AKIA로 시작합니다. 자세한 내용은 IAM 식별자의 고유 ID 접두사 이해 섹션을 참조하세요. IAM 액세스 키가 손상된 IAM 위탁자에 대한 액세스를 격리하려면 액세스 키를 비활성화하거나 삭제합니다. 다음 사항을 명심해야 합니다.
  - 액세스 키는 비활성화 후 다시 활성화할 수 있습니다.

  - 액세스 키는 삭제 후 복구할 수 없습니다.
  - IAM 위탁자는 언제든지 최대 2개의 액세스 키를 가질 수 있습니다.
  - 액세스 키를 사용하는 사용자 또는 애플리케이션은 키가 비활성화되거나 삭제되면 액세스 권한을 잃게 됩니다.
- 임시 보안 자격 증명 취소 - 임시 보안 자격 증명은 조직에서 AWS 리소스에 대한 액세스를 제어하는 데 사용할 수 있으며 접두사 ASIA로 시작합니다. 자세한 내용은 IAM 식별자의 고유 ID 접두사에 대한 이해 섹션을 참조하세요. 임시 자격 증명은 일반적으로 IAM 역할에서 사용되며 수명이 제한적이므로 교체하거나 명시적으로 취소할 필요가 없습니다. 임시 보안 자격 증명 만료 전에 임시 보안 자격 증명과 관련된 보안 이벤트가 발생하는 경우 기존 임시 보안 자격 증명의 유효 권한을 변경해야 할 수 있습니다. 이 작업은 AWS Management Console 내에서 IAM 서비스를 사용하여 완료할 수 있습니다. 임시 보안 자격 증명은 IAM 역할이 아닌 IAM 사용자에게도 발급할 수 있지만, 이 글을 작성하는 현재로서는 AWS Management Console 내에서 IAM 사용자의 임시 보안 자격 증명을 취소할 수 있는 옵션이 없습니다. 임시 보안 자격 증명을 만든 권한이 없는 사용자가 사용자의 IAM 액세스 키를 유출한 보안 이벤트의 경우 두 가지 방법을 사용하여 임시 보안 자격 증명을 해지할 수 있습니다.
  - IAM 사용자에게 보안 토큰 발급 시간을 기반으로 액세스를 방지하는 인라인 정책을 연결합니다. 자세한 내용은 임시 보안 자격 증명에 대한 권한 비활성화의Denying access to temporary security credentials issued before a specific time 섹션을 참조하세요.
  - 손상된 액세스 키를 소유한 IAM 사용자를 삭제합니다. 필요한 경우 사용자를 다시 생성합니다.
- AWS WAF - 권한이 없는 사용자가 사용하는 특정 기법에는 SQL 인젝션과 크로스 사이트 스크립팅(XSS)이 포함된 요청과 같은 일반적인 악성 트래픽 패턴이 포함됩니다. AWS WAF 기본 제공 규칙 문을 사용하여 이러한 기법을 사용하는 트래픽을 일치시키고 거부하도록 AWS WAF를 구성할 수 있습니다.

다음 다이어그램은 기술 및 액세스 격리의 예를 보여줍니다. 인시던트 대응 담당자는 액세스 키를 순환하거나 IAM 정책을 제거하여 IAM 사용자가 Amazon S3 버킷에 액세스하지 못하도록 합니다.



기법 및 액세스 격리 예시

대상 격리

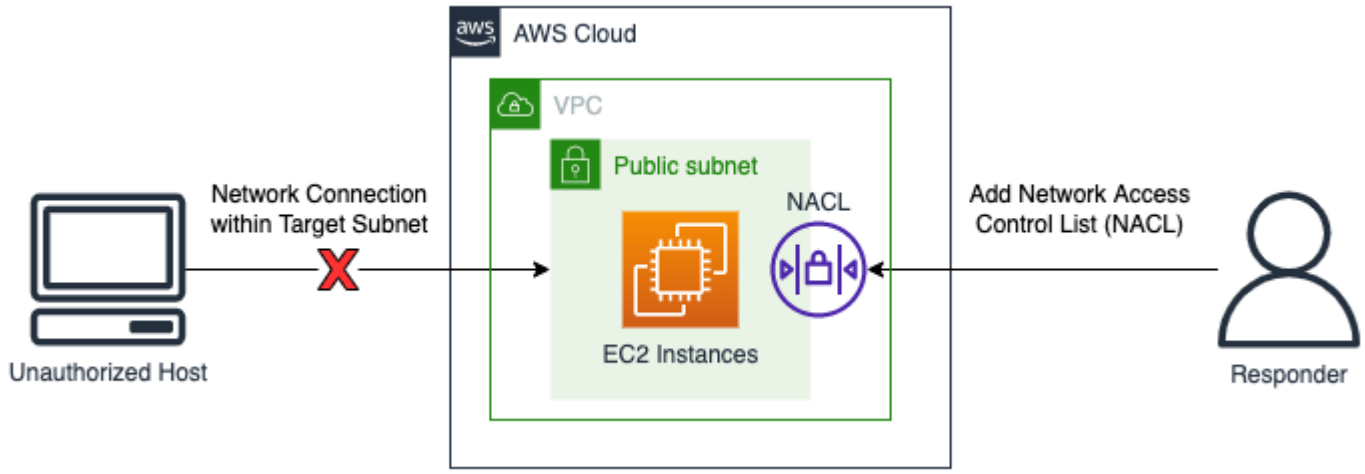
대상 격리는 대상 호스트나 리소스에 대한 액세스를 방지하기 위해 환경 내에서 필터링 또는 라우팅을 적용하는 것입니다. 경우에 따라 대상 격리에는 합법적인 리소스가 가용성을 위해 복제되는지 확인하기 위한 복원력 형태도 포함됩니다. 격리 및 격리를 위해 리소스를 이러한 형태의 복원력에서 분리해야 합니다. AWS 서비스를 사용한 대상 격리의 예는 다음과 같습니다.

- 네트워크 ACL - AWS 리소스가 포함된 서브넷에 구성된 네트워크 ACL에는 거부 규칙이 추가될 수 있습니다. 이러한 거부 규칙을 적용하여 특정 AWS 리소스에 대한 액세스를 방지할 수 있지만 네트워크 액세스 제어 목록(네트워크 ACL)을 적용하면 권한 부여 없이 액세스되는 리소스뿐만 아니라 서브넷의 모든 리소스에도 영향이 있습니다. 네트워크 ACL 내에 나열된 규칙은 하향식 순서로 처리되므로 대상 리소스와 서브넷에 대한 무단 트래픽을 거부하도록 기존 네트워크 ACL의 첫 번째 규칙을 구성해야 합니다. 또는 인바운드 및 아웃바운드 트래픽 모두에 대해 단일 거부 규칙을 사용해서 완전히 새로운 네트워크 ACL을 생성하고 대상 리소스가 포함된 서브넷과 연결해서 새 네트워크 ACL을 사용하여 서브넷에 액세스하지 못하도록 할 수 있습니다.
- 종료 - 리소스를 완전히 종료하면 무단 사용의 영향을 격리하는 데 효과적일 수 있습니다. 리소스를 종료하면 비즈니스 요구 사항에 대한 합법적인 액세스가 차단되고 불안정한 법의학 데이터를 얻을 수 없게 되므로 이는 목적이 있는 결정이어야 하며 조직의 보안 정책에 따라 판단해야 합니다.
- 격리 VPC - 격리 VPC를 사용하여 합법적인 트래픽(예: 바이러스 백신(AV) 또는 인터넷이나 외부 관리 콘솔에 액세스해야 하는 EDR 솔루션)에 대한 액세스를 제공하면서 리소스를 효과적으로 격리할 수 있습니다. 격리 VPC는 보안 이벤트 전에 유효한 IP 주소와 포트를 허용하도록 미리 구성할 수 있으며, 활성 보안 이벤트 중에 대상 리소스를 이 격리 VPC로 즉시 이동하여 리소스를 격리하면서 인시던트 대응의 후속 단계 동안 대상 리소스에서 합법적인 트래픽을 송수신할 수 있도록 할 수 있습니

다. 격리 VPC 사용의 중요한 측면은 EC2 인스턴스와 같은 리소스를 사용하기 전에 새 격리 VPC에서 종료했다가 다시 시작해야 한다는 점입니다. 기존 EC2 인스턴스는 다른 VPC 또는 다른 가용 영역으로 이동할 수 없습니다. 이렇게 하려면 Amazon EC2 인스턴스를 다른 서브넷, 가용 영역 또는 VPC로 이동하려면 어떻게 해야 합니까?에 약술된 단계를 따르세요.

- Auto Scaling 그룹 및 로드 밸런서 - Auto Scaling 그룹과 로드 밸런서에 연결된 AWS 리소스는 대상 격리 절차의 일부로 분리하고 등록 취소해야 합니다. AWS 리소스 분리 및 등록 취소는 AWS Management Console, AWS CLI 및 AWS SDK를 사용하여 수행할 수 있습니다.

다음 다이어그램에서는 승인되지 않은 호스트의 네트워크 연결 요청을 차단하기 위해 인시던트 대응 분석가가 서브넷에 네트워크 ACL을 추가하는 대상 격리의 예를 보여줍니다.



대상 격리 예시

요약

격리는 인시던트 대응 프로세스의 한 단계이며 수동 또는 자동일 수 있습니다. 전반적인 방지 전략은 조직의 보안 정책 및 비즈니스 요구 사항에 부합해야 하며, 제거 및 복구 전에 부정적인 영향이 최대한 효율적으로 완화되는지 확인해야 합니다.

근절

보안 인시던트 대응과 관련하여 제거는 계정을 알려진 안전한 상태로 되돌리기 위해 의심스럽거나 승인되지 않은 리소스를 제거하는 것입니다. 근절 전략은 조직의 비즈니스 요구 사항에 따라 달라지는 여러 요인에 따라 달라집니다.

NIST SP 800-61 Computer Security Incident Handling Guide에서는 근절을 위한 몇 가지 단계를 제공합니다.

1. 악용된 모든 취약성을 식별하고 완화합니다.
2. 맬웨어, 부적절한 재료 및 기타 구성 요소를 제거합니다.
3. 영향을 받는 호스트가 더 많이 검색되면(예: 새로운 맬웨어 감염) 탐지 및 분석 단계를 반복하여 영향을 받는 다른 모든 호스트를 식별한 다음 해당 호스트에 대한 인시던트를 방지하고 근절합니다.

AWS 리소스의 경우 CloudWatch Logs, Amazon GuardDuty 등의 사용 가능한 로그 또는 자동화된 도구를 통해 탐지되고 분석된 이벤트를 통해 이를 더욱 세분화할 수 있습니다. 이러한 이벤트는 환경을 알려진 안전한 상태로 적절하게 복원하기 위해 수행해야 하는 문제 해결을 결정하는 기준이 되어야 합니다.

근절의 첫 번째 단계는 AWS 계정 내에서 어떤 리소스가 영향을 받았는지 파악하는 것입니다. 이는 사용 가능한 로그 데이터 소스, 리소스 및 자동 도구의 분석을 통해 이루어집니다.

- 계정의 IAM ID에서 수행한 무단 작업을 식별합니다.
- 계정에 대한 무단 액세스 또는 변경 사항을 식별합니다.
- 승인되지 않은 리소스 또는 IAM 사용자의 생성을 식별합니다.
- 무단 변경이 있는 시스템 또는 리소스를 식별합니다.

리소스 목록이 확인되면 각 리소스를 평가하여 리소스를 삭제하거나 복원할 경우 비즈니스에 미치는 영향을 결정해야 합니다. 예를 들어, 웹 서버가 비즈니스 애플리케이션을 호스팅하고 있고 이를 삭제하면 가동 중지 시간이 발생하는 경우, 영향을 받는 서버를 삭제하기 전에 검증된 안전한 백업에서 리소스를 복구하거나 깨끗한 AMI에서 시스템을 다시 시작하는 것이 좋습니다.

비즈니스 영향 분석을 완료한 후 로그 분석의 이벤트를 사용하여 계정으로 이동하여 다음과 같은 적절한 문제 해결을 수행해야 합니다.

- 키 교체 또는 삭제 - 이 단계에서는 행위자가 계정 내에서 활동을 계속 수행할 수 있는 기능이 제거됩니다.
- 잠재적으로 승인되지 않은 IAM 사용자 자격 증명을 교체합니다.
- 인식할 수 없거나 승인되지 않은 리소스를 삭제합니다.

> **Important**
>
> 조사를 위해 리소스를 유지해야 하는 경우 해당 리소스를 백업하는 것이 좋습니다. 예를 들어 규제, 규정 준수 또는 법적 이유로 Amazon EC2 인스턴스를 유지해야 하는 경우 인스턴스를 제거하기 전에 Amazon EBS 스냅샷을 생성합니다.

- 맬웨어 감염의 경우 AWS Partner 또는 다른 벤더에 문의해야 할 수 있습니다. AWS는 맬웨어 분석 또는 제거를 위한 기본 도구를 제공하지 않습니다. 그러나 Amazon EBS용 GuardDuty 맬웨어 모듈을 사용하는 경우 제공된 조사 결과에 대한 권장 사항을 사용할 수 있습니다.

식별된 영향을 받는 리소스를 근절하면 AWS는 계정에 대한 보안 검토를 수행할 것을 권장합니다. 이는 AWS Config 규칙을 사용하거나 Prowler 및 ScoutSuite와 같은 오픈 소스 솔루션을 사용하거나 다른 벤더를 통해 수행할 수 있습니다. 또한 공개(인터넷) 대면 리소스에 대한 취약성 스캔을 수행하여 잔여 위험을 평가하는 것도 고려해야 합니다.

근절은 인시던트 대응 프로세스의 한 단계이며 인시던트와 영향을 받는 리소스에 따라 수동 또는 자동일 수 있습니다. 전반적인 전략은 조직의 보안 정책 및 비즈니스 요구 사항에 부합해야 하며 부적절한 리소스 또는 구성이 제거되면 부정적인 영향이 완화되는지 확인해야 합니다.

복구

복구는 시스템을 알려진 안전 상태로 복원하고, 복원 전에 백업이 안전하거나 인시던트의 영향을 받지 않는지 검증하고, 복원 후 시스템이 제대로 작동하는지 테스트하고, 보안 이벤트와 관련된 취약성을 해결하는 프로세스입니다.

복구 순서는 조직의 요구 사항에 따라 다릅니다. 복구 프로세스의 일환으로 최소한 다음을 결정하기 위해 비즈니스 영향 분석을 수행해야 합니다.

- 비즈니스 또는 종속성 우선순위
- 복원 계획
- 인증 및 권한 부여

NIST SP 800-61 Computer Security Incident Handling Guide에서는 시스템 복구를 위한 몇 가지 단계를 제공합니다.

- 클린 백업에서 시스템 복원
  - 시스템으로 복원하기 전에 백업을 평가하여 감염이 없는지 확인하고 보안 이벤트의 재발을 방지하세요.

    백업 메커니즘이 제대로 작동하고 데이터 무결성이 복구 시점 목표를 충족하는지 확인하기 위해 재해 복구 테스트의 일환으로 백업을 정기적으로 평가해야 합니다.
  - 가능하면 근본 원인 분석의 일부로 식별된 첫 번째 이벤트 타임스탬프 이전의 백업을 사용하세요.
- 자동화를 사용하여 신뢰할 수 있는 소스에서 다시 배포하는 것을 포함하여 시스템을 처음부터 다시 구축합니다. 이 작업은 새로운 AWS 계정에서 수행됩니다.

- 클린 버전으로 손상된 파일 교체

  이 작업을 수행할 때는 각별히 주의해야 합니다. 복구 중인 파일이 인시던트의 영향을 받지 않고 안전한 것으로 알려져 있는지 반드시 확인해야 합니다.
- 패치 설치
- 암호 변경
  - 여기에는 침해되었을 수 있는 IAM 위탁자의 암호가 포함됩니다.
  - 가능하면 최소 권한 전략의 일부로 IAM 위탁자 및 페더레이션에 역할을 사용하는 것이 좋습니다.
- 네트워크 경계 보안 강화(방화벽 규칙 세트, 경계 라우터 액세스 제어 목록).

리소스가 복구되면 파악한 내용을 수집하여 인시던트 대응 정책, 절차 및 가이드를 업데이트하는 것이 중요합니다.

요약하면 알려진 안전한 작업으로의 반환을 용이하게 하는 복구 프로세스를 구현하는 것이 중요합니다. 복구에는 오랜 시간이 걸릴 수 있으며, 비즈니스 영향과 재인증 위험의 균형을 맞추려면 격리 전략과의 밀접한 연결이 필요합니다. 복구 절차에는 리소스 및 서비스, IAM 위탁자를 복원하고 계정에 대한 보안 검토를 수행하여 잔여 위험을 평가하는 단계가 포함되어야 합니다.

결론

각 운영 단계에는 고유한 목표, 기법, 방법론 및 전략이 있습니다. 표 4에는 이러한 단계와 이 섹션에서 다루는 몇 가지 기법 및 방법론이 요약되어 있습니다.

표 4 - 운영 단계: 목표, 기법 및 방법론

Phase(단계)	목표	기법 및 방법론
탐지	잠재적 보안 이벤트를 파악합니다.	• 탐지를 위한 보안 제어 • 동작 및 규칙 기반 탐지 • 사람 기반 탐지
분석	보안 이벤트가 인시던트인지 판단하고 인시던트 범위를 평가하세요.	• 알림 검증 및 범위 지정 • 로그 쿼리 • 위협 인텔리전스 • 자동화

Phase(단계)	목표	기법 및 방법론
격리	보안 이벤트의 영향을 최소화하고 제한합니다.	• 소스 격리 • 기법 및 액세스 격리 • 대상 격리
근절	보안 이벤트와 관련된 승인되지 않은 리소스 또는 아티팩트를 제거합니다.	• 손상되거나 승인되지 않은 자격 증명 교체 또는 삭제 • 승인되지 않은 리소스 삭제 • 맬웨어 제거 • 보안 스캔
복구	시스템을 알려진 정상 상태로 복원하고 이러한 시스템을 모니터링하여 위협이 다시 발생하지 않는지 확인합니다.	• 백업에서 시스템 복원 • 처음부터 시스템 다시 빌드됨 • 클린 버전으로 손상된 파일 교체됨

인시던트 사후 활동

위협 환경은 끊임없이 변화하므로 환경을 효과적으로 보호할 수 있는 조직의 역량도 그에 못지않게 역동적으로 대처하는 것이 중요합니다. 지속적인 개선의 핵심은 발생 가능한 보안 인시던트를 효과적으로 탐지, 대응 및 조사할 수 있는 능력을 향상시키고, 발생 가능한 취약성을 줄이며, 대응 시간을 단축하고, 안전한 운영으로 돌아갈 수 있도록 인시던트 및 시뮬레이션의 결과를 반복해서 검토하는 것입니다. 다음 메커니즘은 조직이 상황에 관계없이 효과적으로 대응할 수 있는 최신 역량과 지식을 갖추고 있는지 확인하는 데 도움이 될 수 있습니다.

인시던트로부터 학습하기 위한 프레임워크 구축

파악한 내용 프레임워크와 방법론을 구현하면 인시던트 대응 능력을 개선하는 데 도움이 될 뿐만 아니라 인시던트의 재발을 방지하는 데도 도움이 됩니다. 각 인시던트에서 교훈을 얻음으로써 동일한 실수, 노출 또는 잘못된 구성을 반복하지 않도록 하여 보안 태세를 개선할 뿐만 아니라 사전에 방지 가능한 상황으로 인한 시간 손실을 최소화할 수 있습니다.

다음 사항을 높은 수준에서 설정하고 달성하는 학습한 교훈 프레임워크를 구현하는 것이 중요합니다.

- 학습한 교훈은 언제 적용하게 되나요?

- 학습한 교훈 과정에는 무엇이 포함되나요?
- 학습한 교훈은 어떻게 수행되나요?
- 누가 어떻게 이 과정에 참여하나요?
- 개선이 필요한 부분은 어떻게 확인할 수 있나요?
- 개선 사항을 효과적으로 추적하고 구현할 수 있도록 어떻게 해야 할까요?

이러한 개략적인 결과 외에도, 프로세스에서 최대한의 가치(실행 가능한 개선으로 이어지는 정보)를 이끌어낼 수 있도록 올바른 질문을 하는 것이 중요합니다. 다음 질문을 고려하면 학습한 교훈 토론을 시작하는 데 도움이 됩니다.

- 어떤 인시던트였나요?
- 인시던트가 언제 처음 확인되었나요?
- 어떻게 식별되었나요?
- 어떤 시스템에서 해당 활동에 대해 경고했나요?
- 어떤 시스템, 서비스 및 데이터가 관련되어 있나요?
- 구체적으로 어떤 일이 발생했나요?
- 어떤 점이 잘 작동했나요?
- 어떤 점이 잘 작동하지 않았나요?
- 인시던트에 대응하기 위해 어떤 프로세스 또는 절차가 실패했거나 조정되지 못했나요?
- 다음 영역에서 개선할 수 있는 사항:
  - 사람
    - 연락이 필요한 직원이 실제로 연락이 가능했고 연락처 목록이 최신 상태였나요?
    - 인시던트에 효과적으로 대응하고 조사하는 데 필요한 교육이나 역량을 갖춘 직원이 없었나요?
    - 적절한 리소스가 준비되어 있고 이용 가능했나요?
  - 프로세스
    - 프로세스와 절차를 준수했나요?
    - 이 (유형의) 인시던트에 대한 프로세스와 절차가 문서화되어 있고 사용 가능했나요?
    - 필요한 프로세스 및 절차가 누락되지는 않았나요?
    - 대응 담당자가 문제를 대응하는 데 필요한 정보에 적시에 액세스할 수 있었나요?
  - 기술
    - 기존 경고 시스템이 활동을 효과적으로 식별하고 경고했나요?

    - 기존 경고 시스템을 개선해야 하나요? 아니면 이 인시던트 유형에 대해 새로운 경고 시스템을 구축해야 하나요?
    - 기존 툴링으로 인시던트를 효과적으로 조사(검색 및 분석)할 수 있었나요?
- 이 (유형의) 인시던트를 더 빨리 식별하려면 어떻게 해야 할까요?
- 이 (유형의) 인시던트가 재발하는 것을 방지하려면 어떻게 해야 할까요?
- 개선 계획의 담당자는 누구이며 개선 계획이 실행되었는지 어떻게 테스트할 예정인가요?
- 추가 모니터링/예방적 통제/프로세스를 구현하고 테스트하는 일정은 어떻게 되나요?

이 목록은 모든 것을 포함하지는 않지만, 조직 및 비즈니스 요구 사항이 무엇인지 식별하고 인시던트로부터 가장 효과적으로 학습하고 보안 태세를 지속적으로 개선하기 위해 이를 분석할 수 있는 방법을 식별하기 위한 출발점이 될 수 있습니다. 가장 중요한 것은 인시던트 대응 프로세스, 문서화 및 이해관계자 전반의 기대치에서 학습한 교훈을 표준으로 삼아 통합하는 것부터 시작하는 것입니다.

성공을 위한 지표 설정

지표는 인시던트 대응 기능을 효과적으로 측정, 평가 및 개선하는 데 필요합니다. 측정항목이 없으면 조직의 성과가 얼마나 좋은지 또는 나쁜지 정확하게 측정하거나 파악할 수 있는 기준이 없습니다. 운영 우수성을 위해 노력하기 위한 기대치와 기준을 설정하려는 조직에 좋은 출발점이 될 수 있는 몇 가지 인시던트 대응에 공통적인 지표가 있습니다.

평균 탐지 시간

평균 탐지 시간은 가능한 보안 인시던트를 발견하는 데 걸리는 평균 시간입니다. 특히, 이는 첫 번째 손상 지표 발생과 초기 식별 또는 알림 사이의 시간입니다.

이 지표를 사용하여 탐지 및 알림 시스템의 성능을 추적할 수 있습니다. 효과적인 탐지 및 알림 메커니즘은 가능한 보안 인시던트가 환경 내에 남아 있지 않은지 확인하기 위한 핵심 요소입니다.

평균 탐지 시간이 길수록 가능한 보안 인시던트를 식별하고 발견하기 위해 더 효과적인 알림 및 메커니즘을 추가로 구축해야 할 필요성이 커집니다. 평균 탐지 시간이 짧을수록 탐지 및 알림 메커니즘이 더 잘 작동합니다.

평균 승인 시간

평균 승인 시간은 가능한 보안 인시던트를 확인하고 우선순위를 지정하는 데 걸리는 평균 시간입니다. 구체적으로는 알림이 생성된 후 SOC 또는 인시던트 대응 담당자가 알림을 식별하고 처리 우선순위를 정하기까지의 시간을 말합니다.

이 지표를 사용하여 팀이 알림을 얼마나 잘 처리하고 우선순위를 정하고 있는지 추적할 수 있습니다. 팀이 알림을 효과적으로 식별하고 우선순위를 지정하지 못하면 대응이 지연되고 비효율적이 됩니다.

평균 승인 시간이 길수록 팀이 보안 인시던트를 신속하게 인지하고 대응 우선순위를 정할 수 있도록 적절한 인력과 교육을 받았는지 확인해야 할 필요성이 커집니다. 평균 인지 시간이 짧을수록 팀이 보안 알림에 효과적으로 대응하고 우선순위를 잘 정할 수 있음을 의미합니다.

평균 대응 시간

평균 대응 시간은 가능한 보안 인시던트에 대한 초기 대응을 시작하는 데 걸리는 평균 시간입니다. 구체적으로는 보안 인시던트의 최초 알림 또는 발견부터 대응을 위한 첫 번째 조치까지의 시간을 의미합니다. 이는 평균 승인 시간과 비슷하지만 상황의 간단한 인식 또는 승인과 비교하여 특정 대응 작업(예: 시스템 데이터 획득, 시스템 격리)을 측정하는 것입니다.

이 지표를 사용하여 보안 인시던트에 대응할 준비를 추적할 수 있습니다. 앞서 언급했듯이 준비는 효과적인 대응의 핵심입니다. 이 문서의 the section called “준비” 섹션을 참조하세요.

평균 대응 시간이 길수록 팀이 대응 방법에 대한 교육을 제대로 받았는지 확인하여 대응 프로세스가 효과적으로 문서화되고 활용되고 있는지 확인해야 할 필요성이 커집니다. 평균 대응 시간이 짧을수록 팀이 식별된 알림에 대한 적절한 대응을 파악하고 안전한 운영으로 돌아가는 여정을 시작하는 데 필요한 대응 조치를 더 잘 수행할 수 있습니다.

평균 격리 시간

평균 격리 시간은 가능한 보안 인시던트를 격리하는 데 걸리는 평균 시간입니다. 구체적으로는 보안 인시던트의 최초 알림 또는 발견부터 공격자나 손상된 시스템이 추가적인 피해를 입지 않도록 효과적으로 대응 조치를 완료할 때까지의 시간을 의미합니다.

이 지표를 사용하여 팀이 가능한 보안 인시던트를 얼마나 잘 완화하거나 격리할 수 있는지 추적할 수 있습니다. 가능한 보안 인시던트를 빠르고 효과적으로 격리할 수 없는 경우 추가 침해 가능성에 대한 영향, 범위 및 노출이 증가합니다.

평균 대응 시간이 길어질수록 발생하는 보안 인시던트를 신속하고 효과적으로 완화하고 격리하기 위한 지식과 역량을 모두 구축해야 할 필요성이 커집니다. 평균 격리 시간이 짧을수록 팀이 식별된 위협을 완화하고 격리하는 데 필요한 조치를 더 잘 이해하고 적용하여 비즈니스에 미치는 영향, 범위 및 위험을 줄일 수 있습니다.

평균 복구 시간

평균 복구 시간은 보안 인시던트로부터 안전하게 운영할 수 있도록 완전히 복귀하는 데 걸리는 평균 시간입니다. 구체적으로는 보안 인시던트의 최초 알림 또는 발견 시점부터 인시던트의 영향을 받지 않고 비즈니스가 정상적으로 안전하게 운영될 때까지의 시간을 의미합니다.

이 지표를 사용하여 보안 인시던트 발생 후 팀이 시스템, 계정 및 환경을 안전한 운영 상태로 되돌리는 데 얼마나 효과적인지 추적할 수 있습니다. 안전한 운영으로 신속하고 효과적으로 복귀하지 못하면 보안에 영향을 미칠 뿐만 아니라 비즈니스와 운영에 미치는 영향과 비용도 증가할 수 있습니다.

평균 복구 시간이 길수록 보안 인시던트가 운영 및 비즈니스에 미치는 영향을 최소화하기 위해 팀과 환경에 적절한 메커니즘(예: 장애 조치 프로세스 및 깨끗한 시스템을 안전하게 재배포하기 위한 CI/CD 파이프라인)을 준비해야 할 필요성이 커집니다. 평균 복구 시간이 짧을수록 팀은 보안 인시던트가 운영 및 비즈니스에 미치는 영향을 최소화하는 데 더 효과적으로 대응할 수 있습니다.

공격자 체류 시간

공격자 체류 시간은 권한이 없는 사용자가 시스템 또는 환경에 액세스할 수 있는 평균 시간입니다. 이 기간은 공격자가 시스템 또는 환경에 처음 액세스한 시점부터 시작하여 최초 알림 또는 발견 시점보다 빠를 수 있다는 점을 제외하면 평균 격리 시간과 유사합니다.

이 지표를 사용하여 공격자 또는 위협이 환경에 영향을 미치는 시간, 액세스 및 기회를 줄이기 위해 시스템과 메커니즘이 모두 얼마나 잘 작동하는지 추적할 수 있습니다. 공격자 체류 시간을 줄이는 것이 팀과 비즈니스의 최우선 과제여야 합니다.

공격자의 체류 시간이 길수록 인시던트 대응 프로세스에서 개선이 필요한 부분을 파악하여 팀이 환경에서 위협이나 공격의 영향과 범위를 최소화할 수 있는 능력을 확보해야 할 필요성이 커집니다. 공격자의 체류 시간이 짧을수록 팀은 위협이나 공격자가 사용자 환경 내에 머무는 시간과 기회를 최소화하여 궁극적으로 운영과 비즈니스에 미치는 위험과 영향을 줄일 수 있습니다.

지표 요약

인시던트 대응을 위한 지표를 설정하고 추적하면 인시던트 대응 기능을 효과적으로 측정, 평가 및 개선할 수 있습니다. 이를 달성하기 위해 이 섹션에서 강조한 몇 가지 일반적인 인시던트 대응 지표가 있습니다. 표 5에는 이러한 지표가 요약되어 있습니다.

표 5 - 인시던트 대응 지표

지표	설명
평균 탐지 시간	가능한 보안 인시던트를 발견하는 데 걸리는 평균 시간
평균 승인 시간	가능한 보안 인시던트를 승인하고 우선순위를 지정하는 데 걸리는 평균 시간

지표	설명
평균 대응 시간	가능한 보안 인시던트에 대한 초기 대응을 시작하는 데 걸리는 평균 시간
평균 격리 시간	가능한 보안 인시던트를 격리하는 데 걸리는 평균 시간
평균 복구 시간	가능한 보안 인시던트로부터 안전한 운영을 위해 완전히 복귀하는 데 걸리는 평균 시간
공격자 체류 시간	공격자가 시스템 또는 환경에 액세스할 수 있는 평균 시간

손상의 표시자(IOC) 사용

손상 지표(IOC)는 네트워크, 시스템 또는 환경에서 관찰된 아티팩트로, 높은 수준의 신뢰도로 악의적인 활동이나 보안 인시던트를 식별할 수 있습니다. IOC는 IP 주소, 도메인, TCP 플래그 또는 페이로드와 같은 네트워크 수준 아티팩트, 실행 파일, 파일 이름 및 해시, 로그 파일 항목 또는 레지스트리 항목과 같은 시스템 또는 호스트 수준 아티팩트 등의 다양한 형태로 존재할 수 있습니다. 또한 특정 위협, 공격 또는 공격자의 방법론을 나타낼 수 있는 특정 항목 또는 아티팩트(특정 파일 또는 파일 및 레지스트리 항목 세트)의 존재, 특정 순서로 수행되는 작업(특정 IP에서 시스템에 로그인한 후 특정 비정상적인 명령이 이어지는 경우) 또는 네트워크 활동(특정 도메인을 오가는 비정상적인 인바운드 또는 아웃바운드 트래픽) 등의 항목 또는 활동의 조합일 수도 있습니다.

인시던트 대응 프로그램을 반복적으로 개선하기 위해 노력할 때 탐지 및 알림을 지속적으로 구축 및 개선하고 조사의 속도와 효율성을 개선하기 위한 메커니즘으로 IOC를 수집, 관리 및 활용하는 프레임워크를 구현해야 합니다. 먼저 인시던트 대응 프로세스의 분석 및 조사 단계에 IOC의 수집 및 관리를 통합하는 것부터 시작할 수 있습니다. 프로세스의 표준 부분으로 IOC를 선제적으로 식별, 수집, 저장하면 보다 포괄적인 위협 인텔리전스 프로그램의 일환으로 데이터 리포지토리를 구축하여 기존 탐지와 알림을 개선하고, 추가 탐지 및 알림을 구축하고, 이전에 아티팩트가 발견된 위치와 시간을 식별하고, 이전에 일치하는 IOC와 관련된 조사를 수행한 방법에 대한 문서를 작성하고 참조하는 데 사용할 수 있습니다.

지속적인 교육 및 훈련

교육과 훈련은 진화하고 지속적인 노력이므로 목적을 가지고 추진하고 유지해야 합니다. 팀이 진화하는 기술 상태 및 위협 환경에 상응하는 인식, 지식 및 역량을 유지하고 있는지 확인하는 다양한 메커니즘이 있습니다.

한 가지 메커니즘은 팀의 목표와 운영의 표준으로 평생 교육을 도입하는 것입니다. 준비 섹션에서 언급한 대로, 인시던트 대응 담당자와 이해관계자는 AWS 내에서 발생하는 인시던트를 탐지하고 대응하고 조사하는 방법에 대한 효과적인 교육을 받아야 합니다. 하지만 교육은 '한 번으로 끝나는 것'이 아닙니다. 팀이 대응의 효과성과 효율성을 개선하는 데 활용할 수 있는 최신 기술 발전, 업데이트 및 개선 사항과 조사 및 분석을 개선하는 데 활용할 수 있는 데이터 추가 사항이나 업데이트 사항에 대한 인식을 유지하고 있는지 확인하기 위해 지속적으로 교육을 실시해야 합니다.

또 다른 메커니즘은 시뮬레이션이 정기적으로(예: 분기별) 수행되고 비즈니스의 특정 성과에 초점을 두고 있는지 확인하는 것입니다. 이 문서의 the section called "정기 시뮬레이션 실행" 섹션을 참조하세요.

초기 테이블탑 연습을 실시하는 것은 개선을 위한 초기 기준을 생성하는 훌륭한 방법이지만, 지속적인 개선과 현재 운영 상태를 정확하게 반영하는 최신 정보를 유지하려면 지속적인 테스트가 중요합니다. 최신의 가장 중요한 보안 상황과 가장 중요하거나 새로운 대응 역량을 테스트하고, 이를 통해 파악한 내용을 교육, 운영, 프로세스/절차에 통합하면 대응 프로세스와 프로그램 전체를 지속적으로 개선할 수 있습니다.

결론

클라우드 여정을 계속 진행하면서 AWS 환경에 대한 기본적인 보안 인시던트 대응 개념을 고려하는 것이 중요합니다. 사용 가능한 제어, 클라우드 기능 및 문제 해결 옵션을 결합하여 클라우드 환경의 보안을 개선할 수 있습니다. 또한 소규모로 시작하여 대응 속도를 개선하는 자동화 기능을 도입하면서 반복하여 보안 이벤트가 발생할 때 더 잘 대비할 수 있습니다.

기여자

다음은 이 문서의 현재 및 과거 기여자입니다.

- Anna McAbee, Amazon Web Services의 Senior Security Solutions Architect
- Freddy Kasprzykowski, Amazon Web Services Senior Security Consultant
- Jason Hurst, Amazon Web Services Senior Security Engineer
- Jonathon Poling, Amazon Web Services Principal Security Consultant

- Josh Du Lac, Amazon Web Services Security Solutions Architecture Senior Manager
- Paco Hope, Amazon Web Services Principal Security Engineer
- Ryan Tick, Amazon Web Services Senior Security Engineer
- Steve de Vera, Amazon Web Services Senior Security Engineer

부록 A: 클라우드 기능 정의

AWS는 200개 이상의 클라우드 서비스와 수천 개의 기능을 제공합니다. 이러한 기능 중 다수는 기본 탐지, 예방 및 대응 기능을 제공하며, 다른 기능은 맞춤형 보안 솔루션을 설계하는 데 사용할 수 있습니다. 이 섹션에는 클라우드의 인시던트 대응과 가장 관련이 있는 서비스의 하위 세트가 포함되어 있습니다.

주제

로깅 및 이벤트

AWS CloudTrail - AWS 계정의 거버넌스, 규정 준수, 운영 감사 및 위험 감사를 지원하는 AWS CloudTrail 서비스입니다. CloudTrail을 사용하면 AWS 서비스 전반의 작업과 관련된 계정 활동을 로깅하고, 지속적인 모니터링하고, 유지할 수 있습니다. CloudTrail은 AWS Management Console, AWS SDK, 명령줄 도구 및 기타 AWS 서비스를 통해 수행된 작업을 포함하여 AWS 계정 활동의 이벤트 기록을 제공합니다. 이 이벤트 기록은 보안 분석, 리소스 변경 추적 및 문제 해결을 간소화합니다. CloudTrail은 두 가지 유형의 AWS API 작업을 로깅합니다.

- CloudTrail 관리 이벤트(컨트롤 플레인 작업이라고도 함)는 AWS 계정의 리소스에서 수행되는 관리 작업을 보여줍니다. 여기에는 Amazon S3 버킷 생성, 로깅 설정 등의 작업이 포함됩니다.
- 데이터 플레인 작업이라고도 하는 CloudTrail 데이터 이벤트는 AWS 계정의 리소스에서 수행된 리소스 작업을 보여줍니다. 이러한 작업은 대량의 활동인 경우가 많습니다. 여기에는 Amazon S3 객체 수준 API 활동(예:`GetObject`, `DeleteObject` 및 `PutObject` API 작업) 및 Lambda 함수 간접 호출 활동과 같은 작업이 포함됩니다.

AWS Config – AWS Config는 고객이 AWS 리소스 구성을 평가, 감사 및 검증할 수 있도록 지원하는 서비스입니다. AWS Config는 AWS 리소스 구성을 지속적으로 모니터링하고 기록하며, 기록된 구성을 원하는 구성과 비교하여 자동으로 평가할 수 있도록 지원합니다. AWS Config를 사용하면 고객은 AWS 리소스 간 구성 및 관계의 변경 사항을 수동 또는 자동으로 검토하고, 자세한 리소스 구성 내역을 검토하고, 고객 지침에 지정된 구성에 대한 전반적인 규정 준수 여부를 확인할 수 있습니다. 이를 통해 규정 준수 감사, 보안 분석, 변경 관리 및 운영 문제 해결이 간소화됩니다.

Amazon EventBridge – Amazon EventBridge는 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트 스트림을 거의 실시간으로 제공하거나 AWS CloudTrail에서 API 직접 호출이 게시되는 시점을 알려줍니다. 신속하게 설정할 수 있는 단순 규칙을 사용하여 일치하는 이벤트를 검색하고 하나 이상의 대상 함수 또는 스트림으로 이를 라우팅할 수 있습니다. EventBridge는 운영 변경 사항이 발생할 때 이를 인식하게 됩니다. EventBridge는 환경에 대응하기 위한 메시지를 전송하고 함수를 활성화하고 변경을 수행하고 상태 정보를 기록하는 등 이러한 운영 변경 사항에 대응하고 필요에 따라 시정 조치를 취할 수 있습니다. Amazon GuardDuty와 같은 일부 보안 서비스는 EventBridge 이벤트 형태로 출력을 생성합니다. 또한 많은 보안 서비스에서 출력을 Amazon S3로 전송하는 옵션을 제공합니다.

Amazon S3 액세스 로그 - 민감한 정보가 Amazon S3 버킷에 저장되는 경우 고객은 Amazon S3 액세스 로그를 활성화하여 해당 데이터에 대한 모든 업로드, 다운로드 및 수정을 기록할 수 있습니다. 이 로그는 버킷 자체의 변경 사항(액세스 정책 및 수명 주기 정책 변경 등)을 기록하는 CloudTrail 로그와 별개로 작성되며 이에 추가됩니다. 액세스 로그 레코드는 최대한 전송하겠지만 항상 모든 레코드가 전송된다고 보장할 수는 없다는 점에 주목할 필요가 있습니다. 버킷에 대해 적절히 로깅이 구성된 대부분의 요청은 로그 레코드가 전송됩니다. 모든 서버 로깅이 제때 전송될 것이라고 보장할 수는 없습니다.

Amazon CloudWatch Logs - 고객은 Amazon CloudWatch Logs를 사용하여 CloudWatch Logs 에이전트가 있는 Amazon EC2 인스턴스에서 실행되는 운영 체제, 애플리케이션 및 기타 소스에서 생성된 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. CloudWatch Logs는 AWS CloudTrail, Route 53 DNS 쿼리, VPC 흐름 로그, Lambda 함수 등의 대상이 될 수 있습니다. 그런 다음 고객은 CloudWatch Logs에서 관련 로그 데이터를 검색할 수 있습니다.

Amazon VPC 흐름 로그 – VPC 흐름 로그를 사용하여 고객은 VPC의 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 캡처할 수 있습니다. 흐름 로그를 활성화한 후 Amazon CloudWatch Logs와 Amazon S3로 스트리밍할 수 있습니다. VPC 흐름 로그를 사용하면 특정 트래픽이 인스턴스에 도달하지 않는 이유의 문제 해결, 지나치게 제한적인 보안 그룹 규칙 진단, 이를 보안 도구로 사용하여 EC2 인스턴스로의 트래픽을 모니터링하는 등의 다양한 태스크를 수행할 수 있습니다. 가장 강력한 필드를 얻으려면 최신 버전의 VPC 흐름 로깅을 사용하세요.

AWS WAF 로그 - AWS WAF는 서비스에서 검사하는 모든 웹 요청의 전체 로깅을 지원합니다. 고객은 이를 Amazon S3에 저장하여 규정 준수 및 감사 요구 사항을 충족하고 디버깅 및 포렌식을 수행할 수

있습니다. 이러한 로그는 고객이 시작된 규칙과 차단된 웹 요청의 근본 원인을 파악하는 데 도움이 됩니다. 로그는 타사 SIEM 및 로그 분석 도구와 통합할 수 있습니다.

Route 53 Resolver 쿼리 로그 - Route 53 Resolver 쿼리 로그를 사용하면 Amazon Virtual Private Cloud(Amazon VPC) 내의 리소스에서 수행한 모든 DNS 쿼리를 로깅할 수 있습니다. Amazon EC2 인스턴스, AWS Lambda 함수, 컨테이너 등 어떤 것이든 Amazon VPC에 있고 DNS 쿼리를 수행하면 이 기능이 이를 기록하여 애플리케이션이 어떻게 작동하는지 탐색하고 더 잘 이해할 수 있습니다.

기타 AWS 로그 - AWS는 새로운 로깅 및 모니터링 기능을 갖춘 고객을 위해 서비스 기능을 지속적으로 릴리스합니다. 각 AWS 서비스에 사용할 수 있는 기능에 대한 자세한 내용은 공개 설명서를 참조하세요.

가시성 및 알림

AWS 보안 인시던트 대응 - AWS 보안 인시던트 대응은(는) 자동화된 기능과 전문가의 지원을 결합하여 조직이 수명 주기 동안 보안 이벤트를 처리할 수 있도록 지원하는 포괄적인 서비스입니다. 이 서비스는 자동화된 모니터링 및 조사 기능을 활용하여 조직 리소스를 확보하는 동시에 보안 감독을 철저히 유지하고, 보안 이벤트가 발생하면 신속한 대응 시간을 위해 이해관계자 간의 커뮤니케이션 및 조정을 가속화합니다. 이 서비스는 보안 이벤트의 준비 및 시뮬레이션, 활성 인시던트에 대한 대응, 간소화된 인시던트 후 보고 및 분석 등 여러 사용 사례를 지원하므로 조직은 모든 단계에서 보안 문제를 처리할 수 있도록 잘 대비할 수 있게 됩니다.

AWS Security Hub CSPM - AWS Security Hub CSPM는 고객에게 AWS 계정 전반의 우선순위가 높은 보안 알림과 규정 준수 상태에 대한 포괄적인 보기를 제공합니다. Security Hub CSPM은 Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Partner 솔루션 등의 AWS 서비스에서 나온 위협 조사 결과를 집계 및 정리하고 우선순위를 지정합니다. 조사 결과는 실행 가능한 그래프와 표가 포함된 통합 대시보드에 시각적으로 요약됩니다. AWS 모범 사례와 조직에서 따르는 업계 표준을 기반으로 한 자동 규정 준수 검사를 사용하여 환경을 지속적으로 모니터링할 수도 있습니다.

Amazon GuardDuty - Amazon GuardDuty는 고객이 AWS 계정과 워크로드를 보호할 수 있도록 악의적이거나 승인되지 않은 동작을 지속적으로 모니터링하는 관리형 위협 탐지 서비스입니다. 이 서비스는 비정상적인 API 직접 호출이나 잠재적으로 승인되지 않은 배포와 같은 활동을 모니터링하여 악의적인 행위자에 의한 Amazon EC2 인스턴스, Amazon S3 버킷의 계정 또는 리소스 손상이나 정찰 가능성을 보여줍니다.

GuardDuty는 기계 학습을 사용하여 계정 및 워크로드 활동의 이상을 탐지하는 통합 위협 인텔리전스 피드를 통해 의심스러운 공격자를 식별합니다. 잠재적 위협이 탐지되면 서비스는 GuardDuty 콘솔과 CloudWatch Events에 자세한 보안 알림을 전송합니다. 따라서 알림을 실행 가능하고 간단하게 기존 이벤트 관리 및 워크플로 시스템에 통합할 수 있습니다.

GuardDuty는 또한 특정 서비스의 위협을 모니터링하기 위한 두 가지 추가 기능인 Amazon S3 보호를 위한 Amazon GuardDuty와 Amazon EKS 보호를 위한 Amazon GuardDuty를 제공합니다. Amazon S3 보호는 GuardDuty가 객체 수준 API 작업을 모니터링하도록 활성화하여 Amazon S3 버킷 내 데이터에서 잠재적인 보안 위험을 식별하는 데 도움이 됩니다. Kubernetes 보호를 통해 GuardDuty는 Amazon EKS 내에서 Kubernetes 클러스터의 의심스러운 활동 및 잠재적 손상을 탐지할 수 있습니다.

Amazon Macie - Amazon Macie는 AWS에 저장된 민감한 데이터를 자동으로 검색, 분류 및 보호하여 데이터 손실을 방지하는 데 도움이 되는 AI 기반 보안 서비스입니다. Macie는 기계 학습(ML)을 사용하여 개인 식별 정보(PII) 또는 지적 재산과 같은 민감한 데이터를 인식하고, 비즈니스 가치를 할당하고, 이 데이터가 저장되는 위치와 조직에서 사용되는 방식에 대한 가시성을 제공합니다. Amazon Macie는 데이터 액세스 활동에 이상이 있는지 지속적으로 모니터링하고 무단 액세스 또는 의도하지 않은 데이터 유출 위험을 탐지하면 알림을 제공합니다.

AWS Config 규칙 - AWS Config 규칙은 리소스에 대한 기본 구성을 나타내며 AWS Config에서 기록한 대로 관련 리소스의 구성 변경 사항에 대해 평가됩니다. 대시보드에서 리소스 구성에 대해 규칙을 평가한 결과를 볼 수 있습니다. AWS Config 규칙을 사용하면 구성 관점에서 전체 규정 준수 및 위험 상태를 평가하고, 시간 경과에 따른 규정 준수 추세를 보고, 어떤 구성 변경으로 인해 리소스가 규칙을 준수하지 않게 되었는지 확인할 수 있습니다.

AWS Trusted Advisor - AWS Trusted Advisor는 AWS 환경을 최적화하여 비용을 절감하고, 성능을 높이고, 보안을 강화하는 데 도움이 되는 온라인 리소스입니다. Trusted Advisor는 AWS 모범 사례에 따라 리소스를 프로비저닝하는 데 도움이 되는 실시간 지침을 제공합니다. CloudWatch Events 통합을 포함한 전체 Trusted Advisor 검사 세트는 Business Support 및 Enterprise Support 플랜 고객이 사용할 수 있습니다.

Amazon CloudWatch – Amazon CloudWatch는 AWS 클라우드 리소스 및 AWS에서 실행하는 애플리케이션을 모니터링하는 서비스입니다. CloudWatch를 사용하여 지표를 수집 및 추적하고, 로그 파일을 수집 및 모니터링하며, 경보를 설정하고, AWS 리소스 변경에 자동으로 대응할 수 있습니다. CloudWatch는 Amazon EC2 인스턴스, Amazon DynamoDB 테이블, Amazon RDS DB 인스턴스와 같은 AWS 리소스뿐만 아니라 애플리케이션 및 서비스에서 생성된 사용자 지정 지표와 애플리케이션이 생성하는 모든 로그 파일을 모니터링할 수 있습니다. Amazon CloudWatch를 사용하여 시스템 전반의 리소스 사용률, 애플리케이션 성능, 운영 상태를 파악할 수 있습니다. 상황에 대처하고 애플리케이션을 원활하게 운영하는 데 이러한 정보를 사용할 수 있습니다.

Amazon Inspector - Amazon Inspector는 AWS에 배포된 애플리케이션의 보안 및 규정 준수를 개선하는 데 도움이 되는 자동 보안 평가 서비스입니다. Amazon Inspector는 자동으로 애플리케이션의 취약점 또는 모범 사례와의 차이를 평가합니다. 평가를 수행한 후, Amazon Inspector는 상세한 보안 평가 결과 목록을 제공하며, 이 목록은 심각도 수준에 따라 구성되어 있습니다. 이러한 조사 결과를 직접 검

토하거나 Amazon Inspector 콘솔 또는 API를 통해 사용할 수 있는 세부 평가 보고서의 일부로 검토할 수 있습니다.

Amazon Detective - Amazon Detective는 AWS 리소스에서 로그 데이터를 자동으로 수집하고 기계 학습, 통계 분석 및 그래프 이론을 사용하여 연결된 데이터 세트를 구축하여 더 빠르고 효율적인 보안 조사를 수행할 수 있는 보안 서비스입니다. Detective는 VPC 흐름 로그, CloudTrail 및 GuardDuty와 같은 여러 데이터 소스의 수조 개의 이벤트를 분석할 수 있으며, 시간 경과에 따른 리소스, 사용자 및 상호 작용에 대한 통합된 대화형 보기를 자동으로 생성합니다. 이 통합 보기를 사용하면 모든 세부 정보와 컨텍스트를 한 곳에서 시각화하여 조사 결과의 기본 원인을 식별하고, 관련 기록 활동을 자세히 살펴보고, 근본 원인을 신속하게 확인할 수 있습니다.

자동화

AWS Lambda – AWS Lambda는 이벤트에 대한 대응으로 코드를 실행하고 자동으로 기본 컴퓨팅 리소스를 관리하는 서버리스 컴퓨팅 서비스입니다. Lambda를 사용하여 사용자 지정 로직으로 다른 AWS 서비스를 확장하거나 AWS 규모와 성능, 보안에 따라 작동하는 자체 백엔드를 만들 수 있습니다. Lambda는 고가용성 컴퓨팅 인프라에서 코드를 실행하고 컴퓨팅 리소스 관리를 수행합니다. 여기에는 서버 및 운영 체제 유지 관리, 용량 프로비저닝 및 오토 스케일링, 코드 및 보안 패치 배포, 코드 모니터링 및 로깅이 포함됩니다. 코드를 제공하기만 하면 됩니다.

AWS Step Functions – AWS Step Functions는 시각적 워크플로우를 사용해 분산 애플리케이션 및 마이크로서비스의 구성 요소를 손쉽게 조정하도록 해주는 웹 서비스입니다. Step Functions는 애플리케이션의 구성 요소를 일련의 단계로 정리하고 시각화할 수 있는 그래픽 콘솔을 제공합니다. 따라서 다단계 애플리케이션을 간단하게 빌드하고 실행할 수 있습니다. Step Functions는 각 단계를 자동으로 시작하고 추적하며 오류가 발생하면 재시도하므로 애플리케이션이 순서에 따라 예상대로 실행됩니다.

Step Functions는 각 단계의 상태를 기록합니다. 따라서 무언가 잘못된 경우 빠르게 문제를 진단하고 디버깅할 수 있습니다. 코드를 작성하지 않고도 단계를 변경하고 추가할 수 있으므로 애플리케이션을 발전시키고 더 빠르게 혁신할 수 있습니다. AWS Step Functions는 AWS 서버리스의 일부로, 서버리스 애플리케이션을 위한 AWS Lambda 함수를 간단하게 오케스트레이션할 수 있습니다. Amazon EC2 및 Amazon ECS와 같은 컴퓨팅 리소스를 사용하여 마이크로서비스 오케스트레이션에 Step Functions를 사용할 수도 있습니다.

AWS Systems Manager – AWS Systems Manager는 AWS의 인프라에 대한 가시성 및 제어 기능을 제공합니다. Systems Manager는 통합된 사용자 인터페이스를 제공하므로 여러 AWS 서비스의 운영 데이터를 보고 AWS 리소스 전체에서 운영 태스크를 자동화할 수 있습니다. Systems Manager를 사용하면 애플리케이션별로 리소스를 그룹화하고, 모니터링 및 문제 해결을 위한 운영 데이터를 보고, 리소스 그룹에 대해 조치를 취할 수 있습니다. Systems Manager는 인스턴스를 정의된 상태로 유지하고, 애플

리케이션 업데이트 또는 쉘 스크립트 실행과 같은 온디맨드 변경을 수행하고, 기타 자동화 및 패치 적용 태스크를 수행할 수 있습니다.

보안 스토리지

Amazon Simple Storage Service – Amazon S3는 어디서든 원하는 양의 데이터를 저장하고 검색할 수 있도록 구축된 객체 스토리지입니다. 이는 99.999999999%의 내구성을 제공하도록 설계되었으며 모든 업계의 시장 리더가 사용하는 수백만 개의 애플리케이션에 대한 데이터를 저장합니다. Amazon S3는 포괄적인 보안을 제공하며 규제 요구 사항을 충족하는 데 도움이 되도록 설계되었습니다. 이를 통해 고객은 비용 최적화, 액세스 제어 및 규정 준수를 위해 데이터를 관리하는 데 사용하는 방법을 유연하게 선택할 수 있습니다. Amazon S3는 Amazon S3의 저장 데이터에 대해 직접 강력한 분석을 실행할 수 있는 인플레이스 쿼리 기능을 제공합니다. Amazon S3는 타사 솔루션, 시스템 통합 파트너 및 기타 AWS 서비스로 구성된 가장 큰 커뮤니티 중 하나에서 통합된 고도로 지원되는 클라우드 스토리지 서비스입니다.

Amazon Glacier – Amazon Glacier는 데이터 보관 및 장기 백업을 위한 안전하고 안정적이며 극히 저렴한 클라우드 스토리지 서비스입니다. 또한 99.999999999%의 내구성을 제공하도록 설계되었으며, 포괄적인 보안을 제공하고, 규제 요구 사항을 충족하는 데 도움이 되도록 설계되었습니다. Amazon Glacier는 아카이브 저장 데이터에 대해 직접 강력한 분석을 실행할 수 있는 인플레이스 쿼리 기능을 제공합니다. 비용을 낮추면서도 다양한 검색 요구 사항에 적합하도록 Amazon Glacier는 몇 분에서 몇 시간까지 아카이브에 액세스할 수 있는 세 가지 옵션을 제공합니다.

미래 및 사용자 지정 보안 기능

앞서 언급한 서비스와 기능은 전체 목록이 아닙니다. AWS는 지속적으로 새로운 기능을 추가하고 있습니다. 자세한 내용은 AWS의 새로운 소식 및 AWS 클라우드 보안 페이지를 참조하세요. AWS가 기본 클라우드 서비스로 제공하는 보안 서비스 외에도, AWS 서비스를 기반으로 자체 역량을 구축하는 데 관심이 있을 수 있습니다.

계정 내에서 AWS CloudTrail, Amazon GuardDuty, Amazon Macie 등의 기본 보안 서비스 세트를 활성화하는 것이 좋지만, 로그 자산에서 추가 가치를 도출하기 위해 이러한 기능을 확장하는 것이 좋습니다. APN Security Competency 프로그램에 나열된 도구를 비롯한 다양한 파트너 도구를 사용할 수 있습니다. 로그를 검색하기 위해 쿼리를 직접 작성할 수도 있습니다. AWS에서 제공하는 다양한 관리형 서비스 덕분에 이 작업은 그 어느 때보다 쉬워졌습니다. 이 백서의 범위를 벗어나는 조사에 도움이 되는 추가 AWS 서비스로는 Amazon Athena, Amazon OpenSearch Service, Amazon Quick, Amazon Machine Learning, Amazon EMR 등이 있습니다.

부록 B: AWS 인시던트 대응 리소스

AWS는 고객이 인시던트 대응 기능을 개발하는 데 도움이 되는 리소스를 게시합니다. 대부분의 예시 코드와 절차는 AWS 외부 GitHub 퍼블릭 리포지토리에서 찾을 수 있습니다. 다음은 인시던트 대응을 수행하는 방법의 예를 제공하는 몇 가지 리소스입니다.

플레이북 리소스

- 인시던트 대응을 위한 프레임워크 플레이북 - 고객이 AWS 서비스 사용 시 잠재적인 공격 시나리오에 대비하여 보안 플레이북을 생성, 개발 및 통합할 수 있는 예시 프레임워크입니다.
- 인시던트 대응 플레이북 샘플 - AWS 고객이 직면한 일반적인 시나리오를 다루는 플레이북입니다.
- AWS에서 공개적으로 사용 가능한 5개의 워크샵 출시를 발표합니다.

포렌식 리소스

- 자동 인시던트 대응 및 포렌식 프레임워크 - 이 프레임워크와 솔루션은 격리, 획득, 검사 및 분석 단계로 구성된 표준 디지털 포렌식 프로세스를 제공합니다. AWS Λ 함수를 활용하여 자동화된 반복 가능한 방식으로 인시던트 대응 프로세스를 트리거합니다. 자동화 단계를 운영하고, 아티팩트를 저장하고, 포렌식 환경을 생성하기 위한 계정 분리를 제공합니다.
- Amazon EC2용 자동 포렌식 오케스트레이터 - 이 구현 가이드는 잠재적 보안 문제가 탐지되는 경우 포렌식 분석을 위해 EC2 인스턴스와 연결된 볼륨에서 데이터를 캡처하고 검사하는 셀프 서비스 솔루션을 제공합니다. 솔루션을 배포하기 위한 AWS CloudFormation 템플릿이 있습니다.
- AWS에서 포렌식 디스크 수집을 자동화하는 방법 - 이 AWS 블로그에서는 잠재적 보안 인시던트의 범위와 영향을 확인하기 위해 분석을 위한 디스크 증거를 캡처하도록 자동화 워크플로를 설정하는 방법을 자세히 설명합니다. 솔루션을 배포하기 위한 AWS CloudFormation 템플릿도 포함되어 있습니다.

Notices

문서 이력

다음 표에서는 2026년 1월 1일 이후의 AWS Security Incident Response 설명서에 대한 중요 추가 사항을 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드에 가입하면 됩니다.

변경 사항	설명	날짜
AWS Security Incident Response 분류 서비스 역할 정책의 정책 설명 업데이트	해당 서비스가 서비스 조정을 개선하고 잠재적 인시던트를 조사하기 위한 정보를 수집할 수 있도록 하는 변경 사항을 반영하여 AWS Security Incident Response 분류 서비스 역할 정책의 정책 설명을 업데이트합니다.	2026년 3월 27일
메타데이터 제출	AWS Support 사례를 통해 메타데이터 제출에 대한 지침을 추가했습니다.	2026년 3월 27일
격리 기본 설정 제출	AWS Support 사례를 통해 격리 기본 설정 제출에 대한 지침을 추가했습니다.	2026년 3월 27일
격리 StackSet 템플릿	격리 StackSet CloudFormation 템플릿을 업데이트했습니다.	2026년 3월 27일
위임된 관리자 계정에 대한 AWS 리전 고려 사항을 명확히 함	초기 설정 중에 하나의 AWS 리전에서 위임된 AWS Security Incident Response 관리자 계정을 지정하지만, 해당 서비스는 지원되는 모든 AWS 리전에서 조직 전체 범위를 지원한다는 점을 명확히 했습니다.	2026년 3월 20일
격리 작업 기본 설정 정의	현재 옵션과 일치하도록 격리 작업 기본 설정 섹션을 업데이트했습니다.	2026년 3월 19일

선제적 대응 및 알림 분류	사전 대응 및 알림 분류 워크플로가 선택 사항이라는 참조 내용을 제거했습니다.	2026년 3월 3일
응답 타임라인	사례 승인에 15분 SLO, 사례 종결 전 고객 응답에 영업일 기준 5일로 응답 타임라인을 업데이트했습니다.	2026년 2월 24일
커뮤니케이션 모범 사례	중요한 정보 요청에 대한 고객 응답에 영업일 기준 5일로 사례 종결 타임라인을 업데이트했습니다.	2026년 2월 24일
AWS CloudShell를 사용하여 Security Incident Response과 상호 작용에 AWS CLI 참조 추가함	AWS Security Incident Response용 AWS Command Line Interface Reference 참조의 링크를 추가했습니다.	2026년 2월 24일
RACI 매트릭스	RACI 매트릭스에서 ‘CIRT 격리 작업 권한 부여’를 ‘격리 작업 권한 부여’로 업데이트했습니다.	2026년 2월 13일
격리 기본 설정	격리 기본 설정 옵션을 '격리 작업 없음', '승인을 통한 격리', '자동 격리'에서 '승인 필요', '확인 항목 격리', '의심 항목 격리'로 업데이트하고 설명을 수정했습니다.	2026년 2월 13일
Security Incident Response의 사후 배포	AWS Security Incident Response: 새 통합 및 OU 수준 구독 데모에 대한 링크를 추가했습니다.	2026년 2월 4일
모니터링 및 조사	이 페이지의 소개 및 하위 섹션에 수정된 내용을 추가했습니다.	2026년 2월 4일

탐지 및 분석	이 페이지의 소개 및 하위 섹션에 수정된 내용을 추가했습니다.	2026년 2월 4일
격리	이 페이지에 수정된 내용을 추가했습니다.	2026년 2월 4일
AI 조사 에이전트	이 페이지에 고객 데이터 사용 면책 조항을 추가했습니다. 면책 조항: AI 조사 에이전트는 모델 훈련에 고객 데이터를 사용하지 않으며 고객 데이터를 서드 파티와 공유하지 않습니다.	2026년 2월 4일

변경	설명	날짜
멤버십 취소	멤버십 및 서비스가 결제 주기 종료 시점이 아닌 취소 즉시 종료된다는 것을 알리도록 멤버십 취소 페이지를 업데이트했습니다.	2025년 11월 20일
AWS 관리형 정책	서비스에서 제공되는 작업 목록에 사례 업데이트, 사례 설명 생성, 사례 나열, 사례 설명 나열을 추가했습니다.	2025년 11월 19일
서비스 연결 역할 사용	서비스에서 제공되는 작업 목록에 사례 업데이트, 사례 설명 생성, 사례 나열, 사례 설명 나열을 추가했습니다.	2025년 11월 19일
통신 기본 설정	생성 및 업데이트 새로운 기능 설명서에 통신 기본 설정 섹션이 추가됨	2025년 11월 12일

변경	설명	날짜
온보딩 가이드 추가 및 업데이트	생성 및 업데이트 다음 섹션을 포함한 온보딩 가이드가 추가됨 Security Incident Response 활성화 섹션을 추가했습니다. Security Incident Response 엔지니어가 위협 격리 작업을 수행하도록 권한 승인 섹션을 추가했습니다. Security Incident Response의 사후 배포 섹션을 추가했습니다. 인시던트 대응 팀 업데이트 섹션이 추가되었습니다. GuardDuty 결과 및 억제 규칙 섹션이 추가되었습니다. Amazon EventBridge 섹션이 추가되었습니다. 통합 및 외부 도구 워크플로 섹션이 추가되었습니다. 외부 도구 워크플로 섹션이 추가되었습니다. 부록 A: 연락 담당자 섹션이 추가되었습니다.	2025년 11월 12일

변경	설명	날짜
규정 준수 및 결제 언어 업데이트	AWS 보안 인시던트 대응은 프레임워크에서 다루지 않는다는 문구가 제거되도록 업데이트되었습니다. AWS 보안 인시던트 대응은 이제 HITRUST에서 다루며 향후 더 많은 기능이 제공될 예정입니다. AWS 보안 인시던트 대응을 추가하도록 가시성 및 제어가 업데이트되었습니다. 서비스 결제 기간을 명확히 하기 위해 멤버십 취소가 업데이트되었습니다. 일반적인 작업 시 AWS 보안 인시던트 대응 사용을 시작하기 위한 추가 컨텍스트를 제공하는 비디오를 시작하기에 추가했습니다.	2025년 8월 15일

변경	설명	날짜
업데이트됨 - AWSSecurityIncidentResponseServiceRolePolicy	이제 정책에 `"organizations:DescribeAccount"` , `"organizations:ListDelegatedAdministrators"` 에 대한 두 가지 새 작업과 새 조건이 포함됩니다. `"Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } }`	TBD
기능 업데이트: 특정 조직 단위(OU) 또는 전체 AWS 조직 구독	특정 조직 단위(OU) 또는 전체 AWS 조직을 구독하기 위한 업데이트를 반영하도록 사용자 인터페이스의 도움말 패널이 업데이트되었습니다. 조직 단위(OU)의 멤버십 관리를 위한 새 페이지 생성 새로운 OU 관리 기능을 반영하도록 AWS Organizations에 관련된 페이지가 업데이트되었습니다.	2025년 8월 7일

변경	설명	날짜
업데이트된 Service Quotas	사용자를 AWS 보안 인시던트 대응 엔드포인트 및 할당량에 대한 AWS 일반 참조 가이드로 안내하도록 Service Quotas 페이지가 업데이트되었습니다.	2025년 8월 7일
사용자 피드백 업데이트	서비스에 대한 하이퍼링크가 AWS 보안 인시던트 대응 사례에 추가되었습니다. 보안 기술 가이드용의 컴퓨터 보안 인시던트 처리 가이드 SP 800-61 r3을 반영하도록 업데이트되었습니다.	2025년 8월 7일
AWS Security Incident Response와 Amazon EventBridge 통합을 위한 페이지 추가	AWS Security Incident Response에 Amazon EventBridge가 어떻게 통합되는지 설명하는 새로운 콘텐츠 섹션입니다.	2025년 6월 26일
서비스 자격을 지원하기 위한 권한을 추가하는 SLR 업데이트	AWSSecurityIncidentResponseTriageServiceRolePolicy가 업데이트되어 security-ir:GetMembership, security-ir:ListMemberships, security-ir:UpdateCase, guardduty:ListFilters, guarduty:UpdateFilter, guardduty:DeleteFilter 및 guardduty:GetAdministratorAccount 권한이 추가되었습니다. guardduty:GetAdministratorAccount가 추가되어 위임 계정에서 GuardDuty 자동 아카이브 필터를 쉽게 관리할 수 있습니다.	2025년 6월 2일

변경	설명	날짜
리소스 업데이트	고객이 사용할 수 있는 활성 워크숍을 반영하도록 https://docs.aws.amazon.com/security-ir/latest/userguide/appendix-b-incident-response-resources.html#playbook-resources가 업데이트되었습니다.	2025년 5월 23일
서비스는 일본어를 지원합니다.	일본 현지 시간으로 일본어 지원을 확인할 수 있도록 지원되는 구성이 업데이트되었습니다. 영어는 전 세계에서 지원됩니다.	2025년 5월 13일
콘텐츠 업데이트 및 고객 피드백.	위임 관리자 계정을 설정의 일부로 사용할 때 추가 태스크를 반영하도록 https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html에 참고 사항이 추가되었습니다. 서비스 생성 사례와 탐지 및 분석 작업 시 고객 경험이 업데이트되었습니다. 멤버십 취소 시 결제에 미치는 영향을 보다 명확하게 파악할 수 있도록 계정 취소 세부 정보가 업데이트되었습니다.	2025년 5월 9일
지원되는 새 리전 3개 추가	https://docs.aws.amazon.com/security-ir/latest/userguide/supported-configs.html에 3개의 새 리전 뭄바이, 상파울루, 파리가 추가되었습니다.	2025년 5월 7일

변경	설명	날짜
업데이트됨: 문서에 대한 고객 의견에 따른 업데이트	여러 페이지의 철자 및 문법 오류가 수정되었습니다. security-ir을 서비스 접두사로 정확하게 반영하도록 https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/organizations_permissions.html이 업데이트되었습니다. Route53 및 DNS와 관련하여 https://docs.aws.amazon.com/security-ir/latest/userguide/source-containment.html에 참고 사항이 추가되었습니다.	2025년 2월 7일

변경	설명	날짜
업데이트됨: 문서에 대한 고객 의견에 따른 업데이트	https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html이 스택 세트 템플릿으로 업데이트되었습니다. triage.security-ir.com 항목이 triage.security-ir.amazonaws.com으로 수정되었습니다. https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html에 AWSSupport-ContainEC2Reversible에 대한 추적되는 연결 참고 사항이 추가되었습니다. https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html에서 끊어진 링크가 수정되었습니다. https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html에 멤버십 계정에 대한 정의가 추가되었습니다. https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/using-service-linked-roles.html에 AWS Organizations 관리 계정에 대한 설명 참고 사항이 추가되었습니다.	2024년 12월 20일

변경	설명	날짜
업데이트됨: 문서에 대한 고객 의견에 따른 업데이트	텍스트에서 중복된 AWS AWS를 여러 개 제거했습니다. https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html과 https://docs.aws.amazon.com/security-ir/latest/userguide/service-name-info-in-cloudtrail.html에서 끊어진 링크가 수정되었습니다. https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html이 업데이트되었습니다. 첫 번째 단락에서 >가 제거되었습니다. AWSSupport-ContainEC2Reversible이 AWSSupport-ContainEC2Instance로 바뀌었습니다. AWSSupport-ContainIAMReversible이 AWSSupport-ContainIAMPrincipal로 바뀌었습니다. AWSSupport-ContainS3Reversible이 AWSSupport-ContainS3Resource로 바뀌었습니다. https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/issues.html의 서식이 업데이트되었습니다. 고객에게 지원 티켓을 통해 Security Incident Response	2024년 12월 10일

변경	설명	날짜
	에 문의하도록 안내할 때 이제 https://docs.aws.amazon.com/security-ir/latest/userguide/understand-response-teams-and-support.html에서 지원 양식에서 선택할 수 있는 옵션을 제공합니다. https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html에서 CloudWatch Events가 제거되고 EventBridge로 바뀌었습니다. ttps://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html에서 문법이 업데이트되었습니다. https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html에서 게시 날짜가 제거되고 이 표의 업데이트로 바뀌었습니다.	
업데이트됨: AWS 관리형 정책 및 서비스 연결 역할	관리형 정책 및 서비스 연결 역할 업데이트	2024년 12월 1일
서비스 시작	re:Invent 2024에서 서비스 출시를 위한 초기 서비스 문서	2024년 12월 1일