AWS 보안 인시던트 대응 사용 설명서

버전 December 1, 2024

AWS 보안 인시던트 대응 사용 설명서:

Table of Contents

AWS 보안 인시던트 대응이란 무엇입니까? 1
지원되는 구성 1
기능 요약 2
모니터링 및 조사 2
인시던트 대응 간소화 2
셀프 서비스 보안 솔루션 2
가시성을 위한 대시보드 3
보안 태세 3
신속 지원 3
준비 및 준비 3
개념 및 용어 4
시작하기 6
멤버십 계정 선택 6
멤버십 세부 정보 설정 7
계정과 연결 AWS Organizations 7
사전 대응 및 알림 분류 워크플로 설정 8
사용자 작업 9
대시보드 9
인시던트 대응 팀 관리 9
에 대한 계정 연결 AWS Organizations 10
모니터링 및 조사 2
준비 11
탐지 및 분석 11
포함 14
제거 16
복구 16
인시던트 후 보고서 17
Cases 18
AWS 지원되는 사례 생성 18
자체 관리형 사례 생성 20
AWS 생성된 사례에 대한 응답 21
사례 관리 21
사례 상태 변경 22
해석기 변경 22
작업 항목 22

사례 편집 23
통신 24
권한 24
첨부 24
Tags 25
사례 활동 25
사례 종료 25
AWS CloudFormation 스택 세트 작업 26
멤버십 취소 32
AWS 보안 인시던트 대응 리소스에 태그 지정 34
사용 AWS CloudShell 35
에 대한 IAM 권한 획득 AWS CloudShell 35
를 사용하여 보안 인시던트 대응과 상호 작용 AWS CloudShell 36
CloudTrail 로그 37
의 보안 인시던트 대응 정보 CloudTrail 37
보안 인시던트 대응 로그 파일 항목 이해 38
AWS Organizations을(를) 사용하여 계정 관리 41
사용 고려 사항 및 권장 사항 41
트러스트된 액세스 42
위임된 보안 인시던트 대응 관리자 계정을 지정하는 데 필요한 권한 43
위임된 관리자 AWS 보안 인시던트 대응 지정 45
AWS 보안 인시던트 대응에 멤버 추가 46
AWS 보안 인시던트 대응에서 멤버 제거 47
문제 해결 48
문제 48
오류 48
Support 49
보안 50
AWS 보안 인시던트 대응의 데이터 보호 50
데이터 암호화 51
인터네트워크 트래픽 개인 정보 보호 52
서비스와 온프레미스 클라이언트 및 애플리케이션 간의 트래픽 52
같은 리전에 있는 AWS 리소스 사이의 트래픽 52
ID 및 액세스 관리 53
ID를 통한 인증 53
AWS 보안 인시던트 대응의 작동 방식 IAM 56
AWS 보안 인시던트 대응 자격 증명 및 액세스 문제 해결 63

서비스 역할 사용 ... 65
서비스 연결 역할 사용 ... 65
AWSServiceRoleForSecurityIncidentResponse ... 66
AWSServiceRoleForSecurityIncidentResponse_평가 ... 67
에 지원되는 리전 SLRs ... 68
AWS 관리형 정책 ... 68
관리형 정책: AWSSecurityIncidentResponseServiceRolePolicy ... 69
관리형 정책: AWSSecurityIncidentResponseAdmin ... 70
관리형 정책: AWSSecurityIncidentResponseReadOnlyAccess ... 70
관리형 정책: AWSSecurityIncidentResponseCaseFullAccess ... 71
관리형 정책: AWSSecurityIncidentResponseTriageServiceRolePolicy ... 72
SLRs 및 관리형 정책에 대한 업데이트 ... 72
인시던트 대응 ... 74
규정 준수 확인 ... 74
AWS 보안 인시던트 대응의 로깅 및 모니터링 ... 75
복원성 ... 76
인프라 보안 ... 76
구성 및 취약성 분석 ... 76
교차 서비스 혼동된 대리인 방지 ... 77
Service Quotas ... 78
AWS 보안 인시던트 대응 ... 78
AWS 보안 인시던트 대응 기술 안내서 ... 80
요약 ... 80
귀사는 Well-Architected입니까? ... 80
소개 ... 81
시작하기 전 준비 사항 ... 81
AWS 인시던트 응답 개요 ... 82
준비 ... 87
사람 ... 88
프로세스 ... 91
기술 ... 98
준비 항목 요약 ... 104
운영 ... 108
탐지 ... 109
분석 ... 112
격리 ... 116
근절 ... 121

복구 123
결론 124
인시던트 사후 활동 125
인시던트에서 학습하기 위한 프레임워크 설정 125
성공을 위한 지표 설정 127
손상 지표 사용 130
지속적인 교육 및 훈련 130
결론 131
기여자 131
부록 A: 클라우드 기능 정의 131
로깅 및 이벤트 132
가시성 및 알림 134
자동화 135
보안 스토리지 136
미래 및 사용자 지정 보안 기능 137
부록 B: AWS 인시던트 응답 리소스 137
플레이북 리소스 137
포렌식 리소스 137
고지 사항 138
문서 기록 139
..... cxliii

AWS 보안 인시던트 대응이란 무엇입니까?

AWS 보안 인시던트 대응을 사용하면 보안 인시던트 복구에 도움이 되는 지침을 신속하게 준비, 대응 및 받을 수 있습니다. 여기에는 계정 탈취, 데이터 침해, 랜섬웨어 공격과 같은 인시던트가 포함됩니다.

AWS Security Incident Response는 조사 결과를 분류하고, 보안 이벤트를 에스컬레이션하고, 즉각적인 주의가 필요한 사례를 관리합니다. 또한 AWS 고객 인시던트 대응 팀(CIRT)에 액세스하여 영향을 받는 리소스를 조사할 수 있습니다.

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

AWS 보안 인시던트 대응은 다른 AWS 탐지 및 대응 서비스와 함께 작동하여 탐지에서 복구에 이르기까지 전체 인시던트 수명 주기를 안내합니다.

내용

- 지원되는 구성
- 기능 요약

지원되는 구성

AWS 보안 인시던트 대응은 다음 언어 및 리전 구성을 지원합니다.

- 언어: AWS 보안 인시던트 대응은 영어로 제공됩니다.
- 지원되는 AWS 리전:

  AWS 보안 인시던트 대응은의 하위 집합에서 사용할 수 있습니다 AWS 리전. 이러한 지원되는 리전에서는 멤버십을 생성하고, 사례를 생성 및 보고, 대시보드에 액세스합니다.
  - 미국 동부(오하이오)
  - 미국 서부(오리건)
  - 미국 동부(버지니아)
  - EU(프랑크푸르트)
  - EU(아일랜드)

- EU(런던)
- EU(스톡홀름)
- 아시아 태평양(싱가포르)
- 아시아 태평양(서울)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 캐나다(중부)

모니터링 및 조사 기능을 활성화하면 AWS 보안 인시던트 대응은 모든 활성 상용 제품의 Amazon GuardDuty 결과를 모니터링합니다 AWS 리전. 보안 모범 사례로는 지원되는 모든 AWS 리전 GuardDuty 에서를 활성화하는 AWS 것을 권장합니다. 이 구성을 사용하면 리소스를 적극적으로 배포하지 않는 AWS 리전 경우에도가 무단 또는 비정상적인 활동에 대한 결과를 GuardDuty 생성할 수 있습니다. 이렇게 하면 전반적인 보안 태세를 강화하고 AWS 환경 전체에서 포괄적인 위협 탐지 범위를 유지할 수 있습니다.

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

기능 요약

모니터링 및 조사

AWS Security Incident Response는 Amazon GuardDuty 및 타사와의 통합의 보안 알림을 신속하게 검토하여 팀이 분석해야 하는 수를 AWS Security Hub줄입니다. 환경을 기반으로 억제 규칙을 구성하여 분류 및 조사하는 데 필요한 우선 순위가 낮은 알림을 줄입니다.

인시던트 대응 간소화

관련 이해관계자, 타사 서비스 및 도구를 사용하여 몇 분 안에 인시던트 대응을 확장하고 실행합니다.

셀프 서비스 보안 솔루션

AWS 보안 인시던트 대응은 APIs를 통합하여 자체 사용자 지정 보안 솔루션을 구축할 수 있도록 합니다.

가시성을 위한 대시보드

인시던트 대응 준비 상태를 모니터링하고 측정합니다.

보안 태세

보안 평가 및 신속한 인시던트 대응 조사를 위한 AWS 모범 사례 및 검증된 도구에 액세스합니다.

신속 지원

AWS의 고객 인시던트 대응 팀(CIRT)과 연결하여 보안 이벤트에서 복구하는 방법을 조사, 억제 및 지침을 받습니다.

준비 및 준비

미리 정의된 권한 정책을 사용하여 지정된 개인 또는 그룹에 알림을 트리거하는 Incident Response 팀을 설정하여 간소화된 알림을 구현합니다.

개념 및 용어

다음 용어 및 개념은 AWS 보안 인시던트 대응 서비스와 작동 방식을 이해하는 데 중요합니다.

범위: AWS 보안 인시던트 대응은 미국 국립표준기술연구소(NIST) 800-61 컴퓨터 보안 인시던트 처리 가이드에 따라 업계 모범 사례와 관련된 보안 이벤트 관리에 대한 일관된 접근 방식을 제공합니다.

분석: 보안 이벤트의 범위, 영향 및 근본 원인을 이해하기 위한 보안 이벤트의 세부 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 커뮤니케이션 및 보고가 용이해집니다.

커뮤니케이션: 인시던트 대응 프로세스 중에 AWS 보안 인시던트 대응 팀과 고객 간의 지속적인 대화 및 정보 공유입니다.

봉쇄, 근절 및 복구: 승인되지 않은 리소스 제거 및 원래 취약성(근절)과 함께 추가 승인되지 않은 활동(봉쇄)을 방지하고 리소스를 복구하여 정상적으로 다시 비즈니스에 복귀합니다.

지속적 개선: AWS 보안 인시던트 대응은 이전 계약에서 얻은 피드백과 교훈을 통합하여 탐지 기능, 조사 프로세스 및 문제 해결 조치를 개선합니다. AWS 또한 보안 인시던트 대응은 up-to-date 진화하는 보안 문제를 해결하기 위한 최신 보안 위협 및 모범 사례를 따릅니다.

사이버 보안 이벤트: 시스템 또는 네트워크에서 보안 정책, 허용되는 사용 정책 또는 표준 보안 관행을 위반하거나 위반할 위협이 되는 관찰 가능한 모든 발생.

인시던트 대응 팀: 활성 보안 이벤트 중에 지원을 제공하는 개인 그룹입니다. AWS 지원되는 사례의 경우 AWS 고객 인시던트 대응 팀(CIRT)입니다.

인시던트 대응 워크플로: NIST800-61 표준에 따라 보안 이벤트 관리에 관련된 end-to-end 정의된 단계 및 활동 시퀀스입니다.

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

학습한 교훈: 보안 이벤트 대응의 검토 및 문서화를 통해 개선이 필요한 영역을 식별하고 향후 인시던트 대응 계획을 알립니다.

모니터링 및 조사: AWS 보안 인시던트 대응은 Amazon의 보안 알림을 빠르게 검토하여 팀이 분석해야 하는 가장 중요한 알림을 GuardDuty제공합니다. 불필요한 알림을 방지하기 위해 환경의 세부 정보를 기반으로 억제 규칙을 구성합니다.

준비: 인시던트 대응 계획 및 테스트 절차 개발과 같이 조직이 보안 이벤트에 효과적으로 대응하고 관리할 수 있도록 준비하기 위해 수행되는 활동입니다.

보고 및 커뮤니케이션: 자동 알림, 통화 브리지, 조사 아티팩트 전달을 포함하여 인시던트 대응 프로세스 전반에 걸쳐 정보를 제공하는 데 사용되는 프로세스입니다. AWS 보안 인시던트 대응은에서 중앙 집중식 단일 대시보드 AWS Management Console 를 제공하여 모든 AWS 보안 인시던트 대응 작업을 관리합니다.

응답자 생성 인텔리전스: 침해 지표, 전술, 기법 및 절차, 조사에서 AWS CIRT 관찰된 관련 패턴.

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

공동 책임 모델: AWS 와 고객 간의 보안 책임 부서로, 여기서 AWS 는 클라우드의 보안을 담당하고 고객은 클라우드의 보안을 담당합니다.

위협 인텔리전스: 진화하는 보안 위협을 식별하고 대응하는 데 도움이 되는 무단 활동에 대한 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 대응 및 다음 단계를 결정하기 위한 보안 이벤트의 초기 평가 및 우선 순위 지정입니다.

워크플로: 보안 이벤트 관리에 관련된 end-to-end 정의된 단계 및 활동 시퀀스입니다.

시작하기

내용

- 멤버십 계정 선택
- 멤버십 세부 정보 설정
- 계정과 연결 AWS Organizations
- 사전 대응 및 알림 분류 워크플로 설정

멤버십 계정 선택

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

를 사용하여 AWS 보안 인시던트 대응 멤버십 계정을 선택하는 방법에는 두 가지가 있습니다 AWS Organizations. Organizations 관리 계정 또는 Organizations 위임 관리자 계정에서 멤버십을 생성할 수 있습니다.

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

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

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

권한을 추가하는 특정 단계는 IAM 자격 증명 권한 추가 및 제거를 참조하세요.

AWS 보안 인시던트 대응 관리형 정책을 참조하세요.

IAM 권한을 확인하려면 다음 단계를 수행합니다.

- IAM 정책 확인: 사용자, 그룹 또는 역할에 연결된 IAM 정책을 검토하여 필요한 권한을 부여했는지 확인합니다. 로 이동하여 `Users` 옵션을 https://console.aws.amazon.com/iam/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 경우를 시도합니다`ListCases`. 필요한 권한이 없는 경우 오류 메시지가 표시됩니다.
- AWS CLI 또는 사용SDK: AWS Command Line Interface 명령줄 인터페이스(CLI) 또는 원하는 프로그래밍 언어로 AWS SDK를 사용하여 권한을 테스트할 수 있습니다. 예를 들어를 사용하여 `aws sts get-caller-identity` 명령을 실행하여 현재 사용자 권한을 확인할 AWS Command Line Interface수 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 정책이 권한에 미치는 영향을 확인할 수 있는 도구입니다.

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

멤버십 세부 정보 설정

- 멤버십 및 사례가 저장될 AWS 리전 를 선택합니다.

> **Warning**
>
> 초기 멤버십 등록 AWS 리전 후에는 기본값을 변경할 수 없습니다.

- 선택적으로이 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.

계정과 연결 AWS Organizations

멤버십은 연결된 모든에 대한 적용 범위를 부여합니다 AWS 계정 AWS Organizations. 연결된 계정은 조직에서 계정이 추가되거나 제거될 때 자동으로 업데이트됩니다.

사전 대응 및 알림 분류 워크플로 설정

사전 대응 및 알림 분류 워크플로는 활성화된 보안 서비스를 모니터링하기 위해 조직 내에서 활성화하는 선택적 기능입니다. 활성화할 기능 옆의 토글을 선택합니다.

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

사전 대응 및 알림 분류: AWS 보안 인시던트 대응은 Amazon 및 GuardDuty Security Hub 통합에서 생성된 알림을 모니터링하고 조사합니다. 이 기능을 사용하려면 Amazon이 활성화되어 있어야 GuardDuty 합니다. AWS 보안 인시던트 대응은 서비스 자동화를 통해 우선순위가 낮은 알림을 분류하므로 팀이 가장 중요한 문제에 집중할 수 있습니다. AWS 보안 인시던트 대응이 Amazon에서 작동하는 방식에 대한 자세한 내용은 사용 설명서의 탐지 및 분석 섹션을 참조 GuardDuty AWS Security Hub하세요.

이 기능을 사용하면 AWS Security Incident Response가 조직에서 지원되는 모든 계정 및 활성 AWS 리전 계정의 조사 결과를 모니터링하고 조사할 수 있습니다. 이 기능을 용이하게 하기 위해 AWS 보안 인시던트 대응은 내 모든 멤버 계정에 서비스 연결 역할을 자동으로 생성합니다 AWS Organizations. 그러나 관리 계정의 경우 모니터링을 활성화하려면 서비스 연결 역할을 수동으로 생성해야 합니다.

서비스는 관리 계정에서 서비스 연결 역할을 생성할 수 없습니다. AWS CloudFormation 스택 세트를 사용하여 관리 계정에서이 역할을 수동으로 생성해야 합니다.

방지: 보안 인시던트가 발생하는 경우 AWS 보안 인시던트 대응은 억제 작업을 실행하여 손상된 호스트 격리 또는 보안 인증 정보 교체와 같은 영향을 신속하게 완화할 수 있습니다. 보안 인시던트 대응은 기본적으로 억제 기능을 활성화하지 않습니다. 이러한 격리 작업을 실행하려면 먼저 서비스에 필요한 권한을 부여해야 합니다. 이는 필요한 역할을 생성하는 AWS CloudFormation StackSet를 배포하여 수행할 수 있습니다.

사용자 작업

내용

- 대시보드
- 인시던트 대응 팀 관리
- 에 대한 계정 연결 AWS Organizations
- 모니터링 및 조사
- Cases
- 사례 관리
- AWS CloudFormation 스택 세트 작업
- 멤버십 취소

대시보드

AWS 보안 인시던트 대응 콘솔에서 대시보드는 인시던트 대응 팀, 사전 대응 상태 및 4주 롤링 사례 수에 대한 개요를 제공합니다.

인시던트 대응 팀원의 세부 정보에 `View incident response team` 액세스하려면 선택합니다.

경고 분류가 활성화되어 있는지 `proactive response` 확인하려면 선택합니다. `alert triaging` 워크플로를 활성화하지 않은 경우 상태를 모니터링하고 활성화`Proactive Response`하도록 선택할 수 있습니다.

대시보드의 내 사례 섹션에는 지정된 기간 내에 할당된 자체 관리형 사례와 함께 열린 사례와 닫힌 AWS 지원 사례 수가 표시됩니다. 또한 종료된 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 팀원, 보안 분석가, 애플리케이션 소유자 및 보안 리더십 팀이 있습니다.

외부 이해관계자의 예로는 인시던트 대응 프로세스에 포함하려는 독립 소프트웨어 공급업체(ISV) 및 관리형 서비스 공급자(MSP)의 개인이 있습니다.

> **Note**
>
> 인시던트 대응 팀을 설정해도 팀원에게 멤버십 및 사례와 같은 서비스 리소스에 대한 액세스 권한이 자동으로 부여되지는 않습니다. AWS 보안 인시던트 대응에 관리 AWS 형 정책을 사용하여 리소스에 대한 읽기 및 쓰기 액세스 권한을 부여할 수 있습니다. 자세한 내용을 알아보려면 여기를 클릭하십시오.

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

인시던트 대응 팀은 다음 이벤트에 대한 이메일 알림을 받게 됩니다.

- 사례(생성, 삭제, 업데이트)
- 주석(생성, 삭제, 업데이트)
- 첨부 파일(생성, 삭제, 업데이트)
- 멤버십(생성, 업데이트, 취소, 재개)

에 대한 계정 연결 AWS Organizations

AWS 보안 인시던트 대응을 활성화하면 멤버십이 생성되어에 맞춰집니다 AWS Organizations. 조직 내 모든 계정은 AWS 보안 인시던트 대응 멤버십에 맞게 조정됩니다.

자세한 내용은 를 사용하여 AWS 보안 인시던트 대응 계정 관리를 AWS Organizations 참조하세요.

모니터링 및 조사

AWS Security Incident Response는 Amazon의 보안 알림을 검토하고 분류한 GuardDuty AWS Security Hub다음 불필요한 알림을 방지하기 위해 환경을 기반으로 억제 규칙을 구성합니다. 팀은 AWS CIRT 분류되지 않은 조사 결과를 조사하고 잠재적 문제를 신속하게 억제하도록 팀을 신속하게 에스컬레이션하고 안내합니다. 원하는 경우 AWS 보안 인시던트 대응에 사용자를 대신하여 억제 작업을 구현할 수 있는 권한을 부여할 수 있습니다.

AWS 보안 인시던트 대응은 보안 이벤트 대응을 위한 NIST 800-61r2 컴퓨터 보안 이벤트 처리 안내서에 부합합니다. AWS 보안 인시던트 대응은이 업계 표준에 따라 보안 이벤트 관리에 대한 일관된 접근 방식을 제공하고 AWS 환경의 보안 이벤트를 보호하고 대응하는 모범 사례를 준수합니다.

AWS 보안 인시던트 대응 서비스에서 보안 알림을 식별하거나 보안 지원을 요청하면가 AWS CIRT 조사합니다. 팀은 GuardDuty 알림과 같은 로그 이벤트 및 서비스 데이터를 수집하고, 해당 데이터를 분류 및 분석하며, 문제 해결 및 억제 활동을 수행하고, 인시던트 후 보고를 제공합니다.

내용

- 준비
- 탐지 및 분석
- 포함
- 제거
- 복구
- 인시던트 후 보고서

준비

AWS 보안 인시던트 대응 팀은 보안 이벤트 대응 수명 주기 전반에 걸쳐 조사하고 협력합니다. 보안 이벤트가 발생하기 전에이 팀을 설정하고 필요한 권한을 할당하는 것이 좋습니다.

탐지 및 분석

AWS 보안 인시던트 대응은 Amazon 및를 통한 통합의 보안 결과를 모니터링, 분류 GuardDuty 및 조사합니다 AWS Security Hub. AWS Security Incident Response의 모니터링 및 조사 기능의 범위와 효과를 크게 향상시킬 수 있는 추가 작업은 다음과 같습니다.

지원되는 탐지 소스 활성화

> **Note**
>
> AWS Security Incident Response 서비스 비용에는 지원되는 다른 AWS 서비스 탐지 또는 사용 소스와 관련된 사용량 및 기타 비용 및 요금이 포함되지 않습니다. 비용 세부 정보는 개별 기능 또는 서비스 페이지를 참조하세요.

Amazon GuardDuty

GuardDuty 는 AWS 환경의 데이터 소스 및 로그를 지속적으로 모니터링, 분석 및 처리하는 위협 탐지 서비스입니다. AWS 보안 인시던트 대응을 사용하려면 활성화 GuardDuty 할 필요가 없지만 사전 대응 및 알림 분류 기능을 사용하려면 Amazon을 활성화해야 GuardDuty 합니다.

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

지원되는 모든 GuardDuty 에서를 활성화하는 것이 좋습니다 AWS 리전. 이렇게 하면 GuardDuty 가 적극적으로 사용하지 않는 리전에서도 승인되지 않았거나 비정상적인 활동에 대한 결과를 생성할 수 있습니다. 자세한 내용은 Amazon GuardDuty 리전 및 엔드포인트를 참조하세요.

활성화를 사용하면 중요한 위협 탐지 데이터에 대한 AWS 보안 인시던트 대응 액세스 권한을 GuardDuty 제공하여 AWS 환경의 잠재적 보안 문제를 식별하고 대응하는 기능을 강화할 수 있습니다.

AWS Security Hub

Security Hub는 여러 AWS 서비스 및 지원되는 타사 보안 솔루션에서 보안 결과를 수집할 수 있습니다. 이러한 통합은 AWS 보안 인시던트 대응이 다른 탐지 도구에서 얻은 결과를 모니터링하고 조사하는 데 도움이 될 수 있습니다.

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

Security Hub에서 통합을 활성화하는 방법에는 여러 가지가 있습니다. 타사 제품 통합의 경우에서 통합을 구매한 AWS Marketplace다음 통합을 구성해야 할 수 있습니다. 통합 정보는 이러한 작업을 수행할 수 있는 링크를 제공합니다. AWS Security Hub 통합을 활성화하는 방법에 대해 자세히 알아봅니다.

AWS 보안 인시던트 대응은 다음 도구와 통합될 때 다음 도구의 결과를 모니터링하고 조사할 수 있습니다 AWS Security Hub.

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

이러한 통합을 활성화하면 AWS Security Incident Response의 모니터링 및 조사 기능의 범위와 효율성을 크게 개선할 수 있습니다.

조사 결과 분석.

AWS 보안 인시던트 대응 자동화 및 AWS CIRT 서비스 팀은 지원되는 도구의 모든 결과를 분석합니다. AWS Support Cases를 사용하여 사용자와 통신하여 사용자 환경에 대해 알아봅니다. 예를 들어 조사 결과가 예상되는 행동인지 아니면 인시던트로 에스컬레이션되어야 하는지를 이해해야 하는 경우입니다. 사용자 환경에서 더 많은 것을 배우면 통신 수를 줄이기 위해 서비스를 사용자 지정하고를 줄일 것입니다.

이벤트를 보고합니다.

보안 인시던트 대응 서비스 포털을 통해 AWS 보안 이벤트를 생성할 수 있습니다. 보안 이벤트 중에 기다리지 않는 것이 중요합니다. AWS Security Incident Response는 자동 및 수동 기술을 사용하여 보안 이벤트를 조사하고, 로그를 분석하고, 변칙적인 패턴을 찾습니다. 파트너십과 환경에 대한 이해는이 분석을 가속화합니다.

커뮤니케이션.

AWS 보안 인시던트 대응은 이벤트 티켓을 통해 보안 담당자를 참여시켜 조사 중에 정보를 제공합니다. 여러 팀원이 이벤트를 지원할 수 있으며, 모두 고객 제공 콘텐츠 및 AWS 업데이트에 이벤트 티켓을 사용합니다.

통신에는 보안 알림이 생성될 때 자동 알림, 이벤트 분석 중 통신, 호출 브리지 설정, 로그 파일과 같은 아티팩트의 지속적 분석, 보안 이벤트 중 조사 결과 가져오기가 포함될 수 있습니다.

AWS 보안 인시던트 대응은 두 가지 사례 유형을 사용하여 사용자와 통신합니다. 아웃바운드 통신의 Support 경우 이벤트를 사용자에게 알리고, AWS 보안 인시던트 대응 사례는 사용자가 열어본 사례에 대해 통신합니다.

AWS 지원 사례: 서비스는 AWS 지원 사례를 사용하여 팀과 통신합니다. 조사 결과가 생성된 각 AWS 계정 에 대한 지원 사례를 생성합니다. 이 접근 방식은 특정 워크로드를 소유한 여러 팀과의 통신을 용이하게 합니다. 책임 영역에서 발생하는 이벤트에 대해 더 많은 지식을 갖기 때문입니다.

AWS 보안 인시던트 대응 사례: 조사 결과를 보안 인시던트로 에스컬레이션해야 한다고 판단되면 AWS 보안 인시던트 대응 사례를 생성합니다. 이렇게 하면 중요한 보안 문제가 적절한 수준의 관심과 응답을 받을 수 있습니다.

이러한 커뮤니케이션에 적극적으로 참여하고 적시에 대응하면 AWS 보안 인시던트 대응 서비스가 다음을 수행할 수 있습니다.

- 환경과 예상되는 행동을 더 잘 이해합니다.
- 시간 경과에 따라 오탐을 줄입니다.
- 알림의 정확성과 관련성을 개선합니다.
- 실제 보안 인시던트에 신속하게 대응합니다.
- AWS 보안 인시던트 대응 서비스의 효율성은 협업을 통해 개선되므로 보다 안전하고 효율적으로 모니터링되는 AWS 환경이 됩니다.

포함

AWS 보안 인시던트 대응은 이벤트를 포함하기 위해 사용자와 협력합니다. AWS 보안 인시던트 대응에 대한 서비스 역할을 구성하여 알림에 대한 응답으로 계정에서 자동 및 수동 작업을 수행할 수 있습니다. SSM 문서를 사용하여 직접 또는 타사 관계와 협력하여 격리를 수행할 수도 있습니다.

봉쇄의 필수 부분은 시스템 종료, 네트워크에서 리소스 격리, 액세스 끄기 또는 세션 종료와 같은 의사 결정입니다. 이러한 결정은 이벤트를 포함할 미리 결정된 전략과 절차가 있는 경우에 더 쉽게 이루어집니다. AWS 보안 인시던트 대응은 억제 전략을 제공하고, 잠재적 영향을 알리고, 관련된 위험을 고려하고 동의한 후에만 솔루션을 구현하도록 안내합니다.

AWS Security Incident Response는 사용자를 대신하여 지원되는 억제 작업을 실행하여 대응을 가속화하고 위협 행위자가 환경에 손상을 입힐 수 있는 시간을 줄입니다. 이 기능을 사용하면 식별된 위협을 더 빠르게 완화하여 잠재적 영향을 최소화하고 전반적인 보안 태세를 강화할 수 있습니다. 분석 중인 리소스에 따라 다양한 억제 옵션이 있습니다. 지원되는 억제 작업은 다음과 같습니다.

- EC2 방지: `AWSSupport-ContainEC2Instance` 격리 자동화는 EC2 인스턴스의 되돌릴 수 있는 네트워크 격리를 수행하여 인스턴스를 그대로 두고 실행하지만 새 네트워크 활동에서 격리하고 내부 및 외부의 리소스와 통신하지 못하도록 합니다VPC.

  > **Important**
  >
  > 보안 그룹 변경으로 인해 추적된 기존 연결이 종료되지는 않으며, 향후 트래픽만 새 보안 그룹과이 SSM 문서에 의해 효과적으로 차단된다는 점에 유의해야 합니다. 자세한 내용은 서비스 기술 안내서의 소스 격리 섹션에서 확인할 수 있습니다.

- IAM 억제: `AWSSupport-ContainIAMPrincipal` 억제 자동화는 IAM 사용자 또는 역할에 대한 되돌릴 수 있는 네트워크 억제를 수행하여 사용자 또는 역할을에 그대로 두IAM지만 계정 내의 리소스와 통신하지 못하도록 합니다.
- S3 격납: `AWSSupport-ContainS3Resource` 격납 자동화는 S3 버킷의 가역 격납을 수행하여 버킷에 객체를 두고 액세스 정책을 수정하여 Amazon S3 버킷 또는 객체를 격리합니다.

> **Important**
>
> AWS 보안 인시던트 대응은 기본적으로 억제 기능을 활성화하지 않습니다. 이러한 억제 작업을 실행하려면 먼저 역할을 사용하여 서비스에 필요한 권한을 부여해야 합니다. 필요한 역할을 생성하는 AWS CloudFormation 스택 세트 작업을 통해 계정별로 또는 조직 전체에서 이러한 역할을 개별적으로 생성할 수 있습니다.

AWS 보안 인시던트 대응은 위험 선호도에 맞는 각 주요 이벤트 유형에 대한 억제 전략을 고려하는 것이 좋습니다. 이벤트 중 의사 결정에 도움이 되는 명확한 기준을 문서화합니다. 고려할 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 효과(예: 부분적 봉쇄와 전체 봉쇄)
- 솔루션의 영구성(예: 되돌릴 수 있는 솔루션과 되돌릴 수 없는 솔루션)
- 솔루션 기간(예: 긴급 해결 방법, 임시 해결 방법, 영구 솔루션) 위험을 낮추고 더 효과적인 억제 전략을 정의하고 구현할 시간을 허용할 수 있는 보안 제어를 적용합니다.

AWS 보안 인시던트 대응은 리소스 유형에 따른 단기 및 장기 전략을 포함하여 효율적이고 효과적인 억제를 달성하기 위한 단계적 접근 방식을 권장합니다.

- 억제 전략
  - AWS 보안 인시던트 대응이 보안 이벤트의 범위를 식별할 수 있습니까?
    - 그렇다면 모든 리소스(사용자, 시스템, 리소스)를 식별합니다.
    - 아니요인 경우 식별된 리소스에서 다음 단계를 실행하는 것과 함께 조사합니다.
  - 리소스를 격리할 수 있습니까?
    - 그렇다면 영향을 받는 리소스를 격리합니다.
    - 그렇지 않은 경우 시스템 소유자 및 관리자와 협력하여 문제를 억제하는 데 필요한 추가 작업을 결정합니다.
  - 영향을 받는 모든 리소스가 영향을 받지 않는 리소스와 격리되어 있습니까?
    - 그렇다면 다음 단계로 계속 진행합니다.
    - 그렇지 않은 경우 영향을 받는 리소스를 계속 격리하여 단기 격리를 완료하고 이벤트가 더 이상 확대되지 않도록 합니다.
- 시스템 백업
  - 추가 분석을 위해 영향을 받는 시스템의 백업 복사본이 생성되었습니까?
  - 포렌식 복사본이 암호화되어 안전한 위치에 저장됩니까?
    - 그렇다면 다음 단계로 계속 진행합니다.

- 그렇지 않은 경우 포렌식 이미지를 암호화한 다음, 실수로 사용, 손상 및 변조되지 않도록 안전한 위치에 저장합니다.

제거

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

단계적 접근 방식을 사용하여 근절 및 복구를 수행하고 문제 해결 단계의 우선순위를 지정하는 것이 모범 사례입니다. 초기 단계의 목적은 향후 이벤트를 방지하기 위해 고부가가치 변경으로 전체 보안을 빠르게(일에서 몇 주) 높이는 것입니다. 이후 단계에서는 장기 변경(예: 인프라 변경)과 엔터프라이즈를 최대한 안전하게 유지하기 위한 지속적인 작업에 집중할 수 있습니다. 각 사례는 고유하며 필요한 작업을 평가하기 위해 사용자와 협력 AWS CIRT합니다.

다음을 고려하세요.

- 시스템을 다시 이미지화하고 패치 또는 기타 대책을 사용하여 시스템을 강화하여 공격 위험을 방지하거나 줄일 수 있습니까?
- 감염된 시스템을 새 인스턴스 또는 리소스로 교체하여 감염된 항목을 종료하는 동안 깨끗한 기준을 활성화할 수 있습니까?
- 무단 사용으로 인해 남아 있는 모든 맬웨어 및 기타 아티팩트를 제거하고 영향을 받는 시스템을 추가 공격으로부터 강화했습니까?
- 영향을 받는 리소스에 대한 포렌식 요구 사항이 있나요?

복구

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

- 영향을 받는 시스템이 최근 공격에 대해 패치되고 강화됩니까?
- 시스템을 프로덕션으로 복원하기 위한 실행 가능한 타임라인은 무엇입니까?
- 복원된 시스템을 테스트, 모니터링 및 확인하는 데 사용할 도구는 무엇입니까?

인시던트 후 보고서

AWS 보안 인시던트 대응은 팀과 당사 간의 보안 활동이 종료된 후 이벤트에 대한 요약을 제공합니다.

매월 말에 AWS 보안 인시던트 대응 서비스는 이메일을 통해 각 고객의 기본 연락처로 월별 보고서를 전송합니다. 보고서는 아래에 설명된 지표를 사용하여 PDF 형식으로 전달됩니다. 고객은 1개당 하나의 보고서를 받게 됩니다 AWS Organizations.

사례 지표

- 생성된 사례
  - 차원 이름: 유형
  - 차원 값: AWS 지원됨, 자체 지원됨
  - 단위: 수
  - 설명: 생성된 사례 수입니다.
- 사례 종료됨
  - 차원 이름: 유형
  - 차원 값: AWS 지원, 자체 관리형
  - 단위: 수
  - 설명: 종료된 총 사례 수의 측정치입니다.
- 열린 사례
  - 차원 이름: 유형
  - 차원 값: AWS 지원됨, 자체 지원됨
  - 단위: 수
  - 설명: 미해결 사례 수입니다.

지표 분류

- 조사 결과 수신됨
  - 단위: 수
  - 설명: 분류로 전송된 조사 결과 수입니다.
- 보관된 결과
  - 단위: 수
  - 설명: 수동 조사 없이 처리된 후 보관된 조사 결과 수입니다.

- 조사 결과 수동으로 조사됨
  - 단위: 수
  - 설명: 수동 조사가 수행된 결과 수입니다.
- 보관된 조사
  - 단위: 수
  - 설명: 수동 조사의 결과로 오탐이 발생하고 아카이브를 위해 전송된 수
- 에스컬레이션된 조사
  - 단위: 수
  - 설명: 보안 인시던트를 초래하는 수동 조사 수

Cases

AWS 보안 인시던트 대응을 사용하면 AWS 지원 또는 자체 관리형 사례의 두 가지 유형의 사례를 생성할 수 있습니다.

AWS 지원되는 사례 생성

AWS 보안 인시던트 대응, API또는에서 AWS 지원되는 사례를 생성할 수 있습니다 AWS Command Line Interface. AWS 지원되는 사례를 통해 AWS 고객 인시던트 대응 팀()의 지원을 받을 수 있습니다 CIRT.

> **Note**
>
> AWS CIRT는 15분 이내에 사례에 응답합니다. 응답 시간은의 첫 번째 응답에 대한 시간입니다 AWS CIRT. 이 기간 내에 초기 요청에 응답하기 위해 모든 합리적인 노력을 기울일 것입니다. 이 응답 시간은 후속 응답에는 적용되지 않습니다.

다음 예제에서는 콘솔 사용에 대해 설명합니다.

1. AWS Management Console에 로그인합니다. 에서 보안 인시던트 대응 콘솔을 엽니다 https://console.aws.amazon.com/security-ir/.
2. 사례 생성을 선택합니다.
3. 를 사용하여 사례 해결을 AWS선택합니다.
4. 요청 유형 선택

a. 활성 보안 인시던트:이 유형은 긴급 인시던트 대응 지원 및 서비스를 위한 것입니다.

b. 조사: 조사를 통해가 AWS CIRT 로그 분석 및 인시던트 대응 조사의 보조 확인을 지원할 수 있는 인지된 보안 인시던트에 대한 지원을 받을 수 있습니다.

5. 시작일 추정치를 인시던트의 가장 빠른 지표 날짜로 설정합니다. 예를 들어, 비정상적인 동작을 처음 경험했거나 첫 번째 관련 보안 경고를 받은 경우입니다.

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 보고했습니까?

c. 사례의 영향을 받는 사람은 누구입니까?

d. 알려진 영향은 무엇입니까?

e. 이 사례의 긴급성은 무엇입니까?

f. 사례 범위에 속하는 하나 이상의 AWS 계정 IDs를 추가합니다.

8. 선택적 사례 세부 정보 추가:

a. 드롭다운 목록에서 영향을 받는 기본 서비스를 선택합니다.

b. 드롭다운 목록에서 영향을 받는 기본 리전을 선택합니다.

c. 이 사례의 일부로 식별한 하나 이상의 위협 행위자 IP 주소를 추가합니다.

9. 알림을 수신할 사례에 선택적 추가 인시던트 대응 담당자를 추가합니다. 개인을 추가하려면 다음을 수행합니다.

a. 이메일 주소를 추가합니다.

b. 선택 사항인 이름과 성을 추가합니다.

c. 새로 추가를 선택하여 다른 개인을 추가합니다.

d. 개인을 제거하려면 개인에 대해 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 지원되는 사례가 생성 AWS CIRT되면 및 인시던트 대응 팀에 즉시 알립니다.

자체 관리형 사례 생성

AWS 보안 인시던트 대응, API또는에서 자체 관리형를 생성할 수 있습니다 AWS Command Line Interface. 이러한 유형의 사례는에 DOES NOT 관여합니다 AWS CIRT. 다음 예제에서는 콘솔 사용에 대해 설명합니다.

1. AWS Management Console에 로그인합니다. 에서 보안 인시던트 대응 콘솔을 엽니다 https://console.aws.amazon.com/security-ir/.
2. Create Case(사례 생성)을 선택합니다.
3. 자체 인시던트 대응 팀과 함께 사례 해결을 선택합니다.
4. 시작일 추정치를 인시던트의 가장 빠른 지표 날짜로 설정합니다. 예를 들어, 비정상적인 동작을 처음 경험했거나 첫 번째 관련 보안 경고를 받은 경우입니다.
5. 사례에 대한 제목을 정의합니다. 제목 생성 옵션을 선택할 때 제안된 대로 데이터를 사례 제목에 포함하는 것이 좋습니다.
6. 사례의 일부인를 입력합니다 AWS 계정 IDs. 계정 ID를 추가하려면 다음을 수행합니다.
   a. 12자리 계정 ID를 입력하고 계정 추가를 선택합니다.
   b. 계정을 제거하려면 사례에서 제거할 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 보고했습니까?
      iii. 사례의 영향을 받는 사람은 누구입니까?
      iv. 알려진 영향은 무엇입니까?
      v. 이 사례의 긴급성은 무엇입니까?
8. 선택적 사례 세부 정보 추가:
   a. 드롭다운 목록에서 영향을 받는 기본 서비스를 선택합니다.
   b. 드롭다운 목록에서 영향을 받는 기본 리전을 선택합니다.
   c. 이 사례의 일부로 식별한 하나 이상의 위협 행위자 IP 주소를 추가합니다.

9. 알림을 수신할 사례에 선택적 추가 인시던트 대응 담당자를 추가합니다. 개인을 추가하려면 다음을 수행합니다.
   a. 이메일 주소를 추가합니다.
   b. 선택 사항인 이름과 성을 추가합니다.
   c. 새로 추가를 선택하여 다른 개인을 추가합니다.
   d. 개인을 제거하려면 개인에 대해 제거 옵션을 선택합니다.
   e. 추가를 선택하여 나열된 모든 개인을 사례에 추가합니다. 여러 개인을 선택하고 제거를 선택하여 목록에서 삭제할 수 있습니다.
10사례에 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.

인시던트 대응 팀은 사례가 생성된 후 이메일로 알림을 받게 됩니다.

AWS 생성된 사례에 대한 응답

AWS 보안 인시던트 대응은 계정 또는 리소스에 영향을 미칠 수 있는 조치를 취하거나 이를 알아야 하는 아웃바운드 알림 또는 사례를 생성할 수 있습니다. 이는 구독의 일부로 활성화된 사전 대응 및 알림 분류 워크플로를 활성화한 경우에만 발생합니다.

이러한 알림은 Support 센터에 표시됩니다. Support 사용 설명서에는 이러한 사례를 업데이트, 해결 및 다시 열기 위한 정보와 세부 단계가 나와 있습니다.

사례 관리

내용

- 사례 상태 변경
- 해석기 변경
- 작업 항목
- 사례 편집
- 통신
- 권한

- 첨부
- Tags
- 사례 활동
- 사례 종료

사례 상태 변경

사례는 다음 상태 중 하나입니다.

- 제출됨: 사례의 초기 상태입니다. 이 상태의 사례는 요청된에서 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.
- 봉쇄, 제거 및 복구:이 상태에서 인시던트 대응 담당자가 제거하기 위해 추가 노력이 필요한 의심스러운 활동을 식별했습니다. 인시던트 대응 담당자가 비즈니스 위험 분석 및 추가 작업에 대한 권장 사항을 제공합니다. 서비스에 대한 옵트인 기능을 활성화한 경우 AWS 인시던트 대응 담당자가 영향을 받는 계정(들)의 SSM 문서로 억제 작업을 수행하는 데 대한 동의를 구합니다.
- 인시던트 후 활동:이 상태에서 기본 보안 이벤트가 포함되었습니다. 이제는 비즈니스 운영을 복구하고 정상으로 되돌리는 데 중점을 둡니다. 사례에 대한 해석기가 AWS지원되는 경우 요약 및 근본 원인 분석이 제공됩니다.
- 종료됨: 워크플로의 최종 상태입니다. 닫힌 상태의 사례는 작업이 완료되었음을 나타냅니다. 종료된 사례는 다시 열 수 없으므로이 상태로 전환하기 전에 모든 작업이 완료되었는지 확인하세요.

작업/상태 업데이트를 선택하여 자체 관리형 사례의 사례 상태를 변경합니다. AWS 지원되는 사례의 경우 상태는 응답기에 의해 AWS CIRT 설정됩니다.

해석기 변경

자체 관리형 사례의 경우 인시던트 대응 팀이 도움을 요청할 수 있습니다 AWS. 이 사례에 대한 해석기를 로 변경하려면 에서 도움말 가져오기 AWS를 선택합니다 AWS. 사례가 AWS 지원으로 업데이트되면 상태가 제출됨으로 변경됩니다. 기존 사례 기록을 사용할 수 있습니다 AWS CIRT. 에 도움을 요청 AWS 하면 다시 자체 관리형으로 변경할 수 없습니다.

작업 항목

사례를 처리하는 AWS CIRT 대응 담당자가 내부 팀에 작업을 요청할 수 있습니다.

사례가 생성된 후 나타나는 작업 항목은 다음과 같습니다.

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

고객 작업이 보류 중인 경우의 작업 항목:

- 사례를 진행하기 위해 새 의견에 대한 조치 요청

사례를 종료할 준비가 되면 작업 항목:

- 사례 보고서 검토 요청
- 사례 종료 요청

사례 편집

편집을 선택하여 사례의 세부 정보를 변경합니다.

AWS 지원되는 사례 및 자체 관리형 사례의 경우:

사례가 생성된 후 다음 사례 세부 정보를 변경할 수 있습니다.

- Title
- 설명

AWS 지원되는 사례만 해당:

추가 필드를 변경할 수 있습니다.

- 요청 유형:
  - 활성 보안 인시던트:이 유형은 긴급 인시던트 대응 지원 및 서비스를 위한 것입니다.
  - 조사: 조사를 통해가 로그 분석 및 인시던트 대응 조사의 보조 확인을 지원할 수 있는 AWS CIRT 인지된 보안 인시던트에 대한 지원을 받을 수 있습니다. 이벤트.
- 시작 날짜 추정:이 사례에 대해 처음 제공된 시작 날짜 이전의 지표를 받은 경우이 필드를 변경합니다. 설명 필드에 새로 감지된 지표와 관련된 추가 세부 정보를 제공하거나 통신 탭에 주석을 추가하는 것이 좋습니다.

통신

AWS CIRT는 사례에 대해 작업할 때 활동을 문서화하는 설명을 추가할 수 있습니다. 다른 AWS CIRT 대응 담당자가 동시에 사례에 대해 작업할 수 있습니다. 통신 로그 내에서 AWS 응답자로 표시됩니다.

권한

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

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

콘솔에서 사례에 대한 액세스 권한 제공

에서 사례에 대한 액세스를 제공하려면 IAM 권한 정책 템플릿을 복사하고이 권한을 사용자 또는 역할에 추가할 AWS Management Console수 있습니다.

사용자 또는 역할에 IAM 정책 추가:

1. IAM 권한 정책을 복사합니다.
2. 를 통해 IAM에서를 엽니다https://console.aws.amazon.com/iam/.
3. 탐색 창에서 사용자 또는 역할을 선택합니다.
4. 사용자 또는 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

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

> **Note**
>
> AWS 지원되는 사례를 선택하면 첨부 파일을 볼 AWS 수 없습니다. AWS 지원되는 사례에 대한 모든 세부 정보는 사례 설명을 통해 공유하거나 선호하는 통신 기술을 사용하여 화면 공유를 제공해야 합니다.

업로드를 선택하여 컴퓨터에서 사례에 추가할 파일을 선택합니다.

> **Note**
>
> 업로드된 모든 첨부 파일은 사례가 된 후 7일 후에 삭제됩니다`Closed`.

Tags

태그는 사례에 할당하여 해당 리소스에 대한 메타데이터를 보유할 수 있는 선택적 레이블입니다. 각 태그는 키와 값(선택 사항)으로 구성됩니다. 태그를 사용하여 리소스에 대한 권한을 검색, 비용 할당 및 인증할 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 세부 시간 기록을 제공합니다. 이벤트 후 활동에 중요한 정보를 제공하고 잠재적 개선 사항을 식별하는 데 도움이 됩니다. 사례 변경의 시간, 사용자, 작업 및 세부 정보는 사례 감사 추적에 기록됩니다.

사례 종료

AWS 지원되는 사례의 경우 사례 세부 정보 페이지에서 사례 닫기를 선택하여 모든 상태에서 사례를 영구적으로 닫습니다. 일반적으로 케이스는 영구적으로 닫히기 전에 닫을 준비가 됨 상태에 도달합니

다. 종료 준비 완료 이외의 다른 상태에서 사례를 조기에 종료하는 경우에 AWS 지원되는이 사례에 대한 작업이 중지되도록 AWS CIRT 요청하고 있습니다.

인시던트 대응 팀이 대응자인 경우 사례 세부 정보 페이지에서 작업/사례 종료를 선택합니다.

> **Note**
>
> '닫기 준비 완료' 상태는 사례가 영구적으로 닫힐 수 있고 사례에 대해 수행할 추가 작업이 없음을 나타냅니다.

사례가 영구적으로 닫힌 후에는 다시 열 수 없습니다. 모든 정보는 읽기 전용으로 제공됩니다. 실수로 종료되는 것을 방지하기 위해 사례를 종료할 것인지 확인하라는 메시지가 표시됩니다.

AWS CloudFormation 스택 세트 작업

> **Important**
>
> AWS 보안 인시던트 대응은 기본적으로 억제 기능을 활성화하지 않습니다. 이러한 억제 작업을 실행하려면 먼저 역할을 사용하여 서비스에 필요한 권한을 부여해야 합니다. 필요한 역할을 생성하는를 배포하여 계정별로 또는 조직 전체에 걸쳐 이러한 역할을 AWS CloudFormation StackSets개별적으로 생성할 수 있습니다.

서비스 관리형 권한으로 스택 세트를 생성하는 방법에 대한 구체적인 지침을 찾을 수 있습니다.

다음은 AWSSecurityIncidentResponseContainment 및 AWSSecurityIncidentResponseContainmentExecution 역할을 생성하기 위한 템플릿 스택 세트입니다.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS Security Incident Response containment roles'

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

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

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

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

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

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

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

멤버십 취소

AWS 보안 인시던트 대응 CancelMembership 권한이 있는 역할은 콘솔, API또는에서 멤버십을 취소할 수 있습니다 AWS Command Line Interface.

> **Important**
>
> 멤버십이 취소되면 과거 사례 데이터를 볼 수 없습니다. 취소는 결제 주기가 끝날 때 발생합니다. 월중에 취소하면 월말까지 멤버십을 사용할 수 있습니다. 결제 주기 종료 시 최종 멤버십 취소 시 종료되거나 종료`ready to close`될 리소스 `Active` 또는 조사.

> **Important**
>
> 서비스를 다시 구독하면 새 멤버십이 생성되고 취소 전에 다운로드한 경우에만 이전 멤버십에 속한 사례 리소스에 액세스할 수 있습니다.

멤버십이 취소되면 멤버십 인시던트 대응 팀의 모든 사람에게 이메일로 알립니다.

> **Important**
>
> 위임된 관리자 계정을 사용하여 멤버십을 생성하고 AWS Organizations API를 사용하여 계정에서 위임된 관리자 지정을 제거하면 멤버십이 즉시 종료됩니다.

AWS 보안 인시던트 대응 리소스에 태그 지정

태그는 사용자가 할당하거나 AWS 리소스에 AWS 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 구성합니다. 많은가 태그 지정을 AWS 서비스 지원하므로 서로 다른 서비스의 리소스에 동일한 태그를 할당하여 리소스가 관련이 있음을 나타낼 수 있습니다.
- AWS 비용을 추적합니다. 대시보드에서 AWS Billing 이러한 태그를 활성화합니다.는 태그를 AWS 사용하여 비용을 분류하고 월별 비용 할당 보고서를 제공합니다. 자세한 내용은 AWS 결제 사용 설명서의 비용 할당 태그 사용을 참조하세요.
- AWS 리소스에 대한 액세스를 제어합니다. 자세한 내용은 IAM 사용 설명서의 태그를 사용하여 액세스 제어를 참조하세요.

태그 지정은 AWS 보안 인시던트 대응 API 참조를 참조하세요.

AWS CloudShell 를 사용하여 AWS 보안 인시던트 대응 작업

AWS CloudShell 는 브라우저 기반 사전 인증된 셸로,에서 직접 시작할 수 있습니다 AWS Management Console. 원하는 쉘(배시 PowerShell 또는 Z 쉘)을 사용하여 AWS 서비스에 대한 AWS CLI 명령(AWS 보안 인시던트 대응 포함)을 실행할 수 있습니다. 또한 명령줄 도구를 다운로드하거나 설치할 필요 없이 이 작업을 수행할 수 있습니다.

AWS CloudShell 에서를 시작 AWS Management Console하면 콘솔에 로그인하는 데 사용한 AWS 자격 증명이 새 쉘 세션에서 자동으로 사용할 수 있습니다. 이 AWS CloudShell 사용자 사전 인증을 사용하면 AWS CLI 버전 2(셸의 컴퓨팅 환경에 사전 설치됨)를 사용하여 보안 인시던트 대응과 같은 AWS 서비스와 상호 작용할 때 자격 증명 구성을 건너뛸 수 있습니다.

내용

- 에 대한 IAM 권한 획득 AWS CloudShell
- 를 사용하여 보안 인시던트 대응과 상호 작용 AWS CloudShell

에 대한 IAM 권한 획득 AWS CloudShell

AWS Identity and Access Management관리자는에서 제공하는 액세스 관리 리소스를 사용하여 IAM 사용자에게 환경의 기능에 액세스 AWS CloudShell 하고 사용할 수 있는 권한을 부여할 수 있습니다.

관리자가 사용자에게 액세스 권한을 부여하는 가장 빠른 방법은 AWS 관리형 정책을 통하는 것입니다. AWS 관리형 정책은 AWS에서 생성 및 관리하는 독립 실행형 정책입니다. 에 대한 다음 AWS 관리형 정책을 IAM 자격 증명에 연결할 CloudShell 수 있습니다.

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

IAM 사용자가 수행할 수 있는 작업 범위를 제한하려면 `AWSCloudShellFullAccess` 관리형 정책을 템플릿으로 사용하는 사용자 지정 정책을 생성할 AWS CloudShell수 있습니다. 에서 사용자가 사용할 수 있는 작업을 제한하는 방법에 대한 자세한 내용은 AWS CloudShell 사용 설명서의 IAM 정책을 사용하여 AWS CloudShell 액세스 및 사용량 관리를 CloudShell참조하세요.

> **Note**
>
> 또한 자격 IAM 증명에는 보안 인시던트 대응을 호출할 수 있는 권한을 부여하는 정책이 필요합니다.

를 사용하여 보안 인시던트 대응과 상호 작용 AWS CloudShell

AWS CloudShell 에서를 시작한 후 명령줄 인터페이스를 사용하여 보안 인시던트 대응과 즉시 상호 작용할 AWS Management Console수 있습니다.

> **Note**
>
> AWS CLI 에서를 사용하는 AWS CloudShell경우 추가 리소스를 다운로드하거나 설치할 필요가 없습니다. 또한 셸 내에서 이미 인증되었기 때문에 직접 호출을 하기 전에 보안 인증을 구성하지 않아도 됩니다.

AWS CloudShell 및 보안 인시던트 대응 작업

- 에서 탐색 모음에서 사용할 AWS Management Console수 있는 다음 옵션을 CloudShell 선택하여를 시작할 수 있습니다.
  - CloudShell 아이콘을 선택합니다.
  - 검색 상자에 “cloudshell”을 입력한 다음 옵션을 CloudShell 선택합니다.

를 사용하여 AWS 보안 인시던트 응답 API 호출 로깅 AWS CloudTrail

AWS 보안 인시던트 대응은 보안 인시던트 대응에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다.는 보안 인시던트 대응에 대한 모든 API 호출을 이벤트로 CloudTrail 캡처합니다. 캡처된 호출에는 보안 인시던트 대응 콘솔의 호출과 보안 인시던트 대응 API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하는 경우 보안 인시던트 대응 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. 에서 수집한 정보를 사용하여 보안 인시던트 대응에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 CloudTrail수 있습니다.

자세한 내용은 AWS CloudTrail 사용 설명서를 CloudTrail참조하세요.

의 보안 인시던트 대응 정보 CloudTrail

CloudTrail 는 계정을 생성할 AWS 계정 때에서 활성화됩니다. 보안 인시던트 대응에서 활동이 발생하면 해당 활동은 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 이벤트 기록을 사용하여 CloudTrail 이벤트 보기를 참조하세요.

AWS 계정 지난 90일 동안의 이벤트를 지속적으로 기록하려면 추적 또는 CloudTrail Lake 이벤트 데이터 스토어를 생성합니다.

CloudTrail 추적

추적 CloudTrail 을 사용하면가 Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 를 사용하여 생성된 모든 추적 AWS Management Console 은 다중 리전입니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 추적을 생성할 수 있습니다. 계정 AWS 리전 의 모든에서 활동을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다. 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.

추적을 생성하여에서 진행 중인 관리 이벤트의 사본 하나를 Amazon S3 버킷 CloudTrail 에 무료로 전송할 수 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 SQL기반 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 AWS CloudTrail Lake 작업을 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.

모든 보안 인시던트 대응 작업은에서 로깅 CloudTrail 하며 AWS 보안 인시던트 대응 API 참조에 문서화됩니다. 예를 들어를 호출`CreateMembershipCreateCase`하고 `UpdateCase` 작업을 수행하면 CloudTrail 로그 파일에 항목이 생성됩니다.

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

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에 의해 이루어졌는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

보안 인시던트 대응 로그 파일 항목 이해

추적은 사용자가 지정한 Amazon S3 버킷으로 이벤트를 전송할 수 있도록 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함됩니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업의 날짜 및 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 정렬된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

다음 예제에서는 CreateCase 작업을 보여주는 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"
}
```

를 사용하여 AWS 보안 인시던트 대응 계정 관리 AWS Organizations

AWS 보안 인시던트 대응은와 통합됩니다 AWS Organizations. 조직의 AWS Organizations 관리 계정은 보안 AWS 인시던트 대응을 위한 위임된 관리자로 계정을 지정할 수 있습니다. 이 작업을 통해 AWS에서 보안 인시던트 대응을 신뢰할 수 있는 서비스로 사용할 수 있습니다 AWS Organizations. 이러한 권한이 부여되는 방법에 대한 자세한 내용은 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하세요.

다음 섹션에서는 위임된 보안 인시던트 대응 관리자 계정으로 수행할 수 있는 다양한 작업을 안내합니다.

내용

- 에서 AWS 보안 인시던트 대응을 사용하기 위한 고려 사항 및 권장 사항 AWS Organizations
- 에 대한 신뢰할 수 있는 액세스 활성화 AWS Account Management
- 위임된 보안 인시던트 대응 관리자 계정을 지정하는 데 필요한 권한
- AWS 보안 인시던트 대응을 위해 위임된 관리자 지정
- AWS 보안 인시던트 대응에 멤버 추가
- AWS 보안 인시던트 대응에서 멤버 제거

에서 AWS 보안 인시던트 대응을 사용하기 위한 고려 사항 및 권장 사항 AWS Organizations

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

위임된 보안 인시던트 대응 관리자 계정은 리전별입니다.

위임된 보안 인시던트 대응 관리자 계정과 멤버 계정은를 통해 추가해야 합니다 AWS Organizations.

AWS 보안 인시던트 대응을 위한 위임된 관리자 계정입니다.

멤버 계정 하나를 위임된 보안 인시던트 대응 관리자 계정으로 지정할 수 있습니다. 예를 들어 *111122223333*에서 멤버 계정을 지정하는 경우 *555555555555*에서 다른 멤버 계정을 지정할

*Europe (Ireland)*수 없습니다*Canada (Central)*. 다른 모든 리전에서는 위임된 보안 인시던트 대응 관리자 계정과 동일한 계정을 사용해야 합니다.

조직의 관리를 위임된 보안 인시던트 대응 관리자 계정으로 설정하는 것은 권장되지 않습니다.

조직의 관리는 위임된 보안 인시던트 대응 관리자 계정이 될 수 있습니다. 하지만 AWS 보안 모범 사례는 최소 권한 원칙을 따르므로 이 구성을 권장하지 않습니다.

실시간 구독에서 위임된 보안 인시던트 대응 관리자 계정을 제거하면 구독이 즉시 취소됩니다.

위임된 보안 인시던트 대응 관리자 계정을 제거하면 AWS 보안 인시던트 대응은이 위임된 보안 인시던트 대응 관리자 계정과 연결된 모든 멤버 계정을 제거합니다. AWS 이러한 모든 멤버 계정에 대해 보안 인시던트 대응이 더 이상 활성화되지 않습니다.

에 대한 신뢰할 수 있는 액세스 활성화 AWS Account Management

AWS 보안 인시던트 대응에 대한 신뢰할 수 있는 액세스를 활성화하면 관리 계정의 위임된 관리자가의 각 멤버 계정에 고유한 정보 및 메타데이터(예: 기본 또는 대체 연락처 세부 정보)를 수정할 수 있습니다 AWS Organizations.

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 대해 신뢰할 수 있는 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. IAM 사용자로 로그인하거나, IAM 역할을 맡거나, 조직의 관리 계정에서 루트 사용자(권장되지 않음)로 로그인해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS 보안 인시던트 응답을 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

에 대해 신뢰할 수 있는 액세스를 활성화하려면 AWS Account Management

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

- AWS CLI: enable-aws-service-access

  다음 예제에서는 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 보안 인시던트 대응 관리자 계정을 지정하는 데 필요한 권한

위임된 관리자를 사용하여 AWS 보안 인시던트 대응 멤버십을 설정하도록 선택할 수 있습니다 AWS Organizations. 이러한 권한이 부여되는 방법에 대한 자세한 내용은 다른 AWS 서비스와 함께 사용을 AWS Organizations참조하세요.

> **Note**
>
> AWS 보안 인시던트 대응은 설정 및 관리에 콘솔을 사용할 때 AWS Organizations 신뢰할 수 있는 관계를 자동으로 활성화합니다. CLI/SDK를 사용하는 경우 E nableAWSServiceAccess API to trust를 사용하여 수동으로 활성화해야 합니다`security-ir.amazonaws.com`.

AWS Organizations 관리자로서 조직의 위임된 보안 인시던트 대응 관리자 계정을 지정하기 전에 `sir:CreateMembership` 및 AWS 보안 인시던트 대응 작업을 수행할 수 있는지 확인합니다`sir:UpdateMembership`. 이러한 작업을 통해 보안 인시던트 대응을 사용하여 조직의 위임된 AWS 보안 인시던트 대응 관리자 계정을 지정할 수 있습니다. 또한 조직에 대한 정보를 검색하는 데 도움이 되는 AWS Organizations 작업을 수행할 수 있는지 확인해야 합니다.

이러한 권한을 부여하려면 계정의 AWS Identity and Access Management (IAM) 정책에 다음 문을 포함합니다.

```
{
    "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 관리를 위임된 보안 인시던트 대응 관리자 계정으로 지정하려면 계정에 라는 IAM 작업도 필요합니다`CreateServiceLinkedRole`. 이 작업을 사용하면 관리를 위해 AWS 보안 인시던트 응답을 초기화할 수 있습니다. 그러나 권한 추가를 진행하기 전에 에서 AWS 보안 인시던트 대응을 사용하기 위한 고려 사항 및 권장 사항 AWS Organizations를 검토합니다.

관리를 위임된 보안 인시던트 대응 관리자 계정으로 지정하려면 IAM 정책에 다음 문을 추가하고를 조직 관리의 AWS 계정 ID*111122223333*로 바꿉니다.

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

```
  }
 }
}
```

AWS 보안 인시던트 대응을 위해 위임된 관리자 지정

이 섹션에서는 AWS 보안 인시던트 대응 조직에서 위임된 관리자를 지정하는 단계를 제공합니다.

AWS 조직의 관리자로서 위임된 보안 인시던트 대응 관리자 계정의 작동 방식에 사용 고려 사항 및 권장 사항 대해를 읽어야 합니다. 계속하기 전에 위임된 보안 인시던트 대응 관리자 계정을 지정하는 데 필요한 권한가 있는지 확인하세요.

조직의 위임된 보안 인시던트 대응 관리자 계정을 지정하려면 선호하는 액세스 방법을 선택합니다. 관리진만이 단계를 수행할 수 있습니다.

Console

1. 에서 보안 인시던트 대응 콘솔을 엽니다. https://console.aws.amazon.com/security-ir/

   로그인하려면 AWS Organizations 조직의 관리 자격 증명을 사용합니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 조직의 위임된 보안 인시던트 대응 관리자 계정을 지정할 리전을 선택합니다.
3. 설정 마법사에 따라 위임된 관리자 계정을 포함하여 멤버십을 생성합니다.

API/CLI

- 조직 관리의 보안 인증 정보를 CreateMembership 사용하여 AWS 계정 를 실행합니다.
  - 또는 AWS Command Line Interface 를 사용하여이 작업을 수행할 수 있습니다. 다음 AWS CLI 명령은 위임된 보안 인시던트 대응 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 AWS 보안 인시던트 대응 관리자 계정에 대해 보안 인시던트 대응이 활성화되지 않은 경우 조치를 취할 수 없습니다. 아직 활성화하지 않은 경우 새로 지정된 위임된 AWS 보안 인시던트 대응 관리자 계정에 대해 보안 인시던트 대응을 활성화해야 합니다.

AWS 보안 인시던트 대응에 멤버 추가

AWS Organizations 및 AWS 보안 인시던트 대응 멤버십과 일대일 관계가 있습니다. Organizations에서 계정이 추가(또는 제거)되면 보안 AWS 인시던트 대응 멤버십의 적용 계정에 반영됩니다.

멤버십에 계정을 추가하려면를 사용하여 조직의 계정 관리를 AWS Organizations 위한 옵션 중 하나를 따릅니다.

AWS 보안 인시던트 대응에서 멤버 제거

멤버십에서 계정을 제거하려면 조직에서 멤버 계정을 제거하는 절차를 따릅니다.

문제 해결

AWS 보안 인시던트 대응과 관련된 작업 수행과 관련된 문제가 발생하면이 섹션의 주제를 참조하세요.

ERROR는 일부 또는 모든 작업의 오류를 나타내는 작업의 상태입니다. 또는 문제가 발생했지만 태스크가 여전히 완료되면 경고가 표시됩니다.

내용

- 문제
- 오류
- Support

문제

올바른 컨텍스트에서 요청을 전송하지 않습니다.

AWS 보안 인시던트 대응에 대한 모든 호출은 서비스 위임된 관리자 또는 멤버십 계정의 IAM 보안 주체로부터 시작APIs되어야 합니다. 조직의 AWS 보안 인시던트 대응 위임된 관리자 또는 멤버십 계정 AWS 계정 인의 올바른 IAM 보안 주체에서 운영 중인지 확인합니다.

오류

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

AWS 관리자와 협력하여 AWS Security Incident Response 위임 관리자 또는 멤버십 계정에서 IAM 역할을 수임할 수 있는 권한이 있는지 확인하세요. 또한 역할에 요청된 작업을 허용하는 IAM 정책이 있는지 확인합니다. 자세한 내용은 AWS 보안 인시던트 대응을 IAM참조하세요.

ConflictException

요청이 일관되지 않은 상태를 발생시킵니다.

지정한 모든 사례 첨부 파일 이름 또는 기본 응답 팀원이 고유한지 확인하세요. 또한AWS 보안 인시던트 대응 서비스 멤버십이 아직 구성되지 않았는지 확인합니다. 에서 https://console.aws.amazon.com/security-ir/ 보안 인시던트 대응 콘솔을 열고 로 이동합니다`Membership Details`.

InternalServerException

요청을 처리하는 동안 예기치 않은 오류가 발생했습니다. 몇 분 후에 다시 시도하세요. 문제가 지속되면 로 사례를 제기 Support합니다.

ResourceNotFoundException

요청은 존재하지 않는 리소스를 참조합니다.

요청에 지정된 하나 이상의 리소스가 존재하지 않습니다. 지정된 모든 리소스 ARNs 또는 IDs가 올바른지 확인하세요. 이는 계정 AWS Organizations IDs, IAM 역할IDs, 멤버십, 사례, 대응 팀원, 사례, 사례 대응 담당자, 사례 첨부 파일 및 사례 의견에 적용됩니다.

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

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

ValidationException

입력이에서 지정한 제약 조건을 충족하지 못합니다 AWS 서비스.

요청의 하나 이상의 데이터 필드가 검증 및/또는 논리적 조합 요구 사항을 충족하지 않았습니다. 모든 리소스가 ARNs 완료되었고 텍스트 값이 AWS 보안 인시던트 대응 API 참조 가이드의 크기 및 형식 제약 조건을 충족하는지 확인하세요. 또한 값 업데이트가 허용되는지 확인합니다. 예를 들어 사례를 AWS 지원되는에서 자체 관리형으로 변경하는 것은 불가능합니다.

Support

추가 지원이 필요한 경우 문제 해결을 위해 Support 센터에 문의하세요. 다음 정보를 준비해 두십시오.

- AWS 리전 사용한
- 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
- 인터네트워크 트래픽 개인 정보 보호
- ID 및 액세스 관리
- AWS 보안 인시던트 대응 자격 증명 및 액세스 문제 해결
- 서비스 역할 사용
- 서비스 연결 역할 사용
- AWS 관리형 정책
- 인시던트 대응
- 규정 준수 확인
- AWS 보안 인시던트 대응의 로깅 및 모니터링
- 복원성
- 인프라 보안
- 구성 및 취약성 분석
- 교차 서비스 혼동된 대리자 방지

AWS 보안 인시던트 대응의 데이터 보호

내용

- 데이터 암호화

AWS 공동 책임 모델은 보안 인시던트 대응 서비스의 데이터 보호에 AWS 적용됩니다. 이 모델에 설명된 대로 AWS 는 AWS 클라우드에서 제공되는 서비스를 실행하는 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 또한 사용하는 AWS 서비스에 대한 보안 구성 및 관리 작업을 책임져야 합니다. 데이터 개인 정보 보호에 대한 자세한 내용은 데이터 개인 정보 보호 섹션을 FAQ참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

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

합니다IAM. 이렇게 하면 각 사용자에게 직무를 수행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다단계 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- 를 API 사용하여 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- AWS 암호화 솔루션과 AWS 서비스 내 모든 기본 보안 제어를 사용합니다.
- FIPS 140-3은 현재 서비스에서 지원되지 않습니다.

이메일 주소와 같은 기밀 또는 민감한 정보를 태그 또는 이름 필드와 같은 자유 형식 텍스트 필드에 입력해서는 안 됩니다. 여기에는 콘솔, API AWS CLI또는를 사용하여 AWS 지원 또는 기타 AWS 서비스를 사용하는 경우가 포함됩니다 AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드를 입력하는 모든 데이터는 결제 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL를 제공하는 경우 해당 서버에 대한 요청을 검증URL하기 위해에 자격 증명 정보를 포함하지 않는 것이 좋습니다.

데이터 암호화

내용

- 저장 시 암호화
- 전송 중 암호화
- 키 관리

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 대응에서 수집하고 액세스하는 데이터는 전송 계층 보안(TLS) 보호 채널을 통해서만 제공됩니다.

키 관리

AWS Security Incident Response는 와의 통합을 구현 AWS KMS 하여 사례 및 연결 데이터에 대한 저장 시 암호화를 제공합니다.

AWS 보안 인시던트 대응은 고객 관리형 키를 지원하지 않습니다.

인터네트워크 트래픽 개인 정보 보호

서비스와 온프레미스 클라이언트 및 애플리케이션 간의 트래픽

프라이빗 네트워크와 간에는 AWS두 가지 연결 옵션이 있습니다.

- AWS Site-to-Site VPN 연결입니다. 자세한 내용은 AWS Site-to-Site VPN사용 설명서의 AWS Site-to-Site VPN 이란 무엇입니까? 섹션을 참조하십시오.
- AWS Direct Connect 연결입니다. 자세한 내용은 AWS Direct Connect사용 설명서의 AWS Direct Connect 이란 무엇입니까? 섹션을 참조하십시오.

네트워크를 통한 AWS 보안 인시던트 대응에 대한 액세스는 AWS 게시된를 통해 이루어집니다APIs. 클라이언트는 전송 계층 보안(TLS) 1.2를 지원해야 합니다. 1.3TLS을 권장합니다. 또한 클라이언트는 Ephemeral Diffie-Hellman(PFS) 또는 Elliptic Curve Diffie-Hellman Ephemeral()과 같은 Perfect Forward 보안(DHE)을 사용하는 암호 제품군을 지원해야 합니다ECDHE. 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)을 사용하여 요청에 서명할 수 있는 임시 보안 자격 증명을 생성 할 수 있습니다.

같은 리전에 있는 AWS 리소스 사이의 트래픽

AWS 보안 인시던트 대응을 위한 Amazon Virtual Private Cloud(AmazonVPC) 엔드포인트는 AWS 보안 인시던트 대응에만 연결을 VPC 허용하는 내의 논리적 개체입니다. Amazon은 요청을 AWS 보안 인시던트 응답으로 VPC 라우팅하고 응답을 다시 로 라우팅합니다VPC. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 참조하세요. VPC 엔드포인트에서 액세스를 제어하는 데 사용할 수 있는 정책의 예는 IAM 정책 사용을 참조하여 DynamoDB에 대한 액세스를 제어합니다.

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

ID 및 액세스 관리

AWS Identity and Access Management(IAM)는 관리자가 AWS 리소스에 대한 액세스를 제어하는 데 도움이 되는 AWS 서비스입니다. IAM 관리자는 AWS 보안 인시던트 대응 리소스를 사용하도록 인증된(로그인된) 보안 주체 및 승인된(권한이 있는) 보안 주체를 제어합니다. IAM는 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

내용

- ID를 통한 인증
- AWS 보안 인시던트 대응의 작동 방식 IAM

대상

사용 방법 AWS Identity and Access Management (IAM)은 AWS 보안 인시던트 대응에서 수행하는 작업에 따라 다릅니다.

보안 관리자

이러한 사용자는 AWSSecurityIncidentResponseFullAccess 관리형 정책을 사용하여 멤버십 및 사례 리소스에 대한 읽기 및 쓰기 액세스 권한을 갖도록 하는 것이 좋습니다.

사례 감시자

이러한 개인은 모든 사례에 대한 권한 있는 액세스 권한이 있는 것은 아니지만 명시적 권한을 부여하는 개별 사례에 대한 권한 있는 액세스 권한이 있습니다.

인시던트 대응 팀원

팀원은 전체 멤버십과 사례 액세스 권한을 모두 부여받을 수 있습니다. 모든 개인이 서비스 멤버십에 대한 권위 있는 조치를 취하는 것은 아니지만 서비스를 통해 생성되고 관리되는 모든 사례에 액세스할 수 있어야 합니다. 자세한 내용은 AWS 보안 인시던트 대응 관리형 정책을 참조하세요.

ID를 통한 인증

인증은 자격 증명 AWS 으로에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증(로그인 AWS)을 받아야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 연합 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center(IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인하는 경우 관리

자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정한 상태입니다. 페더레이션을 사용하여 AWS에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 에 로그인하는 방법에 대한 자세한 내용은 로그인AWS 사용 설명서의 계정에 로그인하는 방법을 AWS참조하세요.AWS

AWS 프로그래밍 방식으로에 액세스하는 경우는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공하여 자격 증명을 사용하여 요청에 암호화 방식으로 서명합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은IAM 사용 설명서의AWS API 요청 서명을 참조하세요.

사용하는 인증 방법에 관계없이 추가 보안 정보를 제공해야 할 수 있습니다. 예를 들어,는 다중 인증(MFA)을 사용하여 계정의 보안을 강화하도록 AWS 권장합니다. 자세한 내용은AWS IAM Identity Center 사용 설명서의멀티 팩터 인증및IAM 사용 설명서의 멀티 팩터 인증 사용(MFA) AWS을 참조하세요.

AWS 계정 루트 사용자

AWS 계정을 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 전체 액세스 권한이 있는 로그인 자격 증명 하나로 시작합니다. 이 자격 증명을 Accountroot 사용자라고 AWS 하며 계정을 생성하는 데 사용한 8개의 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 말고 루트 사용자 자격 증명을 보호하기 위한 조치를 취합니다. 루트 사용자만 수행할 수 있는 작업을 수행하는 데만 사용합니다. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 ID

관리자 액세스가 필요한 사용자를 포함하여 사람이 자격 증명 공급자와의 연동을 사용하여 임시 자격 증명을 사용하여 AWS 서비스에 액세스하도록 요구하는 것이 가장 좋습니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS 디렉터리 서비스, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명이 계정에 액세스할 AWS 때 역할을 수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 IAM Identity Center를 사용하는 AWS 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 AWS 계정 및 애플리케이션에서 사용할 수 있도록 자체 자격 증명 소스의 사용자 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 IAM Identity Center 사용 설명서의 Identity Center란 무엇입니까?를 참조하세요.AWS IAM

IAM 사용자 및 그룹

IAM 사용자는 AWS 계정 내에서 단일 사용자 또는 애플리케이션에 대한 특정 권한이 있는 자격 증명입니다. 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. IAM 사용자와 함께 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 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 라는 그룹을 지정IAMAdmins하고 해당 그룹에 IAM 리소스를 관리할 수 있는 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 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은IAM 사용 설명서의 (역할 대신) IAM 사용자를 생성할 시기를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 있는 AWS 계정 내 자격 증명입니다. 이 역할은 IAM 사용자와 비슷하지만, 특정 개인과 연결되지 않습니다. IAM 역할을 전환하여 AWS 관리 콘솔에서 역할을 일시적으로 수임할 수 있습니다. 또는 AWS API 작업을 호출하거나 사용자 지정를 AWS CLI 사용하여 역할을 수임할 수 있습니다URL. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 자격 증명이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 자격 증명에 권한을 할당하려면 역할을 생성하고 역할에 대한 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션을 위한 역할에 대한 자세한 내용은IAM 사용 설명서의 타사 자격 증명 공급자의 역할 생성을 참조하세요. IAM 자격 증명 센터를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를의 역할과 상호 연관시킵니다IAM. 권한 세트에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 특정 작업에 대해 일시적으로 다른 권한을 맡을 IAM 역할을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 누군가(신뢰할 수 있는 보안 주체)가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스의 경우 (역할을 프록시로 사용하는 대신) 정책을 리소스에 직접 연결할 수

있습니다. 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면IAM 사용 설명서의 의 교차 계정 리소스 액세스를 IAM참조하세요.

- 교차 서비스 액세스 - 일부 AWS 서비스는 다른 AWS 서비스의 기능을 사용합니다. 예를 들어 서비스에서 호출할 때 해당 서비스가 Amazon에서 애플리케이션을 실행EC2하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는 직접적으로 호출하는 보안 주체의 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 수임하는IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정, 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은 서비스에 연결된 AWS 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS 계정에 표시되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon에서 실행되는 애플리케이션 EC2- IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 또는 AWS API 요청을 하는 AWS CLI 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 해당 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며, EC2 인스턴스에서 실행되는 프로그램이 임시 자격 증명을 얻을 수 있도록 합니다. 자세한 내용은IAM 사용 설명서의IAM역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

IAM 역할 또는 IAM 사용자를 사용할지 여부를 알아보려면IAM 사용 설명서의 IAM 역할 생성 시기(사용자 대신)를 참조하세요.

AWS 보안 인시던트 대응의 작동 방식 IAM

AWS Identity and Access Management(IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 지원하는 AWS 서비스입니다. IAM 관리자는 보안 인시던트 대응 리소스를 사용하도록 AWS 인증(로그인) 및 권한 부여(권한 있음)를 받을 수 있는 사용자를 제어합니다. IAM는 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

IAM AWS 보안 인시던트 대응과 함께 사용할 수 있는 기능	
IAM 기능	서비스 정렬
ID 기반 정책	예

IAM AWS 보안 인시던트 대응과 함께 사용할 수 있는 기능	
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예(글로벌)
ACLs	No
ABAC (정책의 태그)	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	아니요
서비스 링크 역할	예

내용

- AWS 보안 인시던트 대응을 위한 자격 증명 기반 정책

AWS 보안 인시던트 대응을 위한 자격 증명 기반 정책

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

IAM 자격 증명 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 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

내용

- 자격 증명 기반 정책 예제

- 정책 모범 사례
- AWS 보안 인시던트 대응 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 보안 인시던트 대응을 위한 AWS 정책 조건 키
- AWS 보안 인시던트 대응의 액세스 제어 목록(ACLs)

자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AWS 보안 인시던트 대응 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS 명령줄 인터페이스(AWS CLI) 또는를 사용하여 작업을 수행할 수 없습니다 AWS API. 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 수임할 수 있습니다.

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

각 리소스 유형에 대한 형식을 포함하여 보안 인시던트 대응에서 정의한 AWS 작업 및 리소스 유형에 ARNs 대한 자세한 내용은 서비스 승인 참조의 AWS 보안 인시던트 대응에 대한 작업, 리소스 및 조건 키를 참조하세요.

정책 모범 사례

자격 증명 기반 정책은 계정에서 보안 AWS 인시던트 대응 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이러한 작업으로 AWS 인해 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. AWS 계정에서 사용할 수 있습니다. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 관한AWS 관리형 정책을 참조하세요.

최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 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 정책 조건을 작성하여를 사용하여 모든 요청을 전송하도록 지정할 수 있습니다SSL. 와 같은 특정 서비스를 통해 사용되는 경우 조건을 사용하여 AWS 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

IAM Access Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 정책이 정책 언어(JSON) 및 IAM 모범 사례를 준수하도록 새 정책 및 기존 IAM 정책을 검증합니다. IAM Access Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 확인 및 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.

다중 인증 필요(MFA) - IAM 사용자 또는 AWS 계정의 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 MFA 위해를 켭니다. API 작업을 호출할 MFA 때를 요구하려면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA-보호된 API 액세스 구성을 참조하세요.

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

AWS 보안 인시던트 대응 콘솔 사용

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

또는 에만 AWS CLI 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다 AWS API. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스하도록 허용합니다.

AWS 보안 인시던트 대응 액세스 또는 ReadOnly AWS 관리형 정책을 연결하여 사용자와 역할이 서비스 콘솔을 사용할 수 있도록 합니다. 자세한 내용은 IAM사용 설명서의 사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여 줍니다. 이 정책에는 콘솔에서 또는 또는를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 AWS CLI 권한이 포함되어 있습니다 AWS API.

```
{
"Version": "2012-10-17",
```

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

AWS 보안 인시던트 대응 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 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 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연합된 사용자 또는 AWS 서비스가 포함될 수 있습니다.

자세한 내용은 IAM 사용 설명서의에서 교차 계정 리소스 액세스를 IAM 참조하세요.

AWS 보안 인시던트 대응에 대한 정책 작업

지원 정책 작업: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 작업 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 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 승인 참조의 AWS 보안 인시던트 대응에서 정의한 작업을 참조하세요.

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

AWS 보안 인시던트 대응 - 자격 증명

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

“작업”: [“AWS 보안 인시던트 대응 -identity:action1”, “AWS 보안 인시던트 대응 -identity:action2”]

Amazon AWS 보안 인시던트 대응을 위한 정책 리소스

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

리소스 JSON 정책 요소는 작업이 적용되는 객체를 지정합니다. 문에는 리소스 또는 NotResource 요소가 포함되어야 합니다. 가장 좋은 방법은 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정하는 것입니다. 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": "*"

보안 인시던트 대응을 위한 AWS 정책 조건 키

서비스별 정책 조건 키 지원:아니요

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

조건 요소(또는 조건 블록)를 사용하면 문이 적용되는 조건을 지정할 수 있습니다. Condition 요소는 선택 사항입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

문에 여러 조건 요소를 지정하거나 단일 조건 요소에 여러 키를 지정하는 경우는 논리적 AND 작업을 사용하여 해당 요소를 AWS 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 OR 작업을 사용하여 조건을 AWS 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.

AWS 는 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 액세스 제어 목록(ACLs)

지원: ACLs 아니요

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

AWS 보안 인시던트 대응을 통한 속성 기반 액세스 제어(ABAC)

지원ABAC(정책의 태그):예

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. 엔터티 및 리소스에 태그를 지정하는 것은의 첫 번째 단계입니다ABAC. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로워지는 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 AWS:ResourceTag/key-name, AWS:RequestTag/key-name 또는 AWS:TagKeys condition 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다. 서비스가 모든 리소스 유형에 대해 3개의 조건 키를 모두 지원하는 경우 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 개의 조건 키를 모두 지원하는 경우 값은 부분적입니다.에 대한 자세한

내용은 IAM 사용 설명서의 란 무엇입니까ABAC?를 ABAC참조하세요. 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어 사용(ABAC)을 ABAC참조하세요.

Amazon AWS Security Incident Response를 사용한 임시 자격 증명

임시 자격 증명 지원: 예

AWS 임시 자격 증명을 사용하여 로그인하면 서비스가 작동하지 않습니다. 임시 자격 증명으로 작업하는 AWS 서비스를 비롯한 자세한 내용은 IAM 사용 설명서의 AWS 에서 작업하는 서비스를 IAM 참조하세요. 사용자 이름 및 암호를 제외한 방법을 사용하여 AWS Management Console에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 Single Sign-On(SSO) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

CLI 또는를 AWS 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS API. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 동적으로 임시 자격 증명을 생성하는 access AWS. AWS recommends에 액세스할 수 있습니다. 자세한 내용은 의 임시 보안 자격 증명을 IAM참조하세요.

AWS 보안 인시던트 대응을 위한 전달 액세스 세션

전달 액세스 세션 지원(FAS): 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 호출하는 보안 주체의 권한을 요청 AWS 서비스와 결합하여 다운스트림 서비스에 대한 요청을 합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신하는 경우에만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 액세스 세션 전달을 참조하세요.

AWS 보안 인시던트 대응 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 보안 인시던트 대응 및 작업 AWS 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다IAM.

주제

- 작업을 수행할 권한이 없음
- iam을 수행할 권한이 없습니다.PassRole

- 내 AWS 계정 외부의 사람이 내 AWS 보안 인시던트 대응 리소스에 액세스하도록 허용하고 싶습니다.

작업을 수행할 권한이 없음

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 my-example-widget 리소스에 대한 세부 정보를 보려고 하지만 가상 AWS 보안 인시던트 대응 :GetWidget 권한이 없는 경우에 발생합니다.

사용자: arn:AWS:iam::123456789012:user/mateojackson은 다음 작업을 수행할 권한이 없습니다.AWS 보안 인시던트 대응: 리소스GetWidget: my-example-widget

이 경우 AWS 보안 인시던트 대응 :GetWidget action을 사용하여 리소스에 대한 액세스를 my-example-widget 허용하도록 mateojackson 사용자의 정책을 업데이트해야 합니다.

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

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

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

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 보안 인시던트 대응에서 AWS 작업을 수행하려고 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

사용자: arn:AWS:iam::123456789012:user/marymajor는 iam:PassRole

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

내 AWS 계정 외부의 사람이 내 AWS 보안 인시던트 대응 리소스에 액세스하도록 허용하고 싶습니다.

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.

자세히 알아보려면 다음을 참조하세요.

- Amazon AWS Security Incident Response가 이러한 기능을 지원하는지 알아보려면에서 AWS 보안 인시던트 대응이 작동하는 방식을 참조하세요IAM.
- 소유한 계정에서 AWS 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른 AWS 계정의 IAM 사용자에게 액세스 권한 제공을 참조하세요.
- 타사 AWS 계정에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 소유 AWS 계정에 대한 액세스 권한 제공을 참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 교차 계정 액세스를 위한 역할 및 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 에서 교차 계정 리소스 액세스를 IAM 참조하세요.

서비스 역할 사용

서비스 역할 지원:아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정, 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 권한을 위임하는 역할 생성을 참조하세요.

서비스 연결 역할 사용

AWS 보안 인시던트 대응을 위한 서비스 연결 역할

내용

- AWS SLR: AWSServiceRoleForSecurityIncidentResponse
- AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage
- AWS Security Incident Response 서비스 연결 역할에 지원되는 리전

서비스 링크 역할 지원: 예

서비스 연결 역할은 서비스에 연결된 AWS 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 AWS 보안 인시던트 대응을 더 쉽게 설정할 수 있습니다. AWS 보안 인시던트 대응은 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 AWS 보안 인시던트 대응만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 개체에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 서비스 연결 역할 열에서 AWS 로 작업하는 서비스를 IAM 참조하고 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse

AWS 보안 인시던트 대응은 – AWS 보안 인시던트 대응 정책이라는 AWSServiceRoleForSecurityIncidentResponse 서비스 연결 역할(SLR)을 사용하여 구독한 계정을 식별하고, 사례를 생성하고, 관련 리소스에 태그를 지정합니다.

권한

AWSServiceRoleForSecurityIncidentResponse 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

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

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

- AWS Organizations: 서비스가 서비스에 사용할 멤버십 계정을 조회할 수 있도록 허용합니다.
- CreateCase: 서비스가 멤버십 계정을 대신하여 서비스 사례를 생성하도록 허용합니다.
- TagResource: 서비스의 일부로 구성된 서비스 태그 리소스를 허용합니다.

역할 관리

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI또는에서 AWS 보안 인시던트 대응에 온보딩하면 AWS API서비스가 서비스 연결 역할을 생성합니다.

> **Note**
>
> 위임된 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 서비스 연결 역할이 다시 생성됩니다.

IAM 개체(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage

AWS 보안 인시던트 대응은 - AWS 보안 인시던트 대응 정책이라는 AWSServiceRoleForSecurityIncidentResponse_Triage 서비스 연결 역할(SLR)을 사용하여 환경에 보안 위협이 있는지 지속적으로 모니터링하고, 보안 서비스를 조정하여 경보 노이즈를 줄이고, 정보를 수집하여 잠재적 인시던트를 조사합니다.

권한

AWSServiceRoleForSecurityIncidentResponse_Triage 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

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

AWS AWSSecurityIncidentResponseTriageServiceRolePolicy 관리형 정책이 이 역할에 연결됩니다. 서비스는 역할을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- 이벤트: 서비스가 Amazon EventBridge 관리형 규칙을 생성하도록 허용합니다. 이 규칙은 AWS 계정에서 서비스로 이벤트를 전송하는 데 필요한 인프라입니다. 이 작업은에서 관리하는 모든 AWS 리소스에서 수행됩니다`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: 서비스가 보안 서비스를 조정하여 알림 노이즈를 줄이고 잠재적 인시던트를 조사하기 위한 정보를 수집할 수 있도록 허용합니다. 이 작업은 모든 AWS 리소스에서 수행됩니다.
- AWS Security Hub: 서비스가 보안 서비스를 조정하여 알림 노이즈를 줄이고 잠재적 인시던트를 조사하기 위한 정보를 수집할 수 있도록 허용합니다. 이 작업은 모든 AWS 리소스에서 수행됩니다.

역할 관리

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI또는에서 AWS 보안 인시던트 대응에 온보딩하면 AWS API서비스가 서비스 연결 역할을 생성합니다.

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

IAM 개체(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS Security Incident Response 서비스 연결 역할에 지원되는 리전

AWS 보안 인시던트 대응은 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다.

- 미국 동부(오하이오)
- 미국 서부(오리건)
- 미국 동부(버지니아)
- EU(프랑크푸르트)
- EU(아일랜드)
- EU(런던)
- EU(스톡홀름)
- 아시아 태평양(싱가포르)
- 아시아 태평양(서울)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 캐나다(중부)

AWS 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀이 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하는 데는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이러한 정책은 일반적인 사용 사례를 다루며 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 서비스는 연결된 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책의 권한은 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 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 중단되지 않습니다.

또한 여러 서비스에 걸쳐 있는 작업 함수에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 작업 함수 정책의 목록 및 설명은 IAM 사용 설명서의 AWS 작업 함수에 대한 관리형 정책을 참조하세요.

내용

- AWS 관리형 정책: AWSSecurityIncidentResponseServiceRolePolicy
- AWS 관리형 정책: AWSSecurityIncidentResponseFullAccess
- AWS 관리형 정책: AWSSecurityIncidentResponseReadOnlyAccess
- AWS 관리형 정책: AWSSecurityIncidentResponseCaseFullAccess
- AWS 관리형 정책: AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWS SLRs 및 관리형 정책에 대한 보안 인시던트 대응 업데이트

AWS 관리형 정책: AWSSecurityIncidentResponseServiceRolePolicy

AWS 보안 인시던트 대응은 AWSSecurityIncidentResponseServiceRolePolicy AWS 관리형 정책을 사용합니다. 이 AWS 관리형 정책은 AWSServiceRoleForSecurityIncidentResponse 서비스 연결 역할에 연결됩니다. 이 정책은 AWS 보안 인시던트 대응에 대한 액세스를 제공하여 구독한 계정을 식별하고, 사례를 생성하고, 관련 리소스에 태그를 지정합니다.

> **Important**
>
> 개인 식별 정보(PII) 또는 기타 기밀 또는 민감한 정보를 태그에 저장하지 마십시오. AWS Security Incident Response는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 프라이빗 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- AWS Organizations: 서비스가 서비스에 사용할 멤버십 계정을 조회할 수 있도록 허용합니다.

- CreateCase: 서비스가 멤버십 계정을 대신하여 서비스 사례를 생성하도록 허용합니다.
- TagResource: 서비스의 일부로 구성된 서비스 태그 리소스를 허용합니다.

에 대한 AWS 관리형 정책에서이 정책과 연결된 권한을 볼 수 있습니다 AWSSecurityIncidentResponseServiceRolePolicy.

AWS 관리형 정책: AWSSecurityIncidentResponseFullAccess

AWS 보안 인시던트 대응은 AWSSecurityIncidentResponseAdmin AWS 관리형 정책을 사용합니다. 이 정책은 서비스 리소스에 대한 전체 액세스 권한과 관련에 대한 액세스 권한을 부여합니다 AWS 서비스. IAM 보안 주체와 함께이 정책을 사용하여 AWS 보안 인시던트 대응에 대한 권한을 빠르게 추가할 수 있습니다.

> **Important**
>
> 개인 식별 정보(PII) 또는 기타 기밀 또는 민감한 정보를 태그에 저장하지 마십시오. AWS Security Incident Response는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 프라이빗 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

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

에 대한 AWS 관리형 정책에서이 정책과 연결된 권한을 볼 수 있습니다 AWSSecurityIncidentResponseFullAccess.

AWS 관리형 정책: AWSSecurityIncidentResponseReadOnlyAccess

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

> **Important**
>
> 개인 식별 정보(PII) 또는 기타 기밀 또는 민감한 정보를 태그에 저장하지 마십시오. AWS Security Incident Response는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 프라이빗 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

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

에 대한 AWS 관리형 정책에서이 정책과 연결된 권한을 볼 수 있습니다 AWSSecurityIncidentResponseReadOnlyAccess.

AWS 관리형 정책: AWSSecurityIncidentResponseCaseFullAccess

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

> **Important**
>
> 개인 식별 정보(PII) 또는 기타 기밀 또는 민감한 정보를 태그에 저장하지 마십시오. AWS Security Incident Response는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 프라이빗 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

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

에 대한 AWS 관리형 정책에서이 정책과 연결된 권한을 볼 수 있습니다 AWSSecurityIncidentResponseCaseFullAccess.

AWS 관리형 정책: AWSSecurityIncidentResponseTriageServiceRolePolicy

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

이 정책은 AWS 보안 인시던트 대응에 대한 액세스를 제공하여 보안 위협에 대해 환경을 지속적으로 모니터링하고, 보안 서비스를 조정하여 알림 노이즈를 줄이고, 잠재적 인시던트를 조사하기 위한 정보를 수집합니다. IAM 개체에 이 정책을 연결할 수 없습니다.

> **Important**
>
> 개인 식별 정보(PII) 또는 기타 기밀 또는 민감한 정보를 태그에 저장하지 마십시오. AWS Security Incident Response는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 프라이빗 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

권한 세부 정보

서비스는이 정책을 사용하여 다음 리소스에 대한 작업을 수행합니다.

- 이벤트: 서비스가 Amazon EventBridge 관리형 규칙을 생성하도록 허용합니다. 이 규칙은 AWS 계정에서 서비스로 이벤트를 전송하는 데 필요한 인프라입니다. 이 작업은에서 관리하는 모든 AWS 리소스에서 수행됩니다`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: 서비스가 보안 서비스를 조정하여 알림 노이즈를 줄이고 잠재적 인시던트를 조사하기 위한 정보를 수집할 수 있도록 허용합니다. 이 작업은 모든 AWS 리소스에서 수행됩니다.
- AWS Security Hub: 서비스가 보안 서비스를 조정하여 알림 노이즈를 줄이고 잠재적 인시던트를 조사하기 위한 정보를 수집할 수 있도록 허용합니다. 이 작업은 모든 AWS 리소스에서 수행됩니다.

에 대한 AWS 관리형 정책에서이 정책과 연결된 권한을 볼 수 있습니다 AWSSecurityIncidentResponseTriageServiceRolePolicy.

AWS SLRs 및 관리형 정책에 대한 보안 인시던트 대응 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 AWS 보안 인시던트 대응 SLRs 및 관리형 정책 역할의 업데이트에 대한 세부 정보를 봅니다.

변경 사항	설명	날짜
신규 SLR - AWSServiceRoleForSecurityIncidentResponse 새로운 관리형 정책 - AWSSecurityIncidentResponseServiceRolePolicy.	새 서비스 연결 역할 및 연결된 정책을 통해 AWS Organizations 계정에 대한 서비스 액세스를 통해 멤버십을 식별할 수 있습니다.	2024년 12월 1일
신규 SLR - AWSServiceRoleForSecurityIncidentResponse_Triage 새로운 관리형 정책 - AWSSecurityIncidentResponseTriageServiceRolePolicy	AWS Organizations 계정에 대한 서비스 액세스를 허용하여 보안 이벤트를 분류할 수 있는 새로운 서비스 연결 역할 및 연결된 정책입니다.	2024년 12월 1일
새로운 관리형 정책 - AWSSecurityIncidentResponseFullAccess	AWS 보안 인시던트 대응은 서비스에 대한 읽기 및 쓰기 작업을 위해 IAM 보안 주체에 SLR 연결할 새를 추가합니다.	2024년 12월 1일
새로운 관리형 정책 역할 - AWSSecuri	AWS 보안 인시던트 대응에서 읽기 작업을 위해 IAM 보안 주체SLR에 연결할 새를 추가합니다.	2024년 12월 1일

변경 사항	설명	날짜
tyIncidenTResponseReadOnlyAccess		
새로운 관리형 정책 역할 - AWSSecurityIncidenTResponseCaseFullAccess	AWS 보안 인시던트 대응은 서비스 사례에 대한 읽기 및 쓰기 작업을 위해 IAM 보안 주체에 SLR 연결할 새를 추가합니다.	2024년 12월 1일
변경 사항 추적을 시작했습니다.	AWS 보안 인시던트 대응 SLRs 및 관리형 정책에 대한 변경 사항 추적 시작	2024년 12월 1일

인시던트 대응

보안 및 규정 준수는 AWS 와 고객 간의 공동 책임입니다. 이 공유 모델은 호스트 운영 체제 및 가상화 계층에서 서비스가 AWS 운영되는 시설의 물리적 보안에 이르기까지 운영, 관리 및 제어 시 고객의 운영 부담을 완화하는 데 도움이 될 수 있습니다. 고객은 게스트 운영 체제(업데이트 및 보안 패치 포함), 기타 관련 애플리케이션 소프트웨어 및 AWS 제공된 보안 그룹 방화벽의 구성에 대한 책임과 관리를 맡습니다. 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 주제일 수 있으므로 인시던트 대응과 선택 사항이 기업 목표에 미치는 영향을 더 잘 이해할 수 있도록 다음 리소스를 검토하는 것이 좋습니다. AWS 보안 모범 사례 백서 및 AWS 클라우드 채택 프레임워크의 보안 관점(CAF) 백서.

규정 준수 확인

타사 감사자는 여러 규정 준수 AWS 프로그램의 일환으로 서비스의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, 연준RAMP, HIPAA, 기타 등이 포함됩니다.

AWS 보안 인시던트 대응은 앞서 언급한 프로그램을 준수하는지 평가되지 않았습니다.

특정 규정 준수 프로그램 범위의 AWS 서비스 목록은 AWS 규정 준수 프로그램별 범위 내 서비스를 참조하세요. 일반 정보는 AWS 규정 준수 프로그램을 참조하세요.

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

AWS 서비스 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 해당 l AWS 및 규정에 따라 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 및 규정 준수 빠른 시작 가이드 -이 배포 가이드에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수 중심 기준 환경을 배포하기 위한 단계를 제공합니다 AWS.
- HIPAA 보안 및 규정 준수를 위한 설계 백서 -이 백서에서는 기업이 HIPAA AWS 를 사용하여 규정을 준수하는 애플리케이션을 생성하는 방법을 설명합니다.
- AWS 규정 준수 리소스 - 산업 및/또는 위치에 따라 적용되는 워크북 및 가이드 모음입니다.
- AWS Config 개발자 안내서 –Config;의 Config 규칙을 사용하여 리소스 평가는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다. AWS AWS
- AWS Security Hub -이 AWS 서비스는 내 보안 상태를 포괄적으로 보여줍니다 AWS. Security Hub는 보안 제어를 사용하여 AWS 리소스를 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 의심스러운 악의적인 활동이 있는지 환경을 모니터링하여 AWS 계정, 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 탐지합니다.는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족DSS하여 PCI와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 GuardDuty 수 있습니다.
- AWS Audit Manager -이 AWS 서비스는 AWS 사용량을 지속적으로 감사하여 위험 및 규정 및 업계 표준 준수를 관리하는 방법을 간소화하는 데 도움이 됩니다.

AWS 보안 인시던트 대응의 로깅 및 모니터링

모니터링은 AWS 보안 인시던트 대응 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS 보안 인시던트 대응은 현재 조직과 조직 내에서 발생하는 활동을 모니터링하기 위해 다음 AWS 서비스를 지원합니다.

AWS CloudTrail -를 CloudTrail 사용하여 AWS 보안 인시던트 대응 콘솔에서 API 호출을 캡처할 수 있습니다. 예를 들어, 사용자가 인증할 때는 요청의 IP 주소, 요청을 한 사람, 요청이 수행된 시간과 같은 세부 정보를 CloudTrail 기록할 수 있습니다.

Amazon 지표 CloudWatch - CloudWatch 지표를 사용하면 이벤트 발생 시 거의 실시간으로 자동 작업을 모니터링, 보고 및 수행할 수 있습니다. 예를 들어 제공된 지표에 CloudWatch 대시보드를 생성하여 AWS 보안 인시던트 대응 사용량을 모니터링하거나 제공된 지표에 CloudWatch 경보를 생성하여 설정된 임계값 위반 시 알릴 수 있습니다.

서비스의 네임스페이스는 AWS/Usage/입니다ServiceName. 사용 가능한 지표 이름은 ActiveManagedCases 및 입니다 SelfManagedCases.

AWS 서비스 약관에 따라 AWS 보안 인시던트 대응 대응 팀은 CloudTrailVPC, DNS 및 S3 로그 데이터의 기록에 액세스할 수 있습니다. 이 데이터는 보안 인시던트 대응 서비스 포털에서 AWS 사례가 열려 있는 활성 보안 인시던트 중에 사용할 수 있습니다.

복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 기반으로 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 대응은 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스와가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 AWS 보안 인시던트 대응에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- DHE (Ephemeral Diffie-HellmanPFS) 또는 (Elliptic Curve Ephemeral Diffie-Hellman)과 같은 완벽한 순방향 보안ECDHE()이 포함된 Cipher 제품군입니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 보안 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

구성 및 취약성 분석

서비스 억제 역할 및 관련 AWS CloudFormation 스택 세트를 관리할 책임은 사용자에게 있습니다.

AWS 는 게스트 운영 체제(OS) 및 데이터베이스 패치 적용, 방화벽 구성, 재해 복구와 같은 기본 보안 작업을 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. 에서 서비스 AWS간 위장은 혼동된 대리자 문제를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 직접적으로 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 통해 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 AWS 제공합니다.

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

혼동된 대리자 문제를 방지하는 가장 효과적인 방법은 허용하려는 리소스의 정확한 Amazon 리소스 이름(ARN)을 사용하는 것입니다. 리소스 ARN 전체를 모르거나 여러 리소스를 지정하는 경우의 알 수 없는 부분에 와일드카드(*)와 함께 AWS:SourceArn global 컨텍스트 조건 키를 사용합니다ARN. 예: arn:AWS:servicename::region-name::your AWS account ID:*.

혼동된 대리자 문제를 방지하는 방법을 보여주는 수임 역할 정책의 예는 혼동된 대리자 방지 정책을 참조하세요.

Service Quotas

AWS 보안 인시던트 대응

다음 표에는 AWS계정의AWS 보안 인시던트 대응 리소스에 대한 할당량이 나열되어 있습니다. 일부 할당량은 서비스 관리자의 승인을 받아 아래에 명시된 할당량 이상으로 증가할 수 있습니다. 달리 표시되지 않는 한 이러한 할당량은 리전당 할당량입니다.

	명칭	기본값	조정 가능	설명
1	활성 AWS 지원 사례	10	예(최대 50개)	에서 지원을 요청하는 활성 사례 수입니다 AWS CIRT.
2	활성 자체 관리형 사례	50	예(최대 100개)	도움 없이 플랫폼을 사용하는 활성 사례 수입니다 AWS CIRT.
3	24시간 이내에 생성된 서비스 지원 사례	10	No	24시간 롤링 기간에 생성된의 지원을 요청하는 AWS CIRT 생성된 사례 수입니다.
4	기본 인시던트 대응 팀의 최대 엔터티 수	10	No	기본 인시던트 대응 팀의 최대 개체 수입니다.
5	사례의 최대 추가 멤버 수	30	No	사례와 연결된 최대 개체 수입니다. 이는 처음에 기본 인시던트 대응 팀의 엔터티로 채워집니다.

	명칭	기본값	조정 가능	설명
6	최대 사례 첨부 파일 수	50	예(최대 100개)	사례에 연결할 수 있는 최대 파일 수입니다.
7	최대 사례 설명 크기	1000	No	대/소문자 설명의 최대 문자 수입니다.
8	최대 사례 첨부 파일 이름 크기	255	No	파일 이름의 최대 문자 수입니다.

AWS 보안 인시던트 대응 기술 안내서

내용

- 요약
- 귀사는 Well-Architected입니까?
- 소개
- 준비
- 운영
- 인시던트 사후 활동
- 결론
- 기여자
- 부록 A: 클라우드 기능 정의
- 부록 B: AWS 인시던트 응답 리소스
- 고지 사항

요약

이 안내서는 고객의 Amazon Web Services(AWS) 클라우드 환경 내에서 보안 인시던트에 대응하는 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 역할을 수행하는 사용자를 대상으로 하며 정보 보안의 일반적인 원칙을 숙지하고, 현재 온프레미스 환경에서 보안 인시던트 대응에 대한 기본적인 이해를 갖추고, 클라우드 서비스에 대해 어느 정도 잘 알고 있다고 가정합니다.

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 사용할 수 AWS Well-Architected Tool있는를 사용하면 각 영역에 대한 일련의 질문에 답하여 이러한 모범 사례에 대해 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

보안은의 최우선 순위입니다 AWS. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 지원하기 위해 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다. AWS 에는 공동 책임 모델이 있습니다. 클라우드의 보안을 AWS 관리하고 고객은 클라우드의 보안을 책임집니다. 즉, 보안 목표를 충족하는 데 도움이 되는 여러 도구 및 서비스에 대한 액세스를 포함하여 보안 구현을 완벽하게 제어할 수 있습니다. 이러한 기능은에서 실행되는 애플리케이션의 보안 기준을 설정하는 데 도움이 됩니다 AWS 클라우드.

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

보안 인시던트 대응은 복잡할 수 있으므로 핵심 보안 서비스로 시작하고, 기본 탐지 및 대응 기능을 구축한 다음, 플레이북을 개발하여 반복 및 개선할 인시던트 대응 메커니즘의 초기 라이브러리를 생성하는 등 반복적인 접근 방식을 구현하는 것이 좋습니다.

시작하기 전에

에서 보안 이벤트에 대한 인시던트 대응에 대해 알아보기 전에 AWS 보안 및 인시던트 대응에 대한 관련 표준 및 프레임워크를 AWS숙지하세요. 이러한 기반은이 가이드에 제시된 개념과 모범 사례를 이해하는 데 도움이 됩니다.

AWS 보안 표준 및 프레임워크

먼저 보안, 자격 증명 및 규정 준수 모범 사례, 보안 원칙 - AWS ell-Architected Framework 및 AWS 클라우드 채택 프레임워크 개요의 보안 관점(AWS CAF) 백서를 검토하는 것이 좋습니다.

는 클라우드로 AWS CAF 이동하는 조직의 여러 부분 간의 조정을 지원하는 지침을 제공합니다. 이 AWS CAF 지침은 클라우드 기반 IT 시스템 구축과 관련된 관점이라고 하는 여러 중점 영역으로 나뉩니다. 보안 관점에서는 워크스트림 간에 보안 프로그램을 구현하는 방법을 설명합니다.이 중 하나는 인시던트 대응입니다. 이 문서는 고객과 협력하여 효과적이고 효율적인 보안 인시던트 대응 프로그램 및 기능을 구축하는 데 도움이 되는 경험의 결과물입니다.

산업 인시던트 대응 표준 및 프레임워크

이 백서는 National Institute of Standards and Technology()에서 만든 컴퓨터 보안 인시던트 처리 가이드 SP 800-61 r2의 인시던트 대응 표준 및 모범 사례를 따릅니다NIST. 에서 도입한 개념을 읽고 이해하는 NIST 것은 유용한 사전 조건입니다. 이 NIST 가이드의 개념과 모범 사례는이 백서의 AWS 기술에 적용됩니다. 그러나 온프레미스 인시던트 시나리오는이 가이드의 범위를 벗어납니다.

AWS 인시던트 응답 개요

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

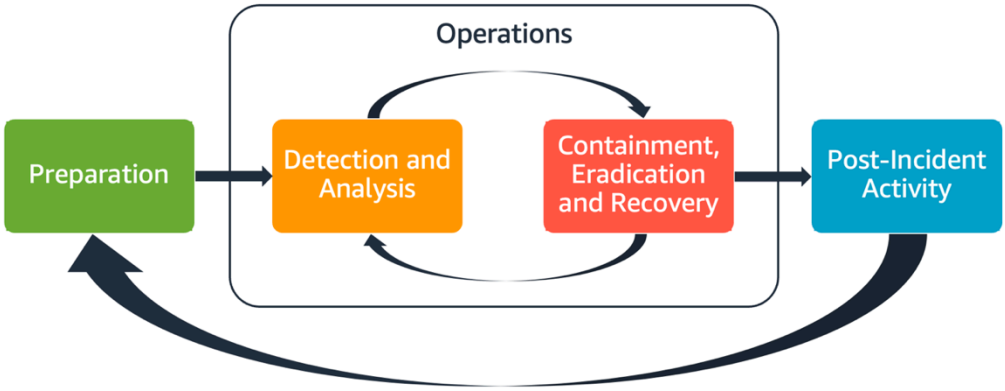
AWS 인시던트 대응의 측면

조직 내 모든 AWS 사용자는 보안 인시던트 대응 프로세스를 기본적으로 이해하고 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. 클라우드에서 성공적인 인시던트 대응 프로그램의 토대는 준비, 운영 및 인시던트 후 활동입니다.

이러한 각 측면을 이해하려면 다음 설명을 고려하세요.

- 준비 - 탐지 제어를 AWS 활성화하고 필요한 도구 및 클라우드 서비스에 대한 적절한 액세스를 확인하여 인시던트 대응 팀이 내부에서 인시던트를 탐지하고 대응할 수 있도록 준비합니다. 또한 신뢰할 수 있는 일관된 응답을 보장하는 데 필요한 수동 및 자동 런북을 준비합니다.
- 운영 - NIST의 인시던트 대응 단계인 탐지, 분석, 포함, 근절 및 복구에 따라 보안 이벤트 및 잠재적 인시던트에 대해 운영합니다.
- 인시던트 후 활동 - 보안 이벤트 및 시뮬레이션의 결과를 반복하여 대응의 유효성을 개선하고, 대응 및 조사에서 파생된 가치를 높이고, 위험을 추가로 줄입니다. 인시던트를 통해 배우고 개선 활동에 대한 강한 주인의식을 가져야 합니다.

이러한 각 측면은이 가이드에서 자세히 설명합니다. 다음 다이어그램은 앞서 언급한 NIST 인시던트 대응 수명 주기와 일치하지만 억제, 근절 및 복구를 통한 탐지 및 분석을 포함하는 작업에 따라 이러한 측면의 흐름을 보여줍니다.



AWS 인시던트 대응의 측면

AWS 인시던트 대응 원칙 및 설계 목표

NIST SP 800-61 컴퓨터 보안 인시던트 처리 가이드에 정의된 인시던트 대응의 일반적인 프로세스 및 메커니즘은 합리적이지만 클라우드 환경에서 보안 인시던트에 대응하는 것과 관련된 다음과 같은 특정 설계 목표도 고려하는 것이 좋습니다.

- 대응 목표 설정 - 이해관계자, 법률 고문 및 조직 리더십과 협력하여 인시던트에 대한 대응 목표를 결정합니다. 몇 가지 일반적인 목표에는 문제를 포함 및 완화하고, 영향을 받는 리소스를 복구하고, 포렌식에 대한 데이터를 보존하고, 알려진 안전한 작업으로 되돌리고, 궁극적으로 인시던트에서 학습하는 것이 포함됩니다.
- 클라우드를 사용하여 대응 - 이벤트 및 데이터가 발생하는 클라우드 내에서 응답 패턴을 구현합니다.
- 무엇이 있고 무엇이 필요한지 파악 - 로그, 리소스, 스냅샷 및 기타 증거를 복사하여 응답 전용 중앙 집중식 클라우드 계정에 저장하여 보존합니다. 태그, 메타데이터, 보존 정책을 적용하는 메커니즘을 사용합니다. 사용하는 서비스를 파악한 다음 해당 서비스를 조사하기 위한 요구 사항을 식별해야 합니다. 환경을 이해하는 데 도움이 되도록이 문서의 뒷부분 the section called “태그 지정 전략 개발 및 구현” 섹션에서 다루는 태그 지정을 사용할 수도 있습니다.
- 재배포 메커니즘 사용 - 잘못된 구성으로 인해 보안 이상이 발생할 수 있는 경우 적절한 구성으로 리소스를 재배포하여 분산을 제거하는 것만큼 간단한 문제 해결이 가능할 수 있습니다. 가능한 침해가 식별되면 재배포에 근본 원인의 성공적이고 확인된 완화가 포함되어 있는지 확인합니다.
- 가능한 경우 자동화 - 문제가 발생하거나 인시던트가 반복되면 프로그래밍 방식으로 일반적인 이벤트를 분류하고 대응하는 메커니즘을 구축합니다. 자동화가 충분하지 않은 고유하거나 복잡하거나 민감한 인시던트에는 인적 응답을 사용합니다.
- 확장 가능한 솔루션 선택 - 클라우드 컴퓨팅에 대한 조직의 접근 방식의 확장성에 맞게 노력합니다. 환경 전반에 걸쳐 확장되는 탐지 및 대응 메커니즘을 구현하여 탐지와 대응 사이의 시간을 효과적으로 줄입니다.

- 프로세스 학습 및 개선 - 프로세스, 도구 또는 인력의 격차를 사전에 식별하고 이를 해결하기 위한 계획을 구현합니다. 시뮬레이션은 격차를 찾고 프로세스를 개선하는 안전한 방법입니다. 프로세스를 반복하는 방법에 대한 자세한 내용은이 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 때 포렌식으로 건전한 대응 방법을 사용하는 것이 가장 좋습니다. 경우에 따라 이러한 응답 작업에 대해 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 도메인

AWS 환경에서 보안 이벤트에 효과적으로 대비하고 대응하려면 클라우드 보안 인시던트의 일반적인 유형을 이해해야 합니다. 고객의 책임 내에는 서비스, 인프라 및 애플리케이션이라는 세 가지 도메인이 있습니다. 도메인마다 다양한 지식, 도구 및 응답 프로세스가 필요합니다. 다음 도메인을 고려합니다.

- 서비스 도메인 - 서비스 도메인의 인시던트는 사용자 AWS 계정, AWS Identity and Access Management (IAM) 권한, 리소스 메타데이터, 결제 또는 기타 영역에 영향을 미칠 수 있습니다. 서비스 도메인 이벤트는 메커니즘으로 AWS API만 응답하거나 구성 또는 리소스 권한과 관련된 근본 원인이 있고 관련 서비스 지향 로깅이 있을 수 있는 이벤트입니다.
- 인프라 도메인 - 인프라 도메인의 인시던트에는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 프로세스 및 데이터, 가상 프라이빗 클라우드() 내의 Amazon EC2 인스턴스로의 트래픽, 컨테이너 또는 기타 향후 서비스와 같은 기타 영역VPC과 같은 데이터 또는 네트워크 관련 활동이 포함됩니다. 인프라 도메인 이벤트에 대한 응답에는 포렌식 분석을 위해 인시던트 관련 데이터를 획득하는 것이 포함되는 경우가 많습니다. 여기에는 인스턴스의 운영 체제와의 상호 작용이 포함될 수 있으며, 다양한 경우에 메커니즘이 포함될 AWS API 수도 있습니다. 인프라 도메인에서는 포렌식 분석 및 조사 수행 전용 Amazon EC2 인스턴스와 같은 게스트 운영 체제 내에서 및 디지털 포렌식/인시던트 응답(DFIR) 도구의 AWS APIs 조합을 사용할 수 있습니다. 인프라 도메인 인시던트에는 네트워크 패킷 캡처, Amazon Elastic Block Store(Amazon) 볼륨의 디스크 블록 또는 인스턴스에서 획득한 휘발성 메모리 분석이 포함될 수 있습니다. EBS
- 애플리케이션 도메인 - 애플리케이션 도메인의 인시던트는 애플리케이션 코드 또는 서비스 또는 인프라에 배포된 소프트웨어에서 발생합니다. 이 도메인은 클라우드 위협 탐지 및 대응 플레이북에 포함되어야 하며 인프라 도메인의 응답과 유사한 응답을 통합할 수 있습니다. 적절하고 사려 깊은 애플리케이션 아키텍처를 사용하면 자동화된 획득, 복구 및 배포를 사용하여 클라우드 도구를 사용하여 이 도메인을 관리할 수 있습니다.

이러한 도메인에서는 AWS 계정, 리소스 또는 데이터에 대해 조치를 취할 수 있는 공격자를 고려합니다. 내부 또는 외부에서 위험 프레임워크를 사용하여 조직에 대한 특정 위험을 결정하고 그에 따라 준비합니다. 또한 인시던트 대응 계획 및 사려 깊은 아키텍처 구축에 도움이 될 수 있는 위협 모델을 개발해야 합니다.

에서 인시던트 대응의 주요 차이점 AWS

인시던트 대응은 온프레미스 또는 클라우드에서 사이버 보안 전략의 중요한 부분입니다. 최소 권한 및 심층 방어와 같은 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 지원하는 여러 인시던트 대응 패턴이 적합합니다. 차이점은 고객이 클라우드에서 이러한 패턴을 설계하고 엔지니어링하기 시작할 때 시작됩니다. 다음은 인시던트 대응의 주요 차이점입니다 AWS.

차이 #1: 공동 책임으로서의 보안

보안 및 규정 준수에 대한 책임은 AWS 와 고객 간에 공유됩니다. 이 공동 책임 모델은 호스트 운영 체제 및 가상화 계층에서 서비스가 운영되는 시설의 물리적 보안까지 구성 요소를 AWS 운영, 관리 및 제어하기 때문에 고객의 운영 부담을 일부 덜어 줍니다. 공동 책임 모델에 대한 자세한 내용은 공동 책임 모델 설명서를 참조하세요.

클라우드에서 공동 책임이 변경되면 인시던트 대응 옵션도 변경됩니다. 이러한 장단점을 계획하고 이해하며 거버넌스 요구 사항에 맞추는 것은 인시던트 대응의 중요한 단계입니다.

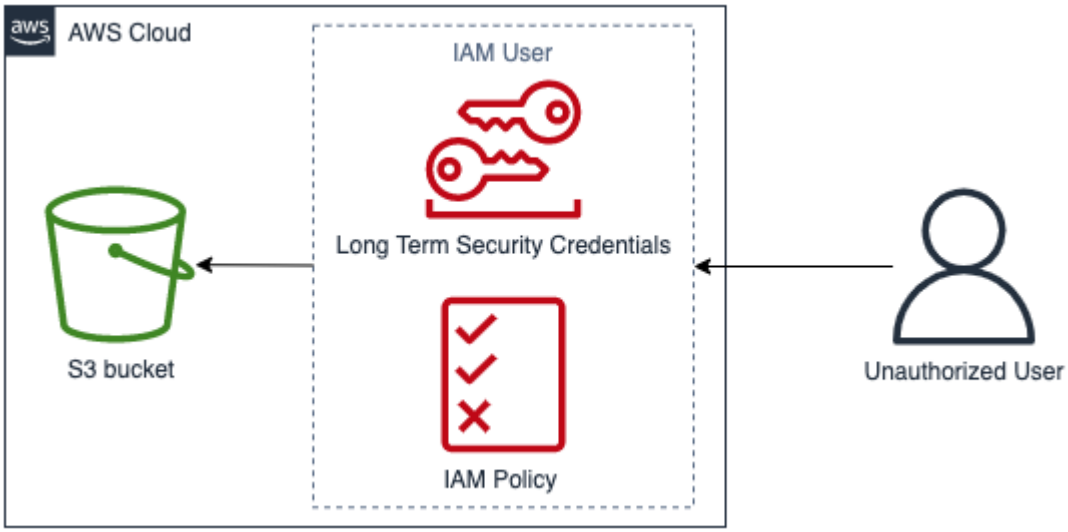
와의 직접적인 관계 외에도 특정 책임 모델에 책임이 있는 다른 엔터티가 AWS있을 수 있습니다. 예를 들어 운영의 일부 측면을 책임지는 내부 조직 단위가 있을 수 있습니다. 또한 일부 클라우드 기술을 개발, 관리 또는 운영하는 다른 당사자와 관계를 맺고 있을 수 있습니다.

운영 모델과 일치하는 적절한 인시던트 대응 계획과 적절한 플레이북을 생성하고 테스트하는 것이 매우 중요합니다.

차이 #2: 클라우드 서비스 도메인

클라우드 서비스에 존재하는 보안 책임의 차이로 인해 보안 인시던트에 대한 새 도메인인 서비스 도메인이 도입되었습니다.이 도메인은 인시던트 도메인 섹션 앞부분에서 설명되었습니다. 서비스 도메인에는 고객의 AWS 계정, IAM 권한, 리소스 메타데이터, 결제 및 기타 영역이 포함됩니다. 이 도메인은 대응 방식 때문에 인시던트 대응에 대해 다릅니다. 서비스 도메인 내의 응답은 일반적으로 기존 호스트 기반 및 네트워크 기반 응답이 아닌 API 호출을 검토하고 실행하여 수행됩니다. 서비스 도메인에서는 영향을 받는 리소스의 운영 체제와 상호 작용하지 않습니다.

다음 다이어그램은 아키텍처 패턴 방지를 기반으로 하는 서비스 도메인의 보안 이벤트 예를 보여줍니다. 이 경우 권한이 없는 사용자는 IAM 사용자의 장기 보안 자격 증명을 획득합니다. IAM 사용자에게는 Amazon Simple Storage Service(Amazon S3) 버킷에서 객체를 검색할 수 있도록 허용하는 IAM 정책이 있습니다. 이 보안 이벤트에 응답하려면 AWS APIs를 사용하여 AWS CloudTrail 및 Amazon S3 액세스 AWS 로그와 같은 로그를 분석합니다. 또한를 사용하여 AWS APIs 인시던트를 억제하고 복구합니다.



서비스 도메인 예제

차이 #3: 인프라 APIs 프로비저닝

또 다른 차이점은 온디맨드 셀프 서비스의 클라우드 특성입니다. 주요 시설 고객은 전 세계 여러 지리적 위치에서 사용할 수 있는 퍼블릭 및 프라이빗 엔드포인트RESTfulAPI를 통해를 AWS 클라우드 사용하여와 상호 작용합니다. 고객은 AWS 자격 증명을 APIs 사용하여 이러한 정보에 액세스할 수 있습니다. 온프레미스 액세스 제어와 달리 이러한 자격 증명이 반드시 네트워크 또는 Microsoft Active Directory 도메인에 의해 바인딩되는 것은 아닙니다. 자격 증명은 대신 AWS 계정 내부의 IAM 보안 주체와 연결됩니다. 이러한 API 엔드포인트는 기업 네트워크 외부에서 액세스할 수 있으므로, 보안 인증 정보가 예상 네트워크 또는 지리적 위치 외부에서 사용되는 인시던트에 대응할 때 이를 이해하는 것이 중요합니다.

의 API기반 특성으로 인해 보안 이벤트에 응답하기 위한 AWS중요한 로그 소스는 AWS 계정에서 수행된 관리 API 호출을 AWS CloudTrail추적하고 API 호출의 소스 위치에 대한 정보를 찾을 수 있는 위치입니다.

차이 #4: 클라우드의 동적 특성

클라우드는 동적이므로 리소스를 빠르게 생성하고 삭제할 수 있습니다. 자동 조정을 사용하면 트래픽 증가에 따라 리소스를 분산하고 분산할 수 있습니다. 수명이 짧은 인프라와 빠른 변경 사항으로 인해 조사 중인 리소스가 더 이상 존재하지 않거나 수정되었을 수 있습니다. AWS 리소스의 일시적 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 호출을 통해 수집됩니다. 이 교대 근무를 준비APIs하려면에서 데이터 수집을 수행하는 방법을 연습하고 이해해야 하며, 효과적인 수집 및 액세스를 위한 적절한 스토리지를 확인해야 합니다.

차이 #6: 자동화의 중요성

고객이 클라우드 채택의 이점을 완전히 실현하려면 운영 전략이 자동화를 수용해야 합니다. 코드형 인프라(IaC)는 AWS CloudFormation 또는 타사 솔루션과 같은 네이티브 IaC 서비스가 지원하는 코드를 사용하여 AWS 서비스가 배포, 구성, 재구성 및 파괴되는 매우 효율적인 자동화 환경의 패턴입니다. 이렇게 하면 인시던트 대응이 고도로 자동화되도록 구현됩니다. 특히 증거를 처리할 때 인적 실수를 방지하는 것이 좋습니다. 자동화는 온프레미스에서 사용되지만 에서는 더 간단하고 필수적입니다 AWS 클라우드.

이러한 차이점 해결

이러한 차이를 해결하려면 다음 섹션에 설명된 단계에 따라 사람, 프로세스 및 기술 전반에 걸쳐 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 대한 프로세스를 준비하려면 아키텍처 문서화, 철저한 인시던트 대응 계획 개발, 보안 이벤트에 대한 일관된 대응을 위한 플레이북 생성이 필요합니다.
- 기술 - 보안 인시던트에 대비하려면 액세스 설정, 필요한 로그 집계 및 모니터링, 효과적인 알림 메커니즘 구현, 대응 및 조사 기능 개발이 필요합니다.

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 응답하려면 보안 이벤트에 대한 응답을 지원할 이해관계자를 식별해야 합니다. 또한 효과적인 대응을 통해 AWS 기술 및 AWS 환경에 대한 교육을 받는 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 지역에서 해야 할 일과 해서는 안 되는 일을 규제하는 현지 법률이 있습니다. 보안 대응 계획에 대한 책임 있고, 책임감 있고, 컨설팅되고, 정보에 입각한 (RACI) 차트를 구축하는 것이 관료적인 것처럼 보일 수 있지만, 이를 통해 빠르고 직접적인 커뮤니케이션이 가능하며 이벤트의 다양한 단계에서 리더십을 명확하게 설명할 수 있습니다.

영향을 받는 애플리케이션 및 리소스의 소유자/개발자를 포함한 인시던트 중에는 영향을 측정하는 데 도움이 되는 정보와 컨텍스트를 제공할 수 있는 주제 전문가(SMEs)이기 때문에 이러한 내용이 중요합니다. 개발자 및 애플리케이션 소유자의 인시던트 대응 전문 지식에 의존하기 전에 이들과 함께 연습하고 관계를 구축해야 합니다. 클라우드 관리자 또는 엔지니어와 SMEs같은 애플리케이션 소유자 또는는 환경이 익숙하지 않거나 복잡하거나 대응 담당자가 액세스할 수 없는 상황에서 조치를 취해야 할 수 있습니다.

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

인시던트 대응 직원 교육

조직이 사용하는 기술에 대해 인시던트 대응 직원을 교육하는 것은 보안 이벤트에 적절하게 대응하는 데 매우 중요합니다. 직원이 기본 기술을 이해하지 못하면 응답이 연장될 수 있습니다. 기존 인시던트 대응 개념 외에도 AWS 서비스와 AWS 환경을 이해하는 것도 중요합니다. 온라인 훈련 및 강의실 훈련과 같이 인시던트 직원을 훈련시키는 여러 가지 기존 메커니즘이 있습니다. 또한 게임데이 또는 시뮬레이션 실행을 훈련 메커니즘으로 고려해야 합니다. 시뮬레이션을 실행하는 방법에 대한 자세한 내용은 이 문서의 the section called “정기적인 시뮬레이션 실행” 섹션을 참조하세요.

AWS 클라우드 기술 이해

종속성을 줄이고 응답 시간을 줄이려면 보안 팀과 대응 담당자가 클라우드 서비스에 대한 교육을 받고 조직에서 사용하는 특정 클라우드 환경에서 실습을 할 기회를 가져야 합니다. 인시던트 대응 담당자가 효과를 발휘하려면 AWS 파운데이션, IAM, AWS Organizations, AWS 로깅 및 모니터링 서비스, AWS 보안 서비스를 이해하는 것이 중요합니다.

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

AWS 환경 이해

AWS 서비스, 사용 사례 및 서로 통합하는 방법을 이해하는 것 외에도 조직의 AWS 환경이 실제로 어떻게 설계되고 어떤 운영 프로세스가 마련되어 있는지 이해하는 것도 마찬가지로 중요합니다. 이러한 내부 지식은 문서화되지 않고 소수의 도메인 전문가만 이해하며, 이는 종속성을 생성하고 혁신을 방해하며 응답 시간을 늦출 수 있습니다.

이러한 종속성을 방지하고 응답 시간을 단축하려면 보안 분석가가 AWS 환경에 대한 내부 지식을 문서화하고, 액세스하고, 이해해야 합니다. 전체 클라우드 공간을 이해하려면 관련 보안 이해관계자와 클라우드 관리자 간의 협업이 필요합니다. 인시던트 대응을 위한 프로세스 준비의 일부로이 백서의 the section called “아키텍처 다이어그램 문서화 및 중앙 집중화”뒷부분에 있는 아키텍처 다이어그램을 문서화하고 중앙 집중화하는 것이 포함됩니다. 하지만 사람의 관점에서는 분석가가 AWS 환경과 관련된 다이어그램 및 운영 프로세스에 액세스하고 이를 이해할 수 있어야 합니다.

AWS 대응 팀 및 지원 이해

Support

Support는 AWS 솔루션의 성공 및 운영 상태를 지원하는 도구와 전문 지식에 대한 액세스를 제공하는 다양한 계획을 제공합니다. AWS 환경을 계획, 배포 및 최적화하는 데 도움이 되는 기술 지원과 더 많은 리소스가 필요한 경우 AWS 사용 사례에 가장 적합한 지원 계획을 선택할 수 있습니다.

AWS 리소스에 영향을 미치는 문제에 대한 지원을 받으려면의 지원 센터 AWS Management Console (로그인 필요)를 중앙 연락 창구로 간주합니다. 에 대한 액세스 Support 는에 의해 제어됩니다IAM. AWS 지원 기능에 액세스하는 방법에 대한 자세한 내용은 시작하기를 참조하세요 Support.

또한 남용을 보고해야 하는 경우 AWS Tust and Safety 팀에 문의하십시오.

AWS 고객 인시던트 대응 팀(CIRT)

AWS 고객 인시던트 대응 팀(CIRT)은 AWS 공동 책임 모델의 고객 측에서 활성 보안 이벤트 중에 고객에게 지원을 제공하는 전문적이고 항상 사용 가능한 글로벌 AWS 팀입니다.

에서 AWS CIRT 사용자를 지원하면의 활성 보안 이벤트에 대한 분류 및 복구에 대한 지원을 받게 됩니다 AWS. 서비스 AWS 로그를 사용하여 근본 원인 분석을 지원하고 복구를 위한 권장 사항을 제공합니다. 또한 향후 보안 이벤트를 방지하는 데 도움이 되는 보안 권장 사항 및 모범 사례를 제공합니다.

AWS 고객은 AWS 지원 사례를 통해를 AWS CIRT 사용할 수 있습니다.

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

- 개발자 Support 플랜이 있는 고객:
  1. 계정 및 청구(Account and billing)
  2. 서비스: 계정
  3. 범주: 보안
  4. 심각도: 중요 질문

- 비즈니스 Support 플랜을 보유한 고객:
  1. 계정 및 청구(Account and billing)
  2. 서비스: 계정
  3. 범주: 보안
  4. 심각도: 긴급한 비즈니스 영향 질문

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

- AWS 보안 인시던트 대응 구독이 있는 고객:에서 보안 인시던트 대응 콘솔을 엽니다. https://console.aws.amazon.com/security-ir/

DDoS 응답 지원

AWS 는에서 실행되는 웹 애플리케이션을 보호하는 관리형 분산 서비스 거부(DDoS) 보호 서비스를 AWS Shield제공하는를 제공합니다 AWS.는 애플리케이션 가동 중지 시간 및 지연 시간을 최소화할 수 있는 상시 감지 및 자동 인라인 완화 기능을 AWS Shield 제공하므로 DDoS 보호의 이점을 활용 Support 하기 위해 참여할 필요가 없습니다. Shield Standard와 AWS Shield Shield Advanced의 두 가지 계층이 있습니다. 이 두 계층 간의 차이점에 대해 알아보려면 Shield 기능 설명서를 참조하세요.

AWS Managed Services (AMS)

AWS Managed Services (AMS)는 인프라에 대한 지속적인 관리를 제공하므로 애플리케이션에 집중할 AWS 수 있습니다. 인프라를 유지하기 위한 모범 사례를 구현하면는 운영 오버헤드와 위험을 줄이는 데 AMS 도움이 됩니다.는 변경 요청, 모니터링, 패치 관리, 보안 및 백업 서비스와 같은 일반적인 활동을 AMS 자동화하고 인프라를 프로비저닝, 실행 및 지원할 전체 수명 주기 서비스를 제공합니다.

AMS는 보안 탐지 제어 제품군을 배포할 책임이 있으며 매일 알림에 대한 첫 번째 대응을 제공합니다. 알림이 시작되면는 표준 자동 및 수동 플레이북 세트를 AMS 따라 일관된 응답을 확인합니다. 이러한 플레이북은 온보딩 중에 AMS 고객과 공유되므로 고객이와 함께 응답을 개발하고 조정할 수 있습니다 AMS.

프로세스

철저하고 명확하게 정의된 인시던트 대응 프로세스를 개발하는 것은 성공적이고 확장 가능한 인시던트 대응 프로그램의 핵심입니다. 보안 이벤트가 발생하면 명확한 단계와 워크플로를 통해 적시에 대응할 수 있습니다. 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 개발할 첫 번째 문서는 인시던트 대응 계획입니다. 인시던트 대응 계획은 인시던트 대응 프로그램 및 전략의 기초가 되도록 설계되었습니다. 인시던트 대응 계획은 일반적으로 다음 섹션을 포함하는 상위 수준 문서입니다.

- 인시던트 대응 팀 개요 - 인시던트 대응 팀의 목표와 기능을 간략하게 설명합니다.
- 역할 및 책임 - 인시던트 대응 이해관계자를 나열하고 인시던트 발생 시 해당 역할을 자세히 설명합니다.

- 커뮤니케이션 계획 - 연락처 정보와 인시던트 발생 시 커뮤니케이션 방법을 자세히 설명합니다.

  인시던트 통신을 위한 백업으로 통신을 사용하는 out-of-band 것이 가장 좋습니다. 보안 out-of-band 통신 채널을 제공하는 애플리케이션의 예는 AWS Wickr입니다.
- 인시던트 대응 단계 및 취해야 할 조치 - 인시던트 대응 단계, 예를 들어 감지, 분석, 근절, 억제 및 복구 단계를 열거합니다. 여기에는 해당 단계 내에서 취해야 할 상위 수준 조치가 포함됩니다.
- 인시던트 심각도 및 우선 순위 정의 - 인시던트의 심각도를 분류하는 방법, 인시던트의 우선 순위 지정 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 구축해야 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 패턴을 설계하는 애플리케이션 간의 일관성을 확인하는 데도 중요합니다. 또한이 설명서가 최신 상태이고 새로운 아키텍처 패턴에 따라 정기적으로 업데이트되는지 확인해야 합니다. 다음과 같은 항목을 자세히 설명하는 설명서 및 내부 리포지토리를 개발해야 합니다.

- AWS 계정 구조 - 다음을 알아야 합니다.
  - AWS 계정이 몇 개 있습니까?
  - 이러한 AWS 계정은 어떻게 구성되나요?
  - AWS 계정의 사업자는 누구입니까?
  - 서비스 제어 정책(SCPs)을 사용하나요? 그렇다면를 사용하여 구현되는 조직 가드레일은 무엇입니까SCPs?
  - 사용할 수 있는 리전과 서비스를 제한합니까?
  - 사업부와 환경(dev/test/prod) 간에는 어떤 차이가 있나요?
- AWS 서비스 패턴
  - 어떤 AWS 서비스를 사용하십니까?
  - 가장 널리 사용되는 AWS 서비스는 무엇입니까?
- 아키텍처 패턴
  - 어떤 클라우드 아키텍처를 사용하십니까?
- AWS 인증 패턴
  - 개발자는 일반적으로에 어떻게 인증하나요 AWS?

  - IAM 역할 또는 사용자(또는 둘 다)를 사용하나요? 에 대한 인증이 자격 증명 공급자(IdP)에 AWS 연결되어 있습니까?
  - IAM 역할 또는 사용자를 직원 또는 시스템에 매핑하려면 어떻게 해야 합니까?
  - 누군가 더 이상 권한이 없으면 액세스가 어떻게 취소되나요?
- AWS 권한 부여 패턴
  - 개발자는 어떤 IAM 정책을 사용하나요?
  - 리소스 기반 정책을 사용하나요?
- 로깅 및 모니터링
  - 어떤 로깅 소스를 사용하며 어디에 저장되나요?
  - AWS CloudTrail 로그를 집계합니까? 그렇다면 어디에 저장되나요?
  - CloudTrail 로그를 쿼리하려면 어떻게 해야 합니까?
  - Amazon을 GuardDuty 활성화했습니까?
  - GuardDuty 조사 결과(예: 콘솔, 티켓팅 시스템, SIEM)에 액세스하려면 어떻게 해야 합니까?
  - 조사 결과 또는 이벤트가에 집계됩니까SIEM?
  - 티켓이 자동으로 생성되나요?
  - 조사를 위해 로그를 분석하기 위해 어떤 도구가 마련되어 있습니까?
- 네트워크 토폴로지
  - 네트워크의 디바이스, 엔드포인트 및 연결은 물리적 또는 논리적으로 어떻게 배열되나요?
  - 네트워크는와 어떻게 연결되나요 AWS?
  - 환경 간에 네트워크 트래픽은 어떻게 필터링되나요?
- 외부 인프라
  - 외부용 애플리케이션은 어떻게 배포되나요?
  - 공개적으로 액세스할 수 있는 AWS 리소스는 무엇입니까?
  - 외부에서 직면한 인프라가 포함된 AWS 계정은 무엇입니까?
  - 무엇 DDoS 또는 외부 필터링이 있나요?

내부 기술 다이어그램 및 프로세스를 문서화하면 인시던트 대응 분석가의 작업이 쉬워지므로 보안 이벤트에 대응할 수 있는 제도적 지식을 신속하게 얻을 수 있습니다. 내부 기술 프로세스의 철저한 문서화는 보안 조사를 간소화할 뿐만 아니라 프로세스의 합리화 및 평가에 맞게 조정합니다.

인시던트 대응 플레이북 개발

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.

에 대한 플레이북을 생성하는 방법

다음과 같은 인시던트 시나리오에 대한 플레이북을 만들어야 합니다.

- 예상 인시던트 - 예상 인시던트에 대해 플레이북을 생성해야 합니다. 여기에는 서비스 거부(DoS), 랜섬웨어, 자격 증명 유출과 같은 위협이 포함됩니다.
- 알려진 보안 조사 결과 또는 알림 - 조사 결과와 같은 알려진 보안 GuardDuty 조사 결과 및 알림에 대해 플레이북을 생성해야 합니다. GuardDuty 조사 결과를 받아서 “이제 무엇을?”라고 생각할 수 있습니다. GuardDuty 결과를 잘못 처리하거나 무시하지 않으려면 각 잠재적 GuardDuty 결과에 대한 플레이북을 생성합니다. 일부 수정 세부 정보 및 지침은 GuardDuty 설명서에서 확인할 수 있습니다. 기본적으로 GuardDuty 가 활성화되어 있지 않고 비용이 발생한다는 점에 유의해야 합니다. 에 대한 자세한 내용은 부록 A: 클라우드 기능 정의 -에서 확인할 GuardDuty 수 있습니다the section called “가시성 및 알림”.

플레이북에 포함할 내용

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

플레이북에 포함할 항목은 다음과 같습니다.

- 플레이북 개요 -이 플레이북이 다루는 위험 또는 인시던트 시나리오는 무엇입니까? 플레이북의 목표는 무엇인가요?
- 사전 조건 -이 인시던트 시나리오에 필요한 로그 및 탐지 메커니즘은 무엇입니까? 예상되는 알림은 무엇인가요?
- 이해관계자 정보 - 관련된 사람은 누구이며 연락처 정보는 무엇입니까? 관련된 각 이해관계자의 책임은 무엇인가요?
- 대응 단계 - 인시던트 대응 단계에서 어떤 전술적 단계를 수행해야 합니까? 분석가는 어떤 쿼리를 실행해야 하나요? 원하는 결과를 얻으려면 어떤 코드를 실행해야 하나요?
  - 감지 - 인시던트는 어떻게 감지되나요?
  - 분석 - 영향 범위는 어떻게 결정되나요?
  - 포함 - 범위를 제한하기 위해 인시던트를 격리하려면 어떻게 해야 합니까?

  - 제거 - 위협이 환경에서 어떻게 제거되나요?
  - 복구 - 영향을 받는 시스템 또는 리소스가 어떻게 프로덕션 환경으로 복귀합니까?
- 예상 결과 - 쿼리 및 코드를 실행한 후 플레이북의 예상 결과는 무엇입니까?

각 플레이북에서 일관된 정보를 확인하려면 다른 보안 플레이북에서 사용할 플레이북 템플릿을 생성하는 것이 도움이 될 수 있습니다. 이해관계자 정보와 같이 이전에 나열된 항목 중 일부는 여러 플레이북에서 공유할 수 있습니다. 이 경우 해당 정보에 대한 중앙 집중식 설명서를 생성하고 플레이북에서 참조한 다음 플레이북의 명시적 차이를 열거할 수 있습니다. 이렇게 하면 모든 개별 플레이북에서 동일한 정보를 업데이트할 필요가 없습니다. 템플릿을 생성하고 플레이북에서 공통 또는 공유 정보를 식별하면 플레이북 개발을 간소화하고 속도를 높일 수 있습니다. 마지막으로 플레이북은 시간이 지남에 따라 발전할 수 있습니다. 단계가 일관된지 확인하면 자동화 요구 사항이 됩니다.

샘플 플레이북

여러 샘플 플레이북은의 부록 B에서 찾을 수 있습니다the section called “플레이북 리소스”. 이 예제는 생성할 플레이북과 플레이북에 포함할 플레이북을 안내하는 데 사용할 수 있습니다. 그러나 비즈니스와 가장 관련된 위험을 통합하는 플레이북을 만드는 것이 중요합니다. 플레이북 내의 단계와 워크플로에 기술과 프로세스가 포함되어 있는지 확인해야 합니다.

정기적인 시뮬레이션 실행

조직은 위협 환경과 마찬가지로 시간이 지남에 따라 성장하고 발전합니다. 따라서 인시던트 대응 기능을 지속적으로 검토하는 것이 중요합니다. 시뮬레이션은이 평가를 수행하는 데 사용할 수 있는 한 가지 방법입니다. 시뮬레이션은 위협 행위자의 전술, 기법 및 절차(TTPs)를 모방하도록 설계된 실제 보안 이벤트 시나리오를 사용하며, 조직이 이러한 모의 사이버 이벤트가 실제로 발생할 수 있는 상황에 대응하여 인시던트 대응 기능을 연습하고 평가할 수 있도록 합니다.

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.

- 모의 연습 - 시뮬레이션에 대한 모의 연습 접근 방식은 역할 및 책임을 연습하고 확립된 커뮤니케이션 도구와 플레이북을 사용하기 위해 다양한 인시던트 대응 이해관계자가 참여하는 토론 기반 세션입니다. 연습 촉진은 일반적으로 가상 장소, 물리적 장소 또는 이들의 조합에서 하루 종일 수행할 수 있습니다. 토론 기반 특성으로 인해 모의 연습은 프로세스, 사람 및 협업에 중점을 둡니다. 기술은 토론의 중요한 부분이지만 인시던트 대응 도구 또는 스크립트의 실제 사용은 일반적으로 모의 연습의 일부가 아닙니다.
- 퍼플 팀 연습 - 퍼플 팀 연습은 인시던트 대응 담당자(블루 팀)와 시뮬레이션된 위협 공격자(레드 팀) 간의 협업 수준을 높입니다. 블루팀은 일반적으로 보안 운영 센터(SOC)의 구성원으로 구성되지만 실제 사이버 이벤트 중에 관여할 다른 이해관계자도 포함할 수 있습니다. Red Team은 일반적으로 공격적인 보안에 대한 교육을 받은 침투 테스트 팀 또는 주요 이해관계자로 구성됩니다. Red Team은 시나리오를 설계할 때 연습 진행자와 협력하여 시나리오가 정확하고 실행 가능하도록 합니다. 퍼플 팀 연습 중에 주요 초점은 인시던트 대응 노력을 지원하는 탐지 메커니즘, 도구 및 표준 운영 절차(SOPs)입니다.
- Red Team 연습 - Red Team 연습 중에 위반(Red Team)은 시뮬레이션을 수행하여 미리 결정된 범위에서 특정 목표 또는 일련의 목표를 달성합니다. 방어자(블루 팀)는 연습의 범위와 기간을 반드시 알 필요는 없으며, 실제 인시던트에 대응하는 방법에 대한 보다 현실적인 평가를 제공합니다. Red Team 연습은 침습 테스트일 수 있으므로 주의해야 하며, 연습이 환경에 실제 피해를 주지 않는지 확인하기 위한 제어를 구현해야 합니다.

> **Note**
>
> AWS 는 고객이 퍼플 팀 또는 레드 팀 연습을 수행하기 전에 침투 테스트 웹 사이트에서 사용할 수 있는 침투 테스트 정책을 검토하도록 요구합니다.

표 1에는 이러한 시뮬레이션 유형의 몇 가지 주요 차이점이 요약되어 있습니다. 정의는 일반적으로 느슨한 정의로 간주되며 조직의 요구 사항에 맞게 사용자 지정할 수 있습니다.

표 1 - 시뮬레이션 유형

	테이블탑 연습	퍼플 팀 연습	Red Team 연습
요약	특정 보안 인시던트 시나리오 하나에 초점을 맞춘 종이 기반 연습입니다. 이는 상위 수준 또는 기술적일 수 있으	테이블탑 연습에 비해 더 사실적인 제안입니다. 퍼플 팀 연습 중에 진행자는 참가자와 협력하여 연습 참여를 높	일반적으로 고급 시뮬레이션 제안입니다. 일반적으로 참가자가 연습의 모든 세부 정보를 알지 못할 수 있는 높

	테이블탑 연습	퍼플 팀 연습	Red Team 연습
	며 일련의 종이 주입으로 구동됩니다.	이고 필요한 경우 훈련을 제공합니다.	은 수준의 기밀성이 있습니다.
필요한 리소스	제한된 기술 리소스 필요	다양한 이해관계자가 필요하고 높은 수준의 기술 리소스가 필요함	다양한 이해관계자가 필요하고 높은 수준의 기술 리소스가 필요함
복잡성	낮음	중간	높음

정기적으로 사이버 시뮬레이션을 진행하는 것이 좋습니다. 각 연습 유형은 참가자와 조직 전체에 고유한 이점을 제공할 수 있으므로 덜 복잡한 시뮬레이션 유형(예: 테이블탑 연습)으로 시작하고 더 복잡한 시뮬레이션 유형(레드 팀 연습)으로 진행하도록 선택할 수 있습니다. 보안 성숙도, 리소스, 원하는 성과에 따라 시뮬레이션 유형을 선택해야 합니다. 일부 고객은 복잡성과 비용으로 인해 Red Team 연습을 수행하지 않을 수 있습니다.

연습 수명 주기

선택한 시뮬레이션 유형에 관계없이 시뮬레이션은 일반적으로 다음 단계를 따릅니다.

1. 핵심 연습 요소 정의 - 시뮬레이션 시나리오와 시뮬레이션의 목표를 정의합니다. 이 두 가지 모두 리더의 승인을 받아야 합니다.
2. 주요 이해관계자 식별 - 최소한 연습에는 연습 진행자와 참가자가 필요합니다. 시나리오에 따라 법무, 커뮤니케이션 또는 경영진과 같은 추가 이해관계자가 참여할 수 있습니다.
3. 시나리오 빌드 및 테스트 - 특정 요소가 실행 가능하지 않은 경우 시나리오가 빌드 중이므로 시나리오를 다시 정의해야 할 수 있습니다. 이 단계의 결과로 최종 시나리오가 도출될 것으로 예상됩니다.
4. 시뮬레이션 촉진 - 시뮬레이션 유형에 따라 사용되는 촉진이 결정됩니다(고도의 기술적 시뮬레이션 시나리오와 비교하여 종이 기반 시나리오). 진행자는 연습 목표에 맞게 촉진 전략을 조정해야 하며 가능한 한 모든 연습 참가자를 참여시켜 최대한의 이점을 확보해야 합니다.
5. 사후 보고서 개발(AAR) - 잘 진행된 영역, 개선 사항을 사용할 수 있는 영역 및 잠재적 격차를 식별합니다. 는 시뮬레이션의 효과와 시뮬레이션된 이벤트에 대한 팀의 응답을 측정하여 향후 시뮬레이션을 통해 시간 경과에 따라 진행 상황을 추적할 수 있도록 AAR해야 합니다.

기술

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

AWS 계정 구조 개발

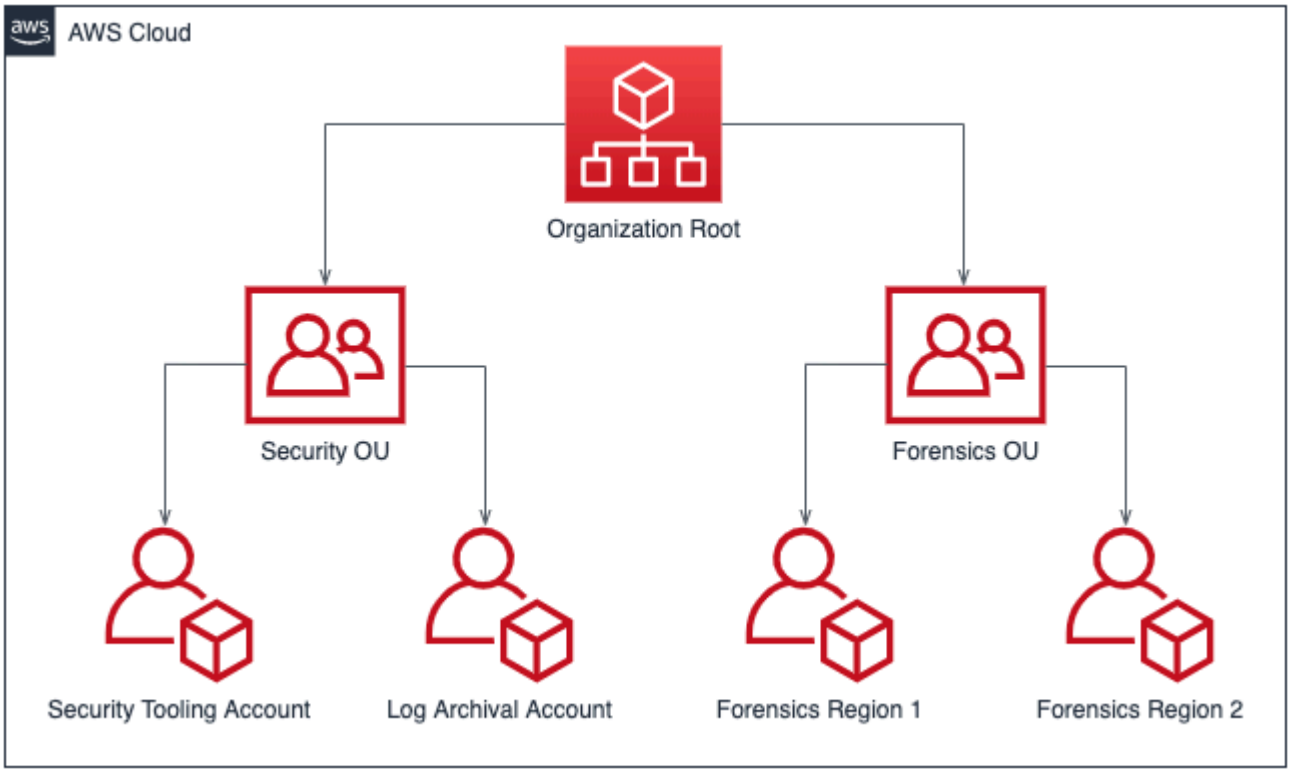
AWS Organizations는 AWS 리소스를 성장 및 확장할 때 AWS 환경을 중앙에서 관리하고 관리하는 데 도움이 됩니다. AWS 조직은 AWS 계정을 단일 단위로 관리할 수 있도록 계정을 통합합니다. 조직 단위(OUs)를 사용하여 계정을 그룹화하여를 단일 단위로 관리할 수 있습니다.

인시던트 대응의 경우 보안 OU 및 포렌식 OU를 포함하는 인시던트 대응의 기능을 지원하는 AWS 계정 구조를 갖는 것이 유용합니다. 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) 및 미국 서부(오레곤)(us-west-2)에서만 운영하는 경우 포렌식 OU에 us-east-1용 계정과 us-west-2용 계정 두 개가 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

비즈니스 사용 사례 및 AWS 리소스를 둘러싼 관련 내부 이해관계자에 대한 컨텍스트 정보를 얻는 것은 어려울 수 있습니다. 이를 위한 한 가지 방법은 AWS 리소스에 메타데이터를 할당하고 사용자 정의 키와 값으로 구성된 태그의 형태입니다. 태그를 생성하여 리소스를 목적, 소유자, 환경, 처리되는 데이터 유형 및 기타 원하는 기준에 따라 분류할 수 있습니다.

일관된 태그 지정 전략을 사용하면 AWS 리소스에 대한 컨텍스트 정보를 빠르게 식별하고 식별할 수 있으므로 응답 시간을 단축할 수 있습니다. 태그는 응답 자동화를 시작하는 메커니즘으로도 사용할 수 있습니다. 태그를 지정할 항목에 대한 자세한 내용은 AWS 리소스 태그 지정에 대한 설명서를 참조하세요. 먼저 조직 전체에 구현할 태그를 정의하는 것이 좋습니다. 그런 다음 이 태그 지정 전략을 구현하고 적용합니다. 구현 및 적용에 대한 자세한 내용은 AWS 블로그 AWS Tag Policies and Service Control Policies(SCPs)를 사용하여 AWS 리소스 태그 지정 전략 구현에서 확인할 수 있습니다.

AWS 계정 연락처 정보 업데이트

각 AWS 계정에 대해 정확한 연락처 정보를 확보하여 올바른 이해관계자가 보안, 결제 및 운영과 up-to-date 같은 주제에 AWS 대한 중요한 알림을 받을 수 있도록 하는 것이 중요합니다. 각 AWS 계정에

는 보안, 결제 및 작업을 위한 기본 연락처와 대체 연락처가 있습니다. 이러한 고객 응대의 차이점은 AWS 계정 관리 참조 가이드에서 확인할 수 있습니다.

대체 연락처 관리에 대한 자세한 내용은 AWS 대체 연락처 추가, 변경 또는 제거 설명서를 참조하세요. 팀이 결제, 운영 및 보안 관련 문제를 관리하는 경우 이메일 배포 목록을 사용하는 것이 가장 좋습니다. 이메일 배포 목록은 한 사람에 대한 종속성을 제거하므로 사무실 외부에 있거나 회사를 떠날 경우 차단이 발생할 수 있습니다. 또한 전화번호를 포함한 이메일 및 계정 연락처 정보가 루트 계정 암호 재설정 및 멀티 팩터 인증(MFA) 재설정으로부터 잘 보호되는지 확인해야 합니다.

를 사용하는 고객의 경우 AWS Organizations조직 관리자는 각 계정에 대한 자격 증명을 요구하지 않고 관리 계정 또는 위임된 관리자 계정을 사용하여 멤버 계정의 대체 연락처를 중앙에서 관리할 수 AWS 있습니다. 또한 새로 생성된 계정에 정확한 연락처 정보가 있는지 확인해야 합니다. 새로 생성된 AWS 계정 블로그 게시물은 대체 연락처 자동 업데이트를 참조하세요.

에 대한 액세스 준비 AWS 계정

인시던트 중에 인시던트 대응 팀은 인시던트와 관련된 환경 및 리소스에 액세스할 수 있어야 합니다. 이벤트가 발생하기 전에 팀이 자신의 임무를 수행할 수 있는 적절한 액세스 권한을 가지고 있는지 확인합니다. 이렇게 하려면 팀원에게 필요한 액세스 수준(예: 팀원이 수행할 가능성이 높은 작업의 종류)을 알고 최소 권한 액세스를 미리 프로비저닝해야 합니다.

이 액세스를 구현하고 프로비저닝하려면 조직의 클라우드 아키텍트와 계정 전략 및 클라우드 자격 증명 전략을 식별하고 논의 AWS 하여 어떤 인증 및 권한 부여 방법이 구성되어 있는지 이해해야 합니다. 이러한 자격 증명의 권한 있는 특성으로 인해 구현의 일부로 승인 흐름을 사용하거나 볼트 또는 안전에서 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 사용은 제한, 모니터링 및 일상 활동에 사용되지 않아야 합니다.

위협 환경 이해

위협 모델 개발

조직은 위협 모델을 개발하여 권한이 없는 사용자가 할 수 있기 전에 위협 및 완화 조치를 식별할 수 있습니다. 위협 모델링에는 여러 전략과 접근 방식이 있습니다. 위협 모델링에 접근하는 방법 블로그 게시물을 참조하세요. 인시던트 대응의 경우 위협 모델은 공격자가 인시던트 중에 사용했을 수 있는 공격 벡터를 식별하는 데 도움이 될 수 있습니다. 적시에 대응하려면 방어 대상을 이해하는 것이 중요합

니다. 위협 모델링 AWS Partner 에를 사용할 수도 있습니다. 파트너를 검색 AWS 하려면를 사용합니다AWS Partner Network.

사이버 위협 인텔리전스 통합 및 사용

사이버 위협 인텔리전스는 위협 행위자의 의도, 기회 및 기능에 대한 데이터 및 분석입니다. 위협 인텔리전스를 확보하고 사용하는 것은 인시던트를 조기에 탐지하고 위협 공격자 행동을 더 잘 이해하는 데 도움이 됩니다. 사이버 위협 인텔리전스에는 IP 주소 또는 맬웨어의 파일 해시와 같은 정적 지표가 포함됩니다. 여기에는 행동 패턴 및 의도와 같은 상위 수준 정보도 포함됩니다. 여러 사이버 보안 공급업체와 오픈 소스 리포지토리에서 위협 인텔리전스를 수집할 수 있습니다.

AWS 환경에 대한 위협 인텔리전스를 통합하고 극대화하기 위해 몇 가지 out-of-the-box 기능을 사용하고 자체 위협 인텔리전스 목록을 통합할 수 있습니다. Amazon은 AWS 내부 및 타사 위협 인텔리전스 소스를 GuardDuty 사용합니다. DNS 방화벽 및 AWS WAF 규칙과 같은 다른 AWS 서비스도 AWS의 고급 위협 인텔리전스 그룹에서 입력을 받습니다. 일부 GuardDuty 조사 결과는 MITRE ATT&CK 프레임워크에 매핑되며,이 프레임워크는 공격자 전술 및 기술에 대한 실제 관찰에 대한 정보를 제공합니다.

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 단원에서는 이러한 각 작업을 검토합니다. 자세한 내용은 보안 인시던트 대응 블로그 게시물의 로깅 전략을 AWS 참조하세요.

로그 소스 선택 및 활성화

보안 조사 전에 AWS 계정의 활동을 소급 재구성하려면 관련 로그를 캡처해야 합니다. AWS 계정 워크로드와 관련된 로그 소스를 선택하고 활성화합니다.

AWS CloudTrail 는 서비스 활동을 캡처하는 AWS 계정에 대한 API 호출을 추적하는 로깅 AWS 서비스입니다. 기본적으로 AWS Management Console, AWS CLI또는를 사용하여 CloudTrail이벤트 기록 기능을 통해 검색할 수 있는 관리 이벤트를 90일 동안 보존하여 활성화됩니다 AWS SDK. 데이터 이벤트의 보존 및 가시성을 높이려면 Amazon S3 버킷과 연결된 CloudTrail 추적을 생성하고 선택적으로 로그 그룹과 CloudWatch 연결해야 합니다. 또는 최대 7년 동안 CloudTrail 로그를 유지하고 SQL기반 쿼리 기능을 제공하는 CloudTrail Lake를 생성할 수 있습니다.

AWS 에서는를 사용하는 고객이 VPC 각각 Flow Logs 및 Amazon Route 53 해석기 쿼리 DNS 로그를 사용하여 Amazon S3 버킷 또는 CloudWatch 로그 그룹으로 스트리밍하는 네트워크 트래픽 및 로그를 VPC 활성화할 것을 권장합니다. VPC, 서브넷 또는 네트워크 인터페이스에 대한 VPC 흐름 로그를 생

성할 수 있습니다. VPC 흐름 로그의 경우 흐름 로그를 활성화하는 방법과 위치를 선택하여 비용을 절감할 수 있습니다.

AWS CloudTrail 로그, VPC 흐름 로그 및 Route 53 해석기 쿼리 로그는 보안 조사를 지원하는 기본 로깅 트리펙타입니다 AWS.

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

로그 스토리지 선택

로그 스토리지 선택은 일반적으로 사용하는 쿼리 도구, 보존 기능, 친숙성 및 비용과 관련이 있습니다. AWS 서비스 로그를 활성화할 때 일반적으로 Amazon S3 버킷 또는 CloudWatch 로그 그룹과 같은 스토리지 기능을 제공합니다.

Amazon S3 버킷은 선택적 수명 주기 정책을 통해 비용 효율적인 내구성 있는 스토리지를 제공합니다. Amazon S3 버킷에 저장된 로그는 Amazon Athena와 같은 서비스를 사용하여 기본적으로 쿼리할 수 있습니다. CloudWatch 로그 그룹은 CloudWatch Logs Insights를 통해 내구성 있는 스토리지와 내장 쿼리 기능을 제공합니다.

적절한 로그 보존 식별

S3 버킷 또는 CloudWatch 로그 그룹을 사용하여 로그를 저장할 때는 각 로그 소스에 적절한 수명 주기를 설정하여 스토리지 및 검색 비용을 최적화해야 합니다. 고객은 일반적으로 쿼리에 3~12개월의 로그를 쉽게 사용할 수 있으며 최대 7년 동안 보존됩니다. 가용성 및 보존에 대한 선택은 보안 요구 사항과 법적, 규제 및 비즈니스 의무의 조합과 일치해야 합니다.

로그에 대한 쿼리 메커니즘 선택 및 구현

에서 로그를 쿼리하는 데 사용할 수 있는 AWS주요 서비스는 로그 CloudWatch 그룹에 저장된 데이터에 대한 CloudWatch Logs Insights와 Amazon S3에 저장된 데이터에 대한 Amazon Athena Amazon S3 Amazon OpenSearch Service입니다. 보안 정보 및 이벤트 관리()와 같은 타사 쿼리 도구를 사용할 수도 있습니다SIEM.

로그 쿼리 도구를 선택하는 프로세스는 보안 작업의 인력, 프로세스 및 기술 측면을 고려해야 합니다. 운영, 비즈니스 및 보안 요구 사항을 충족하고 장기적으로 액세스 가능하고 유지 관리할 수 있는 도구를 선택합니다. 로그 쿼리 도구는 스캔할 로그 수가 도구의 한도 내에서 유지될 때 최적으로 작동합니다. 비용 또는 기술적 제약으로 인해 고객이 여러 쿼리 도구를 사용하는 것은 드문 일이 아닙니다. 예를

들어 고객은의 로그 수집 비용으로 인해 타사SIEM를 사용하여 지난 90일 동안의 데이터에 대한 쿼리를 수행하고 Athena를 사용하여 90일 이후의 쿼리를 수행할 수 있습니다SIEM. 구현에 관계없이 접근 방식이 특히 보안 이벤트 조사 중에 운영 효율성을 극대화하는 데 필요한 도구 수를 최소화하는지 확인합니다.

알림에 로그 사용

AWS 는 기본적으로 Amazon, GuardDuty AWS Security Hub및와 같은 보안 서비스를 통해 알림을 제공합니다 AWS Config. 이러한 서비스에서 다루지 않는 보안 알림 또는 환경과 관련된 특정 알림에 사용자 지정 알림 생성 엔진을 사용할 수도 있습니다. 이러한 알림 및 탐지를 빌드하려면 the section called “탐지”이 문서의 이라는 섹션에서 다룹니다.

포렌식 기능 개발

보안 인시던트에 앞서 보안 이벤트 조사를 지원하기 위한 포렌식 기능을 개발하는 것이 좋습니다. 의 포렌식 기술을 인시던트 대응에 통합하는 안내서는 이러한 지침을 NIST 제공합니다.

의 포렌식 AWS

기존 온프레미스 포렌식의 개념이에 적용됩니다 AWS. 블로그 게시물의 포렌식 조사 환경 전략 AWS 클라우드은 포렌식 전문 지식을 마이그레이션하기 시작할 수 있는 주요 정보를 제공합니다 AWS.

포렌식에 대한 환경 및 AWS 계정 구조를 설정한 후에는 다음 4단계에서 포렌식으로 건전한 방법론을 효과적으로 수행하는 데 필요한 기술을 정의해야 합니다.

- 컬렉션 - AWS CloudTrail,, AWS Config VPC 흐름 AWS 로그 및 호스트 수준 로그와 같은 관련 로그를 수집합니다. 영향을 받는 AWS 리소스의 스냅샷, 백업 및 메모리 덤프를 수집합니다.
- 검사 - 관련 정보를 추출하고 평가하여 수집된 데이터를 검사합니다.
- 분석 - 수집된 데이터를 분석하여 인시던트를 이해하고 인시던트에서 결론을 도출합니다.
- 보고 - 분석 단계에서 얻은 정보를 제공합니다.

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. 에서는 다양한 리소스의 스냅샷을 생성할 AWS수 있습니다. 스냅샷은 이러한 리소스의 백업을 제공합니다 point-in-time. 백업 및 복구를 지원할 수 있는 많은 AWS 서비스가 있습니다. 이러한 서비스 및 백업 및 복구 접근 방식에 대한 자세한 내용은 백업 및 복구 규범 지침을 참조하세요. 자세한 내용은 백업을 사용하여 보안 인시던트에서 복구 블로그 게시물을 참조하세요.

특히 랜섬웨어와 같은 상황에서는 백업의 보안을 잘 유지하는 것이 중요합니다. 백업 보안에 대한 지침은 블로그 게시물의 백업 보안을 위한 상위 10가지 보안 모범 사례를 AWS 참조하세요. 백업의 보안을 유지하는 것 외에도 정기적으로 백업 및 복원 프로세스를 테스트하여 보유한 기술과 프로세스가 정상적으로 작동하는지 확인해야 합니다.

에서 포렌식 자동화 AWS

보안 이벤트 중에 인시던트 대응 팀은 이벤트를 둘러싼 기간 동안 정확성을 유지하면서 신속하게 증거를 수집하고 분석할 수 있어야 합니다. 인시던트 대응 팀이 클라우드 환경, 특히 많은 인스턴스 및 계정에서 관련 증거를 수동으로 수집하는 것은 어렵고 시간이 많이 걸립니다. 또한 수작업으로 수집하는 경우 인적 오류가 발생하기 쉽습니다. 이러한 이유로 고객은 포렌식을 위한 자동화를 개발하고 구현해야 합니다.

AWS 는의 부록에 통합된 포렌식에 대한 여러 자동화 리소스를 제공합니다the section called “포렌식 리소스”. 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 이벤트에 대응하기 위한 철저한 준비는 시기 적절하고 효과적인 인시던트 대응에 매우 중요합니다. 인시던트 대응 준비에는 사람, 프로세스 및 기술이 포함됩니다. 이러한 세 도메인 모두 준비에 똑같이 중요합니다. 세 도메인 모두에서 인시던트 대응 프로그램을 준비하고 발전시켜야 합니다.

표 2에는이 섹션에 자세히 설명된 준비 항목이 요약되어 있습니다.

표 2 - 인시던트 대응 준비 항목

도메인	준비 항목	작업 항목
사람	역할 및 책임을 정의합니다.	• 관련 인시던트 대응 이해관계자를 식별합니다. • 인시던트에 대한 책임 있고 정보에 입각한 컨설팅(RACI) 차트를 개발합니다.
사람	인시던트 대응 직원을 교육합니다 AWS.	• 인시던트 대응 이해관계자에게 AWS 기반에 대해 교육합니다.

도메인	준비 항목	작업 항목
		• AWS 보안 및 모니터링 서비스에 대해 인시던트 대응 이해관계자를 교육합니다. • AWS 환경에 대한 인시던트 대응 이해관계자와 이를 설계하는 방법을 교육합니다.
사람	AWS 지원 옵션을 이해합니다.	• AWS 지원, 고객 인시던트 대응 팀(CIRT), DDoS 대응 팀(DRT) 및의 차이점을 이해합니다AMS. • 필요한 경우 활성 보안 이벤트 CIRT 중에에 도달하기 위한 분류 및 에스컬레이션 경로를 이해합니다.
프로세스	인시던트 대응 계획을 개발합니다.	• 인시던트 대응 프로그램 및 전략을 정의하는 상위 수준 문서를 생성합니다. • 인시던트 대응 계획에 대한 RACI, 커뮤니케이션 계획, 인시던트 정의 및 인시던트 대응 단계를 포함합니다.
프로세스	아키텍처 다이어그램을 문서화하고 중앙 집중화합니다.	• 계정 구조, 서비스 사용량, IAM 패턴 및 AWS 구성의 기타 핵심 기능 전반에 걸쳐 AWS 환경이 구성된 방법에 대한 세부 정보를 문서화합니다. • 클라우드 아키텍처의 아키텍처 다이어그램을 개발합니다.

도메인	준비 항목	작업 항목
프로세스	인시던트 대응 플레이북을 개발합니다.	• 플레이북의 구조를 위한 템플릿을 생성합니다. • 예상 보안 이벤트를 위한 플레이북을 빌드합니다. • GuardDuty 조사 결과와 같은 알려진 보안 알림을 위한 플레이북을 빌드합니다.
프로세스	정기적인 시뮬레이션을 실행합니다.	• 인시던트 시뮬레이션을 실행할 정기적인 주기를 개발합니다. • 배운 결과와 교훈을 사용하여 인시던트 대응 프로그램을 반복합니다.
기술	AWS 계정 구조를 개발합니다.	• 워크로드를 계정별로 분리하는 방법에 대한 AWS 계정 구조를 계획합니다. • 보안 도구 및 로그 아카이브 계정을 사용하여 보안 OU를 생성합니다. • 운영하는 각 리전에 대한 포렌식 계정을 사용하여 포렌식 OU를 생성합니다.
기술	대응 담당자가 조사 결과에 대한 소유권과 컨텍스트를 식별하는 데 도움이 되는 태그 지정 전략을 개발하고 구현합니다.	• 태깅 전략과 리소스와 연결할 태그를 계획합니다 AWS . • 태그 지정 전략을 구현하고 적용합니다.

도메인	준비 항목	작업 항목
기술	AWS 계정 연락처 정보를 업데이트합니다.	• AWS 계정에 연락처 정보가 나열되어 있는지 확인합니다. • 연락처 정보에 대한 이메일 배포 목록을 생성하여 단일 장애 지점을 제거합니다. • 계정 정보와 연결된 이메일 AWS 계정을 보호합니다.
기술	AWS 계정에 대한 액세스를 준비합니다.	• 인시던트 대응 담당자가 인시던트에 대응하는 데 필요한 액세스를 정의합니다. • 액세스를 구현, 테스트 및 모니터링합니다.
기술	위협 환경을 이해합니다.	• 환경 및 애플리케이션의 위협 모델을 개발합니다. • 사이버 위협 인텔리전스를 통합하고 사용합니다.
기술	로그를 선택하고 설정합니다.	• 조사를 위한 로그를 식별하고 활성화합니다. • 로그 스토리지를 선택합니다. • 로그 보존을 식별하고 구현합니다. • 로그 및 아티팩트를 검색하고 쿼리하는 메커니즘을 개발합니다. • 경고에 로그를 사용합니다.

도메인	준비 항목	작업 항목
기술	포렌식 기능을 개발합니다.	• 포렌식 수집에 필요한 아티팩트를 식별합니다. • 키 시스템의 백업을 캡처하고 보호합니다. • 식별된 로그 및 아티팩트 분석을 위한 메커니즘을 정의합니다. • 포렌식 분석을 위한 자동화를 구현합니다.

인시던트 대응 준비에는 반복적 접근 방식이 권장됩니다. 이러한 모든 준비 항목은 하룻밤 사이에 수행할 수 없습니다. 작게 시작하고 시간이 지남에 따라 인시던트 대응 기능을 지속적으로 개선하기 위한 계획을 만들어야 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 3에서 확인할 수 있습니다.

표 3 - 작업 단계

Phase(단계)	목표
감지	잠재적 보안 이벤트를 파악합니다.
분석	보안 이벤트가 인시던트인지 확인하고 인시던트의 범위를 평가합니다.
격납	보안 이벤트의 범위를 최소화하고 제한합니다.
근절	보안 이벤트와 관련된 승인되지 않은 리소스 또는 아티팩트를 제거합니다. 보안 인시던트를 일으킨 완화 조치를 구현합니다.

Phase(단계)	목표
복구	시스템을 알려진 안전 상태로 복원하고 이러한 시스템을 모니터링하여 위협이 반환되지 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 감지 단계의 주요 구성 요소입니다. 관심 있는 AWS 계정 활동을 기반으로 인시던트 대응 프로세스를 시작하라는 알림을 생성합니다.

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

- 감지 메커니즘은 기준 편차, 알려진 패턴 및 내부 또는 외부 엔터티의 알림을 기반으로 합니다.
- 기술과 사람의 예측할 수 없는 특성으로 인해 보안 인시던트의 수단과 행위자는 각각 시간이 지남에 따라 기준이 변경됩니다. 비인증 패턴은 새로운 또는 수정된 공격자 전술, 기법 및 절차()를 통해 나타납니다TTPs.
- 사람, 기술 및 프로세스에 대한 변경 사항은 인시던트 대응 프로세스에 즉시 통합되지 않습니다. 일부는 조사 진행 중에 발견됩니다.

알림 소스

다음 소스를 사용하여 알림을 정의하는 것을 고려해야 합니다.

- 조사 결과 - Amazon GuardDuty, AWS Security Hub, Amazon Macie, Amazon Inspector, AWS Config, IAM Access Analyzer 및 Network Access Analyzer와 같은 AWS 서비스는 알림을 생성하는 데 사용할 수 있는 조사 결과를 생성합니다.
- 로그 - Amazon S3 버킷 및 로그 그룹에 저장된 AWS 서비스, 인프라 및 애플리케이션 CloudWatch 로그를 구문 분석하고 상관관계를 파악하여 알림을 생성할 수 있습니다.

- 결제 활동 y - 결제 활동이 갑자기 변경되면 보안 이벤트가 발생할 수 있습니다. 결제 경보 생성의 설명서에 따라 이를 모니터링할 예상 AWS 요금을 모니터링합니다.
- 사이버 위협 인텔리전스 - 타사 사이버 위협 인텔리전스 피드를 구독하는 경우 해당 정보를 다른 로깅 및 모니터링 도구와 연결하여 이벤트의 잠재적 지표를 식별할 수 있습니다.
- 파트너 도구 - (APN)의 AWS Partner Network 파트너는 보안 목표를 달성하는 데 도움이 되는 최상위 제품을 제공합니다. 인시던트 대응의 경우 엔드포인트 탐지 및 대응(EDR) 또는가 인시던트 대응 목표를 지원하는 데 도움이 SIEM되는 제품을 파트너로 제공합니다. 자세한 내용은의 보안 파트너 솔루션 및 보안 솔루션을 참조하세요. AWS Marketplace
- AWS 신뢰 및 안전 - 악의적이거나 악의적인 활동을 식별하면 고객에게 연락할 Support 수 있습니다.
- 일회성 고객 응대 - 조직 내 고객, 개발자 또는 기타 직원이 비정상적인 것을 발견할 수 있으므로 보안 팀에 연락하는 잘 알려진 잘 알려진 방법을 마련하는 것이 중요합니다. 인기 있는 선택 사항에는 티켓팅 시스템, 연락처 이메일 주소 및 웹 양식이 포함됩니다. 조직이 일반 대중과 협력하는 경우, 퍼블릭 보안 연락 메커니즘이 필요할 수도 있습니다.

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

보안 제어 엔지니어링의 일부로 감지

탐지 메커니즘은 보안 제어 개발의 중요한 부분입니다. 지시적 및 예방적 제어가 정의되므로 관련 탐지 및 대응 제어를 구성해야 합니다. 예를 들어, 조직은 AWS 계정의 루트 사용자와 관련된 지시 제어를 설정하며, 이는 특정하고 매우 잘 정의된 활동에만 사용해야 합니다. 조직의 AWS 서비스 제어 정책()을 사용하여 구현된 예방 제어와 연결합니다SCP. 예상 기준을 초과하는 루트 사용자 활동이 발생하는 경우 EventBridge 규칙 및 SNS 주제로 구현된 탐지 제어는 보안 운영 센터(SOC)에 알립니다. 대응 제어에는 적절한 플레이북 SOC 선택, 분석 수행 및 인시던트가 해결될 때까지 작업이 수반됩니다.

보안 제어는에서 실행되는 워크로드의 위협 모델링에 의해 가장 잘 정의됩니다 AWS. 탐지 제어의 중요도는 특정 워크로드에 대한 비즈니스 영향 분석(BIA)을 검토하여 설정됩니다. 탐지 제어에 의해 생성된 경보는 들어오는 대로 처리되지 않고 분석 중에 조정될 초기 중요도를 기반으로 합니다. 초기 중요도 세트는 우선 순위 지정을 위한 보조 도구입니다. 알림이 발생한 컨텍스트에 따라 실제 중요도가 결정됩니다. 예를 들어 조직은 Amazon GuardDuty 을 워크로드의 일부인 EC2 인스턴스에 사용되는 탐지 제어의 구성 요소로 사용합니다. 결과가 생성`Impact:EC2/SuspiciousDomainRequest.Reputation`되어 워크로드 내에 나열된 Amazon EC2 인스턴스가 악성으로 의심되는 도메인 이름을 쿼리하고 있음을 알려줍니다. 이 알림은 기본적으로 심각도가 낮은 것으로 설정되며, 분석 단계가 진행됨에 따라 권한이 없는 액터`p4d.24xlarge`가 수백 개의 유형의 EC2 인스턴스를 배포하여 조직의 운영 비용이 크게 증가한 것으로 확인되었습니다. 이 시점에서 인시던트

대응 팀은이 알림의 중요도를 높음으로 조정하여 긴급성을 높이고 추가 조치를 신속하게 처리하기로 결정합니다. GuardDuty 결과 심각도는 변경할 수 없습니다.

탐지 제어 구현

탐지 제어가 구현되는 방식을 이해하는 것이 중요합니다. 탐지 제어는 특정 이벤트에 경보를 사용하는 방법을 결정하는 데 도움이 되기 때문입니다. 기술적 탐지 제어에는 두 가지 주요 구현이 있습니다.

- 동작 감지는 일반적으로 기계 학습(ML) 또는 인공 지능(AI)이라고 하는 수학적 모델에 의존합니다. 감지는 추론을 통해 이루어지므로 알림이 반드시 실제 이벤트를 반영하지는 않을 수 있습니다.
- 규칙 기반 감지는 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 함께 제공됩니다. 다음은를 사용한 규칙 기반 및 동작 감지의 몇 가지 예입니다 GuardDuty.

- 조사 결과가 `Exfiltration:IAMUser/AnomalousBehavior` 생성되면 '계정에서 이상 API 요청이 관찰되었습니다.'라는 메시지가 표시됩니다. 설명서를 자세히 살펴보면 'ML 모델은 계정의 모든 API 요청을 평가하고 공격자가 사용하는 기법과 관련된 이상 이벤트를 식별합니다.'라는 메시지가 표시되며, 이는이 결과가 행동적 성격을 지니는 것임을 나타냅니다.
- 조사 결과의 경우 `CloudTrailImpact:S3/MaliciousIPCaller` GuardDuty 는의 Amazon S3 서비스의 API 호출을 분석하여 `SourceIPAddress` 로그 요소를 위협 인텔리전스 피드가 포함된 퍼블릭 IP 주소 테이블과 비교합니다. 항목과 직접 일치하는 항목을 찾으면 결과가 생성됩니다.

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

사람 기반 탐지

지금까지 기술 기반 탐지에 대해 논의했습니다. 또 다른 중요한 탐지 소스는 고객 조직 내부 또는 외부의 사람들에서 비롯됩니다. 내부자는 직원 또는 계약자로 정의될 수 있으며 외부자는 보안 연구원, 법 집행 기관, 뉴스 및 소셜 미디어와 같은 법인입니다.

기술 기반 탐지는 체계적으로 구성할 수 있지만, 사람 기반 탐지는 이메일, 티켓, 우편, 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 문화는 보안에 대한 심층 방어 접근 방식을 위해 사람 기반 탐지 메커니즘을 통합, 촉진 및 강화해야 합니다.

요약

탐지에서는 규칙 기반 알림과 행동 기반 알림을 혼합하는 것이 중요합니다. 또한 내부 및 외부 사람들이 보안 문제에 대한 티켓을 제출할 수 있는 메커니즘이 마련되어 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 MITRE ATT&CK와 같은 프레임워크를 사용하여 공격자 전술, 기법 및 절차()를 이해할 수 있습니다 TTPs. MITRE ATT&CK 프레임워크는 다양한 탐지 메커니즘에서 공통 언어로를 사용하는 데 도움이 될 수 있습니다.

분석

로그, 쿼리 기능 및 위협 인텔리전스는 분석 단계에서 필요한 몇 가지 지원 구성 요소입니다. 탐지에 사용된 것과 동일한 로그 중 다수가 분석에도 사용되며 쿼리 도구의 온보딩 및 구성이 필요합니다.

알림의 영향 검증, 범위 지정 및 평가

분석 단계에서는 경보를 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 워크로드 소유자와 직접 소통합니다.
- 스코핑은 관련된 모든 리소스가 인벤토리되고 이해관계자가 거짓 양성일 가능성이 낮다고 합의한 후 알림 중요도가 조정되는 다음 단계입니다.
- 마지막으로 영향 분석은 실제 비즈니스 중단을 자세히 설명합니다.

영향을 받는 워크로드 구성 요소가 식별되면 범위 조정 결과가 관련 워크로드의 복구 시점 목표(RPO) 및 복구 시간 목표()와 상관관계가 있을 수 있으며, 경보 중요도에 맞게 RTO조정하여 리소스 할당 및 다음에 발생하는 모든 활동을 시작합니다. 모든 인시던트가 비즈니스 프로세스를 지원하는 워크로드의 운영을 직접적으로 방해하는 것은 아닙니다. 민감한 데이터 공개, 지적 재산 도용 또는 리소스 하이재킹(암호화 채굴과 같은)과 같은 인시던트는 비즈니스 프로세스를 즉시 중단하거나 약화시키지 않을 수 있지만 나중에 결과가 발생할 수 있습니다.

보안 로그 및 조사 결과 강화

위협 인텔리전스 및 조직 컨텍스트로 강화

분석 과정에서 관찰 가능한 관심 대상은 경보의 컨텍스트화를 강화해야 합니다. 준비 섹션에 설명된 대로 사이버 위협 인텔리전스를 통합하고 활용하는 것은 보안 결과에 대해 자세히 이해하는 데 도움이 될 수 있습니다. 위협 인텔리전스 서비스는 퍼블릭 IP 주소, 도메인 이름 및 파일 해시에 평판 및 속성 소유권을 할당하는 데 사용됩니다. 이러한 도구는 유료 및 무료 서비스로 사용할 수 있습니다.

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

AWS 는 위협 인텔리전스를 고객에게 직접 제공하지 않지만 Amazon과 같은 서비스는 위협 인텔리전스를 사용하여 보강 및 결과 생성을 GuardDuty 수행합니다. 자체 위협 인텔리전스를 GuardDuty 기반으로에 사용자 지정 위협 목록을 업로드할 수도 있습니다.

자동화를 통한 강화

자동화는 AWS 클라우드 거버넌스의 중요한 부분입니다. 인시던트 대응 수명 주기의 다양한 단계에서 사용할 수 있습니다.

탐지 단계의 경우 규칙 기반 자동화는 로그의 위협 모델에서 관심 있는 패턴을 일치시키고 알림 전송과 같은 적절한 조치를 취합니다. 분석 단계에서는 탐지 메커니즘을 활용하고 경고 본문을 엔진에 전달하여 로그를 쿼리하고 이벤트 컨텍스트화를 위해 관찰 가능한 항목을 보강할 수 있습니다.

기본 형식의 알림 본문은 리소스와 자격 증명으로 구성됩니다. 예를 들어, 경보 시점을 기준으로 경보 본문의 자격 증명 또는 리소스에서 수행한 CloudTrail 활동을 쿼리 AWS API하는 자동화를 구현하여 식별된 API 활동의 `eventSource`, `SourceIPAddress`, 및 `eventName`를 포함한 추가 인사이트`userAgent`를 제공할 수 있습니다. 이러한 쿼리를 자동화된 방식으로 수행하면 대응 담당자가 분류 중에 시간을 절약하고 추가 컨텍스트를 확보하여 정보에 입각한 더 나은 결정을 내릴 수 있습니다.

자동화를 사용하여 AWS 보안 조사 결과를 보강하고 분석을 간소화하는 방법에 대한 예는 계정 메타데이터 블로그 게시물로 Security Hub 조사 결과를 보강하는 방법을 참조하세요.

포렌식 증거 수집 및 분석

이 문서의 the section called “준비” 섹션에 언급된 포렌식은 인시던트 대응 중에 아티팩트를 수집하고 분석하는 프로세스입니다. 에서는 네트워크 트래픽 패킷 캡처 AWS, 운영 체제 메모리 덤프와 같은 인프라 도메인 리소스와 AWS CloudTrail 로그와 같은 서비스 도메인 리소스에 적용됩니다.

포렌식 프로세스에는 다음과 같은 기본 특성이 있습니다.

- 일관성 - 편차 없이 문서화된 정확한 단계를 따릅니다.
- 반복 가능 - 동일한 아티팩트에 대해 반복할 때 정확히 동일한 결과를 생성합니다.
- 통상 - 공개적으로 문서화되고 널리 채택됩니다.

인시던트 대응 중에 수집된 아티팩트에 대한 관리 연속성을 유지하는 것이 중요합니다. 자동화를 사용하고이 컬렉션에 대한 자동 설명서를 생성하면 읽기 전용 리포지토리에 아티팩트를 저장하는 것 외에도 도움이 될 수 있습니다. 무결성을 유지하기 위해 수집된 아티팩트의 정확한 복제본에 대해서만 분석을 수행해야 합니다.

관련 아티팩트 수집

이러한 특성을 염두에 두고 영향 및 범위에 대한 관련 알림 및 평가를 기반으로 추가 조사 및 분석과 관련된 데이터를 수집해야 합니다. 서비스/제어 영역 로그(, Amazon S3 데이터 이벤트CloudTrail, VPC 흐름 로그), 데이터(Amazon S3 메타데이터 및 객체), 리소스(데이터베이스, Amazon EC2 인스턴스)를 포함하여 조사와 관련이 있을 수 있는 다양한 데이터 유형 및 소스입니다.

서비스/컨트롤 플레인 로그는 로컬 분석을 위해 수집하거나 네이티브 AWS 서비스(해당하는 경우)를 사용하여 직접 쿼리하는 것이 좋습니다. 데이터(메타데이터 포함)를 직접 쿼리하여 관련 정보를 얻거나 소스 객체를 획득할 수 있습니다. 예를 들어를 사용하여 Amazon S3 버킷 및 객체 메타데이터를 획득하고 소스 객체 AWS CLI 를 직접 획득합니다. 리소스는 리소스 유형 및 의도된 분석 방법과 일치하는 방식으로 수집해야 합니다. 예를 들어 전체 데이터베이스 자체copy/snapshot of the system running the database, creating a copy/snapshot의를 생성하거나 조사와 관련된 데이터베이스에서 특정 데이터 및 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 응답 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 중지로 설정(종료로 설정된 경우), 연결된 EBS 볼륨에 대해 종료 시 삭제 속성을 비활성화, 시각적 표시 및 가능한 응답 자동화에 사용할 수 있는 적절한 태그 적용(예: 이름 `Status` 및 값이 인 태그를 적용할 때 데이터의 포렌식 획득을 `Quarantine`수행하고 인스턴스를 격리)과 같은 인스턴스 보호를 활성화합니다.

3. 디스크 획득(EBS 스냅샷) - 연결된 EBS 볼륨의 EBS 스냅샷을 획득합니다. 각 스냅샷에는 (스냅샷을 찍은 순간부터) 데이터를 새 EBS 볼륨으로 복원하는 데 필요한 정보가 포함되어 있습니다. 인스턴스 스토어 볼륨을 사용하는 경우 라이브 응답/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 소스 또는 상용 도구를 사용하여 시스템 메모리 이미지를 획득해야 합니다.
5. (선택 사항) 라이브 응답/아티팩트 수집 수행 - 디스크 또는 메모리를 달리 획득할 수 없거나 유효한 비즈니스 또는 운영 이유가 있는 경우에만 시스템의 라이브 응답을 통해 대상 데이터 수집(disk/memory/logs)을 수행합니다. 이렇게 하면 중요한 시스템 데이터와 아티팩트가 수정됩니다.
6. 인스턴스 폐기 - Auto Scaling 그룹에서 인스턴스를 분리하고, 로드 밸런서에서 인스턴스를 등록 취소하고, 권한이 최소화되거나 없는 사전 빌드된 인스턴스 프로파일을 조정하거나 적용합니다.
7. 인스턴스 격리 또는 포함 - 인스턴스와의 현재 및 향후 연결을 종료하고 방지하여 환경 내 다른 시스템 및 리소스에서 인스턴스가 효과적으로 격리되었는지 확인합니다. 자세한 내용은이 문서의 the section called “격리” 섹션을 참조하세요.
8. 응답자의 선택 - 상황과 목표에 따라 다음 중 하나를 선택합니다.
   - 시스템을 폐기하고 종료합니다(권장).

     사용 가능한 증거가 확보되면 시스템을 종료하여 인스턴스가 환경에 미칠 수 있는 향후 영향에 대한 가장 효과적인 완화 조치를 확인합니다.
   - 모니터링을 위해 계측된 격리된 환경 내에서 인스턴스를 계속 실행합니다.

     표준 접근 방식으로 권장되지는 않지만 상황에 따라 인스턴스를 지속적으로 관찰해야 하는 경우(예: 인스턴스에 대한 포괄적인 조사 및 분석을 수행하기 위해 추가 데이터 또는 지표가 필요한 경우) 인스턴스 종료를 고려할 수 있습니다. 인스턴스AMI의 생성 및 인스턴스의 거의 지속적인 모니터링을 용이하게 하기 위해 계측을 사용하여 완전히 격리되고 구성되도록 사전 계측된 샌드박스 환경 내의 전용 포렌식 계정에서 인스턴스를 다시 시작(예: VPC 흐름 로그 또는 VPC 트래픽 미러링).

> **Note**
>
> 사용 가능한 휘발성(및 가치 있는) 데이터를 캡처하려면 라이브 응답 활동 또는 시스템 격리 또는 종료 전에 메모리를 캡처해야 합니다.

서술 개발

분석 및 조사 중에 후속 단계 및 최종 보고서에서 사용할 수 있도록 수행한 작업, 수행된 분석 및 식별된 정보를 문서화합니다. 이러한 서술은 간단하고 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. 예:

> 마케팅 및 영업 부서는 2022년 3월 15일에 민감한 데이터의 공개 게시를 방지하기 위해 암호화폐 결제를 요구하는 랜섬 메모를 받았습니다. 는 마케팅 및 판매에 속하는 Amazon RDS 데이터베이스에 2022년 2월 20일에 공개적으로 액세스할 수 있다고 SOC 결정했습니다. SOC 쿼리된 RDS 액세스 로그는 웹 개발자 중 하나인 Major Mary에게 *mm03434* 속한 자격 증명과 함께 2022년 2월 20일에 IP 주소 198.51.100.23이 사용되었다고 판단했습니다. SOC 쿼리된 VPC Flow Logs는 약 256MB의 데이터가 동일한 IP 주소로 동일한 날짜(타임스탬프 2022-02-20T15:50+00Z)에 송신되었다고 판단했습니다. 는 오픈 소스 위협 인텔리전스를 통해 자격 증명을 퍼블릭 리포지토리의 일반 텍스트로 현재 사용할 수 있다고 SOC 판단됩니다*https[:]//example[.]com/majormary/rds-utils*.

격리

인시던트 대응과 관련된 봉쇄의 한 가지 정의는 보안 이벤트의 범위를 최소화하고 환경 내에서 무단 사용의 영향을 포함하는 보안 이벤트를 처리하는 동안 전략의 프로세스 또는 구현입니다.

억제 전략은 수많은 요인에 따라 달라지며, 억제 전술, 타이밍 및 목적의 적용 측면에서 조직마다 다를 수 있습니다. NIST SP 800-61 컴퓨터 보안 인시던트 처리 안내서는 다음을 포함하여 적절한 억제 전략을 결정하기 위한 몇 가지 기준을 간략하게 설명합니다.

- 리소스의 잠재적 손상 및 도난
- 증거 보존의 필요성
- 서비스 가용성(네트워크 연결, 외부 당사자에게 제공되는 서비스)
- 전략을 구현하는 데 필요한 시간 및 리소스
- 전략의 효과(부분 또는 전체 봉쇄)
- 솔루션 기간(4시간 내에 긴급 해결 방법 제거, 2주 내에 임시 해결 방법 제거, 영구 솔루션)

AWS그러나의 서비스와 관련하여 기본 억제 단계는 세 가지 범주로 나눌 수 있습니다.

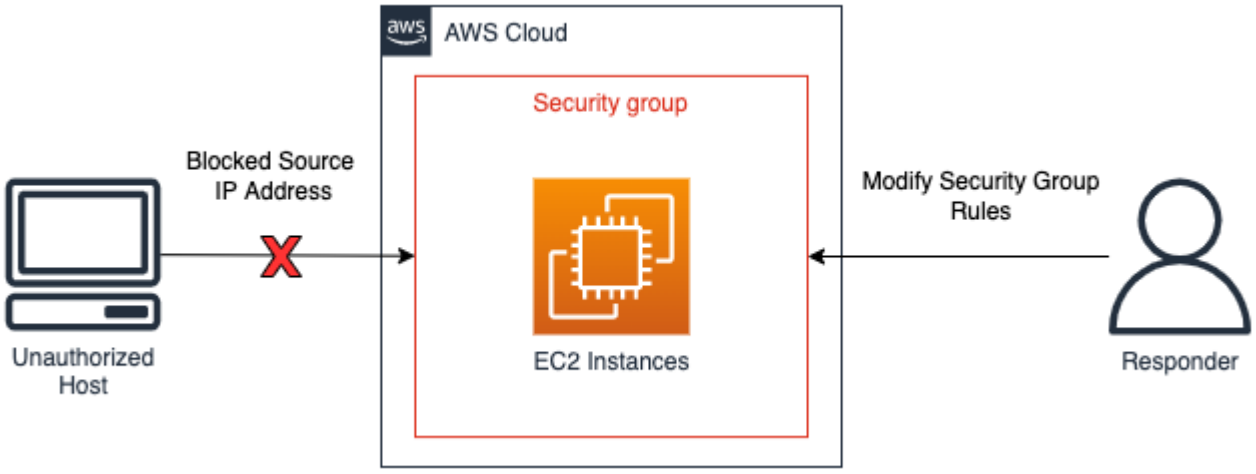
- 소스 봉쇄 - 필터링 및 라우팅을 사용하여 특정 소스로부터의 액세스를 방지합니다.
- 기술 및 액세스 억제 - 영향을 받는 리소스에 대한 무단 액세스를 방지하기 위해 액세스를 제거합니다.
- 대상 봉쇄 - 필터링 및 라우팅을 사용하여 대상 리소스에 대한 액세스를 방지합니다.

소스 격리

소스 격리는 환경 내에서 필터링 또는 라우팅을 사용하고 적용하여 특정 소스 IP 주소 또는 네트워크 범위의 리소스에 대한 액세스를 방지하는 것입니다. AWS 서비스를 사용하는 소스 억제의 예는 다음과 같습니다.

- 보안 그룹 - 격리 보안 그룹을 생성하여 Amazon EC2 인스턴스에 적용하거나 기존 보안 그룹에서 규칙을 제거하면 Amazon EC2 인스턴스 또는 AWS 리소스에 대한 무단 트래픽을 억제하는 데 도움이 될 수 있습니다. 기존 추적 연결은 보안 그룹 변경으로 인해 종료되지 않으며, 향후 트래픽만 새 보안 그룹에 의해 효과적으로 차단된다는 점에 유의해야 합니다(추적 및 추적되지 않은 연결에 대한 자세한 내용은 이 Incident Response Playbook 및 보안 그룹 연결 추적 참조).
- 정책 - IP 주소, 네트워크 범위 또는 VPC 엔드포인트로부터의 트래픽을 차단하거나 허용하도록 Amazon S3 버킷 정책을 구성할 수 있습니다. 정책은 의심스러운 주소와 Amazon S3 버킷에 대한 액세스를 차단하는 기능을 생성합니다. 버킷 정책에 대한 자세한 내용은 Amazon S3 콘솔을 사용하여 버킷 정책 추가에서 확인할 수 있습니다.
- AWS WAF – 리소스가 응답 AWS WAF 하는 웹 요청에 대한 세분화된 제어를 제공하도록 웹 액세스 제어 목록(웹 ACLs)을에서 구성할 수 있습니다. 에 구성된 IP 세트에 IP 주소 또는 네트워크 범위를 추가 AWS WAF하고, IP 세트에 블록과 같은 일치 조건을 적용할 수 있습니다. 이렇게 하면 발신 트래픽의 IP 주소 또는 네트워크 범위가 IP 세트 규칙에 구성된 것과 일치할 경우 리소스에 대한 웹 요청이 차단됩니다.

다음 다이어그램에서는 특정 IP 주소로만 새 연결을 제한하기 위해 Amazon EC2 인스턴스의 보안 그룹을 수정하는 인시던트 대응 분석가가 있는 소스 격리의 예를 볼 수 있습니다. 보안 그룹 글머리 기호에 설명된 대로, 기존 추적 연결은 보안 그룹 변경으로 인해 종료되지 않습니다.



소스 격리 예제

기술 및 액세스 억제

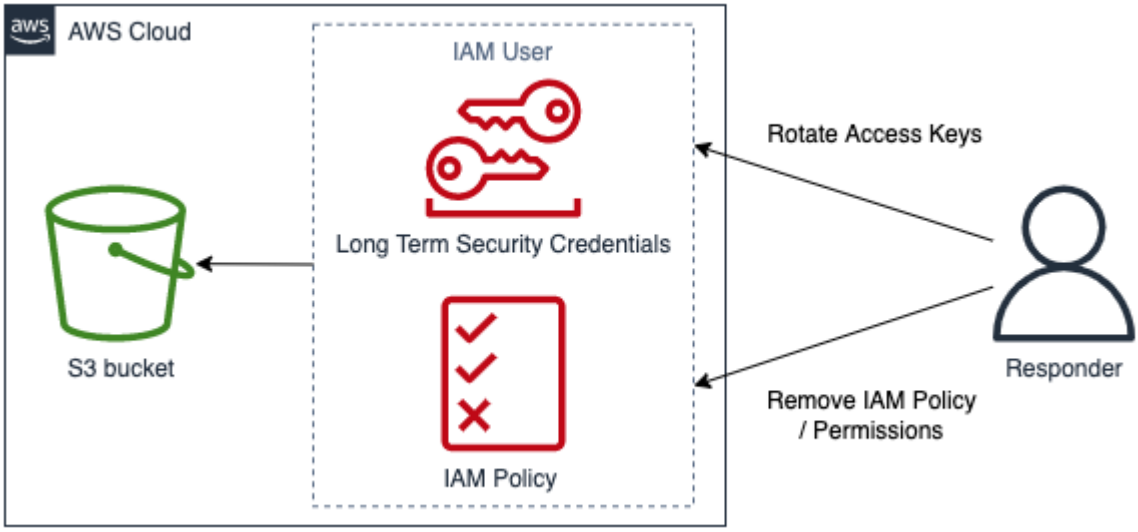
리소스에 액세스할 수 있는 함수와 IAM 보안 주체를 제한하여 리소스의 무단 사용을 방지합니다. 여기에는 리소스에 액세스할 수 있는 IAM 보안 주체의 권한 제한과 임시 보안 자격 증명 취소도 포함됩니다. AWS 서비스를 사용하는 기법 및 액세스 억제의 예는 다음과 같습니다.

- 권한 제한 - IAM 보안 주체에 할당된 권한은 최소 권한 원칙을 따라야 합니다. 그러나 활성 보안 이벤트 중에는 특정 IAM 보안 주체의 대상 리소스에 대한 액세스를 더 제한해야 할 수 있습니다. 이 경우 포함할 IAM 보안 주체에서 권한을 제거하여 리소스에 대한 액세스를 포함할 수 있습니다. 이는 IAM 서비스에서 수행되며 AWS Management Console, AWS CLI, 또는를 사용하여 적용할 수 있습니다 AWS SDK.
- 키 취소 - IAM 보안 주체는 IAM 액세스 키를 사용하여 리소스에 액세스하거나 관리합니다. 이는 AWS CLI 또는 AWS API에 대한 프로그래밍 방식 요청에 서명하고 접두사로 시작하는 장기 정적 자격 증명입니다AKIA(자세한 내용은 식별자의 고유 ID 접두사 이해 섹션을 참조하세요). IAM 액세스 키가 손상된 IAM 보안 주체에 대한 IAM 액세스를 포함하려면 액세스 키를 비활성화하거나 삭제할 수 있습니다. 다음 사항에 유의해야 합니다.
  - 액세스 키는 비활성화된 후 다시 활성화할 수 있습니다.
  - 액세스 키는 삭제된 후에는 복구할 수 없습니다.
  - 보안 IAM 주체는 언제든지 최대 2개의 액세스 키를 가질 수 있습니다.
  - 액세스 키를 사용하는 사용자 또는 애플리케이션은 키가 비활성화되거나 삭제되면 액세스 권한을 상실합니다.
- 임시 보안 자격 증명 취소 - 조직에서 임시 보안 자격 증명을 사용하여 리소스에 대한 액세스를 AWS 제어하고 접두사로 시작할 수 있습니다ASIA(자세한 내용은 식별자의 고유 ID 접두사 이해 섹션을 참

조하세요). IAM 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 내 IAM 서비스를 사용하여 AWS Management Console 완료할 수 있습니다. 임시 보안 자격 증명은 IAM 사용자에게도 발급할 수 있지만(IAM역할이 아님),이 글을 쓰는 시점에는 내 IAM 사용자의 임시 보안 자격 증명을 취소할 수 있는 옵션이 없습니다 AWS Management Console. 임시 보안 자격 증명을 생성한 권한이 없는 사용자가 사용자의 IAM 액세스 키를 손상시키는 보안 이벤트의 경우 다음 두 가지 방법을 사용하여 임시 보안 자격 증명을 취소할 수 있습니다.

  - 보안 토큰 발급 시간을 기준으로 액세스를 차단하는 인라인 정책을 IAM 사용자에게 연결합니다 (자세한 내용은 임시 보안 자격 증명에 대한 권한 비활성화의 특정 시간 이전에 발급된 임시 보안 자격 증명에 대한 액세스 거부 단원 참조). https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_control-access_disable-perms.html
  - 손상된 액세스 키를 소유한 IAM 사용자를 삭제합니다. 필요한 경우 사용자를 다시 생성합니다.
- AWS WAF - 권한이 없는 사용자가 사용하는 특정 기법에는 SQL 삽입 및 교차 사이트 스크립팅(XSS)이 포함된 요청과 같은 일반적인 악성 트래픽 패턴이 포함됩니다.는 AWS WAF 기본 제공 규칙 문을 사용하여 이러한 기법을 사용하는 트래픽과 일치시키고 거부하도록 구성할 AWS WAF 수 있습니다.

다음 다이어그램에서는 인시던트 대응 담당자가 액세스 키를 교체하거나 IAM 정책을 제거하여 IAM 사용자가 Amazon S3 버킷에 액세스하지 못하도록 하는 기법 및 액세스 억제의 예를 볼 수 있습니다.



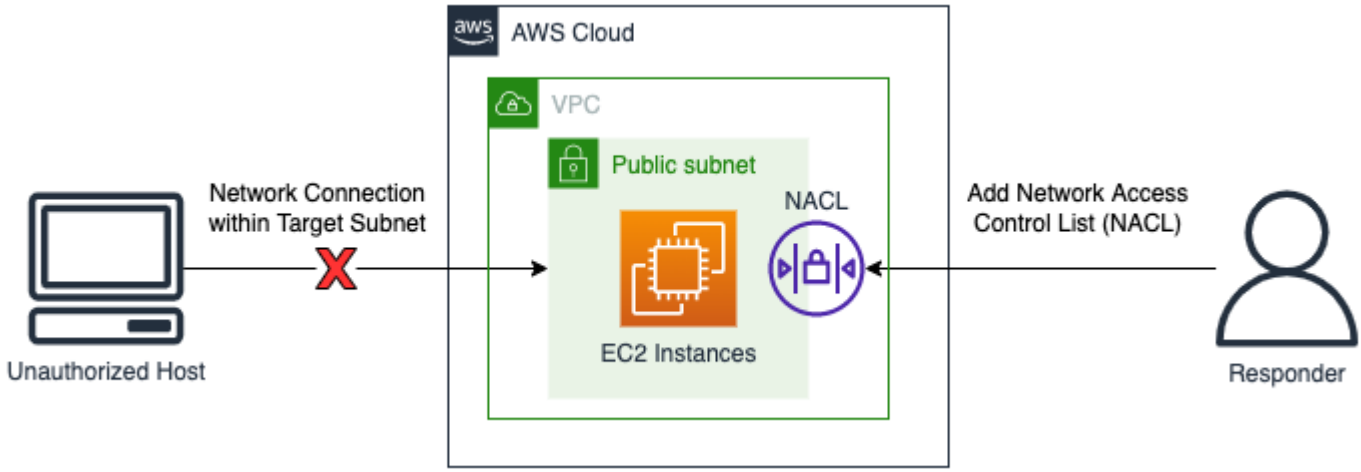
기술 및 액세스 억제 예제

대상 봉쇄

대상 억제는 대상 호스트 또는 리소스에 대한 액세스를 방지하기 위해 환경 내에서 필터링 또는 라우팅을 적용하는 것입니다. 경우에 따라 대상 봉쇄에는 합법적인 리소스가 가용성을 위해 복제되는지 확인하기 위한 복원력의 형태도 포함됩니다. 격리 및 봉쇄를 위해 리소스를 이러한 형태의 복원력에서 분리해야 합니다. AWS 서비스를 사용한 대상 억제의 예는 다음과 같습니다.

- 네트워크 ACLs - AWS 리소스가 포함된 서브넷에 구성된 네트워크ACLs(네트워크 ACLs)에는 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 영향을 미칩니다. 네트워크 내에 나열된 규칙ACL은 하향식 순서로 처리되므로 기존 네트워크의 첫 번째 규칙은 대상 리소스 및 서브넷에 대한 무단 트래픽을 거부하도록 구성되어야 ACL 합니다. 또는 인바운드 및 아웃바운드 트래픽 모두에 대한 단일 거부 규칙으로 완전히 새로운 네트워크를 생성하고 대상 리소스가 포함된 서브넷과 연결하여 새 네트워크를 사용하여 서브넷에 대한 액세스를 방지할 ACL 수 있습니다ACL.
- 종료 - 리소스를 완전히 종료하면 무단 사용의 영향을 억제하는 데 효과적일 수 있습니다. 또한 리소스를 종료하면 비즈니스 요구 사항에 대한 합법적인 액세스가 방지되고 휘발성 포렌식 데이터가 획득되지 않으므로 이는 의도적인 결정이어야 하며 조직의 보안 정책에 따라 판단되어야 합니다.
- 격리 VPCs - 격리를 사용하여 리소스를 효과적으로 억제하면서 합법적인 트래픽(예: 바이러스 백신(AV) 또는 인터넷 또는 외부 관리 콘솔에 액세스해야 하는 EDR 솔루션)에 대한 액세스를 제공할 VPCs 수 있습니다. 보안 이벤트 전에 격리를 VPCs 사전 구성하여 유효한 IP 주소 및 포트를 허용할 수 있으며, 활성 보안 이벤트 VPC 중에 대상 리소스를 즉시이 격리로 이동하여 리소스를 포함하는 동시에 인시던트 대응의 후속 단계에서 대상 리소스가 합법적인 트래픽을 보내고 받을 수 있습니다. 격리 사용의 중요한 측면VPC은 EC2 인스턴스와 같은 리소스를 사용하기 VPC 전에 새 격리에서 종료하고 다시 시작해야 한다는 것입니다. 기존 EC2 인스턴스는 다른 가용 영역VPC으로 이동할 수 없습니다. 이렇게 하려면 Amazon EC2 인스턴스를 다른 서브넷, 가용 영역 또는 로 이동하려면 어떻게 해야 하나요VPC?에 설명된 단계를 따르세요.
- Auto Scaling 그룹 및 로드 밸런서 - AWS Auto Scaling 그룹 및 로드 밸런서에 연결된 리소스는 대상 격리 절차의 일부로 분리 및 등록 취소해야 합니다. AWS 리소스 분리 및 등록 취소는 AWS Management Console AWS CLI및를 사용하여 수행할 수 있습니다 AWS SDK.

다음 다이어그램에서는 승인되지 않은 호스트의 네트워크 연결 요청을 차단하기 위해 인시던트 대응 분석가가 ACL 서브넷에 네트워크를 추가하는 대상 격리의 예를 보여줍니다.



대상 억제 예제

요약

격리는 인시던트 대응 프로세스의 한 단계이며 수동 또는 자동화가 가능합니다. 전반적인 억제 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 컴퓨터 보안 인시던트 처리 안내서는 근절을 위한 몇 가지 단계를 제공합니다.

1. 악용된 모든 취약성을 식별하고 완화합니다.
2. 맬웨어, 부적절한 자료 및 기타 구성 요소를 제거합니다.
3. 영향을 받는 호스트가 더 많이 검색되면(예: 새 맬웨어 감염) 탐지 및 분석 단계를 반복하여 영향을 받는 다른 모든 호스트를 식별한 다음 해당 호스트에 대한 인시던트를 억제하고 근절합니다.

AWS 리소스의 경우, 사용 가능한 로그 또는 CloudWatch 로그 및 Amazon과 같은 자동화된 도구를 통해 탐지되고 분석된 이벤트를 통해 이를 더욱 개선할 수 있습니다 GuardDuty. 이러한 이벤트는 환경을 알려진 안전 상태로 적절하게 복원하기 위해 수행해야 하는 문제 해결을 결정하는 기반이 되어야 합니다.

근절의 첫 번째 단계는 AWS 계정 내에서 영향을 받은 리소스를 결정하는 것입니다. 이는 사용 가능한 로그 데이터 소스, 리소스 및 자동화된 도구 분석을 통해 이루어집니다.

- 계정의 IAM 자격 증명이 수행한 무단 작업을 식별합니다.
- 계정에 대한 무단 액세스 또는 변경 사항을 식별합니다.
- 승인되지 않은 리소스 또는 IAM 사용자의 생성을 식별합니다.
- 무단 변경 사항이 있는 시스템 또는 리소스를 식별합니다.

리소스 목록이 식별되면 각를 평가하여 리소스가 삭제되거나 복원될 경우 비즈니스에 미치는 영향을 확인해야 합니다. 예를 들어 웹 서버가 비즈니스 애플리케이션을 호스팅하고 이를 삭제하면 가동 중지 시간이 발생할 수 있으므로 영향을 받는 서버를 삭제하기 AMI 전에 확인된 안전한 백업에서 리소스를 복구하거나 클린에서 시스템을 다시 시작하는 것을 고려해야 합니다.

비즈니스 영향 분석을 완료한 후 로그 분석의 이벤트를 사용하여 계정으로 이동하여 다음과 같은 적절한 문제 해결을 수행해야 합니다.

- 키 교체 또는 삭제 -이 단계에서는 액터가 계정 내에서 활동을 계속 수행할 수 있는 기능을 제거합니다.
- 잠재적으로 승인되지 않은 IAM 사용자 자격 증명을 교체하세요.
- 인식되지 않거나 승인되지 않은 리소스를 삭제합니다.

> **Important**
>
> 조사를 위해 리소스를 보관해야 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 감염 시 AWS Partner 또는 다른 공급업체에 문의해야 할 수 있습니다. AWS 는 맬웨어 분석 또는 제거를 위한 네이티브 도구를 제공하지 않습니다. 그러나 Amazon용 GuardDuty 맬웨어 모듈을 사용하는 경우 제공된 결과에 대한 EBS권장 사항을 사용할 수 있습니다.

식별된 영향을 받는 리소스를 제거한 후에는 계정의 보안 검토를 수행하는 것이 AWS 좋습니다. 이는 AWS Config 규칙을 사용하거나 Prowler 및 같은 오픈 소스 솔루션을 사용하거나 다른 공급업체를 ScoutSuite통해 수행할 수 있습니다. 또한 퍼블릭-(인터넷) 관련 리소스에 대한 취약성 스캔을 수행하여 잔여 위험을 평가하는 것도 고려해야 합니다.

근절은 인시던트 대응 프로세스의 한 단계이며 인시던트 및 영향을 받는 리소스에 따라 수동 또는 자동화할 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 우선 순위
- 복원 계획
- 인증 및 권한 부여

NIST SP 800-61 컴퓨터 보안 인시던트 처리 안내서는 시스템을 복구하기 위한 몇 가지 단계를 제공합니다.

- 깨끗한 백업에서 시스템 복원.
  - 시스템에 복원하기 전에 백업을 평가하여 감염이 없는지 확인하고 보안 이벤트가 다시 발생하지 않도록 합니다.

    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 사용합니다.
- 자동화를 사용하여 신뢰할 수 있는 소스에서 재배포하는 등 시스템을 처음부터 다시 빌드합니다 AWS .
- 손상된 파일을 깨끗한 버전으로 바꿉니다.

  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 남용되었을 수 있는 IAM 보안 주체의 암호가 포함됩니다.
  - 가능하면 최소 권한 전략의 일부로 IAM 보안 주체 및 연동에 역할을 사용하는 것이 좋습니다.

- 네트워크 경계 보안 강화(방화벽 규칙 세트, 경계 라우터 액세스 제어 목록).

리소스가 복구되면 인시던트 대응 정책, 절차 및 가이드를 업데이트하기 위해 배운 교훈을 수집하는 것이 중요합니다.

요약하면 알려진 안전한 작업으로의 반환을 용이하게 하는 복구 프로세스를 구현하는 것이 중요합니다. 복구에는 오랜 시간이 걸릴 수 있으며, 비즈니스 영향과 재감염 위험 간의 균형을 맞추려면 억제 전략과의 밀접한 연결이 필요합니다. 복구 절차에는 리소스 및 서비스, IAM 보안 주체를 복원하고 계정의 보안 검토를 수행하여 잔여 위험을 평가하는 단계가 포함되어야 합니다.

결론

각 운영 단계에는 고유한 목표, 기법, 방법론 및 전략이 있습니다. 표 4에는 이러한 단계와이 섹션에서 다루는 몇 가지 기법 및 방법론이 요약되어 있습니다.

표 4 - 운영 단계: 목표, 기법 및 방법론

Phase(단계)	목표	기법 및 방법론
감지	잠재적 보안 이벤트를 파악합니다.	• 탐지를 위한 보안 제어 • 동작 및 규칙 기반 감지 • 사람 기반 탐지
분석	보안 이벤트가 인시던트인지 확인하고 인시던트의 범위를 평가합니다.	• 알림 검증 및 범위 지정 • 로그 쿼리 • 위협 인텔리전스 • 자동화
격납	보안 이벤트의 영향을 최소화하고 제한합니다.	• 소스 격리 • 기술 및 액세스 억제 • 대상 봉쇄
근절	보안 이벤트와 관련된 승인되지 않은 리소스 또는 아티팩트를 제거합니다.	• 손상되거나 승인되지 않은 자격 증명 교체 또는 삭제 • 무단 리소스 삭제 • 맬웨어 제거 • 보안 스캔

Phase(단계)	목표	기법 및 방법론
복구	시스템을 정상 상태로 복원하고 이러한 시스템을 모니터링하여 위협이 반환되지 않도록 합니다.	• 백업에서 시스템 복원 • 처음부터 다시 빌드된 시스템 • 손상된 파일이 클린 버전으로 대체됨

인시던트 사후 활동

위협 환경은 끊임없이 변화하므로 환경을 효과적으로 보호할 수 있는 조직의 역량도 그에 못지않게 역동적으로 대처하는 것이 중요합니다. 지속적인 개선의 핵심은 인시던트 및 시뮬레이션의 결과를 반복하여 가능한 보안 인시던트를 효과적으로 탐지, 대응 및 조사하는 기능을 개선하고, 가능한 취약성, 대응 시간 및 안전한 운영으로의 복귀를 줄이는 것입니다. 다음 메커니즘은 조직이 상황에 관계없이 효과적으로 대응할 수 있는 최신 역량과 지식을 갖추고 있는지 확인하는 데 도움이 될 수 있습니다.

인시던트에서 학습하기 위한 프레임워크 설정

학습한 교훈 프레임워크 및 방법론을 구현하면 인시던트 대응 기능을 개선하는 데 도움이 될 뿐만 아니라 인시던트가 반복되지 않도록 방지하는 데도 도움이 됩니다. 각 인시던트에서 학습하면 동일한 실수, 노출 또는 잘못된 구성을 반복하지 않도록 하여 보안 태세를 개선할 뿐만 아니라 예방 가능한 상황에 드는 시간을 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 구현하려면 어떻게 해야 할까요?

나열된 이러한 상위 수준 결과 외에도 프로세스에서 가장 많은 가치(실행 가능한 개선으로 이어지는 정보)를 도출하려면 올바른 질문을 해야 합니다. 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 도구를 사용하여 인시던트를 효과적으로 조사(검색/분석)할 수 있었습니까?
- 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?
- 추가를 구현하고 테스트monitoring/preventative controls/process할 타임라인은 어떻게 됩니까?

이 목록은 모든 것을 포함하는 것은 아닙니다. 조직 및 비즈니스 요구 사항이 무엇인지, 인시던트에서 가장 효과적으로 배우고 보안 태세를 지속적으로 개선하기 위해 이를 분석하는 방법을 식별하는 출발

점 역할을 하기 위한 것입니다. 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. 지표가 없으면 조직이 얼마나 잘 수행하고 있는지(또는 얼마나 잘 수행하고 있는지) 정확하게 측정하거나 식별할 수 있는 기준이 없습니다. 운영 우수성을 위한 노력에 대한 기대치와 참조를 설정하려는 조직에 좋은 출발점인 인시던트 대응에 공통적인 몇 가지 지표가 있습니다.

평균 감지 시간

평균 탐지 시간은 가능한 보안 인시던트를 발견하는 데 걸리는 평균 시간입니다. 특히이 시간은 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 않음을 확인하는 데 중요합니다.

평균 탐지 시간이 높을수록 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. 특히 알림 생성과 처리 알림을 식별하고 우선 순위를 지정하는 SOC 또는 인시던트 대응 직원의 구성원 사이의 시간입니다.

이 지표를 사용하여 팀이 알림을 얼마나 잘 처리하고 우선순위를 정하고 있는지 추적할 수 있습니다. 팀이 알림을 효과적으로 식별하고 우선 순위를 지정할 수 없는 경우 응답이 지연되고 비효율적입니다.

평균 승인 시간이 높을수록 팀이 적절한 리소스와 훈련을 모두 갖추고 있는지 확인하여 대응을 위해 가능한 보안 인시던트를 신속하게 승인하고 우선 순위를 지정해야 합니다. 평균 승인 시간이 짧을수록 팀이 보안 알림에 더 잘 대응하여 효과적으로 준비되고 우선순위를 잘 정할 수 있음을 보여줍니다.

평균 응답 시간

평균 대응 시간은 가능한 보안 인시던트에 대한 초기 대응을 시작하는 데 걸리는 평균 시간입니다. 특히, 이는 가능한 보안 인시던트의 초기 알림 또는 발견과 대응을 위해 취해진 첫 번째 조치 사이의 시간

입니다. 이는 평균 승인 시간과 유사하지만 상황에 대한 간단한 인식 또는 승인과 비교하여 특정 응답 작업(예: 시스템 데이터 획득, 시스템 포함)을 측정하는 것입니다.

이 지표를 사용하여 보안 인시던트에 대응할 준비를 추적할 수 있습니다. 앞서 언급한 것처럼 준비는 효과적인 대응의 핵심입니다. 이 문서의 the section called “준비” 섹션을 참조하세요.

평균 대응 시간이 높을수록 대응 프로세스를 효과적으로 문서화하고 활용할 수 있도록 팀이 모두 대응 방법에 대한 적절한 교육을 받았는지 확인해야 할 필요성이 커집니다. 평균 대응 시간이 짧을수록 팀이 식별된 알림에 대한 적절한 대응을 식별하고 안전한 운영으로의 여정을 다시 시작하는 데 필요한 대응 조치를 수행하는 것이 좋습니다.

평균 포함 시간

평균 포함 시간은 가능한 보안 인시던트를 포함시키는 데 걸리는 평균 시간입니다. 특히, 이는 가능한 보안 인시던트의 초기 알림 또는 발견과 공격자 또는 손상된 시스템이 추가 피해를 입지 않도록 효과적으로 방지하는 대응 조치 완료 사이의 시간입니다.

이 지표를 사용하여 팀이 가능한 보안 인시던트를 얼마나 잘 완화하거나 억제할 수 있는지 추적할 수 있습니다. 가능한 보안 인시던트를 빠르고 효과적으로 억제할 수 없으면 영향, 범위 및 추가 침해 가능성에 대한 노출이 증가합니다.

평균 억제 시간이 높을수록 경험하고 있는 보안 인시던트를 빠르고 효과적으로 완화하고 억제하기 위해 지식과 기능을 모두 구축해야 할 필요성이 커집니다. 평균 억제 시간이 짧을수록 팀이 비즈니스에 미치는 영향, 범위 및 위험을 줄이기 위해 식별된 위협을 완화하고 억제하는 데 필요한 조치를 더 잘 이해하고 채택할 수 있습니다.

평균 복구 시간

평균 복구 시간은 가능한 보안 인시던트에서 안전한 작업을 완전히 반환하는 데 걸리는 평균 시간입니다. 특히, 이는 가능한 보안 인시던트의 초기 알림 또는 발견 시점과 인시던트의 영향을 받지 않고 비즈니스가 정상적이고 안전하게 운영되는 시점 사이의 시간입니다.

이 지표를 사용하여 보안 인시던트 후 팀이 시스템, 계정 및 환경을 안전한 운영으로 되돌리는 데 얼마나 효과적인지 추적할 수 있습니다. 안전한 운영으로 신속하게 또는 효과적으로 복귀할 수 없는 것은 보안에 영향을 미칠 뿐만 아니라 비즈니스 및 운영에 대한 영향과 비용을 증가시킬 수 있습니다.

평균 복구 시간이 높을수록 보안 인시던트가 운영 및 비즈니스에 미치는 영향을 최소화하기 위해 적절한 메커니즘(예: 장애 조치 프로세스 및 CI/CD 파이프라인을 안전하게 재배포)을 갖추도록 팀과 환경을 준비해야 할 필요성이 커집니다. 평균 복구 시간이 짧을수록 팀이 운영 및 비즈니스에 대한 보안 인시던트의 영향을 최소화하는 데 더 효과적입니다.

공격자 체류 시간

공격자 체류 시간은 권한이 없는 사용자가 시스템 또는 환경에 액세스할 수 있는 평균 시간입니다. 이는 공격자가 초기 알림 또는 검색보다 빠를 수 있는 시스템 또는 환경에 대한 액세스 권한을 얻은 초기 시간으로 시작되는 기간을 제외하고 평균 포함 시간과 유사합니다.

이 지표를 사용하여 공격자 또는 위협이 환경에 영향을 미치는 시간, 액세스 및 기회를 줄이기 위해 시스템 및 메커니즘이 모두 얼마나 잘 작동하는지 추적할 수 있습니다. 공격자 체류 시간을 줄이는 것이 팀과 비즈니스의 최우선 과제가 되어야 합니다.

공격자 체류 시간이 높을수록 환경에서 위협 또는 공격의 영향과 범위를 최소화하는 팀의 능력을 보장하기 위해 인시던트 대응 프로세스의 어떤 부분을 개선해야 하는지 식별할 필요가 커집니다. 공격자 체류 시간이 짧을수록 팀이 환경 내에서 위협 또는 공격자가 갖는 시간과 기회를 최소화하여 운영 및 비즈니스에 미치는 위험과 영향을 줄일 수 있습니다.

지표 요약

인시던트 대응에 대한 지표를 설정하고 추적하면 인시던트 대응 기능을 효과적으로 측정, 평가 및 개선할 수 있습니다. 이를 위해이 단원에서 강조 표시된 여러 가지 일반적인 인시던트 대응 지표가 있습니다. 표 5에는 이러한 지표가 요약되어 있습니다.

표 5 - 인시던트 대응 지표

지표	설명
평균 감지 시간	가능한 보안 인시던트를 발견하는 데 걸리는 평균 시간
평균 승인 시간	가능한 보안 인시던트를 승인(및 우선 순위 지정)하는 데 걸리는 평균 시간
평균 응답 시간	가능한 보안 인시던트에 대한 초기 응답을 시작하는 데 걸리는 평균 시간
평균 포함 시간	가능한 보안 인시던트를 포함하는 데 걸리는 평균 시간
평균 복구 시간	가능한 보안 인시던트에서 안전한 작업을 완전히 반환하는 데 걸리는 평균 시간

지표	설명
공격자 체류 시간	공격자가 시스템 또는 환경에 액세스할 수 있는 평균 시간

손상 지표 사용(IOCs)

손상 지표(IOC)는 네트워크, 시스템 또는 환경에서 관찰되는 아티팩트로서, (신뢰도가 높은) 악성 활동이나 보안 인시던트를 식별할 수 있습니다.는 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 등 다양한 형태로 존재할 IOCs 수 있습니다. 또한 시스템에 특정 항목 또는 아티팩트가 존재하는지 여부(특정 파일 또는 파일 및 레지스트리 항목 세트), 특정 순서로 수행되는 작업(특정 IP에서 시스템에 로그인한 다음 특정 이상 명령 수행) 또는 특정 위협, 공격 또는 공격자 방법론을 나타낼 수 있는 네트워크 활동(특정 도메인에서 오가는 비정상적인 인바운드 또는 아웃바운드 트래픽)과 같은 항목 또는 활동의 조합일 수 있습니다.

인시던트 대응 프로그램을 반복적으로 개선하기 위해 노력할 때 탐지 및 알림을 지속적으로 구축하고 개선하며 조사의 속도와 효율성을 개선하기 위한 메커니즘IOCs으로 수집, 관리 및 활용하는 프레임워크를 구현해야 합니다. 의 수집 및 관리를 인시던트 대응 프로세스의 IOCs 분석 및 조사 단계에 통합하여 시작할 수 있습니다. 프로세스의 표준 부분IOCs으로 선제적으로 식별, 수집 및 저장하면 데이터 리포지토리(보다 포괄적인 위협 인텔리전스 프로그램의 일부)를 구축하여 기존 탐지 및 알림을 개선하고, 추가 탐지 및 알림을 구축하고, 이전에 아티팩트가 발견된 장소와 시기를 식별하고IOCs, 일치하는와 관련하여 이전에 조사가 수행된 방식에 대한 설명서를 구축하고 참조할 수 있습니다.

지속적인 교육 및 훈련

교육과 훈련은 의도적으로 추구하고 유지해야 하는 진화하고 지속적인 노력입니다. 팀이 진화하는 기술 상태 및 위협 환경에 상응하는 인식, 지식 및 기능을 유지하고 있는지 확인하는 다양한 메커니즘이 있습니다.

한 가지 메커니즘은 지속적인 교육을 팀의 목표 및 운영의 표준 부분으로 사용하는 것입니다. 준비 섹션에서 언급한 대로 인시던트 대응 직원과 이해관계자는 내부 인시던트를 감지, 대응 및 조사하는 방법에 대한 교육을 효과적으로 받아야 합니다 AWS. 그러나 교육은 “하나의 노력으로 이루어진” 노력이 아닙니다. 팀이 대응의 효율성과 효과를 개선하는 데 활용할 수 있는 최신 기술 발전, 업데이트 및 개선 사항과 조사 및 분석을 개선하는 데 활용할 수 있는 데이터에 대한 추가 또는 업데이트를 지속적으로 파악하고 있는지 확인해야 합니다.

또 다른 메커니즘은 시뮬레이션이 정기적으로(예: 분기별) 수행되고 비즈니스의 특정 결과에 초점을 맞추고 있는지 확인하는 것입니다. 이 문서의 the section called “정기적인 시뮬레이션 실행” 섹션을 참조하세요.

초기 모의 연습을 실행하는 것은 개선을 위한 초기 기준을 생성하는 훌륭한 방법이지만 지속적 테스트는 지속적인 개선과 up-to-date 현재 운영 상태를 정확하게 반영하는 데 중요합니다. 가장 중요한 최신 보안 상황과 가장 중요하거나 최신 대응 기능을 테스트하고, 다시 학습한 교훈을 교육, 운영 및 프로세스/절차에 통합하면 대응 프로세스와 프로그램을 전체적으로 지속적으로 개선할 수 있는지 확인할 수 있습니다.

결론

클라우드 여정을 계속하면서 AWS 환경에 대한 기본 보안 인시던트 대응 개념을 고려하는 것이 중요합니다. 사용 가능한 제어, 클라우드 기능 및 문제 해결 옵션을 결합하여 클라우드 환경의 보안을 개선할 수 있습니다. 또한 응답 속도를 개선하는 자동화 기능을 채택하면 작게 시작하고 반복할 수 있으므로 보안 이벤트가 발생할 때 더 잘 대비할 수 있습니다.

기여자

이 문서의 현재 및 과거 기여자는 다음과 같습니다.

- Anna McAbee, Amazon Web Services의 Senior Security Solutions Architect
- Freddy Kasprzykowski, Amazon Web Services의 선임 보안 컨설턴트
- Jason Hurst, Amazon Web Services의 선임 보안 엔지니어
- Jonathon Poling, Amazon Web Services의 보안 컨설턴트
- Josh Du Lac, Amazon Web Services의 보안 솔루션 아키텍처 담당 선임 관리자
- Paco Hope, Amazon Web Services의 보안 수석 엔지니어
- Ryan Tick, Amazon Web Services의 선임 보안 엔지니어
- Steve de Vera, Amazon Web Services 선임 보안 엔지니어

부록 A: 클라우드 기능 정의

AWS 는 200개 이상의 클라우드 서비스와 수천 가지 기능을 제공합니다. 이러한 기능 중 다수는 네이티브 탐지, 예방 및 대응 기능을 제공하며, 사용자 지정 보안 솔루션을 설계하는 데 사용할 수 있는 기능

도 있습니다. 이 섹션에는 클라우드의 인시던트 대응과 가장 관련성이 높은 서비스의 하위 집합이 포함되어 있습니다.

주제

- 로깅 및 이벤트
- 가시성 및 알림
- 자동화
- 보안 스토리지
- 미래 및 사용자 지정 보안 기능

로깅 및 이벤트

AWS CloudTrail - AWS 계정의 거버넌스, 규정 준수, 운영 감사 및 위험 감사를 지원하는 AWS CloudTrail 서비스입니다. CloudTrail를 사용하면 AWS 서비스 전반의 작업과 관련된 계정 활동을 로깅, 지속적인 모니터링 및 유지할 수 있습니다. CloudTrail 는 AWS Management Console, AWS SDKs, 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. CloudTrail 는 두 가지 유형의 AWS API 작업을 로깅합니다.

- CloudTrail 관리 이벤트(컨트롤 플레인 작업이라고도 함)는 계정의 AWS 리소스에서 수행되는 관리 작업을 표시합니다. 여기에는 Amazon S3 버킷 생성 및 로깅 설정과 같은 작업이 포함됩니다.
- CloudTrail 데이터 이벤트(데이터 영역 작업이라고도 함)는 계정 AWS 의 리소스에서 또는 리소스 내에서 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 호출 활동과 같은 작업이 포함됩니다.

AWS Config – 고객이 AWS 리소스 구성을 평가, 감사 및 평가할 수 있는 서비스입니다. AWS Config AWS Config 는 AWS 리소스 구성을 지속적으로 모니터링 및 기록하고 원하는 구성에 대해 기록된 구성의 평가를 자동화할 수 있습니다. AWS Config를 사용하면 리소스 간 구성 및 관계의 변경 사항을 AWS 수동 또는 자동으로 검토하고, 자세한 리소스 구성 기록을 검토하고, 고객 지침에 지정된 구성에 대한 전반적인 규정 준수를 확인할 수 있습니다. 이를 통해 규정 준수 감사, 보안 분석, 변경 관리 및 운영 문제 해결을 간소화할 수 있습니다.

Amazon EventBridge - Amazon은 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트의 거의 실시간 스트림을 제공하거나에서 API 호출을 게시할 때 EventBridge 이를 제공합니다 AWS CloudTrail. 빠르게 설정할 수 있는 간단한 규칙을 사용하여 이벤트를 일치시키고 하나 이상의 대상 함수 또는 streams

로 라우팅할 수 있습니다. EventBridge 는 발생하는 운영 변경 사항을 인식합니다. EventBridge 는 환경에 응답하기 위해 메시지를 보내고, 함수를 활성화하고, 변경을 수행하고, 상태 정보를 캡처하여 이러한 운영 변경 사항에 응답하고 필요에 따라 수정 조치를 취할 수 있습니다. Amazon과 같은 일부 보안 서비스는 EventBridge 이벤트 형태로 출력을 GuardDuty생성합니다. 또한 많은 보안 서비스는 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 자체에 대한 변경 사항(액세스 정책 및 수명 주기 정책 변경 등)을 기록하는 CloudTrail 로그와 별개이며 그 외에도 별개입니다. 액세스 로그 레코드는 최선의 노력을 다해 전달된다는 점에 유의해야 합니다. 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 운영 체제, 애플리케이션 및 기타 소스에서 생성된 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다EC2 CloudWatch . CloudWatch 로그는 Route 53 DNS 쿼리 AWS CloudTrail, VPC 흐름 로그, Lambda 함수 등의 대상이 될 수 있습니다. 그런 다음 고객은 Logs에서 연결된 CloudWatch 로그 데이터를 검색할 수 있습니다.

Amazon VPC 흐름 로그 - VPC 흐름 로그를 통해 고객은의 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 캡처할 수 있습니다VPCs. 흐름 로그를 활성화한 후 Amazon CloudWatch Logs 및 Amazon S3로 스트리밍할 수 있습니다. VPC Flow Logs는 특정 트래픽이 인스턴스에 도달하지 않는 이유의 문제 해결, 지나치게 제한적인 보안 그룹 규칙 진단, 이를 보안 도구로 사용하여 EC2 인스턴스에 대한 트래픽을 모니터링하는 등 다양한 작업을 수행하는 고객에게 도움이 됩니다. 최신 버전의 VPC 흐름 로깅을 사용하여 가장 강력한 필드를 가져옵니다.

AWS WAF 로그 - 서비스가 검사하는 모든 웹 요청에 대한 전체 로깅을 AWS WAF 지원합니다. 고객은 이를 Amazon S3에 저장하여 규정 준수 및 감사 요구 사항과 디버깅 및 포렌식을 충족할 수 있습니다. 이러한 로그는 고객이 시작된 규칙 및 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) 내 리소스에서 수행한 모든 DNS 쿼리를 로깅할 수 있습니다VPC. Amazon EC2 인스턴스, AWS Lambda 함수 또는 컨테이너이든 관계없이 Amazon에 상주VPC하고 DNS 쿼리를 수행하는 경우이 기능은 이를 로깅합니다. 그러면 애플리케이션이 작동하는 방식을 탐색하고 더 잘 이해할 수 있습니다.

기타 AWS 로그 - 새로운 로깅 및 모니터링 기능을 사용하는 고객을 위해 서비스 기능을 AWS 지속적으로 릴리스합니다. 각 AWS 서비스에 사용할 수 있는 기능에 대한 자세한 내용은 퍼블릭 설명서를 참조하세요.

가시성 및 알림

AWS Security Hub - AWS 고객에게 계정 전반의 우선 순위가 높은 보안 알림 및 규정 준수 상태를 포괄적 AWS Security Hub 으로 보여줍니다. Security Hub는 Amazon, Amazon Inspector, GuardDutyAmazon Macie 및 AWS Partner 솔루션과 같은 AWS 서비스의 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. Amazon Inspector 조사 결과는 실행 가능한 그래프 및 테이블과 함께 통합 대시보드에 시각적으로 요약됩니다. 또한 조직이 따르는 AWS 모범 사례 및 업계 표준에 따라 자동화된 규정 준수 검사를 사용하여 환경을 지속적으로 모니터링할 수 있습니다.

Amazon GuardDuty - Amazon GuardDuty 은 고객이 AWS 계정과 워크로드를 보호하는 데 도움이 되도록 악의적이거나 승인되지 않은 동작을 지속적으로 모니터링하는 관리형 위협 탐지 서비스입니다. Amazon EC2 인스턴스, Amazon S3 버킷의 계정 또는 리소스 손상 가능성 또는 악의적인 공격자의 정찰을 나타내는 비정상적인 API 호출 또는 잠재적으로 승인되지 않은 배포와 같은 활동을 모니터링합니다.

GuardDuty 는 기계 학습을 사용하여 계정 및 워크로드 활동에서 이상을 탐지하는 통합 위협 인텔리전스 피드를 통해 의심스러운 공격자를 식별합니다. 잠재적 위협이 감지되면 서비스는 GuardDuty 콘솔 및 CloudWatch 이벤트에 자세한 보안 알림을 전송합니다. 따라서 알림을 실행 가능하고 기존 이벤트 관리 및 워크플로 시스템에 쉽게 통합할 수 있습니다.

GuardDuty 또한는 Amazon GuardDuty for Amazon S3 보호 및 Amazon GuardDuty for Amazon EKS 보호라는 특정 서비스의 위협을 모니터링할 수 있는 두 가지 추가 기능을 제공합니다. Amazon S3 보호를 사용하면 GuardDuty 가 객체 수준 API 작업을 모니터링하여 Amazon S3 버킷 내의 데이터에 대한 잠재적 보안 위험을 식별할 수 있습니다. Kubernetes 보호를 사용하면가 Amazon 내에서 의심스러운 활동 및 Kubernetes 클러스터의 잠재적 손상을 감지 GuardDuty 할 수 있습니다EKS.

Amazon Macie - Amazon Macie는에 저장된 민감한 데이터를 자동으로 검색, 분류 및 보호하여 데이터 손실을 방지하는 데 도움이 되는 AI 기반 보안 서비스입니다 AWS. 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 감지하면 알림을 전송합니다.

AWS Config 규칙 - AWS Config 규칙은 리소스에 대한 기본 구성을 나타내며에서 기록한 대로 관련 리소스의 구성 변경 사항에 대해 평가됩니다 AWS Config. 대시보드에서 리소스 구성에 대해 규칙을 평가한 결과를 볼 수 있습니다. AWS Config 규칙을 사용하여 구성 관점에서 전체 규정 준수 및 위험 상태를 평가하고, 시간 경과에 따른 규정 준수 추세를 보고, 리소스가 규칙을 준수하지 않는 구성 변경을 찾을 수 있습니다.

AWS Trusted Advisor – AWS Trusted Advisor 는 AWS 환경을 최적화하여 비용을 절감하고 성능을 높이며 보안을 개선하는 데 도움이 되는 온라인 리소스입니다.는 AWS 모범 사례를 따라 리소스를 프로비저닝하는 데 도움이 되는 실시간 지침을 Trusted Advisor 제공합니다. CloudWatch 이벤트 통합을 포함한 전체 Trusted Advisor 검사 세트는 비즈니스 및 엔터프라이즈 지원 플랜 고객이 사용할 수 있습니다.

Amazon CloudWatch - Amazon CloudWatch 은 리소스 및 실행 중인 애플리케이션에 대한 AWS 클라우드 모니터링 서비스입니다 AWS. CloudWatch 를 사용하여 지표를 수집 및 추적하고, 로그 파일을 수집 및 모니터링하고, 경보를 설정하고, AWS 리소스의 변경 사항에 자동으로 대응할 수 있습니다. CloudWatch 는 Amazon EC2 인스턴스, Amazon DynamoDB 테이블, Amazon RDS DB 인스턴스와 같은 AWS 리소스와 애플리케이션 및 서비스에서 생성된 사용자 지정 지표, 애플리케이션이 생성하는 모든 로그 파일을 모니터링할 수 있습니다. Amazon CloudWatch 을 사용하여 리소스 사용률, 애플리케이션 성능 및 운영 상태에 대한 시스템 전반의 가시성을 얻을 수 있습니다. 이러한 인사이트를 사용하여 그에 따라 대응하고 애플리케이션을 원활하게 실행할 수 있습니다.

Amazon Inspector - Amazon Inspector는 배포된 애플리케이션의 보안 및 규정 준수를 개선하는 데 도움이 되는 자동화된 보안 평가 서비스입니다 AWS. Amazon Inspector는 자동으로 애플리케이션의 취약점 또는 모범 사례와의 차이를 평가합니다. 평가를 수행한 후 Amazon Inspector는 심각도 수준에 따라 우선 순위가 지정된 보안 조사 결과의 세부 목록을 생성합니다. 이러한 결과는 Amazon Inspector 콘솔 또는를 통해 사용할 수 있는 세부 평가 보고서의 일부로 직접 검토할 수 있습니다API.

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 로그와 같은 여러 데이터 소스에서 수조 개의 이벤트를 분석할 수 있으며 CloudTrail, 리소스 GuardDuty, 사용자 및 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰를 자동으로 생성합니다. 이 통합 보기를 사용하면 모든 세부 정보와 컨텍스트를 한 곳에서 시각화하여 조사 결과의 기본 원인을 식별하고, 관련 과거 활동을 자세히 살펴보고, 근본 원인을 신속하게 확인할 수 있습니다.

자동화

AWS Lambda – AWS Lambda 는 이벤트에 대한 응답으로 코드를 실행하고 기본 컴퓨팅 리소스를 자동으로 관리하는 서버리스 컴퓨팅 서비스입니다. Lambda를 사용하여 사용자 지정 로직으로 다른 AWS 서비스를 확장하거나 AWS 규모, 성능 및 보안으로 작동하는 자체 백엔드 서비스를 생성할 수 있습니다. Lambda는 고가용성 컴퓨팅 인프라에서 코드를 실행하고 컴퓨팅 리소스를 자동으로 관리합니다. 여기에는 서버 및 운영 체제 유지 관리, 용량 프로비저닝 및 자동 조정, 코드 및 보안 패치 배포, 코드 모니터링 및 로깅이 포함됩니다. 코드를 입력하기만 하면 됩니다.

AWS Step Functions - 시각적 워크플로를 사용하여 분산 애플리케이션 및 마이크로서비스의 구성 요소를 AWS Step Functions 간단하게 조정할 수 있습니다. Step Functions는 애플리케이션의 구성 요소를 일련의 단계로 정렬하고 시각화할 수 있는 그래픽 콘솔을 제공합니다. 따라서 다단계 애플리케이션을 간단하게 빌드하고 실행할 수 있습니다. Step Functions는 각 단계를 자동으로 시작하고 추적하며 오류가 있을 때 재시도하므로 애플리케이션이 예상대로 순서대로 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 Functions 는 AWS Serverless의 일부이며 서버리스 애플리케이션의 AWS Lambda 함수를 쉽게 오케스트레이션할 수 있습니다. Amazon EC2 및 Amazon과 같은 컴퓨팅 리소스를 사용하여 마이크로서비스 오케스트레이션에 Step Functions를 사용할 수도 있습니다ECS.

AWS Systems Manager - 인프라에 대한 가시성과 제어를 AWS Systems Manager 제공합니다 AWS. Systems Manager는 여러 AWS 서비스의 운영 데이터를 볼 수 있는 통합 사용자 인터페이스를 제공하며 AWS 리소스 전체에서 운영 작업을 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, 애플리케이션 업데이트 또는 셸 스크립트 실행과 같은 온디맨드 변경을 수행하고, 기타 자동화 및 패치 작업을 수행할 수 있습니다.

보안 스토리지

Amazon Simple Storage Service - Amazon S3는 어디서나 원하는 양의 데이터를 저장하고 검색하도록 구축된 객체 스토리지입니다. 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 충족할 수 있도록 설계되었습니다. 이를 통해 고객은 비용 최적화, 액세스 제어 및 규정 준수를 위해 데이터를 관리하는 데 사용하는 메서드에서 유연성을 얻을 수 있습니다. Amazon S3는 query-in-place Amazon S3의 저장 데이터에 대해 강력한 분석을 직접 실행할 수 있는 기능을 제공합니다. Amazon S3는 서드 파티 솔루션, 시스템 통합자 파트너 및 기타 서비스의 가장 큰 커뮤니티 중 하나에서 통합되는 고도로 지원되는 클라우드 스토리지 AWS 서비스입니다.

Amazon S3 Glacier – Amazon S3 Glacier는 데이터 아카이빙 및 장기 백업을 위한 안전하고 내구성이 뛰어나며 매우 저렴한 클라우드 스토리지 서비스입니다. 99.999999999%의 내구성을 제공하고, 포괄적인 보안을 제공하며, 규제 요구 사항을 충족할 수 있도록 설계되었습니다. S3 Glacier는 query-in-place 저장된 아카이브 데이터에 대해 강력한 분석을 직접 실행할 수 있는 기능을 제공합니다. 비용을 낮게 유지하면서 다양한 검색 요구 사항에 적합하도록 S3 Glacier는 몇 분에서 몇 시간까지 아카이브에 액세스할 수 있는 세 가지 옵션을 제공합니다.

미래 및 사용자 지정 보안 기능

앞서 언급한 서비스 및 기능은 전체 목록이 아닙니다. AWS 는 지속적으로 새 기능을 추가합니다. 자세한 내용은 및 AWS 클라우드 보안의 새로운 기능 AWS 페이지를 검토하는 것이 좋습니다. 가 네이티브 클라우드 서비스로 AWS 제공하는 보안 서비스 외에도 AWS 서비스 외에도 자체 기능을 구축하는 데 관심이 있을 수 있습니다.

Amazon GuardDuty및 AWS CloudTrail Amazon Macie와 같은 계정 내 기본 보안 서비스 세트를 활성화하는 것이 좋지만, 로그 자산에서 추가 가치를 도출하기 위해 이러한 기능을 확장하는 것이 좋습니다. APN Security Competency 프로그램에 나열된 도구와 같이 사용할 수 있는 여러 파트너 도구가 있습니다. 로그를 검색하기 위해 자체 쿼리를 작성할 수도 있습니다. 가 AWS 제공하는 관리형 서비스가 매우 많아지면서 이보다 더 쉬워졌습니다. Amazon Athena, Amazon OpenSearch Service, Amazon, Amazon Machine Learning, QuickSightAmazon와 같이이 문서의 범위를 벗어나는 조사를 지원할 수 있는 많은 추가 AWS 서비스가 있습니다EMR. Amazon Machine Learning

부록 B: AWS 인시던트 응답 리소스

AWS 는 고객이 인시던트 대응 기능을 개발하는 데 도움이 되는 리소스를 게시합니다. 대부분의 예제 코드 및 절차는 외부 GitHub 퍼블릭 AWS 리포지토리에서 찾을 수 있습니다. 다음은 인시던트 대응 수행 방법의 예를 제공하는 몇 가지 리소스입니다.

플레이북 리소스

- 사고 대응 플레이북용 프레임워크 - 고객이 AWS 서비스를 사용할 때 잠재적 공격 시나리오에 대비하여 보안 플레이북을 생성, 개발 및 통합할 수 있는 프레임워크의 예입니다.
- 자체 인시던트 대응 플레이북 개발 -이 워크숍은 인시던트 대응 플레이북 개발에 익숙해질 수 있도록 설계되었습니다 AWS.
- 인시던트 대응 플레이북 샘플 - AWS 고객이 직면한 일반적인 시나리오를 다루는 플레이북입니다.
- Jupyter 플레이북 및 CloudTrail Lake를 사용하여 AWS 인시던트 대응 런북 구축 -이 워크숍에서는 Jupyter 노트북 및 CloudTrail Lake를 사용하여 환경에 AWS 맞는 인시던트 대응 플레이북을 구축하는 방법을 안내합니다.

포렌식 리소스

- 자동화된 인시던트 대응 및 포렌식 프레임워크 -이 프레임워크 및 솔루션은 억제, 획득, 검사 및 분석 단계로 구성된 표준 디지털 포렌식 프로세스를 제공합니다. AWS " 함수를 활용하여 자동화된 반복

가능한 방식으로 인시던트 대응 프로세스를 트리거합니다. 자동화 단계를 운영하고, 아티팩트를 저장하고, 포렌식 환경을 생성하기 위해 계정을 분리합니다.

- Amazon용 자동 포렌식 오케스트레이터 EC2 -이 구현 가이드는 잠재적 보안 문제가 감지되는 경우 포렌식 분석을 위해 EC2 인스턴스 및 연결된 볼륨에서 데이터를 캡처하고 검사하는 셀프 서비스 솔루션을 제공합니다. 솔루션을 배포하기 위한 AWS CloudFormation 템플릿이 있습니다.
- 에서 포렌식 디스크 수집을 자동화하는 방법 AWS -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.

고지 사항

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서: (a) 정보 제공용이며, (b)는 예고 없이 변경될 수 있는 현재 AWS 제품 제공 및 관행을 나타내며, (c) AWS 는 및 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 약속이나 보장도 생성하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떤 종류의 보증, 표현 또는 조건 없이 “있는 그대로” 제공됩니다. 고객에 AWS 대한의 책임과 책임은 AWS 계약에 의해 관리되며,이 문서는 AWS 와 고객 간의 계약의 일부이거나 수정하지 않습니다.

문서 이력

변경 사항	설명	날짜
업데이트됨: 문서에 대한 고객 의견의 업데이트입니다.	https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html을 스택 세트 템플릿으로 업데이트했습니다. triage.security-ir.com 항목을 triage.security-ir.amazonaws.com 수정했습니다. on https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html AWSSupport포함EC2Rescue에 대한 추적된 연결 참고가 추가되었습니다. on https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html의 링크 끊김을 수정했습니다. 멤버십 계정 at https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html에 대한 정의를 추가했습니다. 관리 계정의 https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/using-service-linked-roles.html에 AWS	2024년 12월 20일

변경 사항	설명	날짜
	Organizations 대한 설명 메모를 추가했습니다.	

변경 사항	설명	날짜
업데이트됨: 문서에 대한 고객 의견의 업데이트입니다.	텍스트 AWS AWS 에서 여러 중복을 제거했습니다. https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html and https://docs.aws.amazon.com/security-ir/latest/userguide/servicename-info-in-cloudtrail.html의 끊어진 링크를 수정했습니다. 를 https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html 로 업데이트합니다. 첫 번째 단락에서 >를 제거했습니다. AWSSupport- 포함 EC2Reversible을 AWSSupport- 포함으로 대체했습니다 EC2Instance. AWSSupportContainIAMReversible 를 AWSSupportC로 대체했습니다ontainIAMPrincipal. AWSSupport-ContainS3Reversible AWSSupport-ContainS3Resource로 대체됨. https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/issues.html 형식 업데이트 고객에게 지원 티켓을 CIRT 통해에 문의하도록 지시할 때 https://docs.aws.amazon.com/security-ir/latest/userguide/	2024년 12월 10일

변경 사항	설명	날짜
	understand-response-teams-and-support.html은 이제 지원 양식에서 선택할 수 있는 옵션을 제공합니다. CloudWatch 이벤트를 제거하고 EventBridge on https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html 로 대체했습니다. 문법 업데이트 on https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html . 이 표에서 업데이트로 대체된 게시 날짜를 https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html에서 제거했습니다.	
업데이트됨: AWS 관리형 정책 및 서비스 연결 역할.	관리형 정책 및 서비스 연결 역할에 대한 업데이트입니다.	2024년 12월 1일
서비스 시작	re:Invent 2024에서 서비스 시작을 위한 초기 서비스 문서	2024년 12월 1일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.