AWS 기술 가이드

AWS 보안 인시던트 대응 가이드

AWS 보안 인시던트 대응 가이드: AWS 기술 가이드

Table of Contents

AWS 보안 인시던트 대응 가이드

게시 날짜: 2020년 11월 23일(문서 개정)

이 가이드는 고객의 AWS 클라우드 환경 내에서 보안 인시던트에 대응하는 기본 사항에 대한 개요를 제공합니다. 클라우드 보안 및 인시던트 대응 개념에 대해 간략히 살펴보고 보안 문제에 대응하는 고객이 사용할 수 있는 클라우드 기능, 서비스 및 메커니즘에 대해 알아봅니다.

이 백서는 기술 담당자를 대상으로 하며 정보 보안의 일반 원칙에 익숙하고, 현재 온프레미스 환경의 인시던트 대응에 대한 기본적인 이해를 갖추고 있으며, 클라우드 서비스에 대해 어느 정도 잘 알고 있다고 가정합니다.

소개

AWS에서 가장 우선순위가 높은 것이 보안입니다. AWS 고객은 보안에 매우 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다. AWS 클라우드에서는 공동 책임 모델을 사용합니다. AWS는 클라우드의 보안을 관리합니다. 고객은 클라우드에서의 보안을 책임집니다. 즉, 구현하기로 선택한 보안에 대한 제어 권한을 가집니다. 고객은 보안 목표를 달성하는 데 도움이 되는 수백 가지 도구와 서비스에 액세스할 수 있습니다. 이러한 기능을 통해 클라우드에서 실행되는 애플리케이션에 대한 고객의 목표를 충족하는 보안 기준을 설정할 수 있습니다.

기준과의 편차가 발생하는 경우(예: 잘못된 구성) 이에 대응하고 조사해야 할 수 있습니다. 이를 성공적으로 수행하려면 AWS 환경 내 보안 인시던트 대응의 기본 개념과 보안 문제가 발생하기 전에 클라우드 팀을 준비, 교육 및 훈련하는 데 있어 고려해야 할 문제를 이해해야 합니다. 사용할 수 있는 제어와 기능을 파악하고, 잠재적인 문제를 해결하기 위한 주제별 예를 검토하고, 자동화를 활용하고, 대응 속도를 개선하는 데 활용할 수 있는 문제 해결 방법을 식별하는 것이 중요합니다.

보안 인시던트 대응은 복잡한 주제가 될 수 있으므로 소규모로 시작하여 런북을 개발하고 기본 기능을 활용하고 인시던트 대응 메커니즘의 초기 라이브러리를 만들어 반복하고 개선하는 것이 좋습니다. 이 초기 작업에는 법무 부서와 보안에 관여하지 않는 팀이 포함되어야 하며 이를 통해 인시던트 대응(IR)과 선택한 방법이 기업 목표에 미치는 영향을 더 잘 이해할 수 있습니다.

주제

시작하기 전

이 문서 외에도 보안, 자격 증명 및 규정 준수 모범 사례 및 AWS Cloud Adoption Framework(CAF)의 보안 관점 백서를 검토하는 것이 좋습니다. AWS CAF는 클라우드로 이전하는 조직 내 여러 부서 간의 조정을 지원하는 가이드도 제공합니다. CAF 가이드는 클라우드 기반 IT 시스템 구현과 관련된 몇 가지 중점 영역으로 나뉘며, 이를 관점이라고 합니다. 보안 관점은 여러 작업 흐름에 걸쳐 보안 프로그램을 구현하는 방법을 설명하며 그 중 하나는 인시던트 대응에 중점을 둡니다. 이 문서에서는 AWS가 고객이 해당 작업 흐름에서 성공적인 메커니즘을 평가하고 구현할 수 있도록 지원한 몇 가지 경험에 대해 자세히 설명합니다.

AWS CAF 보안 관점

보안 관점에는 다음 네 가지 요소가 포함됩니다.

- 지시 제어는 환경이 운영되는 범위 내에서 거버넌스, 위험 및 규정 준수 모델을 설정합니다.
- 예방 제어는 워크로드를 보호하고 위협과 취약성을 완화합니다.
- 탐지 제어는 AWS에서 실행하는 배포 작업에 대한 완전한 가시성과 투명성을 제공합니다.
- 대응 제어는 보안 기준에서 벗어날 가능성이 있는 사안을 수정합니다.

IR은 일반적으로 대응 제어 요소 아래에 표시되지만 다른 요소에 종속되며 그 영향을 받습니다. 예를 들어, 지시 제어 및 예방 제어는 기준을 설정하는 데 도움이 되며 이 기준과의 편차를 모니터링하고 조사할 수 있습니다. 이 접근 방식은 노이즈를 제거할 뿐만 아니라 방어 보안을 설계하는 데도 도움을 줍니다.

인시던트 대응의 기초

조직 내 모든 AWS 사용자는 보안 인시던트 대응 프로세스에 대한 기본적인 이해가 있어야 하며, 보안 직원은 보안 문제에 대응하는 방법을 깊이 이해해야 합니다. 보안 이벤트를 처리하기에 앞서 클라우드 인시던트 대응 프로그램은 경험과 교육이 필수적입니다. 클라우드에서 성공적인 인시던트 대응 프로그램의 기초는 교육, 준비, 시뮬레이션 및 반복입니다.

이러한 각 측면을 이해하려면 다음 설명을 살펴보세요.

- 클라우드 기술과 조직에서 이러한 기술을 어떻게 사용하고자 하는지에 대해 보안 운영 및 인시던트 대응에 참여하는 직원을 교육합니다.
- 인시던트 대응팀이 클라우드에서 인시던트를 탐지 및 대응하고, 탐지 기능을 활성화하고, 필요한 도구 및 클라우드 서비스에 대한 적절한 액세스를 보장할 수 있도록 준비시킵니다. 또한 안정적이고 일관된 응답을 보장하는 데 필요한 수동 및 자동 런북을 준비합니다. 다른 팀과 협력하여 예상되는 기준 작업을 설정하고, 해당 지식을 사용하여 정상 운영과의 차이를 파악합니다.
- 클라우드 환경 내에서 예상되는 보안 이벤트와 예기치 않은 보안 이벤트를 모두 시뮬레이션하여 얼마나 효과적으로 준비했는지 확인합니다.
- 시뮬레이션 결과를 반복하여 대응 태세를 강화하고, 가치 창출 시간을 단축하고, 위험을 더 줄입니다.

교육

주제

- 공동 책임
- 클라우드에서의 인시던트 대응
- 클라우드 보안 인시던트
- 클라우드 기능 이해

공동 책임

보안 및 규정 준수는 AWS와 사용자 간의 공동 책임입니다. 이 공동 책임 모델을 통해 고객은 운영 부담을 덜 수 있습니다. AWS가 호스트 운영 체제 및 가상화 계층에서 서비스 운영 시설의 물리적 보안에 이르기까지 구성 요소를 운영, 관리, 제어하기 때문입니다.

고객은 게스트 운영 체제(업데이트 및 보안 패치 포함) 및 애플리케이션 소프트웨어를 관리하고, AWS에서 제공한 보안 제어 항목(예: 보안 그룹, 네트워크 액세스 제어 목록, 자격 증명 및 액세스 관리)을 구성할 책임이 있습니다. 선택한 서비스, 서비스를 IT 환경에 통합하는 과정, 준거법과 규제에 따라 책임 범위가 다르기 때문에 사용하고자 하는 서비스에 대해 신중히 검토해야 합니다. 그림 2는 Amazon Elastic Compute Cloud(Amazon EC2)와 같은 인프라 서비스에 적용되는 공동 책임 모델의 일반적인 형태를 보여 줍니다. 대부분의 책임은 클라우드의 보안(AWS에서 관리)과 클라우드에서의 보안(고객이 관리)이라는 두 가지 범주로 나뉩니다. 사용하는 서비스에 따라 책임이 달라질 수 있습니다. Amazon S3 및 Amazon DynamoDB와 같은 추상화 서비스의 경우 AWS는 인프라 계층, 운영 체제, 플랫폼을 운영하고 고객은 데이터를 저장하고 검색하기 위해 엔드포인트에 액세스합니다. 고객은 데이터 관리(암호화 옵션 포함), 자산 분류, 적절한 허가를 부여하는 IAM 도구 사용에 책임이 있습니다.

그러나 운영 모델을 서비스 공급자에게 이전하는 컨테이너 및 기타 서비스가 추가됨에 따라 공동 책임 모델이 변경됩니다. IaaS 및 데이터 센터에서 벗어나 PaaS로 향하는 운영 모델의 왼쪽으로 이동하면 서비스 공급자의 책임이 커집니다. 고객은 클라우드에서의 책임이 적습니다. 그래프 왼쪽으로 이동하여 마이그레이션을 사용할 때 운영이 더 쉬워집니다. 다음 그림에서 클라우드에서의 운영과 작동의 차이를 유의하여 살펴보세요. 클라우드에서의 공동 책임이 변경됨에 따라 인시던트 대응 또는 포렌식 옵션도 변경됩니다. 고객은 인시던트 대응을 계획하는 동안 운영 모델에서 보유한 기능을 중심으로 계획하고 선택한 모델에서 발생할 수 있는 상호 작용이 발생하기 전에 이를 계획해야 합니다. 이러한 절충점을 계획 및 이해하고 이를 거버넌스 요구 사항과 일치시키는 것은 인시던트 대응의 중요한 단계입니다.

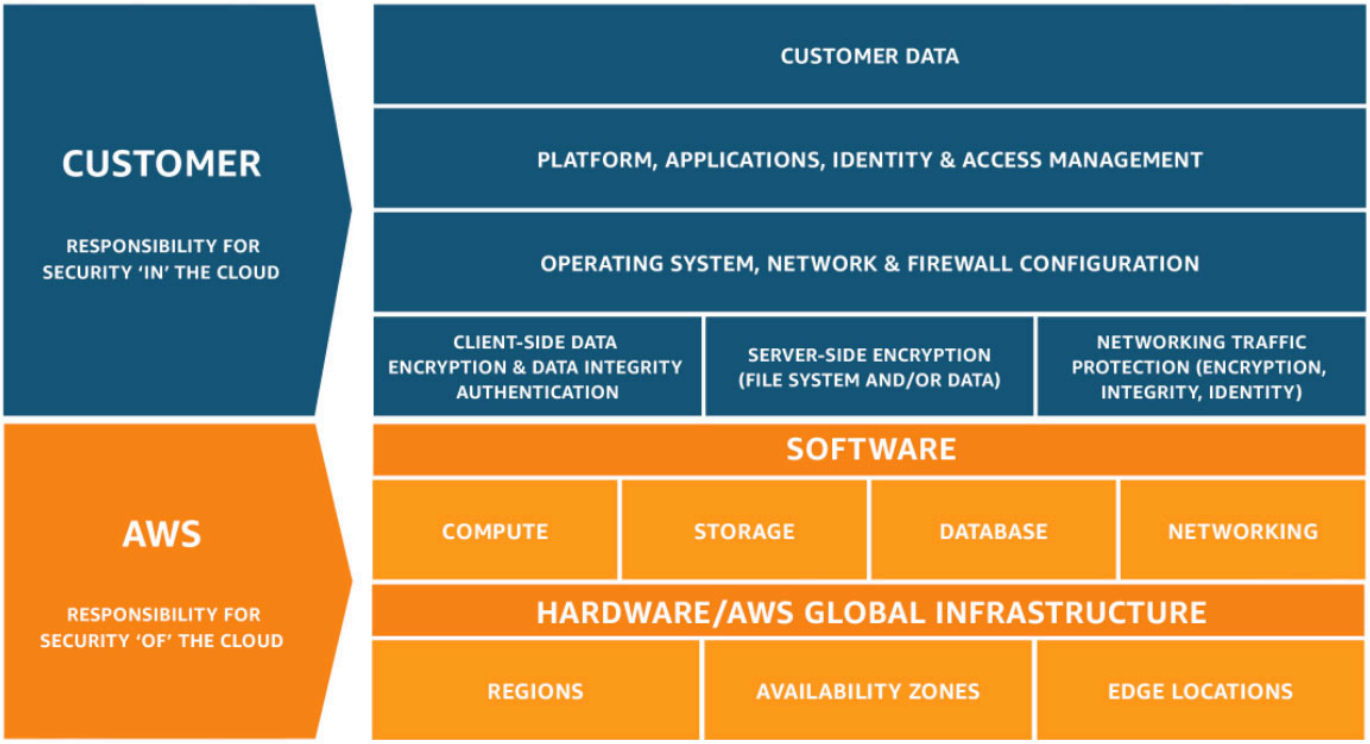
CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

그림 1: 공동 책임 모델

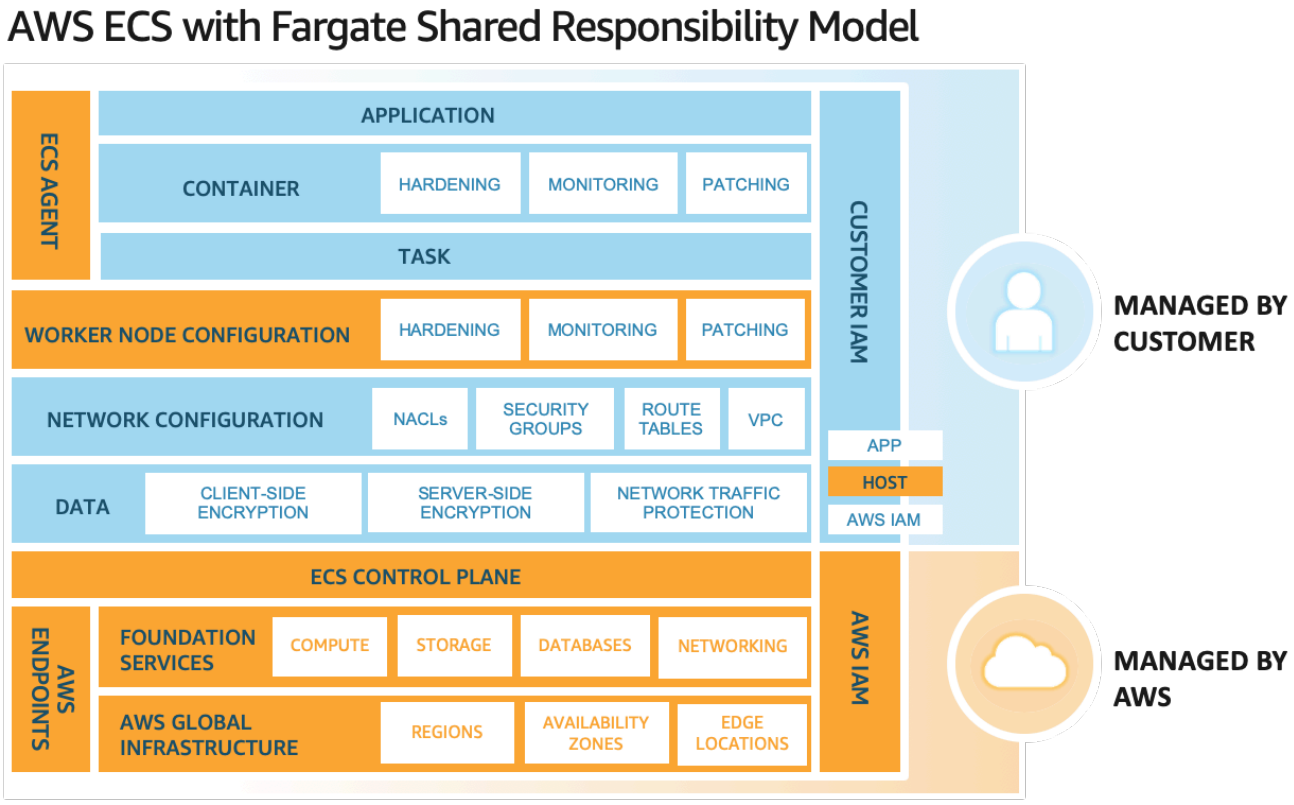

그림 2: AWS Fargate 유형의 공동 책임 모델을 사용하는 Amazon Elastic Container Service(Amazon ECS)

AWS와의 직접적인 관계 외에도 사용하는 책임 모델에서 책임이 있는 다른 단체가 있을 수 있습니다. 예를 들어 운영의 일부 측면을 담당하는 내부 조직 단위가 있을 수 있습니다. 또한 클라우드 기술의 일부를 개발, 관리 또는 운영하는 파트너나 기타 제3자가 있을 수 있습니다.

운영 모델에 맞는 적절한 인시던트 대응 및 포렌식 런북을 만드는 것은 매우 중요합니다. 성공 여부는 선택한 운영 모델에 대해 생성해야 하는 도구 유형 또는 구매해야 하는 도구에 대한 이해에 달려 있습니다. 조직에서 사용 가능한 도구를 더 잘 이해할수록 기업의 GRC(거버넌스 위험 및 규정 준수) 모델 요구 사항을 충족할 수 있도록 더 잘 준비할 수 있습니다.

클라우드에서의 인시던트 대응

클라우드 대응의 설계 목표

NIST SP 800-61 Computer Security Incident Handling Guide에 정의된 일반적인 인시던트 대응 프로세스 및 메커니즘도 여전히 유효하지만, 클라우드 환경에서 보안 인시던트에 대응하는 것과 관련된 구체적인 설계 목표를 고려해 보는 것이 좋습니다.

- 대응 목표 수립 - 이해 관계자, 법률 자문, 조직 리더십과 협력하여 인시던트 대응 목표를 결정합니다. 몇 가지 일반적인 목표로는 문제 억제 및 완화, 영향을 받은 리소스 복구, 포렌식을 위한 데이터 보존, 귀속 등이 있습니다.
- 클라우드를 사용하여 대응 - 이벤트와 데이터가 발생하는 곳에 대응 패턴을 구현합니다.
- 무엇을 가지고 있고 무엇이 필요한지 파악 - 로그, 스냅샷 및 기타 증거를 중앙 집중식 보안 클라우드 계정에 복사하여 보존합니다. 보존 정책을 적용하는 태그, 메타데이터, 메커니즘을 사용합니다. 예를 들어 Linux dd 명령이나 이에 해당하는 Windows 명령을 사용하여 조사 목적을 위한 데이터의 전체 복사본을 만들 수 있습니다.
- 재배포 메커니즘 사용 - 보안 문제의 원인이 잘못된 구성일 수 있는 경우, 적절한 구성의 리소스를 재배포하여 변형을 제거하는 것만으로 간단하게 해결할 수 있습니다. 가능하면 알 수 없는 상태에서 대응 메커니즘을 두 번 이상 실행할 수 있도록 합니다.
- 가능한 경우 자동화 - 반복되는 문제나 인시던트의 경우, 일반적인 상황을 프로그래밍 방식으로 분류하고 이에 대응하는 메커니즘을 구축합니다. 사람은 특별하고, 새롭고, 중요한 인시던트에 대응합니다.
- 확장 가능한 솔루션 선택 - 조직에서 클라우드 컴퓨팅을 확장하는 방식에 맞추고 탐지와 대응 사이의 시간을 단축하기 위해 노력합니다.
- 프로세스 교육 및 개선 - 프로세스, 도구, 인력의 격차가 발견되면 이를 해결하기 위한 계획을 구현합니다. 시뮬레이션은 격차를 찾고 프로세스를 개선할 수 있는 안전한 방법입니다.

NIST 설계 목표는 인시던트 대응과 위협 탐지를 모두 수행할 수 있는 기능에 대한 아키텍처를 검토하도록 상기시키는 것입니다. 클라우드 구현을 계획할 때 인시던트 또는 포렌식 이벤트에 대응하는 방법을 생각해 보세요. 경우에 따라 이러한 대응 작업을 위해 특별히 설정된 여러 조직, 계정 및 도구가 있을 수 있습니다. 이러한 도구와 기능은 배포 파이프라인을 통해 인시던트 대응 담당자가 사용할 수 있도록 해야 하며 더 큰 위험을 초래할 수 있으므로 정적이어서는 안 됩니다.

클라우드 보안 인시던트

주제

인시던트 도메인

고객 책임에서 보안 인시던트는 서비스, 인프라 및 애플리케이션이라는 3가지 도메인에서 발생할 수 있습니다. 도메인 간 차이는 대응 시 사용하는 도구와 관련됩니다. 3가지 도메인은 다음과 같습니다.

- 서비스 도메인 - 서비스 도메인에서 발생하는 인시던트는 AWS 계정, IAM 권한, 리소스 메타데이터, 결제 및 기타 영역에 영향을 미칩니다. 서비스 도메인 이벤트는 AWS API 메커니즘만 사용하여 대응하거나 근본 원인이 구성 또는 리소스 권한과 관련되어 있어 관련된 서비스 중심 로깅이 있을 수 있는 이벤트입니다.
- 인프라 도메인 - 인프라 도메인의 인시던트에는 데이터 또는 네트워크 관련 활동이 포함됩니다. 예를 들어 VPC 내의 Amazon EC2 인스턴스로 향하는 트래픽, Amazon EC2 인스턴스의 프로세스와 데이터, 컨테이너나 향후 출시될 기타 서비스 같은 기타 영역이 포함됩니다. 인프라 도메인 이벤트에 대응할 때는 포렌식을 위해 인시던트 관련 데이터를 검색, 복원 또는 수집하는 작업이 포함됩니다. 인스턴스 운영 체제와의 상호 작용이 포함될 가능성이 높고 경우에 따라 AWS API 메커니즘이 사용될 수도 있습니다.
- 애플리케이션 도메인 - 애플리케이션 도메인의 인시던트는 서비스 또는 인프라에 배포된 애플리케이션 코드 또는 소프트웨어에서 발생합니다. 이 도메인은 클라우드 위협 탐지 및 대응 런북에 포함되어야 하며 인프라 도메인의 대응과 유사한 대응을 포함할 수 있습니다. 적절하고 체계적인 애플리케이션 아키텍처에서는 클라우드 도구를 통해 자동 포렌식, 복구 및 배포를 사용하여 이 도메인을 관리할 수 있습니다.

이러한 도메인에서는 계정, 리소스 또는 데이터에 대해 조치를 취할 수 있는 행위자를 고려해야 합니다. 내부적이든 외부적이든 위험 프레임워크를 사용하여 조직에 대한 특정 위험이 무엇인지 판단하고 그에 따라 대비해야 합니다.

서비스 도메인에서는 AWS API를 사용해서만 목표를 달성합니다. 예를 들어 Amazon S3 버킷의 데이터 누출 인시던트를 처리할 때는 API 호출을 사용하여 버킷의 정책을 검색하고 S3 액세스 로그 및 AWS CloudTrail 로그를 분석하는 작업이 포함됩니다. 이 예제에서 감사 담당자의 조사에는 데이터 포렌식 도구 또는 네트워크 트래픽 분석 도구가 사용되지 않을 가능성이 높습니다.

인프라 도메인에서 감사 담당자는 AWS API와 익숙한 디지털 포렌식/인시던트 대응(DFIR) 소프트웨어를 IR 작업을 위해 준비한 Amazon EC2 인스턴스와 같은 워크스테이션의 운영 체제 안에서 사용할 수 있습니다. 인프라 도메인 인시던트는 네트워크 패킷 캡처, Amazon Elastic Block Store(Amazon EBS) 볼륨의 디스크 블록 또는 인스턴스에서 가져온 휘발성 메모리를 분석하는 작업이 포함될 수 있습니다.

클라우드 보안 이벤트 지표

인시던트로 분류하지 않을 수 있는 보안 이벤트가 많이 있지만 조사하는 것이 현명할 수 있습니다. AWS 클라우드 환경에서 보안 관련 이벤트를 탐지하기 위해 다음 메커니즘을 사용할 수 있습니다. 다음 예는 전체 목록은 아니지만 몇 가지 잠재적 지표를 보여주므로 참조하시기 바랍니다.

- 로그 및 모니터 - AWS 로그(예: Amazon CloudTrail, Amazon S3 액세스 로그 및 VPC 흐름 로그)와 보안 모니터링 서비스(예: Amazon GuardDuty, Amazon Detective, AWS Security Hub 및 Amazon Macie)를 검토합니다. 또한 Amazon Route 53 상태 확인 및 Amazon CloudWatch 경보와 같은 모니터를 사용합니다. 마찬가지로 Windows 이벤트, Linux syslog 로그 및 애플리케이션에서 생성할 수 있는 기타 애플리케이션별 로그를 사용하고 CloudWatch 에이전트를 사용하여 Amazon CloudWatch에 로깅합니다.
- 청구 활동 - 청구 활동이 갑자기 변경되면 보안 이벤트가 발생할 수 있습니다.
- 위협 인텔리전스 - 서드 파티 위협 인텔리전스 피드를 구독하는 경우 해당 정보를 다른 로깅 및 모니터링 도구와 연관시켜 이벤트의 잠재적 지표를 식별할 수 있습니다.
- 파트너 도구 - AWS 파트너 네트워크(APN)의 파트너는 보안 목표를 달성하는 데 도움이 되는 업계 최고의 수백 가지 제품을 제공합니다. 자세한 내용은 보안 파트너 솔루션 및 AWS Marketplace의 보안 파트너 솔루션을 참조하세요.
- AWS Outreach - AWS Support는 악의적인 활동이 확인되면 고객에게 연락할 수 있습니다. 자세한 내용은 부정 사용 및 침해에 대한 AWS 대응 단원을 참조하세요.
- 일회성 연락처 - 고객, 개발자 또는 조직의 다른 직원이 비정상적인 활동을 발견했을 수 있으므로 잘 알려진 공개된 방법으로 보안 팀에 연락하는 것이 중요합니다. 자주 사용하는 방법으로는 티켓팅 시스템, 연락처 이메일 주소 및 웹 양식이 있습니다. 조직이 일반 대중과 협력하는 경우 공개 보안 문의 메커니즘이 필요할 수도 있습니다.

AWS가 자동화 및 탐지를 위해 제공하는 도구 중 하나는 AWS Security Hub입니다. Security Hub는 AWS 계정 전체에서 우선순위가 높은 보안 경고 및 규정 준수 상태를 한 곳에서 포괄적으로 볼 수 있으므로 이러한 지표에 대한 가시성을 높일 수 있습니다. AWS Security Hub는 보안 정보 및 이벤트 관리(SIEM) 소프트웨어가 아니며 로그 데이터를 저장하지 않고, 대신 여러 AWS 서비스에서 보안 경고 또는 결과를 집계, 구성 및 우선순위를 지정합니다. 또한 Security Hub는 여러 소스에서 비롯될 수 있는 사용자 지정 인사이트를 생성할 수 있는 기능을 제공합니다. 이를 통해 보안 운영 팀은 이벤트 발생 시

추가 정보를 확인할 수 있는 옵션과 인사이트를 얻을 수 있습니다. Security Hub는 조직이 따르는 AWS 모범 사례와 산업 표준을 기반으로 자동화된 규정 준수 검사를 사용하여 환경을 지속적으로 모니터링합니다.

덧붙여 Amazon Detective 또는 Amazon Athena에서 보안 및 규정 준수 평가 결과를 조사하고 Amazon CloudWatch Events 또는 이벤트 버스 규칙을 사용하여 이러한 평가 결과에 대한 조치를 취하고 해당 평가 결과를 티켓팅, 채팅, SIEM, 보안 오케스트레이션 자동화 및 대응(SOAR), 인시던트 관리 도구 또는 사용자 지정 문제 해결 플레이북으로 보낼 수 있습니다. 이벤트 기반 자동화를 사용하면 발생하는 인시던트나 이벤트에 자동으로 대응할 수 있습니다. 이 접근 방식은 온프레미스 환경과 비교했을 때 보안과 클라우드에서 이벤트를 처리하는 방식을 변화시킵니다.

클라우드 기능 이해

AWS는 도메인 전반의 보안 이벤트를 조사하는 데 사용할 수 있는 광범위한 보안 기능을 제공합니다. 예를 들어 AWS는 AWS CloudTrail 로그, Amazon CloudWatch Logs, Amazon S3 액세스 로그 등과 같은 다양한 로깅 메커니즘을 제공합니다. 사용 중인 서비스를 검토하고 해당 서비스와 관련된 로그를 활성화해야 합니다. AWS에서는 일반적인 유형의 클라우드 로그를 중앙 집중화하고 저장하는 방법을 이해하는 데 도움이 되는 중앙 집중식 로깅 솔루션도 제공합니다. 이러한 로깅 소스를 활성화한 후에는 Amazon Athena를 사용하여 Amazon S3 버킷에 보관된 로그를 쿼리하는 등 분석 방법을 결정해야 합니다.

또한 APN 보안 컴피턴시 프로그램에 설명된 것과 같이 이러한 로그를 분석할 때 프로세스를 간소화할 수 있는 여러 APN 파트너 제품이 있습니다. Amazon GuardDuty(위협 탐지 서비스) 및 AWS Security Hub와 같이 이러한 데이터에 대한 귀중한 인사이트를 얻는 데 도움이 되는 여러 AWS 서비스가 있으며 이를 통해 AWS 계정 전체에 걸쳐 우선순위가 높은 보안 경고 및 규정 준수 상태를 포괄적으로 파악할 수 있습니다. 또한 Amazon Detective는 AWS 리소스에서 로그 데이터를 수집하고 기계 학습, 통계 분석 및 그래프 이론을 사용하여 잠재적인 보안 문제 또는 의심스러운 활동의 근본 원인을 식별하는 데 도움을 줍니다. 조사 중에 활용할 수 있는 추가 클라우드 기능에 대한 자세한 내용은부록 A: 클라우드 기능 정의를 참조하세요.

주제

- 데이터 프라이버시
- 부정 사용 및 침해에 대한 AWS 대응

데이터 프라이버시

AWS는 고객이 개인 정보 보호 및 데이터 보안에 깊은 관심을 갖고 있다는 것을 알고 있으므로 고객 콘텐츠에 대한 무단 액세스 또는 공개를 방지하도록 설계된 책임감 있고 정교한 기술 및 물리적 제어를 구현합니다. AWS는 고객 신뢰를 유지하기 위해 끊임없이 노력합니다. 데이터 프라이버시 FAQ 페이지에서 AWS 데이터 프라이버시 정책에 대해 자세히 알아볼 수 있습니다.

이러한 의도적이고 자체적인 제어 기능은 고객의 환경 내에서 대응하기 위해 AWS의 능력을 제한합니다. 따라서 공동 책임 모델 내에서 역량을 이해하고 구축하는 데 집중하는 것이 AWS 클라우드에서 성공하기 위한 열쇠입니다. 인시던트가 발생하기 전에 AWS 계정에서 로깅 및 모니터링 기능을 활성화하는 것이 중요하지만, 성공적인 프로그램을 위해서는 인시던트 대응에 필수적인 추가 측면이 있습니다.

캘리포니아 소비자 데이터 프라이버시

2018년 캘리포니아 소비자 개인 정보 보호법(CCPA)은 CCPA의 적용을 받는 '기업이 보유한 소비자와 관련된 개인 정보와 관련하여 소비자에게 다양한 권리'를 부여합니다. CCPA의 적용을 받는 고객과 관련된 AWS 개인 정보 보호 및 데이터 보안 정책에 대한 자세한 내용은 캘리포니아 소비자 개인 정보 보호법 준비 백서를 참조하세요.

일반 데이터 보호 규정

일반 데이터 보호 규정(GDPR)은 2018년 5월 25일에 시행된 유럽 개인 정보 보호법(2016년 4월 27일 유럽 의회 및 이사회의 규정 2016/679)입니다. GDPR은 EU 데이터 보호 지침(Directive 95/46/EC)을 대체하게 되며, 각 회원국에 구속력이 있는 단일 데이터 보호법을 적용함으로써 유럽 연합(EU) 전체에 데이터 보호법을 포괄적으로 적용할 목적으로 제정되었습니다. GDPR과 관련된 AWS 규정 준수에 대한 자세한 내용은 AWS에서의 GDPR 가이드 살펴보기 백서를 참조하세요.

부정 사용 및 침해에 대한 AWS 대응

부정 사용 활동은 AWS 고객의 인스턴스 또는 다른 리소스가 악의적이거나, 불쾌감을 주거나, 불법적이거나, 다른 인터넷 사이트에 피해를 주는 동작을 하는 것이 외부에서 관찰되는 경우를 말합니다. AWS는 고객과 협력하여 AWS 리소스에서 의심스럽고 악의적인 동작을 탐지 및 해결합니다. 고객의 리소스로부터 예상치 못했거나 의심스러운 동작을 발견하는 경우 AWS 리소스가 손상되어 비즈니스에 잠재적인 위험이 발생했음을 나타내는 것일 수 있습니다. AWS 계정에는 대체 연락처가 있습니다. 연락처를 추가할 때는 보안 및 결제를 위해 모범 사례를 활용해야 합니다. 루트 계정 이메일이 AWS와 연락하는 주요 수단이지만, AWS는 보안 문제 및 결제 문제의 경우 보조 이메일 주소로도 연락합니다. 한 사람에게만 배달되는 이메일 주소를 추가하면 AWS 계정에 단일 장애 지점이 추가되었음을 의미합니다. 연락처에 배포 목록을 하나 이상 추가하세요.

AWS는 다음과 같은 메커니즘을 사용하여 리소스에서 부정 사용 활동을 탐지합니다.

- AWS 내부 이벤트 모니터링
- AWS 네트워크 주소 공간을 기준으로 한 외부 보안 인텔리전스
- AWS 리소스를 기준으로 한 인터넷 부정 사용 불만 제기

AWS 부정 사용 대응 팀이 AWS에서 발생하는 무단 활동을 적극적으로 모니터링하고 차단하지만 대부분의 부정 사용 불만 제기는 AWS에서 합법적인 비즈니스를 운영 중인 고객에 대한 내용입니다. 의도하지 않은 부정 사용의 일반적인 원인은 다음과 같습니다.

- 손상된 리소스 - 예를 들어, 패칭되지 않은 Amazon EC2 인스턴스가 감염되어 봇넷 에이전트가 될 수 있습니다.
- 의도하지 않은 부정 사용 - 지나치게 공격적인 웹 크롤러는 일부 인터넷 사이트에서 서비스 거부 공격으로 분류될 수 있습니다.
- 2차 부정 사용 - AWS 고객이 제공하는 서비스의 최종 사용자는 퍼블릭 Amazon S3 버킷에 맬웨어 파일을 게시할 수 있습니다.
- 허위 불만 - 간혹 인터넷 사용자가 합법적인 활동을 부정 사용으로 잘못 신고하는 경우가 있습니다.

AWS는 부정 사용을 방지, 탐지 및 완화하고 향후 재발을 방지하기 위해 AWS 고객과 협력하는 면에서 최선을 다하고 있습니다. Amazon Web Services 및 그 계열사가 제공하는 웹 서비스의 금지된 사용을 설명하는 AWS 이용목적제한방침을 검토하는 것이 좋습니다. AWS의 부정 사용 알림에 적시에 대응할 수 있도록 AWS 계정 연락처 정보가 정확한지 확인하시기 바랍니다. AWS 부정 사용 경고를 수신하면 보안 및 운영 직원은 즉시 그 문제를 조사해야 합니다. 지연이 발생하면 평판에 미치는 영향과 자신과 타인에 대한 법적 영향이 오래 지속될 수 있습니다. 더 중요한 점은 관련된 침해 리소스가 악의적인 사용자에 의해 손상될 수 있고 손상을 무시하면 고객의 비즈니스 피해가 커질 수 있습니다.

준비 - 사람

자동화된 프로세스 덕분에 조직은 클라우드 환경과 애플리케이션의 보안을 강화하는 조치에 더 많은 시간을 할애할 수 있습니다. 또한 자동화된 인시던트 대응을 통해 인시던트 상관관계 파악, 시뮬레이션 연습, 새로운 대응 절차 개발, 연구 수행, 새로운 기술 개발, 새로운 도구 테스트 또는 구축 업무에 인력을 활용할 수 있습니다. 자동화 기능이 향상되어도, 보안 조직 내의 분석가와 대응 담당자에게는 여전히 해야 할 일이 많습니다. 동질적인 팀은 사각지대를 만들 수 있으므로 복잡하고 유동적인 상황에서 다양한 사고 시스템, 문화적 관점, 일과 삶의 경험을 제공하는 다양한 팀을 구성하는 것이 필수적입니다. 이벤트를 계획할 때 할 수 있는 가장 영향력 있는 일 중 하나는 팀과 대응 계획에 다양성을 구축하는 것입니다. 다양한 관점으로 구성된 팀은 잠재적으로 포착되지 않았을 수 있는 사각지대를 파악하고 다른 방법으로는 생각하지 않았을 수 있는 솔루션을 식별할 수 있습니다.

주제

역할과 책임 정의

인시던트 대응의 기술과 메커니즘은 신규 또는 대규모 이벤트를 처리할 때 가장 중요합니다. 이러한 이벤트는 팀이 개발한 서면 표준과 팀이 보유한 관행에 의존합니다. 이벤트가 취할 모든 잠재적 방향을 예측하거나 체계화할 수 없기 때문에 인스턴스 메모리 또는 진단 로그 수집과 같은 단순하고 반복적인 작업을 자동화하여 인간이 어려운 결정을 내릴 수 있도록 합니다. 명확하지 않은 보안 이벤트를 처리하려면 조직 간 규율, 결정적인 조치에 대한 편향 및 결과 제공 능력이 필요합니다. 조직 구조 내에는 HR(인사), 경영진 및 법무 담당자와 같이 인시던트 발생 시 책임을 지거나 자문을 하거나 최신 정보를 제공하는 사람이 많이 있어야 합니다. 이러한 역할과 책임, 그리고 제3자가 참여해야 하는지 여부를 고려합니다. 대부분의 지역에는 할 수 있는 것과 할 수 없는 일을 규정하는 현지 법률이 있습니다. 인시던트에 대해 RACI(책임, 해명, 자문, 정보) 차트를 작성하는 것이 관료적으로 보일 수 있지만, 이렇게 하면 빠르고 직접적인 의사 소통이 가능하며 이벤트의 여러 단계에서 리더십을 명확하게 설명할 수 있습니다.

신뢰할 수 있는 파트너는 조사 또는 대응에 참여할 수 있으며 추가 전문 지식과 귀중한 조사를 제공합니다. 팀에 이러한 기술이 없는 경우 외부 전문가를 고용하여 도움을 받을 수 있습니다. 외부 전문가를 고용하는 경우 이 전문가가 팀원을 교육하도록 하는 것이 좋습니다. 이러한 외부 전문가가 내부 개발자

및 운영 담당자와 협력하면 팀 구성원의 기술을 확장할 수 있으며 향후 IR 프로그램에 새로운 전문 지식을 유용하게 활용할 수 있습니다.

인시던트 중에는 영향을 받는 애플리케이션 및 리소스의 소유자와 개발자를 포함하는 것이 중요합니다. 이들은 정보와 컨텍스트를 제공할 수 있는 SME(주제 전문가)이기 때문입니다. 인시던트 대응을 위해 전문 지식에 의존하기 전에 개발자 및 애플리케이션 소유자와 연습하고 관계를 구축하는 것이 좋습니다. 애플리케이션 소유자 또는 SME는 환경이 익숙하지 않거나 예기치 않게 복잡하거나 대응 담당자가 액세스할 수 없는 상황에서 조치를 취해야 할 수 있습니다. 애플리케이션 SME는 IR 팀과 함께 연습하고 편안하게 작업해야 합니다.

교육 제공

의존도와 대응 시간을 줄이려면 보안 팀과 대응 담당자가 클라우드 서비스에 대한 교육을 받고 조직에서 사용하는 특정 클라우드 플랫폼을 직접 실습할 수 있는 기회를 제공해야 합니다. 이 교육 중 일부는 프로세스 시작 시 수행되는 팀 구축 및 런북 작성에서 제공됩니다. 런북을 작성하는 초기 단계에 가능한 한 많은 사람을 포함시키면 내부 팀을 더 잘 이해할 수 있습니다. 이 교육은 내부 팀이 탁상 연습에서 런북을 따르기 시작함에 따라 더욱 현실적이 됩니다.

또한 AWS 및 기타 서드 파티에서는 다운로드하여 진행할 수 있는 온라인 보안 워크숍(AWS 보안 워크숍)을 제공합니다. 직원에게 프로그래밍 기술, 개발 프로세스(버전 관리 시스템 및 배포 방식 포함), 인프라 자동화를 학습할 수 있는 추가 교육을 제공하는 것이 조직에도 이익이 될 수 있습니다.

AWS는 디지털 교육, 강의실 교육, APN 파트너 및 자격증을 통해 다양한 교육 옵션과 학습 경로를 제공합니다. 자세한 내용은 AWS Training & Certification을 참조하세요.

대응 메커니즘 정의

대응 메커니즘은 거버넌스, 위험 및 규정 준수(GRC) 모델에 따라 다릅니다. 인시던트 대응을 계획하기 전에 GRC 모델을 구축하는 것이 가장 좋습니다. 아직 구축을 시작하지 않았다면 GRC 구축이야말로 탁월한 인시던트 대응 메커니즘을 구축하는 데 필요한 첫 번째 단계입니다. 클라우드에서 인시던트 대응 방식을 다른 팀(예: 법률 자문, 리더십, 비즈니스 이해 관계자, AWS Support Services 등)과 함께 정의할 때는 현재 가지고 있는 것이 무엇인지 그리고 필요한 것은 무엇인지 파악해야 합니다. 이해 관계자 및 관련 담당자를 식별하고 필요한 대응을 수행할 수 있는 적절한 액세스 권한이 있는지 확인합니다.

클라우드는 서비스 API를 통해 더 뛰어난 가시성과 기능을 제공할 수 있지만 GRC 모델은 대응에 이러한 API를 사용하는 방법을 보여줍니다. 팀의 AWS 계정 번호, Virtual Private Cloud(VPC)의 IP 범위, 해당 네트워크 다이어그램, 로그, 데이터 위치 및 데이터 분류를 식별합니다. 이러한 기술 프로세스 중 상

당수는 준비 - 기술 단원에 포함되어 있습니다. 그런 다음 인시던트를 조사하고 해결하는 단계를 정의하는 절차 또는 런북이라고도 하는 인시던트 대응 절차를 문서화하기 시작합니다.

수용적이고 적응적인 보안 문화 조성

AWS에서는 모든 이해 관계자가 민첩하고 대응력이 뛰어난 보안 태세를 유지하기 위해 협력하고 에스컬레이션할 수 있는 문화를 조성하는 보안 팀이 비즈니스와 개발자를 위한 협력 조력자인 경우 고객과 AWS 내부 팀이 가장 성공적이라는 것을 알게 되었습니다. 조직의 보안 문화를 개선하는 것이 이 백서의 주제는 아니지만 보안 팀이 수용적이라고 생각되면 비보안 직원으로부터 관련 인텔리전스를 얻을 수 있습니다. 보안 팀이 개방적이고 접근 가능한 상태에서 경영진의 지원을 받으면 보안 이벤트에 대한 추가 알림, 협력 및 대응을 적시에 받을 가능성이 높아집니다.

일부 조직에서는 직원이 보안 문제를 신고하면 보복을 두려워할 수 있습니다. 때로는 문제를 신고하는 방법을 모르는 경우가 있습니다. 시간을 낭비하고 싶지 않거나 나중에 문제가 아닌 것으로 밝혀진 보안 인시던트로 신고하는 것이 당혹스러울 수 있습니다. 리더십 팀부터 수용 문화를 장려하고 모든 사람이 조직 보안의 일원이 되도록 포용하는 것이 중요합니다. 잠재적 위험이나 위협이 있을 수 있다고 생각되면 누구나 심각도가 높은 티켓을 열 수 있는 명확한 채널을 제공합니다. 열렬하고 열린 마음으로 이러한 알림을 받는 것도 중요하지만 그보다 중요한 것은 비보안 직원에게 이러한 알림을 환영한다는 것을 분명히 하는 것입니다. 알림을 전혀 받지 않는 것보다 잠재적인 문제에 대해 과도한 알림을 받기를 원한다는 점을 강조하세요. 개발자가 자신의 실수를 알린 다음 조사원이 공개 기사에서 문제를 지적하는 것이 훨씬 좋습니다.

이러한 알림은 스트레스 하에서 대응 조사를 연습할 수 있는 귀중한 기회를 제공합니다. 이는 대응 절차를 개발하는 동안 중요한 피드백 루프 역할을 할 수 있습니다.

대응 예측

모든 잠재적 사건을 예측하는 것은 불가능하기 때문에 인간 분석에 계속 의존해야 합니다. 시간을 내어 직원을 신중하게 교육하고 조직을 준비하면 예상치 못한 상황을 예측하는 데 도움이 되지만 조직이 고립되어 준비할 필요는 없습니다. 신뢰할 수 있는 보안 파트너와 협력하여 예기치 않은 보안 이벤트를 식별하면 추가적인 가시성과 인사이트의 이점을 얻을 수 있습니다.

파트너 및 대응 창구

클라우드로의 여정은 모든 조직마다 다릅니다. 그러나 신뢰할 수 있는 보안 파트너는 사용자의 관심을 끌만한 다른 조직에서 이미 접한 패턴과 관행을 보유하고 있습니다. 외부의 전문 지식 그리고 대응 능

력을 강화할 수 있는 다른 관점을 제공할 수 있는 외부 AWS 보안 APN 파트너를 찾는 것이 좋습니다. 신뢰할 수 있는 보안 파트너는 익숙하지 않은 잠재적 위험 또는 위협을 식별하는 데 도움을 줄 수 있습니다.

1955년 Joseph Luft와 Harrington Ingham은 특성을 범주에 매핑하는 연습인 Johari 창을 만들었습니다. 이 창은 다음 다이어그램과 유사하게 네 개의 사분면으로 구성된 그리드로 표시됩니다.

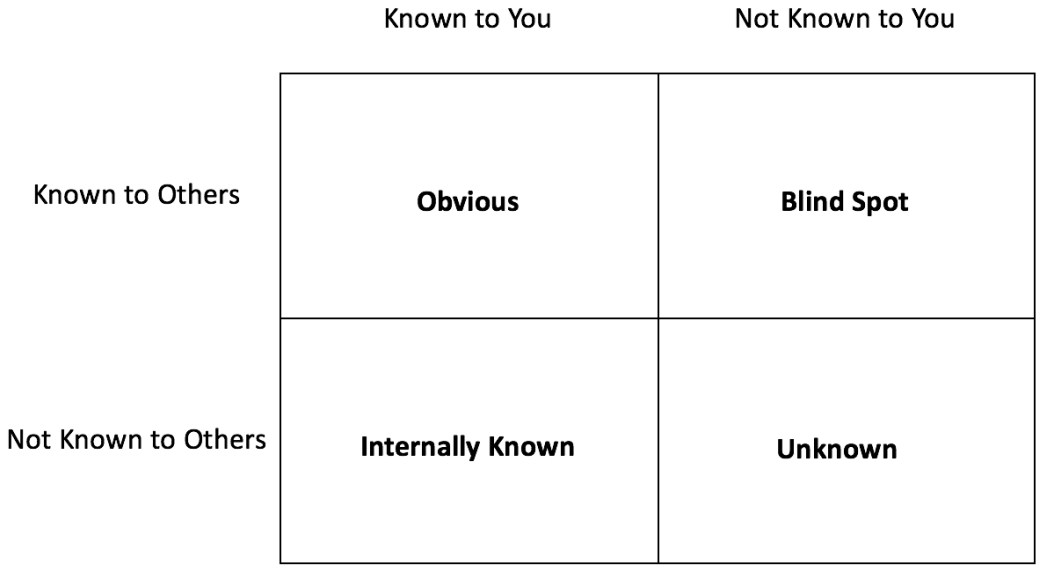

그림 3: 인시던트 대응을 위해 수정된 Johari 창

Johari 창은 원래 정보 보안을 위한 것이 아니었지만 조직의 위협을 평가하는 데 따르는 어려움을 고려하여 간단한 정신 모델로 사용하도록 개념을 수정할 수 있습니다. 수정된 개념에서 네 사분면은 다음과 같습니다.

- 명백함 - 팀과 APN 파트너가 모두 알고 있는 위험입니다.
- 내부적으로 알려짐 - 팀은 익숙하지만 APN 파트너는 그렇지 않은 위험입니다. 이는 내부 전문 지식이나 조직 내 지식이 있음을 의미할 수 있습니다.
- 사각지대 - APN 파트너는 잘 알고 있지만 팀은 그렇지 않은 위험입니다.
- 알 수 없음 - 사용자와 APN 파트너가 모두 잘 모르는 위험입니다.

이 다이어그램은 간단하지만 신뢰할 수 있는 APN 파트너가 달성할 수 있는 가치를 나타냅니다. 가장 중요한 것은 사용자가 모르는 사각지대 항목이 있을 수 있지만 적절한 전문 지식을 갖춘 APN 파트너는 이곳으로 사용자의 주의를 끌 수 있다는 것입니다. 사용자는 명백함 사분면의 위험에 익숙할 수 있지만 APN 파트너는 사용자에게 익숙하지 않은 제어 및 솔루션을 추천할 수 있습니다. 또한 내부적으로 알려

짐 사분면에 있는 이러한 위험을 APN 파트너에게 알릴 수 있지만 APN 파트너는 해당 위험을 완화하기 위해 최적화된 제어를 식별할 수도 있습니다. 개선을 위해 스스로를 측정할 때 APN 파트너에게 문의하여 전문가의 조언을 받아보세요.

알려지지 않은 위험

알림을 조정하고 자동화를 통해 인시던트 대응 절차를 개선하며 보안 방어를 개선하는 데 중점을 두었다면 그 다음에는 무엇을 개선해야 할지 궁금할 것입니다. 그림 3의 알 수 없음 범주에 나와 있는 것처럼 알 수 없는 위험에 대해 궁금할 수 있습니다. 다음 방법을 통해 알 수 없는 위험을 줄일 수 있습니다.

- 보안 어설션 정의 - 단언할 수 있는 몇 가지 사실은 무엇입니까? 사용자 환경에서 절대적으로 사실이어야 하는 보안 기본 요소는 무엇입니까? 이를 명확히 정의하면 그 반대 내용을 알아볼 수 있습니다. 보안 어설션 정의는 나중에 보안 어설션을 리버스 엔지니어링하려고 시도하는 것보다 클라우드 여정의 초기에 수행하면 더 쉬운 일입니다.
- 교육, 커뮤니케이션 및 연구 - 직원을 대상으로 클라우드 보안 전문가를 만들거나 환경을 면밀히 조사하는 데 도움이 되는 전문 파트너를 포함합니다. 가정에 도전하고 미묘한 추론을 조심하세요. 프로세스에 피드백 루프를 생성하고 엔지니어링 팀이 보안 팀과 커뮤니케이션할 수 있는 메커니즘을 제공합니다. 또한 접근 방식을 확장하여 관련 보안 이메일 발송 목록 및 정보 보안 공개를 모니터링할 수 있습니다.
- 공격 표면 감소 - 방어 역량을 향상시켜 위험을 피하고 알려지지 않은 공격에 더 많은 시간을 할애할 수 있습니다. 공격자를 차단하고 속도를 늦추고 공격자가 노이즈를 발생시키도록 합니다.
- 위협 인텔리전스 - 전 세계의 현재 위협 및 관련 위협, 위험 및 지표에 대한 지속적인 피드를 구독합니다.
- 알림 - 비정상적이거나 악의적이거나 비용이 많이 드는 활동에 대해 경고하는 알림을 생성합니다. 예를 들어 사용하지 않는 리전 또는 서비스에서 발생하는 활동에 대한 알림을 생성할 수 있습니다.
- 기계 학습 - 기계 학습을 사용하여 특정 조직 또는 개별 페르소나에 대한 복잡한 이상을 식별합니다. 비정상적인 동작을 식별하는 데 도움이 되도록 네트워크, 사용자 및 시스템의 일반적인 특성을 프로파일링할 수도 있습니다.

사각지대와 알려지지 않음 영역을 고려할 때 위협 인텔리전스가 주요 주제가 됩니다. Johari 창에는 사용자가 아는 것과 모르는 것을 분류하는 방법이 표시되지만 위협 인텔리전스는 아직 모르는 것을 설명하는 방법을 보여 줍니다. 위협 인텔리전스는 기업이 위협 모델의 구석구석을 살펴보고 아직 알지 못하는 위협을 찾는 데 도움이 되는 분야입니다.

일반적으로 위협 인텔리전스는 다음과 같이 구성됩니다.

1. 새로운 위협 발견

2. 새 패턴 정의
3. 새로운 자동 획득 기술 정의
4. 이 프로세스 반복

이러한 유형의 관행이 도움이 될 수 있지만 위협 인텔리전스 팀의 관리 및 유지 관리는 많은 기업, 심지어 대기업에도 부담을 줄 수 있습니다. 결국 문제는 위협 모델, 규모 및 위험을 일치시키는 것입니다. 다음 질문을 고려하시기 바랍니다.

- 위협 모델이 엔터프라이즈의 표준 업종과 충분히 다른가요?
- 그러한 팀이 필요할 정도로 위험 성향이 낮나요?
- 기업을 위해 팀을 운영하는 것이 재정적으로 건전한가요?
- 위험 프로파일이 대의에 합당한 인재를 유치하기에 충분히 흥미로운가요?

이러한 질문 중 하나라도 아니요라고 응답하는 경우 위협 인텔리전스 파트너를 찾을 가능성이 큽니다. 이 서비스는 많은 유명 대기업에서 경쟁적으로 제공합니다.

AWS는 이러한 문제를 직접 관리할 수 있는 도구와 서비스를 제공합니다. 기계 학습을 사용하여 악성 패턴을 식별하는 것은 고객, AWS Professional Services, APN 파트너 및 Amazon GuardDuty 및 Amazon Macie와 같은 AWS 서비스를 통해 구현되는 패턴으로 잘 연구된 연구 분야입니다. 이러한 패턴 중 일부는 AWS re:Invent 컨퍼런스 세션에서 논의되었습니다. 자세한 내용은 이 백서의 미디어 단원을 참조하세요.

또한 고객은 보안 데이터 레이크를 개발할 때 유사한 아키텍처 패턴을 활용하기 위해 기존의 비즈니스 중심 데이터 레이크를 확장하고 있습니다. 보안 운영 팀은 Amazon OpenSearch Service 및 OpenSearch Dashboards와 같은 기존 로깅 및 모니터링 도구의 사용을 빅 데이터 아키텍처로 확장하고 있습니다.

이러한 고객은 AWS CloudTrail 이벤트 로그, VPC 흐름 로그, Amazon CloudFront 액세스 로그, 데이터베이스 로그 및 애플리케이션 로그에서 내부 데이터를 수집한 다음 이 데이터를 공개 데이터 및 위협 인텔리전스와 결합합니다. 이 귀중한 데이터를 통해 고객은 보안 운영 팀에 데이터 과학 및 데이터 엔지니어링 기술을 포함하도록 확장하여 Amazon EMR, Amazon Kinesis Data Analytics, Amazon Redshift, Amazon QuickSight, AWS Glue, Amazon SageMaker 및 Apache MXNet on AWS와 같은 도구를 활용하여 사용자의 비즈니스에 고유한 이상 현상을 식별하고 예측하는 사용자 지정 솔루션을 구축합니다.

마지막으로, 보안 파트너 솔루션에서 온프레미스 환경의 기존 제어 항목에 상응하거나, 일치하거나, 통합되는 APN 파트너의 수백 가지의 업계 최고 제품을 확인하세요. 이러한 제품은 기존 AWS 서비스를

보완하여 클라우드 및 온프레미스 환경에 포괄적인 보안 아키텍처와 보다 원활한 환경을 배포할 수 있도록 해줍니다.

준비 - 기술

주제

AWS 계정에 대한 액세스 준비

인시던트 중에 인시던트 대응팀은 인시던트와 관련된 환경 및 리소스에 액세스할 수 있어야 합니다. 이벤트가 발생하기 전에 팀에 업무 수행에 필요한 적절한 권한이 있어야 합니다. 이를 위해서는 팀원에게 필요한 권한 수준(예: 수행할 가능성이 높은 작업 종류)을 알고 있어야 하며, 권한을 미리 프로비저닝해야 합니다. 이 권한은 회사의 거버넌스, 위험 관리 및 규정 준수(GRC) 정책에서 파생됩니다. 지연 없이 적시에 대응할 수 있도록 이벤트가 발생하기 전에 팀 구성원 인증 및 권한 부여를 문서화하고 테스트해야 합니다. 인시던트에 올바르게 대응하려면 AWS 계정이 배치되는 방식, 교차 계정 역할이 허용되고 구성되는 방법을 검토해야 합니다.

이 단계에서는 개발자, 설계자, 파트너, 거버넌스 팀 및 규정 준수 팀과 긴밀히 협력하여 대응 담당자에게 필요한 권한 수준을 파악해야 합니다. 조직의 클라우드 설계자와 함께 AWS 계정 전략 및 클라우드 자격 증명 전략을 파악하고 논의하여 어떤 인증 및 권한 부여 방법이 구성되어 있는지 파악합니다. 예를 들면 다음과 같습니다.

- 페더레이션 - 사용자가 자격 증명 공급자의 AWS 계정에서 IAM 역할을 맡습니다.
- 교차 계정 액세스 - 사용자가 여러 AWS 계정 간에 IAM 역할을 맡습니다.
- 인증 - 사용자가 단일 AWS 계정 내에서 생성된 AWS IAM 사용자로 인증합니다.

이러한 옵션은 AWS 인증에 대한 기술적 옵션과 대응 중에 권한을 얻는 방법을 정의하지만, 일부 조직에서는 대응을 지원하기 위해 다른 팀이나 파트너의 도움을 받을 수 있습니다. 보안 인시던트에 대응하기 위해 특별히 생성된 역할 또는 사용자는 권한이 충분히 부여된 경우가 많습니다. 따라서 이러한 사용자 계정의 사용은 제한적이어야 하고 일상적인 활동에 사용되어서는 안 됩니다.

새로운 액세스 메커니즘을 생성하기 전에 클라우드 팀과 협력하여 AWS 계정이 어떻게 구성되고 관리되는지 파악합니다. 많은 고객이 중앙 집중식으로 결제를 관리하고 AWS 계정 전체에서 리소스를 공유하며 액세스, 규정 준수 및 보안을 제어하는 데 AWS Organizations를 사용합니다. Organizations의 핵심 기능은 서비스 제어 정책을 계정 그룹에 적용하는 데 활용할 수 있어 규모에 맞게 정책을 관리할 수

있다는 것입니다. 거버넌스 메커니즘을 대규모로 구현하는 방법에 대한 자세한 내용은 대규모 AWS 거버넌스 단원을 참조하세요. 조직에서 AWS 계정을 어떻게 구성하고 관리했는지 파악한 후에는 다음과 같은 일반화된 대응 패턴을 고려하면 조직에 적합한 접근 방식을 파악하는 데 도움이 됩니다.

주제

- 간접 액세스
- 직접 액세스
- 대체 액세스
- 자동화 액세스
- 관리형 서비스 액세스

간접 액세스

간접 액세스를 사용하는 경우 계정 소유자 또는 애플리케이션 팀은 보안 전문가인 인시던트 대응 팀의 전술적 가이드에 따라 AWS 계정에서 권한이 부여된 문제 해결 작업을 수행해야 합니다. 이 방법은 더 느리고 복잡한 작업 실행 방법이지만 대응 담당자가 계정 또는 클라우드 환경에 익숙하지 않은 경우 적절할 수 있습니다.

직접 액세스

인시던트 대응 담당자에게 직접 액세스 권한을 부여하려면 보안 엔지니어 또는 인시던트 대응 담당자가 보안 이벤트 중에 맡을 수 있는 AWS 계정에 AWS IAM 역할을 배포합니다. 인시던트가 일반적인 인증 프로세스에 영향을 주는 경우 인시던트 대응 담당자는 일반적인 페더레이션 프로세스 또는 특수한 비상 프로세스를 통해 인증합니다. 인시던트 대응 IAM 역할에 부여하는 권한은 대응 담당자가 수행할 것으로 예상되는 작업에 따라 다릅니다.

대체 액세스

보안 이벤트가 보안, 자격 증명 또는 통신 시스템에 영향을 준다고 생각되면 그 영향을 조사하고 해결하기 위해 대체 메커니즘과 액세스를 찾아야 할 수 있습니다. 특별히 구축된 새로운 AWS 계정을 사용하면 대응 담당자가 안전한 대체 인프라에서 협업하고 작업할 수 있습니다.

예를 들어, Amazon WorkSpaces를 사용하는 원격 워크스테이션 및 Amazon WorkMail에서 제공하는 이메일 서비스와 같이 클라우드에서 시작되는 새로운 인프라를 활용할 수 있습니다. 안전한 대체 AWS 계정이 영향을 받는 AWS 계정에 대한 권한을 맡을 수 있도록 적절한 액세스 제어(IAM 정책 사용)를 준비하여 액세스 권한을 위임해야 합니다.

적절한 액세스 권한을 위임한 후에는 영향을 받는 계정의 AWS API를 사용하여 로그 및 볼륨 스냅샷과 같은 관련 데이터를 공유하여 격리된 환경에서 조사 작업을 수행할 수 있습니다. 이 교차 계정 액세스에 대한 자세한 내용은 튜토리얼: IAM 역할을 사용하여 AWS 계정 간 액세스 권한 위임 단원을 참조하세요.

자동화 액세스

자동화를 사용하여 보안 이벤트에 대응하도록 마이그레이션하는 경우 자동화 리소스(예: Amazon EC2 인스턴스 또는 AWS Lambda 함수)가 사용할 IAM 역할을 생성해야 합니다. 그러면 이러한 리소스가 IAM 역할을 맡고 역할에 할당된 권한을 상속할 수 있습니다. AWS 자격 증명을 생성하고 배포하는 대신 AWS Lambda 함수 또는 Amazon EC2 인스턴스에 권한을 위임합니다. AWS 리소스는 자동으로 임시 자격 증명 세트를 수신하고 이를 사용하여 API 요청에 서명합니다.

자동화 또는 도구가 Amazon EC2 인스턴스의 운영 체제 내에서 인증되고 실행되는 안전한 방법을 고려해볼 수도 있습니다. 이러한 자동화를 수행할 수 있는 도구는 많지만, Amazon EC2 인스턴스 운영 체제에 설치한 에이전트를 사용하여 원격으로 안전하게 인스턴스를 관리할 수 있도록 해주는 AWS Systems Manager Run Command를 사용하는 방법도 있습니다.

AWS Systems Manager Agent(SSM Agent)는 Microsoft Windows Server 및 Amazon Linux와 같은 일부 Amazon EC2 Amazon Machine Images(AMI) 에 기본적으로 설치됩니다. 하지만 다른 버전의 Linux 및 하이브리드 인스턴스에 에이전트를 수동으로 설치해야 할 수 있습니다. Run Command를 사용하든 다른 도구를 사용하든 조사할 첫 번째 보안 관련 알림을 받기 전에 사전 요구 사항 설정 및 구성을 완료하세요.

관리형 서비스 액세스

조직은 이미 사용자를 대신하여 서비스 및 솔루션을 관리하는 정보 기술 공급자와 파트너 관계를 맺고 있을 수 있습니다. 이러한 파트너는 조직의 보안을 지원하는 공동 책임이 있으며, 이상이 발생하기 전에 이러한 관계를 명확하게 이해하는 것이 중요합니다. AWS 관리형 서비스 공급자(MSP) 파트너, AWS Managed Services 또는 관리형 보안 서비스 파트너와 협력하고 있는지 여부에 관계없이 클라우드 환경과 관련된 각 파트너의 책임, 공급자가 조직의 클라우드 서비스에 대해 이미 가지고 있는 권한, 파트너에게 필요한 액세스 권한, 파트너의 지원이 필요한 시점에 연락 창구 또는 에스컬레이션 경로를 파악해야 합니다. 마지막으로 파트너와 함께 이를 연습하여 대응 계획이 예측 가능하고 성공적인지 확인해야 합니다.

프로세스 준비

적절한 액세스 권한을 프로비저닝하고 테스트한 후 인시던트 대응 팀은 조사 및 해결에 필요한 관련 프로세스를 정의하고 준비해야 합니다. 이 단계는 클라우드 환경 내의 보안 이벤트에 대한 적절한 대응을 충분히 계획해야 하므로 많은 노력이 필요합니다.

내부 클라우드 서비스 팀 및 파트너와 긴밀하게 협력하여 프로세스를 가능하게 만드는 데 필요한 작업이 무엇인지 식별합니다. 서로 협업하거나 대응 활동 작업을 할당하고 필요한 계정 구성이 제대로 되어 있는지 확인합니다. 조직에 다음과 같은 대응 기능을 제공하기 위해 프로세스 및 사전 요구 사항 구성을 미리 준비하는 것이 좋습니다.

주제

- 의사 결정 트리
- 대체 계정 사용
- 데이터 보기 또는 복사
- Amazon EBS 스냅샷 공유
- Amazon CloudWatch Logs 공유
- 변경 불가능한 스토리지 사용
- 이벤트 근처에서 리소스 시작
- 리소스 격리
- 포렌식 워크스테이션 시작

의사 결정 트리

경우에 따라 다른 작업이나 단계가 필요할 수 있습니다. 예를 들어 AWS 계정 유형(개발 및 프로덕션), 리소스 태그, 해당 리소스의 AWS Config 규칙 준수 상태 또는 기타 입력에 따라 다른 작업을 수행할 수 있습니다.

이러한 의사 결정 트리의 작성 및 문서화를 지원하려면 다른 팀 및 이해 관계자와 함께 의사 결정 트리 초안을 작성하는 것이 좋습니다. 순서도와 마찬가지로 의사 결정 트리는 의사 결정을 지원하는 데 활용할 수 있는 도구로, 가능성을 포함한 잠재적 조건 및 입력을 기반으로 최적의 조치와 결과를 결정하는 데 도움이 됩니다.

대체 계정 사용

영향을 받는 계정의 이벤트에 응답하는 것은 필수적이지만, 영향을 받는 계정 외부의 데이터까지 조사하는 것이 이상적입니다. 일부 고객은 프로비저닝해야 하는 리소스를 미리 구성하는 템플릿을 사용하여 격리된 별도의 AWS 계정 환경을 만드는 프로세스를 가지고 있습니다. 이러한 템플릿은 AWS CloudFormation 또는 Terraform과 같은 서비스를 통해 배포되며, 관련 AWS 리소스 모음을 생성하고 이를 질서 정연하고 예측 가능한 방식으로 프로비저닝할 수 있는 간편한 방법을 제공합니다.

템플릿 메커니즘을 사용하여 이러한 계정을 미리 구성하면 인시던트의 초기 단계에서 사람의 상호 작용을 제거하고 감사를 통해 확인할 수 있는 반복 가능하고 예측 가능한 방식으로 환경과 리소스를 준비할 수 있습니다. 또한 이 메커니즘은 포렌식 환경에서 데이터의 보안 및 억제를 유지하는 능력을 향상시킵니다.

이 접근 방식을 사용하려면 클라우드 서비스 및 아키텍트 팀과 협력하여 조사에 사용할 수 있는 적절한 AWS 계정 프로세스를 결정해야 합니다. 예를 들어 클라우드 서비스 팀은 AWS Organizations를 사용하여 새 계정을 생성하고 템플릿 또는 스크립트 방법을 사용하여 해당 계정을 미리 구성하는 데 도움을 줄 수 있습니다.

이 세분화 방법은 대규모 조직에서 잠재적 위협을 제거해야 할 때 가장 적합합니다. 거의 연결되지 않은 새 AWS 계정을 사용하는 이 세분화 방법은 다중 계정 설명서에서 보안 조직 단위(OU)로 레이블이 지정된 조직의 사용자가 계정으로 이동하여 필요한 포렌식 활동을 수행하고 필요한 경우 잠재적으로 계정 전체를 법인에 양도할 수 있음을 의미합니다. 이러한 포렌식 및 귀속 방식은 상당한 검토와 계획이 필요하며 기업의 GRC 정책에 부합해야 합니다. 이 작업은 쉽지 않지만 대규모 계정 기반을 구축하기 전에 수행하면 훨씬 용이합니다.

데이터 보기 또는 복사

대응 담당자는 분석할 로그 또는 기타 증거에 액세스해야 하며 따라서 데이터를 보거나 복사할 수 있는 권한이 있어야 합니다. 대응 담당자에 대한 IAM 권한 정책은 대응 담당자가 최소한 조사를 수행할 수 있도록 읽기 전용 권한을 제공해야 합니다. 적절한 액세스 권한을 지원하기 위해 SecurityAudit 또는 ViewOnlyAccess와 같은 사전 구축된 일부 AWS 관리형 정책을 고려할 수 있습니다.

예를 들어 대응 담당자는 한 계정의 Amazon S3 버킷에서 다른 계정의 Amazon S3 버킷으로 AWS CloudTrail 로그와 같은 데이터의 특정 시점으로 복사본을 만들고자 할 수 있습니다. ReadOnlyAccess 관리형 정책에서 제공하는 권한을 통해 대응 담당자는 이러한 작업을 수행할 수 있습니다. AWS Command Line Interface(CLI)를 사용하여 이를 수행하는 방법을 이해하려면 한 Amazon S3 버킷의 모든 객체를 다른 버킷으로 복사하려면 어떻게 해야 합니까?를 참조하세요.

Amazon EBS 스냅샷 공유

많은 고객이 Amazon EC2 인스턴스와 관련된 보안 이벤트에 대한 조사의 일환으로 Amazon Elastic Block Store(Amazon EBS) 스냅샷을 사용합니다. Amazon EBS 볼륨의 스냅샷은 증분 백업입니다. Amazon EBS 증분 스냅샷에 대한 자세한 내용은 Amazon EBS 스냅샷을 참조하세요.

격리된 별도의 계정에서 Amazon EBS 볼륨을 조사하려면 스냅샷의 권한을 수정하여 지정된 다른 AWS 계정과 공유해야 합니다. 권한이 부여된 사용자는 원본 스냅샷에 아무런 영향을 주지 않으면서 공유된 스냅샷을 토대로 자체 EBS 볼륨을 생성할 수 있습니다. 자세한 내용은 Amazon EBS 스냅샷 공유를 참조하세요.

암호화된 스냅샷을 공유할 때는 해당 스냅샷을 암호화하는 데 사용된 사용자 지정 AWS Key Management Service(AWS KMS) 고객 관리형 키(CMK)도 공유해야 합니다. 생성 당시에 또는 나중에 사용자 지정 CMK에 교차 계정 권한을 적용할 수 있습니다. 스냅샷은 생성된 리전으로 제한되지만 스냅샷을 해당 리전으로 복사하여 다른 리전과 스냅샷을 공유할 수 있습니다. 자세한 내용은 Amazon EBS 스냅샷 복사를 참조하세요.

Amazon CloudWatch Logs 공유

Amazon VPC 흐름 로그와 같이 Amazon CloudWatch Logs에 기록된 로그는 CloudWatch Logs 구독을 통해 다른 계정(예: 중앙 집중식 보안 계정)과 공유할 수 있습니다. 예를 들어 중앙의 Amazon Kinesis 스트림에서 이 로그 이벤트 데이터를 읽어 사용자 지정 처리 및 분석을 수행할 수 있습니다. 사용자 지정 처리는 특히 다수의 계정에서 로깅 데이터를 수집할 때 유용합니다. 보안 관련 이벤트가 발생하기 전에 클라우드 여정의 초기에 이 구성을 생성하는 것이 가장 좋습니다. 자세한 내용은 구독과 교차 계정 로그 데이터 공유를 참조하세요.

변경 불가능한 스토리지 사용

로그 및 기타 증거를 대체 계정에 복사할 때는 복제된 데이터가 보호되는지 확인해야 합니다. 2차 증거를 보호하는 것 외에도 소스에서 데이터의 무결성도 보호해야 합니다. 변경 불가능한 스토리지라고 하는 이러한 메커니즘은 데이터가 변조되거나 삭제되는 것을 방지하여 데이터의 무결성을 보호합니다.

Amazon S3의 기본 기능을 사용하여 데이터 무결성을 보호하도록 Amazon S3 버킷을 구성할 수 있습니다. 예를 들어 S3 객체 잠금을 사용하면 고정된 기간 동안 또는 무기한으로 객체를 삭제하거나 덮어쓰지 않도록 할 수 있습니다. S3 버킷 정책을 통한 액세스 권한 관리, S3 버전 관리 구성 및 MFA Delete 활성화는 데이터 쓰기 또는 읽기 방법을 제한하는 다른 방법입니다. 이러한 유형의 구성은 조사 로그 및 증거를 저장하는 데 유용하며 종종 WORM(Write Once, Read Many)이라고 합니다. 또한 AWS Key Management Service(AWS KMS)로 서버 측 암호화를 사용하고 적절한 IAM 보안 주체만 데이터를 해독할 권한이 있는지 확인하여 데이터를 보호할 수 있습니다.

또한 조사가 완료된 후 데이터를 장기 스토리지에 안전하게 보관하려면 객체 수명 주기 정책을 사용하여 Amazon S3에서 Amazon S3 Glacier로 데이터를 이동하는 것이 좋습니다. Amazon S3 Glacier는 데이터 아카이브 및 장기 백업을 위한 안전하고 안정적이며 비용이 매우 저렴한 클라우드 스토리지 서비스입니다. 99.999999999%의 내구성을 제공하도록 설계되었으며 포괄적인 보안 및 규정 준수 기능을 제공합니다.

또한 저장소 잠금 정책을 통해 개별 Amazon S3 Glacier 저장소에 대한 규정 준수 제어를 쉽게 배포하고 적용할 수 있는 Amazon S3 Glacier 저장소 잠금을 사용하여 Amazon S3 Glacier의 데이터를 보호할 수 있습니다. 저장소 잠금 정책에서는 WORM과 같은 보안 제어 항목을 지정하여 앞으로 편집하지 못하도록 정책을 잠글 수 있습니다. 잠긴 후에는 정책을 변경할 수 없습니다. Amazon S3 Glacier는 저장소 잠금 정책에 제어 항목 세트를 적용하여 데이터 보존과 같은 규정 준수 목표를 달성하도록 지원합니다. AWS Identity and Access Management(IAM) 정책 언어를 사용하여 저장소 잠금 정책에서 다양한 규정 준수 제어를 배포할 수 있습니다.

이벤트 근처에서 리소스 시작

클라우드를 처음 접하는 대응 담당자의 경우 기존 도구가 있는 온프레미스에서 클라우드 조사를 수행하려고 할 수 있습니다. 경험상 클라우드 기술을 사용하여 인시던트에 대응하는 AWS 고객은 더 나은 결과를 얻을 수 있습니다. 즉, 격리를 자동화하고, 사본을 더 쉽게 만들고, 증거를 더 빨리 분석하고, 분석을 더 빠르게 완료할 수 있습니다.

모범 사례는 조사하기 전에 데이터를 데이터 센터로 전송하려고 시도하는 대신 데이터가 있는 클라우드에서 조사 및 포렌식을 수행하는 것입니다. 전 세계 어디에서나 클라우드의 안전한 컴퓨팅 및 스토리지 기능을 사용하여 안전한 대응 작업을 수행할 수 있습니다. 많은 고객이 조사를 수행할 준비가 된 별도의 AWS 계정을 사전 구축하기로 선택하지만, 동일한 AWS 계정에서 분석을 수행하도록 선택하는 경우도 있을 수 있습니다. 조직에서 규정 준수 및 법적 이유로 기록을 보관해야 하는 경우 장기 보관 및 법적 활동을 위해 별도의 계정을 사용하는 것이 현명할 수 있습니다.

데이터를 다른 리전으로 복제하는 대신 이벤트가 발생한 동일한 AWS 리전에서 조사를 수행하는 것도 모범 사례입니다. 리전 간에 데이터를 전송하는 데 추가 시간이 필요하기 때문에 이 방법을 사용하는 것이 좋습니다. 운영 중인 각 AWS 리전에 대해 인시던트 대응 프로세스와 대응 담당자 모두 관련 데이터 프라이버시 법을 준수해야 합니다. 리전 간에 데이터를 이동해야 하는 경우 관할 구역 간 데이터 이동의 법적 영향을 고려합니다. 일반적으로 데이터를 동일한 국가 관할권 내에 보관하는 것이 가장 좋습니다.

보안 이벤트가 보안, 자격 증명 또는 통신 시스템에 영향을 준다고 생각되면 그 영향을 조사하고 해결하기 위해 대체 메커니즘과 액세스를 찾아야 할 수 있습니다. AWS는 안전한 대체 작업 환경에 사용할 수 있는 새로운 인프라를 신속하게 시작할 수 있는 기능을 제공합니다. 예를 들어 상황의 잠재적 심각성을 조사하는 동안 법률 고문, 홍보 및 보안 팀이 의사 소통을 하고 작업을 계속하는 데 필요한

보안 도구를 사용하여 새 AWS 계정을 만들 수 있습니다. AWS WorkSpaces(가상 데스크톱용), AWS WorkMail(이메일용) 및 Amazon Chime(커뮤니케이션용)과 같은 서비스는 대응 팀, 경영진 및 기타 참가자가 의사 소통, 조사 및 문제 해결을 위해 필요한 기능과 연결성을 제공할 수 있습니다.

리소스 격리

조사 과정에서 보안 이상에 대한 대응의 일환으로 리소스를 격리해야 할 수 있습니다. 리소스 격리의 목적은 잠재적 영향을 제한하고, 영향을 받는 리소스의 추가 전파를 방지하며, 의도하지 않은 데이터 노출을 제한하고, 무단 액세스를 방지하는 것입니다.

여타 대응과 마찬가지로 비즈니스, 규제, 법률 또는 기타 고려 사항이 적용될 수 있습니다. 예상하거나 예상치 못한 결과에 대한 의도한 조치를 평가해야 합니다. 클라우드 팀에서 리소스 태그를 사용하는 경우 이러한 태그를 통해 문의할 리소스 또는 소유자의 중요도를 식별할 수 있습니다.

포렌식 워크스테이션 시작

일부 인시던트 대응 활동에는 인시던트와 관련된 디스크 이미지, 파일 시스템, RAM 덤프 또는 기타 아티팩트를 분석하는 것이 포함될 수 있습니다. 많은 고객이 영향을 받는 데이터 볼륨(EBS 스냅샷이라고 함)의 복사본을 탑재하는 데 사용할 수 있는 맞춤형 포렌식 워크스테이션을 구축합니다. 이를 위해서는 다음과 같은 기본 단계를 따릅니다.

1. 포렌식 워크스테이션으로 사용할 수 있는 기본 Amazon Machine Image(AMI)(예: Linux 또는 Microsoft Windows)를 선택합니다.
2. 해당 기본 AMI에서 Amazon EC2 인스턴스를 시작합니다.
3. 운영 체제를 강화하고 불필요한 소프트웨어 패키지를 제거하고 관련 감사 및 로깅 메커니즘을 구성합니다.
4. 선호하는 오픈 소스 또는 프라이빗 도구 키트 제품군과 필요한 공급 업체 소프트웨어 및 패키지를 설치합니다.
5. Amazon EC2 인스턴스를 중지하고 중지된 인스턴스에서 새 AMI를 생성합니다.
6. 주간 또는 월간 프로세스를 생성하여 최신 소프트웨어 패치로 AMI를 업데이트하고 다시 구축합니다.

AMI를 사용하여 포렌식 시스템을 프로비저닝한 후 인시던트 대응 팀은 이 템플릿을 사용하여 새 AMI를 생성하여 각 조사에 대해 새 포렌식 워크스테이션을 시작할 수 있습니다. AMI를 Amazon EC2 인스턴스로 시작하는 프로세스를 미리 구성하여 배포 프로세스를 간소화할 수 있습니다. 예를 들어 필요한 포렌식 인프라 리소스를 텍스트 파일로 저장해 템플릿을 생성하고 AWS CloudFormation을 사용하여 AWS 계정에 배포할 수 있습니다.

템플릿을 통해 리소스를 신속하게 배포할 수 있다면 잘 훈련된 포렌식 전문가가 인프라를 재사용하는 대신 각 조사에 새로운 포렌식 워크스테이션을 사용할 수 있습니다. 이 과정을 통해 다른 포렌식 조사에서 교차 오염이 없는지 확인할 수 있습니다.

인스턴스 유형 및 위치

Amazon EC2는 각 사용 사례에 맞게 최적화된 다양한 인스턴스 유형을 제공합니다. 인스턴스 유형은 CPU, 메모리, 스토리지 및 네트워킹 용량의 다양한 조합으로 구성되며, 애플리케이션에 따라 적합한 리소스 조합을 선택할 수 있는 유연성을 제공합니다. 대부분의 인스턴스 유형에는 여러 인스턴스 크기가 포함되므로 대상 워크로드의 요구 사항에 맞게 리소스 규모를 조정할 수 있습니다. 인시던트 대응 인스턴스의 경우 프로덕션 인스턴스를 실행하는 네트워크의 위치 및 세분화에 대한 회사의 GRC 정책을 따릅니다.

AWS의 향상된 네트워킹에서는 지원되는 인스턴스 유형에서 단일 루트 I/O 가상화(SR-IOV)를 사용하여 고성능 네트워킹 기능을 제공합니다. SR-IOV는 기존 가상 네트워크 인터페이스에 비해 높은 I/O 성능 및 낮은 CPU 사용률을 제공하는 디바이스 가상화 방법입니다. 향상된 네트워킹을 통해 대역폭과 PPS(Packet Per Second) 성능이 높아지고, 인스턴스 간 대기 시간이 지속적으로 낮아집니다. 향상된 네트워킹 사용에 따르는 추가 요금은 없습니다. 10Gbps 또는 25Gbps의 네트워크 속도와 기타 고급 기능을 지원하는 인스턴스 유형에 대한 자세한 내용은 Amazon EC2 인스턴스 유형 단원을 참조하세요.

클라우드 제공업체 지원

주제

- AWS Managed Services
- AWS Support
- DDoS 대응 지원

AWS Managed Services

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

인프라 운영자로서 AMS는 일련의 보안 탐지 제어 기능을 배포하고 Follow-the-Sun 모델에 따라 경고에 대한 연중무휴 24시간 1차 대응을 제공합니다. 경고가 트리거되면 AMS는 일관된 응답을 보장하기

위해 표준 자동/수동 런북 세트를 따릅니다. 이러한 런북은 온보딩 중에 AMS 고객과 공유되므로 AMS와 대응을 개발하고 조정할 수 있습니다. AMS는 실제 인시던트가 발생하기 전에 고객과 보안 대응 시뮬레이션을 공동으로 실행하여 운영 역량을 개발할 것을 권장합니다.

AWS Support

AWS Support는 다양한 플랜을 제공합니다. 이러한 계획을 통해 AWS 솔루션의 성공과 운영 상태를 지원하는 도구 및 전문 지식에 액세스할 수 있습니다. 지원되는 모든 플랜은 고객 서비스, AWS 문서, 백서 및 지원 포럼에 대해 연중무휴 24시간 상시 액세스를 제공합니다. AWS 환경을 계획, 배포, 최적화하는 데 도움이 되는 기술 지원 및 추가 리소스에 액세스해야 하는 경우 AWS 사용 사례에 가장 적합한 지원 플랜을 선택할 수 있습니다.

AWS 리소스에 영향을 미치는 문제에 대한 지원을 받으려면 AWS Management Console의 지원 센터를 중앙 연락 창구로 고려해야 합니다. AWS Support에 대한 액세스는 IAM에 의해 제어됩니다. AWS 지원 기능에 액세스하는 방법에 대한 자세한 내용은 액세스 지원을 참조하세요.

또한 Amazon EC2 부정 사용을 신고해야 하는 경우AWS 부정 사용 팀 문의하세요.

DDoS 대응 지원

서비스 거부(DoS) 공격은 최종 사용자가 웹 사이트 또는 애플리케이션을 사용할 수 없게 만듭니다. 공격자는 네트워크 대역폭이나 기타 리소스를 소비하는 다양한 기술을 사용하여 합법적인 최종 사용자의 액세스를 방해합니다. 가장 간단한 형태로 대상에 대한 DoS 공격은 단일 소스의 단일 공격자에 의해 실행됩니다.

DDoS(분산 서비스 거부) 공격에서 공격자는 협력자 그룹에 의해 손상되거나 제어할 수 있는 여러 소스를 사용하여 대상에 대한 공격을 조정합니다. DDoS 공격에서는 각 협력자 또는 손상된 호스트가 공격에 참여하여 의도한 대상을 압도하는 패킷 또는 요청의 홍수를 생성합니다.

AWS는 AWS에서 실행되는 웹 애플리케이션을 보호하는 관리형 DDoS 보호 서비스인 AWS Shield를 고객에게 제공합니다. AWS Shield는 애플리케이션 가동 중지와 대기 시간을 최소화하는 상시 탐지 및 자동 인라인 통합을 제공하므로 DDoS 보호를 위해 AWS Support를 이용할 필요가 없습니다. AWS Shield에는 Standard와 Advanced라는 두 가지 티어가 있습니다.

모든 AWS 고객은 무료로 AWS Shield Standard에 의한 자동 보호를 받을 수 있습니다. AWS Shield Standard는 웹 사이트나 애플리케이션을 대상으로 가장 흔하고, 자주 발생하는 네트워크 및 전송 계층 DDoS 공격을 방어합니다. Amazon CloudFront와 Amazon Route 53에서 AWS Shield Standard를 사용할 경우에는 이미 알려진 모든 인프라(계층 3 및 4) 공격에 대해 포괄적인 가용성 보호를 받을 수 있습니다.

Amazon Elastic Compute Cloud(Amazon EC2), Elastic Load Balancing(ELB), Amazon CloudFront 및 Amazon Route 53 리소스에서 실행되는 웹 애플리케이션을 대상으로 하는 공격에 대해 더 높은 수준의 보호를 구현하려면 AWS Shield Advanced를 구독하면 됩니다. 또한 AWS Shield Advanced를 구독하면 AWS DDoS 대응 팀(DRT)에 연중무휴 24시간 액세스할 수 있습니다. AWS Shield Standard 및 AWS Shield Advanced에 대한 자세한 내용은 AWS Shield 단원을 참조하세요.

시뮬레이션

주제

보안 인시던트 대응 시뮬레이션

보안 인시던트 대응 시뮬레이션(SIRS)은 실제 시나리오에서 인시던트 대응 계획 및 절차를 실행할 수 있는 체계적인 기회를 제공하는 내부 이벤트입니다. SIRS 이벤트는 기본적으로 대응 능력을 준비하고 반복적으로 개선하기 위한 것입니다. SIRS 활동을 수행하는 것이 중요한 몇 가지 이유는 다음과 같습니다.

- 준비 상태 검증
- 자신감 향상 – 시뮬레이션 및 교육 담당자를 통한 학습
- 규정 준수 또는 계약 의무 준수
- 인증을 위한 아티팩트 생성
- 민첩성을 유지하고 집중하여 점진적으로 개선
- 속도 및 도구 개선
- 커뮤니케이션 및 에스컬레이션 방법 개선
- 드문 상황이나 예기치 않은 상황에 대한 대처 능력 개발

이러한 이유로 SIRS 활동에 참여하는 동안 파생된 가치는 스트레스 이벤트 발생 시 조직의 실효성을 높입니다. 현실적이고 유리한 SIRS 활동을 개발하는 것은 어려운 연습이 될 수 있습니다. 제대로 파악한 이벤트를 처리하는 절차 또는 자동화를 테스트하는 것도 몇 가지 장점이 있지만, 창의적인 SIRS 활동에 참여하여 예기치 않은 상황을 테스트하는 경우도 그만한 가치가 있습니다.

시뮬레이션 단계

자체 SIRS를 설계하든 기반을 제공할 신뢰할 수 있는 파트너가 있든 관계없이 시뮬레이션은 일반적으로 다음 단계를 따릅니다.

1. 중요한 문제 찾기 - 응답을 유발해야 하는 트리거를 정의합니다.

2. 숙련된 보안 엔지니어 식별 - 시뮬레이션에는 빌더와 테스터가 필요합니다.
3. 현실적인 모델 시스템 구축 - 시뮬레이션은 현실적이고 적절해야 합니다. 현실적이지 않을 경우 참가자가 연습을 중요하게 여기지 않을 수 있습니다. 너무 작으면 연습을 사소한 것으로 간주할 수 있습니다. 간단한 연습으로 시작하여 전체 이벤트로 나아가 보세요.
4. 시나리오 요소 구축 및 테스트 - 아티팩트 로깅, 이메일 알림 및 경고, 잠재적 런북 등 관련 시뮬레이션 자료를 작성해야 할 수 있습니다.
5. 다른 보안 담당자 및 여러 조직의 참가자 초대 - 교육 및 참여가 필요한 모든 사람을 초대합니다. 일반 법률 고문, 임원 및 홍보 담당자가 시뮬레이션에 참여하는 경우 해당 직원도 초대해야 합니다.
6. 시뮬레이션 실행 - 직원에게 SIRS 이벤트를 예고해야 하는지 또는 시뮬레이션이 예고 없이 실행되어야 하는지 선택합니다.
7. 축하, 측정, 개선 및 반복 - 시뮬레이션에는 스트레스 요인이 있으므로 참가자의 노력을 장려하고 축하하는 것이 중요합니다. 격려 후에는 다음 시뮬레이션을 위해 측정, 개선 및 반복할 수 있는 기회가 생깁니다. AWS에서는 이러한 활동을 습관화 하도록 권장합니다.

> **Important**
>
> SIRS(보안 인시던트 대응 시뮬레이션)를 계획하는 경우 침투 테스트를 참조하고 진행 방법에 대한 최신 정보는 기타 시뮬레이션 이벤트 단원을 검토하세요.

시뮬레이션 예제

예상 가치를 제공하려면 보안 시뮬레이션이 현실적이어야 합니다. 사용자 또는 파트너가 자체 시뮬레이션을 만들기 위해 노력할 때 항상 과거의 실제 이벤트를 잠재적인 시뮬레이션 연습의 중요한 소스로 간주해야 합니다. 다음은 AWS 고객이 초기 시뮬레이션에 유용하게 사용할 수 있는 몇 가지 예입니다.

- 네트워크 구성 또는 리소스가 무단으로 변경됨
- 개발자의 잘못된 구성으로 인해 자격 증명이 실수로 공개적으로 노출됨
- 개발자의 잘못된 구성으로 인해 민감한 콘텐츠에 공개적으로 액세스할 수 있게 됨
- 의심되는 악성 IP 주소와 통신하는 웹 서버 격리

가치 있고 경험적인 학습 외에도 SIRS 활동을 수행하면 배운 교훈과 같은 결과물이 생성되어 프로그램의 다음 프로세스인 반복에 대한 입력으로 사용할 수 있습니다.

반복

이전 단원에서는 SIRS 활동의 몇 가지 이점을 정의했습니다. 이러한 이점 중에는 점진적인 개선을 통해 민첩성을 확보하는 것이 있었습니다. 시뮬레이션은 보안 대응을 개선하는 데 활용할 수 있는 귀중한 결과를 생성해야 합니다. 시뮬레이션은 조직에 효과가 있는 방법과 그렇지 않은 것에 대한 피드백 루프를 제공합니다. 이러한 지식을 바탕으로 새로운 절차를 점진적으로 생성하거나 기존 절차를 업데이트하여 대응 방법을 개선할 수 있습니다.

주제

- 런북
- 자동화

런북

보안 이상이 탐지될 경우 사고를 통제하고 알려진 정상 상태로 되돌리는 것이 대응 계획의 중요한 요소입니다. 예를 들어 보안 구성 오류로 인해 이상이 발생한 경우 적절한 구성으로 리소스를 재배포하여 변형을 제거하는 것만으로 간단하게 해결할 수 있습니다. 이렇게 하려면 미리 계획을 세우고 런북이라고 하는 자체 보안 대응 절차를 정의해야 합니다.

런북은 작업 또는 일련의 작업을 수행하기 위한 조직 절차를 문서화한 것입니다. 이 문서는 일반적으로 내부 디지털 시스템이나 종이 문서에 저장됩니다. 현재 인시던트 대응 런북이 있을 수도 있고 보안 보증 프레임워크를 준수하기 위해 런북을 새로 생성해야 할 수도 있습니다. 그러나 기존에 작성된 런북을 수동으로 따를 경우 실수를 할 가능성이 높아집니다. 대신 반복 가능한 모든 작업을 자동화하는 것이 좋습니다. 자동화를 통해 대응 팀은 일반적인 작업에서 벗어나 이벤트 상관 관계, 시뮬레이션 연습, 새로운 대응 절차 고안, 연구 수행, 새로운 기술 개발, 새로운 도구 테스트 또는 구축과 같은 더 중요한 작업에 집중할 수 있습니다. 그러나 작업을 프로그래밍 가능한 로직으로 분해하고 반복을 통해 적절한 자동화를 구현하려면 먼저 런북을 작성해야 합니다.

런북 작성

클라우드용 런북을 작성하려면 먼저 현재 생성하고 있는 알림에 집중하는 것이 좋습니다. 알림을 생성하는 경우 알림을 조사하는 것이 중요합니다. 먼저 수행하고 있는 수동 프로세스에 대한 설명을 정의합니다. 그런 다음, 프로세스를 테스트하고 런북 패턴을 반복하여 대응의 핵심 로직을 개선합니다. 어떠한 예외가 있는지 그리고 그러한 시나리오에 대한 대체 해결 방법을 파악합니다. 예를 들어 개발 환경에서 잘못 구성된 Amazon EC2 인스턴스를 종료하고자 할 수 있습니다. 그런데 같은 이벤트가 프로덕

션 환경에서 발생한 경우에는 인스턴스를 종료하는 대신 인스턴스를 중지한 후에 중요한 데이터가 손실되지 않으며 종료해도 괜찮은지를 이해 관계자와 함께 확인하고자 할 수도 있습니다.

최상의 솔루션을 결정한 후에는 로직을 코드 기반 솔루션으로 분해할 수 있습니다. 코드 기반 솔루션은 많은 대응 담당자가 대응을 자동화하고 대응 담당자의 편차나 추측을 제거하는 도구로 사용할 수 있습니다. 이렇게 하면 대응의 수명 주기가 빨라집니다. 다음 목표는 인간 대응 담당자에 의해 실행되는 것이 아니라 알림 또는 이벤트 자체에서 이 코드가 호출되도록 함으로써 완벽한 자동화를 구현하는 것입니다.

시작하기

어디서부터 시작해야 할지 잘 모르는 경우 AWS Trusted Advisor, AWS Security Hub의 기본 보안 모범 사례 및 AWS Config 규칙(AWS Config 규칙 Github 리포지토리 포함)로 생성할 수 있는 알림으로 시작하는 것이 좋습니다. 그런 다음 관심 있는 시스템을 설명하는 서비스에서 생성된 이벤트에 초점을 맞추는 것이 좋습니다.

Amazon GuardDuty 및 Access Analyzer는 애플리케이션이 AWS에서 사용할 많은 도메인을 설명하므로 일반적으로 권장되며, Amazon Inspector와 Amazon Macie는 데이터 및 엔드포인트 문제가 있는 도메인에 사용하기에 적합합니다. Amazon GuardDuty 결과에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서에서 확인할 수 있습니다. Access Analyzer 결과는 Amazon Access Analyzer 사용 설명서에서 확인할 수 있습니다. Macie 결과는 Amazon Macie 사용 설명서에서 확인할 수 있습니다. Amazon Inspector 결과는 Amazon Inspector 사용 설명서에서 확인할 수 있습니다. Security Hub는 이러한 결과를 한 곳으로 통합하고 짧은 대기 시간으로 함께 대응할 수 있는 기능을 제공하므로 문제 해결을 위한 중앙 위치로 권장됩니다.

위의 모든 서비스는 새로 생성된 알림 및 기존 알림에 대한 업데이트를 포함하여 결과 또는 알림에 변경 사항이 발생할 경우 Amazon CloudWatch Events를 통해 알림을 전송합니다. Amazon CloudWatch Events 규칙을 설정하여 이벤트 기반 응답을 수행하는 AWS Lambda 함수를 트리거할 수 있습니다. 그러나 사용자 지정 인사이트를 구축하고 애플리케이션 도메인에서 자체 결과를 추가하는 기능이 있다는 점은 대신 Security Hub를 사용해야 하는 중요한 이유입니다. 자세한 내용은 이벤트 기반 대응 단원을 참조하세요.

자동화

자동화는 전력승수입니다. 즉, 조직의 속도에 맞게 대응 담당자의 작업을 확장합니다. 수동 프로세스에서 자동화된 프로세스로 전환하면 AWS 클라우드 환경의 보안을 강화하는 데 더 많은 시간을 할애할 수 있습니다.

주제

- 인시던트 대응 자동화
- 이벤트 기반 대응

인시던트 대응 자동화

보안 엔지니어링 및 운영 기능을 자동화하기 위해 AWS의 포괄적인 API 및 도구 세트를 사용할 수 있습니다. 자격 증명 관리, 네트워크 보안, 데이터 보호 및 모니터링 기능을 완전히 자동화할 수 있습니다. 보안 자동화를 구축하면 직원이 보안 태세를 모니터링하면서 수동으로 이벤트에 대응하는 것이 아니라 시스템이 모니터링 및 검토하고 대응을 시작하도록 할 수 있습니다.

인시던트 대응팀은 같은 방식으로 계속 알림에 대응할 경우 알림에 대한 피로감을 느낄 위험이 있습니다. 시간이 지남에 따라 팀이 알림에 무감각한 상태가 되어 일상적인 상황을 처리하는 데 실수하거나 비정상적인 알림을 놓칠 수 있습니다. 자동화는 반복적이고 일상적인 알림을 처리하는 기능을 사용함으로써 알림에 대한 피로감을 방지하며, 중요하고 특별한 인시던트만 사람이 직접 처리하도록 합니다.

프로세스의 단계를 프로그래밍 방식으로 자동화하여 수동 프로세스를 개선할 수 있습니다. 이벤트에 대한 문제 해결 패턴을 정의한 후 해당 패턴을 실행 가능한 로직으로 분해하고 코드를 작성하여 해당 로직을 수행할 수 있습니다. 그런 다음, 대응 담당자가 해당 코드를 실행하여 문제를 해결할 수 있습니다. 시간이 지남에 따라 점점 더 많은 단계를 자동화할 수 있으며, 궁극적으로 일반적인 인시던트의 전체 클래스를 자동으로 처리할 수 있습니다.

그러나 목표는 탐지 메커니즘과 대응 메커니즘 간의 시간 간격을 더욱 줄이는 것입니다. 기존에는 이 시간 간격이 몇 시간, 며칠 또는 몇 달이 될 수 있었습니다. 2016년 SANS의 인시던트 대응 설문 조사에 따르면 응답자의 21%가 탐지하는 데 2~7일이 걸렸으며 응답자의 29%만이 동일 기간 내에 이벤트를 해결할 수 있다고 답했습니다. 클라우드에서는 이벤트 기반 대응 기능을 구축하여 대응 시간 간격을 초 단위로 줄일 수 있습니다.

주제

- 대응 자동화를 위한 옵션
- 스캔 방법의 비용 비교

대응 자동화를 위한 옵션

엔터프라이즈 구현과 조직 구조 간에 균형을 이루는 것이 중요합니다. 그림 4는 AWS 구현의 각 자동화된 대응 옵션이 지닌 기술적 속성의 차이를 방사형 차트와 함께 보여 줍니다. 차트에서 기술적 속성이 차트 중앙에서 멀어질수록 해당 자동화된 대응에 대한 기술적 속성의 강도가 커집니다. 예를 들어, AWS Lambda는 더 빠른 속도를 제공하고 기술적 스킬이 덜 필요합니다. AWS Fargate는 더 많은 유연

성을 제공하고 유지 관리 및 기술적 스킬이 덜 필요합니다. 표 1은 이러한 자동화 옵션에 대한 개요와 각 자동화 옵션의 기술적 속성에 대한 요약을 제공합니다.

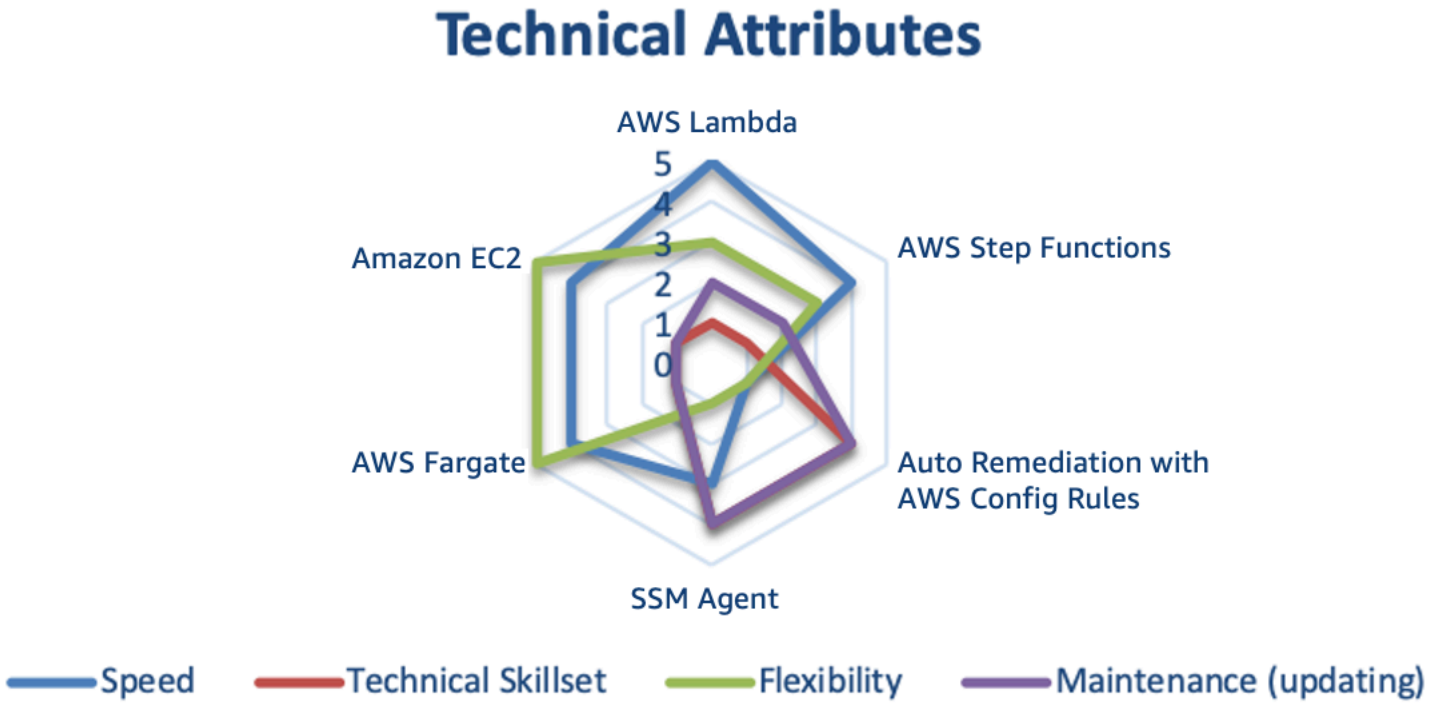

그림 4: 자동화된 대응 방식 전반의 기술적 속성의 차이

표 1: 자동화된 대응 옵션

AWS 서비스 또는 기능	설명	속성 요약*
AWS Lambda	AWS Lambda만 사용하며, 조직의 엔터프라이즈 언어를 사용하는 시스템	속도 유연성 유지 관리 기술 세트
AWS Step Functions	AWS Step Functions, Lambda 및 SSM Agent를 사용하는 시스템	속도 유연성 유지 관리 기술 세트

AWS 서비스 또는 기능	설명	속성 요약*
AWS Config 규칙을 사용한 자동 문제 해결	환경을 평가한 후 승인된 사양으로 다시 푸시하는 일련의 AWS Config 규칙 및 자동 문제 해결 세트	유지 관리 및 기술 세트 속도 및 유연성
SSM Agent	환경 및 내부 시스템의 많은 부분을 검토하고 수정하는 자동화 규칙 및 문서 세트	유지 관리 및 기술 세트 속도 유연성
AWS Fargate	Amazon CloudWatch 및 기타 시스템의 오픈 소스 Step Functions 코드와 이벤트를 사용하여 탐지 및 문제 해결을 수행하는 AWS Fargate 시스템	유연성 속도 유지 관리 및 기술 세트
Amazon EC2	전체 인스턴스에서 실행되는 시스템으로, AWS Fargate 옵션과 유사	유연성 속도 유지 관리 기술 세트

* 속성은 각 서비스 또는 기능에 대해 내림차순으로 나열됩니다. 예를 들어, AWS Lambda는 더 빠른 속도를 제공하고 기술적 스킬이 덜 필요합니다. AWS Fargate는 더 많은 유연성을 제공하며 유지 관리 및 기술적 스킬이 덜 필요합니다.

AWS 환경에서 이러한 자동화 옵션을 고려할 때 중앙 집중화 및 스캔 기간(초당 이벤트 수[EPS])도 고려해야 합니다.

중앙 집중화는 조직의 모든 탐지 및 문제 해결을 수행하는 중앙 계정을 의미합니다. 이 접근 방식은 즉시 사용할 수 있는 최선의 선택처럼 보일 수 있으며 현재 모범 사례입니다. 그러나 일부 상황에서는 이러한 접근 방식에서 벗어나야 하며, 그 시점을 파악하는 것은 하위 계정을 처리하는 방법에 따라 달라집니다. AWS Organizations의 다중 계정 프레임워크 또는 AWS Control Tower의 Security Tooling 계정 접근 방식을 활용하여 시작하는 것이 좋습니다.

표 2: 중앙 집중화의 장단점

	중앙 집중식	탈중앙화
장점	간단한 구성 관리 대응을 취소하거나 수정할 수 없음	단순한 아키텍처 더 빠른 초기 설정
단점	아키텍처의 복잡성 증가 계정 및 리소스 온보딩/오프보딩	관리해야 할 리소스의 증가 소프트웨어 기준을 유지 관리하기가 어려움

이러한 구현에 대한 비용 비교는 최상의 옵션을 결정하는 데 있어 기업의 의사 결정을 주도할 수도 있습니다. 초당 이벤트 수(EPS)는 비용을 가장 잘 예측하기 위해 사용하는 지표입니다. 결국 중앙 집중식 또는 탈중앙화 접근 방식을 사용하는 것이 훨씬 쉽고 저렴할 수 있습니다. 하지만 계정에서 해당 비용을 구체적으로 평가하는 방법을 검토하는 것은 불가능합니다. 이러한 이벤트를 이벤트에 대응할 중앙 계정으로 보낼 때는 EPS를 고려해야 합니다. EPS가 높을수록 이러한 이벤트를 중앙 집중식 계정으로 보내는 데 드는 비용이 증가합니다.

스캔 방법의 비용 비교

비용은 이상을 탐지하는 데 사용되는 스캔 방법과 검증 간 기간에 따라 추가로 결정됩니다. 스캔 방법의 경우 이벤트 기반 또는 정기적 스캔 검토 중에서 선택할 수 있습니다. 표 3은 두 가지 접근 방식의 장단점을 보여줍니다.

표 3: 두 스캔 방법의 장단점

	이벤트 기반	정기적 스캔
장점	이벤트에서 대응까지 걸리는 시간 단축 추가 API 호출을 쿼리해야 하는 필요성이 제한됨	특정 시점을 전체적으로 파악할 수 있음
단점	리소스에 대한 상태 컨텍스트가 제한됨	대규모 계정에 대한 서비스 한도

	이벤트 기반	정기적 스캔
	트리거된 이벤트가 쉽게 사용할 수 없는 리소스에 대한 이벤트일 수 있음	대량의 API 호출로 인해 제한이 발생할 수 있음

대부분의 경우 완전히 성숙한 조직에서는 두 가지 스캔 접근 방식을 조합하는 것이 최선의 선택일 가능성이 높습니다. AWS Security Hub 및 AWS 기본 보안 모범 사례 표준은 두 스캔 방법의 조합을 제공합니다.

그림 5는 각 자동화 접근 방식에 대한 초당 이벤트(EPS) 비용을 비교해 보여 주는 방사형 차트를 제공합니다. 예를 들어 Amazon EC2와 AWS Fargate는 0~10개의 EPS를 실행하는 비용이 가장 높은 반면 AWS Lambda와 AWS Step Functions는 76개 이상의 EPS를 실행하는 비용이 가장 높습니다.

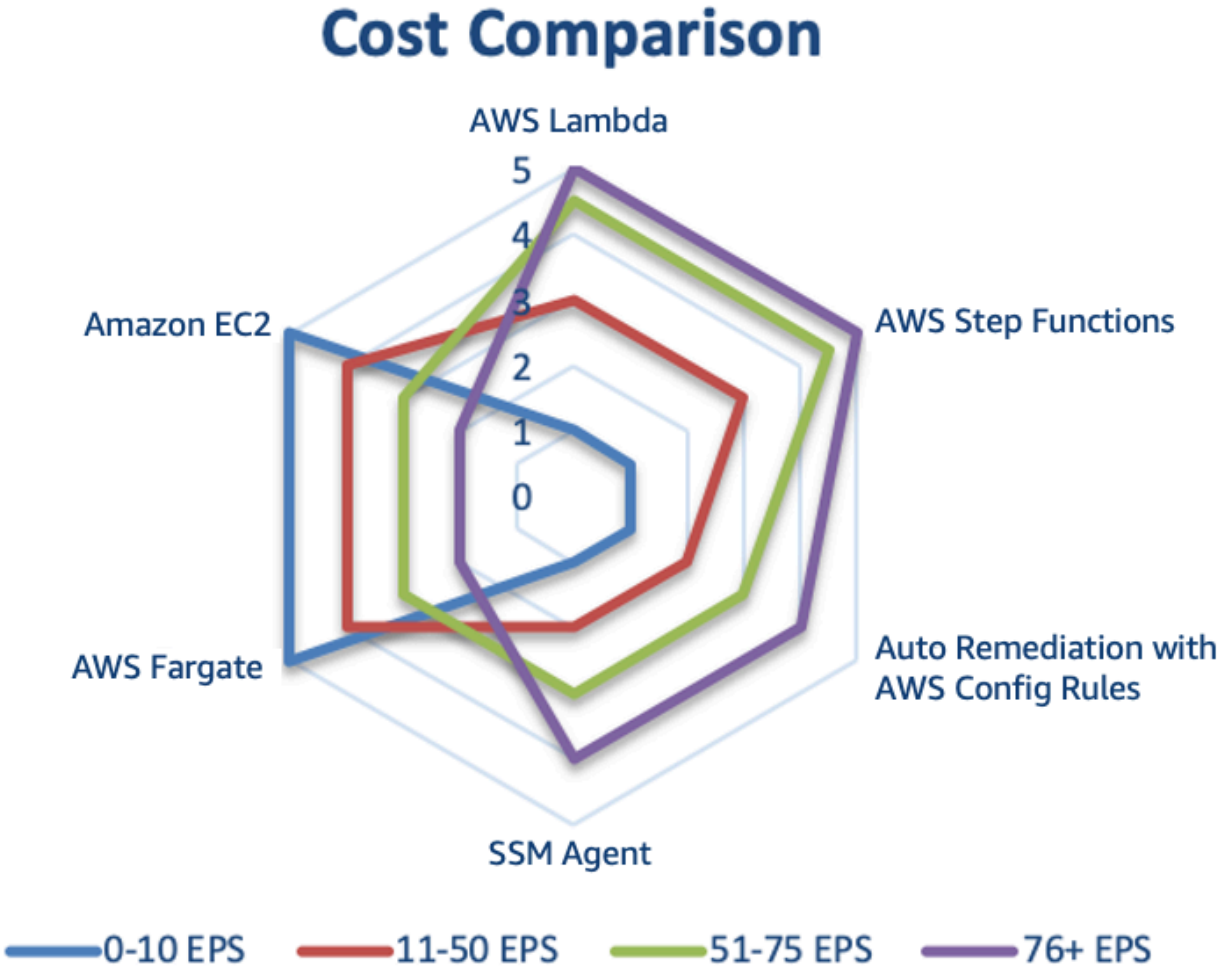

그림 5: 자동화 옵션 스캔 방법의 비용 비교(초당 이벤트 수[EPS])

이벤트 기반 대응

이벤트 기반 대응 시스템을 사용하면 감지 메커니즘이 대응 메커니즘을 트리거하여 이벤트를 자동으로 수정합니다. 이벤트 기반 대응 기능을 사용하여 감지 메커니즘과 대응 메커니즘 간의 가치 실현 시간을 단축할 수 있습니다. 이러한 이벤트 기반 아키텍처를 생성하기 위해 이벤트에 대한 대응으로 코드를 실행하고 기본 컴퓨팅 리소스를 자동으로 관리하는 서버리스 컴퓨팅 서비스인 AWS Lambda를 사용할 수 있습니다.

예를 들어 AWS CloudTrail 서비스가 활성화된 AWS 계정이 있다고 가정해 보겠습니다. AWS CloudTrail이 `cloudtrail:StopLogging` API를 통해 비활성화되어 있는 경우 대응 절차는 서비스를 다시 활성화하고 AWS CloudTrail 로깅을 비활성화한 사용자를 조사하는 것입니다. AWS Management Console에서 이러한 단계를 수동으로 수행하는 대신 `cloudtrail:StartLogging` API를 통해 프로그래밍 방식으로 로깅을 다시 활성화할 수 있습니다. 코드를 사용하여 구현하는 경우 대응 목표는 가능한 한 빨리 이 작업을 수행하고 대응 담당자에게 대응이 수행되었음을 알리는 것입니다.

로직을 간단한 코드로 분해하고 AWS Lambda 함수에서 실행하여 이러한 작업을 수행할 수 있습니다. 그런 다음 Amazon CloudWatch Events를 사용하여 특정 `cloudtrail:StopLogging` 이벤트를 모니터링하고 이벤트가 발생하면 함수를 호출할 수 있습니다. Amazon CloudWatch Events에서 이 AWS Lambda 대응 담당 함수를 호출하면 비활성화된 AWS CloudTrail 보안 주체의 정보, 비활성화된 시간, 영향을 받은 특정 리소스 및 기타 관련 정보와 함께 특정 이벤트의 세부 정보를 이 함수에 전달할 수 있습니다. 이 정보를 사용하여 로그에서 검색 결과를 보강한 다음 응답 분석가가 필요로 하는 특정 값만 사용하여 알림을 생성할 수 있습니다.

이벤트 기반 응답의 목표는 Lambda 대응 담당 함수가 응답 작업을 수행한 후 대응 담당자에게 관련 컨텍스트 정보로 예외 항목이 성공적으로 해결되었음을 알리는 것입니다. 그런 다음 발생한 이유와 향후 재발을 예방할 수 있는 방법을 결정하는 것은 인간 대응 담당자의 몫입니다. 이 피드백 루프는 클라우드 환경의 보안을 더욱 향상시킵니다. 이 목표를 달성하려면 보안 팀이 개발 및 운영 팀과 더 긴밀하게 협력할 수 있는 문화가 조성되어야 합니다.

인시던트 대응 예제

주제

서비스 도메인 인시던트

서비스 도메인 인시던트는 일반적으로 AWS API를 통해서만 처리됩니다.

자격 증명

AWS는 수백만 명의 고객이 새로운 애플리케이션을 구축하고 비즈니스 성과를 창출하는 데 사용하는 API를 AWS 클라우드 서비스에 제공합니다. 이러한 API는 소프트웨어 개발 키트(SDK), AWS CLI, AWS Management Console 등 여러 가지 방법을 통해 호출할 수 있습니다. 이러한 방법으로 AWS와 상호 작용하려는 경우 IAM 서비스를 통해 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있습니다. IAM을 사용하면 리소스를 사용하도록 인증(로그인함) 및 권한 부여(권한 있음)된 대상을 제어할 수 있습니다. IAM과 함께 사용할 수 있는 AWS 서비스 목록은 IAM과 작동하는 AWS 서비스를 참조하세요.

AWS 계정을 처음 생성하는 경우에는 전체 AWS 서비스 및 계정 리소스에 대해 완전한 액세스 권한을 지닌 통합 인증(SSO) 자격 증명으로 시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업, 특히 관리 작업에는 루트 사용자를 사용하지 않는 것이 좋습니다. 대신, IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례를 따르는 것이 좋습니다. 그런 다음 루트 사용자 자격 증명은 안전하게 보관하다가 몇몇 계정 및 서비스 관리 작업을 수행할 때만 사용하세요. 자세한 내용은 개별 IAM 사용자 생성을 참조하세요.

이러한 API는 수백만 명의 고객에게 가치를 제공하지만 악의를 가진 개인이 IAM 계정 또는 루트 자격 증명에 액세스하면 일부 API가 악용될 수 있습니다. 예를 들어, API를 사용하여 사용자의 계정 내에서 로깅(예: AWS CloudTrail)을 활성화할 수 있습니다. 공격자가 사용자의 자격 증명을 알아내 API를 사용하여 이러한 로그를 비활성화할 수도 있습니다. 최소 권한 모델을 따르는 적절한 IAM 권한을 구성하고 IAM 자격 증명을 적절히 보호하여 이러한 유형의 부정 사용을 방지할 수 있습니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 모범 사례를 참조하세요. 이러한 유형의 이벤트가 발생할 경우를 대비하여 AWS CloudTrail, AWS Config, AWS Trusted Advisor, Amazon GuardDuty 및 AWS CloudWatch Events를 포함하여 AWS CloudTrail 로깅이 비활성화되었음을 식별할 수 있는 여러 탐지 컨트롤이 있습니다.

리소스

악용되거나 잘못 구성될 수 있는 기타 기능은 각 고객이 클라우드에서 운영하는 방식에 따라 조직마다 다릅니다. 예를 들어, 일부 조직에서는 특정 데이터 또는 애플리케이션에 공개적으로 액세스할 수 있도록 하고 다른 조직에서는 애플리케이션과 데이터를 내부에서만 사용하도록 허용하고 기밀로 유지하려고 합니다. 모든 보안 이벤트가 악의적 행위를 나타내는 것은 아니며, 일부 이벤트는 의도하지 않거나 부적절한 구성으로 인해 발생할 수 있습니다. 조직에 큰 영향을 미치는 API나 기능이 무엇인지, 해당 API나 기능을 자주 사용하는지 등을 고려하세요.

도구 및 서비스를 사용하면 많은 보안 구성 오류를 식별할 수 있습니다. 예를 들어 AWS Trusted Advisor에서는 모범 사례에 대한 여러 가지 검사를 제공합니다. APN 파트너는 고객 온프레미스 환경의 기존 제어 솔루션과 동등하거나 기존 솔루션과 통합된 업계 최고 수준의 수백 가지 제품을 제공합니다. 이러한 제품 및 솔루션 중 다수는 AWS 파트너 컴피턴시 프로그램을 통해 사전 검증되었습니다. APN 보안 컴피턴시 프로그램의 구성 및 취약성 분석 단원에서 이러한 솔루션을 찾아보고 고유한 요구 사항을 해결할 수 있는지 확인하는 것이 좋습니다.

인프라 도메인 인시던트

인프라 도메인에는 일반적으로 애플리케이션의 데이터 또는 네트워크 관련 활동(예: VPC 내 Amazon EC2 인스턴스에 대한 트래픽 및 Amazon EC2 인스턴스 운영 체제에서 실행되는 프로세스)이 포함됩니다.

예를 들어, 모니터링 솔루션이 Amazon EC2 인스턴스의 잠재적 보안 이상을 알려준다고 가정해 보겠습니다. 이 문제를 해결하기 위한 일반적인 단계는 다음과 같습니다.

1. 환경을 변경하기 전에 Amazon EC2 인스턴스에서 메타데이터를 캡처합니다.
2. 인스턴스에 대해 종료 방지 기능을 활성화하여 Amazon EC2 인스턴스가 실수로 종료되지 않도록 보호합니다.
3. VPC 보안 그룹을 전환하여 Amazon EC2 인스턴스를 격리합니다. 하지만 VPC 연결 추적 및 기타 억제 기술에 유의해야 합니다.
4. Amazon EC2 인스턴스를 AWS Auto Scaling 그룹에서 분리합니다.
5. Amazon EC2 인스턴스를 관련 Elastic Load Balancing 서비스에서 등록 취소합니다.
6. 보존 및 후속 조사를 위해 EC2 인스턴스에 연결된 Amazon EBS 데이터 볼륨의 스냅샷을 생성합니다.
7. Amazon EC2 인스턴스에 조사를 위해 격리된 것으로 태그를 지정하고 조사와 관련된 문제 티켓과 같은 관련 메타데이터를 추가합니다.

AWS API, AWS SDK, AWS CLI 및 AWS Management Console을 사용하여 앞의 모든 단계를 수행할 수 있습니다. 이러한 방법으로 AWS와 상호 작용하려는 경우 IAM 서비스를 통해 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있습니다. IAM을 사용하여 리소스를 사용하도록 인증 및 권한 부여된 사용자를 계정 수준에서 제어합니다. IAM 서비스는 이러한 작업을 수행하고 서비스 도메인과 상호 작용할 수 있도록 인증 및 권한 부여를 제공합니다.

Amazon EBS 볼륨의 스냅샷은 EBS 데이터 볼륨의 특정 시점에 대한 블록 수준 복사본으로, 비동기식으로 발생하며 완료하는 데 시간이 걸릴 수 있지만 앞으로 해당 데이터의 델타입니다. 이러한 사본에서 새 EBS 볼륨을 생성하고 이를 포렌식 EC2 인스턴스에 탑재하여 포렌식 조사관이 오프라인에서 심층 분석하도록 할 수 있습니다. 다음 다이어그램은 결과의 단순화된 버전을 보여 주며 모든 네트워크 구성 요소(예: 서브넷, 라우팅 테이블 및 네트워크 액세스 제어 목록)를 설명하지는 않습니다.

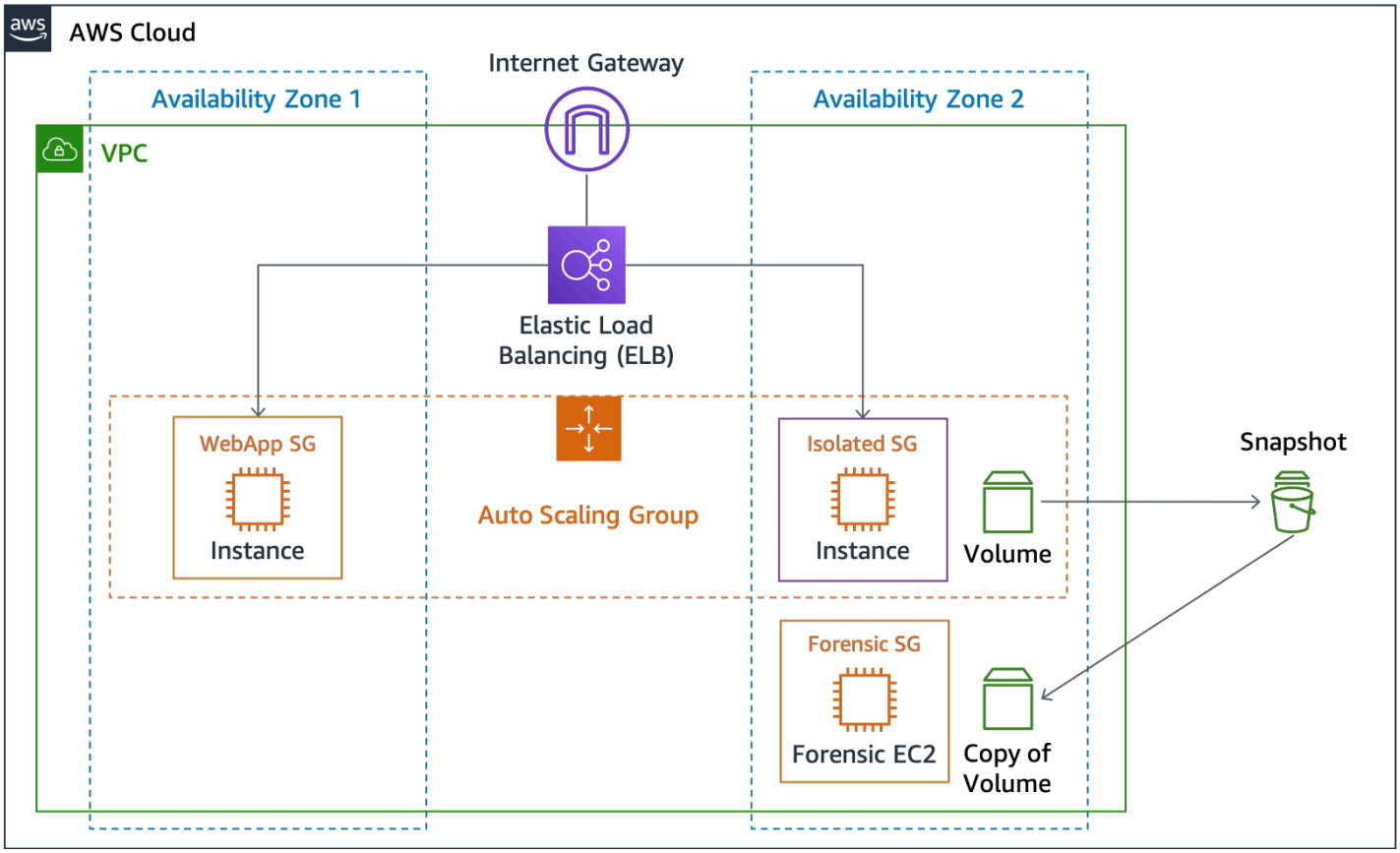

그림 6: EC2 인스턴스 격리 및 스냅샷 생성

주제

- 조사 결정
- 휘발성 데이터 캡처
- AWS Systems Manager 사용
- 캡처 자동화

조사 결정

이때 오프라인 조사(인스턴스 즉시 종료) 또는 온라인 조사(인스턴스 실행 유지) 중에서 선택할 수 있습니다. 오프라인 조사의 한 가지 이점은 인스턴스가 종료된 후에는 기존 환경에 더 이상 영향을 미치지 않는다는 것입니다. 또한 EBS 스냅샷에서 영향을 받는 인스턴스의 사본을 생성하고 조사를 위해 특별히 설계된 격리된 환경에서 격리된 AWS 계정을 사용하여 검토할 수 있습니다. 하지만 온라인 조사를 통해 호스트 운영 체제에서 메모리 또는 네트워크 트래픽과 같은 휘발성 증거를 포착할 수 있는 경우 인스턴스를 즉시 종료하지 않도록 선택할 수 있습니다.

휘발성 데이터 캡처

온라인 조사를 수행하도록 선택하지 않을 수도 있지만 인스턴스에서 휘발성 데이터를 캡처하는 데 필요한 메커니즘을 이해하는 것이 중요합니다. 온라인 조사를 수행하려면 Amazon EC2 인스턴스에서 실행 중인 운영 체제와의 상호 작용이 필요합니다. 이 시나리오에서는 Amazon EC2 인스턴스에서 작업을 실행하기 위해 AWS IAM 서비스 이상의 더 많은 서비스가 필요합니다. 표준 방법(예: Linux 보안 셸(SSH) 또는 Microsoft Windows 원격 데스크톱(RDP))을 사용하여 컴퓨터에 직접 인증할 수 있지만 운영 체제와 수동으로 상호 작용하는 것은 좋은 방법이 아닙니다. 자동화 도구를 프로그래밍 방식으로 사용하여 호스트에서 작업을 실행하는 것이 좋습니다.

AWS Systems Manager 사용

AWS Systems Manager Run Command를 사용하면 대상 인스턴스에서 Linux 셸 스크립트 및 Windows PowerShell 명령을 실행하는 온디맨드 변경을 원격으로 안전하게 수행할 수 있습니다. AWS IAM 서비스의 권한을 통해 Run Command를 호출할 수 있지만, 먼저 Amazon EC2 인스턴스를 관리형 인스턴스로 활성화하고, 시스템에 SSM Agent를 설치하고(기본적으로 설치되지 않은 경우), AWS IAM 권한을 구성해야 합니다. 자동화 또는 대응 활동에 Run Command를 사용하려는 경우 조사를 수행하기 전에 사전 요구 사항 활동을 완료해야 합니다.

Run Command를 포함하는 AWS Systems Manager는 Systems Manager에 의해 또는 Systems Manager를 대신하여 수행된 API 호출을 캡처하고 로그 파일을 지정한 Amazon S3 버킷으로 전송하는 서비스인 AWS CloudTrail과 통합됩니다. AWS CloudTrail에서 수집하는 정보를 참조하여 어떤 요청이 이루어졌는지, 어떤 소스 IP 주소에서 요청했는지, 누가 언제 요청했는지 등을 확인할 수 있습니다. CloudTrail은 Run Command를 사용하여 명령을 실행하거나 Systems Manager 문서를 생성하기 위한 API 요청을 포함하여 모든 Systems Manager API 작업에 대한 로그를 생성합니다.

AWS Systems Manager Run Command 서비스를 사용하여 Linux 셸 스크립트 및 Windows PowerShell 명령을 실행하는 SSM Agent를 호출할 수 있습니다. 이러한 스크립트는 Linux Memory Extractor(LiME) 커널 모듈과 같은 호스트에서 추가 데이터를 캡처하는 특정 도구를 로드하고 실행할

수 있습니다. 그런 다음 메모리 캡처를 VPC 네트워크의 포렌식 Amazon EC2 인스턴스로 또는 안정적인 저장을 위해 Amazon S3 버킷으로 전송할 수 있습니다.

캡처 자동화

SSM Agent를 호출하는 한 가지 방법은 인스턴스에 특정 태그가 지정된 경우 Amazon CloudWatch Events를 통해 Run Command를 대상으로 하는 것입니다. 예를 들어 영향을 받는 인스턴스에 `Response=Isolate+MemoryCapture` 태그를 적용하는 경우 다음 두 가지 작업을 트리거하도록 Amazon CloudWatch Events를 구성할 수 있습니다.

- 격리 활동을 수행하는 Lambda 함수
- 셸 명령을 실행하여 SSM Agent를 통해 Linux 메모리를 내보내는 Run Command

이 태그 기반 응답은 이벤트 기반 응답의 또 다른 방법입니다.

결론

클라우드 여정을 계속하면서 앞서 언급한 AWS 환경을 위한 기본적인 보안 인시던트 대응 개념을 고려하는 것이 중요합니다. 사용 가능한 제어, 클라우드 기능 및 문제 해결 옵션을 함께 활용하여 클라우드 환경의 보안을 개선할 수 있습니다. 또한 소규모로 시작하고 자동화 기능을 통한 반복으로 대응 속도를 높일 수 있으므로 보안 이벤트가 발생할 때 더 잘 대비할 수 있습니다.

추가 리소스

다음에서 추가 정보를 참조하세요.

- AWS Well-Architected
- AWS Cloud Adoption Framework 페이지
- AWS 중앙 집중식 로깅 솔루션
- AWS Glue 및 Amazon QuickSight를 사용하여 AWS CloudTrail 로그 시각화
- How to Monitor Host-Based Intrusion Detection System Alerts on Amazon EC2 Instances
- Store and Monitor OS & Application Log Files with Amazon CloudWatch
- Amazon S3의 Identity and Access Management
- 버전 관리 사용(Amazon S3)
- MFA Delete 사용
- AWS KMS 관리형 키를 사용하는 서버 측 암호화(SSE-KMS)로 데이터 보호
- AWS 콘솔 및 CLI를 사용한 인시던트 대응
- 캘리포니아 소비자 개인 정보 보호법 대비

미디어

- AWS re:Invent 2014(SEC402): 클라우드에서의 침입 탐지
- AWS re:Invent 2014(SEC404): 클라우드에서 인시던트 대응
- AWS re:Invent 2015(SEC308): 클라우드의 보안 이벤트 논의
- AWS re:Invent 2015(SEC316): 보안 인시던트 대응 시뮬레이션으로 아키텍처 강화
- AWS re:Invent 2016(SEC313): 보안 이벤트 대응 자동화 - 아이디어에서 실행 코드까지
- AWS re:Invent 2017(SID302): 자동화 및 Alexa를 통해 보안 팀의 역량 배가
- AWS re:Invent 2016(SAC316): 보안 자동화: 애플리케이션 보안에 소요되는 시간 단축
- AWS re:Invent 2016(SAC304): 예측 보안: 빅 데이터를 사용하여 방어 강화
- AWS re:Invent 2017(SID325): Amazon Macie: 보안 및 규정 준수 워크로드를 위한 기계 학습으로 구동되는 데이터 가시성
- AWS London Summit 2018: AWS에서 인시던트 대응 및 포렌식 자동화

서드 파티 도구

서드 파티 도구에 대한 다음 링크는 외부 링크이며 AWS에서 보증하지 않습니다. AWS는 이러한 도구 또는 페이지에 대해 어떠한 종류의 보증이나 진술도 제공하지 않습니다.

- AWS_IR - 호스트 및 키 손상 완화를 위해 Python으로 설치할 수 있는 명령줄 유틸리티입니다.
- MargaritaShotgun - 원격 메모리 수집 도구입니다.
- ThreatPrep - 인시던트 처리 준비 상태와 관련된 AWS 계정 모범 사례를 평가하기 위한 Python 모듈입니다.
- ThreatResponse 웹 - AWS_IR 명령줄 도구와 함께 사용할 수 있는 웹 기반 분석 플랫폼입니다.
- GRR Rapid Response - 인시던트 대응을 위한 원격 실시간 포렌식 프레임워크입니다.
- Linux Write Blocker - Linux 소프트웨어 쓰기 차단을 지원하기 위한 커널 패치 및 user-space 도구입니다.

업계 참고 자료

- NIST SP 800-61R2: Computer Security Incident Handling Guide

문서 개정

이 백서의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

업데이트 기록-변경	update-history-description	update-history-date
마이너 업데이트	버그 수정 및 수많은 소소한 변경이 이루어졌습니다.	2021년 6월 2일
마이너 업데이트	연결이 끊어진 링크를 수정했습니다.	2021년 3월 5일
백서 업데이트	가독성을 높이기 위해 연결이 끊어진 링크를 수정하고 수많은 텍스트를 변경했습니다.	2020년 11월 23일
마이너 업데이트	'AWS 콘솔 및 CLI를 사용한 인시던트 대응'에 대한 링크를 수정했습니다.	2020년 6월 30일
백서 업데이트	새로운 보안 서비스, 위협 인텔리전스, 컨테이너에 대한 공동 책임, 자동화 및 CCPA를 반영하도록 업데이트되었습니다. 샘플 의사 결정 트리 및 런북과 함께 부록을 추가했습니다.	2020년 6월 11일
최초 게시	처음 게시된 백서	2019년 6월 1일

부록 A: 클라우드 기능 정의

AWS는 150개 이상의 클라우드 서비스와 수천 가지 기능을 제공합니다. 이들 중 다수는 기본 탐지, 예방 및 대응 기능을 제공하며 다른 기능은 사용자 지정 보안 솔루션을 설계하는 데 사용할 수 있습니다. 이 단원에는 클라우드에서의 인시던트 대응과 가장 밀접하게 관련된 서비스 일부가 포함되어 있습니다.

주제

로깅 및 이벤트

AWS CloudTrail - AWS CloudTrail은 AWS 계정의 거버넌스, 규정 준수, 운영 감사 및 위험 감사를 지원하는 서비스입니다. CloudTrail을 사용하면 AWS 인프라에서 계정 활동과 관련된 작업을 기록하고 지속적으로 모니터링하며 보관할 수 있습니다. CloudTrail은 AWS Management Console, AWS SDK, 명령줄 도구 및 기타 AWS 서비스를 통해 수행된 작업을 비롯하여 AWS 계정 활동의 이벤트 기록을 제공합니다. 이러한 이벤트 기록을 통해 보안 분석, 리소스 변경 추적, 문제 해결을 간소화할 수 있습니다.

검증된 로그 파일은 보안 및 포렌식에서 중요한 역할을 합니다. CloudTrail이 로그 파일을 전송한 후 해당 파일이 수정, 삭제 또는 변경되지 않았는지 확인하기 위해 CloudTrail 로그 파일 무결성 검증을 사용할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 감지되지 않으면서 CloudTrail 로그 파일을 수정, 삭제 또는 위조하는 것은 컴퓨팅 방식으로 실행 불가능합니다.

기본적으로 CloudTrail에서 버킷으로 전송하는 로그 파일은 Amazon 서버 측 암호화를 통해 암호화됩니다. 원하는 경우 CloudTrail 로그 파일에 AWS Key Management Service(AWS KMS) 관리형 키(SSE-KMS)를 사용할 수 있습니다.

Amazon CloudWatch Events - Amazon CloudWatch Events는 AWS 리소스의 변경 사항이나 AWS CloudTrail에서 API 호출을 게시하는 시기를 설명하는 시스템 이벤트의 근 실시간 스트림을 제공합니다. 신속하게 설정할 수 있는 단순 규칙을 사용하여 일치하는 이벤트를 검색하고 하나 이상의 대상 함

수 또는 스트림으로 이를 경로 지정할 수 있습니다. CloudWatch Events는 운영 변경 사항이 발생할 때 이를 인식합니다. CloudWatch Events는 이러한 운영 변경에 응답하고, 환경에 응답하기 위한 메시지를 전송하고 함수를 활성화하며 변경을 수행하고 상태 정보를 기록하는 등 필요에 따라 교정 조치를 취합니다. Amazon GuardDuty와 같은 일부 보안 서비스는 CloudWatch Events 형태로 출력을 생성합니다.

AWS Config - AWS Config는 AWS 리소스의 구성을 검토, 감사 및 평가할 수 있는 서비스입니다. Config는 AWS 리소스 구성을 지속적으로 모니터링 및 기록하고, 원하는 구성을 기준으로 기록된 구성의 평가를 자동화할 수 있습니다. Config를 사용하면 AWS 리소스 간 구성 및 관계의 변경을 수동 또는 자동으로 검토할 수 있습니다. 자세한 리소스 구성 기록을 조사하고, 내부 가이드에 지정되어 있는 구성을 기준으로 전반적인 규정 준수 여부를 확인할 수 있습니다. 이에 따라 규정 준수 감사, 보안 분석, 변경 관리 및 운영 문제 해결 작업을 간소화할 수 있습니다.

Amazon S3 액세스 로그 - Amazon S3 버킷에 민감한 정보를 저장하는 경우 S3 액세스 로그를 활성화하여 해당 데이터에 대한 모든 업로드, 다운로드 및 수정 사항을 기록할 수 있습니다. 이 로그는 버킷 자체의 변경 사항(예: 액세스 정책 및 수명 주기 정책 변경)을 기록하는 CloudTrail 로그와는 별개의 로그입니다.

Amazon CloudWatch Logs - Amazon CloudWatch Logs를 사용하면 CloudWatch Logs 에이전트를 통해 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 로그 파일(예: 운영 체제, 애플리케이션 및 사용자 지정 로그 파일)을 모니터링, 저장 및 액세스할 수 있습니다. 또한 Amazon CloudWatch Logs는 AWS CloudTrail, Amazon Route 53 DNS 쿼리, VPC 흐름 로그, Lambda 함수 및 기타 소스에서 로그를 캡처할 수 있습니다. 그런 다음 CloudWatch Logs에서 관련 로그 데이터를 검색할 수 있습니다.

Amazon VPC 흐름 로그 – VPC 흐름 로그를 사용하면 VPC의 네트워크 인터페이스에서 전송되고 수신되는 IP 트래픽에 대한 정보를 캡처할 수 있습니다. 흐름 로그를 생성하고 난 다음 Amazon CloudWatch Logs의 데이터를 확인하고 검색할 수 있습니다. VPC 흐름 로그는 다음과 같은 여러 작업에 도움이 될 수 있습니다. 예를 들어 흐름 로그를 사용하여 특정 트래픽이 인스턴스에 도달하지 않는 이유를 확인하고 해결할 수 있으며 이는 지나치게 제한적인 보안 그룹 규칙을 진단하는 데 도움이 될 수 있습니다. 흐름 로그를 인스턴스에 액세스하는 트래픽을 모니터링하기 위한 보안 도구로 사용할 수도 있습니다.

AWS WAF 로그 - 이제 AWS WAF는 서비스에서 검사하는 모든 웹 요청에 대한 전체 로깅을 지원합니다. 규정 준수 및 감사를 위해서 뿐만 아니라 디버깅과 추가 포렌식을 위해 이러한 로그를 Amazon S3에 저장할 수 있습니다. 이러한 로그는 특정 규칙이 트리거된 이유와 특정 웹 요청이 차단된 이유를 이해하는 데 도움이 됩니다. 또한 로그를 SIEM 및 로그 분석 도구와 통합할 수 있습니다.

기타 AWS 로그 - 혁신의 속도에 발맞춰 AWS는 고객을 위해 거의 매일 새로운 기능을 배포하고 있으며 여기에는 수십 개의 AWS 서비스가 포함됩니다. 각 AWS 서비스에서 사용할 수 있는 기능에 대한 자세한 내용은 해당 서비스에 대한 AWS 설명서를 참조하세요.

가시성 및 알림

AWS Security Hub - AWS Security Hub는 AWS 계정 전체의 우선순위가 높은 보안 알림 및 규정 준수 상태를 종합적으로 보여줍니다. Security Hub를 사용하면 Amazon GuardDuty, Amazon Inspector 및 Amazon Macie와 같은 여러 AWS 서비스 뿐만 아니라 AWS 파트너 솔루션에서 제공되는 보안 경고 또는 평가 결과를 단일 공간에서 수집 및 정리하고 이에 대한 우선순위를 지정하는 서비스를 확보하게 됩니다. 평가 결과는 실행 가능한 그래프 및 표를 포함한 통합 대시보드에 시각적으로 요약됩니다. 또한, AWS 모범 사례 및 조직이 준수하는 업계 표준을 기반으로 하는 자동 규정 준수 검사를 사용하여 환경을 지속적으로 모니터링합니다.

Amazon GuardDuty - Amazon GuardDuty는 악성 또는 인증되지 않은 동작을 지속적으로 모니터링하여 AWS 계정 및 워크로드를 보호하도록 지원하는 관리형 위협 탐지 서비스입니다. 계정 침해 가능성을 나타내는 무단 배포 또는 비정상적인 API 호출과 같은 활동을 모니터링합니다. 또한, GuardDuty는 잠재적 인스턴스 침해 또는 공격자 정찰과 같은 위협을 탐지합니다

GuardDuty는 통합된 위협 인텔리전스 피드를 통해 의심되는 공격자를 파악하고 기계 학습을 사용해 계정 및 워크로드 활동에서 이상 항목을 탐지합니다. 잠재적 위협이 탐지되면, 서비스에서 상세한 보안 알림을 GuardDuty 콘솔과 AWS CloudWatch Events로 전달합니다. 그러면 알림을 토대로 조치를 취할 수 있고 기존 이벤트 관리 및 워크로드 시스템에 손쉽게 통합할 수 있습니다.

Amazon Macie - Amazon Macie는 AWS에 저장된 민감한 데이터를 자동으로 검색, 분류 및 보호하여 데이터 손실을 막아주는 AI 기반 보안 서비스입니다. Amazon Macie는 기계 학습을 사용하여 개인 식별 정보(PII) 또는 지적 재산과 같은 민감한 데이터를 인식하고 비즈니스 가치를 부여하며 이 데이터가 저장된 장소와 이 데이터가 조직에서 어떤 방식으로 사용되는지를 파악합니다. Amazon Macie는 비정상적인 데이터 액세스 활동을 지속적으로 모니터링하여 무단 액세스 또는 의도하지 않은 데이터 유출 위험이 감지될 경우 경고합니다.

AWS Config 규칙 - AWS Config 규칙은 원하는 리소스 구성을 나타내며, AWS Config에서 기록한 관련 리소스의 구성 변경과 비교하여 평가됩니다. 규칙을 리소스 구성과 비교하여 평가한 결과는 대시보드에서 확인할 수 있습니다. Config 규칙을 사용하면 전반적인 규칙 준수 및 위험 상태를 구성 측면에서 평가하고, 시간에 따른 규칙 준수 추세를 확인하여 리소스의 규칙 미준수를 초래한 구성 변경이 무엇인지 찾아낼 수 있습니다.

AWS Trusted Advisor - AWS Trusted Advisor는 AWS 환경을 최적화하여 비용을 줄여주고 성능을 향상시키며 보안을 개선하는 온라인 리소스입니다. Trusted Advisor는 AWS 모범 사례에 따라 리소스를

프로비저닝하는 데 도움이 되는 실시간 가이드를 제공합니다. Business 및 Enterprise Support 플랜 고객은 CloudWatch Events 통합을 비롯하여 모든 Trusted Advisor 검사 항목을 사용할 수 있습니다.

Amazon CloudWatch - Amazon CloudWatch는 AWS 클라우드 리소스 및 AWS에서 실행하는 애플리케이션을 모니터링하는 서비스입니다. Amazon CloudWatch를 사용하여 지표를 수집 및 추적하고, 로그 파일을 수집 및 모니터링하며, 경보를 설정하고, AWS 리소스 변경에 자동으로 대응할 수 있습니다. Amazon CloudWatch는 Amazon EC2 인스턴스, Amazon DynamoDB 테이블, Amazon RDS DB 인스턴스 같은 AWS 리소스 뿐만 아니라 애플리케이션과 서비스에서 생성된 사용자 정의 지표 및 애플리케이션에서 생성된 모든 로그 파일을 모니터링할 수 있습니다. Amazon CloudWatch를 사용하여 시스템 전반의 리소스 사용률, 애플리케이션 성능, 운영 상태를 파악할 수 있습니다. 이러한 분석 정보를 활용해 문제에 빠르게 대응하고 애플리케이션이 원활하게 실행되는 상태를 유지할 수 있습니다.

Amazon Inspector - Amazon Inspector는 AWS에 배포된 애플리케이션의 보안 및 규정 준수를 개선하는 데 도움이 되는 자동 보안 평가 서비스입니다. Amazon Inspector는 애플리케이션의 취약점 또는 모범 사례와의 차이를 자동으로 평가합니다. 평가를 수행한 후, Amazon Inspector는 상세한 보안 평가 결과 목록을 제공하며, 이 목록은 심각도 수준에 따라 우선순위가 지정되어 있습니다. 이러한 평가 결과는 직접 검토하거나, Amazon Inspector 콘솔 또는 API를 통해 제공되는 상세한 평가 보고서에 포함된 내용을 확인해도 됩니다.

Amazon Detective - Amazon Detective는 AWS 리소스에서 로그 데이터를 자동으로 수집하고, 기계 학습, 통계 분석 및 그래프 이론을 사용하여 보다 쉽고 빠르게 효율적인 보안 관련 조사를 시행할 수 있도록 지원하는 연결된 데이터 집합을 구축합니다. Amazon Detective는 Virtual Private Cloud(VPC) 흐름 로그, AWS CloudTrail 및 Amazon GuardDuty와 같은 여러 데이터 원본에서 몇 조에 달하는 이벤트를 분석하고, 시간에 따른 리소스, 사용자 및 이들 간의 상호작용에 대한 통합된 대화형 보기를 자동으로 생성합니다. 이 통합된 보기를 통해 한 곳에서 모든 세부 정보와 컨텍스트를 시각화하여 탐지 결과에 대한 근본적인 이유를 식별하고, 관련 기록 활동을 자세히 탐구하며, 근본 원인을 빠르게 확인할 수 있습니다.

자동화

AWS Lambda - AWS Lambda는 이벤트에 대한 응답으로 코드를 실행하고 자동으로 기본 컴퓨팅 리소스를 관리하는 서버리스 컴퓨팅 서비스입니다. Lambda를 사용하여 사용자 지정 로직으로 기타 AWS 서비스를 확장하거나 AWS 규모, 성능, 보안에 따라 작업하는 자체 백엔드 서비스를 만들 수 있습니다. Lambda는 가용성이 뛰어난 컴퓨팅 인프라에서 코드를 실행하고 컴퓨팅 리소스 관리를 모두 수행합니다. 여기에는 서버 및 운영 체제 유지 관리, 용량 프로비저닝 및 자동 크기 조정, 코드 및 보안 패치 배포와 코드 모니터링 및 로깅이 포함됩니다. 코드를 제공하기만 하면 됩니다.

AWS Step Functions - AWS Step Functions를 사용하면 시각적 워크플로를 통해, 배포된 애플리케이션의 구성 요소 및 마이크로서비스를 조정할 수 있습니다. Step Functions는 애플리케이션의 구성 요소

를 일련의 단계로 배열 및 시각화할 수 있는 그래픽 콘솔을 제공합니다. 그러므로 손쉽게 다단계 애플리케이션을 구축하고 실행할 수 있습니다. Step Functions가 자동으로 각 단계를 트리거 및 추적하고 오류가 발생할 경우 재시도하므로 애플리케이션이 의도대로 정상적으로 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 쉽게 발전시키고 더 빠르게 혁신할 수 있습니다. AWS Step Functions는 AWS 서버리스 플랫폼의 일부이며, 서버리스 애플리케이션을 위한 AWS Lambda 함수를 간단하게 오케스트레이션할 수 있게 해줍니다. 또한 Amazon EC2 및 Amazon ECS와 같은 컴퓨팅 리소스를 사용하는 마이크로서비스 오케스트레이션에도 Step Functions를 사용할 수 있습니다.

AWS Systems Manager - AWS Systems Manager는 AWS 인프라에 대한 가시성과 제어를 제공합니다. Systems Manager는 통합된 사용자 인터페이스를 제공하므로 여러 AWS 서비스의 운영 데이터를 보고 AWS 리소스 전체에서 운영 작업을 자동화할 수 있습니다. Systems Manager를 사용하면 리소스를 애플리케이션별로 그룹화하고, 모니터링과 문제 해결을 위해 운영 데이터를 보고, 리소스 그룹에 조치를 취할 수 있습니다. Systems Manager는 인스턴스를 정의된 상태로 유지하고, 온디맨드 변경(예: 애플리케이션 업데이트 또는 셸 스크립트 실행)을 수행하며, 기타 자동화 및 패치 작업을 수행할 수 있습니다.

안전한 스토리지

Amazon S3 - Amazon S3은 어디서나 원하는 양의 데이터를 저장하고 검색할 수 있도록 구축된 객체 스토리지입니다. 99.999999999%의 내구성을 제공하고 모든 산업에서 선도적인 기업이 사용하는 수많은 애플리케이션 데이터를 저장하도록 설계되었습니다. Amazon S3은 포괄적인 보안을 제공하며 규제 요구 사항을 충족하도록 설계되었습니다. 고객은 S3을 통해 비용 최적화, 액세스 제어 및 규정 준수 데이터를 유연하게 관리할 수 있습니다. Amazon S3은 현재 위치에서 쿼리하는 기능을 제공하므로 Amazon S3에 저장된 데이터에 대해 강력한 분석을 직접 실행할 수 있습니다. Amazon S3은 현재 가장 많이 지원되는 클라우드 스토리지 서비스로서, 가장 큰 규모의 서드 파티 솔루션, 시스템 통합 사업자 파트너 및 다른 AWS 서비스와 통합됩니다.

Amazon S3 Glacier - Amazon S3 Glacier는 데이터 아카이브 및 장기 백업을 위한 안전하고 안정적이며 비용이 매우 저렴한 클라우드 스토리지 서비스입니다. 99.999999999%의 내구성과 포괄적인 보안을 제공하며 규제 요구 사항을 충족하도록 설계되었습니다. Amazon S3 Glacier에서는 현재 위치에서 쿼리하는 기능을 제공하므로 저장된 아카이브 데이터에 직접 강력한 분석을 실행할 수 있습니다. 비용을 낮게 유지하면서 동시에 다양한 검색 요구를 지원하기 위해 Amazon S3 Glacier에서는 아카이브에 액세스하는 3가지 옵션(몇 분에서 몇 시간까지 소요)을 제공합니다.

사용자 지정

앞서 언급한 서비스와 기능은 일부에 불과합니다. AWS는 계속해서 새로운 기능을 추가하고 있습니다. 자세한 내용은 AWS의 새로운 기능 및 AWS 클라우드 보안 페이지를 검토하시기 바랍니다. AWS가 네이티브 클라우드 서비스로 제공하는 보안 서비스 외에도 AWS 서비스를 기반으로 고유한 기능을 구축할 수 있습니다.

계정 내에서 AWS CloudTrail, Amazon GuardDuty 및 Amazon Macie와 같은 기본 보안 서비스 집합을 활성화하는 것이 좋지만 결국에는 이러한 기능을 확장하여 로그 자산에서 추가적인 가치를 창출할 수 있습니다. APN 보안 컴피턴시 프로그램에 나열된 도구 등 다양한 파트너 도구를 사용할 수 있습니다. 직접 쿼리를 작성하여 로그를 검색할 수도 있습니다. AWS가 제공하는 수많은 관리형 서비스를 통해 이 작업이 그 어느 때보다 쉬워졌습니다. 이 백서에서는 다루지 않지만 Amazon Athena, Amazon OpenSearch Service, Amazon QuickSight, Amazon Machine Learning, Amazon EMR 등 조사에 도움이 될 수 있는 많은 추가 AWS 서비스가 있습니다.

부록 B: 샘플 코드

AWS CloudTrail 이벤트 예제

다음 예에서는 `Alice`라는 IAM 사용자가 AWS CLI에서 `ec2-stop-instances`를 사용하여 Amazon EC2 `StopInstancesaction`을 호출하는 방법을 보여 줍니다.

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
    }]}}
}]}
```

AWS CloudWatch Events 예제

다음 Amazon CloudWatch Events 예제는 `jane-roe-test`라는 AWS IAM 사용자가 `www.github.com`에 공개적으로 노출되어 권한이 없는 사용자가 악용할 수 있음을 보여 줍니다.

```
{
  "check-name": "Exposed Access Keys",
  "check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
    "Fraud Type": "Exposed",
    "Location": "www.github.com"
  },
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

인프라 도메인 CLI 활동 예제

다음 AWS CLI 명령은 인프라 도메인 내의 이벤트에 응답하는 예를 보여 줍니다. 이 예에서는 AWS API를 사용하여 이 백서에 설명된 여러 가지 초기 인시던트 대응 활동을 수행합니다.

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
 disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
```

```
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name
 web-asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-
balancer-name web-load-balancer
```

```
# Create an EBS snapshot
> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-
REFERENCE-ID"
```

```
# Create a new EC2 instance from the Forensic Workstation AMI
> aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --
key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e
```

```
# Create a new EBS volume copy from the EBS snapshot
> aws ec2 create-volume --region us-east-1 --availability-zone us-east-1a --snapshot-id
 snap-abcd1234 --volume-type io1 --iops 10000
```

```
# Attach the volume to the forensic workstation
> aws ec2 attach-volume --volume-id vol-1234abcd --instance-id i-new4n6x --device /dev/
sdf
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to
 the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port
 0-65535 --source-group sg-1a2b3c4d
```

```
# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
 Key=Environment,Value=Quarantine:REFERENCE-ID
```

부록 C: 예제 런북

다음 예제 런북은 더 큰 런북의 단일 항목을 나타냅니다. 이 런북은 비공식적이며 예로만 제공됩니다. 런북을 만들 때 각 시나리오는 시작과 손상 지표는 다르지만 결과나 취해야 할 조치가 모두 비슷한 더 큰 항목으로 발전할 수 있습니다. 이런 식으로 변화를 주면 더 나은 또는 더 통찰력 있는 대응을 할 수 있는 상황이 열릴 수도 있습니다.

인시던트 대응 런북 - 루트 사용

목표

이 런북의 목적은 루트 AWS 계정 사용을 관리하는 방법에 대한 구체적인 가이드를 제공하는 것입니다. 이 런북은 심층적인 인시던트 대응 전략을 대체하지 않습니다. 이 런북은 IR 수명 주기에 중점을 둡니다.

- 제어를 설정합니다.
- 영향을 파악합니다.
- 필요한 경우 복구합니다.
- 근본 원인을 조사합니다.
- 개선합니다.

아래에는 IOC(손상 지표), 초기 단계(유출 중지) 및 이러한 단계를 실행하는 데 필요한 자세한 CLI 명령이 나열되어 있습니다.

가정

- CLI가 설치되고 구성되어 있습니다.
- 보고 프로세스가 이미 진행 중입니다.
- Trusted Advisor가 활성화되어 있습니다.
- Security Hub가 활성화되어 있습니다.

손상 지표

- 계정에서 비정상적인 활동이 있습니다.

  - IAM 사용자가 생성되었습니다.
  - CloudTrail이 꺼졌습니다.
  - CloudWatch가 꺼졌습니다.
  - SNS가 일시 중지되었습니다.
  - Step Functions가 일시 중지되었습니다.
- AMI가 예상치 않게 시작되거나 새로 시작되었습니다.
- 계정의 연락처가 변경되었습니다.

문제 해결 단계 - 제어 설정

아래에는 문제가 발생했을 수 있는 계정에 대해 취할 수 있는 AWS 설명서의 구체적인 작업이 나와 있습니다. 문제가 발생했을 수 있는 계정에 대한 설명서는 AWS 계정에서 무단 활동이 발견되면 어떻게 해야 합니까?를 참조하세요.

1. 가능한 한 빨리 AWS Support 및 TAM에 문의합니다.
2. 루트 암호를 변경 및 교체하고 루트와 연결된 MFA 디바이스를 추가합니다.
3. 문제 해결 단계와 관련된 암호, 액세스/비밀 키 및 CLI 명령을 바꿉니다.
4. 루트 사용자가 수행한 작업을 검토합니다.
5. 해당 작업에 대한 런북을 엽니다.
6. 인시던트를 종결합니다.
7. 인시던트를 검토하고 발생한 상황을 파악합니다.
8. 근본적인 문제를 수정하고, 개선 사항을 구현하고, 필요에 따라 런북을 업데이트합니다.

추가 조치 항목 - 영향 파악

생성된 항목과 변이 호출을 검토합니다. 향후 액세스를 허용하기 위해 생성된 항목이 있을 수 있습니다. 확인 사항은 다음과 같습니다.

- IAM 교차 계정 역할
- IAM 사용자
- S3 버킷
- EC2 인스턴스
- [이 목록은 애플리케이션과 인프라에서 생성됩니다.]

고지 사항

고객은 본 문서에 포함된 정보를 독자적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공만을 위한 것이며, (b) 사전 고지 없이 변경될 수 있는 현재의 AWS 제품 제공 서비스 및 사례를 보여 주며, (c) AWS 및 자회사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정 또는 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임과 법적 책임은 AWS 계약서에 준하며 본 문서는 AWS와 고객 간의 계약에 포함되지 않고 계약을 변경하지도 않습니다.