에서 사이버 위협 인텔리전스 공유 AWS

AWS 권장 가이드

AWS 권장 가이드: 에서 사이버 위협 인텔리전스 공유 AWS

Table of Contents

소개 1
CTI 공유 모델 3
클라우드의 보안 3
클라우드 보안 3
CTI 아키텍처 5
위협 인텔리전스 플랫폼 배포 6
CTI 수집 7
보안 제어 자동화 8
Amazon GuardDuty 10
Amazon Route 53 Resolver DNS 방화벽 11
AWS Network Firewall 13
가시성 확보 14
네트워크 트래픽 로깅 14
에서 보안 조사 결과 중앙 집중화 AWS 15
AWS 보안 데이터를 다른 엔터프라이즈 데이터와 통합 17
CTI 공유 17
다음 단계 19
AWS 리소스 19
AWS 서비스 설명서 19
STIX 리소스 19
위협 인텔리전스 플랫폼 20
기여자 21
작성 21
검토 21
기술 작성 21
문서 기록 22
..... xxiii

에서 사이버 위협 인텔리전스 공유 AWS

Amazon Web Services(기여자)

2024년 12월(문서 기록)

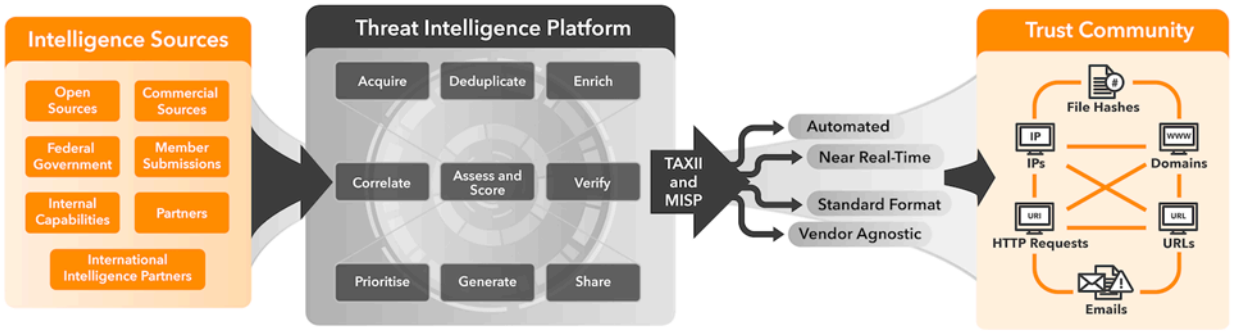
새로운 위험이 발생함에 따라 중요한 클라우드 워크로드를 보호하기 위한 모범 사례가 지속적으로 발전하고 있습니다. 보호가 필요한 인터넷 연결 자산의 수가 증가하면 위협 행위자와 관련된 보안 이벤트 위험도 증가합니다. 사이버 위협 인텔리전스(CTI)는 위협 행위자의 의도, 기회 및 역량을 나타내는 데이터의 수집 및 분석입니다. 증거에 기반하고 실행 가능하며 사이버 방어 활동을 알립니다. 액터 어트리뷰션, 전술 기법 및 절차, 동기 또는 대상과 관련된 정보가 포함되는 경우가 많습니다.

CTI는 조직 내, 신뢰 커뮤니티의 조직 간, 정보 공유 및 분석 센터(ISACs) 또는 정부 기관과 같은 다른 조직과 공유할 수 있습니다. 정부 기관의 예로는 호주 사이버 보안 센터(ACSC)와 미국 사이버 보안 및 인프라 보안 기관(CISA)이 있습니다.

모든 형태의 인텔리전스와 마찬가지로 위협 컨텍스트는 매우 중요합니다. CTI 공유는 동적 사이버 보안 위험 관리에 정보를 제공합니다. 적시에 사이버 보안 방어, 대응 및 복구를 수행하는 데 필수적입니다. 이렇게 하면 사이버 보안 기능의 효율성과 효과가 향상됩니다. 위협 컨텍스트는 다양한 대상과 관련된 CTI 기능 요구 사항을 구별하는 데에도 필수적입니다. 예를 들어, 정교한 액터는 특정 기업이나 정부를 대상으로 하는 반면, 상품 액터는 즉시 사용할 수 있는 도구와 기술을 사용하여 개인과 조직을 광범위하게 공격합니다.

보안 계획, 관찰성, 위협 인텔리전스 분석, 보안 제어 자동화 및 신뢰 커뮤니티 내 공유는 위협 인텔리전스 수명 주기의 주요 부분입니다.는 수동 보안 작업을 자동화하여 더 높은 정확도로 위협을 탐지하고 더 빠르게 대응하며 공유할 수 있는 고품질 위협 인텔리전스를 생성할 수 있도록 AWS 지원합니다. 두 번째 공격이 발생하지 않도록 설계된 속도로 새 사이버 공격을 검색하고, 분석하고, CTI를 생성하고, 공유하고, 적용할 수 있습니다.

이 가이드에서는 위협 인텔리전스 플랫폼을 배포하는 방법을 설명합니다 AWS. 신뢰 커뮤니티는 CTI를 제공하며 플랫폼은 이를 수집하여 실행 가능한 인텔리전스를 식별하고 AWS 환경에서 보호 및 탐지 제어를 자동화합니다. 다음 이미지는 위협 인텔리전스 수명 주기를 보여줍니다. CTI는 소스에서 도착한 다음 위협 인텔리전스 플랫폼이 이를 처리합니다. Trusted Automated Exchange of Intelligence Information(TAXII) 프로토콜 또는 맬웨어 정보 공유 플랫폼 (MISP)을 사용하면 CTI가 작업을 위해 신뢰 커뮤니티와 공유됩니다.



위협 인텔리전스 플랫폼은 CTI를 사용하여 AWS 환경에서 보안 제어를 자동으로 구현하거나 수동 조치가 필요한 경우 보안 팀에 알립니다. 예방 제어는 이벤트 발생을 방지하도록 설계된 보안 제어입니다. 예를 들어 네트워크 방화벽, DNS 해석기 및 기타 침입 방지 시스템(IPSs)을 사용하여 알려진 잘못된 IP 주소 또는 도메인 이름 목록을 차단하는 자동화가 있습니다. 탐지 제어는 이벤트가 발생한 후 탐지, 로깅 및 경고하도록 설계된 보안 제어입니다. 예를 들어 악의적인 활동에 대한 지속적인 모니터링과 문제 또는 이벤트의 증거에 대한 로그 검색이 있습니다.

와 같은 중앙 집중식 보안 관찰성 도구에서 모든 결과를 집계할 수 있습니다AWS Security Hub CSPM. 그런 다음 결과를 신뢰 커뮤니티와 공유하여 포괄적인 위협 상황을 공동으로 구축할 수 있습니다.

CTI 공유를 위한 공동 책임 모델

AWS 공동 책임 모델은 클라우드의 보안 및 규정 준수에 AWS 대한 책임을와 공유하는 방법을 정의합니다.는 클라우드의 보안이라고 하는 AWS 클라우드에서 제공되는 모든 서비스를 실행하는 인프라를 AWS 보호합니다. 데이터 및 애플리케이션과 같은 서비스를 안전하게 사용할 책임은 사용자에게 있습니다. 이를 클라우드의 보안이라고 합니다.

클라우드의 보안

보안은의 최우선 순위입니다 AWS. 보안 문제로 인해 조직이 중단되는 것을 방지하기 위해 최선을 다하고 있습니다. 인프라와 데이터를 보호하기 위해 노력하면서 글로벌 규모의 인사이트를 사용하여 대규모 및 실시간으로 대량의 보안 인텔리전스를 수집하여 사용자를 자동으로 보호합니다. 가능하면 보안 AWS 시스템은 해당 작업이 가장 큰 영향을 미치는 위협을 방해합니다. 이 작업은 백그라운드에서 발생하는 경우가 많습니다.

인프라 전체에서 매일 수백 개의 사이버 공격을 AWS 클라우드 탐지하고 성공적으로 차단합니다. 그렇지 않으면 중단되고 비용이 많이 들 수 있습니다. 이처럼 중요하지만 대부분 보이지 않는 것은 센서로 구성된 글로벌 네트워크와 관련 중단 도구 세트를 통해 달성됩니다. 이러한 기능을 사용하면 네트워크 및 인프라에 대해 사이버 공격을 수행하는 것이 더 어렵고 비용이 많이 듭니다.

AWS 는 모든 클라우드 공급자 중에서 가장 큰 퍼블릭 네트워크 공간을 차지합니다. 이를 통해 AWS 인터넷의 특정 활동에 대한 탁월한 실시간 인사이트를 얻을 수 있습니다. MadPot는 위협 센서(허니팟이라고 함)로 구성된 전 세계에 분산된 네트워크입니다. MadPot는 AWS 보안 팀이 공격자의 전술과 기술을 이해하는 데 도움이 됩니다. 공격자가 위협 센서 중 하나를 대상으로 하려고 할 때마다는 데이터를 AWS 수집하고 분석합니다.

Sonaris는가 네트워크 트래픽을 분석하는 데 AWS 사용하는 또 다른 내부 도구입니다. 많은 수의 계정 및 리소스에 대한 무단 액세스를 식별하고 중지합니다. 2023년 5월부터 2024년 4월까지 Sonaris는 Amazon Simple Storage Service(S3)에 저장된 고객 데이터를 스캔하려는 시도를 240 억 회 이상 거부했습니다.Amazon S3 또한 Amazon Elastic Compute Cloud(Amazon EC2)에서 실행되는 취약한 워크로드를 거의 2.6 조 번 검색하지 못했습니다.

클라우드 보안

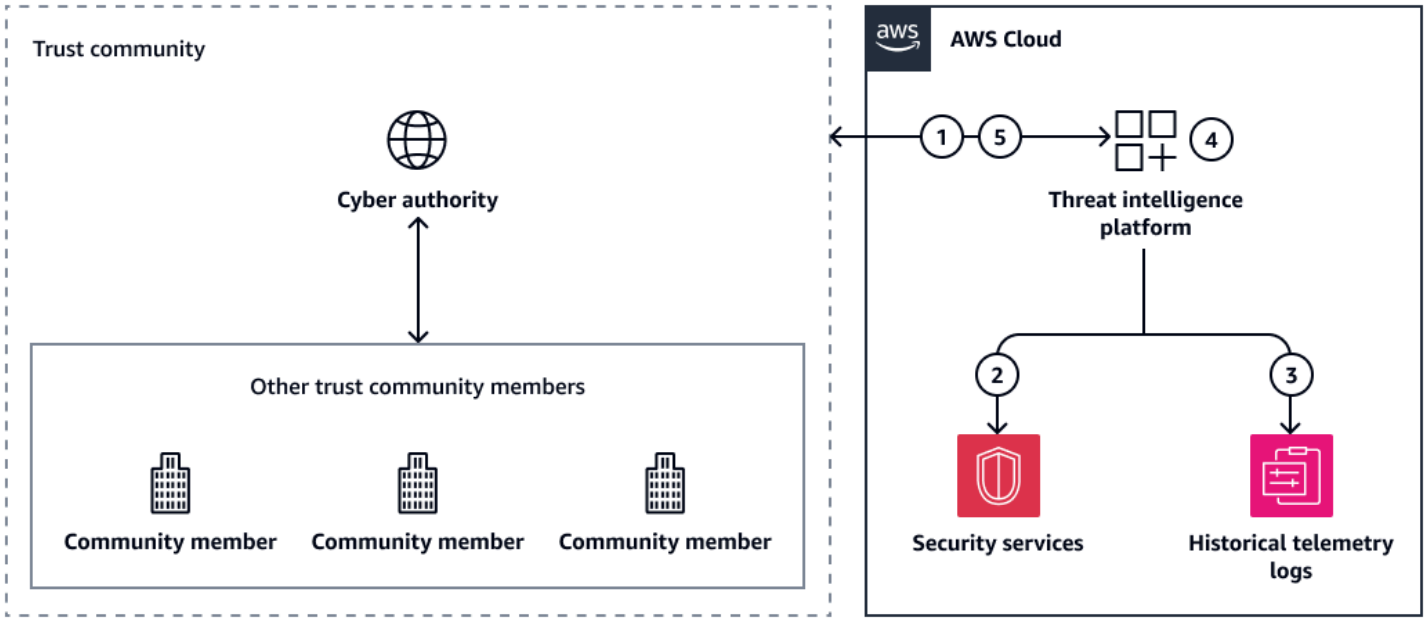
이 지침은의 사이버 위협 인텔리전스(CTI) 모범 사례에 중점을 둡니다 AWS 클라우드. 현지화 및 컨텍스트화된 CTI를 생성하는 것은 사용자의 책임입니다. 데이터가 저장되는 위치, 데이터의 보안 방식 및

데이터에 액세스할 수 있는 사용자를 제어합니다. AWS 는 클라우드의 CTI 기반 보안에 필수적인 로깅, 모니터링 및 감사 데이터를 볼 수 없습니다.

구조화된 위협 정보 표현식(STIX)은 CTI를 교환하는 데 사용되는 오픈 소스 언어 및 직렬화 형식입니다. 파일 해시, 도메인, URLs, HTTP 요청 및 IP 주소와 같은 지표는 위협 차단을 위해 공유해야 할 중요한 출력입니다. 그러나 효과적인 작업은 확실성 등급 및 침입 세트 상관관계와 같은 추가 인텔리전스에 의존합니다. STIX 2.1은 공격 패턴, 행동 방향, 위협 행위자, 지리적 위치 및 멀웨어 정보를 포함하여 18 개의 STIX 도메인 객체를 정의합니다. 또한 개체가 위협 인텔리전스 플랫폼에서 수집하는 대량의 데이터에서 노이즈의 신호를 결정하는 데 도움이 되는 신뢰도 등급 및 관계와 같은 개념을 소개합니다. 환경에서 위협에 대한 이러한 수준의 세부 정보를 탐지, 분석 및 공유할 수 있습니다 AWS . 자세한 내용은 이 안내서의 예방 및 탐지 보안 제어 자동화 섹션을 참조하세요.

의 사이버 위협 인텔리전스 아키텍처 AWS

다음 그림은 위협 피드를 사용하여 사이버 위협 인텔리전스(CTI)를 AWS 환경에 통합하기 위한 일반화된 아키텍처를 보여줍니다. CTI는의 위협 인텔리전스 플랫폼 AWS 클라우드, 선택한 사이버 기관 및 기타 신뢰 커뮤니티 구성원 간에 공유됩니다.



다음 워크플로를 보여줍니다.

1. 위협 인텔리전스 플랫폼은 사이버 기관 또는 다른 신뢰 커뮤니티 구성원으로부터 실행 가능한 CTI를 받습니다.
2. 위협 인텔리전스 플랫폼은 AWS 보안 서비스를 수행하여 이벤트를 탐지하고 방지합니다.
3. 위협 인텔리전스 플랫폼은에서 위협 인텔리전스를 수신합니다 AWS 서비스.
4. 이벤트가 발생하면 위협 인텔리전스 플랫폼은 새 CTI를 큐레이션합니다.
5. 위협 인텔리전스 플랫폼은 새로운 CTI를 사이버 기관과 공유합니다. 또한 다른 신뢰 커뮤니티 구성원과 CTI를 공유할 수도 있습니다.

CTI 피드를 제공하는 사이버 기관은 많습니다. 예를 들어 호주 사이버 보안 센터(ACSC)와 영국 국가 사이버 보안 센터에서 제공하는 Connect Inform Share Protect(CISP) 프로그램, 뉴질랜드 정부 통신 보안국에서 제공하는 맬웨어 프리 네트워크(MFN) 프로그램이 있습니다. 또한 많은 AWS 파트너가 CTI 공유 피드를 제공합니다.

CTI 공유를 시작하려면 다음을 수행하는 것이 좋습니다.

1. 위협 인텔리전스 플랫폼 배포 - 여러 소스에서 다양한 형식으로 위협 인텔리전스 데이터를 수집, 집계 및 구성하는 플랫폼을 배포합니다.
2. 사이버 위협 인텔리전스 수집 - 위협 인텔리전스 플랫폼을 하나 이상의 위협 피드 공급자와 통합합니다. 위협 피드를 받으면 위협 인텔리전스 플랫폼을 사용하여 새 CTI를 처리하고 환경의 보안 운영과 관련된 실행 가능한 인텔리전스를 식별합니다. 최대한 자동화하되 human-in-the-loop 결정이 필요한 몇 가지 상황이 있습니다.
3. 예방 및 탐지 보안 제어 자동화 - 예방 및 탐지 제어를 제공하는 아키텍처의 보안 서비스에 CTI를 배포합니다. 이러한 서비스를 일반적으로 침입 방지 시스템(IPS)이라고 합니다. 에서 서비스 APIs AWS사용하여 위협 피드에 제공된 IP 주소 및 도메인 이름의 액세스를 거부하는 차단 목록을 구성합니다.
4. 관찰성 메커니즘으로 가시성 확보 - 환경에서 보안 작업이 수행되는 동안 새 CTI를 수집하고 있습니다. 예를 들어 위협 피드에 포함된 위협을 관찰하거나 침입과 관련된 침해 지표(예: 제로데이 악용)를 관찰할 수 있습니다. 위협 인텔리전스를 중앙 집중화하면 환경 전체에서 상황 인식이 향상되므로 하나의 시스템에서 기존 CTI와 새로 발견된 CTI를 검토할 수 있습니다.
5. 신뢰 커뮤니티와 CTI 공유 - CTI 공유 수명 주기를 완료하려면 자체 CTI를 생성하고 신뢰 커뮤니티에 다시 공유합니다.

다음 비디오인 AUS 사이버 보안 센터와의 사이버 위협 인텔리전스 공유 조정에서는 이러한 단계에 대해 자세히 설명합니다. 이 동영상에서는 호주 사이버 보안 센터의 CTI 공유 기능에 대해 설명하지만 선택한 위협 피드 또는 위치에 관계없이 단계는 동일합니다.

위협 인텔리전스 플랫폼 배포

위협 인텔리전스 플랫폼은 여러 소스에서 다양한 형식으로 위협 인텔리전스 데이터를 수집, 집계 및 구성합니다. 이를 통해 분석가는 신뢰 커뮤니티에서 받은 사이버 위협 인텔리전스(CTI)를 보고, 우선순위를 지정하고, 조치를 취할 수 있습니다.

OpenCTI 및 MISP는 일반적인 오픈 소스 위협 인텔리전스 플랫폼입니다. 에서 AWS 파트너가 제공하는 솔루션도 있습니다AWS Marketplace. 위협 인텔리전스 플랫폼을 선택할 때는 보안 팀의 기술 수준을 고려해야 합니다. MISP는 강력하지만 복잡할 수 있으며 OpenCTI에는 보다 직관적인 사용자 인터페이스가 있습니다.

위협 인텔리전스 플랫폼을 선택할 때는 다음 사항을 고려하세요.

- 기능 - 플랫폼에서 실시간 모니터링, 위협 탐지 및 분석과 같은 기능을 제공하나요?
- 데이터 소스 - 플랫폼에서 위협 피드, 다크 웹 인텔리전스, 소셜 미디어, 오픈 소스 인텔리전스 등 다양한 소스를 사용하나요?

- 데이터 품질 - 플랫폼에 정보가 정확하고 신뢰할 수 있는지 확인하는 프로세스가 있습니까?
- 확장성 - 플랫폼이 성장 및 진화하는 위협과 같은 조직의 변화하는 요구 사항에 적응할 수 있습니까?
- 통합 - 플랫폼이 기존 보안 도구 및 인프라와 통합할 수 있습니까?
- 사용자 경험 - 플랫폼을 쉽게 탐색하고 사용할 수 있습니까?
- 사용자 지정 - 조직의 특정 요구 사항에 맞게 플랫폼을 사용자 지정할 수 있습니까?
- 비용 - 라이선스 비용 및 유지 관리 요구 사항을 포함하여 플랫폼이 비용 효율적입니까?

Virtual Private Cloud(VPC) 내에 위협 인텔리전스 플랫폼을 배포할 수 있습니다. Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 직접 배포하거나 Amazon Elastic Container Service(Amazon ECS) 또는 같은 컨테이너 기술을 사용하여 배포할 수 있습니다 AWS Fargate. 최신 애플리케이션 개발에 적합한 AWS 컨테이너 서비스를 선택하는 방법에 대한 자세한 내용은 AWS 컨테이너 서비스 선택을 참조하세요.

사이버 위협 인텔리전스 수집

수집 프로세스의 첫 번째 단계는 위협 피드의 사이버 위협 인텔리전스(CTI) 데이터를 위협 인텔리전스 플랫폼이 수집할 수 있는 형식으로 변환하는 것입니다. 이를 CTI 변환이라고 합니다. 위협 피드 데이터는 구조화된 위협 정보 표현식(STIX)과 같은 다양한 형식으로 제공될 수 있습니다. 수신 데이터를 AWS 환경에서 사용 중인 보안 제품에 적합한 예측 가능하고 쉽게 사용할 수 있는 형식으로 재구성해야 합니다.

호환성을 극대화하려면 데이터를 JSON 형식으로 변환하는 것이 좋습니다. 예를 들어는 JSON 형식의 데이터를 사용할 AWS Step Functions 수 있으며 자동화 워크플로는이 형식을 더 쉽고 일관되게 사용할 수 있습니다. 자동화된 워크플로 구축에 대한 자세한 내용은 다음 섹션인 예방 및 탐지 보안 제어 자동화에 나와 있습니다.

CTI 데이터 수집을 가속화하기 위해 데이터 변환을 자동화할 수 있습니다. 데이터는 수집될 때 변환된 다음 위협 인텔리전스 플랫폼으로 직접 전달됩니다. AWS Lambda 함수를 사용하여 변환을 완료하고 AWS Step Functions 또는 Amazon EventBridge와 AWS 서비스 같은를 통해 프로세스를 오케스트레이션할 수 있습니다.

CTI를 수집할 때 추출하고 유지할 속성을 선택할 수 있습니다. 필요한 정확한 세부 정보는 비즈니스 요구 사항에 따라 다를 수 있습니다. 그러나 방화벽 및 기타 보안 서비스를 업데이트하려면 다음과 같은 최소 속성을 사용하는 것이 좋습니다.

- IP 주소 및 도메인

- 위협
- 내부 위협 목록에서 추가 또는 제거

사용하려는 속성을 추출한 다음 구조화된 JSON 템플릿으로 형식을 지정합니다.

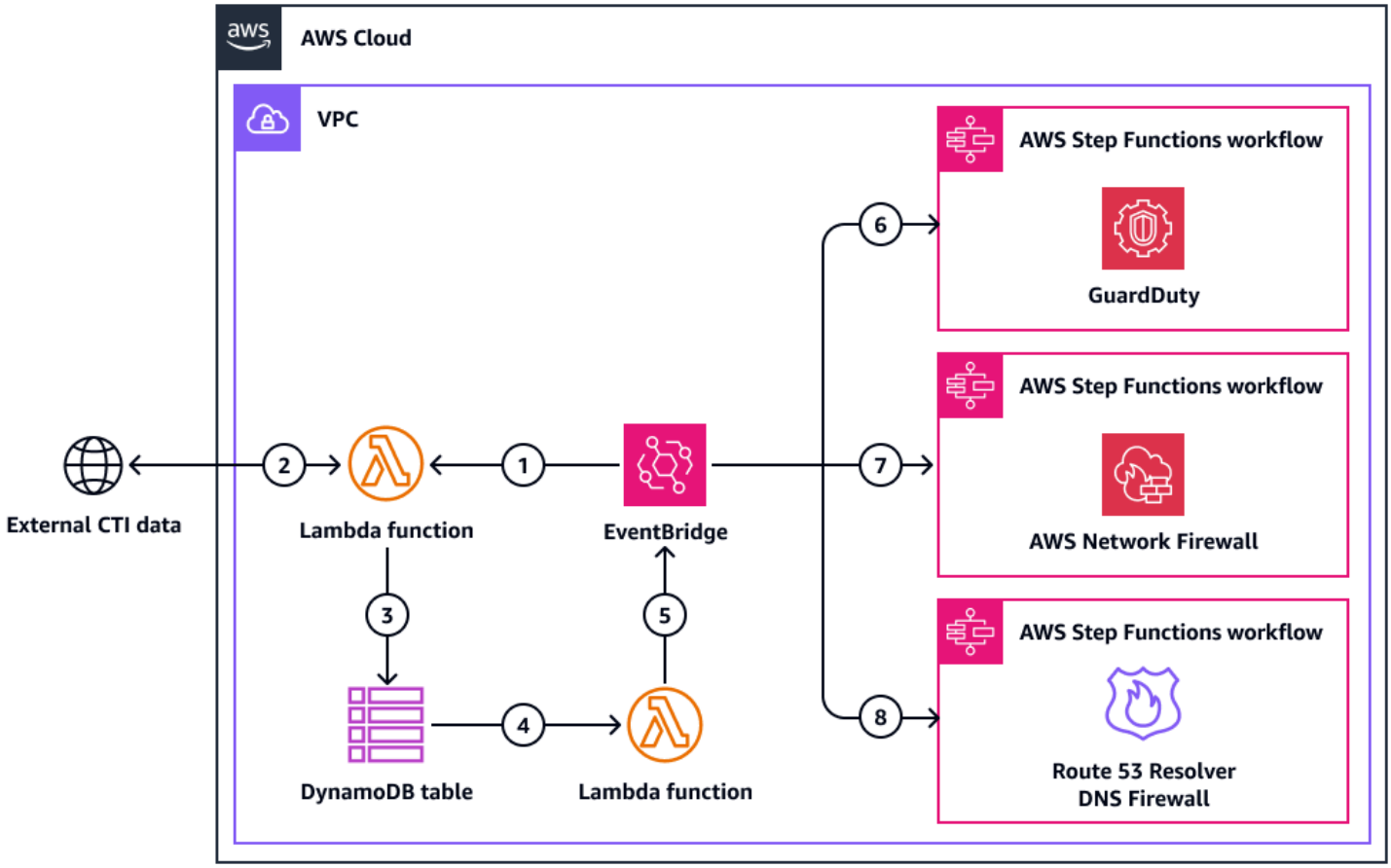
예방 및 탐지 보안 제어 자동화

사이버 위협 인텔리전스(CTI)가 위협 인텔리전스 플랫폼에 수집된 후 데이터에 대한 응답으로 구성을 변경하는 프로세스를 자동화할 수 있습니다. 위협 인텔리전스 플랫폼은 사이버 위협 인텔리전스를 관리하고 환경을 관찰하는 데 도움이 됩니다. 사이버 위협에 대한 기술 및 비기술 정보를 구조화, 저장, 구성 및 시각화하는 기능을 제공합니다. 이를 통해 위협 그림을 구축하고 다양한 인텔리전스 소스를 결합하여 지능형 영구 위협(APTs.

자동화를 통해 위협 인텔리전스 수신과 환경에서 구성 변경 구현 사이의 시간을 줄일 수 있습니다. 모든 CTI 응답을 자동화할 수 있는 것은 아닙니다. 그러나 최대한 많은 응답을 자동화하면 보안 팀이 나머지 CTI의 우선순위를 정하고 시기 적절하게 평가하는 데 도움이 됩니다. 각 조직은 자동화할 수 있는 CTI 응답 유형과 수동 분석이 필요한 CTI 응답을 결정해야 합니다. 위험, 자산 및 리소스와 같은 조직 컨텍스트를 기반으로이 결정을 내립니다. 예를 들어 일부 조직에서는 알려진 잘못된 도메인 또는 IP 주소에 대한 블록을 자동화하도록 선택할 수 있지만 내부 IP 주소를 차단하기 전에 분석가 조사가 필요할 수 있습니다.

이 섹션에서는 Amazon GuardDuty, AWS Network Firewall및 Amazon Route 53 Resolver DNS 방화벽에서 자동 CTI 응답을 설정하는 방법의 예를 제공합니다. 이러한 예제를 서로 독립적으로 구현할 수 있습니다. 조직의 보안 요구 사항과 요구 사항이 결정을 안내하도록 합니다. AWS Step Functions 워크플로(상태 시스템이라고도 함)를 AWS 서비스 통해의 구성 변경을 자동화할 수 있습니다. AWS Lambda 함수가 CTI를 JSON 형식으로 변환을 완료하면 Step Functions 워크플로를 시작하는 Amazon EventBridge 이벤트를 트리거합니다.

다음 다이어그램은 샘플 아키텍처를 보여줍니다. Step Functions 워크플로는 GuardDuty의 위협 목록, Route 53 Resolver DNS 방화벽의 도메인 목록, Network Firewall의 규칙 그룹을 자동으로 업데이트합니다.



그림은 다음 워크플로를 보여줍니다.

1. EventBridge 이벤트는 정기적으로 시작됩니다. 이 이벤트는 함수를 AWS Lambda 시작합니다.
2. Lambda 함수는 외부 위협 피드에서 CTI 데이터를 검색합니다.
3. Lambda 함수는 검색된 CTI 데이터를 Amazon DynamoDB 테이블에 기록합니다.
4. DynamoDB 테이블에 데이터를 쓰면 Lambda 함수를 시작하는 변경 데이터 캡처 스트림 이벤트가 시작됩니다.
5. 변경이 발생하면 Lambda 함수가 EventBridge에서 새 이벤트를 시작합니다. 변경 사항이 없으면 워크플로가 완료됩니다.
6. CTI가 IP 주소 레코드와 관련된 경우 EventBridge는 Amazon GuardDuty에서 위협 목록을 자동으로 업데이트하는 Step Functions 워크플로를 시작합니다. 자세한 내용은이 섹션의 Amazon GuardDuty를 참조하세요.
7. CTI가 IP 주소 또는 도메인 레코드와 관련된 경우 EventBridge는 규칙 그룹을 자동으로 업데이트하는 Step Functions 워크플로를 시작합니다 AWS Network Firewall. 자세한 내용은 이 섹션의 AWS Network Firewall을 참조하세요.

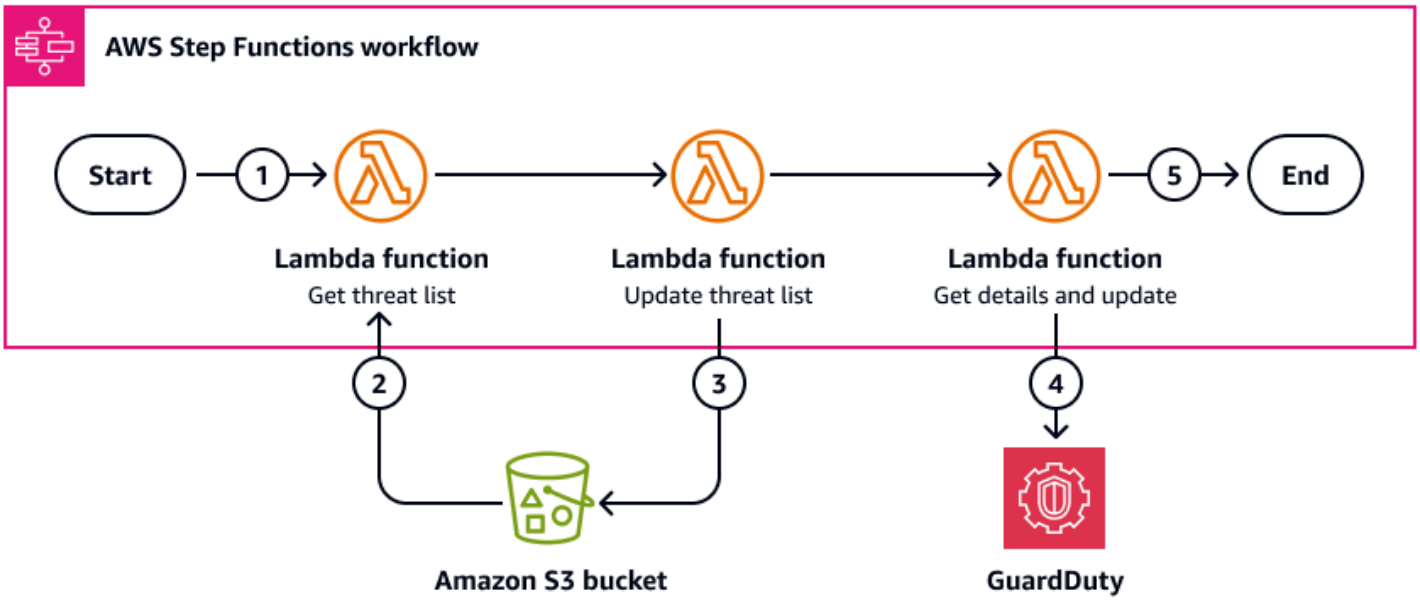
8. CTI가 도메인 레코드와 관련된 경우 EventBridge는 Amazon Route 53 Resolver DNS 방화벽의 도메인 목록을 자동으로 업데이트하는 Step Functions 워크플로를 시작합니다. 자세한 내용은이 섹션의 Amazon Route 53 Resolver DNS 방화벽을 참조하세요.

Amazon GuardDuty

Amazon GuardDuty는 무단 활동이 있는지 AWS 계정 및 워크로드를 지속적으로 모니터링하고 가시성 및 문제 해결을 위해 자세한 보안 조사 결과를 제공하는 위협 탐지 서비스입니다. CTI 피드에서 GuardDuty 위협 목록을 자동으로 업데이트하면 워크로드에 액세스할 수 있는 위협에 대한 인사이트를 얻을 수 있습니다. GuardDuty는 탐지 제어 기능을 개선합니다.

> **Tip**
>
> GuardDuty는 기본적으로와 통합됩니다AWS Security Hub CSPM. Security Hub CSPM은의 보안 상태에 대한 포괄적인 보기를 AWS 제공하며 보안 업계 표준 및 모범 사례를 기준으로 환경을 확인하는 데 도움이 됩니다. GuardDuty를 Security Hub CSPM과 통합하면 GuardDuty 조사 결과가 Security Hub CSPM으로 자동으로 전송됩니다. 그런 다음 Security Hub CSPM은 이러한 결과를 보안 태세 분석에 포함할 수 있습니다. 자세한 내용은 GuardDuty 설명서의 와 통합 AWS Security Hub CSPM을 참조하세요. Security Hub CSPM에서는 자동화를 사용하여 탐지 및 대응 보안 제어 기능을 개선할 수 있습니다.

다음 이미지는 Step Functions 워크플로가 위협 피드의 CTI를 사용하여 GuardDuty의 위협 목록을 업데이트하는 방법을 보여줍니다. Lambda 함수가 CTI를 JSON 형식으로 변환을 완료하면 워크플로를 시작하는 EventBridge 이벤트를 트리거합니다.



이 다이어그램은 다음 단계를 보여 줍니다.

1. CTI가 IP 주소 레코드와 관련된 경우 EventBridge는 Step Functions 워크플로를 시작합니다.
2. Lambda 함수는 Amazon Simple Storage Service(Amazon S3) 버킷에 객체로 저장된 위협 목록을 검색합니다.
3. Lambda 함수는 CTI의 IP 주소 변경 사항으로 위협 목록을 업데이트합니다. 원래 Amazon S3 버킷에 객체의 새 버전으로 위협 목록을 저장합니다. 객체 이름은 변경되지 않습니다.
4. Lambda 함수는 API 호출을 사용하여 GuardDuty 탐지기 ID 및 위협 인텔리전스 세트 ID를 검색합니다. 이 IDs 사용하여 위협 목록의 새 버전을 참조하도록 GuardDuty를 업데이트합니다.

> **Note**
>
> 특정 GuardDuty 감지기 및 IP 주소 목록은 배열로 검색되므로 검색할 수 없습니다. 따라서 대상에 각각 하나만 있는 것이 좋습니다 AWS 계정. 둘 이상의 경우이 워크플로의 최종 Lambda 함수에서 올바른 데이터가 추출되었는지 확인해야 합니다.

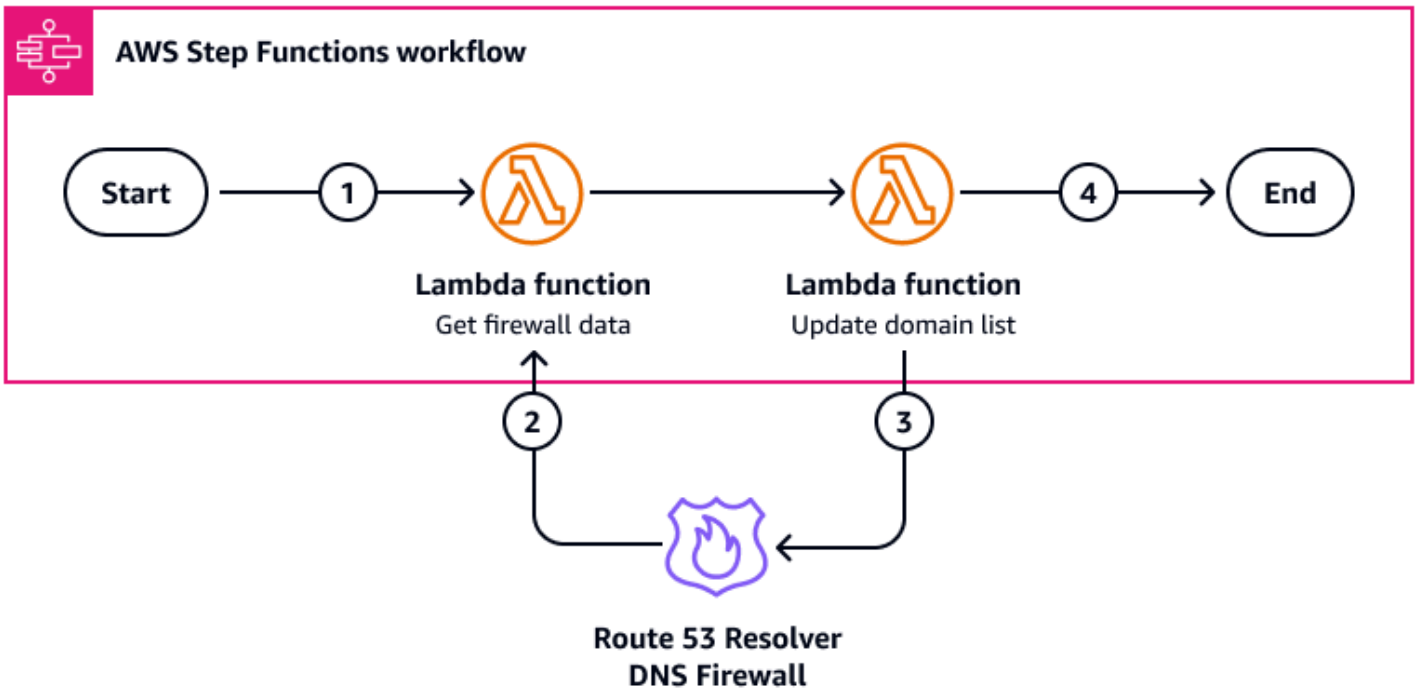
5. Step Functions 워크플로가 종료됩니다.

Amazon Route 53 Resolver DNS 방화벽

Amazon Route 53 Resolver DNS 방화벽을 사용하면 Virtual Private Cloud(VPC)의 아웃바운드 DNS 트래픽을 필터링하고 규제할 수 있습니다. DNS 방화벽에서는 CTI 피드로 식별되는 도메인 주소를

차단하는 규칙 그룹을 생성합니다. 이 규칙 그룹에서 도메인을 자동으로 추가 및 제거하도록 Step Functions 워크플로를 구성합니다.

다음 이미지는 Step Functions 워크플로가 위협 피드의 CTI를 사용하여 Amazon Route 53 Resolver DNS 방화벽의 도메인 목록을 업데이트하는 방법을 보여줍니다. Lambda 함수가 CTI를 JSON 형식으로 변환을 완료하면 워크플로를 시작하는 EventBridge 이벤트를 트리거합니다.



이 다이어그램은 다음 단계를 보여 줍니다.

1. CTI가 도메인 레코드와 관련된 경우 EventBridge는 Step Functions 워크플로를 시작합니다.
2. Lambda 함수는 방화벽의 도메인 목록 데이터를 검색합니다. 이 Lambda 함수 생성에 대한 자세한 내용은 AWS SDK for Python (Boto3) 설명서의 get_firewall_domain_list를 참조하세요.
3. Lambda 함수는 CTI와 검색된 데이터를 사용하여 도메인 목록을 업데이트합니다. 이 Lambda 함수 생성에 대한 자세한 내용은 Boto3 설명서의 update_firewall_domains를 참조하세요. Lambda 함수는 도메인을 추가, 제거 또는 교체할 수 있습니다.
4. Step Functions 워크플로가 종료됩니다.

다음 모범 사례를 따르는 것이 좋습니다.

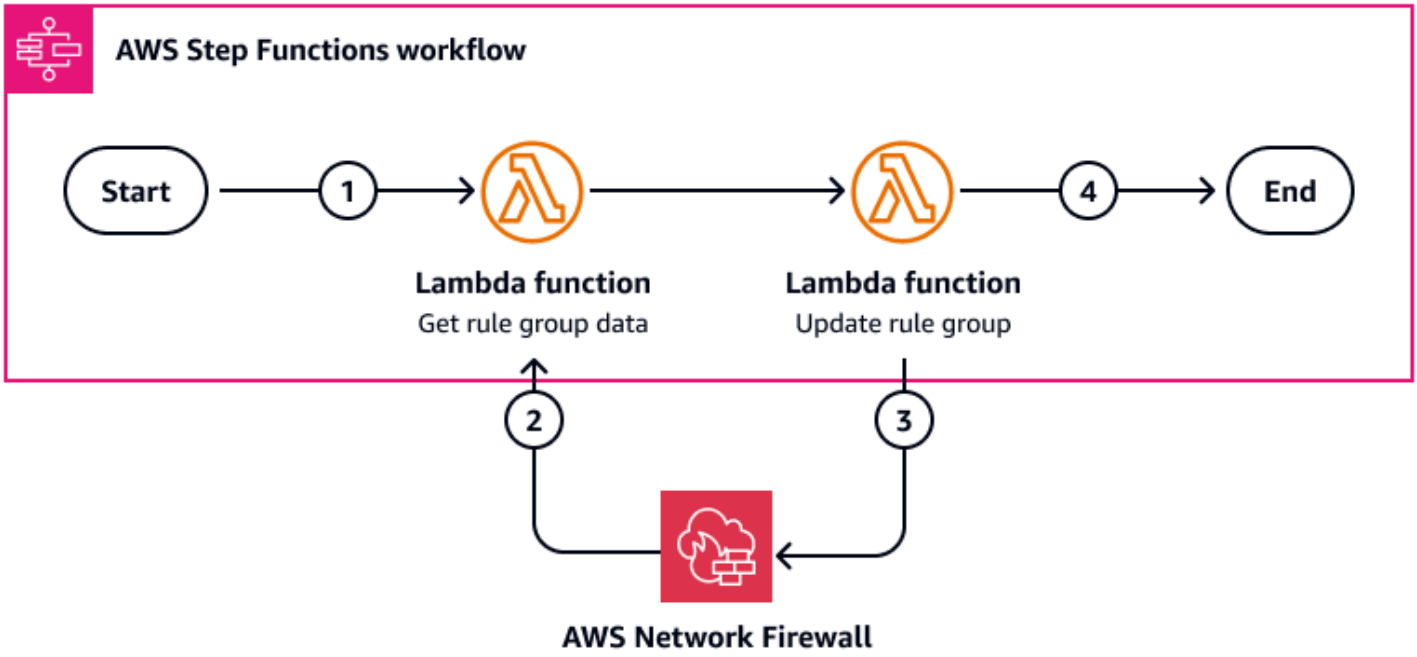
- Route 53 Resolver DNS 방화벽과를 모두 사용하는 것이 좋습니다 AWS Network Firewall. DNS 방화벽은 DNS 트래픽을 필터링하고 Network Firewall은 다른 모든 트래픽을 필터링합니다.

- DNS 방화벽에 대한 로깅을 활성화하는 것이 좋습니다. 제한된 도메인이 방화벽을 통해 트래픽을 전송하려고 할 경우 로그 데이터를 모니터링하고 알림을 보내는 탐지 제어를 생성할 수 있습니다. 자세한 내용은 Amazon CloudWatch를 사용하여 Route 53 Resolver DNS 방화벽 규칙 그룹 모니터링을 참조하세요.

AWS Network Firewall

AWS Network Firewall는의 VPCs에 대한 상태 저장 관리형 네트워크 방화벽 및 침입 탐지 및 방지 서비스입니다 AWS 클라우드. VPC 경계에서 트래픽을 필터링하여 위협을 차단하는 데 도움이 됩니다. 위협 인텔리전스 피드를 사용하여 Network Firewall 규칙 그룹을 자동으로 업데이트하면 조직의 클라우드 워크로드와 데이터를 악의적인 행위자로부터 보호할 수 있습니다.

다음 이미지는 Step Functions 워크플로가 위협 피드의 CTI를 사용하여 Network Firewall에서 하나 이상의 규칙 그룹을 업데이트하는 방법을 보여줍니다. Lambda 함수가 CTI를 JSON 형식으로 변환을 완료하면 워크플로를 시작하는 EventBridge 이벤트를 트리거합니다.



이 다이어그램은 다음 단계를 보여 줍니다.

1. CTI가 IP 주소 또는 도메인 레코드와 관련된 경우 EventBridge는 Network Firewall에서 규칙 그룹을 자동으로 업데이트하는 Step Functions 워크플로를 시작합니다.
2. Lambda 함수는 Network Firewall에서 규칙 그룹 데이터를 검색합니다.

3. Lambda 함수는 CTI를 사용하여 규칙 그룹을 업데이트합니다. IP 주소 또는 도메인을 추가하거나 제거합니다.
4. Step Functions 워크플로가 종료됩니다.

다음 모범 사례를 따르는 것이 좋습니다.

- Network Firewall에는 여러 규칙 그룹이 있을 수 있습니다. 도메인 및 IP 주소에 대해 별도의 규칙 그룹을 생성합니다.
- Network Firewall에 대한 로깅을 활성화하는 것이 좋습니다. 로그 데이터를 모니터링하는 탐지 제어를 생성하고 제한된 도메인 또는 IP 주소가 방화벽을 통해 트래픽을 전송하려고 할 때 알림을 보낼 수 있습니다. 자세한 내용은 네트워크 트래픽 로깅을 참조하세요 AWS Network Firewall.
- Route 53 Resolver DNS 방화벽과를 모두 사용하는 것이 좋습니다 AWS Network Firewall. DNS 방화벽은 DNS 트래픽을 필터링하고 Network Firewall은 다른 모든 트래픽을 필터링합니다.

관찰성 메커니즘으로 가시성 확보

발생한 보안 이벤트를 볼 수 있는 기능은 적절한 보안 제어를 설정하는 것만큼 중요합니다. AWS Well-Architected Framework의 보안 원칙에서 탐지 모범 사례에는 서비스 및 애플리케이션 로깅 구성과 표준화된 위치의 로그, 조사 결과 및 지표 캡처가 포함됩니다. 이러한 모범 사례를 구현하려면 이벤트를 식별하는 데 도움이 되는 정보를 기록한 다음 해당 정보를 사람이 사용할 수 있는 형식으로, 이상적으로는 중앙 위치에서 처리해야 합니다.

이 가이드에서는 Amazon Simple Storage Service(Amazon S3)를 사용하여 로그 데이터를 중앙 집중화할 것을 권장합니다. Amazon S3는 AWS Network Firewall 및 Amazon Route 53 Resolver DNS 방화벽 모두에 대한 로그 스토리지를 지원합니다. 그런 다음 AWS Security Hub CSPM 및 Amazon Security Lake를 사용하여 Amazon GuardDuty 조사 결과 및 기타 보안 조사 결과를 단일 위치로 중앙 집중화합니다.

네트워크 트래픽 로깅

이 가이드의 예방 및 탐지 보안 제어 자동화 섹션에서는 및 Amazon Route 53 Resolver DNS 방화벽을 사용하여 AWS Network Firewall 사이버 위협 인텔리전스(CTI)에 대한 대응을 자동화하는 방법을 설명합니다. 이러한 두 서비스 모두에 대해 로깅을 구성하는 것이 좋습니다. 로그 데이터를 모니터링하는 탐지 제어를 생성하고 제한된 도메인 또는 IP 주소가 방화벽을 통해 트래픽을 전송하려고 할 때 알림을 보낼 수 있습니다.

이러한 리소스를 구성할 때는 개별 로깅 요구 사항을 고려하세요. 예를 들어 Network Firewall에 대한 로깅은 상태 저장 규칙 엔진으로 전달하는 트래픽에만 사용할 수 있습니다. 제로 트러스트 모델을 따르고 모든 트래픽을 상태 저장 규칙 엔진으로 전달하는 것이 좋습니다. 그러나 비용을 절감하려면 조직에서 신뢰하는 트래픽을 제외할 수 있습니다.

Network Firewall과 DNS Firewall 모두 Amazon S3에 대한 로깅을 지원합니다. 이러한 서비스에 대한 로깅 설정에 대한 자세한 내용은 에서 네트워크 트래픽 로깅 AWS Network Firewall 및 DNS 방화벽에 대한 로깅 구성을 참조하세요. 두 서비스 모두를 통해 Amazon S3 버킷에 대한 로깅을 구성할 수 있습니다 AWS Management Console.

에서 보안 조사 결과 중앙 집중화 AWS

AWS Security Hub CSPM는의 보안 상태에 대한 포괄적인 보기를 AWS 제공하며 보안 업계 표준 및 모범 사례를 기준으로 AWS 환경을 평가하는 데 도움이 됩니다. Security Hub CSPM은 보안 제어와 관련된 조사 결과를 생성할 수 있습니다. Amazon GuardDuty AWS 서비스와 같은 다른의 조사 결과를 수신할 수도 있습니다. Security Hub CSPM을 사용하여 및 AWS 계정 AWS 서비스지원되는 타사 제품에서 조사 결과와 데이터를 중앙 집중화할 수 있습니다. 통합에 대한 자세한 내용은 Security Hub CSPM 설명서의 Security Hub CSPM의 통합 이해를 참조하세요.

Security Hub CSPM에는 보안 문제를 분류하고 해결하는 데 도움이 되는 자동화 기능도 포함되어 있습니다. 예를 들어, 보안 검사에 실패할 경우, 자동화 규칙을 사용하여 중요한 조사 결과를 자동으로 업데이트할 수 있습니다. Amazon EventBridge와의 통합을 사용하여 특정 결과에 대한 자동 응답을 시작할 수도 있습니다. 자세한 내용은 Security Hub CSPM 설명서의 Security Hub CSPM 조사 결과 자동 수정 및 조치를 참조하세요.

Amazon GuardDuty를 사용하는 경우 조사 결과를 Security Hub CSPM으로 보내도록 GuardDuty를 구성하는 것이 좋습니다. 그런 다음 Security Hub CSPM은 이러한 결과를 보안 태세 분석에 포함할 수 있습니다. 자세한 내용은 GuardDuty 설명서의 와 통합 AWS Security Hub CSPM을 참조하세요.

Network Firewall과 Route 53 Resolver DNS 방화벽 모두에 대해 로깅 중인 네트워크 트래픽에서 사용자 지정 조사 결과를 생성할 수 있습니다. Amazon Athena는 표준 SQL을 사용하여 Amazon S3에 있는 데이터를 직접 분석할 수 있는 대화형 쿼리 서비스입니다. Athena에서 Amazon S3의 로그를 스캔하고 관련 데이터를 추출하는 쿼리를 구성할 수 있습니다. 지침은 Athena 설명서의 시작하기를 참조하세요. 그런 다음 AWS Lambda 함수를 사용하여 관련 로그 데이터를 AWS Security Finding Format(ASFF)으로 변환하고 결과를 Security Hub CSPM으로 전송할 수 있습니다. 다음은 Network Firewall의 로그 데이터를 Security Hub CSPM 조사 결과로 변환하는 샘플 Lambda 함수입니다.

```
Import { SecurityHubClient, BatchImportFindingsCommand, GetFindingsCommand } from
 "@aws-sdk/client-securityhub";
```

```
Export const handler = async(event) => {
   const date = new Date().toISOString();

   const config = {
      Region: REGION
   };

   const input = {
      Findings: [
         {
            SchemaVersion: '2018-10-08',
            Id: ALERTLOGS3BUCKETID,
            ProductArn: FIREWALLMANAGERARN,
            GeneratorId: 'alertlogs-to-findings',
            AwsAccountId: ACCOUNTID,
            Types: 'Unusual Behaviours/Network Flow/Alert',
            CreatedAt: date,
            UpdatedAt: date,
            Severity: {
               Normalized: 80,
               Product: 8
            },
            Confidence: 100,
            Title: 'Alert Log to Findings',
            Description: 'Network Firewall Alert Log into Finding – add
               top level dynamic detail',
            Resources: [
               {
                  /*these are custom resources. Contain deeper details of your event
 here*/
                  firewallName: 'Example Name',
                  event: 'Example details here'
               }
            ]
         }
      ]
   };

   const client = new SecurityHubClient(config);
   const command = new BatchImportFindingsCommand(input);
   const response = await client.send(command);
   return { statusCode: 200, response };
};
```

Security Hub CSPM으로 정보를 추출하고 전송하기 위해 따르는 패턴은 개별 비즈니스 요구 사항에 따라 달라집니다. 정기적으로 데이터를 전송해야 하는 경우 EventBridge를 사용하여 프로세스를 시작할 수 있습니다. 정보가 추가될 때 알림을 받으려면 Amazon Simple Notification Service(Amazon SNS)를 사용할 수 있습니다. 이 아키텍처에 접근하는 방법에는 여러 가지가 있으므로 비즈니스 요구 사항을 달성할 수 있도록 적절하게 계획하는 것이 중요합니다.

AWS 보안 데이터를 다른 엔터프라이즈 데이터와 통합

Amazon Security Lake는 통합 및 타사 서비스에서 보안 관련 로그 AWS 서비스 및 이벤트 데이터 수집을 자동화할 수 있습니다. 또한 사용자 지정 가능한 보존 및 복제 설정을 통해 데이터 수명 주기를 관리할 수 있습니다. Security Lake는 수집된 데이터를 Apache Parquet 형식과 개방형 사이버 보안 스키마 프레임워크 (OCSF) 라는 표준 오픈 소스 스키마로 변환합니다. Security Lake는 OCSF 지원을 통해 및 광범위한 엔터프라이즈 보안 데이터 소스의 보안 데이터를 정규화 AWS 하고 결합합니다. 다른 AWS 서비스 및 타사 서비스는 사고 대응 및 보안 데이터 분석을 위해 Security Lake에 저장된 데이터를 구독할 수 있습니다.

Security Hub CSPM에서 조사 결과를 수신하도록 Security Lake를 구성할 수 있습니다. 이 통합을 활성화하려면 두 서비스를 모두 활성화하고 Security Hub CSPM을 Security Lake의 소스로 추가해야 합니다. 이 단계를 완료하면 Security Hub CSPM이 모든 조사 결과를 Security Lake로 전송하기 시작합니다. Security Lake는 Security Hub CSPM 조사 결과를 자동으로 정규화하고 OCSF로 변환합니다. Security Lake에서 구독자를 한 명 이상 추가하여 Security Hub CSPM의 조사 결과를 사용할 수 있습니다. 자세한 내용은 Security Lake 설명서의 와 통합 AWS Security Hub CSPM을 참조하세요.

다음 동영상 AWS re:Inforce 2024 - Cyber Threat Intelligence Sharing on AWS에서는 Security Hub CSPM 및 Security Lake 통합을 사용하여 CTI를 공유하는 방법을 설명합니다.

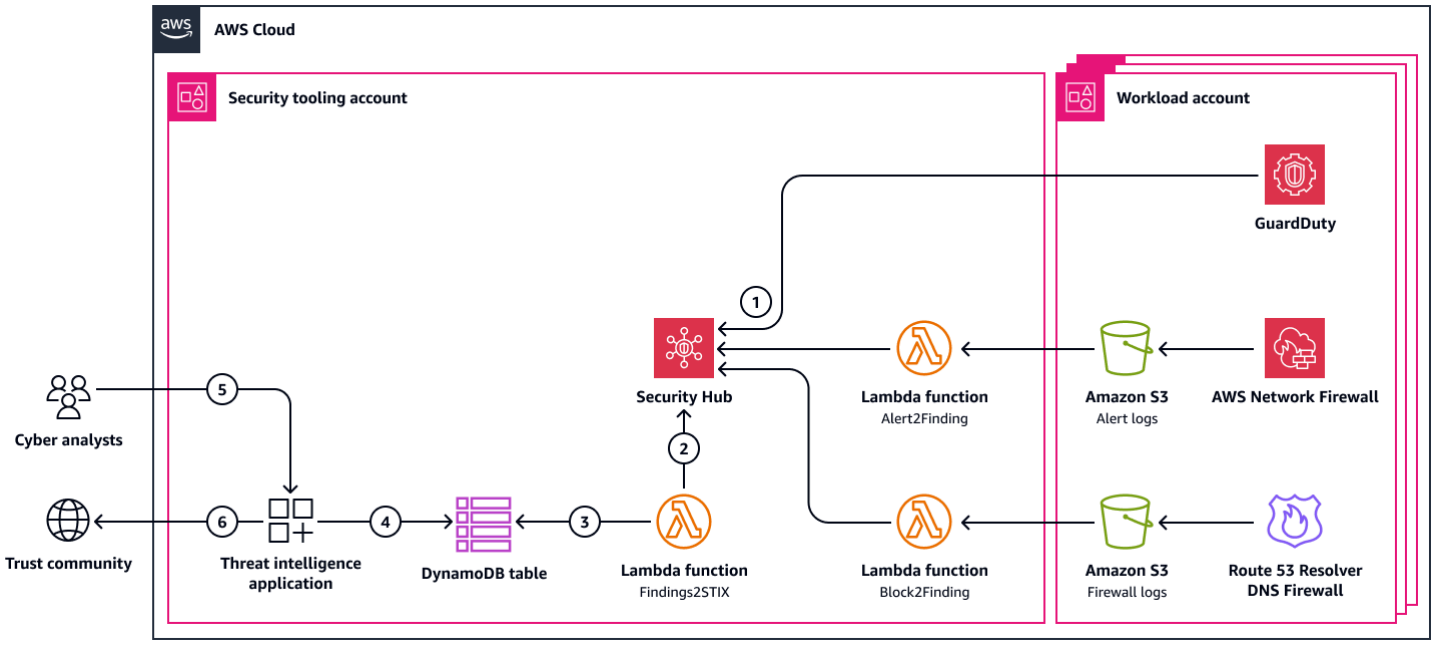
신뢰 커뮤니티와 CTI 공유

사이버 위협 인텔리전스(CTI)를 보내는 커뮤니티는 일반적으로 CTI를 받는 커뮤니티와 동일합니다. 그러나를 더 많이 공유하도록 선택할 수 있습니다. 예를 들어 국가 사이버 보안 센터 또는 정보 공유 및 분석 센터(ISACs)와 같이 신뢰할 수 있는 정부 또는 규제 기관과 공유하도록 선택할 수 있습니다. 목표는 여러 조직의 결과를 풀링하여 CTI를 빠르게 전파하고 구현하는 것입니다. 위협 인텔리전스 플랫폼은 여러 피드와 공유하기 위한 API 통합을 관리합니다.

CTI를 신뢰 커뮤니티에 보내는 것은 예방 및 탐지 제어를 구현하는 것과 동시에 이루어집니다. 로그를 사용하여 보안 이벤트를 식별할 수 있습니다. 그런 다음 이벤트와 결과를 중앙 집중화하여의 보안 태세에 대한 개요를 빠르게 확인할 수 있습니다 AWS 계정. 그러면 사이버 분석가와 같은 보안 팀이 가치 있는 정보를 식별할 수 있습니다. 이미 조사 결과가 있으므로 이러한 조사 결과를 JSON 또는 STIX와

같은 위협 피드에서 사용하는 형식으로 변환 AWS Security Hub CSPM할 수 있습니다. 그런 다음 피드 공급자에게 CTI를 전송합니다. 위협 인텔리전스 플랫폼은 사용자가 제공하는 CTI를 수집, 익명화 및 검증합니다. 그러면 CTI가 더 광범위한 커뮤니티와 공유됩니다.

다음 이미지는 AWS 서비스 를 사용하여 CTI를 생성한 다음 사이버 기관 및 기타 커뮤니티 구성원을 포함한 신뢰 커뮤니티와 공유하는 방법을 보여줍니다.



이 다이어그램은 다음 워크플로를 보여줍니다.

1. 결과는에서 생성됩니다 AWS Security Hub CSPM.
2. AWS Lambda 함수는 Security Hub CSPM에서 결과를 검색하여 JSON 또는 STIX와 같은 공유 가능한 형식으로 변환합니다.
3. Lambda 함수는 조사 결과를 Amazon DynamoDB 테이블에 저장합니다.
4. Amazon Elastic Compute Cloud(Amazon EC2) 또는 Amazon Elastic Container Service(Amazon ECS)에서 실행되는 타사 위협 인텔리전스 플랫폼은 DynamoDB 테이블에서 결과를 검색합니다.
5. 사이버 분석가가 위협 인텔리전스 플랫폼에서 CTI를 검토합니다.
6. 위협 인텔리전스 플랫폼은 다른 CTI 생산자와 소비자로 구성된 신뢰 커뮤니티에 CTI를 게시합니다.

다음 단계 및 리소스

조직의 자산, 부문 및 위협 환경을 고려합니다. 이러한 요인은 신뢰 커뮤니티에 사이버 위협 인텔리전스 공유에 참여하기로 선택했음을 알려야 합니다. 전 세계의 많은 사이버 기관에서 위협 인텔리전스 피드를 제공합니다. 제안 사항을 고려하고 조직의 사용 사례에 가장 적합한 것을 선택합니다. 이 가이드를 모듈식 접근 방식으로 사용하고 조직에 맞게 조정합니다.

다음과 같은 추가 리소스를 검토하는 것이 좋습니다. 이러한 리소스는 AWS 환경에 위협 인텔리전스 플랫폼을 구축 또는 배포하고 사이버 위협 인텔리전스 공유를 설정하는 데 도움이 될 수 있습니다.

AWS 리소스

- AWS 아키텍처 센터
- AWS re:Inforce 2024 -에서 사이버 위협 인텔리전스 공유 AWS(비디오)
- 서AWS 및 ANZ 2023: AUS 사이버 보안 센터(비디오)와 사이버 위협 인텔리전스 공유 조정

AWS 서비스 설명서

- Amazon DynamoDB 설명서
- Amazon EventBridge 설명서
- Amazon GuardDuty 설명서
- AWS Lambda 설명서
- AWS Network Firewall 설명서
- Amazon Route 53 Resolver DNS 방화벽 설명서
- AWS Security Hub CSPM 설명서
- Amazon Security Lake 설명서
- Amazon Simple Storage Service(Amazon S3) 설명서
- AWS Step Functions 설명서

STIX 리소스

- STIX 2.1 예제
- 악성 URL 표시기

위협 인텔리전스 플랫폼

- OpenCTI
- MISP

기여자

다음 개인이이 가이드에 기여했습니다.

작성

- Jess Modini, Senior Technologist, AWS
- Alexa Donovan, Associate Solutions Architect AWS
- 파트너 솔루션 아키텍트인 스티븐 라이언 AWS
- Byron Pogson, 보안 솔루션 아키텍트, AWS

검토

- Brian Farnhill, 선임 소프트웨어 개발 엔지니어, AWS
- Marc Luescher, Senior Solutions Architect AWS
- Stefan Mijic, 보안 보증 전문가, AWS
- Timothy Woodill, 공공 부문 솔루션 아키텍트 AWS

기술 작성

- GxP AbouHarb, Senior Technical Writer, AWS

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2024년 12월 12일

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