AWS 보안 참조 아키텍처(AWS SRA) – 코어 아키텍처

AWS 권장 가이드

AWS 권장 가이드: AWS 보안 참조 아키텍처(AWS SRA) – 코어 아키텍처

Table of Contents

AWS 보안 참조 아키텍처(AWS SRA) - 코어 아키텍처

글로벌 서비스 보안 팀, Amazon Web Services(기여자)

2025년 12월(문서 기록)

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

Amazon Web Services(AWS) 보안 참조 아키텍처(AWS SRA)는 다중 계정 환경에서 AWS 보안 서비스의 전체 보완을 배포하기 위한 전체적인 지침 세트입니다. 이를 사용하여 AWS 권장 사례에 맞게 AWS 보안 서비스를 설계, 구현 및 관리할 수 있습니다. 권장 사항은 AWS 보안 서비스를 포함하는 단일 페이지 아키텍처, 즉 보안 목표를 달성하는 데 도움이 되는 방법,에서 가장 잘 배포 및 관리할 수 있는 위치 AWS 계정, 다른 보안 서비스와 상호 작용하는 방법을 기반으로 구축됩니다. 이 전체 아키텍처 지침은 AWS 보안 설명서 웹 사이트에 있는 권장 사항과 같은 자세한 서비스별 권장 사항을 보완합니다.

아키텍처 및 이에 수반되는 권장 사항은 AWS 엔터프라이즈 고객과의 집단적 경험을 기반으로 합니다. 이 문서는를 사용하여 특정 환경을 AWS 서비스 보호하기 위한 포괄적인 지침 세트인 참조이며, AWS SRA 코드 리포지토리의 솔루션 패턴은이 참조에 설명된 특정 아키텍처에 맞게 설계되었습니다. 고객마다 요구 사항이 다릅니다. 따라서 AWS 환경 설계는 여기에 제공된 예제와 다를 수 있습니다. 개별 환경 및 보안 요구 사항에 맞게 이러한 권장 사항을 수정하고 조정해야 합니다. 문서 전체에서 해당하는 경우 자주 보이는 대체 시나리오에 대한 옵션을 제안합니다.

AWS SRA는 실시간 지침 세트이며 새로운 서비스 및 기능 릴리스, 고객 피드백, 끊임없이 변화하는 위협 환경에 따라 주기적으로 업데이트됩니다. 각 업데이트에는 개정 날짜와 관련 변경 로그가 포함됩니다.

한 페이지짜리 다이어그램을 기반으로 하지만 아키텍처는 단일 블록 다이어그램보다 더 깊어지므로 기초 및 보안 원칙의 잘 구성된 기초를 기반으로 구축해야 합니다. 이 문서는 서술 또는 참조의 두 가지 방법으로 사용할 수 있습니다. 주제는 스토리로 구성되어 있으므로 처음부터(기본 보안 지침) 끝까지(구현할 수 있는 코드 샘플에 대한 설명) 읽을 수 있습니다. 또는 문서를 탐색하여 요구 사항과 가장 관련성이 높은 보안 원칙, 서비스, 계정 유형, 지침 및 예제에 집중할 수 있습니다.

이 문서는 다음 섹션과 부록으로 나뉩니다.

- AWS SRA 라이브러리 정보에서는 AWS SRA 간행물 컬렉션에 포함된 기술 지침 및 코드에 대한 개요를 제공합니다.

- AWS SRA의 가치는 AWS SRA 구축의 동기를 설명하고, 이를 사용하여 보안을 개선하는 방법을 설명하고, 주요 요점을 나열합니다.
- 보안 기반은 AWS 클라우드 채택 프레임워크(AWS CAF), AWS Well-Architected 프레임워크 및 AWS 공동 책임 모델을 검토하고 AWS SRA와 특히 관련된 요소를 강조합니다.
- AWS Organizations, 계정 및 IAM 가드레일은 AWS Organizations 서비스를 도입하고, 기본 보안 기능 및 가드레일에 대해 설명하고, 권장되는 다중 계정 전략에 대한 개요를 제공합니다.
- AWS 보안 참조 아키텍처는 기능 AWS 계정및 일반적으로 사용할 수 있는 보안 서비스 및 기능을 보여주는 단일 페이지 아키텍처 다이어그램입니다.
- 보안을 위한 AI/ML은 백그라운드에서 인공 지능 및 기계 학습(AI/ML)을 AWS 서비스 사용하여 특정 보안 목표를 달성하는 방법을 설명합니다. 설계 AWS 서비스 에 이를 포함시켜 고급 보안 기능을 활용할 수 있습니다.
- 보안 아키텍처 구축 – 단계별 접근 방식은 SRA에서 제공하는 참조를 기반으로 6가지 반복 단계로 자체 보안 아키텍처를 AWS 구축하는 방법에 대한 지침을 제공합니다.
- AWS SRA 모범 사례 체크리스트는 가이드 전체에서 설명하는 권장 사항을 보안 아키텍처 버전을 빌드할 때 따를 수 있는 체크리스트로 추출합니다.
- IAM 리소스는 보안 아키텍처에 중요한 AWS Identity and Access Management (IAM) 지침에 대한 요약 및 포인터 세트를 제공합니다.
- AWS SRA용 코드 리포지토리 예제에서는 개발자와 엔지니어가이 문서에 제시된 몇 가지 지침 및 아키텍처 패턴을 배포하는 데 도움이 되는 관련 GitHub 리포지토리의 개요를 제공합니다. HashiCorp의 AWS CloudFormation 또는 Terraform을 사용하여 샘플을 배포할 수 있습니다. 및 비AWS Control Tower 환경 AWS Control Tower 을 모두 지원합니다.

부록에는 개별 AWS 보안, 자격 증명 및 규정 준수 서비스 목록이 포함되어 있으며 각 서비스에 대한 자세한 정보 링크를 제공합니다. 문서 기록 섹션에서는이 문서의 버전을 추적하기 위한 변경 로그를 제공합니다. 변경 알림을 위해 RSS 피드를 구독할 수도 있습니다.

AWS SRA 라이브러리 정보

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

이 가이드는 보안 아키텍처 설계 및 구축을 위한 아키텍처 청사진과 기술 지침을 제공하는 라이브러리의 일부입니다 AWS. 라이브러리는 구현 코드(AWS SRA 코드 라이브러리), 검증 도구(SRA Verify) 및 코어 아키텍처와 심층 분석 아키텍처를 다루는 두 가지 보완적 범주의 가이드로 구성됩니다.

AWS SRA - 코어 아키텍처(이 가이드)

이 가이드는 권장 AWS 보안 아키텍처의 토대를 나타냅니다. 업계, 애플리케이션 유형 또는 기타 고려 사항에 관계없이 모든 조직에 적용되는 출발점입니다. 이 기반을 통해에서 강력하고 확장 가능한 아키텍처를 구축하고 비즈니스가 성장함에 따라 안전하게 확장할 수 있는 강력한 AWS 다중 계정 보안 기준을 AWS 수립할 수 있습니다.

AWS SRA - 심층 분석 아키텍처

AWS SRA – 핵심 아키텍처 가이드는 특정 보안 기능, 애플리케이션 유형, 규정 준수 또는 규제 요구 사항에 맞는 아키텍처 패턴을 제공하는 추가 간행물로 보완됩니다. 이러한 패턴은 코어 아키텍처를 확장하므로 AWS SRA – 코어 아키텍처 가이드와 함께 사용해야 합니다.

다음 가이드는 특정 보안 기능에 맞는 아키텍처 패턴을 제공합니다.

- AWS SRA - ID 관리는 확장 가능하고 강력하며 중앙 집중식 ID 및 액세스 관리 솔루션을 구현하는 방법에 대한 지침을 제공합니다 AWS.
- AWS SRA - 경계 보안은 중앙 계정 또는 개별 계정에서 엣지 보안을 구현하기 AWS 서비스 위한 아키텍처 패턴 및에 대해 설명합니다.
- AWS SRA - 사이버 포렌식은 포렌식 계정을 조직의 포렌식 기능을 개발하고 보안 인시던트 대응(IR) 준비성을 개선하는 출발점으로 구성하는 AWS 방법을 설명합니다.

다음 가이드에서는 특정 애플리케이션 유형에 대한 아키텍처 패턴을 제공합니다. 기본 보안 아키텍처를 빌드한 후 다음 사항에 집중해야 할 수 있습니다.

- AWS SRA - AI 보안은 생성형 AI 서비스를 사용하여 AWS 생성형 AI 기능을 통합하는 애플리케이션을 설계하고 빌드하기 위한 보안 아키텍처 권장 사항을 제공합니다.
- AWS SRA - IoT는 IoT 애플리케이션을 설계하고 빌드하기 위한 보안 아키텍처 권장 사항을 제공합니다 AWS.

또한 다음 가이드에서는 특정 규정 준수 또는 규제 프레임워크와 일치하는 아키텍처 패턴을 설명합니다.

- AWS 개인 정보 보호 참조 아키텍처(AWS PRA)는 개인 데이터를 처리하는 애플리케이션에 대한 보안 아키텍처를 제공하며 일반 데이터 보호 규정(GDPR), 캘리포니아 소비자 개인 정보 보호법(CCPA) 또는 브라질 일반 데이터 보호법(LGPD)과 같은 광범위한 개인 정보 보호 규정 준수 요구 사항을 지원해야 합니다. AWS PRA는에서 개인 정보 보호 제어의 설계 및 구성과 관련된 일련의 지침을 제공합니다 AWS 서비스.

기본 AWS 아키텍처를 이해하려면 SRA - 핵심 아키텍처 가이드로 시작한 다음 보완 가이드를 참조하여 고급 기능과 구현을 활용하는 것이 좋습니다. 이 콘텐츠 세트에 대한 자세한 내용은 AWS 보안 참조 아키텍처를 참조하세요.

> 아키텍처 다이어그램
>
> 비즈니스 요구 사항에 따라 AWS SRA 라이브러리의 참조 아키텍처 다이어그램을 사용자 지정하려면 다음 .zip 파일을 다운로드하고 내용을 추출할 수 있습니다.
>
> 다이어그램 소스 파일 다운로드(Microsoft PowerPoint 형식)

AWS SRA의 값

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

AWS 에는 대규모(및 증가하는) 보안 및 보안 관련 서비스 세트가 있습니다. 고객은 서비스 설명서, 블로그 게시물, 자습서, 서밋 및 컨퍼런스를 통해 제공되는 자세한 정보에 대해 감사를 표했습니다. 또한 큰 그림을 더 잘 이해하고 AWS 보안 서비스에 대한 전략적 관점을 얻고 싶다고 알려줍니다. 고객과 협력하여 필요한 사항에 대해 더 깊이 이해하면 세 가지 우선 순위가 나타납니다.

- 고객은 AWS 보안 서비스를 전체적으로 배포, 구성 및 운영하는 방법에 대한 자세한 정보와 권장 패턴을 원합니다. 서비스를 배포하고 관리해야 하는 계정과 보안 목표는 무엇입니까? 모든 또는 대부분의 서비스를 운영해야 하는 보안 계정이 하나 있나요? 위치(조직 단위 또는 AWS 계정) 선택은 보안 목표에 어떤 영향을 미치나요? 고객이 알아야 할 장단점(설계 고려 사항)은 무엇입니까?
- 고객은 여러 AWS 보안 서비스를 논리적으로 구성하기 위해 다양한 관점을 보는 데 관심이 있습니다. 이러한 대체 관점은 각 서비스(예: 자격 증명 서비스 또는 로깅 서비스)의 기본 기능 외에도 고객이 보안 아키텍처를 계획, 설계 및 구현하는 데 도움이 됩니다. 이 문서의 뒷부분에서 공유된 예제는 AWS 환경의 권장 구조에 맞게 조정된 보호 계층을 기반으로 서비스를 그룹화합니다.
- 고객은 가장 효과적인 방식으로 보안 서비스를 통합하기 위한 지침과 예제를 찾고 있습니다. 예를 들어 자동화된 감사 및 모니터링 파이프라인에서 과중한 작업을 수행하기 위해 다른 서비스와 가장 잘 정렬하고 연결 AWS Config 해야 하는 방법은 무엇입니까? 고객은 각 AWS 보안 서비스가 다른 보안 서비스에 의존하거나 지원하는 방법에 대한 지침을 요청합니다.

AWS SRA에서 이러한 각 항목을 처리합니다. 목록의 첫 번째 우선 순위(사물 이동 위치)는 기본 아키텍처 다이어그램과이 문서의 관련 토론에 중점을 둡니다. 권장 AWS Organizations 아키텍처와 어떤 서비스가 어디로 이동하는지에 대한 account-by-account 설명을 제공합니다. 목록의 두 번째 우선 순위(전체 보안 서비스 세트에 대해 생각하는 방법)를 시작하려면 AWS 조직 전체에 보안 서비스 적용 섹션을 참조하세요. 이 섹션에서는 AWS 조직의 요소 구조에 따라 보안 서비스를 그룹화하는 방법을 설명합니다. 또한 이러한 동일한 아이디어가 애플리케이션 계정에 대한 설명에 반영됩니다.이 설명에서는 보안 서비스를 운영하여 계정의 특정 계층, 즉 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, Amazon Virtual Private Cloud(Amazon VPC) 네트워크 및 더 광범위한 계정에 집중할 수 있는 방법을 강조합니다. 마지막으로 세 번째 우선순위(서비스 통합)는 지침 전반에 반영됩니다. 특히 AWS SRA 라이브러리의 심층 분석 가이드와 AWS SRA 코드 리포지토리의 코드에서 개별 서비스에 대한 설명에 반영됩니다.

AWS SRA 사용 방법

클라우드 채택 여정의 현재 위치에 따라 AWS SRA를 사용하는 방법에는 여러 가지가 있습니다. 다음은 AWS SRA 자산(아키텍처 다이어그램, 작성된 지침 및 코드 샘플)에서 가장 많은 인사이트를 얻을 수 있는 방법 목록입니다.

- 자체 보안 아키텍처의 대상 상태를 정의합니다.

  AWS 클라우드 여정을 막 시작하든, 첫 번째 계정 집합을 설정하든, 설정된 AWS 환경을 개선할 계획이든, AWS SRA는 보안 아키텍처 구축을 시작할 수 있는 곳입니다. 계정 구조 및 보안 서비스의 포괄적인 기반으로 시작한 다음 특정 기술 스택, 기술, 보안 목표 및 규정 준수 요구 사항에 따라 조정합니다. 더 많은 워크로드를 구축하고 시작할 예정이라면 사용자 지정 버전의 AWS SRA를 가져와 조직의 보안 참조 아키텍처의 기반으로 사용할 수 있습니다. AWS SRA에서 설명하는 대상 상태를 달성하는 방법을 알아보려면 보안 아키텍처 구축 - 단계별 접근 방식을 참조하세요.

- 이미 구현한 설계 및 기능을 검토(수정)합니다.

  이미 보안 설계 및 구현이 있는 경우 AWS SRA와 보안 설계 및 구현을 비교하는 데 시간이 걸릴 수 있습니다. AWS SRA는 포괄적으로 설계되었으며 자체 보안을 검토하기 위한 진단 기준을 제공합니다. 보안 설계가 AWS SRA에 부합하는 경우 사용 시 모범 사례를 따르고 있다고 더 확신할 수 있습니다 AWS 서비스. 보안 설계가 SRA의 지침에 AWS 따라 달라지거나 일치하지 않는 경우 이는 반드시 잘못된 일을 하고 있다는 신호는 아닙니다. 대신이 관찰을 통해 결정 프로세스를 검토할 수 있습니다. AWS SRA 모범 사례를 벗어날 수 있는 합법적인 비즈니스 및 기술 이유가 있습니다. 특정 규정 준수, 규제 또는 조직 보안 요구 사항에 따라 특정 서비스 구성이 필요할 수 있습니다. 또는를 사용하는 대신 AWS 서비스또는 빌드하고 관리하는 AWS Partner Network 사용자 지정 애플리케이션의 제품에 대한 기능 기본 설정이 있을 수 있습니다. 이 검토 중에 이전 결정이 더 이상 적용되지 않는 이전 기술, AWS 기능 또는 비즈니스 제약을 기반으로 이루어졌다는 것을 발견할 수도 있습니다. 이는 업데이트를 검토하고, 우선순위를 지정하고, 엔지니어링 백로그의 적절한 위치에 추가할 수 있는 좋은 기회입니다. AWS SRA를 고려하여 보안 아키텍처를 평가할 때 발견한 내용은 해당 분석을 문서화하는 것이 중요합니다. 결정 및 근거에 대한 기록 기록을 확보하면 향후 결정을 알리고 우선순위를 정하는 데 도움이 될 수 있습니다.

- 자체 보안 아키텍처의 구현을 부트스트랩합니다.

  AWS SRA 코드형 인프라(IaC) 모듈은 보안 아키텍처 구축 및 구현을 빠르고 안정적으로 시작할 수 있는 방법을 제공합니다. 이러한 모듈은 코드 리포지토리 섹션과 퍼블릭 GitHub 리포지토리에 더 자세히 설명되어 있습니다. 이를 통해 엔지니어는 AWS SRA 지침의 패턴에 대한 고품질 예제를 구축할 수 있을 뿐만 아니라 IAM 암호 정책, Amazon Simple Storage Service(Amazon S3) 블록 계정 퍼블릭 액세스, Amazon EC2 기본 Amazon Elastic Block Store(Amazon EBS) 암호화, 와의 통합과 같

은 권장 보안 제어를 통합하여 새 AWS 계정 가 온보딩되거나 폐기될 때 제어를 적용하거나 제거할 수 AWS Control Tower 있습니다.

- AWS 보안 서비스 및 기능에 대해 자세히 알아봅니다.

  AWS SRA의 지침 및 논의에는 개별 AWS 보안 및 보안 관련 서비스에 대한 배포 및 관리 고려 사항 뿐만 아니라 중요한 기능이 포함되어 있습니다. AWS SRA의 한 가지 기능은 AWS 보안 서비스의 폭과 다중 계정 환경에서 함께 작동하는 방식에 대한 개략적인 소개를 제공한다는 것입니다. 이를 통해 다른 소스에서 찾을 수 있는 각 서비스의 기능과 구성을 자세히 살펴볼 수 있습니다. 이에 대한 한 가지 예는 AWS Security Hub 클라우드 보안 태세 관리(AWS Security Hub CSPM)가 다양한 AWS 서비스 AWS Partner 제품 및 자체 애플리케이션의 보안 조사 결과를 수집하는 방법에 대한 설명입니다.

- 조직의 거버넌스 및 보안 책임에 대한 논의를 주도합니다.

  보안 아키텍처 또는 전략을 설계하고 구현하는 데 중요한 요소는 조직에서 보안 관련 책임이 있는 사람을 이해하는 것입니다. 예를 들어 보안 조사 결과를 집계하고 모니터링할 위치에 대한 질문은 해당 활동을 책임질 팀에 대한 질문과 관련이 있습니다. 조직 전체의 모든 조사 결과를 전용 보안 도구 계정에 액세스해야 하는 중앙 팀에서 모니터링하나요? 또는 개별 애플리케이션 팀(또는 사업부)이 특정 모니터링 활동을 담당하므로 특정 알림 및 모니터링 도구에 액세스해야 합니까? 또 다른 예로, 조직에 모든 암호화 키를 중앙에서 관리하는 그룹이 있는 경우이 그룹은 키를 생성 AWS Key Management Service (AWS KMS)할 권한이 있는 사용자와 해당 키를 관리할 계정에 영향을 미칩니다. 조직의 특성, 즉 다양한 팀과 책임을 이해하면 필요에 맞게 AWS SRA를 조정할 수 있습니다. 반대로 보안 아키텍처에 대한 논의가 기존 조직의 책임을 논의하고 잠재적 변경 사항을 고려하기 위한 원동력이 되는 경우가 있습니다.는 워크로드 팀이 워크로드 함수 및 요구 사항을 기반으로 보안 제어를 정의할 책임이 있는 분산된 의사 결정 프로세스를 AWS 권장합니다. 중앙 집중식 보안 및 거버넌스 팀의 목표는 워크로드 소유자가 정보에 입각한 결정을 내리고 모든 당사자가 구성, 조사 결과 및 이벤트를 파악할 수 있는 시스템을 구축하는 것입니다. AWS SRA는 이러한 토론을 식별하고 알리기 위한 수단이 될 수 있습니다.

AWS SRA의 주요 구현 지침

다음은 보안을 설계하고 구현할 때 염두에 두어야 할 AWS SRA의 8가지 주요 사항입니다.

- AWS Organizations 및 적절한 다중 계정 전략은 보안 아키텍처의 필수 요소입니다. 워크로드, 팀 및 기능을 적절하게 분리하면 업무 분리 및 defense-in-depth 있습니다. 이 가이드에서는 이후 단원에서 이에 대해 자세히 설명합니다.
- Defense-in-depth는 조직의 보안 제어를 선택하기 위한 중요한 설계 고려 사항입니다. 구조의 여러 계층에 적절한 보안 제어를 주입 AWS Organizations 하여 문제의 영향을 최소화하는 데 도움이 됩

니다. 한 계층에 문제가 있는 경우 다른 중요한 IT 리소스를 격리하는 제어가 마련되어 있습니다. AWS SRA는 AWS 기술 스택의 여러 계층에서 서로 다른 AWS 서비스 기능이 어떻게 다른지, 그리고 이러한 서비스를 함께 사용하면 defense-in-depth를 달성하는 데 어떻게 도움이 되는지 보여줍니다. 에 대한이 defense-in-depth 개념 AWS 은 애플리케이션 계정 아래에 표시된 설계 예제와 함께 이후 섹션에서 자세히 설명합니다.

- 여러 AWS 서비스 및 기능에 걸쳐 다양한 보안 구성 요소를 사용하여 강력하고 복원력이 뛰어난 클라우드 인프라를 구축합니다. AWS SRA를 특정 요구 사항에 맞게 조정할 때는 AWS 서비스 및 기능(예: 인증, 암호화, 모니터링, 권한 정책)의 기본 기능뿐만 아니라 아키텍처 구조에 어떻게 맞는지도 고려하세요. 가이드의 후반부 섹션에서는 AWS 조직 전체에서 일부 서비스가 작동하는 방식을 설명합니다. 다른 서비스는 단일 계정 내에서 가장 잘 작동하며, 일부는 개별 보안 주체에게 권한을 부여하거나 거부하도록 설계되었습니다. 이 두 가지 관점을 모두 고려하면 보다 유연하고 계층화된 보안 접근 방식을 구축하는 데 도움이 됩니다.
- 가능하면(나중 단원에서 자세히 설명) 모든 계정에 배포할 수 있는를 AWS 서비스 사용하고(중앙 집중식 대신 배포) 워크로드를 오용으로부터 보호하고 보안 이벤트의 영향을 줄이는 데 도움이 되는 일관된 공유 가드레일 세트를 구축합니다. AWS SRA는 AWS Security Hub CSPM (중앙 집중식 결과 모니터링 및 규정 준수 검사), Amazon GuardDuty(위협 탐지 및 이상 탐지), AWS Config (리소스 모니터링 및 변경 탐지), IAM Access Analyzer(리소스 액세스 모니터링), AWS CloudTrail (환경 전반의 로깅 서비스 API 활동) 및 Amazon Macie(데이터 분류)를 모든 AWS 서비스 에 배포할 기본 세트로 사용합니다 AWS 계정.
- 가이드의 위임된 관리 섹션에 설명된 대로 지원되는 AWS Organizations의 위임된 관리 기능을 사용합니다. 이렇게 하면 AWS 멤버 계정을 지원되는 서비스의 관리자로 등록할 수 있습니다. 위임된 관리는 엔터프라이즈 내 여러 팀이 책임에 따라 별도의 계정을 사용하여 환경 AWS 서비스 전체에서를 관리할 수 있는 유연성을 제공합니다. 또한 위임된 관리자를 사용하면 AWS Organizations 관리 계정에 대한 액세스를 제한하고 관리 계정의 권한 오버헤드를 관리할 수 있습니다.
- 조직 전체에 중앙 집중식 모니터링, 관리 및 거버넌스를 구현합니다 AWS . 다중 계정(및 때로는 다중 리전) 집계를 지원하는 AWS 서비스 를 위임된 관리 기능과 함께 사용하면 중앙 보안, 네트워크 및 클라우드 엔지니어링 팀이 적절한 보안 구성 및 데이터 수집을 광범위하게 파악하고 제어할 수 있습니다. 또한 데이터를 워크로드 팀에 다시 제공하여 소프트웨어 개발 수명 주기(SDLC) 초기에 효과적인 보안 결정을 내릴 수 있도록 지원할 수 있습니다.
- AWS Control Tower 를 사용하여 보안 참조 아키텍처 빌드를 부트스트랩하기 위해 사전 구축된 보안 제어를 구현하여 다중 계정 AWS 환경을 설정하고 관리합니다.는 자격 증명 관리, 계정에 대한 페더레이션 액세스, 중앙 집중식 로깅 및 추가 계정을 프로비저닝하기 위한 정의된 워크플로를 제공하는 청사진을 AWS Control Tower 제공합니다. 그런 다음 AWS SRA 코드 리포지토리에 설명된 대로 Customizations for AWS Control Tower (CfCT) 솔루션을 사용하여에서 관리하는 계정을 AWS Control Tower 추가 보안 제어, 서비스 구성 및 거버넌스로 기준선을 지정할 수 있습니다. Account

Factory 기능은 승인된 계정 구성을 기반으로 구성 가능한 템플릿으로 새 계정을 자동으로 프로비저닝하여 AWS 조직 내 계정을 표준화합니다. 거버넌스를 이미 관리되는 조직 단위(OU)에 등록 AWS 계정 하여 기존 개인으로 확장할 수도 있습니다 AWS Control Tower.

- AWS SRA 코드 예제는 코드형 인프라(IaC)를 사용하여 AWS SRA 가이드 내에서 패턴 구현을 자동화하는 방법을 보여줍니다. 패턴을 코드화하면 조직의 다른 애플리케이션처럼 IaC를 처리하고 코드를 배포하기 전에 테스트를 자동화할 수 있습니다. 또한 IaC는 여러(예: SDLC 또는 리전별) 환경에 가드레일을 배포하여 일관성과 반복성을 보장하는 데 도움이 됩니다. SRA 코드 예제는 유무에 관계없이 AWS Organizations 다중 계정 환경에 배포할 수 있습니다 AWS Control Tower. 가 필요한이 리포지토리의 솔루션은 및 Customizations for AWS Control Tower (CfCT)를 사용하여AWS Control Tower환경에 배포 AWS CloudFormation되고 테스트 AWS Control Tower 되었습니다. 필요하지 않은 솔루션은를 사용하여AWS Organizations환경에서 테스트 AWS Control Tower 되었습니다AWS CloudFormation. 를 사용하지 않는 경우 AWS Organizations기반 배포 솔루션을 사용할 AWS Control Tower수 있습니다.

보안 기초

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

AWS SRA는 AWS 클라우드 채택 프레임워크(AWS CAF), AWS ell-Architected, AWS 공동 책임 모델의 세 가지 AWS 보안 기반에 부합합니다.

AWS Professional Services는 기업이 성공적인 클라우드 채택을 위한 가속화된 경로를 설계하고 따를 수 있도록 AWS CAF를 만들었습니다. 프레임워크에서 제공하는 지침과 모범 사례는 기업 전체와 IT 수명 주기 전반에 걸쳐 클라우드 컴퓨팅에 대한 포괄적인 접근 방식을 구축하는 데 도움이 됩니다. AWS CAF는 지침을 관점이라고 하는 6가지 중점 영역으로 구성합니다. 각 관점에서는 기능적으로 관련된 이해관계자가 소유하거나 관리하는 고유한 책임을 다룹니다. 일반적으로 비즈니스, 사람 및 거버넌스 관점은 비즈니스 역량에 중점을 두는 반면, 플랫폼, 보안 및 운영 관점은 기술 역량에 중점을 둡니다.

AWS CAF의 보안 관점은 비즈니스 전반의 제어 선택 및 구현을 구조화하는 데 도움이 됩니다. 보안 원칙의 현재 AWS 권장 사항을 따르면 비즈니스 및 규제 요구 사항을 충족하는 데 도움이 될 수 있습니다.

AWS Well-Architected는 클라우드 아키텍트가 애플리케이션 및 워크로드를 위한 안전하고 성능이 뛰어나며 복원력이 뛰어나고 효율적인 인프라를 구축하는 데 도움이 됩니다. 프레임워크는 운영 우수성, 보안, 신뢰성, 성능 효율성, 비용 최적화 및 지속 가능성이라는 6가지 원칙을 기반으로 하며 고객과 파트너가 아키텍처를 평가하고 시간이 지남에 따라 확장할 수 있는 설계를 구현할 수 있는 일관된 접근 방식을 AWS 제공합니다. 워크로드를 제대로 설계하면 비즈니스 성공 가능성이 높아집니다.

Well-Architected Framework 보안 원칙은 보안 태세를 개선할 수 있는 방식으로 데이터, 시스템 및 자산을 보호하는 데 도움이 되는 클라우드 기술을 활용하는 방법을 설명합니다. 이를 통해 현재 AWS 권장 사항에 따라 비즈니스 및 규제 요구 사항을 충족할 수 있습니다. 거버넌스, 서버리스, AI/ML, 게임과 같은 특정 도메인에 더 많은 컨텍스트를 제공하는 Well-Architected Framework 중점 영역이 추가로 있습니다. 이를 AWS Well-Architected 렌즈라고 합니다.

보안 및 규정 준수는 AWS 와 고객 간의 공동 책임입니다. 이 공유 모델은 호스트 운영 체제 및 가상화 계층에서 서비스가 운영되는 시설의 물리적 보안에 이르기까지 구성 요소를 AWS 운영, 관리 및 제어할 때 운영 부담을 줄이는 데 도움이 될 수 있습니다. 예를 들어 게스트 운영 체제(업데이트 및 보안 패치 포함), 애플리케이션 소프트웨어, 서버 측 데이터 암호화, 네트워크 트래픽 라우팅 테이블 및 AWS 제공 보안 그룹 방화벽의 구성에 대한 책임과 관리를 맡습니다. Amazon S3 및 Amazon DynamoDB와 같은 추상화된 서비스의 경우 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하며 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. 사용자는 데이터(암호화 옵션 포함)를 관리하고, 자산을 분류하

고, IAM 도구를 사용하여 적절한 권한을 적용할 책임이 있습니다. 이 공유 모델은 AWS 가 클라우드의 보안(즉,에서 제공되는 모든 서비스를 실행하는 인프라 보호 AWS 클라우드)을 책임지고, 사용자가 클라우드의 보안(선택한 AWS 클라우드 서비스에 따라 결정됨)을 책임진다고 설명하여 설명되는 경우가 많습니다.

이러한 기본 문서에서 제공하는 지침 내에서 두 가지 개념, 즉 보안 기능 및 보안 설계 원칙은 AWS SRA의 설계 및 이해와 특히 관련이 있습니다.

보안 기능

AWS CAF의 보안 관점은 데이터 및 클라우드 워크로드의 기밀성, 무결성 및 가용성을 달성하는 데 도움이 되는 9가지 기능을 간략하게 설명합니다.

- 조직 AWS 환경 전반에 걸쳐 보안 역할, 책임, 정책, 프로세스 및 절차를 개발하고 전달하는 보안 거버넌스입니다.
- 보안 및 개인 정보 보호 프로그램의 효과를 모니터링, 평가, 관리 및 개선하기 위한 보안 보증.
- ID 및 액세스 관리를 통해 ID 및 권한을 대규모로 관리합니다.
- 위협 탐지를 통해 잠재적인 보안 구성 오류, 위협 또는 예상치 못한 동작을 이해하고 식별합니다.
- 취약성 관리를 통해 보안 취약성을 지속적으로 식별, 분류, 해결 및 완화합니다.
- 워크로드 내의 시스템 및 서비스가 보호되는지 검증하는 데 도움이 되는 인프라 보호.
- 데이터 보호를 통해 데이터에 대한 가시성과 제어, 조직에서 데이터에 액세스하고 사용하는 방법을 유지할 수 있습니다.
- 소프트웨어 개발 프로세스 중에 보안 취약성을 감지하고 해결하는 데 도움이 되는 애플리케이션 보안.
- 보안 인시던트에 효과적으로 대응하여 잠재적 피해를 줄이기 위한 인시던트 대응.

보안 설계 원칙

Well-Architected Framework의 보안 원칙은 특정 보안 영역을 워크로드 보안을 강화하는 데 도움이 되는 실용적인 지침으로 전환하는 7가지 설계 원칙 세트를 캡처합니다. 보안 기능이 전체 보안 전략을 구성하는 경우 이러한 Well-Architected Framework 원칙은 시작할 수 있는 작업을 설명합니다. 이는이 AWS SRA에 매우 의도적으로 반영되며 다음으로 구성됩니다.

- 강력한 자격 증명 기반 구현 – 최소 권한 원칙을 구현하고 AWS 리소스와의 각 상호 작용에 대해 적절한 권한 부여를 통해 업무 분리를 적용합니다. 자격 증명 관리를 중앙 집중화하고 장기적인 정적 자격 증명에 대한 의존도를 해소하는 것을 목표로 합니다.

- 추적성 활성화 – 환경에 대한 작업 및 변경 사항을 실시간으로 모니터링, 알림 생성 및 감사합니다. 로그 및 지표 수집을 시스템과 통합하여 자동으로 조사하고 조치를 취합니다.
- 모든 계층에 보안 적용 – 여러 보안 제어를 통해 defense-in-depth 접근 방식을 적용합니다. 네트워크 엣지, Virtual Private Cloud(VPC), 로드 밸런싱, 인스턴스 및 컴퓨팅 서비스, 운영 체제, 애플리케이션 구성 및 코드를 포함한 여러 유형의 제어(예: 예방 및 탐지 제어)를 모든 계층에 적용합니다.
- 보안 모범 사례 자동화 - 자동화된 소프트웨어 기반 보안 메커니즘은 보다 빠르고 비용 효율적으로 안전하게 확장할 수 있는 기능을 개선합니다. 보안 아키텍처를 생성하고 버전 제어 템플릿에서 코드로 정의 및 관리되는 제어를 구현합니다.
- 전송 중 및 저장 데이터 보호 – 데이터를 민감도 수준으로 분류하고 적절한 경우 암호화, 토큰화 및 액세스 제어와 같은 메커니즘을 사용합니다.
- 데이터에서 사람들을 멀리 하기 – 메커니즘과 도구를 사용하여 데이터에 직접 액세스하거나 수동으로 처리할 필요성을 줄이거나 없앱니다. 이를 통해 민감한 데이터를 처리할 때 잘못된 취급이나 수정 및 수작업으로 인한 오류의 위험을 줄일 수 있습니다.
- 보안 이벤트 준비 – 조직 요구 사항에 맞는 인시던트 관리 및 조사 정책과 프로세스를 마련하여 인시던트를 준비합니다. 인시던트 대응 시뮬레이션을 실행하고 자동화된 도구를 사용하여 감지, 조사 및 복구 속도를 높입니다.

AWS CAF 및 AWS Well-Architected Framework와 함께 AWS SRA를 사용하는 방법

AWS CAF, AWS Well-Architected Framework 및 AWS SRA는 클라우드 마이그레이션 및 현대화 작업을 지원하기 위해 함께 작동하는 보완 프레임워크입니다.

- AWS CAF는 AWS 경험과 모범 사례를 활용하여 클라우드 채택의 가치를 원하는 비즈니스 성과에 맞게 조정하는 데 도움이 됩니다. AWS CAF를 사용하여 혁신 기회를 식별하고 우선순위를 지정하며, 클라우드 준비 상태를 평가 및 개선하고, 혁신 로드맵을 반복적으로 발전시킵니다.
- AWS Well-Architected Framework는 비즈니스 성과를 충족하는 다양한 애플리케이션 및 워크로드를 위한 안전하고 성능이 뛰어나며 복원력이 뛰어나고 효율적인 인프라를 구축하기 위한 AWS 권장 사항을 제공합니다.
- AWS SRA는 AWS CAF 및 AWS Well-Architected Framework의 권장 사항에 맞는 방식으로 보안 서비스를 배포하고 관리하는 방법을 이해하는 데 도움이 됩니다.

예를 들어 AWS CAF 보안 관점에서는 인력 자격 증명과 인증을 중앙에서 관리하는 방법을 평가하는 것이 좋습니다 AWS. 이 정보를 바탕으로 Okta, Active Directory 또는 Ping Identity와 같은 신규 또

는 기존 기업 자격 증명 공급자(IdP) 솔루션을이 용도로 사용하기로 결정할 수 있습니다. AWS Well-Architected Framework의 지침을 따르고 IdP를와 통합하여 직원에게 그룹 멤버십 및 권한을 동기화 AWS IAM Identity Center 할 수 있는 Single Sign-On 환경을 제공하기로 결정합니다. AWS SRA 권장 사항을 검토하여 AWS 조직의 관리 계정에서 IAM Identity Center를 활성화하고 보안 운영 팀이 사용하는 보안 도구 계정을 통해 관리합니다. 이 예제는 AWS CAF가 원하는 보안 태세에 대한 초기 결정을 내리는 데 어떻게 도움이 되는지 보여줍니다. AWS Well-Architected 프레임워크는 해당 목표를 충족하는 데 사용할 수 AWS 서비스 있는를 평가하는 방법에 대한 지침을 제공하며, AWS SRA는 선택한 보안 서비스를 배포하고 관리하는 방법에 대한 권장 사항을 제공합니다.

SRA 빌딩 블록 - AWS Organizations, 계정 및 가드레일

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

AWS 보안 서비스, 제어 및 상호 작용은 AWS 다중 계정 전략과 자격 증명 및 액세스 관리 가드레일의 기반에 가장 잘 사용됩니다. 이러한 가드레일은 최소 권한, 업무 분리 및 개인 정보 보호를 구현할 수 있는 기능을 설정하고 필요한 제어 유형, 각 보안 서비스가 관리되는 위치, AWS SRA에서 데이터와 권한을 공유하는 방법에 대한 결정을 지원합니다.

AWS 계정 는 리소스에 대한 보안, 액세스 및 결제 경계를 AWS 제공하며 리소스 독립성과 격리를 달성할 수 있습니다. 여러 계정을 사용하여 AWS 환경 구성 백서의 여러 섹션을 사용하면 이점 AWS 계정에 설명된 대로 여러 AWS 계정 를 사용하면 보안 요구 사항을 충족하는 데 중요한 역할을 합니다. 예를 들어, 기업의 보고 구조를 미러링하는 대신 함수, 규정 준수 요구 사항 또는 일반적인 제어 세트를 기반으로 조직 단위(OU) 내의 개별 계정 및 그룹 계정에 워크로드를 구성할 수 있습니다. 워크로드가 증가함에 따라 기업이 공통 가드레일을 설정할 수 있도록 보안 및 인프라를 염두에 두세요. 이 접근 방식은 워크로드 간에 강력한 경계와 제어를 제공합니다. 계정 수준 분리 AWS Organizations는와 함께 프로덕션 환경을 개발 및 테스트 환경에서 격리하거나 Payment Card Industry Data Security Standard(PCI DSS) 또는 Health Insurance Portability and Accountability Act(HIPAA)와 같은 다양한 분류의 데이터를 처리하는 워크로드 간에 강력한 논리적 경계를 제공하는 데 사용됩니다. 단일 계정으로 AWS 여정을 시작할 수 있지만 워크로드의 크기와 복잡성이 증가함에 따라 여러 계정을 설정하는 것이 AWS 좋습니다.

권한을 사용하면 AWS 리소스에 대한 액세스를 지정할 수 있습니다. 보안 주체(사용자, 그룹 및 역할)라고 하는 IAM 엔터티에 권한이 부여됩니다. 기본적으로 보안 주체는 권한 없이 시작합니다. IAM 보안 주체는 권한을 부여할 AWS 때까지에서 아무 작업도 수행할 수 없으며, 전체 AWS 조직만큼 광범위하게 적용되거나 보안 주체, 작업, 리소스 및 조건의 개별 조합만큼 세분화된 가드레일을 설정할 수 있습니다.

보안을 AWS Organizations 위한 사용

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

AWS Organizations는 AWS 리소스를 확장하고 확장함에 따라 환경을 중앙에서 관리하고 관리하는 데 도움이 됩니다. 를 사용하면 프로그래밍 방식으로 새 AWS Organizations를 생성하고 AWS 계정, 리소

스를 할당하고, 계정을 그룹화하여 워크로드를 구성하고, 거버넌스를 위해 계정 또는 계정 그룹에 정책을 적용할 수 있습니다. AWS 조직은 단일 단위로 관리할 수 AWS 계정 있도록를 통합합니다. 0개 이상의 멤버 계정과 함께 하나의 관리 계정이 있습니다. 관리 계정 또는 특정에 대해 위임된 관리자로 할당된 계정에 상주해야 하는 일부 중앙 관리형 프로세스를 제외하고 대부분의 워크로드는 멤버 계정에 상주합니다 AWS 서비스. 보안 팀이 AWS 조직을 대신하여 보안 요구 사항을 관리할 수 있도록 중앙 위치에서 도구와 액세스를 제공할 수 있습니다. AWS 조직 내에서 중요한 리소스를 공유하여 리소스 중복을 줄일 수 있습니다. 워크로드의 요구 사항 및 목적에 따라 다양한 환경을 나타낼 수 있는 AWS 조직 단위(OUs)로 계정을 그룹화할 수 있습니다. AWS Organizations 또한는 조직의 모든 멤버 계정에 추가 보안 제어를 중앙에서 적용할 수 있는 여러 정책을 제공합니다. 이 섹션에서는 서비스 제어 정책(SCPs), 리소스 제어 정책(RCPs) 및 선언적 정책에 중점을 둡니다.

를 사용하면 SCPs 및 RCPs 사용하여 AWS 조직, OU 또는 계정 수준에서 권한 가드레일을 적용할 AWS Organizations수 있습니다. SCPs는 관리 계정(이 계정에서 워크로드를 실행하지 않는 이유 중 하나)을 제외하고 조직 계정 내의 보안 주체에 적용되는 가드레일입니다. SCP를 OU에 연결하면 SCP는 해당 OU의 하위 OUs 및 계정에 의해 상속됩니다. SCPs 권한을 부여하지 않습니다. 대신 AWS 조직, OU 또는 계정의 보안 주체에 사용할 수 있는 최대 권한을 지정합니다. 실제로 권한을 부여하려면의 보안 주체 또는 리소스에 자격 증명 기반 또는 리소스 기반 정책을 연결해야 합니다. AWS 계정 예를 들어 SCP가 모든 Amazon S3에 대한 액세스를 거부하는 경우 SCP의 영향을 받는 보안 주체는 IAM 정책을 통해 명시적으로 액세스 권한이 부여되더라도 Amazon S3에 액세스할 수 없습니다. IAM 정책 평가 방법, SCPs, 액세스 권한 부여 또는 거부 방법에 대한 자세한 내용은 IAM 설명서의 정책 평가 로직을 참조하세요.

RCPs는 리소스가 동일한 조직에 속하는지 여부에 관계없이 조직의 계정 내 리소스에 적용되는 가드레일입니다. SCPs와 마찬가지로 RCPs 관리 계정의 리소스에 영향을 주지 않으며 권한을 부여하지 않습니다. RCP를 OU에 연결하면 OU 아래의 하위 OUs 및 계정에 의해 RCP가 상속됩니다. RCPs 조직 내 리소스에 사용할 수 있는 최대 권한을 중앙에서 제어하며 현재의 하위 집합을 지원합니다 AWS 서비스. OUs용 SCPs를 설계할 때는 IAM 정책 시뮬레이터를 사용하여 변경 사항을 평가하는 것이 좋습니다. 또한 IAM에서 마지막으로 액세스한 서비스 데이터를 검토하고 AWS CloudTrail 를 사용하여 API 수준에서 서비스 사용량을 로깅하여 SCP 변경의 잠재적 영향을 이해해야 합니다.

SCP와 RCP는 독립적인 제어입니다. SCPs 또는 RCPs만 활성화하거나 적용하려는 액세스 제어에 따라 두 정책 유형을 함께 사용하도록 선택할 수 있습니다. 예를 들어 조직의 보안 주체가 조직 외부의 리소스에 액세스하지 못하도록 하려면 SCPs를 사용하여이 제어를 적용합니다. 외부 자격 증명이 리소스에 액세스하지 못하도록 제한하려면 RCPs를 사용하여이 제어를 적용합니다. RCP 및 SCPs에 대한 자세한 내용과 사용 사례는 AWS Organizations 설명서의 SCPs 및 RCPs 사용을 참조하세요.

AWS Organizations 선언적 정책을 사용하여 조직 전체에서 지정된에 대해 원하는 구성을 중앙 AWS 서비스 에서 선언하고 적용할 수 있습니다. 예를 들어 조직 전체에서 Amazon VPC 리소스에 대한 퍼블

릭 인터넷 액세스를 차단할 수 있습니다. SCPs 및 RCPs와 같은 권한 부여 정책과 달리 선언적 정책은 AWS 서비스의 컨트롤 플레인에 적용됩니다. 권한 부여 정책은 APIs에 대한 액세스를 규제하는 반면, 선언적 정책은 내구성 있는 의도를 적용하기 위해 서비스 수준에서 직접 적용됩니다. 이러한 정책은 서비스가 새로운 기능 또는 APIs를 도입하더라도 AWS 서비스 에 대한 기준 구성을 항상 유지하도록 보장합니다. 새 계정이 조직에 추가되거나 새 위탁자 및 리소스가 생성될 때도 기준 구성이 유지됩니다. 선언적 정책은 전체 조직 또는 특정 OUs 또는 계정에 적용할 수 있습니다.

모든 AWS 계정 에는 기본적으로 모든 AWS 리소스에 대한 전체 권한을 가진 단일 루트 사용자가 있습니다. 보안 모범 사례로 루트 사용자가 명시적으로 필요한 몇 가지 작업을 제외하고 루트 사용자를 사용하지 않는 것이 좋습니다. 여러를 AWS 계정 통해 관리하는 경우 루트 로그인을 중앙에서 비활성화한 다음 모든 멤버 계정을 대신하여 루트 권한 있는 작업을 수행할 AWS Organizations수 있습니다. 멤버 계정에 대한 루트 액세스를 중앙에서 관리한 후 루트 사용자 암호, 액세스 키 및 서명 인증서를 삭제하고 멤버 계정에 대한 다중 인증(MFA)을 비활성화할 수 있습니다. 중앙 관리형 루트 액세스로 생성된 새 계정에는 기본적으로 루트 사용자 자격 증명이 없습니다. 멤버 계정은 루트 사용자로 로그인하거나 루트 사용자의 암호 복구를 수행할 수 없습니다.

AWS Control Tower는 여러 계정을 설정하고 관리하는 간소화된 방법을 제공합니다. 조직의 계정 AWS 설정을 자동화하고, 프로비저닝을 자동화하고, 제어(예방 및 탐지 제어 포함)를 적용하고, 가시성을 위한 대시보드를 제공합니다. 추가 IAM 관리 정책인 권한 경계는 특정 IAM 보안 주체(사용자 또는 역할)에 연결되며 자격 증명 기반 정책이 IAM 보안 주체에 부여할 수 있는 최대 권한을 설정합니다.

AWS Organizations 는 모든 계정에 AWS 서비스 적용되는를 구성하는 데 도움이 됩니다. 예를 들어 CloudTrail을 사용하여 AWS 조직 전체에서 수행된 모든 작업에 대한 중앙 로깅을 구성하고 멤버 계정이 로깅을 비활성화하지 못하도록 할 수 있습니다. 또한를 사용하여 정의한 규칙에 대한 데이터를 중앙에서 집계할 수 AWS Config있으므로 워크로드의 규정 준수를 감사하고 변경 사항에 신속하게 대응할 수 있습니다. AWS CloudFormation StackSets를 사용하여 AWS 조직의 계정 및 OUs에서 CloudFormation 스택을 중앙에서 관리할 수 있으므로 보안 요구 사항에 맞게 새 계정을 자동으로 프로비저닝할 수 있습니다.

의 기본 구성은 SCPs 거부 목록으로 사용할 수 있도록 AWS Organizations 지원합니다. 거부 목록 전략을 사용하면 멤버 계정 관리자는 특정 서비스 또는 작업 세트를 거부하는 SCP를 생성하고 연결할 때까지 모든 서비스 및 작업을 위임할 수 있습니다. 거부 문은가 새 서비스를 AWS 추가할 때 업데이트할 필요가 없으므로 허용 목록보다 유지 관리가 적게 필요합니다. 거부 문은 일반적으로 문자 길이가 짧기 때문에 SCPs의 최대 크기 이내로 유지하는 것이 더 쉽습니다. `Effect` 요소의 값이 `Deny`인 문에서는 특정 리소스에 대한 액세스를 제한하거나 SCP가 효력을 발휘하는 조건을 정의할 수도 있습니다. 반대로 SCP의 `Allow` 문은 모든 리소스("*")에 적용되며 조건에 의해 제한될 수 없습니다. 자세한 내용과 예제는 AWS Organizations 설명서의 SCPs 사용을 위한 전략을 참조하세요.

설계 고려 사항

- 또는 SCPs 허용 목록으로 사용하려면 AWS 관리형 `FullAWSAccess` SCP를 허용하려는 서비스 및 작업만 명시적으로 허용하는 SCP로 바꿔야 합니다. 지정된 계정에 대해 권한을 활성화하려면 모든 SCP(루트에서 계정에 대한 직접 경로의 각 OU까지, 심지어 계정 자체에 연결됨)가 해당 권한을 허용해야 합니다. 이 모델은 본질적으로 더 제한적이며 규제가 높고 민감한 워크로드에 적합할 수 있습니다. 이 접근 방식을 사용하려면에서 OU까지의 경로에 있는 모든 IAM 서비스 또는 작업을 명시적으로 허용 AWS 계정 해야 합니다.
- 거부 목록과 허용 목록 전략의 조합을 사용하는 것이 가장 좋습니다. 허용 목록을 사용하여 AWS 조직 내에서 사용할 수 있도록 AWS 서비스 승인된 허용 목록을 정의하고 조직의 루트 AWS 에이 SCP를 연결합니다. 개발 환경당 허용되는 서비스 세트가 다른 경우 각 OU에 각 SCPs 연결합니다. 그런 다음 거부 목록을 사용하여 특정 IAM 작업을 명시적으로 거부하여 엔터프라이즈 가드레일을 정의할 수 있습니다.
- RCPs의 하위 집합에 대한 리소스에 적용됩니다 AWS 서비스. 자세한 내용은 설명서의 RCPs를 AWS 서비스 지원하는 목록을 참조하세요. AWS Organizations 의 기본 구성은 RCPs 거부 목록으로 사용할 수 있도록 AWS Organizations 지원합니다. 조직에서 RCPs 활성화하면 라는 AWS 관리형 정책`RCPFullAWSAccess`이 조직 루트, 모든 OU 및 조직의 모든 계정에 자동으로 연결됩니다. 이 정책은 분리할 수 없습니다. 이 기본 RCP를 사용하면 모든 보안 주체 및 작업에 대한 액세스 권한이 RCP 평가를 통과할 수 있습니다. 즉, RCPs 생성 및 연결을 시작할 때까지 기존 IAM 권한은 모두 그대로 작동합니다. 이 AWS 관리형 정책은 액세스 권한을 부여하지 않습니다. 그런 다음 새 RCPs 거부 문 목록으로 작성하여 조직의 리소스에 대한 액세스를 차단할 수 있습니다.

관리 계정, 신뢰할 수 있는 액세스 및 위임된 관리자

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

관리 계정(AWS 조직 관리 계정 또는 조직 관리 계정이라고도 함)은 고유하며 다른 모든 계정과 구별됩니다 AWS Organizations. 조직을 생성하는 계정입니다 AWS . 이 계정에서 AWS 조직에서 AWS 계정 를 생성하고, 조직에 다른 기존 계정을 AWS 초대하고(두 유형 모두 멤버 계정으로 간주), AWS 조직에서 계정을 제거하고, AWS 조직 내 루트, OUs 또는 계정에 IAM 정책을 적용할 수 있습니다.

관리 계정은 조직의 모든 멤버 계정에 영향을 미치는 SCPs, RCPs 및 서비스 배포(예: CloudTrail)를 통해 범용 보안 가드레일을 배포합니다 AWS . 관리 계정의 권한을 추가로 제한하기 위해 가능한 경우 보안 계정과 같은 다른 적절한 계정에 해당 권한을 위임할 수 있습니다.

관리 계정은 지급인 계정을 담당하며 멤버 계정에서 발생한 모든 요금을 지불해야 합니다. AWS 조직의 관리 계정은 전환할 수 없습니다. 는 한 번에 하나의 AWS 조직의 멤버일 AWS 계정 수 있습니다.

관리 계정이 보유한 영향의 기능과 범위 때문에이 계정에 대한 액세스를 제한하고 필요한 역할에만 권한을 부여하는 것이 좋습니다. 이를 지원하는 두 가지 기능은 신뢰할 수 있는 액세스와 위임된 관리자입니다. 신뢰할 수 있는 액세스를 사용하여 신뢰할 수 AWS 서비스 있는 서비스라고 하는 지정한가 사용자를 대신하여 AWS 조직 및 해당 계정에서 작업을 수행할 수 있도록 할 수 있습니다. 이 과정에는 신뢰할 수 있는 서비스에 대한 권한 부여가 포함되지만 IAM 사용자 또는 역할에 대한 권한에는 달리 영향을 미치지 않습니다. 신뢰할 수 있는 액세스를 사용하여 신뢰할 수 있는 서비스가 사용자를 대신하여 AWS 조직의 계정에 유지할 설정 및 구성 세부 정보를 지정할 수 있습니다. 예를 들어 AWS SRA의 조직 관리 계정 섹션에서는 조직의 모든 계정에 AWS CloudTrail 조직 추적을 생성할 수 있는 신뢰할 수 있는 액세스 권한을 CloudTrail 서비스에 부여하는 방법을 설명합니다.

일부는에서 위임된 관리자 기능을 AWS 서비스 지원합니다 AWS Organizations. 이 기능을 사용하면 호환되는 서비스가 AWS 조직의 AWS멤버 계정을 해당 서비스의 AWS 조직 계정에 대한 관리자로 등록할 수 있습니다. 이 기능은 엔터프라이즈 내 여러 팀이 책임에 따라 별도의 계정을 사용하여 환경 AWS 서비스 전체에서를 관리할 수 있는 유연성을 제공합니다. 현재 위임된 관리자를 지원하는 AWS SRA의 AWS 보안 서비스에는 IAM Identity Center, AWS Config, AWS Firewall Manager, Amazon GuardDuty, IAM Access Analyzer, Amazon Macie, AWS Security Hub Cloud Security Posture Management(AWS Security Hub CSPM), Amazon Detective AWS Audit Manager, Amazon Inspector 및가 포함됩니다 AWS Systems Manager. 위임된 관리자 기능의 사용은 AWS SRA에서 모범 사례로 강조되며 보안 관련 서비스의 관리를 보안 도구 계정에 위임합니다.

전용 계정 구조

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

AWS 계정 는 리소스에 대한 보안, 액세스 및 결제 경계를 제공하며 리소스 독립성과 격리를 달성할 수 있습니다 AWS . 기본적으로 계정 간에는 액세스할 수 없습니다.

OU 및 계정 구조를 설계할 때는 보안 및 인프라를 염두에 두고 시작하십시오. 이러한 특정 함수에 대한 기본 OUs 세트를 인프라 및 보안 OUs로 분할하여 생성하는 것이 좋습니다. 이러한 OU 및 계정 권장 사항은 및 다중 계정 구조 설계에 대한 보다 광범위 AWS Organizations 하고 포괄적인 지침의 하위 집

합을 캡처합니다. 전체 권장 사항은 설명서의 여러 계정을 사용하여 AWS 환경 구성 및를 사용한 조직 단위 모범 사례를 AWS Organizations 참조하세요. AWS

AWS SRA는 다음 계정을 활용하여 효과적인 보안 작업을 수행합니다 AWS. 이러한 전용 계정은 업무 분리를 보장하고, 애플리케이션 및 데이터의 다양한 민감한 요소에 대한 다양한 거버넌스 및 액세스 정책을 지원하며, 보안 이벤트의 영향을 완화하는 데 도움이 됩니다. 이어지는 토론에서는 프로덕션(생산) 계정과 관련 워크로드에 중점을 둡니다. 소프트웨어 개발 수명 주기(SDLC) 계정(대개 개발 및 테스트 계정이라고 함)은 결과물을 스테이징하기 위한 것이며 프로덕션 계정과 다른 보안 정책 세트로 운영될 수 있습니다.

Account	OU	보안 역할
관리	—	모든 및 계정의 중앙 거버넌스 AWS 리전 및 관리. 조직의 루트를 호스팅 AWS 계정 하는 입니다 AWS .
보안 도구	보안	광범위하게 적용되는 보안 서비스(예: GuardDuty, Security Hub CSPM, Audit Manager, Detective, Amazon Inspector 및 AWS Config) 운영 AWS 계정, 보안 알림 및 대응 모니터링 및 자동화 AWS 계정 를 위한 전용 서비스입니다. (에서 보안 OU 아래에 있는 계정의 AWS Control Tower기본 이름은 감사 계정입니다.)
로그 보관	보안	AWS 리전 모든 및 AWS 계정에 대한 모든 로깅 및 백업을 수집하고 보관하는 데 전용입니다 AWS 계정. 이는 변경할 수 없는 스토리지로 설계되어야 합니다.
Network	인프라	애플리케이션과 더 광범위한 인터넷 간의 게이트웨이입니

		다. 네트워크 계정은 개별 애플리케이션 워크로드, 보안 및 기타 인프라에서 광범위한 네트워킹 서비스, 구성 및 작업을 격리합니다.
공유 서비스	인프라	이 계정은 여러 애플리케이션과 팀이 결과를 제공하는 데 사용하는 서비스를 지원합니다. 예를 들어 Identity Center 디렉터리 서비스(Active Directory), 메시징 서비스 및 메타데이터 서비스가 있습니다.
애플리케이션	워크로드	AWS 계정 는 AWS 조직의 애플리케이션을 호스팅하고 워크로드를 수행합니다. (이를 워크로드 계정이라고도 합니다.) 팀에 매핑되는 대신 소프트웨어 서비스를 격리하기 위해 애플리케이션 계정을 생성해야 합니다. 이렇게 하면 배포된 애플리케이션이 조직 변화에 대한 복원력을 높일 수 있습니다.

AWS AWS SRA의 조직 및 계정 구조

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

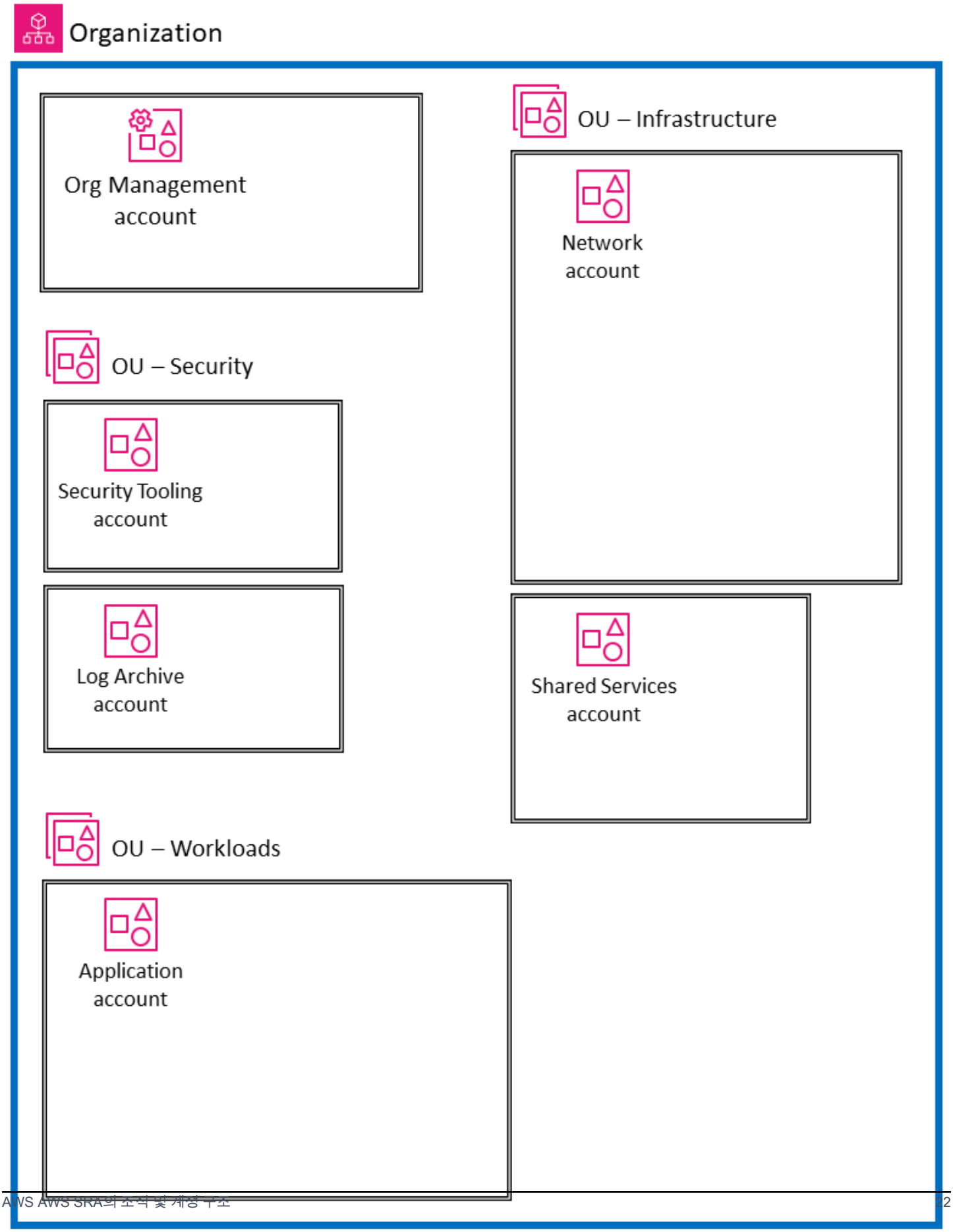
다음 다이어그램은 특정 서비스를 표시하지 않고 AWS SRA의 상위 수준 구조를 캡처합니다. 이전 섹션에서 설명한 전용 계정 구조를 반영하며, 아키텍처의 기본 구성 요소에 대한 논의 방향을 잡기 위해 여기에 다이어그램을 포함합니다.

- 다이어그램에 표시된 모든 계정은 단일 AWS 조직의 일부입니다.
- 다이어그램의 왼쪽 상단에는 AWS 조직을 생성하는 데 사용되는 조직 관리 계정이 있습니다.

- 조직 관리 계정 아래에는 두 개의 특정 계정이 있는 보안 OU가 있습니다. 하나는 보안 도구용이고 다른 하나는 로그 아카이브용입니다.
- 오른쪽에는 네트워크 계정과 공유 서비스 계정이 있는 인프라 OU가 있습니다.
- 다이어그램 하단에는 엔터프라이즈 애플리케이션을 포함하는 애플리케이션 계정과 연결된 워크로드 OU가 있습니다.

이 지침에서 모든 계정은 단일에서 작동하는 프로덕션(prod) 계정으로 간주됩니다 AWS 리전. 대부분 AWS 서비스 (글로벌 서비스 제외)은 리전별로 범위가 지정되므로 서비스에 대한 제어 및 데이터 영역이 각각 독립적으로 존재합니다 AWS 리전. 따라서 전체 AWS 환경에 대한 적용 범위를 보장하려면 사용 AWS 리전 하려는 모든에이 아키텍처를 복제해야 합니다. 특정에 워크로드가 없는 경우 SCPs 사용하거나 로깅 및 모니터링 메커니즘을 사용하여 리전을 비활성화 AWS 리전해야 합니다. Security Hub CSPM을 사용하여 여러에서 단일 집계 리전으로 조사 결과 및 보안 점수를 집계 AWS 리전 하여 중앙 집중식 가시성을 확보할 수 있습니다.

대규모 계정 집합으로 AWS 조직을 호스팅할 때는 계정 배포 및 계정 거버넌스를 용이하게 하는 오케스트레이션 계층을 사용하는 것이 좋습니다.는 AWS 다중 계정 환경을 설정하고 관리하는 간단한 방법을 AWS Control Tower 제공합니다. GitHub 리포지토리의 AWS SRA 코드 샘플은 Customizations for AWS Control Tower (CfCT) 솔루션을 사용하여 AWS SRA 권장 구조를 배포하는 방법을 보여줍니다.

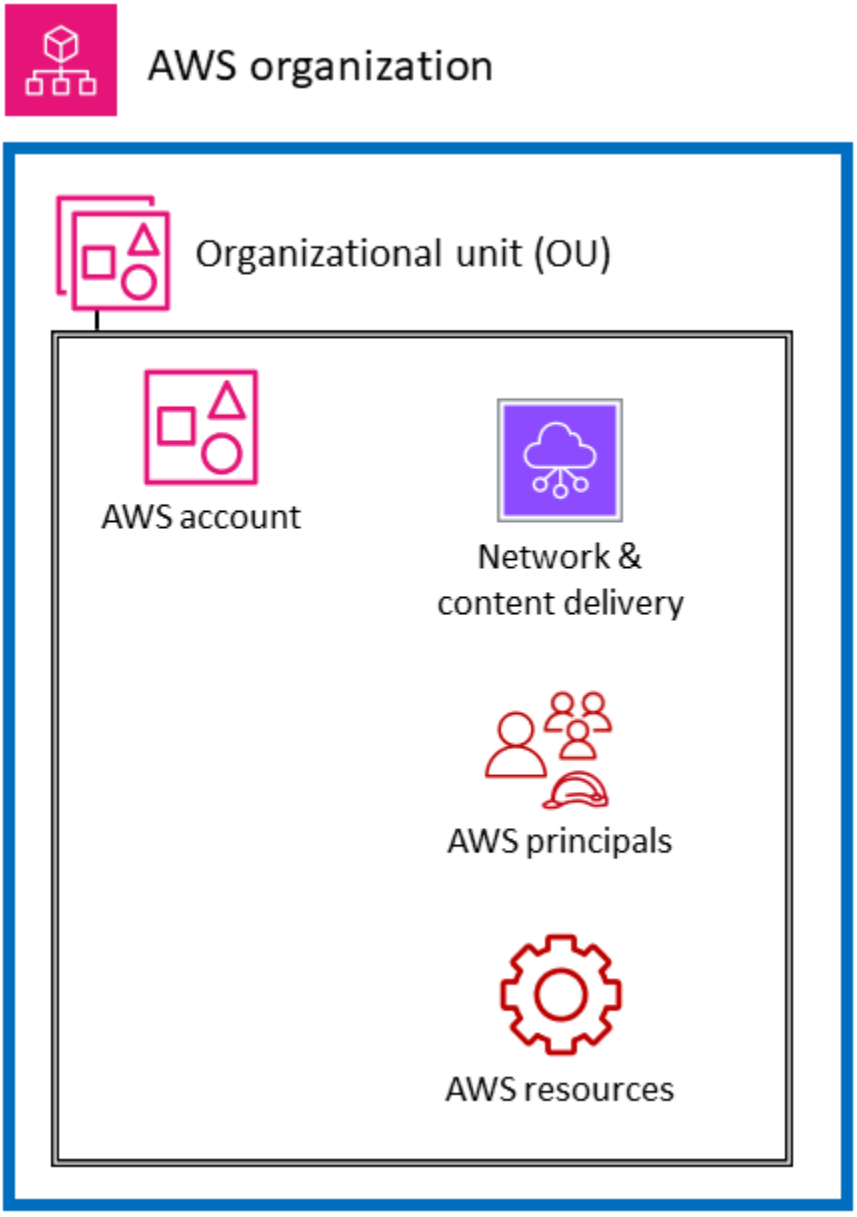

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

AWS 조직 전체에 보안 서비스 적용

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

이전 섹션에서 설명한 대로 고객은 전체 보안 서비스 세트를 AWS 고려하고 전략적으로 구성할 수 있는 추가 방법을 찾고 있습니다. 오늘날 가장 일반적인 조직 접근 방식은 각 서비스의 기능에 따라 기본 함수별로 보안 서비스를 그룹화하는 것입니다. AWS CAF의 보안 관점에는 자격 증명 및 액세스 관리, 인프라 보호, 데이터 보호, 위협 탐지 등 9가지 기능 기능이 나열되어 있습니다. 이러한 기능 역량 AWS 서비스 과 일치시키는 것은 각 영역에서 구현 결정을 내리는 실용적인 방법입니다. 예를 들어 ID 및 액세스 관리를 살펴볼 때 IAM 및 IAM Identity Center는 고려해야 할 서비스입니다. 위협 탐지 접근 방식을 설계할 때 GuardDuty가 첫 번째 고려 사항일 수 있습니다.

이 기능 보기를 보완하기 위해 교차 절단 구조 보기를 사용하여 보안을 볼 수도 있습니다. 즉, "자격 증명, 논리적 액세스 또는 위협 탐지 메커니즘을 제어하고 보호하려면 어떤 방법을 사용해야 AWS 서비스 합니까?"라고 묻는 것 외에도 "전체 AWS 조직에 어떤 방법을 적용 AWS 서비스 해야 합니까? 애플리케이션의 코어에서 Amazon EC2 인스턴스를 보호하기 위해 마련해야 하는 방어 계층은 무엇입니까?" 이 보기에서는 AWS 서비스 및 기능을 AWS 환경의 계층에 매핑합니다. 일부 서비스 및 기능은 전체 AWS 조직에서 제어를 구현하는 데 적합합니다. 예를 들어 Amazon S3 버킷에 대한 퍼블릭 액세스를 차단하는 것은이 계층에서 특정 제어입니다. 개별 계정 설정의 일부가 아닌 루트 조직에서 수행하는 것이 좋습니다. 다른 서비스 및 기능은 내의 개별 리소스를 보호하는 데 가장 적합합니다 AWS 계정. 프라이빗 TLS 인증서가 필요한 계정 내에서 하위 인증 기관(CA)을 구현하는 것이이 범주의 예입니다. 또 다른 똑같이 중요한 그룹화는 AWS 인프라의 가상 네트워크 계층에 영향을 미치는 서비스로 구성됩니다. 다음 다이어그램은 일반적인 AWS 환경의 6개 계층, 즉 AWS 조직, 조직 단위(OU), 계정, 네트워크 인프라, 보안 주체 및 리소스를 보여줍니다.



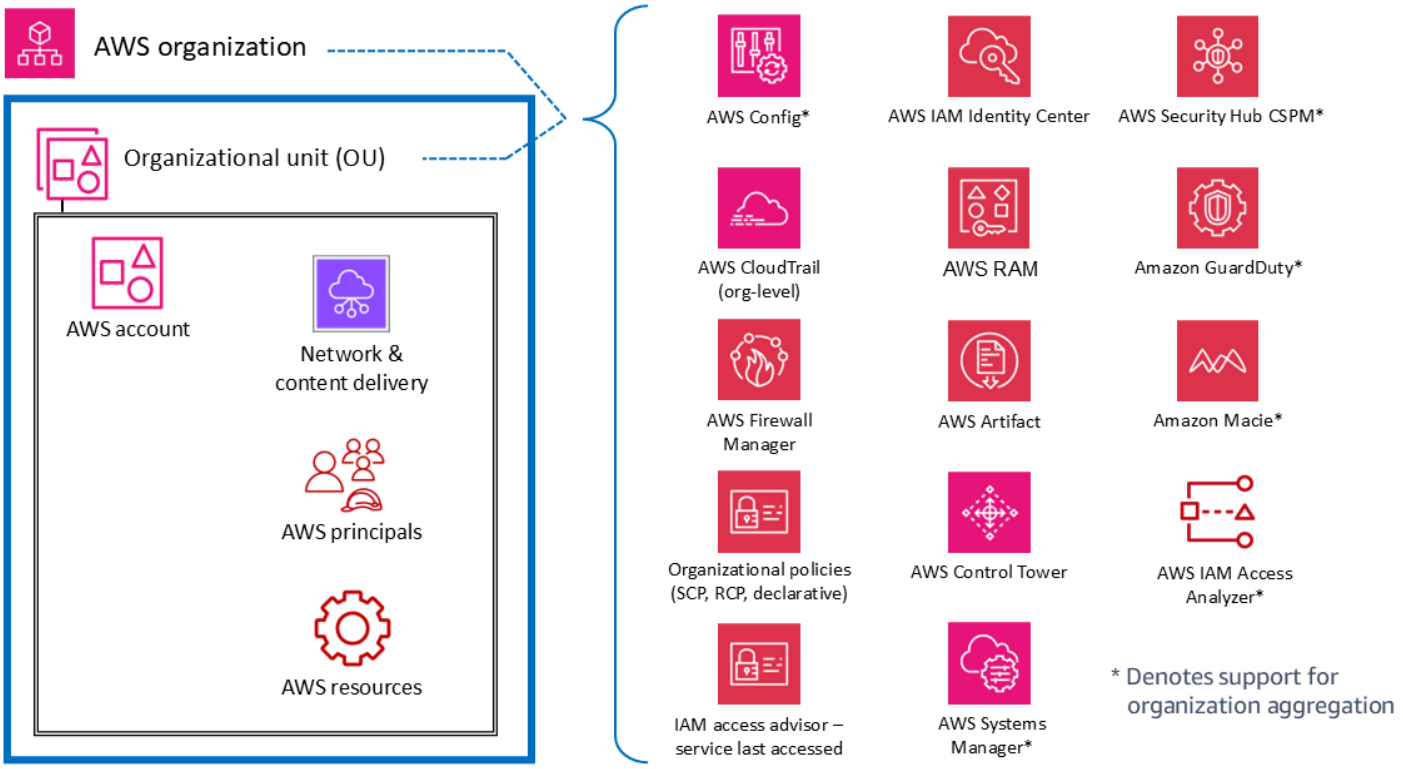
각 계층의 제어 및 보호를 포함하여 이러한 구조적 컨텍스트의 서비스를 이해하면 AWS 환경 전체에서 defense-in-depth 전략을 계획하고 구현하는 데 도움이 됩니다. 이 관점에서는 위에서 아래로(예: "전체 AWS 조직에 보안 제어를 구현하는 데 어떤 서비스를 사용합니까?")와 아래에서 위로(예: "이 EC2 인스턴스에 대한 제어를 관리하는 서비스는 무엇입니까?") 질문에 모두 답할 수 있습니다. 이 섹션에서는 AWS 환경의 요소를 살펴보고 관련 보안 서비스 및 기능을 식별합니다. 물론 일부 에는 광범위한 기능 세트 AWS 서비스 가 있으며 여러 보안 목표를 지원합니다. 이러한 서비스는 AWS 환경의 여러 요소를 지원할 수 있습니다.

명확성을 위해 일부 서비스가 명시된 목표에 어떻게 부합하는지에 대한 간략한 설명을 제공합니다. 다음 섹션에서는 각 섹션 내의 개별 서비스에 대한 추가 설명을 제공합니다 AWS 계정.

조직 전체 또는 여러 계정

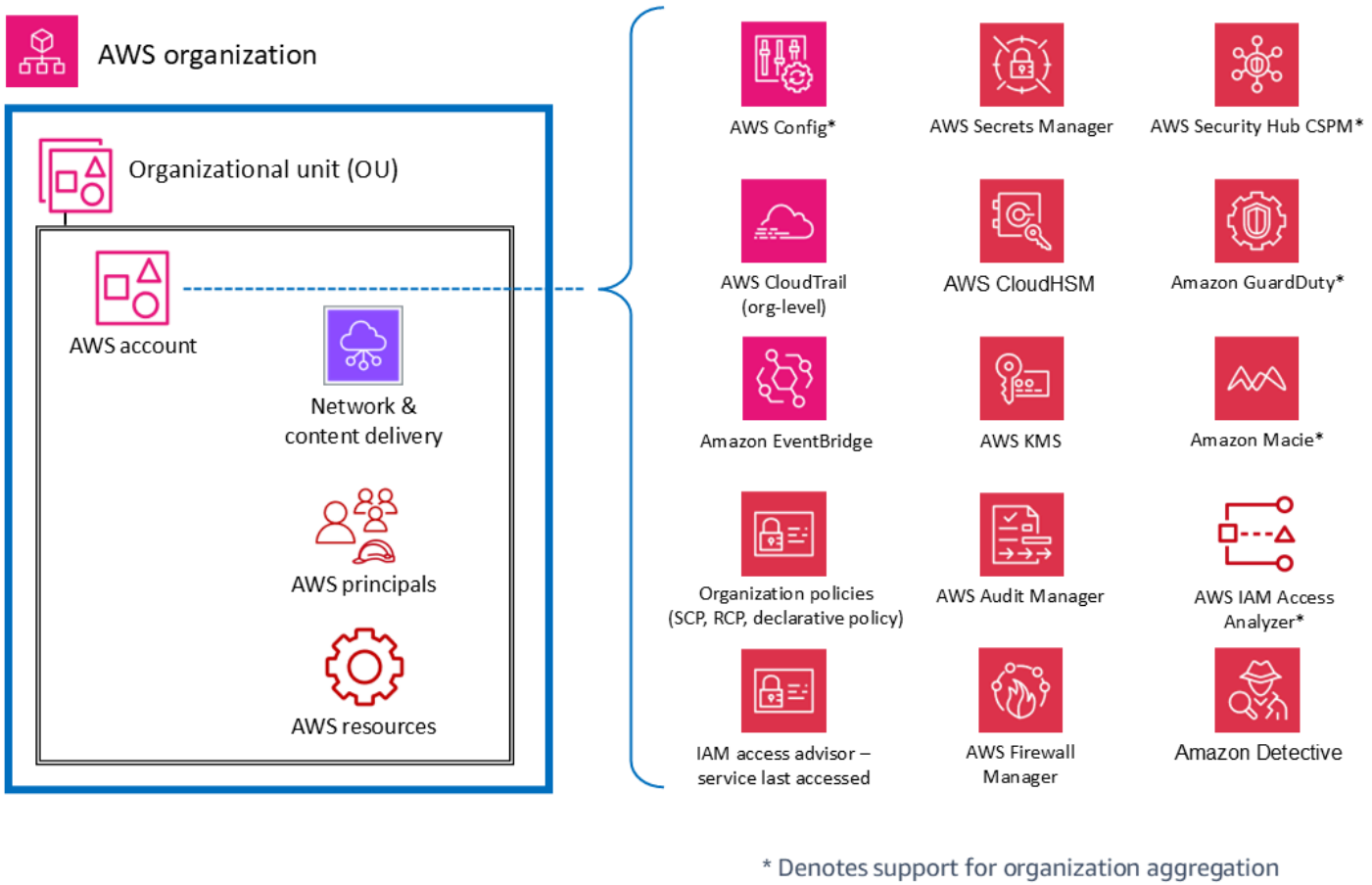
최상위 수준에는 AWS 조직의 여러 계정(전체 조직 또는 특정 OU 포함)에 거버넌스 및 제어 기능 또는 가드레일을 적용하도록 설계된 AWS 서비스 및 기능이 있습니다. OUs 서비스 제어 정책(SCPs) 및 리소스 제어 정책(RCPs)은 예방적 AWS 조직 전체 가드레일을 제공하는 IAM 기능의 좋은 예입니다. AWS Organizations 또한는 AWS 서비스 대규모로에 대한 기준 구성을 중앙에서 정의하고 적용하는 선언적 정책을 제공합니다. 또 다른 예는 해당 조직의 모든에 대한 모든 이벤트를 로깅하는 조직 추적 AWS 계정 을 통해 모니터링을 제공하는 CloudTrail입니다. AWS 이 포괄적인 추적은 각 계정에서 생성될 수 있는 개별 추적과 구별됩니다. 세 번째 예는 AWS 조직의 모든 계정에서 여러 리소스를 구성, 적용 및 관리하는 데 사용할 수 있는 AWS WAF 규칙 AWS Firewall Manager, AWS WAF 클래식 규칙, AWS Shield Advanced 보호, Amazon Virtual Private Cloud(Amazon VPC) 보안 그룹, AWS Network Firewall 정책 및 Amazon Route 53 Resolver DNS 방화벽 정책입니다.

다음 다이어그램에서 별표(*)로 표시된 서비스는 조직 전체 및 계정 중심의 이중 범위로 작동합니다. 이러한 서비스는 기본적으로 개별 계정 내에서 보안을 모니터링하거나 제어하는 데 도움이 됩니다. 그러나 중앙 집중식 가시성 및 관리를 위해 여러 계정의 결과를 조직 전체 계정으로 집계하는 기능도 지원합니다. 명확성을 위해 전체 OU AWS 계정또는 AWS 조직에 적용되는 SCPs를 고려하세요. 반대로 계정 수준(개별 조사 결과가 생성되는 곳)과 결과를 집계하여 보고 관리할 수 있는 AWS 조직 수준(위임된 관리자 기능 사용) 모두에서 GuardDuty를 구성하고 관리할 수 있습니다.



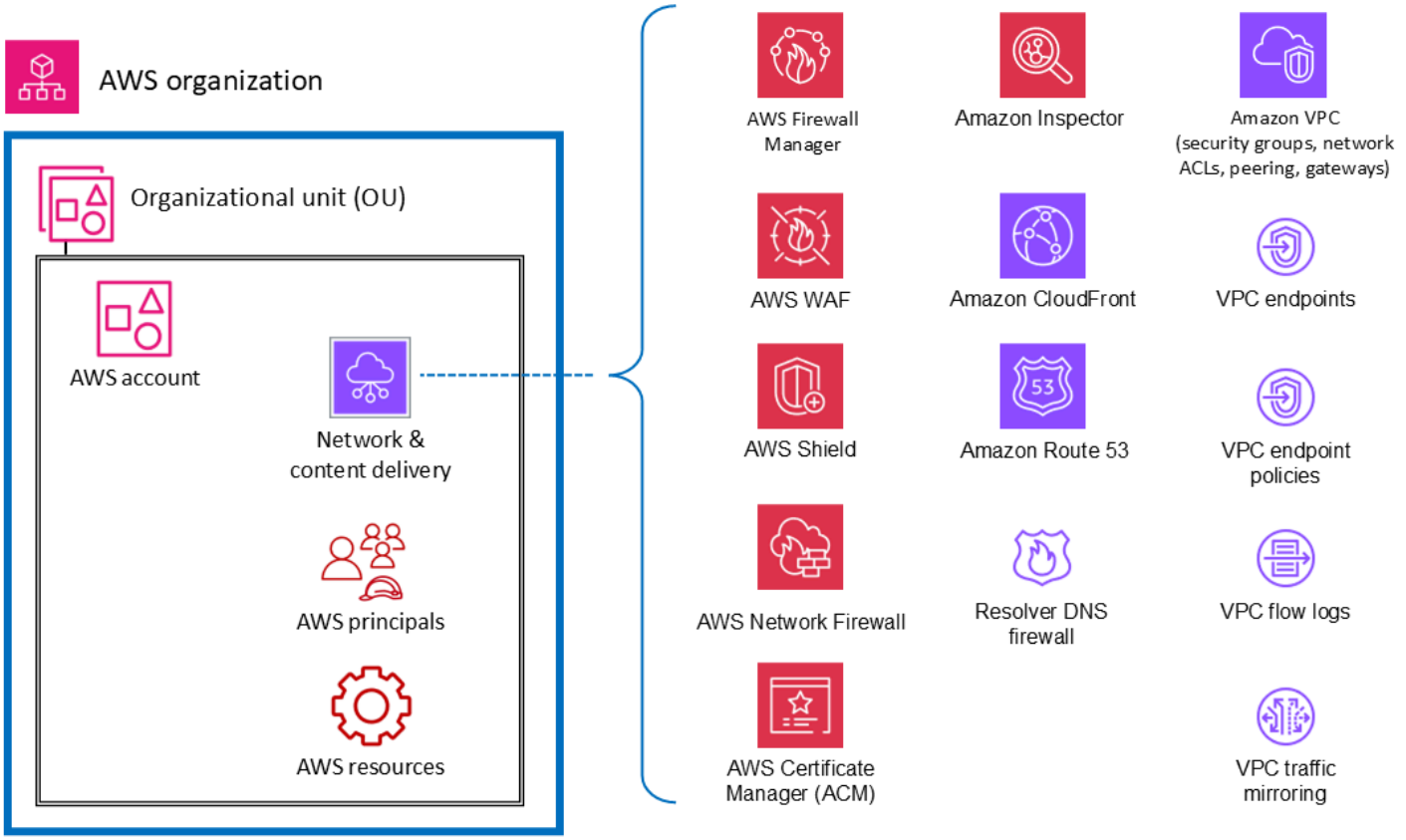
AWS 계정

OUs 내에는 내의 여러 유형의 요소를 보호하는 데 도움이 되는 서비스가 있습니다 AWS 계정. 예를 들어 AWS Secrets Manager 는 일반적으로 특정 계정에서 관리되며 리소스(예: 데이터베이스 자격 증명 또는 인증 정보), 애플리케이션 및 해당 계정 AWS 서비스 의 리소스를 보호합니다. IAM Access Analyzer는 외부의 보안 주체가 지정된 리소스에 액세스할 수 있을 때 결과를 생성하도록 구성할 수 있습니다 AWS 계정. 이전 단원에서 언급했듯이 이러한 서비스 중 대부분은 내에서 구성하고 관리할 수도 AWS Organizations있으므로 여러 계정에서 관리할 수 있습니다. 이러한 서비스는 다이어그램에 별표(*)로 표시됩니다. 또한 여러 계정의 결과를 더 쉽게 집계하고 단일 계정으로 전달할 수 있습니다. 이를 통해 개별 애플리케이션 팀은 워크로드와 관련된 보안 요구 사항을 관리할 수 있는 유연성과 가시성을 제공하면서 중앙 집중식 보안 팀에 거버넌스와 가시성을 제공할 수 있습니다. GuardDuty는 이러한 서비스의 예입니다. GuardDuty는 단일 계정과 연결된 리소스 및 활동을 모니터링하며, 여러 멤버 계정(예: AWS 조직의 모든 계정)의 GuardDuty 조사 결과는 위임된 관리자 계정에서 수집, 확인 및 관리할 수 있습니다.



가상 네트워크, 컴퓨팅 및 콘텐츠 전송

네트워크 액세스는 보안에 매우 중요하며 컴퓨팅 인프라는 많은 AWS 워크로드의 기본 구성 요소이므로 이러한 리소스 전용 AWS 보안 서비스와 기능이 많이 있습니다. 예를 들어 Amazon Inspector는 AWS 워크로드의 취약성을 지속적으로 검사하는 취약성 관리 서비스입니다. 이러한 스캔에는 환경의 Amazon EC2 인스턴스에 허용되는 네트워크 경로가 있음을 나타내는 네트워크 연결성 검사가 포함됩니다. Amazon VPC를 사용하면 AWS 리소스를 시작할 수 있는 가상 네트워크를 정의할 수 있습니다. 이 가상 네트워크는 기존 네트워크와 매우 유사하며 다양한 기능과 이점을 포함합니다. VPC 엔드포인트를 사용하면 인터넷 경로 AWS PrivateLink 없이 VPC를 지원되는 AWS 서비스 및에서 제공하는 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 다음 다이어그램은 네트워크, 컴퓨팅 및 콘텐츠 전송 인프라에 초점을 맞춘 보안 서비스를 보여줍니다.



보안 주체 및 리소스

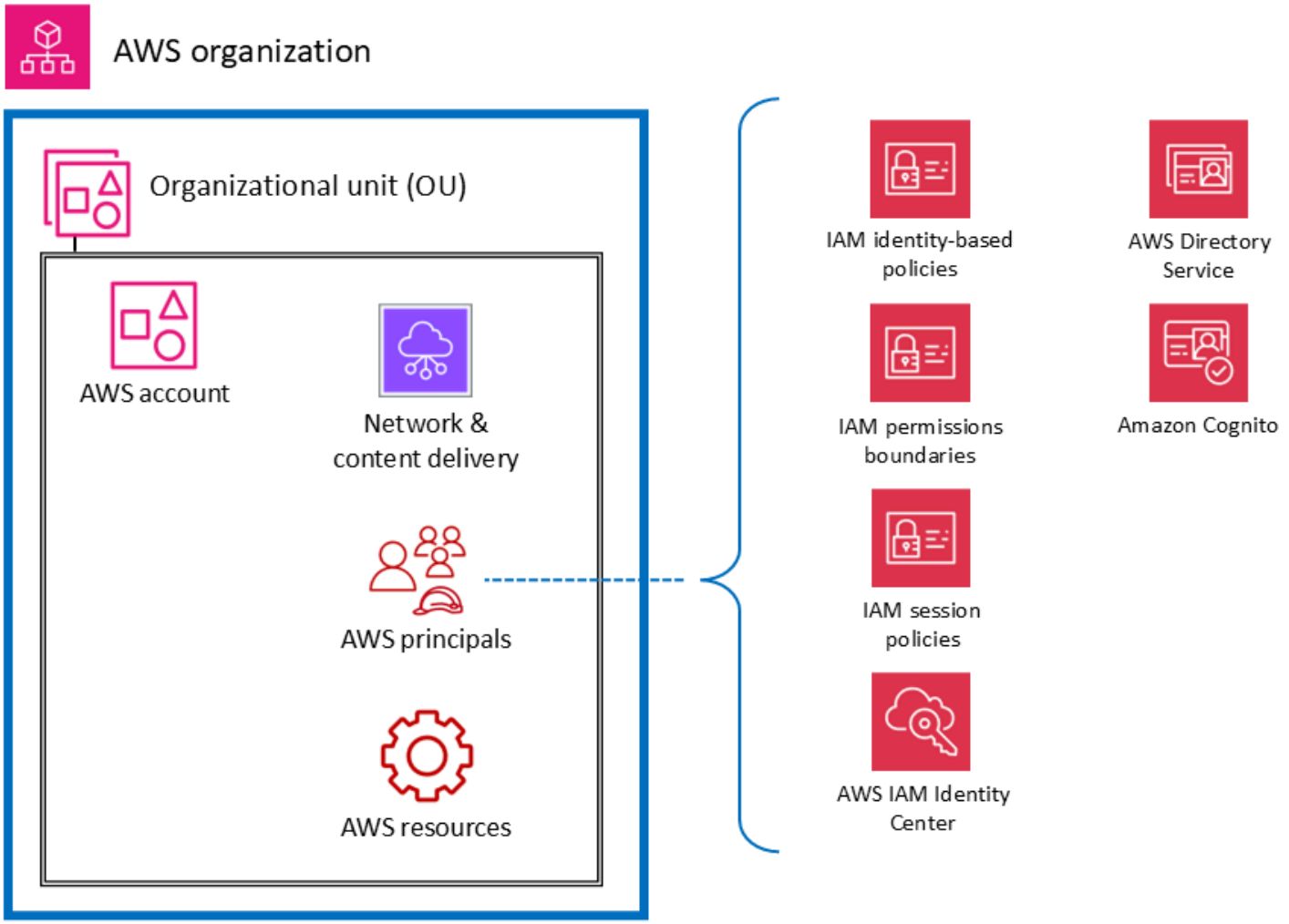
AWS 보안 주체 및 AWS 리소스(IAM 정책과 함께)는 자격 증명 및 액세스 관리의 기본 요소입니다 AWS. 의 인증된 보안 주체는 작업을 수행하고 AWS 리소스에 액세스할 AWS 수 있습니다. 보안 주체는 AWS 계정 루트 사용자 및 IAM 사용자로 인증하거나 역할을 수임하여 인증할 수 있습니다.

> **Note**
>
> AWS 루트 사용자 계정과 연결된 영구 API 키를 생성하지 마십시오. 루트 사용자 계정에 대한 액세스는 루트 사용자가 필요한 작업으로만 제한한 다음 엄격한 예외 및 승인 프로세스를 통해서만 제한해야 합니다. 계정의 루트 사용자를 보호하는 모범 사례는 IAM 설명서를 참조하세요.

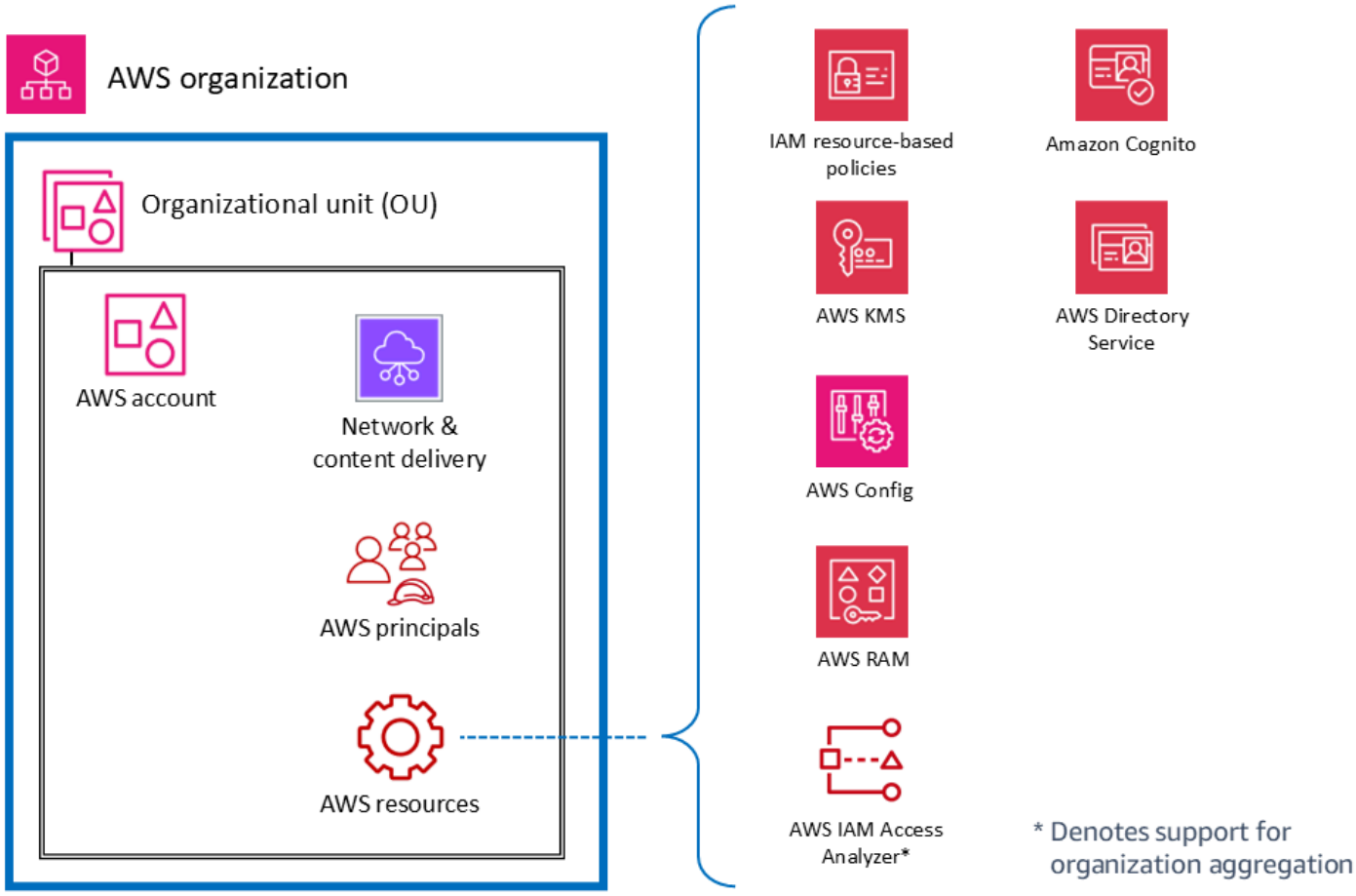
AWS 리소스는 작업할 수 AWS 서비스 있는 내에 있는 객체입니다. 예를 들어 EC2 인스턴스, CloudFormation 스택, Amazon Simple Notification Service(Amazon SNS) 주제 및 S3 버킷이 있습니다. IAM 정책은 IAM 보안 주체(사용자, 그룹 또는 역할) 또는 AWS 리소스와 연결될 때 권한을 정의하는 객체입니다. 자격 증명 기반 정책은 보안 주체(역할, 사용자 및 사용자 그룹)에 연결하여 보안 주체가 수행할 수 있는 작업, 리소스 및 조건을 제어하는 정책 문서입니다. 리소스 기반 정책은 S3 버킷과 같은 리소스에 연결하는 정책 문서입니다. 이러한 정책은 지정된 보안 주체에게 해당 리소스에 대해 특정 작업을 수행하고 해당 권한에 대한 조건을 정의할 수 있는 권한을 부여합니다. 리소스 기반 정책은 인라인 정책입니다. IAM 리소스 섹션에서는 IAM 정책의 유형과 사용 방법을 자세히 살펴봅니다.

이 논의에서 사물을 단순하게 유지하기 위해 계정 보안 주체에서 운영하거나 계정 보안 주체에 적용하는 주요 목적이 있는 IAM 보안 주체에 대한 AWS 보안 서비스 및 기능을 나열합니다. IAM 권한 정책의 유연성과 광범위한 효과를 인정하면서 이러한 단순성을 유지합니다. 정책의 단일 문은 여러 유형의 AWS 엔터티에 영향을 미칠 수 있습니다. 예를 들어 IAM 자격 증명 기반 정책이 IAM 보안 주체와 연결되어 있고 해당 보안 주체에 대한 권한(허용, 거부)을 정의하더라도이 정책은 지정된 작업, 리소스 및 조건에 대한 권한도 암시적으로 정의합니다. 이러한 방식으로 자격 증명 기반 정책은 리소스에 대한 권한을 정의하는 데 중요한 요소일 수 있습니다.

다음 다이어그램은 보안 주체에 대한 AWS AWS 보안 서비스 및 기능을 보여줍니다. 자격 증명 기반 정책은 IAM 사용자, 그룹 또는 역할에 연결됩니다. 이러한 정책으로 자격 증명이 수행할 수 있는 작업(권한)을 지정할 수 있습니다. IAM 세션 정책은 사용자가 역할을 수임할 때 세션에서 전달하는 인라인 권한 정책 입니다. 정책을 직접 전달하거나 자격 증명 이 연동될 때 정책을 삽입하도록 자격 증명 AWS 브로커를 구성할 수 있습니다. 이렇게 하면 여러 사용자가 동일한 역할을 수임하면서도 고유한 세션 권한을 가질 수 있으므로 관리자가 생성해야 하는 역할 수를 줄일 수 있습니다. IAM Identity Center 서비스는 AWS Organizations 및 AWS API 작업과 통합되며 AWS 계정 에서 SSO 액세스 및 사용자 권한을 관리하는 데 도움이 됩니다 AWS Organizations.



다음 다이어그램은 계정 리소스에 대한 서비스 및 기능을 보여줍니다. 리소스 기반 정책은 리소스에 연결됩니다. 예를 들어 리소스 기반 정책을 S3 버킷, Amazon Simple Queue Service(Amazon SQS) 대기열, VPC 엔드포인트 및 AWS KMS 암호화 키에 연결할 수 있습니다. 리소스 기반 정책을 사용하여 리소스에 액세스할 수 있는 사용자와 리소스에 대해 수행할 수 있는 작업을 지정할 수 있습니다. S3 버킷 정책, AWS KMS 키 정책 및 VPC 엔드포인트 정책은 리소스 기반 정책의 유형입니다. IAM Access Analyzer를 사용하면 외부 엔터티와 공유되는 조직 및 계정 내 리소스(예: S3 버킷 또는 IAM 역할)를 식별할 수 있습니다. 이를 통해 리소스 및 데이터에 대한 의도하지 않은 액세스를 식별할 수 있으며, 이는 보안 위험입니다. 이를 AWS Config 통해에서 지원되는 AWS 리소스의 구성을 평가, 감사 및 평가할 수 있습니다 AWS 계정. AWS 리소스 구성을 AWS Config 지속적으로 모니터링 및 기록하고 기록된 구성을 원하는 구성과 비교하여 자동으로 평가합니다.


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

AWS 보안 참조 아키텍처

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

다음 다이어그램은 AWS SRA를 보여줍니다. 이 아키텍처 다이어그램은 모든 AWS 보안 관련 서비스를 통합합니다. 단일 페이지에 들어갈 수 있는 간단한 3계층 웹 아키텍처를 기반으로 구축되었습니다. 이러한 워크로드에는 사용자가 애플리케이션 계층에 연결하고 상호 작용하는 웹 계층이 있으며,이 계층은 애플리케이션의 실제 비즈니스 로직인 사용자로부터 입력을 받고, 일부 계산을 수행하고, 출력을 생성하는 작업을 처리합니다. 애플리케이션 계층은 데이터 계층에서 정보를 저장하고 검색합니다. 이 아키텍처는 의도적으로 모듈식이며 많은 최신 웹 애플리케이션에 높은 수준의 추상화를 제공합니다.

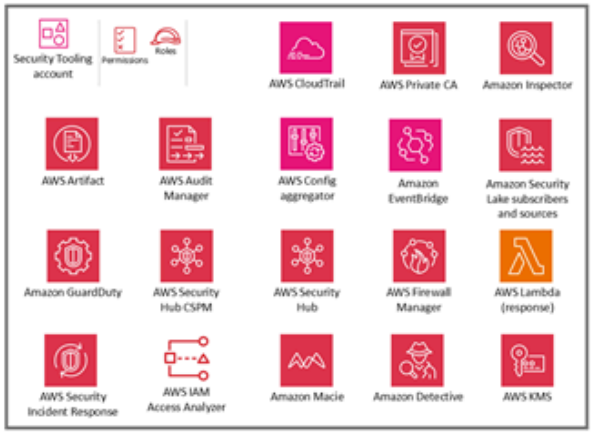
아키텍처 다이어그램

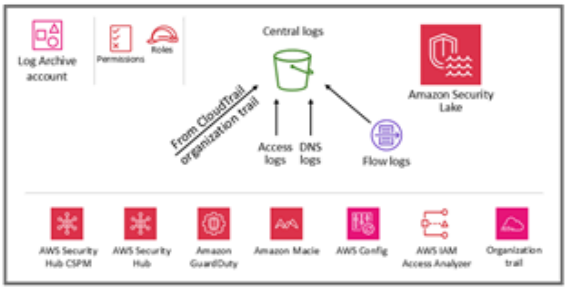
비즈니스 요구 사항에 따라이 가이드의 참조 아키텍처 다이어그램을 사용자 지정하려면 다음 .zip 파일을 다운로드하고 내용을 추출할 수 있습니다.

다이어그램 소스 파일 다운로드(Microsoft PowerPoint 형식)

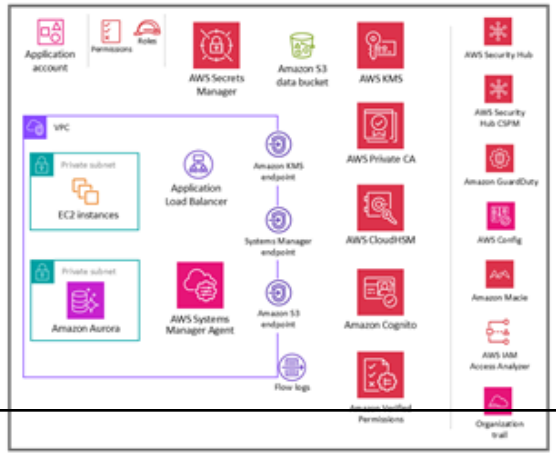
Organization

OU – Security

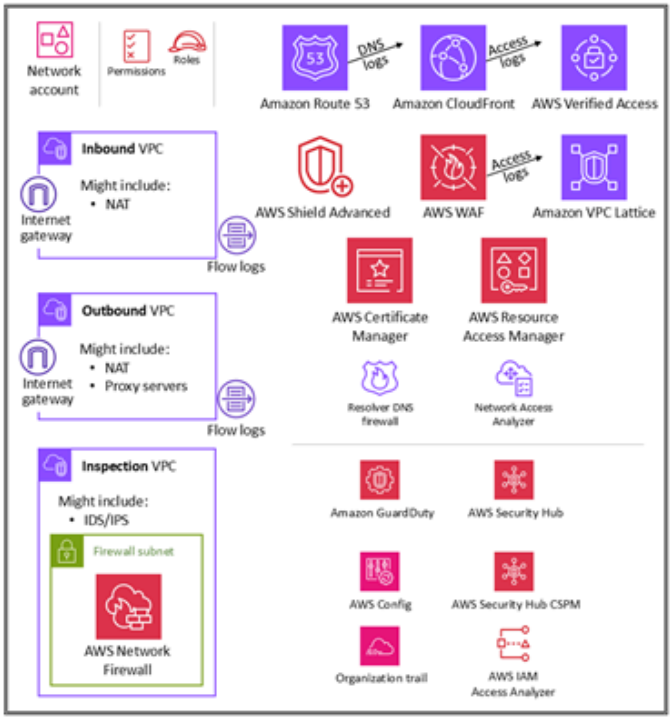


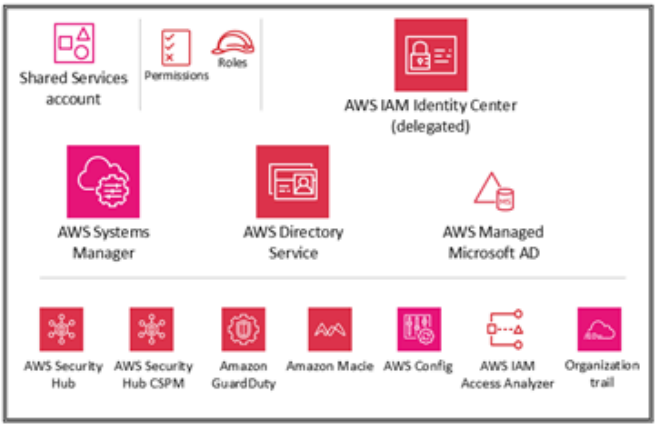


OU – Workloads



OU – Infrastructure





이 참조 아키텍처의 경우 실제 웹 애플리케이션과 데이터 계층은 각각 Amazon EC2 인스턴스와 Amazon Aurora 데이터베이스를 통해 가능한 한 간단하게 의도적으로 표현됩니다. 대부분의 아키텍처 다이어그램은 웹, 애플리케이션 및 데이터 계층에 초점을 맞추고 심층적으로 분석합니다. 가독성을 위해 보안 제어를 생략하는 경우가 많습니다. 이 다이어그램은 가능한 경우 보안을 보여주도록 강조하는 를 뒤집고, 애플리케이션 및 데이터 계층을 필요에 따라 단순하게 유지하여 보안 기능을 의미 있게 보여줍니다.

AWS SRA에는 게시 시점에 사용할 수 있는 모든 AWS 보안 관련 서비스가 포함되어 있습니다. (문서 기록 참조) 그러나 모든 워크로드 또는 환경이 고유한 위협 노출을 기반으로 모든 보안 서비스를 배포해야 하는 것은 아닙니다. 당사의 목표는 이러한 서비스가 아키텍처적으로 어떻게 함께 적용되는지에 대한 설명을 포함하여 다양한 옵션에 대한 참조를 제공하여 비즈니스가 위험을 기반으로 인프라, 워크로드 및 보안 요구 사항에 가장 적합한 결정을 내릴 수 있도록 하는 것입니다.

다음 섹션에서는 각 OU 및 계정을 살펴보고 목표와 관련된 개별 AWS 보안 서비스를 이해합니다. 이 문서는 각 요소(일반적으로 AWS 서비스)에 대해 다음 정보를 제공합니다.

- AWS SRA의 요소 및 보안 목적에 대한 간략한 개요입니다. 개별 서비스에 대한 자세한 설명과 기술 정보는 부록을 참조하세요.
- 서비스를 가장 효과적으로 활성화하고 관리하기 위한 권장 배치입니다. 이는 각 계정 및 OU의 개별 아키텍처 다이어그램에 캡처됩니다.
- 구성, 관리 및 다른 보안 서비스에 대한 데이터 공유 링크입니다. 이 서비스는 다른 보안 서비스에 어떻게 의존하거나 지원하나요?
- 설계 고려 사항. 먼저이 문서에서는 보안에 중요한 영향을 미치는 선택적 기능 또는 구성을 강조합니다. 둘째, 일반적으로 대체 요구 사항 또는 제약 조건의 결과로 수행하는 권장 사항의 일반적인 변형이 팀의 경험에 포함되는 경우 문서는 이러한 옵션을 설명합니다.

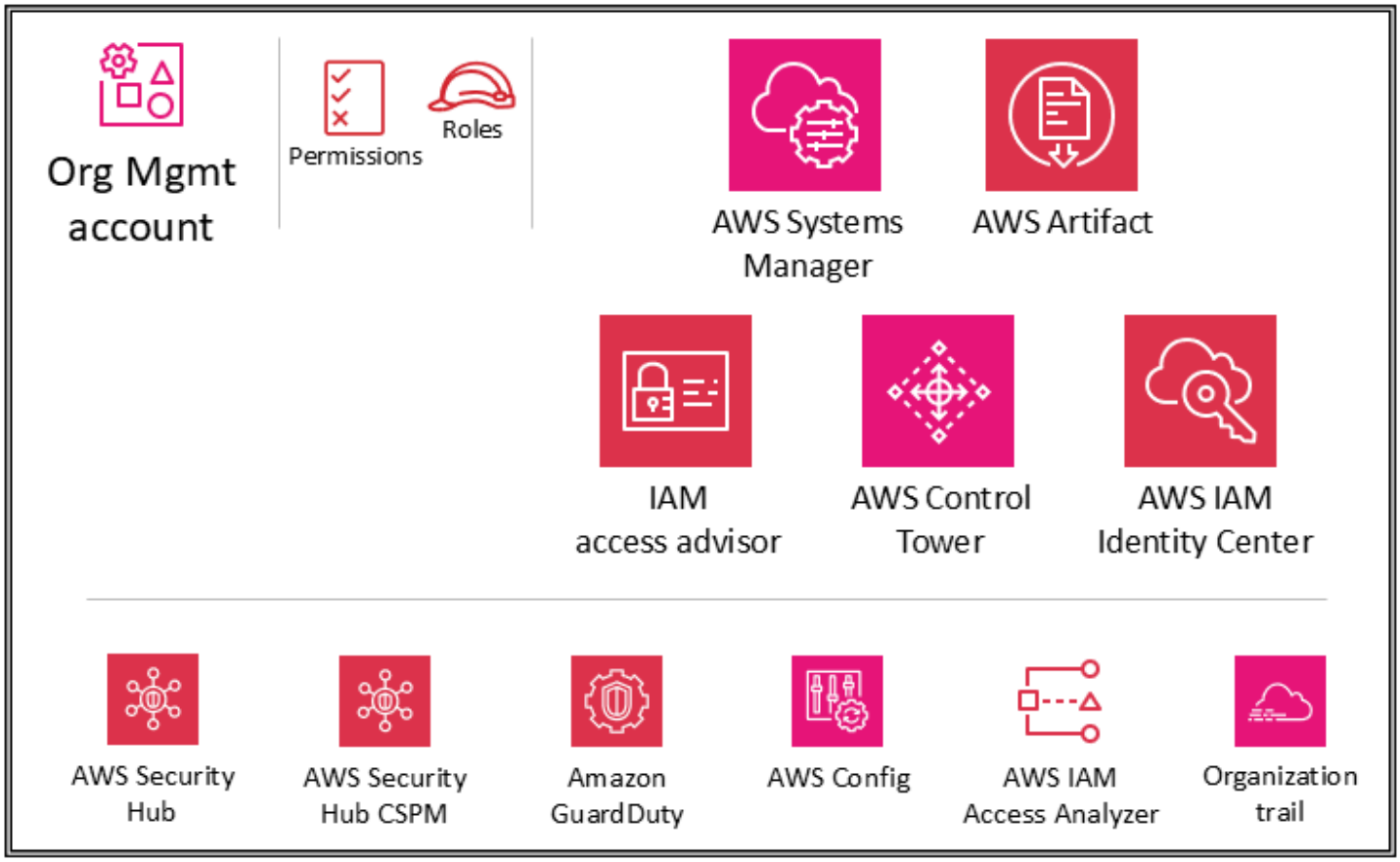
OUs 및 계정

- 조직 관리 계정
- 보안 OU - 보안 도구 계정
- 보안 OU - 로그 아카이브 계정
- 인프라 OU - Network 계정
- 인프라 OU - 공유 서비스 계정
- 워크로드 OU – 애플리케이션 계정

조직 관리 계정

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

다음 다이어그램은 조직 관리 계정에 구성된 AWS 보안 서비스를 보여줍니다.



이 가이드의 앞부분에서 보안 AWS Organizations 에 사용 및 관리 계정, 신뢰할 수 있는 액세스 및 위임된 관리자 단원에서는 조직 관리 계정의 목적과 보안 목표에 대해 자세히 설명했습니다. 조직 관리 계정의 보안 모범 사례를 따릅니다. 여기에는 비즈니스에서 관리하는 이메일 주소 사용, 올바른 관리 및 보안 연락처 정보 유지(예: 이벤트 AWS 시 계정 소유자에게 문의해야 하는 경우 계정에 전화번호 연결), 모든 사용자에 대한 멀티 팩터 인증(MFA) 활성화, 조직 관리 계정에 액세스할 수 있는 사용자를 정기적으로 검토하는 것이 포함됩니다. 조직 관리 계정에 배포된 서비스는 해당 서비스의 관리자(조직 관리 계정에서 액세스해야 함)가 다른 서비스에 부적절하게 액세스할 수 없도록 적절한 역할, 신뢰 정책 및 기타 권한으로 구성해야 합니다.

서비스 제어 정책

를 사용하면 여러에서 정책을 중앙에서 관리할 AWS Organizations수 있습니다 AWS 계정. 예를 들어 조직의 구성원 AWS 계정 인 여러에 서비스 제어 정책 (SCPs)을 적용할 수 있습니다. SCPs 사용하면 조직 구성원의 IAM 보안 주체(예: IAM 사용자 및 역할)가 실행할 수 있는 API와 실행할 수 없는 AWS 서비스 APIs를 정의할 수 있습니다 AWS 계정. SCPs는 조직을 생성할 때 AWS 계정 사용한 인 조직 관리 계정에서 생성 및 적용됩니다. SCPs에 대한 자세한 내용은이 참조의 앞부분에서 보안 AWS Organizations 에 사용 단원을 참조하십시오.

AWS Control Tower 를 사용하여 AWS 조직을 관리하는 경우 SCPs 세트를 예방 가드레일로 배포합니다(필수, 적극 권장 또는 선택으로 분류됨). 이러한 가드레일은 조직 전체의 보안 제어를 적용하여 리소스를 관리하는 데 도움이 됩니다. 이러한 SCPs 값이 managed-by-control-tower인 aws-control-tower 태그를 자동으로 사용합니다. managed-by-control-tower

> 설계 고려 사항
>
> SCPs 조직의 멤버 계정에 AWS 만 영향을 미칩니다. 조직 관리 계정에서 적용되지만 해당 계정의 사용자 또는 역할에는 영향을 미치지 않습니다. SCP 평가 로직의 작동 방식에 대해 알아보고 권장 구조의 예를 보려면 AWS 블로그 게시물 에서 서비스 제어 정책을 사용하는 방법을 참조하세요 AWS Organizations.

리소스 제어 정책

리소스 제어 정책(RCPs)은 조직 내 리소스에 사용 가능한 최대 권한을 중앙 집중식으로 제어합니다. RCP는 권한 가드레일을 정의하거나 자격 증명이 조직의 리소스에 대해 수행할 수 있는 작업에 대한 제한을 설정합니다. RCPs 사용하여 리소스에 액세스할 수 있는 사용자를 제한하고 조직의 멤버에서 리소스에 액세스하는 방법에 대한 요구 사항을 적용할 수 있습니다 AWS 계정. RCP를 개별 계정, OU 또는 조직 루트에 직접 연결할 수 있습니다. RCPs의 작동 방식에 대한 자세한 설명은 AWS Organizations 설명서의 RCP 평가를 참조하세요. 이 참조의 앞부분에서 보안에 사용 섹션에서 RCPs에 대해 자세히 알아보세요. AWS Organizations

AWS Control Tower 를 사용하여 AWS 조직을 관리하는 경우 RCPs 세트를 예방 가드레일로 배포합니다(필수, 적극 권장 또는 선택으로 분류됨). 이러한 가드레일은 조직 전체의 보안 제어를 적용하여 리소스를 관리하는 데 도움이 됩니다. 이러한 SCPs 값이 인 `aws-control-tower` 태그를 자동으로 사용합니다`managed-by-control-tower`.

설계 고려 사항

- RCP는 조직의 멤버 계정에만 영향을 미칩니다. 관리 계정의 리소스에는 영향을 미치지 않습니다. 이는 또한 RCP가 위임된 관리자로 지정된 멤버 계정에도 적용됨을 의미합니다.
- RCPs의 하위 집합에 대한 리소스에 적용됩니다 AWS 서비스. 자세한 내용은 설명서 의 RCPs를 AWS 서비스 지원하는 목록을 참조하세요. AWS Organizations 및 AWS Lambda 함수를 사용하여 AWS Config 규칙 현재 RCPs.

선언적 정책

선언적 정책은 조직 전체에서 지정된 AWS 서비스 에 대해 원하는 구성을 중앙에서 선언하고 적용하는 데 도움이 되는 AWS Organizations 관리 정책의 한 유형입니다. 선언적 정책은 현재 Amazon EC2, Amazon VPC 및 Amazon EBS 서비스를 지원합니다. 사용 가능한 서비스 속성에는 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 적용, EC2 직렬 콘솔을 통한 문제 해결 허용, Amazon Machine Image(AMI) 설정 허용, Amazon EBS 스냅샷, Amazon EC2 AMIs. 지원되는 최신 서비스 및 속성은 AWS Organizations 설명서의 선언적 정책을 참조하세요.

AWS Organizations 및 AWS Control Tower 콘솔에서 AWS 서비스 몇 가지를 선택하거나 몇 가지 AWS Command Line Interface (AWS CLI) 및 AWS SDK 명령을 사용하여에 대한 기준 구성을 적용할 수 있습니다. 선언적 정책은 서비스의 컨트롤 플레인에 적용됩니다. 즉, 서비스에 새 기능 또는 APIs가 도입되거나 새 계정이 조직에 추가되거나 새 보안 주체 및 리소스가 생성되더라도에 대한 기본 구성이 AWS 서비스 항상 유지됩니다. 선언적 정책은 전체 조직 또는 특정 OUs 또는 계정에 적용할 수 있습니다. 유효 정책은 계정에 직접 연결된 정책과 함께 조직 루트 및 OUs에서 상속되는 규칙 세트입니다. 선언적 정책이 분리 되면 선언적 정책이 연결되기 전에 속성 상태가 해당 상태로 롤백됩니다.

선언적 정책을 사용하여 사용자 지정 오류 메시지를 생성할 수 있습니다. 예를 들어 선언적 정책으로 인해 API 작업이 실패하는 경우 오류 메시지를 설정하거나 내부 Wiki에 대한 링크 또는 실패를 설명하는 메시지에 대한 링크와 같은 사용자 지정 URL을 제공할 수 있습니다. 이렇게 하면 사용자가 문제를 직접 해결할 수 있도록 더 많은 정보를 제공하는 데 도움이 됩니다. 를 사용하여 선언적 정책을 생성하고, 선언적 정책을 업데이트하고, 선언적 정책을 삭제하는 프로세스를 감사할 수도 있습니다 AWS CloudTrail.

선언적 정책은 계정 상태 보고서를 제공하므로 범위 내 계정에 대한 선언적 정책에서 지원하는 모든 속성의 현재 상태를 검토할 수 있습니다. 보고서 범위에 포함할 계정 및 OUs를 선택하거나 루트를 선택하여 전체 조직을 선택할 수 있습니다. 이 보고서는 분석을 제공하고 속성의 현재 상태가 계정 간에 균

일한 지(값을 통해 numberOfMatchedAccounts) 아니면 계정 간에 일관되지 않은 지(값을 통해) AWS 리전 지정하여 준비 상태를 평가하는 데 도움이 됩니다 numberOfUnmatchedAccounts.

> 설계 고려 사항
>
> 선언적 정책을 사용하여 서비스 속성을 구성하면 정책이 여러 APIs. 규정을 준수하지 않는 작업은 모두 실패합니다. 계정 관리자는 개별 계정 수준에서 서비스 속성의 값을 수정할 수 없습니다.

중앙 집중식 루트 액세스

의 모든 멤버 계정에 AWS Organizations 는 해당 멤버 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 자격 증명인 자체 루트 사용자가 있습니다. IAM은 중앙 집중식 루트 액세스 관리를 제공하여 모든 멤버 계정에서 루트 액세스를 관리합니다. 이렇게 하면 멤버 루트 사용자 사용을 방지하고 대규모 복구를 제공하는 데 도움이 됩니다. 중앙 집중식 루트 액세스 기능에는 루트 자격 증명 관리와 루트 세션이라는 두 가지 필수 기능이 있습니다.

- 루트 자격 증명 관리 기능은 중앙 관리를 허용하고 모든 관리 계정에서 루트 사용자를 보호하는 데 도움이 됩니다. 이 기능에는 장기 루트 자격 증명 제거, 멤버 계정의 루트 자격 증명 복구 방지, 기본적으로 루트 자격 증명 없이 새 멤버 계정 프로비저닝이 포함됩니다. 또한 규정 준수를 쉽게 입증할 수 있는 방법을 제공합니다. 루트 사용자 관리가 중앙 집중화되면 루트 사용자 암호, 액세스 키 및 서명 인증서를 제거하고 모든 멤버 계정에서 다중 인증(MFA)을 비활성화할 수 있습니다.
- 루트 세션 기능을 사용하면 조직 관리 계정 또는 위임된 관리자 계정의 멤버 계정에서 단기 자격 증명을 사용하여 권한이 있는 루트 사용자 작업을 수행할 수 있습니다. 이 기능을 사용하면 최소 권한 원칙을 준수하여 특정 작업으로 범위가 지정된 단기 루트 액세스를 활성화할 수 있습니다.

중앙 집중식 루트 자격 증명 관리를 위해서는 조직 관리 계정 또는 위임된 관리자 계정의 조직 수준에서 루트 자격 증명 관리 및 루트 세션 기능을 활성화해야 합니다. AWS SRA 모범 사례에 따라 이 기능을 보안 도구 계정에 위임합니다. 중앙 집중식 루트 사용자 액세스 구성 및 사용에 대한 자세한 내용은 AWS 보안 블로그 게시물,를 사용하는 고객의 루트 액세스 중앙 관리를 참조하세요 AWS Organizations.

IAM Identity Center

AWS IAM Identity Center는 모든 AWS 계정, 보안 주체 및 클라우드 워크로드에 대한 SSO 액세스를 중앙에서 관리하는 데 도움이 되는 ID 페더레이션 서비스입니다. 또한 IAM Identity Center를 사용하

면 일반적으로 사용되는 타사 서비스형 소프트웨어(SaaS) 애플리케이션에 대한 액세스 및 권한을 관리할 수 있습니다. 자격 증명 공급자는 SAML 2.0을 사용하여 IAM Identity Center와 통합됩니다. SCIM(System for Cross-Domain Identity Management)을 사용하여 대량 및 just-in-time 프로비저닝을 수행할 수 있습니다. 또한 IAM Identity Center는를 사용하여 자격 증명 공급자로서 온프레미스 또는 AWS관리형 Microsoft Active Directory(AD) 도메인과 통합할 수 있습니다 AWS Directory Service. IAM Identity Center에는 최종 사용자가 할당된 AWS 계정 IAM Identity Center, 역할, 클라우드 애플리케이션 및 사용자 지정 애플리케이션을 한 곳에서 찾고 액세스할 수 있는 사용자 포털이 포함되어 있습니다.

IAM Identity Center는 기본적으로 조직 관리 계정과 통합 AWS Organizations 되고 실행됩니다. 그러나 최소 권한을 행사하고 관리 계정에 대한 액세스를 엄격하게 제어하기 위해 IAM Identity Center 관리를 특정 멤버 계정에 위임할 수 있습니다. AWS SRA에서 공유 서비스 계정은 IAM Identity Center의 위임된 관리자 계정입니다. IAM Identity Center에 대해 위임된 관리를 활성화하기 전에 다음 고려 사항을 검토하세요. 위임에 대한 자세한 내용은 공유 서비스 계정 섹션에서 확인할 수 있습니다. 위임을 활성화한 후에도 조직 관리 계정에서 프로비저닝된 권한 세트 관리를 포함하여 특정 IAM Identity Center 관련 작업을 수행하려면 IAM Identity Center를 조직 관리 계정에서 실행해야 합니다.

IAM Identity Center 콘솔 내에서 계정은 캡슐화 OU로 표시됩니다. 이를 통해를 빠르게 검색하고 AWS 계정, 공통 권한 세트를 적용하고, 중앙 위치에서 액세스를 관리할 수 있습니다.

IAM Identity Center에는 특정 사용자 정보를 저장해야 하는 ID 스토어가 포함되어 있습니다. 그러나 IAM Identity Center가 인력 정보의 신뢰할 수 있는 소스일 필요는 없습니다. 기업에 이미 신뢰할 수 있는 소스가 있는 경우 IAM Identity Center는 다음과 같은 유형의 ID 제공업체(IdPs 지원합니다.

- IAM Identity Center ID 스토어 - 다음 두 가지 옵션을 사용할 수 없는 경우이 옵션을 선택합니다. ID 스토어에서 사용자가 생성되고, 그룹이 할당되고, 권한이 할당됩니다. 신뢰할 수 있는 소스가 IAM Identity Center 외부에 있더라도 보안 주체 속성의 사본이 자격 증명 저장소에 저장됩니다.
- Microsoft Active Directory(AD) -의 디렉터리 AWS Directory Service for Microsoft Active Directory 또는 Active Directory의 자체 관리형 디렉터리에서 사용자를 계속 관리하려면이 옵션을 선택합니다.
- 외부 ID 제공업체 - 외부 타사 SAML 기반 IdP에서 사용자를 관리하려면이 옵션을 선택합니다.

엔터프라이즈 내에 이미 있는 기존 IdP를 사용할 수 있습니다. 이렇게 하면 단일 위치에서 액세스를 생성, 관리 및 취소하므로 여러 애플리케이션과 서비스에 대한 액세스를 더 쉽게 관리할 수 있습니다. 예를 들어 누군가 팀을 떠나는 경우 한 위치에서 모든 애플리케이션 및 서비스(포함 AWS 계정)에 대한 액세스를 취소할 수 있습니다. 이렇게 하면 여러 자격 증명의 필요성이 줄어들고 인사(HR) 프로세스와 통합할 수 있는 기회가 제공됩니다.

설계 고려 사항

엔터프라이즈에서 해당 옵션을 사용할 수 있는 경우 외부 IdP를 사용합니다. IdP가 SCIM(System for Cross-domain Identity Management)을 지원하는 경우 IAM Identity Center의 SCIM 기능을 활용하여 사용자, 그룹 및 권한 프로비저닝(동기화)을 자동화합니다. 이를 통해 신입 직원, 다른 팀으로 이동하는 직원 및 퇴사하는 직원을 위한 회사 워크플로와 동기화된 AWS 상태로 액세스할 수 있습니다. 언제든지 디렉터리 하나 또는 SAML 2.0 자격 증명 공급자 하나만 IAM Identity Center에 연결할 수 있습니다. 그러나 다른 자격 증명 공급자로 전환할 수 있습니다.

IAM 액세스 어드바이저

IAM 액세스 어드바이저는 AWS 계정 및 OUs에 대해 마지막으로 액세스한 서비스 정보의 형태로 추적성 데이터를 제공합니다. 이 탐지 제어를 사용하여 최소 권한 전략에 기여합니다. IAM 보안 주체의 경우 마지막으로 액세스한 두 가지 유형의 정보, 즉 허용된 AWS 서비스 정보와 허용된 작업 정보를 볼 수 있습니다. 이 정보에는 시도한 날짜와 시간이 포함됩니다.

조직 관리 계정 내의 IAM 액세스를 통해 조직의 조직 관리 계정, OU, 멤버 계정 또는 IAM 정책에 대해 마지막으로 액세스한 서비스 데이터를 볼 수 있습니다 AWS . 이 정보는 관리 계정의 IAM 콘솔에서 사용할 수 있으며 AWS CLI 또는 프로그래밍 클라이언트에서 IAM Access Advisor APIs를 사용하여 프로그래밍 방식으로 얻을 수도 있습니다. 이 정보는 조직 또는 계정에서 서비스에 마지막으로 액세스하려고 시도한 보안 주체와 그 시기를 나타냅니다. 마지막으로 액세스한 정보는 실제 서비스 사용에 대한 인사이트를 제공하므로(예제 시나리오 참조) 실제로 사용되는 서비스로만 IAM 권한을 줄일 수 있습니다.

AWS Systems Manager

의 기능인 빠른 설정 AWS Organizations 및 탐색기는 AWS Systems Manager조직 관리 계정을 지원하고 운영합니다.

빠른 설정은 Systems Manager의 자동화 기능입니다. 이를 통해 조직 관리 계정은 Systems Manager가 AWS 조직의 여러 계정에서 사용자를 대신하여 참여할 수 있는 구성을 쉽게 정의할 수 있습니다. 조직 전체에서 AWS 빠른 설정을 활성화하거나 특정 OUs 선택할 수 있습니다. 빠른 설정은 AWS Systems Manager 에이전트(SSM 에이전트)가 EC2 인스턴스에서 격주 업데이트를 실행하도록 예약하고 해당 인스턴스에 대한 일일 스캔을 설정하여 누락된 패치를 식별할 수 있습니다.

Explorer는 AWS 리소스에 대한 정보를 보고하는 사용자 지정 가능한 작업 대시보드입니다. 탐색기는 AWS 계정 및 여러 계정의 작업 데이터에 대한 집계된 보기를 표시합니다 AWS 리전. 여기에는 EC2 인

스턴스 및 패치 규정 준수 세부 정보에 대한 데이터가 포함됩니다. 내에서 통합 설정(Systems Manager OpsCenter도 포함)을 완료한 후 Explorer에서 OU별로 또는 전체 AWS 조직에 대해 데이터를 집계할 AWS Organizations수 있습니다. Systems Manager는 데이터를 탐색기에 표시하기 전에 AWS 조직 관리 계정으로 집계합니다.

이 가이드의 뒷부분에 있는 워크로드 OU 섹션에서는 애플리케이션 계정의 EC2 인스턴스에서 SSM 에이전트를 사용하는 방법을 설명합니다.

AWS Control Tower

AWS Control Tower는 랜딩 존이라고 하는 안전한 다중 계정 AWS 환경을 설정하고 관리하는 간단한 방법을 제공합니다.는를 사용하여 랜딩 존을 AWS Control Tower 생성하고 지속적인 계정 관리 AWS Organizations및 거버넌스와 구현 모범 사례를 제공합니다. AWS Control Tower 를 사용하여 몇 단계로 새 계정을 프로비저닝하는 동시에 계정이 조직 정책을 준수하는지 확인할 수 있습니다. 기존 계정을 새 AWS Control Tower 환경에 추가할 수도 있습니다.

AWS Control Tower 에는 광범위하고 유연한 기능 세트가 있습니다. 주요 기능은 AWS Organizations AWS Service Catalog및 IAM Identity Center를 AWS 서비스포함하여 다른 여러의 기능을 오케스트레이션하여 랜딩 존을 구축하는 기능입니다. 예를 들어는 기본적으로를 AWS Control Tower AWS CloudFormation 사용하여 기준, AWS Organizations 구성 변경을 방지하는 서비스 제어 정책(SCPs) 및 규정 미준수를 지속적으로 감지하는 AWS Config 규칙 규칙을 설정합니다.는 AWS Well Architected 보안 기반 설계 원칙에 따라 다중 계정 AWS 환경을 신속하게 조정하는 데 도움이 되는 청사진을 AWS Control Tower 적용합니다. 거버넌스 기능 중에서 AWS Control Tower 는 선택한 정책을 준수하지 않는 리소스의 배포를 방지하는 가드레일을 제공합니다.

를 사용하여 AWS SRA 지침 구현을 시작할 수 있습니다 AWS Control Tower. 예를 들어는 권장 다중 계정 아키텍처를 사용하여 AWS 조직을 AWS Control Tower 설정합니다. ID 관리를 제공하고, 계정에 대한 페더레이션 액세스를 제공하고, 로깅을 중앙 집중화하고, 교차 계정 보안 감사를 설정하고, 새 계정을 프로비저닝하기 위한 워크플로를 정의하고, 네트워크 구성을 사용하여 계정 기준을 구현하는 청사진을 제공합니다.

AWS SRA에서 AWS Control Tower 는 조직 관리 계정 내에 있습니다.는이 계정을 AWS Control Tower 사용하여 AWS 조직을 자동으로 설정하고 해당 계정을 관리 계정으로 지정하기 때문입니다. 이 계정은 조직 전체 AWS 의 결제에 사용됩니다. 또한 Account Factory 계정 프로비저닝, OUs 관리, 가드레일 관리에 사용됩니다. 기존 AWS 조직에서 AWS Control Tower 를 시작하는 경우 기존 관리 계정을 사용할 수 있습니다. AWS Control Tower 는 해당 계정을 지정된 관리 계정으로 사용합니다.

설계 고려 사항

계정 전체에서 제어 및 구성에 대한 추가 기준선을 지정하려면 AWS Control Tower (CfCT)에 대한 사용자 지정을 사용할 수 있습니다. CfCT를 사용하면 CloudFormation 템플릿과 SCP를 사용하여 AWS Control Tower 랜딩 존을 사용자 지정할 수 있습니다. SCPs 사용자 지정 템플릿 및 정책을 조직 내 개별 계정 및 OUs에 배포할 수 있습니다. CfCT는 AWS Control Tower 수명 주기 이벤트와 통합되어 리소스 배포가 랜딩 존과 동기화되도록 합니다.

AWS Artifact

AWS Artifact는 AWS 보안 및 규정 준수 보고서와 일부 온라인 계약에 대한 온디맨드 액세스를 제공합니다. 에서 사용할 수 있는 보고서에 AWS Artifact 는 SOC(System and Organization Controls) 보고서, PCI(Payment Card Industry) 보고서, AWS 보안 제어의 구현 및 운영 효율성을 검증하는 지역 및 규정 준수 수직 부문의 인증 기관의 인증서가 포함됩니다.는 보안 제어 환경에 대한 투명성을 강화 AWS 하여에 대한 실사를 수행하는 데 AWS Artifact 도움이 됩니다. 또한 새 보고서에 즉시 액세스할 수 AWS 있도록의 보안 및 규정 준수를 지속적으로 모니터링할 수 있습니다.

AWS Artifact 계약을 통해 개별 계정 및 조직의 일부인 계정에 대한 BAA(Business Associate Addendum)와 같은 계약 상태를 AWS 검토, 수락 및 추적할 수 있습니다 AWS Organizations.

AWS 감사 아티팩트를 AWS 보안 제어의 증거로 감사자 또는 규제 기관에 제공할 수 있습니다. 일부 AWS 감사 아티팩트에서 제공하는 책임 지침을 사용하여 클라우드 아키텍처를 설계할 수도 있습니다. 이 지침은 시스템의 특정 사용 사례를 지원하기 위해 마련할 수 있는 추가 보안 제어를 결정하는 데 도움이 됩니다.

AWS Artifact 는 계약을 검토, 수락 및 관리할 수 있는 중앙 위치를 제공하기 위해 조직 관리 계정에서 호스팅됩니다 AWS. 이는 관리 계정에서 수락된 계약이 멤버 계정으로 흐르기 때문입니다.

설계 고려 사항

조직 관리 계정 내의 사용자는의 계약 기능만 사용하도록 제한해야 하며 다른 기능은 사용할 수 AWS Artifact 없습니다. 업무 분리를 구현하기 위해 AWS Artifact 는 보안 도구 계정에서도 호스팅됩니다.이 계정에서는 규정 준수 이해관계자 및 외부 감사자에게 감사 아티팩트에 액세스할 수 있는 권한을 위임할 수 있습니다. 세분화된 IAM 권한 정책을 정의하여 이러한 분리를 구현할 수 있습니다. 예제는 AWS 설명서의 IAM 정책 예제를 참조하세요.

분산 및 중앙 집중식 보안 서비스 가드레일

AWS SRA, AWS Security Hub, AWS Security Hub CSPM,, Amazon GuardDuty, AWS Config, IAM Access Analyzer, AWS CloudTrail 조직 추적 및 종종 Amazon Macie는 계정 간에 적절한 위임된 가드레일 집합과 함께 배포되며 AWS 조직 전체에 중앙 집중식 모니터링, 관리 및 거버넌스를 제공합니다. 이 서비스 그룹은 AWS SRA에 표시되는 모든 유형의 계정에서 찾을 수 있습니다. 이는 계정 온보딩 및 기준 설정 프로세스의 일부로 프로비저닝해야 AWS 서비스 하는의 일부여야 합니다. GitHub 코드 리포지토리는 AWS 조직 관리 계정을 포함하여 계정 전체에서 보안 중심 서비스의 샘플 구현 AWS 을 제공합니다.

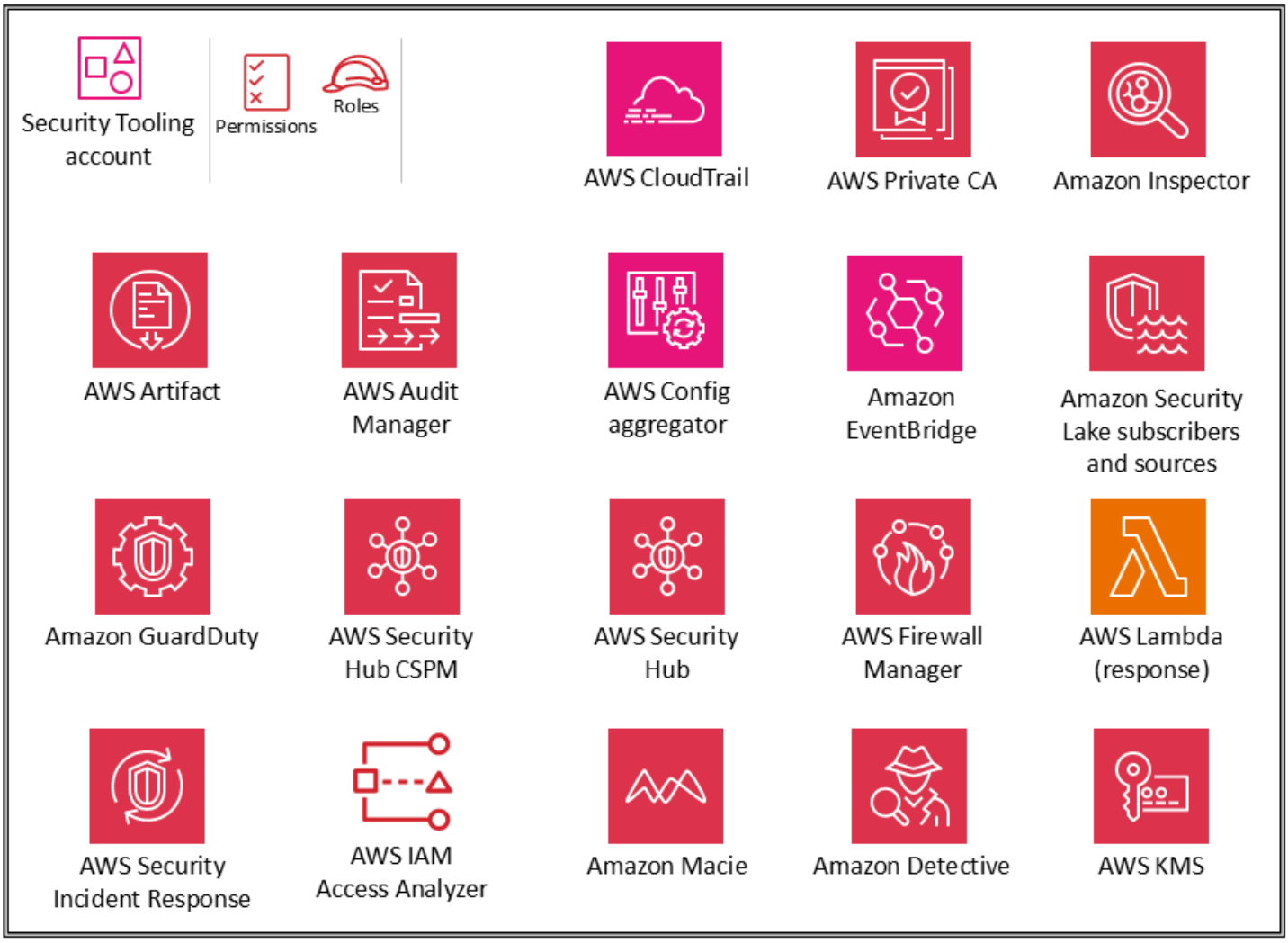
이러한 서비스 외에도 AWS SRA에는 통합 및 위임된 관리자 기능을 지원하는 두 가지 보안 중심 서비스 AWS Audit Manager인 Amazon Detective 및가 포함되어 있습니다 AWS Organizations. 그러나 이는 계정 기준 설정을 위한 권장 서비스의 일부로 포함되지 않습니다. 이러한 서비스는 다음 시나리오에서 가장 잘 사용되는 것으로 나타났습니다.

- 이러한 디지털 포렌식 및 IT 감사 기능을 수행하는 전담 팀 또는 리소스 그룹이 있습니다. Detective는 보안 분석가 팀에서 가장 잘 활용되며 Audit Manager는 내부 감사 또는 규정 준수 팀에 유용합니다.
- 프로젝트 시작 AWS Security Hub CSPM 시 AWS Config Amazon GuardDuty AWS Security Hub및와 같은 핵심 도구 세트에 집중한 다음 추가 기능을 제공하는 서비스를 사용하여 이를 기반으로 구축하려고 합니다.

보안 OU - 보안 도구 계정

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

다음 다이어그램은 AWS Security Tooling 계정에 구성된 보안 서비스를 보여줍니다.



Security Tooling 계정은 보안 서비스 운영, 모니터링 AWS 계정, 보안 알림 및 응답 자동화 전용입니다. 보안 목표에는 다음이 포함됩니다.

- 보안 가드레일, 모니터링 및 대응에 대한 액세스를 관리할 수 있는 제어된 액세스 권한을 전용 계정에 제공합니다.
- 적절한 중앙 집중식 보안 인프라를 유지하여 보안 운영 데이터를 모니터링하고 추적성을 유지합니다. 탐지, 조사 및 대응은 보안 수명 주기의 필수 부분이며 품질 프로세스, 법적 또는 규정 준수 의무, 위협 식별 및 대응 노력을 지원하는 데 사용할 수 있습니다.
- 암호화 키 및 보안 그룹 설정과 같은 적절한 보안 구성 및 작업에 대한 또 다른 제어 계층을 유지하여 defense-in-depth 조직 전략을 추가로 지원합니다. 보안 운영자가 작동하는 계정입니다. AWS 조직 전체의 정보를 보기 위한 읽기 전용/감사 역할은 일반적인 반면, 쓰기/수정 역할은 수가 제한되고 엄격하게 제어되고 모니터링되며 로깅됩니다.

설계 고려 사항

- AWS Control Tower 는 기본적으로 보안 OU에서 감사 계정 아래에 계정 이름을 지정합니다. AWS Control Tower 설정 중에 계정 이름을 바꿀 수 있습니다.
- 보안 도구 계정이 두 개 이상 있는 것이 적절할 수 있습니다. 예를 들어 보안 이벤트 모니터링 및 대응은 전담 팀에 할당되는 경우가 많습니다. 네트워크 보안은 클라우드 인프라 또는 네트워크 팀과 협력하여 자체 계정 및 역할을 보증할 수 있습니다. 이러한 분할은 중앙 집중식 보안 엔클레이브를 분리하는 목표를 유지하고 업무 분리, 최소 권한 및 팀 할당의 잠재적 단순성을 더욱 강조합니다. 를 사용하는 경우 보안 OU에서 추가 생성을 AWS Control Tower제한 AWS 계정 합니다.

보안 서비스에 대한 위임된 관리자

Security Tooling 계정은 전체에서 관리자/멤버 구조로 관리되는 보안 서비스의 관리자 계정 역할을 합니다 AWS 계정. 앞서 언급했듯이 이는 AWS Organizations 위임된 관리자 기능을 통해 처리됩니다. 현재 위임된 관리자를 지원하는 AWS SRA의 서비스에는 루트 액세스 AWS Config,,,, Amazon GuardDuty AWS Firewall Manager, IAM Access Analyzer, Amazon Macie, AWS Security Hub, AWS Security Hub CSPM Amazon Detective, AWS Audit Manager, Amazon Inspector AWS CloudTrail및에 대한 IAM 중앙 집중식 관리가 포함됩니다 AWS Systems Manager. 보안 팀은 이러한 서비스의 보안 기능을 관리하고 보안 관련 이벤트 또는 조사 결과를 모니터링합니다.

AWS IAM Identity Center 는 멤버 계정에 대한 위임된 관리를 지원합니다. AWS SRA는 공유 서비스 계정의 뒷부분 IAM Identity Center 섹션에 설명된 대로 공유 서비스 계정을 IAM Identity Center의 위임된 관리자 계정으로 사용합니다.

중앙 집중식 루트 액세스

Security Tooling 계정은 루트 액세스 기능의 IAM 중앙 집중식 관리를 위한 위임된 관리자 계정 입니다. 멤버 계정에서 자격 증명 관리 및 권한 있는 루트 작업을 활성화하여 조직 수준에서이 기능을 활성화해야 합니다. 멤버 계정을 대신하여 권한 있는 루트 작업을 수행할 수 있으려면 위임된 관리자에게 명시적으로 `sts:AssumeRoot` 권한을 부여해야 합니다. 이 권한은 조직 관리 또는 위임된 관리자 계정에서 멤버 계정의 권한 있는 루트 작업이 활성화된 후에만 사용할 수 있습니다. 이 권한을 사용하면 사용자는 Security Tooling 계정에서 멤버 계정에 대한 권한 있는 루트 사용자 작업을 중앙에서 수행할 수 있습니다. 권한 있는 세션을 시작한 후 잘못 구성된 S3 버킷 정책을 삭제하고, 잘못 구성된 SQS 대기열 정책을 삭제하고, 멤버 계정에 대한 루트 사용자 자격 증명을 삭제하고, 멤버 계정에 대한 루트 사용

자 자격 증명을 다시 활성화할 수 있습니다. 콘솔에서 AWS Command Line Interface (AWS CLI)를 사용하거나 APIs.

AWS CloudTrail

AWS CloudTrail는 내 활동의 거버넌스, 규정 준수 및 감사를 지원하는 서비스입니다 AWS 계정. CloudTrail을 사용하면 AWS 인프라 전반의 작업과 관련된 계정 활동을 로깅, 지속적인 모니터링 및 유지할 수 있습니다. CloudTrail은와 통합되며 AWS Organizations, 해당 통합을 사용하여 조직의 모든 계정에 대한 모든 이벤트를 로깅하는 단일 추적을 AWS 생성할 수 있습니다. 이를 조직 추적이라고 합니다. 조직의 관리 계정 내에서 또는 위임된 관리자 계정에서만 조직 추적을 생성하고 관리할 수 있습니다. 조직 추적을 생성하면 지정한 이름의 추적이 AWS 조직에 AWS 계정 속한 모든에 생성됩니다. 추적은 AWS 조직의 관리 계정을 포함한 모든 계정에 대한 활동을 기록하고 로그를 단일 S3 버킷에 저장합니다. 이 S3 버킷의 민감도 때문에이 가이드 뒷부분의 Amazon S3 중앙 로그 스토어 섹션에 설명된 모범 사례를 따라 보호해야 합니다. AWS 조직의 모든 계정은 추적 목록에서 조직 추적을 볼 수 있습니다. 그러나 멤버 AWS 계정 는이 추적에 대한 보기 전용 액세스 권한을 가집니다. 기본적으로 CloudTrail 콘솔에서 조직 추적을 생성하면 추적은 다중 리전 추적입니다. 추가 보안 모범 사례는 CloudTrail 설명서를 참조하세요.

AWS SRA에서 보안 도구 계정은 CloudTrail을 관리하기 위한 위임된 관리자 계정입니다. 조직 추적 로그를 저장할 해당 S3 버킷이 로그 아카이브 계정에 생성됩니다. 이는 CloudTrail 로그 권한의 관리 및 사용을 분리하기 위한 것입니다. 조직 추적에 대한 로그 파일을 저장하기 위해 S3 버킷을 생성하거나 업데이트하는 방법에 대한 자세한 내용은 CloudTrail 설명서를 참조하세요. 보안 모범 사례로 조직 추적의 조건 키를 S3 버킷의 리소스 정책(및 KMS 키 또는 SNS 주제와 같은 기타 리소스)에 추가합니다 `aws:SourceArn` . 이렇게 하면 S3 버킷이 특정 추적과 연결된 데이터만 수락합니다. 추적은 로그 파일 무결성 검증을 위한 로그 파일 검증으로 구성됩니다. 로그 및 다이제스트 파일은 SSE-KMS를 사용하여 암호화됩니다. 또한 조직 추적은 CloudWatch Logs의 로그 그룹과 통합되어 장기 보존을 위한 이벤트를 전송합니다.

> **Note**
>
> 관리 계정과 위임된 관리자 계정 모두에서 조직 추적을 생성하고 관리할 수 있습니다. 그러나 가장 좋은 방법은 관리 계정에 대한 액세스를 제한하고 사용 가능한 경우 위임된 관리자 기능을 사용하는 것입니다.

설계 고려 사항

- CloudTrail은 기본적으로 데이터 이벤트를 로깅하지 않습니다. 대용량 활동인 경우가 많기 때문입니다. 그러나 S3 버킷, Lambda 함수, CloudTrail 레이크로 AWS 전송되는 외부의 로그 이벤트, SNS 주제와 같은 특정 중요 AWS 리소스에 대한 데이터 이벤트를 캡처해야 합니다. 이렇게 하려면 각 개별 리소스의 ARNs을 지정하여 특정 리소스의 데이터 이벤트를 포함하도록 조직 추적을 구성합니다.
- 멤버 계정이 자신의 계정에 대한 CloudTrail 로그 파일에 액세스해야 하는 경우 중앙 S3 버킷에서 조직의 CloudTrail 로그 파일을 선택적으로 공유할 수 있습니다. 그러나 멤버 계정에 계정의 CloudTrail 로그에 로컬 Amazon CloudWatch 로그 그룹이 필요하거나 조직 추적과 다르게 로그 관리 및 데이터 이벤트(읽기 전용, 쓰기 전용, 관리 이벤트, 데이터 이벤트)를 구성하려는 경우 적절한 제어를 사용하여 로컬 추적을 생성할 수 있습니다. CloudTrail 로컬 계정별 추적에는 추가 비용이 발생합니다.

AWS Security Hub CSPM

이전에 로 알려진 AWS Security Hub 클라우드 보안 태세 관리(AWS Security Hub CSPM)는의 보안 태세에 대한 포괄적인 보기를 AWS Security Hub제공하고 보안 업계 표준 및 모범 사례를 기준으로 환경을 확인하는 AWS 데 도움이 됩니다. Security Hub CSPM은 AWS 통합 서비스, 지원되는 타사 제품 및 사용할 수 있는 기타 사용자 지정 보안 제품에서 보안 데이터를 수집합니다. 이 서비스는 보안 추세를 지속적으로 모니터링 및 분석하고 우선 순위가 가장 높은 보안 문제를 식별하는 데 도움을 줍니다. 수집된 소스 외에도 Security Hub CSPM은 하나 이상의 보안 표준에 매핑되는 보안 제어로 표시되는 자체 조사 결과를 생성합니다. 이러한 표준에는 AWS Foundational Security Best Practices(FSBP), Center for Internet Security(CIS) AWS Foundations Benchmark v1.20 및 v1.4.0, National Institute of Standards and Technology(NIST) SP 800-53 Rev. 5, Payment Card Industry Data Security Standard(PCI DSS) 및 서비스 관리형 표준이 포함됩니다. 현재 보안 표준 목록과 특정 보안 제어에 대한 세부 정보는 Security Hub CSPM 설명서의 Security Hub CSPM에 대한 표준 참조를 참조하세요.

Security Hub CSPM은와 통합되어 AWS 조직의 모든 기존 및 향후 계정에서 보안 태세 관리를 AWS Organizations 간소화합니다. 위임된 관리자 계정(이 경우 Security Tooling)의 Security Hub CSPM 중앙 구성 기능을 사용하여 여러 리전의 조직 계정 및 조직 단위(OUs)에서 Security Hub CSPM 서비스, 보안 표준 및 보안 제어를 구성하는 방법을 지정할 수 있습니다. 홈 리전이라고 하는 한 기본 리전에서 몇 단계로 이러한 설정을 구성할 수 있습니다. 중앙 구성을 사용하지 않는 경우 각 계정 및 리전에서 Security Hub CSPM을 별도로 구성해야 합니다. 위임된 관리자는 계정 및 OUs 각 리전에서 별도로 설정을 구성할 수 있는 자체 관리형 또는 위임된 관리자가 여러 리전에서 멤버 계정 또는 OU를 구성할 수

있는 중앙 관리형으로 지정할 수 있습니다. 조직의 모든 계정과 OU를 중앙 관리형, 자체 관리형 또는 이 둘의 조합으로 지정할 수 있습니다. 이렇게 하면 각 OU 및 계정에 대해 수정할 수 있는 유연성을 제공하면서 일관된 구성의 적용을 간소화할 수 있습니다.

Security Hub CSPM 위임된 관리자 계정은 모든 멤버 계정의 조사 결과를 보고, 인사이트를 보고, 세부 정보를 제어할 수도 있습니다. 위임된 관리자 계정 내에서 집계 리전을 추가로 지정하여 계정 및 연결된 리전에서 조사 결과를 중앙 집중화할 수 있습니다. 조사 결과는 집계자 리전과 다른 모든 리전 간에 지속적으로 양방향으로 동기화됩니다.

Security Hub CSPM은 여러 와의 통합을 지원합니다 AWS 서비스. Amazon GuardDuty, AWS Config, Amazon Macie, IAM Access Analyzer AWS Firewall Manager, Amazon Inspector, Amazon Route 53 Resolver DNS Firewall 및 AWS Systems Manager Patch Manager는 Security Hub CSPM에 조사 결과를 제공할 수 있습니다. Security Hub CSPM은 AWS Security Finding Format(ASFF)이라는 표준 형식을 사용하여 조사 결과를 처리합니다. Security Hub CSPM은 통합 제품 전반의 조사 결과를 상호 연관시켜 가장 중요한 조사 결과의 우선순위를 지정합니다. Security Hub CSPM 조사 결과의 메타데이터를 보강하여 보안 조사 결과의 컨텍스트화, 우선 순위 지정 및 조치를 개선할 수 있습니다. 이 보강은 Security Hub CSPM에 수집된 모든 결과에 리소스 태그, 새 AWS 애플리케이션 태그 및 계정 이름 정보를 추가합니다. 이를 통해 자동화 규칙에 대한 조사 결과를 미세 조정하고, 조사 결과 및 인사이트를 검색 또는 필터링하고, 애플리케이션별로 보안 태세 상태를 평가할 수 있습니다. 또한 자동화 규칙을 사용하여 조사 결과를 자동으로 업데이트할 수 있습니다. Security Hub CSPM은 조사 결과를 수집할 때 조사 결과 억제, 심각도 변경, 조사 결과에 메모 추가와 같은 다양한 규칙 작업을 적용할 수 있습니다. 이러한 규칙 작업은 조사 결과가 연결된 리소스 또는 계정 IDs 또는 제목과 같이 조사 결과가 지정된 기준과 일치할 때 적용됩니다. 자동화 규칙을 사용하여 ASFF에서 선택 결과 필드를 업데이트할 수 있습니다. 규칙은 새로운 조사 결과와 업데이트된 조사 결과 모두에 적용됩니다.

보안 이벤트를 조사하는 동안 Security Hub CSPM에서 Amazon Detective로 이동하여 GuardDuty 조사 결과를 조사할 수 있습니다. Security Hub CSPM은 원활한 통합을 위해 Detective(있는 경우)와 같은 서비스에 대해 위임된 관리자 계정을 정렬할 것을 권장합니다. 예를 들어 Detective와 Security Hub CSPM 간에 관리자 계정을 정렬하지 않으면 조사 결과에서 Detective로 이동하는 것이 작동하지 않습니다. 전체 목록은 Security Hub CSPM 설명서의 Security Hub CSPM과의 AWS 서비스 통합 개요를 참조하세요.

Security Hub CSPM을 Amazon VPC의 Network Access Analyzer 기능과 함께 사용하여 AWS 네트워크 구성의 규정 준수를 지속적으로 모니터링할 수 있습니다. 이렇게 하면 원치 않는 네트워크 액세스를 차단하고 중요한 리소스가 외부에 액세스하지 못하도록 방지할 수 있습니다. 추가 아키텍처 및 구현 세부 정보는 블로그 게시물 Amazon VPC Network Access Analyzer 및를 AWS 사용한 네트워크 규정 준수의 지속적 확인을 참조하세요. AWS Security Hub CSPM

Security Hub CSPM은 모니터링 기능 외에도 Amazon EventBridge와의 통합을 지원하여 특정 조사 결과의 문제 해결을 자동화합니다. 결과를 수신할 때 수행할 사용자 지정 작업을 정의할 수 있습니다. 예를 들어, 조사 결과를 티켓팅 시스템 또는 자동 문제 해결 시스템으로 전송하도록 사용자 지정 작업을 구성할 수 있습니다. 추가 토론 및 예제는 AWS 블로그 게시물를 사용한 자동 응답 및 문제 해결 AWS Security Hub CSPM 및 Security Hub CSPM 자동 응답 및 문제 해결을 위한 AWS 솔루션 배포 방법을 참조하세요.

Security Hub CSPM은 서비스 연결을 사용하여 제어 AWS Config 규칙 에 대한 대부분의 보안 검사를 수행합니다. 이러한 제어를 지원하려면 Security Hub CSPM AWS 리전 이 AWS Config 활성화된 각에서 관리자(또는 위임된 관리자) 계정 및 멤버 계정을 포함한 모든 계정에서를 활성화해야 합니다.

설계 고려 사항

- PCI-DSS와 같은 규정 준수 표준이 Security Hub CSPM에 이미 있는 경우 완전 관리형 Security Hub CSPM 서비스가 이를 운영하는 가장 쉬운 방법입니다. 그러나 보안, 운영 또는 비용 최적화 검사를 포함할 수 있는 자체 규정 준수 또는 보안 표준을 통합하려는 경우 AWS Config 적합성 팩은 간소화된 사용자 지정 프로세스를 제공합니다. (AWS Config 및 적합성 팩에 대한 자세한 내용은 AWS Config 섹션을 참조하세요.)
- Security Hub CSPM의 일반적인 사용 사례는 다음과 같습니다.
  - 리소스의 AWS 보안 및 규정 준수 태세에 대한 애플리케이션 소유자의 가시성을 제공하는 대시보드
  - 보안 운영, 인시던트 대응 담당자 및 위협 헌터가 AWS 계정 및 리전 전반의 보안 및 규정 준수 조사 결과를 분류하고 조치를 취하는 데 사용하는 AWS 보안 조사 결과의 중앙 보기
  - AWS 계정 및 리전 전체에서 중앙 집중식 보안 정보 및 이벤트 관리(SIEM) 또는 기타 보안 오케스트레이션 시스템으로 보안 및 규정 준수 조사 결과를 집계하고 라우팅하려면

  설정 방법을 포함하여 이러한 사용 사례에 대한 추가 지침은 블로그 게시물 세 가지 기본 Security Hub CSPM 사용 패턴 및 배포 방법을 참조하세요.

구현 예제

AWS SRA 코드 라이브러리는 Security Hub CSPM의 샘플 구현을 제공합니다. 여기에는 서비스의 자동 활성화, 멤버 계정에 대한 위임된 관리(보안 도구), AWS 조직의 모든 기존 및 향후 계정에 대해 Security Hub CSPM을 활성화하는 구성이 포함됩니다.

AWS Security Hub

AWS Security Hub는 중요한 보안 위협의 우선순위를 정하고 대규모 대응을 지원하는 통합 클라우드 보안 솔루션입니다. Security Hub는 태세 관리(AWS Security Hub CSPM), 취약성 관리(Amazon Inspector), 민감한 데이터(Amazon Macie) 및 위협 탐지(Amazon GuardDuty)와 같은 여러 소스의 보안 신호를 자동으로 상호 연관시키고 보강하여 보안 문제를 거의 실시간으로 탐지합니다. 이를 통해 보안 팀은 자동화된 분석 및 컨텍스트별 인사이트를 통해 클라우드 환경에서 활성 위험을 우선적으로 처리할 수 있습니다. Security Hub는 공격자가 노출 조사 결과와 관련된 리소스에 액세스하기 위해 악용할 수 있는 잠재적 공격 경로를 시각적으로 보여줍니다. 이렇게 하면 복잡한 보안 신호가 실행 가능한 인사이트로 변환되므로 정보에 입각한 보안 결정을 신속하게 내릴 수 있습니다.

Security Hub는 보안 결과에 도달하기 위해 연결된 보안 서비스 구성 요소의 활성화를 간소화하기 위해 전략적으로 재설계되었습니다. 위협 매트릭스의 보안 조사 결과를 다양한 보안 신호에 거의 실시간으로 상호 연관시켜 가장 중요한 위험의 우선 순위를 지정할 수 있습니다. 결과는 AWS 리소스와 관련된 노출을 감지하기 위해 상관관계가 있습니다. 노출도는 보안 제어, 잘못된 구성 또는 활성 위협으로 악용될 수 있는 기타 영역의 광범위한 약점을 나타냅니다. 예를 들어, 노출이 인터넷에서 연결할 수 있고 악용 가능성이 높은 소프트웨어 취약성이 있는 EC2 인스턴스일 수 있습니다.

Security Hub 및 Security Hub CSPM은 보완 서비스입니다. Security Hub CSPM은 보안 태세에 대한 포괄적인 보기를 제공하고 보안 업계 표준 및 모범 사례를 기준으로 클라우드 환경을 평가하는 데 도움이 됩니다. Security Hub는 중요한 보안 문제의 우선순위를 정하고 이에 대응하는 데 도움이 되는 통합 환경을 제공합니다. Security Hub CSPM 조사 결과는 자동으로 Security Hub로 라우팅되며, 여기서 Amazon Inspector와 같은 다른 보안 서비스의 조사 결과와 상호 연관되어 노출을 생성합니다. 이를 통해 환경에서 가장 중요한 위험을 식별할 수 있습니다.

또한 Security Hub는 유형 및 관련 조사 결과별로 AWS 환경의 리소스에 대한 요약을 제공합니다. 리소스는 노출 및 공격 시퀀스에 따라 우선순위가 지정됩니다. 리소스 유형을 선택하면 해당 리소스 유형과 연결된 모든 리소스를 검토할 수 있습니다.

최적의 환경을 위해 Security Hub 및 Security Hub CSPM을 활성화하고 Amazon GuardDuty, Amazon Inspector 및 Amazon Macie와 같은 기타 보안 서비스를 활성화하는 것이 좋습니다. Security Hub 적용 범위 조사 결과를 사용하여 조직의 모든 멤버 계정에서 이러한 서비스 및 기능이 균일하게 활성화되었는지 여부를 파악할 수 있습니다.

AWS SRA에서 Security Tooling 계정은 Security Hub, Security Hub CSPM 및 기타 AWS 보안 서비스의 위임된 관리자 역할을 합니다. Security Tooling 계정 내에서 멤버 계정과 연결된 모든 리소스를 볼 수 있습니다. 홈의 모든 리소스를 연결된 AWS 리전 에서 볼 수도 있습니다 AWS 리전.

구현 노트

Security Hub를 활성화하려면 이전에 Security Hub CSPM을 활성화했는지 여부를 고려하는 절차를 포함하여 세 단계가 필요합니다. Security Hub는 기본적으로와 통합되어 구성 및 구현 프로세스를 AWS Organizations간소화하고 모든 결과를 단일 위치로 중앙 집중화 및 집계합니다. AWS SRA 모범 사례에 따라 Security Tooling 계정을 위임된 관리자 계정으로 사용하여 Security Hub를 관리하고 구성합니다. Security Hub 구성 설정을 사용하여 향후 리전 및 계정을 포함하여 모든 리전, OUs 및 계정을 자동으로 활성화합니다. 또한 여러의 조사 결과, 리소스 및 추세를 단일 홈 리전 AWS 리전 으로 집계하도록 교차 리전 집계를 설정해야 합니다. 구성 중에 Jira Cloud 또는 ServiceNow와 같은 기본 통합을 활성화할 수도 있습니다.

설계 고려 사항

- Security Hub 조사 결과는 Open Cybersecurity Schema Framework(OCSF)에서 서식이 지정됩니다. Security Hub는 OCSF에서 결과를 생성하고 Security Hub CSPM 및 기타로부터 OCSF에서 결과를 수신합니다 AWS 서비스. 이러한 OCSF 조사 결과는 자동화를 위해 Amazon EventBridge를 통해 전송하거나 보안 로그 분석 및 보존을 수행하기 위해 중앙 로그 집계 계정에 저장할 수 있습니다.
- AWS 조직 관리 계정은 자신을 Security Hub에서 위임된 관리자로 지정할 수 없습니다. 이는 Security Tooling 계정을 위임된 관리자로 지정하는 AWS SRA 모범 사례에 부합합니다. 또한 다음 사항에 유의하세요.
  - Security Hub CSPM의 지정된 관리자 계정이 자동으로 Security Hub의 지정된 관리자가 됩니다.
  - Security Hub를 통해 위임된 관리를 제거하면 Security Hub CSPM에 대한 위임된 관리도 제거됩니다. 마찬가지로 Security Hub CSPM을 통해 위임된 관리를 제거하면 Security Hub에서도 제거됩니다.
- Security Hub에는 사양에 따라 조사 결과를 자동으로 수정하고 조치를 취하는 기능이 포함되어 있으며, Security Hub는 다음과 같은 유형의 자동화를 지원합니다.
  - 정의된 기준에 따라 거의 실시간으로 조사 결과를 자동으로 업데이트하고, 조사 결과를 억제하고, 조사 결과를 티켓팅 도구로 전송하는 자동화 규칙입니다.
  - 자동 응답 및 문제 해결 - 특정 조사 결과 및 인사이트에 대해 수행할 자동 작업을 정의하는 사용자 지정 EventBridge 규칙을 생성합니다.
- Security Hub는 정책을 통해 모든 멤버 계정 및 리전에서 Amazon Inspector를 구성할 수 있으며 배포를 통해 GuardDuty 및 Security Hub CSPM을 구성할 수 있습니다. 정책은 계정 및

리전에 대한 AWS Organizations 정책을 생성합니다. 배포는 선택한 계정 및 리전에서 보안 기능을 활성화하는 일회성 작업입니다. 새로 활성화된 계정에는 배포가 적용되지 않습니다. 또는 GuardDuty 및 Security Hub CSPM에서 새 멤버 계정에 대한 기능을 자동으로 활성화할 수 있습니다.

Amazon GuardDuty

Amazon GuardDuty는 악의적인 활동 및 무단 동작을 지속적으로 모니터링하여 AWS 계정 및 워크로드를 보호하는 위협 탐지 서비스입니다. 모니터링 및 감사 목적으로 항상 적절한 로그를 캡처하고 저장해야 하지만 GuardDuty는 AWS CloudTrail Amazon VPC 흐름 로그 및 AWS DNS 로그에서 직접 독립적인 데이터 스트림을 가져옵니다. Amazon S3 버킷 정책을 관리하거나 로그를 수집하고 저장하는 방법을 수정할 필요가 없습니다. GuardDuty 권한은 GuardDuty를 비활성화하여 언제든지 취소할 수 있는 서비스 연결 역할로 관리됩니다. 이렇게 하면 복잡한 구성 없이 서비스를 쉽게 활성화할 수 있으며, IAM 권한 수정 또는 S3 버킷 정책 변경이 서비스 운영에 영향을 미칠 위험을 제거할 수 있습니다.

기본 데이터 소스를 제공하는 것 외에도 GuardDuty는 보안 결과를 식별하는 선택적 기능을 제공합니다. 여기에는 EKS 보호, RDS 보호, S3 보호, 맬웨어 보호 및 Lambda 보호가 포함됩니다. 새 감지기의 경우 이러한 선택적 기능은 수동으로 활성화해야 하는 EKS 보호를 제외하고 기본적으로 활성화됩니다.

- GuardDuty S3 보호를 통해 GuardDuty는 기본 CloudTrail 관리 이벤트 외에도 CloudTrail의 Amazon S3 데이터 이벤트를 모니터링합니다. 데이터 이벤트를 모니터링하면 GuardDuty가 객체 수준 API 작업을 모니터링하여 S3 버킷 내의 데이터에 대한 잠재적 보안 위험을 모니터링할 수 있습니다.
- GuardDuty 맬웨어 보호는 연결된 Amazon Elastic Block Store(Amazon EBS) 볼륨에서 에이전트 없는 스캔을 시작하여 Amazon EC2 인스턴스 또는 컨테이너 워크로드에 맬웨어가 있는지 감지합니다. 또한 GuardDuty는 새로 업로드된 객체 또는 기존 객체의 새 버전을 스캔하여 S3 버킷에서 잠재적 맬웨어를 탐지합니다.
- GuardDuty RDS 보호는 데이터베이스 성능에 영향을 주지 않고 Amazon Aurora 데이터베이스에 대한 액세스 활동을 프로파일링하고 모니터링하도록 설계되었습니다.
- GuardDuty EKS 보호에는 EKS 감사 로그 모니터링 및 EKS 런타임 모니터링이 포함됩니다. EKS 감사 로그 모니터링을 통해 GuardDuty는 Amazon EKS 클러스터의 Kubernetes 감사 로그를 모니터링하고 잠재적으로 악의적이고 의심스러운 활동이 있는지 분석합니다. EKS 런타임 모니터링은 GuardDuty 보안 에이전트(Amazon EKS 추가 기능)를 사용하여 개별 Amazon EKS 워크로드에 대한 런타임 가시성을 제공합니다. GuardDuty 보안 에이전트는 잠재적으로 손상된 Amazon EKS 클러스터 내의 특정 컨테이너를 식별하는 데 도움이 됩니다. 또한 개별 컨테이너에서 기본 Amazon EC2 호스트 또는 더 광범위한 AWS 환경으로 권한을 에스컬레이션하려는 시도를 감지할 수 있습니다.

또한 GuardDuty는 데이터 소스, 여러 유형의 AWS 리소스 및 내의 시간에 걸친 다단계 공격을 자동으로 탐지하는 확장 위협 탐지라는 기능을 제공합니다 AWS 계정. GuardDuty는 신호라고 하는 이러한 이벤트를 상호 연관시켜 AWS 환경에 대한 잠재적 위협으로 나타나는 시나리오를 식별한 다음 공격 시퀀스 결과를 생성합니다. 여기에는 AWS 자격 증명 오용과 관련된 침해 및의 데이터 침해 시도와 관련된 위협 시나리오가 포함됩니다 AWS 계정. GuardDuty는 모든 공격 시퀀스 조사 결과 유형을 중요한 것으로 간주합니다. 이 기능은 기본적으로 활성화되어 있으며 이와 관련된 추가 비용은 없습니다.

AWS SRA에서 GuardDuty는를 통해 모든 계정에서 활성화되며 AWS Organizations, GuardDuty 위임된 관리자 계정(이 경우 Security Tooling 계정)의 적절한 보안 팀이 모든 결과를 보고 조치를 취할 수 있습니다. GuardDuty 활성 결과는 로그 아카이브 계정의 중앙 S3 버킷으로 내보내지므로 90일 후에도 결과를 유지할 수 있습니다. 결과는 위임된 관리자 계정에서 내보내며 동일한 리전에 있는 연결된 멤버 계정의 모든 결과도 포함합니다. S3 버킷의 결과는 AWS KMS 고객 관리형 키로 암호화됩니다. S3 버킷 정책 및 KMS 키 정책은 GuardDuty만 리소스를 사용하도록 구성됩니다.

AWS Security Hub CSPM 이 활성화되면 GuardDuty 조사 결과가 Security Hub CSPM 및 Security Hub로 자동으로 흐릅니다. Amazon Detective가 활성화되면 GuardDuty 조사 결과가 Detective 로그 수집 프로세스에 포함됩니다. GuardDuty 및 Detective는 교차 서비스 사용자 워크플로를 지원합니다. 여기서 GuardDuty는 선택한 결과에서 해당 결과를 조사하기 위해 큐레이션된 시각화 세트가 포함된 Detective 페이지로 리디렉션하는 콘솔의 링크를 제공합니다. 예를 들어 GuardDuty를 Amazon EventBridge와 통합하여 새 GuardDuty 결과에 대한 응답 자동화와 같은 GuardDuty 모범 사례를 자동화할 수도 있습니다. GuardDuty

> 구현 예제
>
> AWS SRA 코드 라이브러리는 GuardDuty의 샘플 구현을 제공합니다. 여기에는 AWS 조직의 모든 기존 및 향후 계정에 대한 암호화된 S3 버킷 구성, 위임된 관리 및 GuardDuty 활성화가 포함됩니다.

AWS Config

AWS Config는에서 지원되는 AWS 리소스의 구성을 평가, 감사 및 평가할 수 있는 서비스입니다 AWS 계정. AWS 리소스 구성을 AWS Config 지속적으로 모니터링 및 기록하고, 기록된 구성을 원하는 구성과 비교하여 자동으로 평가합니다. 또한 AWS Config 다른 서비스와 통합하여 자동화된 감사 및 모니터링 파이프라인에서 과중한 작업을 수행할 수 있습니다. 예를 들어는에서 개별 보안 암호의 변경 사항을 AWS Config 모니터링할 수 있습니다 AWS Secrets Manager.

를 사용하여 AWS 리소스의 구성 설정을 평가할 수 있습니다AWS Config 규칙.는 관리형 규칙이라고 하는 사용자 지정 가능하고 사전 정의된 규칙 라이브러리를 AWS Config 제공하거나 자체 사용자 지정

규칙을 작성할 수 있습니다. 사전 예방적 모드(리소스가 배포되기 전) 또는 탐지 모드(리소스가 배포된 후) AWS Config 규칙 에서를 실행할 수 있습니다. 구성 변경이 발생할 때, 주기적인 일정에 따라 또는 둘 다에 따라 리소스를 평가할 수 있습니다.

적합성 팩은 계정 및 리전 또는의 조직 전체에 단일 엔터티로 배포할 수 있는 AWS Config 규칙 및 문제 해결 작업의 모음입니다 AWS Organizations. 적합성 팩은 AWS Config 관리형 또는 사용자 지정 규칙 및 수정 작업 목록이 포함된 YAML 템플릿을 작성하여 생성됩니다. AWS 환경 평가를 시작하려면 샘플 적합성 팩 템플릿 중 하나를 사용합니다.

AWS Config 는와 통합되어 AWS Config 관리형 및 사용자 지정 규칙 평가 결과를 Security Hub CSPM으로 AWS Security Hub CSPM 보냅니다.

AWS Config 규칙 는와 함께 사용하여 규정 미준수 리소스를 AWS Systems Manager 효과적으로 해결할 수 있습니다. Systems Manager Explorer를 사용하여 AWS 계정 에서 규칙의 AWS Config 규정 준수 상태를 수집한 AWS 리전 다음 Systems Manager Automation 문서(런북)를 사용하여 규정 미준수 AWS Config 규칙을 해결합니다. 구현 세부 정보는 블로그 게시물 AWS Systems Manager 자동화 실행서를 사용하여 규정 미준수 AWS Config 규칙 수정을 참조하세요.

애그리게이터는 AWS Config 의 여러 계정, 리전 및 조직에서 구성 및 규정 준수 데이터를 수집합니다 AWS Organizations. 집계자 대시보드에는 집계된 리소스의 구성 데이터가 표시됩니다. 인벤토리 및 규정 준수 대시보드는 조직 전체 AWS 리전, AWS 계정전체 또는 조직 내 AWS AWS 리소스 구성 및 규정 준수 상태에 대한 필수 및 최신 정보를 제공합니다. 이를 통해 AWS Config 고급 쿼리를 작성할 필요 없이 AWS 리소스 인벤토리를 시각화하고 평가할 수 있습니다. 리소스별 규정 준수 요약, 규정 미준수 리소스가 있는 상위 10개 계정, 유형별 EC2 인스턴스 실행 및 중지 비교, 볼륨 유형 및 크기별 EBS 볼륨과 같은 필수 인사이트를 얻을 수 있습니다.

AWS Control Tower 를 사용하여 AWS 조직을 관리하는 경우 일련의 AWS Config 규칙을 탐지 가드레일로 배포합니다(필수, 적극 권장 또는 선택으로 분류됨). 이러한 가드레일은 리소스를 관리하고 AWS 조직의 계정 간 규정 준수를 모니터링하는 데 도움이 됩니다. 이러한 AWS Config 규칙은 값이 인 `aws-control-tower` 태그를 자동으로 사용합니다`managed-by-control-tower`.

AWS Config 는 AWS 조직의 각 멤버 계정에 대해 활성화되어야 하며 보호하려는 리소스가 AWS 리전 포함되어 있어야 합니다. AWS 조직 내 모든 계정에서 AWS Config 규칙을 중앙에서 관리(예: 생성, 업데이트 및 삭제)할 수 있습니다. AWS Config 위임된 관리자 계정에서 모든 계정에 공통 규칙 세트를 배포하고 AWS Config 규칙을 생성해서는 AWS Config 안 되는 계정을 지정할 수 있습니다. AWS Config 위임된 관리자 계정은 모든 멤버 계정의 리소스 구성 및 규정 준수 데이터를 집계하여 단일 보기를 제공할 수도 있습니다. 위임된 관리자 계정의 APIs를 사용하여 AWS 조직의 멤버 계정에서 기본 AWS Config 규칙을 수정할 수 없도록 하여 거버넌스를 적용합니다. Security Hub CSPM이 활성화되어 있고

하나 이상의 AWS Config 관리형 또는 사용자 지정 규칙이 있는 경우 AWS Security Hub CSPM는 기본적으로 결과를 전송하도록 통합 AWS Config 됩니다.

AWS SRA에서 AWS Config 위임된 관리자 계정은 보안 도구 계정입니다. AWS Config 전송 채널은 로그 아카이브 계정의 중앙 집중식 S3 버킷에 리소스 구성 스냅샷을 전송하도록 구성됩니다. 로그 아카이브 계정은 중앙 로그 리포지토리 저장소이므로 리소스 구성을 저장하는 데 사용됩니다.

설계 고려 사항

- AWS Config 는 구성 및 규정 준수 변경 알림을 Amazon EventBridge로 스트리밍합니다. 즉, EventBridge의 기본 필터링 기능을 사용하여AWS Config 이벤트를 필터링하여 특정 유형의 알림을 특정 대상으로 라우팅할 수 있습니다. 예를 들어 특정 규칙 또는 리소스 유형에 대한 규정 준수 알림을 특정 이메일 주소로 보내거나 구성 변경 알림을 외부 IT 서비스 관리(ITSM) 또는 구성 관리 데이터베이스(CMDB) 도구로 라우팅할 수 있습니다. 자세한 내용은 블로그 게시물 AWS Config 모범 사례를 참조하세요.
- AWS Config 사전 예방적 규칙 평가를 사용하는 것 외에도 리소스 구성 규정 준수를 사전에 확인하는 policy-as-code 평가 도구AWS CloudFormation Guard인를 사용할 수 있습니다. AWS CloudFormation Guard 명령줄 인터페이스(CLI)는 정책을 코드로 표현하는 데 사용할 수 있는 선언적 도메인별 언어(DSL)를 제공합니다. 또한 AWS CLI 명령을 사용하여 CloudFormation 변경 세트, JSON 기반 Terraform 구성 파일 또는 Kubernetes 구성과 같은 JSON 형식 또는 YAML 형식의 구조화된 데이터를 검증할 수 있습니다. AWS CloudFormation Guard CLI를 작성 프로세스의 일부로 사용하여 로컬에서 평가를 실행하거나 배포 파이프라인 내에서 실행할 수 있습니다. AWS Cloud Development Kit (AWS CDK) 애플리케이션이 있는 경우 cdk-nag를 사용하여 모범 사례를 사전에 확인할 수 있습니다.

구현 예제

AWS SRA 코드 라이브러리는 AWS 조직 내 모든 AWS 계정 및 리전에 AWS Config 적합성 팩을 배포하는 샘플 구현을 제공합니다. AWS Config 애그리게이터 모듈은 조직 관리 계정 내의 멤버 계정(보안 도구)에 관리를 위임한 다음 조직의 모든 기존 및 향후 계정에 대해 위임된 관리자 계정 내에서 AWS Config 애그리게이터를 구성 AWS Config 하여 애그리게이터를 AWS 구성하는 데 도움이 됩니다. AWS Config Control Tower 관리 계정 모듈을 사용하여 조직 관리 계정 AWS Config 내에서를 활성화할 수 있습니다.는 활성화하지 않습니다 AWS Control Tower.

Amazon Security Lake

Amazon Security Lake는 완전 관리형 보안 데이터 레이크 서비스입니다. Security Lake를 사용하여 AWS 환경, 서비스형 소프트웨어(SaaS) 공급자, 온프레미스 및 타사 소스의 보안 데이터를 자동으로 중앙 집중화할 수 있습니다. Security Lake를 사용하면 보안 데이터에 대한 분석 도구 사용을 간소화하는 정규화된 데이터 소스를 구축할 수 있으므로 조직 전체에서 보안 태세를 더 완벽하게 이해할 수 있습니다. 데이터 레이크는 Amazon Simple Storage Service(S3) 버킷에서 지원되며, 데이터에 대한 소유권은 사용자에게 있습니다. Security Lake는 Amazon VPC AWS 서비스, Amazon Route 53 AWS CloudTrail, Amazon S3, Amazon AWS Lambda EKS 감사 로그, AWS Security Hub CSPM 조사 결과 및 로그를 포함한 AWS WAF 로그를 자동으로 수집합니다.

AWS SRA는 로그 아카이브 계정을 Security Lake의 위임된 관리자 계정으로 사용할 것을 권장합니다. 위임된 관리자 계정 설정에 대한 자세한 내용은 보안 OU – 로그 아카이브 계정 섹션의 Amazon Security Lake를 참조하세요. Security Lake 데이터에 액세스하거나 사용자 지정 추출, 변환 및 로드(ETL) 함수를 사용하여 Security Lake 버킷에 기본이 아닌 로그를 작성하는 기능이 필요한 보안 팀은 Security Tooling 계정 내에서 운영되어야 합니다.

Security Lake는 다양한 클라우드 공급자의 로그, 타사 솔루션의 로그 또는 기타 사용자 지정 로그를 수집할 수 있습니다. Security Tooling 계정을 사용하여 ETL 함수를 수행하여 로그를 Open Cybersecurity Schema Framework(OCSF) 형식으로 변환하고 Apache Parquet 형식으로 파일을 출력하는 것이 좋습니다. Security Lake는 Security Tooling 계정과 Lambda 함수 또는 AWS Glue 크롤러가 지원하는 사용자 지정 소스에 대한 적절한 권한을 가진 교차 계정 역할을 생성하여 Security Lake용 S3 버킷에 데이터를 씁니다.

Security Lake 관리자는 Security Tooling 계정을 사용하고 Security Lake가 구독자로 수집하는 로그에 액세스해야 하는 보안 팀을 구성해야 합니다. Security Lake는 두 가지 유형의 구독자 액세스를 지원합니다.

- 데이터 액세스 - 구독자는 Security Lake용 Amazon S3 객체에 직접 액세스할 수 있습니다. Security Lake는 인프라와 권한을 관리합니다. Security Tooling 계정을 Security Lake 데이터 액세스 구독자로 구성하면 계정에 Amazon Simple Queue Service(Amazon SQS)를 통해 Security Lake 버킷의 새 객체에 대한 알림이 전송되고 Security Lake는 이러한 새 객체에 액세스할 수 있는 권한을 생성합니다.
- 쿼리 액세스 - 구독자는 Amazon Athena와 같은 서비스를 사용하여 S3 버킷의 AWS Lake Formation 테이블에서 소스 데이터를 쿼리할 수 있습니다. 교차 계정 액세스는 Lake Formation을 사용하여 쿼리 액세스를 위해 자동으로 설정됩니다. Security Tooling 계정을 Security Lake 쿼리 액세스 구독자로 구성하면 계정에 Security Lake 계정의 로그에 대한 읽기 전용 액세스 권한이 부여됩니다. 이 구독자 유형을 사용하면 Athena 및 AWS Glue 테이블이 Security Lake Log Archive 계정에서 AWS

Resource Access Manager ()를 통해 Security Tooling 계정과 공유됩니다AWS RAM. 이 기능을 활성화하려면 교차 계정 데이터 공유 설정을 버전 3 으로 업데이트해야 합니다.

구독자 생성에 대한 자세한 내용은 Security Lake 설명서의 구독자 관리를 참조하세요.

사용자 지정 소스 수집 모범 사례는 Security Lake 설명서의 사용자 지정 소스에서 데이터 수집을 참조하세요.

Amazon Quick Sight, Amazon OpenSearch Service 및 Amazon SageMaker를 사용하여 Security Lake에 저장하는 보안 데이터에 대한 분석을 설정할 수 있습니다.

> 설계 고려 사항
>
> 애플리케이션 팀이 비즈니스 요구 사항을 충족하기 위해 Security Lake 데이터에 대한 쿼리 액세스 권한이 필요한 경우 Security Lake 관리자는 해당 애플리케이션 계정을 구독 자로 구성해야 합니다.

Amazon Macie

Amazon Macie는 기계 학습 및 패턴 일치를 사용하여 민감한 데이터를 검색하고 보호하는 완전 관리형 데이터 보안 및 데이터 개인 정보 보호 서비스입니다 AWS. 적절한 제어가 적용되도록 워크로드가 처리 중인 데이터의 유형과 분류를 식별해야 합니다. Macie를 사용하면 민감한 데이터 자동 검색을 수행하고 민감한 데이터 검색 작업을 생성 및 실행하는 두 가지 방법으로 민감한 데이터의 검색 및 보고를 자동화할 수 있습니다. 민감한 데이터 자동 검색을 통해 Macie는 매일 S3 버킷 인벤토리를 평가하고 샘플링 기술을 사용하여 버킷에서 대표적인 S3 객체를 식별하고 선택합니다. 그런 다음 Macie는 선택한 객체를 검색 및 분석하여 민감한 데이터가 있는지 검사합니다. 민감한 데이터 검색 작업은 더 심층적이고 더 대상화된 분석을 제공합니다. 이 옵션을 사용하면 분석할 S3 버킷, 샘플링 깊이, S3 객체의 속성에서 파생되는 사용자 지정 기준을 포함하여 분석의 폭과 깊이를 정의할 수 있습니다. Macie가 버킷의 보안 또는 프라이버시와 관련된 잠재적 문제를 탐지하면 Macie가 정책 조사 결과를 생성합니다. 자동 데이터 검색은 모든 신규 Macie 고객에게 기본적으로 활성화되어 있으며 기존 Macie 고객은 클릭 한 번으로 활성화할 수 있습니다.

Macie는를 통해 모든 계정에서 활성화됩니다 AWS Organizations. 위임된 관리자 계정(이 경우 Security Tooling 계정)에 적절한 권한이 있는 보안 주체는 모든 계정에서 Macie를 활성화 또는 일시 중지하고, 멤버 계정이 소유한 버킷에 대한 민감한 데이터 검색 작업을 생성하고, 모든 멤버 계정에 대한 모든 정책 조사 결과를 볼 수 있습니다. 민감한 데이터 조사 결과는 민감한 조사 결과 작업을 생성한 계

정에서만 볼 수 있습니다. 자세한 내용은 Macie 설명서의 조직으로 여러 Macie 계정 관리를 참조하세요.

Macie 조사 결과는 검토 및 분석을 AWS Security Hub CSPM 위해 로 전달됩니다. 또한 Macie는 Amazon EventBridge와 통합되어 알림, 보안 정보 및 이벤트 관리(SIEM) 시스템에 대한 피드, 자동 문제 해결과 같은 결과에 대한 자동 응답을 용이하게 합니다.

설계 고려 사항

- S3 객체가 관리하는 AWS Key Management Service (AWS KMS) 키로 암호화된 경우 Macie가 데이터를 스캔할 수 있도록 해당 KMS 키에 Macie 서비스 연결 역할을 키 사용자로 추가할 수 있습니다.
- Macie는 Amazon S3에서 객체를 스캔하는 데 최적화되어 있습니다. 따라서 Amazon S3에 배치할 수 있는 모든 Macie 지원 객체 유형(영구 또는 임시)에서 민감한 데이터를 스캔할 수 있습니다. 즉, Amazon Relational Database Service(RDS) 또는 Amazon Aurora 데이터베이스의 주기적 스냅샷 내보내기, 내보 낸 Amazon DynamoDB 테이블 또는 네이티브 또는 타사 애플리케이션에서 추출한 텍스트 파일과 같은 다른 소스의 데이터를 Amazon S3로 이동하여 Macie가 평가할 수 있습니다.

구현 예제

AWS SRA 코드 라이브러리는 Amazon Macie의 샘플 구현을 제공합니다. 여기에는 멤버 계정에 관리를 위임하고 AWS 조직의 모든 기존 및 향후 계정에 대해 위임된 관리자 계정 내에서 Macie를 구성하는 작업이 포함됩니다. Macie는에서 고객 관리형 키로 암호화된 중앙 S3 버킷으로 조사 결과를 보내도록 구성되어 있습니다 AWS KMS.

IAM Access Analyzer

AWS 클라우드 채택 여정을 가속화하고 계속 혁신함에 따라 세분화된 액세스(권한)를 엄격하게 제어하고, 액세스 확산을 억제하고, 권한이 효과적으로 사용되도록 하는 것이 중요합니다. 과도하게 사용하지 않는 액세스는 보안 문제를 야기하며 기업이 최소 권한 원칙을 적용하기가 더 어려워집니다. 이 원칙은 보안 요구 사항과 운영 및 애플리케이션 개발 요구 사항의 균형을 맞추기 위해 지속적으로 적절한 크기의 IAM 권한을 포함하는 중요한 보안 아키텍처 원칙입니다. 이러한 노력에는 중앙 보안 및 Cloud Center of Excellence(CCoE) 팀과 분산된 개발 팀을 비롯한 여러 이해관계자 페르소나가 포함됩니다.

AWS Identity and Access Management Access Analyzer는 엔터프라이즈 보안 표준을 충족하는 데 도움이 되도록 미사용 액세스를 제거하여 세분화된 권한을 효율적으로 설정하고, 의도한 권한을 확인하고, 권한을 구체화하는 도구를 제공합니다. 대시보드 및를 통해 AWS 리소스에 대한 외부 및 내부 액세스와 미사용 액세스 조사 결과에 대한 가시성을 제공합니다AWS Security Hub CSPM. 또한 이벤트 기반 사용자 지정 알림 및 문제 해결 워크플로를 위해 Amazon EventBridge를 지원합니다.

IAM Access Analyzer 외부 액세스 분석기 조사 결과 기능은 외부 엔터티와 공유되는 Amazon S3 버킷 또는 IAM 역할과 같은 AWS 조직 및 계정의 리소스를 식별하는 데 도움이 됩니다. 선택한 AWS 조직 또는 계정을 신뢰 영역이라고 합니다. 분석기는 자동 추론을 사용하여 신뢰 영역 내에서 지원되는 모든 리소스를 분석하고 신뢰 영역 외부에서 리소스에 액세스할 수 있는 보안 주체에 대한 결과를 생성합니다. 이러한 결과는 외부 엔터티와 공유되는 리소스를 식별하고 리소스 권한을 배포하기 전에 정책이 리소스에 대한 퍼블릭 및 크로스 계정 액세스에 미치는 영향을 미리 보는 데 도움이 됩니다. 추가 비용 없이 사용할 수 있습니다.

마찬가지로 IAM Access Analyzer 내부 액세스 분석기 결과 기능은 AWS 조직 내 리소스와 조직 또는 계정 내 내부 보안 주체와 공유되는 계정을 식별하는 데 도움이 됩니다. 이 분석은 조직 내 의도한 보안 주체만 지정된 리소스에 액세스할 수 있도록 하여 최소 권한 원칙을 지원합니다. 이는 유료 기능이며 검사할 리소스의 명시적 구성이 필요합니다. 이 기능을 신중하게 사용하여 설계상 내부적으로도 잠가야 하는 민감한 특정 리소스를 모니터링합니다.

또한 IAM Access Analyzer 조사 결과는 다음을 포함하여 조직 및 계정에 부여된 미사용 액세스를 식별하는 데 도움이 됩니다. AWS

- 미사용 IAM 역할 - 지정된 사용 기간 내에 액세스 활동이 없는 역할입니다.
- 미사용 IAM 사용자, 자격 증명 및 액세스 키 - IAM 사용자에게 속하고 AWS 서비스 및 리소스에 액세스하는 데 사용되는 자격 증명입니다.
- 미사용 IAM 정책 및 권한 - 지정된 사용 기간 내에 역할이 사용하지 않은 서비스 수준 및 작업 수준 권한입니다. IAM Access Analyzer는 역할에 연결된 자격 증명 기반 정책을 사용하여 해당 역할이 액세스할 수 있는 서비스 및 작업을 결정합니다. 분석기는 모든 서비스 수준 권한에 대한 미사용 권한을 검토합니다.

IAM Access Analyzer에서 생성된 조사 결과를 사용하여 조직의 정책 및 보안 표준에 따라 의도하지 않거나 사용되지 않은 액세스를 파악하고 수정할 수 있습니다. 문제 해결 후 이러한 결과는 다음에 분석기를 실행할 때 해결 된 것으로 표시됩니다. 조사 결과가 의도적인 경우 IAM Access Analyzer에 아카이브 된 것으로 표시하고 보안 위험이 더 큰 다른 조사 결과의 우선순위를 지정할 수 있습니다. 또한 특정 결과를 자동으로 아카이브하도록 아카이브 규칙을 설정할 수 있습니다. 예를 들어, 정기적으로 액세

스 권한을 부여한 특정 Amazon S3 버킷에 대한 조사 결과를 자동으로 아카이브하는 아카이브 규칙을 생성할 수 있습니다.

빌더는 IAM Access Analyzer를 사용하여 개발 및 배포(CI/CD) 프로세스 초기에 자동화된 IAM 정책 검사를 수행하여 기업 보안 표준을 준수할 수 있습니다. IAM Access Analyzer 사용자 지정 정책 확인 및 정책 검토를와 통합하여 개발 팀의 CI/CD 파이프라인의 일부로 정책 검토를 자동화 AWS CloudFormation 할 수 있습니다. 여기에는 다음이 포함됩니다.

- IAM 정책 검증 - IAM Access Analyzer는 IAM 정책 문법 및 AWS 모범 사례를 기준으로 정책을 검증합니다. 보안 경고, 오류, 일반 경고 및 정책에 대한 제안을 포함하여 정책 검증 검사에 대한 결과를 볼 수 있습니다. 현재 100개 이상의 정책 검증 검사를 사용할 수 있으며 AWS Command Line Interface (AWS CLI) 및 APIs.
- IAM 사용자 지정 정책 검사 - IAM Access Analyzer 사용자 지정 정책 검사는 지정된 보안 표준에 따라 정책을 검증합니다. 사용자 지정 정책 검사는 자동 추론을 사용하여 기업 보안 표준을 충족하는 데 더 높은 수준의 보장을 제공합니다. 사용자 지정 정책 검사 유형은 다음과 같습니다.
  - 참조 정책을 기준으로 확인: 정책을 편집할 때 정책의 기존 버전과 같은 참조 정책과 비교하여 업데이트가 새 액세스 권한을 부여하는지 확인할 수 있습니다. CheckNoNewAccess API는 두 정책(업데이트된 정책과 참조 정책)을 비교하여 업데이트된 정책이 참조 정책에 대한 새 액세스를 도입하는지 여부를 확인하고 통과 또는 실패 응답을 반환합니다.
  - IAM 작업 목록과 대조 확인: CheckAccessNotGranted API를 사용하여 정책이 보안 표준에 정의된 중요 작업 목록에 대한 액세스 권한을 부여하지 않는지 확인할 수 있습니다. 이 API는 정책과 최대 100개의 IAM 작업 목록을 가져와서 정책이 하나 이상의 작업을 허용하는지 확인하고 통과 또는 실패 응답을 반환합니다.

보안 팀과 기타 IAM 정책 작성자는 IAM Access Analyzer를 사용하여 IAM 정책 문법 및 보안 표준을 준수하는 정책을 작성할 수 있습니다. 적절한 크기의 정책을 수동으로 작성하면 오류가 발생하기 쉽고 시간이 많이 걸릴 수 있습니다. IAM Access Analyzer 정책 생성 기능은 보안 주체의 액세스 활동을 기반으로 하는 IAM 정책을 작성하는 데 도움이 됩니다. IAM Access Analyzer는 지원되는 서비스에 대한 AWS CloudTrail 로그를 검토하고 지정된 날짜 범위에서 보안 주체가 사용한 권한이 포함된 정책 템플릿을 생성합니다. 그런 다음이 템플릿을 사용하여 필요한 권한만 부여하는 세분화된 권한으로 정책을 생성할 수 있습니다.

- 계정에서 액세스 활동을 기반으로 정책을 생성하려면 CloudTrail 추적이 활성화되어 있어야 합니다.
- IAM Access Analyzer는 생성된 정책에서 Amazon S3 데이터 이벤트와 같은 데이터 이벤트에 대한 작업 수준 활동을 식별하지 않습니다.
- `iam:PassRole` 작업은 CloudTrail에서 추적되지 않으며 생성된 정책에 포함되지 않습니다.

IAM Access Analyzer는의 위임된 관리자 기능을 통해 보안 도구 계정에 배포됩니다 AWS Organizations. 위임된 관리자는 AWS 조직을 신뢰 영역으로 사용하여 분석기를 생성하고 관리할 수 있는 권한이 있습니다.

> **설계 고려 사항**
>
> 계정 범위 조사 결과(계정이 신뢰할 수 있는 경계 역할을 하는 경우)를 가져오려면 각 멤버 계정에 계정 범위 분석기를 생성합니다. 이는 계정 파이프라인의 일부로 수행할 수 있습니다. 계정 범위 조사 결과는 멤버 계정 수준에서 Security Hub CSPM으로 전달됩니다. 여기에서 Security Hub CSPM 위임된 관리자 계정(보안 도구)으로 이동합니다.

> **구현 예제**
>
> - AWS SRA 코드 라이브러리는 IAM Access Analyzer의 샘플 구현을 제공합니다. 위임된 관리자 계정 내에서 조직 수준 분석기를 구성하고 각 계정 내에서 계정 수준 분석기를 구성하는 방법을 보여줍니다.
> - 사용자 지정 정책 검사를 빌더 워크플로에 통합하는 방법에 대한 자세한 내용은 AWS 블로그 게시물 IAM Access Analyzer 사용자 지정 정책 검사 소개를 참조하세요.

AWS Firewall Manager

AWS Firewall Manager는 여러 계정 및 리소스에서 AWS WAF, AWS Network Firewall, AWS Shield Advanced Amazon VPC 보안 그룹 및 Amazon Route 53 Resolver DNS 방화벽에 대한 관리 및 유지 관리 작업을 간소화하여 네트워크를 보호합니다. Firewall Manager를 사용하면 AWS WAF 방화벽 규칙, Shield Advanced 보호, Amazon VPC 보안 그룹, Network Firewall 방화벽 및 DNS 방화벽 규칙 그룹 연결을 한 번만 설정합니다. 새 계정을 추가하는 즉시 서비스에서 계정과 리소스 전체에 규칙과 보호가 자동으로 적용됩니다.

Firewall Manager는 소수의 특정 계정 및 리소스 대신 전체 AWS 조직을 보호하거나 보호하려는 새 리소스를 자주 추가할 때 특히 유용합니다. Firewall Manager는 보안 정책을 사용하여 배포해야 하는 관련 규칙, 보호 및 작업과 포함하거나 제외할 계정 및 리소스(태그로 표시됨)를 포함한 구성 세트를 정의할 수 있습니다. 세분화되고 유연한 구성을 생성하는 동시에 많은 수의 계정 및 VPCs. 이러한 정책은 새 계정과 리소스가 생성되더라도 사용자가 구성하는 규칙을 자동으로 일관되게 적용합니다. Firewall Manager는를 통해 모든 계정에서 활성화되며 AWS Organizations Firewall Manager 위임된 관리자 계정(이 경우 Security Tooling 계정)의 적절한 보안 팀이 구성 및 관리를 수행합니다.

보호하려는 리소스 AWS 리전 가 포함된 각에 AWS Config 대해를 활성화해야 합니다. 모든 리소스 AWS Config 에 대해를 활성화하지 않으려면 사용하는 Firewall Manager 정책 유형과 연결된 리소스에 대해 활성화해야 합니다. AWS Security Hub CSPM 및 Firewall Manager를 모두 사용하는 경우 Firewall Manager는 조사 결과를 Security Hub CSPM으로 자동으로 전송합니다. Firewall Manager는 규정을 준수하지 않는 리소스 및 탐지한 공격에 대한 조사 결과를 생성하고 조사 결과를 Security Hub CSPM으로 전송합니다. 에 대한 Firewall Manager 정책을 설정할 때 모든 범위 내 계정에 대해 웹 액세스 제어 목록(웹 ACLs)에 대한 로깅을 중앙에서 활성화하고 단일 계정에서 로그를 중앙 집중화 AWS WAF할 수 있습니다.

Firewall Manager를 사용하면 조직의 방화벽 리소스를 관리할 수 있는 한 명 또는 여러 명의 관리자가 있을 수 있습니다. 여러 관리자를 할당할 때 제한적인 관리 범위 조건을 적용하여 각 관리자가 관리할 수 있는 리소스(계정, OUs, 리전, 정책 유형)를 정의할 수 있습니다. 이렇게 하면 조직 내에서 다양한 관리자 역할을 유연하게 사용할 수 있으며, 최소 권한 액세스 담당자를 유지할 수 있습니다. AWS SRA는 전체 관리 범위가 Security Tooling 계정에 위임된 하나의 관리자를 사용합니다.

> 설계 고려 사항
>
> AWS 조직 내 개별 멤버 계정의 계정 관리자는 특정 요구 사항에 따라 Firewall Manager 관리형 서비스에서 추가 제어(예: AWS WAF 규칙 및 Amazon VPC 보안 그룹)를 구성할 수 있습니다.

> 구현 예제
>
> AWS SRA 코드 라이브러리는 Firewall Manager의 샘플 구현을 제공합니다. 위임된 관리(보안 도구)를 보여주고, 허용되는 최대 보안 그룹을 배포하고, 보안 그룹 정책을 구성하고, 여러 AWS WAF 정책을 구성합니다.

Amazon EventBridge

Amazon EventBridge는 애플리케이션을 다양한 소스의 데이터와 간단하게 연결할 수 있는 서버리스 이벤트 버스 서비스입니다. 보안 자동화에 자주 사용합니다. 라우팅 규칙을 설정하여 데이터를 전송할 위치를 결정하여 모든 데이터 소스에 실시간으로 반응하는 애플리케이션 아키텍처를 구축할 수 있습니다. 사용자 지정 이벤트 버스를 생성하여 각 계정의 기본 이벤트 버스를 사용하는 것 외에도 사용자 지정 애플리케이션에서 이벤트를 수신할 수 있습니다. Security Tooling 계정에서 AWS 조직의 다른 계정으로부터 보안 관련 이벤트를 수신할 수 있는 이벤트 버스를 생성할 수 있습니다. 예를 들어 AWS

Config 규칙, Amazon GuardDuty 및를 EventBridge AWS Security Hub CSPM 와 연결하면 보안 데이터를 라우팅하고, 알림을 생성하고, 문제를 해결하기 위한 작업을 관리하기 위한 유연하고 자동화된 파이프라인을 생성할 수 있습니다.

설계 고려 사항

- EventBridge는 여러 대상으로 이벤트를 라우팅할 수 있습니다. 보안 작업을 자동화하는 한 가지 중요한 패턴은 적절한 조치를 취하는 개별 AWS Lambda 대응자에게 특정 이벤트를 연결하는 것입니다. 예를 들어, 특정 상황에서는 EventBridge를 사용하여 버킷 정책을 수정하고 퍼블릭 권한을 제거하는 Lambda 응답기로 퍼블릭 S3 버킷 결과를 라우팅할 수 있습니다. 이러한 대응 담당자는 조사 플레이북 및 런북에 통합되어 대응 활동을 조정할 수 있습니다.
- 성공적인 보안 운영 팀의 모범 사례는 보안 이벤트 및 조사 결과의 흐름을 티켓팅 시스템, 버그/문제 시스템 또는 다른 보안 정보 및 이벤트 관리(SIEM) 시스템과 같은 알림 및 워크플로 시스템에 통합하는 것입니다. 이렇게 하면 워크플로가 이메일 및 정적 보고서에서 제거되고 이벤트 또는 결과를 라우팅, 에스컬레이션 및 관리하는 데 도움이 됩니다. EventBridge의 유연한 라우팅 기능은이 통합을 위한 강력한 활성화 도구입니다.

Amazon Detective

Amazon Detective는 보안 분석가를 위한 보안 조사 결과 또는 의심스러운 활동의 근본 원인을 쉽게 분석, 조사 및 식별할 수 있도록 하여 대응형 보안 제어 전략을 지원합니다. Detective는 로그 및 Amazon VPC 흐름 AWS CloudTrail 로그에서 로그인 시도, API 호출, 네트워크 트래픽과 같은 시간 기반 이벤트를 자동으로 추출합니다. Detective는 CloudTrail 로그 및 Amazon VPC 흐름 로그의 독립적인 스트림을 사용하여 이러한 이벤트를 사용합니다. Detective를 사용하여 최대 1년의 과거 이벤트 데이터에 액세스할 수 있습니다. Detective는 기계 학습 및 시각화를 사용하여 시간 경과에 따른 리소스의 동작과 상호 작용에 대한 통합된 대화형 보기를 생성합니다. 이를 동작 그래프라고 합니다. 동작 그래프를 탐색하여 실패한 로그온 시도 또는 의심스러운 API 호출과 같은 서로 다른 작업을 검사할 수 있습니다.

Detective는 Amazon Security Lake와 통합되어 보안 분석가가 Security Lake에 저장된 로그를 쿼리하고 검색할 수 있도록 합니다. 이 통합을 사용하면 Detective에서 보안 조사를 수행하는 동안 Security Lake에 저장된 CloudTrail 로그 및 Amazon VPC 흐름 로그에서 추가 정보를 가져올 수 있습니다.

또한 Detective는 Amazon GuardDuty GuardDuty에서 탐지된 결과를 수집합니다. 계정이 Detective를 활성화하면 동작 그래프의 관리자 계정이 됩니다. Detective를 활성화하기 전에 계정이 최소 48시간 동안 GuardDuty에 등록되었는지 확인합니다. 이 요구 사항을 충족하지 않으면 DetectiveDetective 활성화할 수 없습니다.

Detective에 대한 추가 선택적 데이터 소스에는 Amazon EKS 감사 로그 및가 포함됩니다 AWS Security Hub CSPM. Amazon EKS 감사 로그 데이터 소스는 Amazon EKS 클러스터, Kubernetes 포드, 컨테이너 이미지 및 Kubernetes 주체와 같은 엔터티 유형에 대해 제공되는 정보를 개선합니다. Security Hub 데이터 소스는 제품 전반의 AWS 결과를 Security Hub로 상호 연관시키고 Detective로 수집하는 보안 조사 결과의 일부입니다.

Detective는 단일 보안 손상 이벤트와 관련된 여러 조사 결과를 조사 결과 그룹으로 자동으로 그룹화합니다. 위협 행위자는 일반적으로 시간과 리소스에 분산된 여러 보안 조사 결과를 초래하는 일련의 작업을 수행합니다. 따라서 조사 결과 그룹은 여러 엔터티 및 조사 결과와 관련된 조사의 시작점이어야 합니다. 또한 Detective는 결과 그룹을 자동으로 분석하고 자연어로 인사이트를 제공하여 보안 조사를 가속화하는 생성형 AI를 사용하여 결과 그룹 요약을 제공합니다.

Detective는와 통합됩니다 AWS Organizations. 조직 관리 계정은 멤버 계정을 Detective 관리자 계정으로 위임합니다. AWS SRA에서 이는 보안 도구 계정입니다. Detective 관리자 계정은 조직의 모든 현재 멤버 계정을 Detective 멤버 계정으로 자동으로 활성화하고 AWS 조직에 추가될 때 새 멤버 계정을 추가할 수 있습니다. 또한 Detective 관리자 계정은 현재 AWS 조직에 속하지 않지만 동일한 리전 내에 있는 멤버 계정을 초대하여 기본 계정의 동작 그래프에 데이터를 제공할 수 있습니다. 멤버 계정이 초대를 수락하고 활성화되면 Detective는 멤버 계정의 데이터를 수집하여 해당 동작 그래프로 추출하기 시작합니다.

> 설계 고려 사항
>
> GuardDuty 및 AWS Security Hub CSPM 콘솔에서 Detective 결과 프로필로 이동할 수 있습니다. 이러한 링크는 조사 프로세스를 간소화하는 데 도움이 될 수 있습니다. 계정은 Detective와 피벗하려는 서비스(GuardDuty 또는 Security Hub CSPM) 모두에 대한 관리 계정이어야 합니다. 기본 계정이 서비스에 대해 동일한 경우 통합 링크가 원활하게 작동합니다.

AWS Audit Manager

AWS Audit Manager를 사용하면 AWS 사용량을 지속적으로 감사하여 감사 및 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다. 이를 통해 증거를 수동으로 수집, 검토 및 관리하는 것에서 증거 수집을 자동화하고, 감사 증거의 출처를 추적하고, 공동 작업을 활성화하고, 증거 보안 및 무결성을 관리하는 데 도움이 되는 솔루션으로 이동할 수 있습니다. 감사 시기에 Audit Manager는 귀하의 컨트롤에 대한 이해 관계자들의 검토를 관리할 수 있습니다.

Audit Manager를 사용하면 인터넷 보안 센터(CIS) 벤치마크, CIS AWS 파운데이션 벤치마크, 시스템 및 조직 제어 2(SOC 2), 결제 카드 산업 데이터 보안 표준(PCI DSS)과 같은 사전 구축된 프레임워크에

대해 감사할 수 있습니다. 또한 내부 감사에 대한 특정 요구 사항에 따라 표준 또는 사용자 지정 제어를 사용하여 자체 프레임워크를 생성할 수 있습니다.

Audit Manager는 네 가지 유형의 증거를 수집합니다. AWS Config 및의 규정 준수 검사 증거 AWS Security Hub CSPM,의 관리 이벤트 증거 AWS CloudTrail, AWS service-to-service API 호출의 구성 증거 등 세 가지 유형의 증거가 자동화됩니다. 자동화할 수 없는 증거의 경우 Audit Manager를 사용하여 수동 증거를 업로드할 수 있습니다.

기본적으로 Audit Manager의 데이터는 AWS 관리형 키를 사용하여 암호화됩니다. AWS SRA는 암호화에 고객 관리형 키를 사용하여 논리적 액세스를 더 효과적으로 제어합니다. 또한 Audit Manager가 평가 보고서를 게시 AWS 리전 하는에서 S3 버킷을 구성해야 합니다. 이 버킷은 고객 관리형 키로 암호화되어야 하며 Audit Manager만 보고서를 게시할 수 있도록 구성된 버킷 정책이 있어야 합니다.

> **Note**
>
> Audit Manager는 특정 규정 준수 표준 및 규정 준수 확인과 관련된 증거 수집을 지원합니다. 그러나 규정 준수를 평가하지는 않습니다. 따라서 Audit Manager를 통해 수집된 증거에는 감사에 필요한 운영 프로세스에 대한 세부 정보가 포함되지 않을 수 있습니다. Audit Manager는 법률 고문 또는 규정 준수 전문가를 대체하지 않습니다. 평가 대상 규정 준수 프레임워크(들)에 대한 인증을 받은 타사 평가자의 서비스를 이용하는 것이 좋습니다.

Audit Manager 평가는 AWS 조직의 여러 계정에서 실행할 수 있습니다. Audit Manager는 증거를 수집하여의 위임된 관리자 계정으로 통합합니다 AWS Organizations. 이 감사 기능은 주로 규정 준수 및 내부 감사 팀에서 사용하며에 대한 읽기 액세스 권한만 필요합니다 AWS 계정.

> **설계 고려 사항**
>
> - Audit Manager는 위험 관리 프레임워크를 구현 AWS Config 하는 데 도움이 되도록 AWS Security Hub CSPM및 AWS Security Hub와 같은 다른 AWS 보안 서비스를 보완합니다. Audit Manager는 독립적인 위험 보증 기능을 제공하는 반면, Security Hub CSPM은 위험을 감독하는 데 도움이 AWS Config 되고 적합성 팩은 위험을 관리하는 데 도움이 됩니다. IIA(Institute of Internal Auditors)에서 개발한 3줄 모델에 익숙한 감사 전문가는이 조합이 세 줄의 방어에 AWS 서비스 도움이 된다는 점에 유의해야 합니다. 자세한 내용은 AWS 클라우드 운영 및 마이그레이션 블로그의 두 부분으로 구성된 블로그 시리즈를 참조하세요.

- Audit Manager가 Security Hub CSPM 증거를 수집하려면 두 서비스의 위임된 관리자 계정이 동일해야 합니다 AWS 계정. 따라서 AWS SRA에서 보안 도구 계정은 Audit Manager의 위임된 관리자입니다.

AWS Artifact

AWS Artifact는 보안 도구 계정 내에서 호스팅되어 규정 준수 아티팩트 관리 기능을 AWS 조직 관리 계정과 분리합니다. 반드시 필요한 경우가 아니면 배포에 AWS 조직 관리 계정을 사용하지 않는 것이 좋습니다. 대신 멤버 계정에 배포를 전달합니다. 감사 아티팩트 관리는 멤버 계정에서 수행할 수 있고 함수는 보안 및 규정 준수 팀과 밀접하게 일치하므로 보안 도구 계정은 관리자 계정으로 지정됩니다 AWS Artifact. AWS Artifact 보고서를 사용하여 AWS ISO 인증, 결제 카드 산업(PCI), 시스템 및 조직 제어(SOC) 보고서와 같은 AWS 보안 및 규정 준수 문서를 다운로드할 수 있습니다.

AWS Artifact 는 위임된 관리 기능을 지원하지 않습니다. 대신이 기능을 감사 및 규정 준수 팀과 관련된 보안 도구 계정의 IAM 역할로만 제한하여 필요에 따라 외부 감사자에게 해당 보고서를 다운로드, 검토 및 제공할 수 있습니다. IAM 정책을 통해 특정 AWS Artifact 보고서에만 액세스할 수 있도록 특정 IAM 역할을 추가로 제한할 수 있습니다. 샘플 IAM 정책은 AWS Artifact 설명서를 참조하세요.

> 설계 고려 사항
>
> 감사 및 규정 준수 팀 AWS 계정 전용를 사용하기로 선택한 경우 보안 도구 계정과 별도의 보안 감사 계정 AWS Artifact 에서를 호스팅할 수 있습니다. AWS Artifact 보고서는 조직이 문서화된 프로세스를 따르고 있거나 특정 요구 사항을 충족하고 있음을 입증하는 증거를 제공합니다. 감사 아티팩트는 시스템 개발 수명 주기 전반에 걸쳐 수집 및 보관되며 내부 또는 외부 감사 및 평가에서 증거로 사용할 수 있습니다.

AWS KMS

AWS Key Management Service (AWS KMS)를 사용하면 암호화 키를 생성 및 관리하고 광범위한 및 애플리케이션에서 암호화 키의 AWS 서비스 사용을 제어할 수 있습니다. AWS KMS 는 하드웨어 보안 모듈을 사용하여 암호화 키를 보호하는 안전하고 복원력이 뛰어난 서비스입니다. 키의 저장, 교체 및 액세스 제어와 같은 키 구성 요소에 대한 업계 표준 수명 주기 프로세스를 따릅니다. AWS KMS 는 암호화 및 서명 키로 데이터를 보호하는 데 도움이 될 수 있으며 AWS 암호화 SDK를 통해 서버 측 암호화와 클라이언트 측 암호화 모두에 사용할 수 있습니다. 보호 및 유연성을 위해는 고객 관리형 키, AWS 관리형 키 및 AWS 소유 키의 세 가지 유형의 키를 AWS KMS 지원합니다. 고객 관리형 키는 AWS 계정 사용자가 생성, 소유 및 관리하는의 AWS KMS 키입니다. AWS 관리형 키는와 통합된 AWS KMS 에

서 사용자를 대신하여 생성, 관리 및 사용하는 계정의 키 AWS 서비스 입니다 AWS KMS. AWS 소유 키는가 여러에서 사용하기 위해 AWS 서비스 소유하고 관리하는 AWS KMS 키 모음입니다 AWS 계정. AWS KMS 키 사용에 대한 자세한 내용은 AWS KMS 설명서 및 AWS KMS 암호화 세부 정보를 참조하세요.

한 가지 배포 옵션은 AWS KMS 키와 IAM 정책의 조합을 사용하여 애플리케이션 리소스별로 애플리케이션 계정의 키 사용 기능을 위임하면서 키 관리 책임을 단일 계정으로 중앙 집중화하는 것입니다. 이 접근 방식은 안전하고 관리하기 쉽지만 제한 제한, 계정 서비스 제한, 보안 팀이 운영 키 관리 작업으로 인해 장애물 AWS KMS 이 발생할 수 있습니다. 또 다른 배포 옵션은가 여러 계정에 상주 AWS KMS 하도록 허용하는 분산 모델을 보유하는 것이며, 특정 계정의 인프라 및 워크로드를 담당하는 사용자가 자체 키를 관리할 수 있도록 허용하는 것입니다. 이 모델은 워크로드 팀에 암호화 키 사용에 대한 제어, 유연성 및 민첩성을 제공합니다. 또한 API 제한을 피하고 영향 범위를 하나로 AWS 계정 만 제한하며 보고, 감사 및 기타 규정 준수 관련 작업을 간소화하는 데 도움이 됩니다. 분산형 모델에서는 분산형 키가 동일한 방식으로 관리되고 키 사용이 AWS KMS 설정된 모범 사례 및 정책에 따라 감사되도록 가드레일을 배포하고 적용하는 것이 중요합니다. 자세한 내용은 AWS Key Management Service 모범 사례 백서를 참조하세요. AWS SRA는 키가 사용되는 계정 내에서 로컬로 상주하는 분산 AWS KMS 키 관리 모델을 권장합니다. 모든 암호화 함수에 대해 단일 계정에서 단일 키를 사용하지 않는 것이 좋습니다. 키는 함수 및 데이터 보호 요구 사항에 따라 생성하고 최소 권한 원칙을 적용할 수 있습니다. 경우에 따라 암호화 권한은 복호화 권한과 별도로 유지되며 관리자는 수명 주기 함수를 관리하지만 자신이 관리하는 키로 데이터를 암호화하거나 복호화할 수 없습니다.

Security Tooling 계정에서는 조직에서 관리하는 AWS CloudTrail 조직 추적과 같은 중앙 집중식 보안 서비스의 암호화를 AWS 관리하는 데 AWS KMS 사용됩니다.

AWS Private CA

AWS Private Certificate Authority (AWS Private CA)는 EC2 인스턴스, 컨테이너, IoT 디바이스 및 온프레미스 리소스에 대한 프라이빗 최종 엔터티 TLS 인증서의 수명 주기를 안전하게 관리하는 데 도움이 되는 관리형 프라이빗 CA 서비스입니다. 이를 통해 실행 중인 애플리케이션에 대한 암호화된 TLS 통신을 허용합니다. 를 사용하면 자체 CA 계층 구조(루트 CA, 하위 CAs를 통해 최종 엔터티 인증서까지)를 생성하고 인증서를 발급하여 내부 사용자 AWS Private CA, 컴퓨터, 애플리케이션, 서비스, 서버 및 기타 디바이스를 인증하고 컴퓨터 코드에 서명할 수 있습니다. 프라이빗 CA에서 발급한 인증서는 인터넷이 아닌 AWS 조직 내에서만 신뢰할 수 있습니다.

퍼블릭 키 인프라(PKI) 또는 보안 팀은 모든 PKI 인프라를 관리할 책임이 있습니다. 여기에는 프라이빗 CA의 관리 및 생성이 포함됩니다. 그러나 워크로드 팀이 인증서 요구 사항을 자체적으로 처리할 수 있도록 허용하는 프로비저닝이 있어야 합니다. AWS SRA는 루트 CA가 보안 도구 계정 내에서 호스팅되는 중앙 집중식 CA 계층 구조를 보여줍니다. 이렇게 하면 루트 CA가 전체 PKI의 기반이므로 보안 팀

이 엄격한 보안 제어를 적용할 수 있습니다. 그러나 프라이빗 CA에서 프라이빗 인증서를 생성하는 것은 AWS Resource Access Manager ()를 사용하여 CA를 애플리케이션 계정에 공유함으로써 애플리케이션 개발 팀에 위임됩니다AWS RAM.는 교차 계정 공유에 필요한 권한을 AWS RAM 관리합니다. 이렇게 하면 모든 계정에서 프라이빗 CA가 필요하지 않으며 보다 비용 효율적인 배포 방법이 제공됩니다. 워크플로 및 구현에 대한 자세한 내용은 블로그 게시물 How to use AWS RAM to share your AWS Private CA cross-account를 참조하세요.

> **Note**
>
> AWS Certificate Manager 또한 (ACM)을 사용하면에서 사용할 퍼블릭 TLS 인증서를 프로비저닝, 관리 및 배포할 수 있습니다 AWS 서비스. 이 기능을 지원하려면 ACM이 퍼블릭 인증서를 사용하는에 AWS 계정 상주해야 합니다. 이 설명서 뒷부분의 애플리케이션 계정 섹션에서 설명합니다.

> **설계 고려 사항**
>
> - 를 사용하면 최대 5개 수준의 인증 기관 계층을 생성할 AWS Private CA수 있습니다. 또한 각각이 자체 루트를 가진 계층을 여러 개 만들 수 있습니다. AWS Private CA 계층 구조는 조직의 PKI 설계를 준수해야 합니다. 그러나 CA 계층 구조를 늘리면 인증 경로의 인증서 수가 증가하여 최종 엔터티 인증서의 검증 시간이 늘어납니다. 잘 정의된 CA 계층 구조는 각 CA에 적합한 세분화된 보안 제어, 다른 애플리케이션에 대한 하위 CA 위임, 관리 작업 분할, 취소 가능한 신뢰가 제한된 CA 사용, 다양한 유효 기간을 정의할 수 있는 기능, 경로 제한을 적용할 수 있는 기능을 포함하는 이점을 제공합니다. 이상적으로는 루트 CA와 하위 CAs 별도의에 있습니다 AWS 계정. 를 사용하여 CA 계층 구조를 계획하는 방법에 대한 자세한 내용은 AWS Private CA 설명서 및 블로그 게시물 자동차 및 제조를 위한 엔터프라이즈 규모 AWS Private CA 계층 구조를 보호하는 방법을 AWS Private CA참조하세요.
> - AWS Private CA 는 기존 CA 계층 구조와 통합할 수 있으므로 현재 사용하는 기존 신뢰 루트와 함께 ACM의 자동화 및 기본 AWS 통합 기능을 사용할 수 있습니다. 온프레미스의 상위 CA가 AWS Private CA 지원하는에서 하위 CA를 생성할 수 있습니다. 구현에 대한 자세한 내용은 AWS Private CA 설명서의 외부 상위 CA에서 서명한 하위 CA 인증서 설치를 참조하세요.

Amazon Inspector –

Amazon Inspector는 소스 코드 관리자 내에서 Amazon EC2 인스턴스, Amazon Elastic Container Registry(Amazon ECR)의 컨테이너 이미지, AWS Lambda 함수 및 코드 리포지토리를 자동으로 검색하고 스캔하여 알려진 소프트웨어 취약성 및 의도하지 않은 네트워크 노출을 확인하는 자동화된 취약성 관리 서비스입니다.

Amazon Inspector는 리소스를 변경할 때마다 리소스를 자동으로 스캔하여 리소스의 수명 주기 동안 환경을 지속적으로 평가합니다. 리소스 재스캔을 시작하는 이벤트에는 EC2 인스턴스에 새 패키지 설치, 패치 설치, 리소스에 영향을 미치는 새로운 일반적인 취약성 및 노출(CVE) 보고서 게시가 포함됩니다. Amazon Inspector는 EC2 인스턴스의 운영 체제에 대한 CIS(인터넷 보안 센터) 벤치마크 평가를 지원합니다.

Amazon Inspector는 컨테이너 이미지 평가를 위해 Jenkins 및 TeamCity와 같은 개발자 도구와 통합됩니다. 지속적 통합 및 지속적 전달(CI/CD) 도구 내에서 컨테이너 이미지의 소프트웨어 취약성을 평가하고 소프트웨어 개발 수명 주기의 이전 지점으로 보안을 푸시할 수 있습니다. CI/CD 도구의 대시보드에서 평가 결과를 사용할 수 있으므로 컨테이너 레지스트리에 대한 차단된 빌드 또는 이미지 푸시와 같은 중요한 보안 문제에 대응하여 자동화된 작업을 수행할 수 있습니다. 활성 상태인 경우 CI/CD 도구 마켓플레이스에서 Amazon Inspector 플러그인을 설치하고 Amazon Inspector 서비스를 활성화할 필요 없이 빌드 파이프라인에 Amazon Inspector 스캔을 추가할 AWS 계정수 있습니다. 이 기능은 온프레미스 AWS, 하이브리드 클라우드 등 어디서나 호스팅되는 CI/CD 도구와 함께 작동하므로 모든 개발 파이프라인에서 단일 솔루션을 일관되게 사용할 수 있습니다. Amazon Inspector가 활성화되면 모든 EC2 인스턴스, Amazon ECR 및 CI/CD 도구의 컨테이너 이미지, 대규모 Lambda 함수를 자동으로 검색하고 알려진 취약성을 지속적으로 모니터링합니다.

Amazon Inspector의 네트워크 연결성 조사 결과는 가상 게이트웨이를 통해 인터넷 게이트웨이, VPC 피어링 연결 또는 가상 프라이빗 네트워크(VPNs)와 같은 VPC 엣지와 EC2 인스턴스 간의 액세스 가능성을 평가합니다. 이러한 규칙은 AWS 네트워크 모니터링을 자동화하고 잘못 관리되는 보안 그룹, 액세스 제어 목록(ACLs), 인터넷 게이트웨이 등을 통해 EC2 인스턴스에 대한 네트워크 액세스가 잘못 구성될 수 있는 위치를 식별하는 데 도움이 됩니다. 자세한 내용은 Amazon Inspector 설명서를 참조하세요.

Amazon Inspector가 취약성 또는 열린 네트워크 경로를 식별하면 조사할 수 있는 결과가 생성됩니다. 결과에는 위험 점수, 영향을 받는 리소스, 문제 해결 권장 사항을 포함하여 취약성에 대한 포괄적인 세부 정보가 포함됩니다. 위험 점수는 환경에 맞게 특별히 조정되며up-to-date CVE 정보를 네트워크 접근성 및 악용성 정보와 같은 시간 및 환경 요인과 상호 연관시켜 컨텍스트 조사 결과를 제공함으로써 계산됩니다.

Amazon Inspector Code Security는 자사 애플리케이션 소스 코드, 타사 애플리케이션 종속성 및 코드형 인프라(IaC)에서 취약성을 검사합니다. 코드 보안을 활성화한 후 스캔 구성을 생성하여 코드 리포지토리에 적용하여 스캔할 빈도, 스캔 유형 및 리포지토리를 결정할 수 있습니다. 코드 보안은 정적 애플리케이션 보안 테스트(SAST), 소프트웨어 구성 분석(SCA) 및 IaC 스캔을 지원합니다. 빈도를 구성하려면 온디맨드, 코드 변경 또는 주기적으로 스캔을 정의할 수 있습니다. 코드 스캔은 코드 스니펫을 캡처하여 탐지된 취약성을 강조 표시합니다. 코드 조각은 KMS 키로 암호화된 상태로 저장됩니다. 조직의 위임된 관리자는 멤버 계정에 속한 코드 조각을 볼 수 없습니다. 소스 코드 관리자(SCMs 코드 보안과 통합하면 모든 코드 리포지토리가 Amazon Inspector 콘솔에 프로젝트로 나열됩니다. 코드 보안은 각 리포지토리의 기본 브랜치만 모니터링합니다. Amazon Inspector는 개발자가 작업하는 곳에서 직접 특정 코드 수정 권장 사항을 제공하여 보안 문제 해결을 간소화합니다. SCM과의 양방향 통합은 중요하고 높은 조사 결과에 대한 풀 요청(PRs) 및 병합 요청(MRs) 내의 설명으로 수정 사항을 자동으로 제안하고 개발자에게 워크플로를 중단하지 않고 해결해야 할 가장 중요한 취약성을 알립니다.

취약성을 검사하려면 AWS Systems Manager 에이전트(SSMAgent)를 사용하여에서 AWS Systems Manager EC2 인스턴스를 관리해야 합니다. Amazon ECR 또는 Lambda 함수에서 EC2 인스턴스의 네트워크 연결성 또는 컨테이너 이미지의 취약성 스캔에 에이전트가 필요하지 않습니다.

Amazon Inspector는와 통합 AWS Organizations 되며 위임된 관리를 지원합니다. SRA에서 AWS 보안 도구 계정은 Amazon Inspector의 위임된 관리자 계정이 됩니다. Amazon Inspector 위임된 관리자 계정은 조사 결과 데이터와 AWS 조직 구성원에 대한 특정 설정을 관리할 수 있습니다. 여기에는 모든 멤버 계정에 대해 집계된 조사 결과의 세부 정보 보기, 멤버 계정에 대한 스캔 활성화 또는 비활성화, AWS 조직 내에서 스캔한 리소스 검토가 포함됩니다.

설계 고려 사항

- Amazon Inspector는 두 서비스가 모두 활성화되면 AWS Security Hub CSPM 및 Security Hub와 자동으로 통합됩니다. 이 통합을 사용하여 Amazon Inspector의 모든 조사 결과를 Security Hub CSPM으로 전송할 수 있습니다. 그러면 해당 조사 결과가 보안 태세 분석에 포함됩니다.
- Amazon Inspector는 조사 결과, 리소스 범위 변경 및 개별 리소스의 초기 스캔에 대한 이벤트를 Amazon EventBridge로 자동으로 내보내고, 선택적으로 Amazon Simple Storage Service(Amazon S3) 버킷으로 내보냅니다. 활성 결과를 S3 버킷으로 내보내려면 Amazon Inspector가 결과를 암호화하는 데 사용할 수 있는 AWS KMS 키와 Amazon Inspector가 객체를 업로드할 수 있는 권한이 있는 S3 버킷이 필요합니다. EventBridge 통합을 사용하면 기존 보안 및 규정 준수 워크플로의 일부로 결과를 거의 실시간으로 모니터링하고 처리할 수 있습니다. EventBridge 이벤트는 시작된 멤버 계정 외에도 Amazon Inspector 위임된 관리자 계정에 게시됩니다.

- Amazon Inspector Code Security와 GitHub SaaS, GitHub Enterprise Cloud 및 GitHub Enterprise Server의 통합에는 퍼블릭 인터넷 액세스가 필요합니다.

구현 예제

AWS SRA 코드 라이브러리는 Amazon Inspector의 샘플 구현을 제공합니다. 위임된 관리(보안 도구)를 보여주고 조직의 모든 기존 및 향후 계정에 대해 Amazon Inspector를 AWS 구성합니다.

AWS 보안 인시던트 대응

AWS 보안 인시던트 대응는 환경 AWS 의 보안 인시던트를 준비하고 대응하는 데 도움이 되는 서비스입니다. 조사 결과를 분류하고 보안 이벤트를 에스컬레이션합니다. 및는 즉각적인 주의가 필요한 사례를 관리합니다. 또한 고객 인시던트 대응 팀(CIRT)에 AWS 액세스할 수 있습니다. 영향을 받는 리소스를 조사하는 . AWS 보안 인시던트 대응 는 문서(SSM 문서)를 통해 AWS Systems Manager 자동화된 응답 및 문제 해결 기능도 제공합니다. 보안 팀이 대응하고 복구할 수 있습니다. 보안 인시던트는 보다 효율적으로. AWS 보안 인시던트 대응 Amazon GuardDuty 및와 통합되어 AWS Security Hub CSPM 보안 조사 결과를 수신하고 자동화된 응답을 오케스트레이션합니다.

AWS SRA에서 AWS 보안 인시던트 대응 는 Security Tooling 계정에 위임된 관리자 계정으로 배포됩니다. Security Tooling 계정은 보안 서비스를 운영하고 보안 알림 및 응답을 자동화하는 계정의 목적에 부합하기 때문에 선택됩니다. 또한 Security Tooling 계정은 Security Hub CSPM 및 GuardDuty의 위임된 관리자 계정 역할을 합니다.이 계정은 워크플로 관리를 간소화하는 AWS 보안 인시던트 대응데 도움이 됩니다. AWS 보안 인시던트 대응 는 작업하도록 구성되어 AWS Organizations있으므로 Security Tooling 계정에서 조직의 계정 전체에서 인시던트 응답을 관리할 수 있습니다.

AWS 보안 인시던트 대응 는 인시던트 대응 수명 주기의 다음 단계를 구현하는 데 도움이 됩니다.

- 준비: 억제 작업을 위한 대응 계획 및 SSM 문서를 생성하고 유지 관리합니다.
- 탐지 및 분석: 보안 조사 결과를 자동으로 분석하고 인시던트 심각도를 결정합니다.
- 탐지 및 분석: 서비스 지원 사례를 열고 AWS CIRT에 문의하여 추가 지원을 받으세요. CIRT는 활성 보안 이벤트 중에 지원을 제공하는 개인 그룹입니다.
- 억제 및 근절: SSM 문서를 통해 자동 억제 작업을 실행합니다.
- 인시던트 후 활동: 인시던트 세부 정보를 문서화하고 인시던트 후 분석을 수행합니다.

또한 AWS 보안 인시던트 대응 를 사용하여 자체 관리형 사례를 생성할 수 AWS 보안 인시던트 대응 있습니다.는 계정 또는 리소스에 영향을 미칠 수 있는 사항을 알고 있거나 조치를 취해야 할 때 아웃바운드 알림 또는 사례를 생성할 수 있습니다. 이 기능은 구독의 일부로 사전 대응 및 알림 분류 워크플로를 활성화한 경우에만 사용할 수 있습니다.

설계 고려 사항

- 구현 시 프로덕션 환경에서 자동 응답 작업을 활성화하기 전에 이를 AWS 보안 인시던트 대응주의 깊게 검토하고 테스트하세요. 자동화는 인시던트 대응 속도를 높일 수 있지만 잘못 구성된 자동 작업은 합법적인 워크로드에 영향을 미칠 수 있습니다.
- 일반적인 인시던트 유형에 대한 서비스의 기본 제공 모범 사례를 유지하면서에서 SSM 문서를 사용하여 조직별 격리 절차를 구현하는 AWS 보안 인시던트 대응 것이 좋습니다.
- VPC AWS 보안 인시던트 대응 에서를 사용하려는 경우 프라이빗 서브넷에서 억제 작업을 활성화하기 위해 Systems Manager 및 기타 통합 서비스에 대해 구성된 적절한 VPC 엔드포인트가 있는지 확인합니다.

모든 내에 공통 보안 서비스 배포 AWS 계정

이 참조의 앞부분에 있는 조직 전체에 AWS 보안 서비스 적용 섹션에서는를 보호하는 보안 서비스를 강조 AWS 계정표시했으며 이러한 서비스 중 상당수는 내에서 구성하고 관리할 수도 있다는 점에 유의했습니다 AWS Organizations. 이러한 서비스 중 일부는 모든 계정에 배포되어야 하며 AWS SRA에 표시됩니다. 이를 통해 일관된 가드레일 세트를 활성화하고 AWS 조직 전체에서 중앙 집중식 모니터링, 관리 및 거버넌스를 제공할 수 있습니다.

Security Hub CSPM, GuardDuty AWS Config, IAM Access Analyzer 및 CloudTrail 조직 추적은 모든 계정에 표시됩니다. 처음 3개는 앞서 관리 계정, 신뢰할 수 있는 액세스 및 위임된 관리자 섹션에서 설명한 위임된 관리자 기능을 지원합니다. CloudTrail은 현재 다른 집계 메커니즘을 사용합니다.

AWS SRA GitHub 코드 리포지토리는 AWS 조직 관리 계정을 포함한 모든 계정에서 Security Hub CSPM AWS Config, GuardDuty AWS Firewall Manager및 CloudTrail 조직 추적을 활성화하는 샘플 구현을 제공합니다.

설계 고려 사항

- 특정 계정 구성에는 추가 보안 서비스가 필요할 수 있습니다. 예를 들어 S3 버킷을 관리하는 계정(애플리케이션 및 로그 아카이브 계정)에는 Amazon Macie도 포함되어야 하며 이러

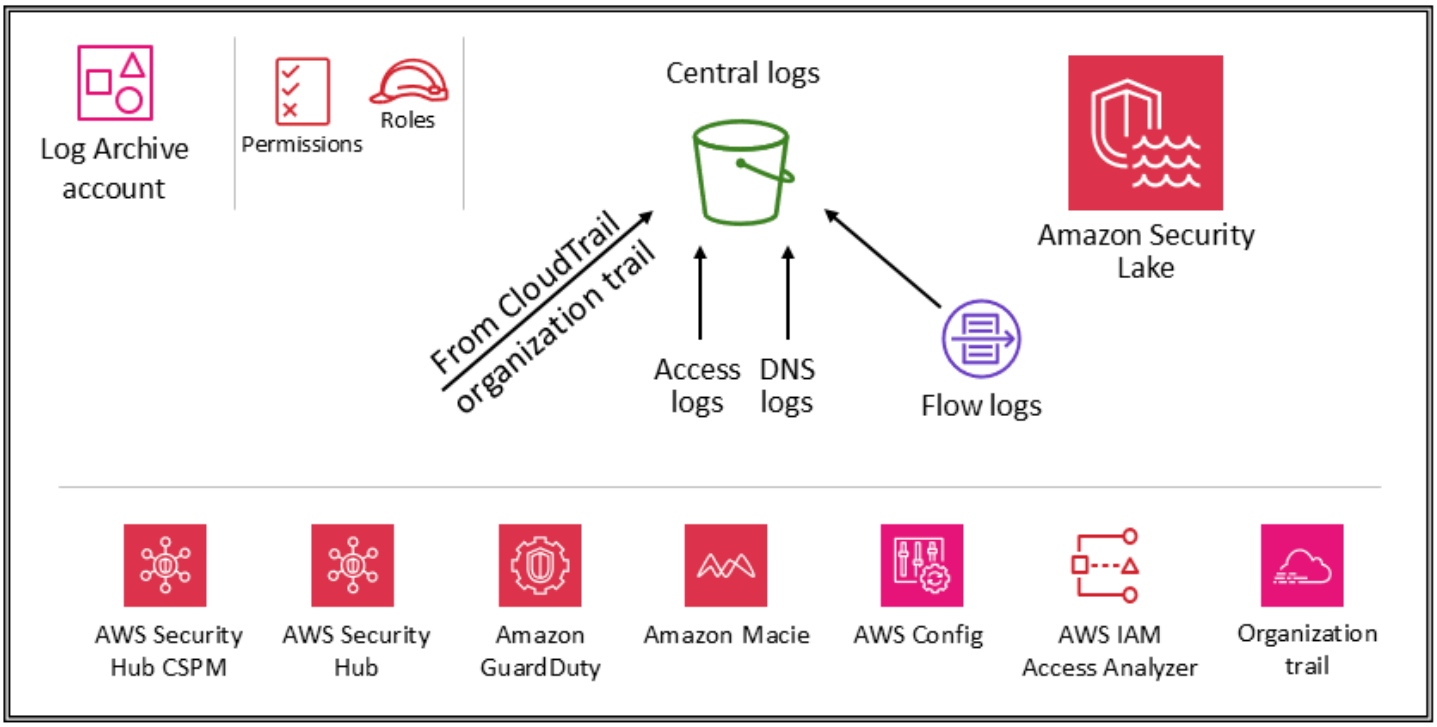
한 일반적인 보안 서비스에서 CloudTrail S3 데이터 이벤트 로깅을 활성화하는 것이 좋습니다. (Macie는 중앙 집중식 구성 및 모니터링을 통해 위임된 관리를 지원합니다.) 또 다른 예는 EC2 인스턴스 또는 Amazon ECR 이미지를 호스팅하는 계정에만 적용되는 Amazon Inspector입니다.

- 이 단원에서 앞서 설명한 서비스 외에도 AWS SRA에는 AWS Organizations 통합과 위임된 관리자 기능을 지원하는 두 가지 보안 중심 서비스 AWS Audit Manager인 Amazon Detective 및가 포함되어 있습니다. 그러나 이러한 서비스는 다음 시나리오에서 가장 잘 사용되는 것으로 확인되었으므로 계정 기준 설정을 위한 권장 서비스의 일부로 포함되지 않습니다.
  - 이러한 기능을 수행하는 전담 팀 또는 리소스 그룹이 있습니다. Detective는 보안 분석가 팀에서 가장 잘 활용되며 Audit Manager는 내부 감사 또는 규정 준수 팀에 유용합니다.
  - 프로젝트 시작 시 GuardDuty 및 Security Hub CSPM과 같은 핵심 도구 세트에 집중한 다음 추가 기능을 제공하는 서비스를 사용하여 이를 기반으로 구축하려고 합니다.

보안 OU - 로그 아카이브 계정

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

다음 다이어그램은 로그 아카이브 계정에 구성된 AWS 보안 서비스를 보여줍니다.



로그 아카이브 계정은 모든 보안 관련 로그 및 백업을 수집하고 보관하는 전용 계정입니다. 중앙 집중식 로그를 사용하면 Amazon S3 객체 액세스, 자격 증명별 무단 활동, IAM 정책 변경 및 민감한 리소스에서 수행되는 기타 중요한 활동을 모니터링, 감사 및 알릴 수 있습니다. 보안 목표는 간단합니다. 이는 변경 불가능한 스토리지여야 하며, 제어, 자동화 및 모니터링 메커니즘으로만 액세스하고 내구성을 위해 구축되어야 합니다(예: 적절한 복제 및 보관 프로세스 사용). 제어 기능을 심층적으로 구현하여 로그 및 로그 관리 프로세스의 무결성과 가용성을 보호할 수 있습니다. 액세스에 사용할 최소 권한 역할 할당 및 제어된 AWS KMS 키로 로그 암호화와 같은 예방 제어 외에도와 같은 탐지 제어를 사용하여 예상치 못한 변경 사항이 있는지이 권한 모음 AWS Config 을 모니터링(및 알림 및 수정)합니다.

> 설계 고려 사항
>
> 인프라, 운영 및 워크로드 팀에서 사용하는 운영 로그 데이터는 보안, 감사 및 규정 준수 팀에서 사용하는 로그 데이터와 겹치는 경우가 많습니다. 운영 로그 데이터를 로그 아카이브 계정으로 통합하는 것이 좋습니다. 특정 보안 및 거버넌스 요구 사항에 따라이 계정에 저장된 운영 로그 데이터를 필터링해야 할 수 있습니다. 로그 아카이브 계정의 운영 로그 데이터에 액세스할 수 있는 사용자를 지정해야 할 수도 있습니다.

로그 유형

AWS SRA에 표시된 기본 로그에는 AWS CloudTrail (조직 추적), Amazon VPC 흐름 로그, Amazon CloudFront의 액세스 로그 및 Amazon Route 53의 DNS 로그 AWS WAF가 포함됩니다. 이러한 로그는 사용자, 역할 AWS 서비스또는 네트워크 엔터티(예: IP 주소로 식별됨)가 수행한(또는 시도한) 작업에 대한 감사를 제공합니다. 다른 로그 유형(예: 애플리케이션 로그 또는 데이터베이스 로그)도 캡처하고 보관할 수 있습니다. 로그 소스 및 로깅 모범 사례에 대한 자세한 내용은 각 서비스의 보안 설명서를 참조하세요.

Amazon S3를 중앙 로그 스토어로 사용

기본적으로 또는 독점적으로 Amazon S3의 많은 AWS 서비스 로그 정보입니다. AWS CloudTrail, Amazon VPC 흐름 로그, Elastic Load Balancing AWS Config, Amazon GuardDuty 및 AWS WAF 는 Amazon S3에 정보를 로깅하는 서비스의 몇 가지 예입니다. 즉, 로그 무결성은 S3 객체 무결성을 통해 달성되고, 로그 기밀성은 S3 객체 액세스 제어를 통해 달성되며, 로그 가용성은 S3 객체 잠금, S3 객체 버전 및 S3 수명 주기 규칙을 통해 달성됩니다. 전용 계정에 있는 중앙 집중식 전용 S3 버킷에 정보를 로깅하면 몇 개의 버킷에서만 이러한 로그를 관리하고 엄격한 보안 제어, 액세스 및 업무 분리를 적용할 수 있습니다.

AWS SRA에서 Amazon S3에 저장된 기본 로그는 CloudTrail에서 가져오므로이 섹션에서는 이러한 객체를 보호하는 방법을 설명합니다. 이 지침은 자체 애플리케이션 또는 다른 애플리케이션에서 생성한 다른 S3 객체에도 적용됩니다 AWS 서비스. Amazon S3에 높은 무결성, 강력한 액세스 제어, 자동 보존 또는 폐기가 필요한 데이터가 있을 때마다 이러한 패턴을 적용합니다.

S3 버킷에 업로드되는 모든 새 객체(CloudTrail 로그 포함)는 기본적으로 Amazon S3-managed형 암호화 키(SSE-S3)를 사용한 Amazon 서버 측 암호화를 사용하여 암호화됩니다. 이렇게 하면 저장 데이터를 보호하는 데 도움이 되지만 액세스 제어는 IAM 정책에 의해서만 제어됩니다. 추가 관리형 보안 계층을 제공하기 위해 모든 보안 S3 버킷에서 관리하는 AWS KMS 키(SSE-KMS)와 함께 서버 측 암호화를 사용할 수 있습니다. 이렇게 하면 두 번째 수준의 액세스 제어가 추가됩니다. 로그 파일을 읽으려면 사용자에게 Amazon S3 S3 읽기 권한과 연결된 키 정책에 따라 복호화할 수 있는 권한을 허용하는 IAM 정책 또는 역할이 모두 적용되어 있어야 합니다.

두 가지 옵션을 사용하면 Amazon S3에 저장된 CloudTrail 로그 객체의 무결성을 보호하거나 확인할 수 있습니다. CloudTrail은 로그 파일을 전송한 후 로그 파일이 수정 또는 삭제되었는지 여부를 확인하기 위해 로그 파일 무결성 검증을 제공합니다. CloudTrail 다른 옵션은 S3 객체 잠금입니다.

S3 버킷 자체를 보호하는 것 외에도 로깅 서비스(예: CloudTrail) 및 로그 아카이브 계정에 대한 최소 권한 원칙을 준수할 수 있습니다. 예를 들어 AWS 관리형 IAM 정책에서 부여한 권한이 있는 사용자는 자신의에서 가장 민감하고 중요한 감사 함수를 비활성화하거나 재구

성AWSCloudTrail_FullAccess할 수 있습니다 AWS 계정. 이 IAM 정책의 적용을 가능한 한 적은 수의 개인으로 제한합니다.

AWS Config 및 IAM Access Analyzer에서 제공하는 것과 같은 탐지 제어를 사용하여 예기치 않은 변경 사항이 있는지이 광범위한 예방 제어 집합을 모니터링(및 알림 및 해결)합니다.

S3 버킷의 보안 모범 사례에 대한 자세한 내용은 Amazon S3 설명서, 온라인 기술 강연 및 블로그 게시물 Amazon S3의 데이터 보안을 위한 상위 10가지 보안 모범 사례를 참조하세요.

> 구현 예제
>
> AWS SRA 코드 라이브러리는 Amazon S3 블록 계정 퍼블릭 액세스의 샘플 구현을 제공합니다. 이 모듈은 AWS 조직의 모든 기존 및 향후 계정에 대한 Amazon S3 퍼블릭 액세스를 차단합니다.

Amazon Security Lake

AWS SRA는 로그 아카이브 계정을 Amazon Security Lake의 위임된 관리자 계정으로 사용할 것을 권장합니다. 이렇게 하면 Security Lake는 다른 SRA 권장 보안 로그와 동일한 계정의 전용 S3 버킷에서 지원되는 로그를 수집합니다.

로그의 가용성과 로그 관리 프로세스를 보호하기 위해 Security Lake용 S3 버킷은 Security Lake 서비스 또는 소스 또는 구독자를 위해 Security Lake에서 관리하는 IAM 역할만 액세스해야 합니다. 액세스를 위한 최소 권한 역할 할당 및 제어된 AWS KMS 키로 로그 암호화와 같은 예방 제어를 사용하는 것 외에도와 같은 탐지 제어를 사용하여 예상치 못한 변경 사항이 있는지이 권한 모음 AWS Config 을 모니터링(및 알림 및 수정)합니다.

Security Lake 관리자는 AWS 조직 전체에서 로그 수집을 활성화할 수 있습니다. 이러한 로그는 Log Archive 계정의 리전 S3 버킷에 저장됩니다. 또한 로그를 중앙 집중화하고 더 쉬운 저장 및 분석을 용이하게 하기 위해 Security Lake 관리자는 모든 리전 S3 버킷의 로그가 통합되고 저장되는 하나 이상의 롤업 리전을 선택할 수 있습니다. 지원되는의 로그 AWS 서비스 는 Open Cybersecurity Schema Framework(OCSF)라는 표준화된 오픈 소스 스키마로 자동 변환되고 Security Lake S3 버킷에 Apache Parquet 형식으로 저장됩니다. OCSF 지원을 통해 Security Lake는 AWS 및 기타 엔터프라이즈 보안 소스의 보안 데이터를 효율적으로 정규화하고 통합하여 보안 관련 정보의 통합되고 신뢰할 수 있는 리포지토리를 생성합니다.

Security Lake는 Amazon S3 및에 대한 AWS CloudTrail 관리 이벤트 및 CloudTrail 데이터 이벤트와 관련된 로그를 수집할 수 있습니다 AWS Lambda. Security Lake에서 CloudTrail 관리 이벤트를 수집 하

려면 CloudTrail 관리 이벤트를 읽고 쓰는 CloudTrail 다중 리전 조직 추적이 하나 이상 있어야 합니다. 추적에 대한 로깅이 활성화되어 있어야 합니다. 다중 리전 추적은 단일에 대해 여러 리전의 로그 파일을 단일 S3 버킷으로 전송합니다 AWS 계정. 리전이 다른 국가에 있는 경우 데이터 내보내기 요구 사항을 고려하여 다중 리전 추적을 활성화할 수 있는지 확인합니다.

AWS Security Hub CSPM 는 Security Lake에서 지원되는 네이티브 데이터 소스이므로 Security Hub CSPM 조사 결과를 Security Lake에 추가해야 합니다. Security Hub CSPM은 다양한 AWS 서비스 타사 통합에서 결과를 생성합니다. 이러한 결과는 규정 준수 태세와 AWS 및 AWS Partner 솔루션에 대한 보안 권장 사항을 따르고 있는지 여부에 대한 개요를 파악하는 데 도움이 됩니다.

로그 및 이벤트에서 가시성과 실행 가능한 인사이트를 얻기 위해 Amazon Athena, Amazon OpenSearch Service, Amazon Quick 및 타사 솔루션과 같은 도구를 사용하여 데이터를 쿼리할 수 있습니다. Security Lake 로그 데이터에 액세스해야 하는 사용자는 로그 아카이브 계정에 직접 액세스해서는 안 됩니다. 보안 도구 계정에서만 데이터에 액세스해야 합니다. 또는 OpenSearch Service, Quick과 같은 분석 도구 AWS 계정 또는 보안 정보 및 이벤트 관리(SIEM) 도구와 같은 타사 도구를 제공하는 다른 위치 또는 온프레미스 위치를 사용할 수 있습니다. 데이터에 대한 액세스를 제공하려면 관리자는 로그 아카이브 계정에서 Security Lake 구독자를 구성하고 데이터에 액세스해야 하는 계정을 쿼리 액세스 구독자로 구성해야 합니다. 자세한 내용은이 가이드의 보안 OU – 보안 도구 계정 섹션에서 Amazon Security Lake를 참조하세요.

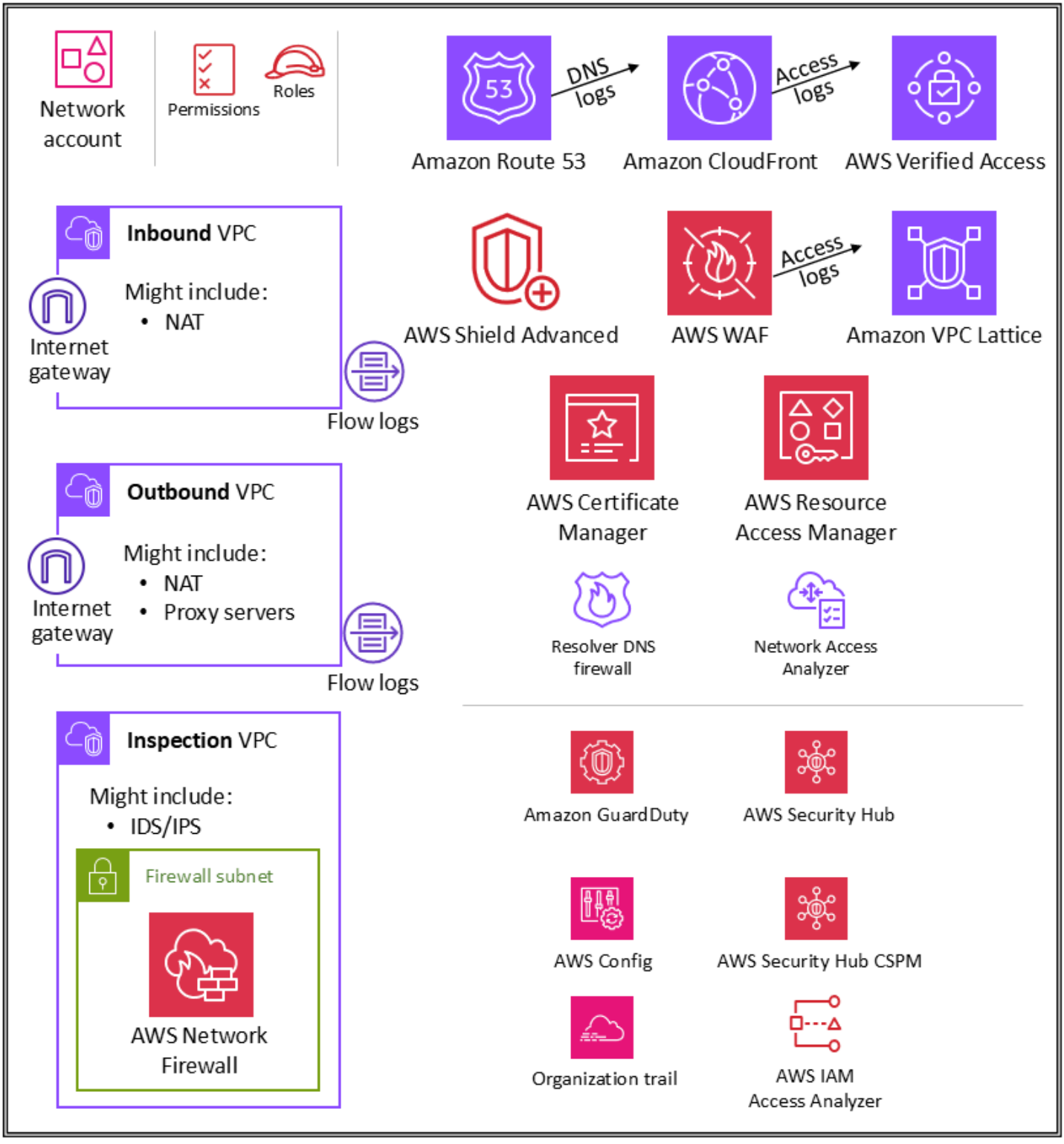
Security Lake는 서비스에 대한 관리자 액세스를 관리하는 데 도움이 되는 AWS 관리형 정책을 제공합니다. 자세한 내용은 Security Lake 사용 설명서를 참조하세요. 가장 좋은 방법은 개발 파이프라인을 통해 Security Lake의 구성을 제한하고 AWS 콘솔 또는 AWS Command Line Interface ()를 통해 구성 변경을 방지하는 것입니다AWS CLI. 또한 Security Lake를 관리하는 데 필요한 권한만 제공하도록 엄격한 IAM 정책 및 서비스 제어 정책(SCPs)을 설정해야 합니다. 이러한 S3 버킷에 대한 직접 액세스를 감지하도록 알림을 구성할 수 있습니다.

> **설계 고려 사항**
>
> Security Lake에서 CloudTrail 관리 이벤트를 활성화하면 Security Lake 요금이 발생합니다. Security Lake에서 CloudTrail 관리 이벤트를 수집하려면 읽기 및 쓰기 CloudTrail 관리 이벤트를 수집하는 CloudTrail 다중 리전 조직 추적이 필요합니다. 이 첫 번째 추적은 무료로 사용할 수 있습니다. CloudTrail 관리 이벤트는 일반적으로 총 CloudTrail 이벤트 중 적은 비율(약 5%)을 차지합니다. 이는 로그 아카이브 계정에서 중앙 집중식 CloudTrail 로그를 AWS Control Tower 사용하거나 보유한 고객에게 적용됩니다.

인프라 OU - Network 계정

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

다음 다이어그램은 네트워크 계정에 구성된 AWS 보안 서비스를 보여줍니다.



Network 계정은 애플리케이션과 광범위한 인터넷 사이의 게이트웨이를 관리합니다. 양방향 인터페이스 보호에 있어 중요합니다. Network 계정은 네트워킹 서비스, 구성 및 운영을 개별 애플리케이션 워크로드, 보안 및 기타 인프라로부터 분리합니다. 이를 통해 연결성, 권한 및 데이터 흐름을 제한할 뿐

만 아니라 이러한 계정을 운영해야 하는 팀의 업무 및 최소 권한 분리를 지원합니다. 네트워크 흐름을 별도의 인바운드 및 아웃바운드 Virtual Private Cloud(VPC)로 분리하여 원치 않는 액세스로부터 민감한 인프라와 트래픽을 보호할 수 있습니다. 인바운드 네트워크는 일반적으로 위험이 더 크다고 간주되며 적절한 라우팅, 모니터링 및 잠재적 문제 완화 조치가 필요합니다. 이러한 인프라 계정은 Org Management 계정과 인프라 OU의 권한 가드레일을 상속합니다. 네트워킹 (및 보안) 팀에서 이 계정의 인프라 대부분을 관리합니다.

네트워크 아키텍처

네트워크 설계 및 세부 정보는이 문서의 범위를 벗어나지만 다양한 계정 간의 네트워크 연결에 VPC 피어링 AWS PrivateLink및의 세 가지 옵션을 사용하는 것이 좋습니다 AWS Transit Gateway. 이들 중에서 선택할 때 고려해야 할 중요한 사항은 운영 기준, 예산, 특정 대역폭 요구 사항입니다.

- VPC 피어링 – 두 VPC를 연결하는 가장 간단한 방법은 VPC 피어링을 사용하는 것입니다. 연결을 통해 VPC 간에 완전한 양방향 연결이 가능합니다. 별도의 계정에 있고 함께 피어링 AWS 리전 할 수도 있는 VPCs입니다. VPC가 수십, 수백 개인 경우 피어링으로 상호 연결하면 수백, 수천 개의 피어링 연결 메시가 생성되므로 관리 및 확장이 어려울 수 있습니다. VPC 피어링은 한 VPC에 있는 리소스가 다른 VPC의 리소스와 통신해야 하고, 두 VPC 모두의 환경이 제어 및 보호되며, 연결할 VPC의 수가 10개 미만인 경우(각 연결을 개별적으로 관리할 수 있음)에 가장 적합합니다.
- AWS PrivateLink – PrivateLink는 VPCs, 서비스 및 애플리케이션 간에 프라이빗 연결을 제공합니다. VPC에서 자체 애플리케이션을 생성하고 PrivateLink 구동 서비스(엔드포인트 서비스라고도 함)로서 구성할 수 있습니다. 다른 AWS 보안 주체는 서비스 유형에 따라 인터페이스 VPC 엔드포인트 또는 Gateway Load Balancer 엔드포인트를 사용하여 VPC에서 엔드포인트 서비스로의 연결을 생성할 수 있습니다. Load Balancer PrivateLink를 사용하는 경우 서비스 트래픽은 공개적으로 라우팅할 수 있는 네트워크를 통과하지 않습니다. 클라이언트-서버 설정을 통해 하나 이상의 소비자 VPC에 서비스 공급자 VPC의 특정 서비스 또는 인스턴스 세트에 대한 단방향 액세스 권한을 부여하려는 경우 PrivateLink를 사용하세요. PrivateLink는 서비스 공급자와의 IP 충돌이 없도록 클라이언트 VPC 내에서 탄력적 네트워크 인터페이스를 사용하기 때문에 두 VPC의 클라이언트와 서버의 IP 주소가 겹칠 때 좋은 옵션입니다.
- AWS Transit Gateway – Transit Gateway는 가상 어플라이언스를 프로비저닝할 필요 없이 VPCs와 온프레미스 네트워크를 완전 관리형 서비스로 연결하기 위한 hub-and-spoke 설계를 제공합니다.는 고가용성 및 확장성을 AWS 관리합니다. 전송 게이트웨이는 리전 리소스이며 동일한 내에서 수천 VPCs를 연결할 수 있습니다 AWS 리전. 하이브리드 연결(VPN 및 AWS Direct Connect 연결)을 단일 전송 게이트웨이에 연결하여 AWS 조직의 전체 라우팅 구성을 한 곳에서 통합하고 제어할 수 있습니다. 전송 게이트웨이는 여러 VPC 피어링 연결을 대규모로 생성하고 관리할 때 발생하는 복잡성을 해결합니다. 이 옵션은 대부분의 네트워크 아키텍처에서 기본값이지만, 비용, 대역폭 및 지연 시간과 관련된 특정 요구 사항의 경우 VPC 피어링이 더 적합할 수 있습니다.

인바운드(수신) VPC

인바운드 VPC는 애플리케이션 외부에서 시작된 네트워크 연결을 수락, 검사 및 라우팅하기 위한 것입니다. 애플리케이션의 특성에 따라 이 VPC에서 일부 Network Address Translation(NAT)을 볼 수 있을 것입니다. 이 VPC의 흐름 로그는 캡처되어 Log Archive 계정에 저장됩니다.

아웃바운드(송신) VPC

아웃바운드 VPC는 애플리케이션 내에서 시작된 네트워크 연결을 처리합니다. 애플리케이션의 세부 사항에 따라 트래픽 NAT, AWS 서비스특정 VPC 엔드포인트 및이 VPC의 외부 API 엔드포인트 호스팅을 확인할 수 있습니다. 이 VPC의 흐름 로그는 캡처되어 Log Archive 계정에 저장됩니다.

검사 VPC

전용 검사 VPC는 VPCs(동일하거나 다른 AWS 리전), 인터넷 및 온프레미스 네트워크 간의 검사를 관리하기 위한 간소화된 중앙 접근 방식을 제공합니다. AWS SRA의 경우 VPCs 간의 모든 트래픽이 검사 VPC를 통과하는지 확인하고 다른 워크로드에 검사 VPC를 사용하지 마세요.

AWS Network Firewall

AWS Network Firewall는 VPC를 위한 고가용성 관리형 네트워크 방화벽 서비스입니다. 이를 통해 상태 저장 검사, 침입 방지 및 탐지, 웹 필터링을 손쉽게 배포하고 관리하여 가상 네트워크를 보호할 수 있습니다 AWS. Network Firewall을 사용하여 TLS 세션을 복호화하고 인바운드 및 아웃바운드 트래픽을 검사할 수 있습니다. Network Firewall 구성에 대한 자세한 내용은 AWS Network Firewall – VPC의 새로운 관리형 방화벽 서비스 블로그 게시물을 참조하세요.

VPC의 가용 영역별로 방화벽을 사용합니다. 각 가용 영역에 대해 트래픽을 필터링하는 방화벽 엔드포인트를 호스팅할 서브넷을 선택합니다. 가용 영역의 방화벽 엔드포인트는 가용 영역이 위치한 서브넷을 제외하고 영역 내의 모든 서브넷을 보호할 수 있습니다. 사용 사례 및 배포 모델에 따라 방화벽 서브넷은 퍼블릭 또는 프라이빗일 수 있습니다. 방화벽은 트래픽 흐름에 완전히 투명하며 Network Address Translation(NAT)을 수행하지 않습니다. 소스 및 대상 주소를 보존합니다. 이 참조 아키텍처에서 방화벽 엔드포인트는 검사 VPC에서 호스팅됩니다. 인바운드 VPC에서 아웃바운드 VPC로 향하는 모든 트래픽은 검사를 위해 이 방화벽 서브넷을 통해 라우팅됩니다.

Network Firewall은 Amazon CloudWatch 지표를 통해 방화벽 활동을 실시간으로 표시하고 Amazon Simple Storage Service(Amazon S3), CloudWatch 및 Amazon Data Firehose로 로그를 전송하여 네트워크 트래픽에 대한 가시성을 높입니다. Network Firewall은 AWS 파트너의 기술을 포함하여 기존 보안 접근 방식과 상호 운용할 수 있습니다. 또한 내부적으로 작성되었거나 타사 공급업체 또는 오픈 소스 플랫폼에서 외부 소싱되었을 수 있는 기존 Suricata 규칙 세트를 가져올 수 있습니다.

AWS SRA에서는 서비스의 네트워크 제어 중심 기능이 계정의 의도와 일치하기 때문에 네트워크 방화벽이 네트워크 계정 내에서 사용됩니다.

설계 고려 사항

- AWS Firewall Manager 는 Network Firewall을 지원하므로 조직 전체에서 Network Firewall 규칙을 중앙에서 구성하고 배포할 수 있습니다. (자세한 내용은 AWS 설명서의 Firewall Manager에서 AWS Network Firewall 정책 사용을 참조하세요.) Firewall Manager를 구성하면 지정한 계정 및 VPC에 일련의 규칙이 포함된 방화벽이 자동으로 생성됩니다. 또한 퍼블릭 서브넷이 포함된 모든 가용 영역의 전용 서브넷에 엔드포인트가 배포됩니다. 동시에 중앙에서 구성된 규칙 세트에 대한 모든 변경 사항은 배포된 Network Firewall 방화벽의 다운스트림에서 자동으로 업데이트됩니다.
- Network Firewall에서는 여러 배포 모델을 사용할 수 있습니다. 적합한 모델은 사용 사례 및 요구 사항에 따라 다릅니다. 예는 다음과 같습니다.
  - Network Firewall이 개별 VPC에 배포되는 분산 배포 모델.
  - Network Firewall이 east-west(VPC-to-VPC) 또는 north-south(인터넷 송신 및 수신, 온프레미스) 트래픽에 대한 중앙 집중식 VPC에 배포되는 중앙 집중식 배포 모델.
  - Network Firewall이 east-west 트래픽과 north-south 트래픽의 하위 집합에 대한 중앙 집중식 VPC에 배포되는 결합형 배포 모델.
- 가장 좋은 방법은 Network Firewall 서브넷을 사용하여 다른 서비스를 배포하지 않는 것입니다. 이는 Network Firewall이 방화벽의 서브넷 내 소스 또는 대상에서 오는 트래픽을 검사할 수 없기 때문입니다.

Network Access Analyzer

Network Access Analyzer는 리소스에 대한 의도하지 않은 네트워크 액세스를 식별하는 Amazon VPC의 기능입니다. Network Access Analyzer를 사용하여 네트워크 세분화를 검증하고, 인터넷에서 액세스할 수 있거나 신뢰할 수 있는 IP 주소 범위에서만 액세스할 수 있는 리소스를 식별하고, 모든 네트워크 경로에 적절한 네트워크 제어가 있는지 검증할 수 있습니다.

Network Access Analyzer는 자동화된 추론 알고리즘을 사용하여 패킷이 네트워크의 리소스 간에 취할 수 있는 AWS 네트워크 경로를 분석하고 정의된 네트워크 액세스 범위와 일치하는 경로에 대한 결과를 생성합니다. Network Access Analyzer는 네트워크 구성의 정적 분석을 수행합니다. 따라서 이 분석의 일환으로 네트워크에서 패킷이 전송되지 않습니다.

Amazon Inspector Network Reachability 규칙은 관련 기능을 제공합니다. 이러한 규칙에 의해 생성된 조사 결과는 Application 계정에서 사용됩니다. Network Access Analyzer와 Network Reachability는 모두 AWS 검증된 보안 이니셔티브의 최신 기술을 사용하며,이 기술을 다양한 중점 영역에 적용합니다. Network Reachability 패키지는 특히 EC2 인스턴스와 해당 인터넷 접근성에 중점을 둡니다.

네트워크 계정은 AWS 환경 안팎의 트래픽을 제어하는 중요한 네트워크 인프라를 정의합니다. 이 트래픽을 면밀하게 모니터링해야 합니다. AWS SRA에서 Network Access Analyzer는 의도하지 않은 네트워크 액세스를 식별하고, 인터넷 게이트웨이를 통해 인터넷에 액세스할 수 있는 리소스를 식별하고, 리소스와 인터넷 게이트웨이 간의 모든 네트워크 경로에 네트워크 방화벽 및 NAT 게이트웨이와 같은 적절한 네트워크 제어가 있는지 확인하는 데 도움이 되도록 네트워크 계정 내에서 사용됩니다.

> 설계 고려 사항
>
> Network Access Analyzer는 Amazon VPC의 기능이며 VPC가 AWS 계정 있는 모든에서 사용할 수 있습니다. 네트워크 관리자는 범위가 좁은 교차 계정 IAM 역할을 가져와 승인된 네트워크 경로가 각각 내에 적용되는지 확인할 수 있습니다 AWS 계정.

AWS RAM

AWS Resource Access Manager (AWS RAM)를 사용하면 한에서 생성한 AWS 리소스를 다른 AWS 계정 와 안전하게 공유할 수 있습니다 AWS 계정.는 리소스 공유를 관리하고 계정 간에이 경험을 표준화할 수 있는 중앙 위치를AWS RAM 제공합니다. 따라서 관리 및 청구 격리를 활용하면서 리소스를 더욱 쉽게 관리하고, 다중 계정 전략이 제공하는 영향 억제 혜택의 범위를 줄일 수 있습니다. 계정이에서 관리되는 경우 AWS Organizations조직의 모든 계정 또는 하나 이상의 지정된 조직 단위(OU) 내의 계정과만 리소스를 AWS RAM 공유할 수 있습니다.OUs 계정이 조직의 일부인지 여부에 관계없이 계정 ID AWS 계정 별로 특정와 공유할 수도 있습니다. 지원되는 일부 리소스 유형을 특정 IAM 역할 및 사용자와 공유할 수도 있습니다.

AWS RAM 를 사용하면 VPC 서브넷 및 Route 53 규칙과 같은 IAM 리소스 기반 정책을 지원하지 않는 리소스를 공유할 수 있습니다. 또한 리소스 AWS RAM소유자는 공유한 개별 리소스에 액세스할 수 있는 보안 주체를 확인할 수 있습니다. IAM 보안 주체는 IAM 리소스 정책에서 공유하는 리소스로는 수행할 수 없는 공유 리소스 목록을 직접 검색할 수 있습니다. AWS RAM 를 사용하여 AWS 조직 외부에서 리소스를 공유하면 초대 프로세스가 시작됩니다. 수신자는 리소스에 대한 액세스 권한이 부여되기 전에 초대를 수락해야 합니다. 그러면 추가 확인 및 밸런스가 제공됩니다.

AWS RAM 는 공유 리소스가 배포된 계정에서 리소스 소유자가 호출하고 관리합니다. AWS SRA에 AWS RAM 설명된의 일반적인 사용 사례 중 하나는 네트워크 관리자가 VPC 서브넷 및 전송 게이트웨이를 전체 AWS 조직과 공유하는 것입니다. 이를 통해 AWS 계정 및 네트워크 관리 기능을 분리할 수

있으며 업무 분리를 달성할 수 있습니다. VPC 공유에 대한 자세한 내용은 AWS 블로그 게시물 VPC 공유: 여러 계정 및 VPC 관리에 대한 새로운 접근 방식 및 AWS 네트워크 인프라 백서를 참조하세요.

> 설계 고려 사항
>
> AWS RAM 서비스는 AWS SRA의 네트워크 계정 내에만 배포되지만 일반적으로 둘 이상의 계정에 배포됩니다. 예를 들어 데이터 레이크 관리를 단일 데이터 레이크 계정으로 중앙 집중화한 다음 AWS Lake Formation 데이터 카탈로그 리소스(데이터베이스 및 테이블)를 AWS 조직의 다른 계정과 공유할 수 있습니다. 자세한 내용은 AWS Lake Formation 설명서와 AWS 블로그 게시물를 AWS 계정 사용하여 간에 데이터를 안전하게 공유를 참조하세요 AWS Lake Formation. 또한 보안 관리자는 AWS RAM 를 사용하여 AWS Private Certificate Authority 계층 구조를 구축할 때 모범 사례를 따를 수 있습니다. CAs는 CA 계층 구조에 액세스하지 않고도 인증서를 발급할 수 있는 외부 타사와 공유할 수 있습니다. 이를 통해 기존 조직은 타사 액세스를 제한하고 철회할 수 있습니다.

AWS Verified Access

AWS Verified Access는 VPN 없이 회사 애플리케이션 및 리소스에 대한 보안 액세스를 제공합니다. 사전 정의된 요구 사항에 따라 각 액세스 요청을 실시간으로 평가하여 보안 태세를 개선하고 제로 트러스트 액세스를 적용하는 데 도움이 됩니다. 자격 증명 데이터 및 디바이스 상태를 기반으로 하는 조건으로 각 애플리케이션에 대한 고유한 액세스 정책을 정의할 수 있습니다. Verified·Access는 Git 리포지토리, 데이터베이스 및 EC2 인스턴스 그룹과 같은 애플리케이션의 TCP, SSH 및 RDP 프로토콜을 통해 브라우저 기반 애플리케이션과 같은 HTTP(S) 애플리케이션과 비 HTTP(S) 애플리케이션에 대한 보안 액세스를 제공합니다. 명령줄 터미널을 사용하거나 데스크톱 애플리케이션에서 액세스할 수 있습니다. 또한 Verified Access는 관리자가 액세스 정책을 효율적으로 설정하고 모니터링할 수 있도록 지원하여 보안 작업을 간소화합니다. 따라서 정책을 업데이트하고, 보안 및 연결 사고에 대응하고, 규정 준수 표준을 감사할 시간을 확보할 수 있습니다. 또한 Verified Access는 와의 통합을 지원 AWS WAF 하여 SQL 주입 및 교차 사이트 스크립팅(XSS)과 같은 일반적인 위협을 필터링하는 데 도움이 됩니다. Verified·Access는와 원활하게 통합되어 사용자가 SAML 기반 서드 파티 자격 증명 공급자(IdP)로 인증할 AWS IAM Identity Center수 있습니다.IdPs OpenID Connect(OIDC)와 호환되는 사용자 지정 IdP 솔루션이 이미 있는 경우 Verified Access는 IdP에 직접 연결하여 사용자를 인증할 수도 있습니다. Verified Access는 모든 액세스 시도를 로깅하므로 보안 사고 및 감사 요청에 신속하게 대응할 수 있습니다. Verified·Access는 이러한 로그를 Amazon Simple Storage Service(Amazon S3), Amazon CloudWatch Logs 및 Amazon Data Firehose로 전송할 수 있도록 지원합니다.

Verified Access는 두 가지 일반적인 기업 애플리케이션 패턴인 내부 및 인터넷 경계를 지원합니다. Verified Access는 Application Load Balancer 또는 탄력적 네트워크 인터페이스를 사용하여 애플리케

이션과 통합됩니다. Application Load Balancer를 사용하는 경우 Verified Access에는 내부 로드 밸런서가 필요합니다. Verified·Access는 인스턴스 수준에서 AWS WAF 를 지원하므로 Application Load Balancer와 통합된 기존 애플리케이션은 AWS WAF 로드 밸런서에서 Verified·Access 인스턴스로 정책을 이동할 수 있습니다. 기업 애플리케이션은 Verified Access 엔드포인트로 표시됩니다. 각 엔드포인트는 Verified Access 그룹과 연결되며 그룹에 대한 액세스 정책을 상속합니다. Verified Access 그룹은 Verified Access 엔드포인트와 그룹 수준의 확인된 액세스 정책의 모음입니다. 그룹은 정책 관리를 간소화하고 IT 관리자가 기준을 설정할 수 있도록 지원합니다. 애플리케이션 소유자는 애플리케이션의 민감도에 따라 세분화된 정책을 추가로 정의할 수 있습니다.

AWS SRA에서 Verified·Access는 네트워크 계정 내에서 호스팅됩니다. 중앙 IT 팀은 중앙에서 관리되는 구성을 설정합니다. 예를 들어 ID 제공업체(예: Okta)와 디바이스 신뢰 제공업체(예: Jamf)와 같은 신뢰 제공자를 연결하고, 그룹을 생성하고, 그룹 수준 정책을 결정할 수 있습니다. 그런 다음를 사용하여 이러한 구성을 수십, 수백 또는 수천 개의 워크로드 계정과 공유할 수 있습니다 AWS RAM. 이를 통해 애플리케이션 팀은 다른 팀의 오버헤드 없이 애플리케이션을 관리하는 기본 엔드포인트를 관리할 수 있습니다.는 다양한 워크로드 계정에서 호스팅되는 기업 애플리케이션에 Verified Access를 활용할 수 있는 확장 가능한 방법을 AWS RAM 제공합니다.

> 설계 고려 사항
>
> 보안 요구 사항이 유사한 애플리케이션에 대한 엔드포인트를 그룹화하여 정책 관리를 간소화하고, 이 그룹을 애플리케이션 계정과 공유할 수 있습니다. 그룹 내 모든 애플리케이션은 그룹 정책을 공유합니다. 엣지 케이스 때문에 그룹의 애플리케이션에 특정 정책이 필요한 경우 해당 애플리케이션에 애플리케이션 수준 정책을 적용할 수 있습니다.

Amazon VPC Lattice

Amazon VPC Lattice는 service-to-service 통신을 연결, 모니터링 및 보호하는 애플리케이션 네트워킹 서비스입니다. 마이크로서비스라고도 하는 서비스는 특정 작업을 제공하는 독립적으로 배포 가능한 소프트웨어 단위입니다. VPC Lattice는 기본 네트워크 연결, 프런트엔드 로드 밸런서 또는 사이드카 프록시를 관리할 필요 AWS 계정 없이 VPCs 및 간의 서비스 간 네트워크 연결 및 애플리케이션 계층 라우팅을 자동으로 관리합니다. 경로 및 헤더와 같은 요청 특성을 기반으로 애플리케이션 수준 라우팅을 제공하는 종합 관리형 애플리케이션 계층 프록시를 제공합니다. VPC Lattice는 VPC 인프라에 내장되어 있으므로 Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Kubernetes Service(Amazon EKS) 및와 같은 다양한 컴퓨팅 유형에서 일관된 접근 방식을 제공합니다 AWS Lambda. 또한 VPC Lattice는 블루/그린 및 canary 스타일 배포에 대한 가중치 기반 라우팅을 지원합니다. VPC Lattice를 사용하여 서비스 검색 및 연결을 자동으로 구현하는 논리적 경계가 있는 서비스 네

트워크를 생성할 수 있습니다. VPC Lattice는 인증 정책을 사용한 service-to-service 인증 및 권한 부여를 위해 IAM과 통합됩니다.

VPC Lattice는와 통합되어 서비스 및 서비스 네트워크를 공유할 AWS RAM 수 있습니다. AWS SRA는 개발자 또는 서비스 소유자가 애플리케이션 계정에서 VPC Lattice 서비스를 생성하는 분산 아키텍처를 보여줍니다. 서비스 소유자는 인증 정책과 함께 리스너, 라우팅 규칙 및 대상 그룹을 정의합니다. 그런 다음 서비스를 다른 계정과 공유하고, 서비스를 VPC Lattice 서비스 네트워크와 연결합니다. 이러한 네트워크는 네트워크 관리자가 Network 계정에서 생성하고 Application 계정과 공유합니다. 네트워크 관리자는 서비스 네트워크 수준 인증 정책 및 모니터링을 구성합니다. 관리자는 VPC와 VPC Lattice 서비스를 하나 이상의 서비스 네트워크와 연결합니다. 이 분산 아키텍처에 대한 자세한 내용은 AWS 블로그 게시물 Amazon VPC Lattice를 사용하여 애플리케이션을 위한 안전한 다중 계정 다중 VPC 연결 구축을 참조하세요.

설계 고려 사항

- 조직의 서비스 또는 서비스 네트워크 가시성 운영 모델에 따라 네트워크 관리자는 서비스 네트워크를 공유하고 서비스 소유자에게 서비스 및 VPCs를 이러한 서비스 네트워크와 연결할 수 있는 제어 권한을 부여할 수 있습니다. 또는 서비스 소유자가 서비스를 공유하고, 네트워크 관리자는 서비스를 서비스 네트워크에 연결할 수 있습니다.
- 클라이언트는 동일한 서비스 네트워크와 연결된 VPC에 있는 경우에만 서비스 네트워크와 연결된 서비스에 요청을 보낼 수 있습니다. VPC 피어링 연결 또는 전송 게이트웨이를 통과하는 클라이언트 트래픽은 거부됩니다.

엣지 보안

엣지 보안에는 일반적으로 보안 콘텐츠 전송, 네트워크 및 애플리케이션 계층 보호, 분산 서비스 거부(DDoS) 완화라는 세 가지 유형의 보호가 수반됩니다. 권장 버전의 TLS를 사용하여 엔드포인트 간 통신을 암호화하여 데이터, 비디오, 애플리케이션, API와 같은 콘텐츠를 빠르고 안전하게 제공해야 합니다. 또한 콘텐츠에는 서명된 URL, 서명된 쿠키 및 토큰 인증을 통한 액세스 제한이 적용되어야 합니다. 애플리케이션 수준 보안은 봇 트래픽을 제어하고, SQL 명령어 삽입 또는 크로스 사이트 스크립팅(XSS)과 같은 일반적인 공격 패턴을 차단하고, 웹 트래픽 가시성을 제공하도록 설계되어야 합니다. 엣지에서 DDoS 완화는 미션 크리티컬 비즈니스 운영 및 서비스의 지속적인 가용성을 보장하는 중요한 방어 계층을 제공합니다. 애플리케이션과 API는 SYN 플러드, UDP 플러드 또는 기타 반사 공격으로부터 보호되어야 하며 기본적인 네트워크 계층 공격을 차단할 수 있는 인라인 완화 기능을 갖추어야 합니다.

AWS 는 코어 클라우드에서 AWS 네트워크 엣지에 이르기까지 안전한 환경을 제공하는 데 도움이 되는 여러 서비스를 제공합니다. Amazon CloudFront, AWS Certificate Manager (ACM) AWS Shield AWS WAF및 Amazon Route 53은 유연하고 계층화된 보안 경계를 생성하는 데 도움이 됩니다. CloudFront를 사용하면 TLSv1.3을 사용하여 최종 사용자 클라이언트와 CloudFront 간의 통신을 암호화하고 보호하여 HTTPS를 통해 콘텐츠, APIs 또는 애플리케이션을 제공할 수 있습니다. ACM을 사용하여 사용자 지정 SSL 인증서를 생성하고 CloudFront 배포에 무료로 배포할 수 있습니다. ACM은 인증서 갱신을 자동으로 처리합니다. Shield는에서 실행되는 애플리케이션을 보호하는 데 도움이 되는 관리형 DDoS 보호 서비스입니다 AWS. 애플리케이션 가동 중지 시간과 지연 시간을 최소화하는 동적 탐지 및 자동 인라인 완화 기능을 제공합니다. 특정 조건(IP 주소, HTTP 헤더 및 본문 또는 사용자 지정 URIs), 일반적인 웹 공격 및 퍼베이시브 봇을 기반으로 웹 트래픽을 필터링하는 규칙을 AWS WAF 생성할 수 있습니다. Route 53은 가용성과 확장성이 뛰어난 DNS 웹 서비스입니다. Route 53는 사용자 요청을 AWS 또는 온프레미스에서 실행되는 인터넷 애플리케이션에 연결합니다. AWS SRA는 네트워크 계정 내에서 AWS Transit Gateway호스팅되는를 사용하여 중앙 집중식 네트워크 수신 아키텍처를 채택하므로 엣지 보안 인프라도이 계정에서 중앙 집중식입니다.

Amazon CloudFront

Amazon CloudFront는 공통 네트워크 계층 및 전송 DDoS 시도에 대한 고유한 보호 기능을 제공하는 안전한 콘텐츠 배포 네트워크(CDN)입니다. TLS 인증서를 사용하여 콘텐츠, API 또는 애플리케이션을 배포할 수 있으며, 고급 TLS 기능은 자동으로 활성화됩니다. ACM 섹션의 뒷부분에 설명된 대로 AWS Certificate Manager (ACM)을 사용하여 사용자 지정 TLS 인증서를 생성하고 최종 사용자와 CloudFront 간에 HTTPS 통신을 적용할 수 있습니다. 추가로 CloudFront와 사용자 지정 오리진 간의 통신에서 전송 시 종단 간 암호화를 구현하도록 요구할 수 있습니다. 이 시나리오의 경우 오리진 서버에 TLS 인증서를 설치해야 합니다. 오리진이 탄력적 로드 밸런서인 경우 ACM에서 생성한 인증서 또는 타사 인증 기관(CA)에서 검증하고 ACM으로 가져온 인증서를 사용할 수 있습니다. S3 버킷 웹 사이트 엔드포인트가 CloudFront의 오리진 역할을 하는 경우 Amazon S3가 웹 사이트 엔드포인트에 HTTPS를 지원하지 않으므로 오리진과 함께 HTTPS를 사용하도록 CloudFront를 구성할 수 없습니다. (하지만 최종 사용자와 CloudFront 사이에 HTTPS를 요구할 수 있습니다.) HTTPS 인증서 설치를 지원하는 다른 모든 오리진의 경우 신뢰할 수 있는 타사 CA에서 서명한 인증서를 사용해야 합니다.

CloudFront는 콘텐츠에 대한 액세스를 보호하고 제한하는 여러 옵션을 제공합니다. 예를 들어 서명된 URL과 서명된 쿠키를 사용하여 Amazon S3 오리진에 대한 액세스를 제한할 수 있습니다. 자세한 내용은 CloudFront 설명서의 보안 액세스 구성 및 콘텐츠에 대한 액세스 제한을 참조하세요.

AWS SRA는를 사용하여 구현된 중앙 집중식 네트워크 패턴과 일치하므로 네트워크 계정의 중앙 집중식 CloudFront 배포를 보여줍니다 AWS Transit Gateway. Network 계정에서 CloudFront를 배포하고 배포를 관리하면 중앙 집중식 제어의 이점을 얻을 수 있습니다. 모든 CloudFront 배포를 한 곳에서 관리할 수 있으므로 모든 계정의 액세스를 제어하고, 설정을 구성하고, 사용량을 모니터링하기 더욱 쉽습

니다. 또한 하나의 중앙화된 계정에서 ACM 인증서, DNS 레코드 및 CloudFront 로깅을 관리할 수 있습니다.

CloudFront 보안 대시보드는 CloudFront 배포에서 직접 AWS WAF 가시성과 제어를 제공합니다. 애플리케이션의 주요 보안 추세, 허용 및 차단된 트래픽, 봇 활동을 파악할 수 있습니다. 시각적 로그 분석기 및 기본 제공 차단 제어와 같은 조사 도구를 사용하여 로그를 쿼리하거나 보안 규칙을 작성하지 않고도 트래픽 패턴을 격리하고 트래픽을 차단할 수 있습니다.

설계 고려 사항

- 또는 Application 계정에서 애플리케이션의 일부로 CloudFront를 배포할 수도 있습니다. 이 시나리오에서 애플리케이션 팀은 CloudFront 배포의 배포 방법과 같은 결정을 내리고, 적절한 캐시 정책을 결정하고, CloudFront 배포의 거버넌스, 감사, 모니터링을 담당합니다. CloudFront 배포를 여러 계정에 분산하면 추가 서비스 할당량 이점을 누릴 수 있습니다. 또 다른 이점으로 CloudFront의 고유하고 자동화된 오리진 액세스 ID(OAI) 및 오리진 액세스 제어(OAC) 구성을 사용하여 Amazon S3 오리진에 대한 액세스를 제한할 수 있습니다.
- CloudFront와 같은 CDN을 통해 웹 콘텐츠를 배포하는 경우 최종 사용자가 CDN을 우회하여 오리진 콘텐츠에 직접 액세스하는 것을 방지해야 합니다. 이 오리진 액세스 제한을 달성하려면 CloudFront 및 AWS WAF 를 사용하여 사용자 지정 오리진에 요청을 전달하기 전에 사용자 지정 헤더를 추가하고 헤더를 확인할 수 있습니다. 이 솔루션에 대한 자세한 설명은 AWS 보안 블로그 게시물 AWS WAF 및를 사용하여 Amazon CloudFront 오리진 보안을 강화하는 방법을 참조하세요 AWS Secrets Manager. 대체 방법은 Application Load Balancer와 연결된 보안 그룹의 CloudFront 접두사 목록만 제한하는 것입니다. 이렇게 하면 CloudFront 배포만 로드 밸런서에 액세스할 수 있게 됩니다.

AWS WAF

AWS WAF는 애플리케이션 가용성에 영향을 미치거나, 보안을 손상시키거나, 과도한 리소스를 소비할 수 있는 일반적인 취약성 및 봇과 같은 웹 악용으로부터 웹 애플리케이션을 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. Amazon CloudFront 배포, Amazon API Gateway REST API, Application Load Balancer, an AWS AppSync GraphQL API, Amazon Cognito 사용자 풀 및 AWS App Runner 서비스와 통합할 수 있습니다.

AWS WAF 는 웹 액세스 제어 목록(ACLs)을 사용하여 AWS 리소스 세트를 보호합니다. 웹 ACL은 검사 기준을 정의하는 규칙 세트와 웹 요청이 기준을 충족하는 경우 수행할 관련 작업(봇 제어 차단, 허용, 계산 또는 실행)입니다.는 일반적인 애플리케이션 취약성에 대한 보호를 제공하는 관리형 규칙 세트를

AWS WAF 제공합니다. 이러한 규칙은 AWS 및 AWS Partners에서 큐레이션하고 관리합니다. AWS WAF 또한는 사용자 지정 규칙을 작성하기 위한 강력한 규칙 언어를 제공합니다. 사용자 지정 규칙을 사용하여 특정 요구 사항에 맞는 검사 기준을 작성할 수 있습니다. IP 제한, 지리적 제한, 특정 애플리케이션 동작에 더 적합한 관리형 규칙의 사용자 지정 버전 등을 예로 들 수 있습니다.

AWS WAF 는 공통 및 대상 봇과 계정 탈취 방지(ATP)를 위한 지능형 계층 관리형 규칙 세트를 제공합니다. Bot Control 및 ATP 규칙 그룹을 사용하는 경우 구독 요금과 트래픽 검사 요금이 부과됩니다. 따라서 트래픽을 먼저 모니터링하고 무엇을 사용할지 결정하는 것이 좋습니다. 콘솔에서 AWS WAF 무료로 사용할 수 있는 봇 관리 및 계정 탈취 대시보드를 사용하여 이러한 활동을 모니터링한 다음 지능형 계층 AWS WAF 규칙 그룹이 필요한지 여부를 결정할 수 있습니다.

AWS SRA에서 AWS WAF 는 네트워크 계정의 CloudFront와 통합됩니다. 이 구성에서 AWS WAF 규칙 처리는 VPC 내부가 아닌 엣지 로케이션에서 수행됩니다. 이를 통해 콘텐츠를 요청한 최종 사용자와 가까운 곳에서 악성 트래픽을 필터링할 수 있고, 코어 네트워크로 들어오는 악성 트래픽을 제한할 수 있습니다.

S3 버킷에 AWS WAF 대한 교차 계정 액세스를 구성하여 로그 아카이브 계정의 S3 버킷에 전체 로그를 전송할 수 있습니다. 자세한 내용은이 주제에 대한 AWS re:Post 문서를 참조하세요.

설계 고려 사항

- 네트워크 계정에서 AWS WAF 중앙에 배포하는 대신 애플리케이션 계정에 배포하면 일부 사용 사례를 더 잘 충족할 AWS WAF 수 있습니다. 예를 들어 애플리케이션 계정에 CloudFront 배포를 배포하거나 퍼블릭 Application Load Balancer가 있거나 웹 애플리케이션 앞에 API Gateway를 사용하는 경우이 옵션을 선택할 수 있습니다. AWS WAF 각 애플리케이션 계정에 배포하기로 결정한 경우 AWS Firewall Manager 를 사용하여 중앙 집중식 보안 도구 계정에서 이러한 계정의 규칙을 관리합니다 AWS WAF .
- 또한 CloudFront 계층에서 일반 AWS WAF 규칙을 추가하고 Application Load Balancer 또는 API 게이트웨이와 같은 리전 리소스에서 애플리케이션별 AWS WAF 규칙을 추가할 수 있습니다.

AWS Shield

AWS Shield는에서 실행되는 애플리케이션을 보호하는 관리형 DDoS 보호 서비스입니다 AWS. Shield에는 Shield Standard와 Shield Advanced라는 두 가지 티어가 있습니다. Shield Standard는 모든 AWS 고객에게 추가 비용 없이 가장 일반적인 인프라(계층 3 및 4) 이벤트에 대한 보호를 제공합니다. Shield

Advanced는 보호된 Amazon EC2, Elastic Load Balancing(Elastic Load Balancing), CloudFront AWS Global Accelerator및 Route 53 호스팅 영역의 애플리케이션을 대상으로 하는 무단 이벤트에 대해 보다 정교한 자동 완화 기능을 제공합니다. 가시성이 높은 웹 사이트를 소유하거나 DDoS 공격이 자주 발생하는 경우 Shield Advanced가 제공하는 추가 기능을 고려할 수 있습니다.

Shield Advanced 자동 애플리케이션 계층 DDoS 완화 기능을 사용하여 보호된 CloudFront 배포, Elastic Load Balancing(Elastic Load Balancing) 로드 밸런서(애플리케이션, 네트워크 및 클래식), Amazon Route 53 호스팅 영역, Amazon EC2 탄력적 IP 주소 및 AWS Global Accelerator 표준 액셀러레이터에 대한 애플리케이션 계층(계층 7) 공격을 자동으로 완화하도록 Shield Advanced를 구성할 수 있습니다. 이 기능을 활성화하면 Shield Advanced는 DDoS 공격을 완화하기 위한 사용자 지정 AWS WAF 규칙을 자동으로 생성합니다. 또한 Shield Advanced는 AWS Shield 대응 팀(SRT)에 대한 액세스 권한을 제공합니다. 진행 중인 DDoS 공격 중에 언제든지 SRT에 문의하여 애플리케이션에 대한 사용자 지정 완화 기능을 만들고 관리할 수 있습니다. SRT에서 보호되는 리소스를 사전에 모니터링하고 DDoS 시도 중에 연락을 취하도록 하려면 사전 참여 기능을 활성화하는 것이 좋습니다.

설계 고려 사항

- CloudFront, Application Load Balancer 또는 Network Load Balancer와 같은 애플리케이션 계정의 인터넷 연결 리소스가 앞에 있는 워크로드가 있는 경우 애플리케이션 계정에서 Shield Advanced를 구성하고 해당 리소스를 Shield 보호에 추가합니다. AWS Firewall Manager 를 사용하여 이러한 옵션을 대규모로 구성할 수 있습니다.
- Application Load Balancer 앞에 CloudFront 배포와 같이 데이터 흐름에 여러 리소스가 있는 경우 진입점 리소스만 보호된 리소스로 사용합니다. 이렇게 하면 두 리소스에 대해 Shield 데이터 전송(DTO) 요금을 두 번 지불하지 않아도 됩니다.
- Shield Advanced는 Amazon CloudWatch에서 모니터링할 수 있는 지표를 기록합니다. (자세한 내용은 AWS 설명서의 Amazon CloudWatch를 사용한 모니터링을 참조하세요.) DDoS 이벤트가 탐지되면 보안 센터로 SNS 알림을 수신하도록 CloudWatch 경보를 설정합니다. DDoS 이벤트가 의심되는 경우 지원 티켓을 제출하고 가장 높은 우선 순위를 할당하여 AWS 엔터프라이즈 지원 팀에 문의하세요. Enterprise Support 팀은 이벤트 처리 시 Shield 대응 팀(SRT)을 포함할 것입니다. 또한 AWS Shield 참여 Lambda 함수를 사전 구성하여 지원 티켓을 생성하고 SRT 팀에 이메일을 보낼 수 있습니다.

AWS Certificate Manager (ACM)

AWS Certificate Manager (ACM)를 사용하면 및 내부 연결 리소스와 함께 사용할 퍼블릭 및 프라이빗 TLS 인증서를 프로비저닝, 관리 AWS 서비스 및 배포할 수 있습니다. ACM을 사용하면 인증서를 빠르

게 요청하고, Amazon API Gateway의 Elastic Load Balancing 로드 밸런서, CloudFront 배포 및 APIs와 같은 ACM 통합 AWS 리소스에 배포하고, ACM이 인증서 갱신을 처리하도록 할 수 있습니다. ACM 퍼블릭 인증서를 요청할 때 키 페어 또는 인증서 서명 요청(CSR)을 생성하거나, 인증 기관(CA)에 CSR을 제출하거나, 인증서를 수신할 때 인증서를 업로드하고 설치할 필요가 없습니다. 또한 ACM은 타사 CA에서 발급한 TLS 인증서를 가져와 ACM 통합 서비스에 배포할 수 있는 옵션을 제공합니다. ACM을 사용하여 인증서를 관리하는 경우 강력한 암호화 및 키 관리 모범 사례를 사용하여 인증서 프라이빗 키를 안전하게 보호하고 저장합니다. ACM을 사용하면 퍼블릭 인증서 프로비저닝에 대한 추가 비용이 없으며, ACM에서 갱신 프로세스를 관리합니다.

Network 계정에서 ACM은 퍼블릭 TLS 인증서를 생성하는 데 사용되고, CloudFront 배포에서는 이를 사용하여 최종 사용자와 CloudFront 간에 HTTPS 연결을 설정합니다. 자세한 내용은 CloudFront 설명서를 참조하세요.

> 설계 고려 사항
>
> 외부 인증서의 경우 ACM은 인증서를 프로비저닝하는 리소스와 동일한 계정에 있어야 합니다. 인증서는 계정 간에 공유될 수 없습니다.

Amazon Route 53

Amazon Route 53는 가용성과 확장성이 뛰어난 DNS 웹 서비스입니다. Route 53을 사용하여 세 가지 주요 기능, 즉 도메인 등록, DNS 라우팅, 상태 확인을 실행할 수 있습니다.

Route 53을 DNS 서비스로 사용하여 도메인 이름을 EC2 인스턴스, S3 버킷, CloudFront 배포 및 기타 AWS 리소스에 매핑할 수 있습니다. AWS DNS 서버의 분산 특성은 최종 사용자가 애플리케이션에 일관되게 라우팅되도록 하는 데 도움이 됩니다. Route 53 트래픽 흐름 및 라우팅 제어와 같은 기능은 신뢰성을 개선하는 데 도움이 됩니다. 기본 애플리케이션 엔드포인트를 사용할 수 없게 되는 경우 사용자를 다른 위치로 다시 라우팅하도록 장애 조치를 구성할 수 있습니다. Route 53 Resolver는 AWS Direct Connect 또는 AWS 관리형 VPN을 통해 VPC 및 온프레미스 네트워크에 대한 재귀 DNS를 제공합니다.

Route 53에서 IAM 서비스를 사용하면 DNS 데이터를 업데이트할 수 있는 사용자를 세밀하게 제어할 수 있습니다. DNS Security Extensions(DNSSEC) 서명을 활성화하여 DNS 해석기가 DNS 응답이 Route 53에서 왔으며 변조되지 않았는지 검증할 수 있습니다.

Route 53 Resolver DNS Firewall은 VPC의 아웃바운드 DNS 요청을 보호합니다. 이러한 요청은 도메인 이름 해석을 위해 Route 53 Resolver를 통과합니다. DNS 방화벽 보호의 주된 용도는 데이터의

DNS 유출을 방지하는 것입니다. DNS 방화벽을 사용하면 애플리케이션에서 쿼리할 수 있는 도메인을 모니터링하고 제어할 수 있습니다. 잘못된 것으로 알고 있는 도메인에 대한 액세스를 거부하고 다른 모든 쿼리가 통과하도록 허용할 수 있습니다. 또는 명시적으로 신뢰하는 도메인을 제외한 모든 도메인에 대한 액세스를 거부할 수 있습니다. DNS 방화벽을 사용하여 VPC 엔드포인트 이름을 포함하여 프라이빗 호스팅 영역(공유 또는 로컬 호스팅 영역)의 리소스에 대한 해석 요청을 차단할 수도 있습니다. 또한 퍼블릭 또는 프라이빗 EC2 인스턴스 이름에 대한 요청을 차단할 수도 있습니다.

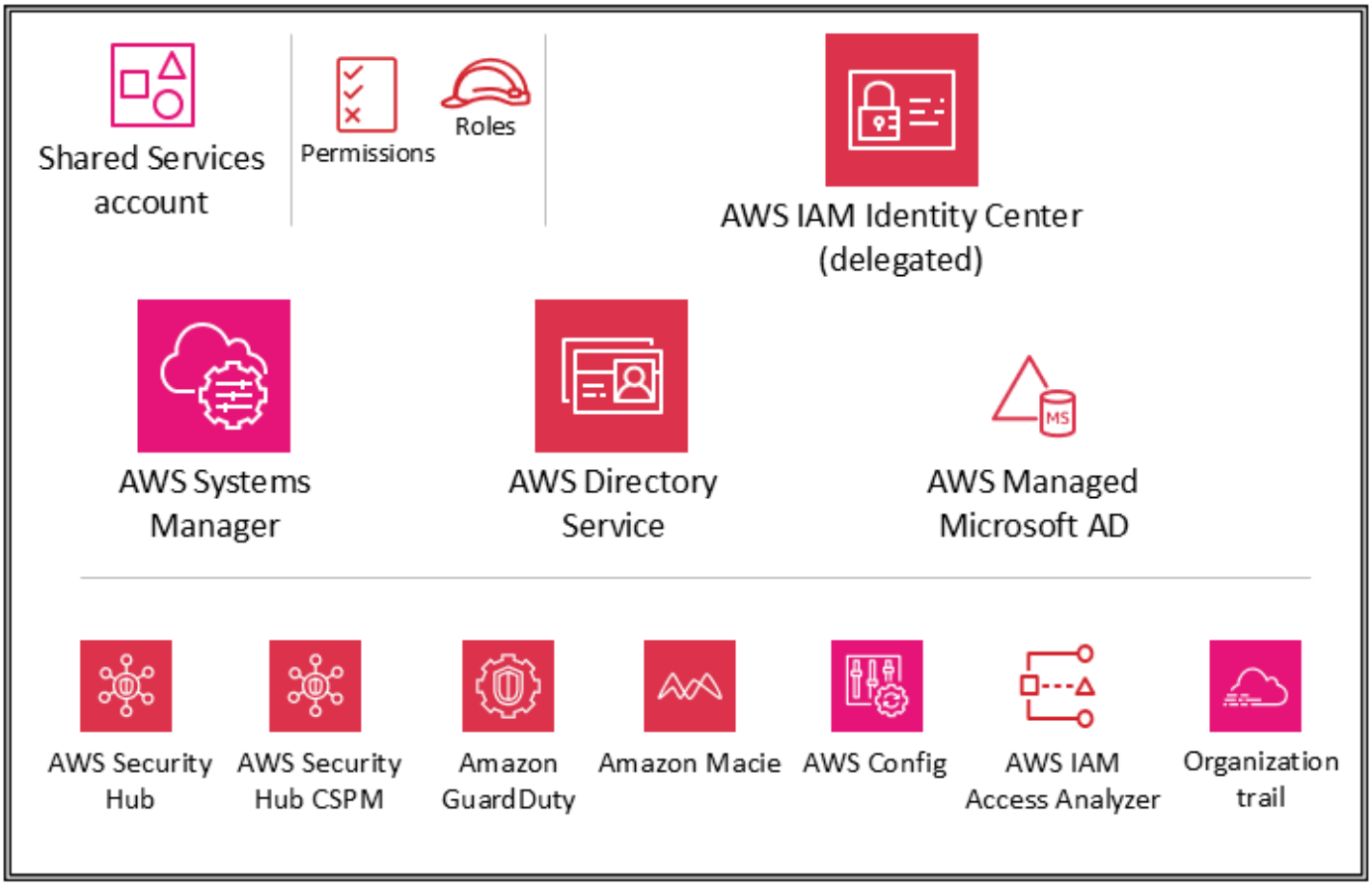
Route 53 해석기는 기본적으로 모든 VPC의 일부분으로 생성됩니다. AWS SRA에서 Route 53은 주로 DNS 방화벽 기능에 네트워크 계정에서 사용됩니다.

> 설계 고려 사항
>
> DNS 방화벽과는 AWS Network Firewall 모두 도메인 이름 필터링을 제공하지만 트래픽 유형은 다릅니다. DNS 방화벽과 네트워크 방화벽을 함께 사용하여 두 가지 네트워크 경로를 통한 애플리케이션 계층 트래픽에 대한 도메인 기반 필터링을 구성할 수 있습니다.
>
> - DNS 방화벽은 VPC 내의 애플리케이션에서 Route 53 Resolver를 통과하는 아웃바운드 DNS 쿼리에 대한 필터링을 제공합니다. 쿼리에 대한 사용자 지정 응답을 차단된 도메인 이름에 전송하도록 DNS 방화벽을 구성할 수도 있습니다.
> - Network Firewall은 네트워크 및 애플리케이션 계층 트래픽 모두에 대한 필터링을 제공하지만 Route 53 Resolver에서 만든 쿼리는 표시하지 않습니다.

인프라 OU - 공유 서비스 계정

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

다음 다이어그램은 공유 서비스 계정에 구성된 AWS 보안 서비스를 보여줍니다.



공유 서비스 계정은 인프라 OU의 일부이며, 그 목적은 여러 애플리케이션과 팀이 결과를 제공하는 데 사용하는 서비스를 지원하는 것입니다. 예를 들어 디렉터리 서비스(Active Directory), 메시징 서비스 및 메타데이터 서비스는이 범주에 속합니다. AWS SRA는 보안 제어를 지원하는 공유 서비스를 강조 표시합니다. 네트워크 계정도 인프라 OU의 일부이지만 업무 분리를 지원하기 위해 공유 서비스 계정에서 제거됩니다. 이러한 서비스를 관리할 팀은 네트워크 계정에 대한 권한이나 액세스 권한이 필요하지 않습니다.

AWS Systems Manager

AWS Systems Manager (조직 관리 계정 및 애플리케이션 계정에도 포함됨)는 AWS 리소스의 가시성과 제어를 지원하는 기능 모음을 제공합니다. 이러한 기능 중 하나인 Systems Manager Explorer는 AWS 리소스에 대한 정보를 보고하는 사용자 지정 가능한 작업 대시보드입니다. AWS Organizations 및 Systems Manager Explorer를 사용하여 AWS 조직의 모든 계정에서 작업 데이터를 동기화할 수 있습니다. Systems Manager는의 위임된 관리자 기능을 통해 공유 서비스 계정에 배포됩니다 AWS Organizations.

Systems Manager는 관리형 인스턴스를 스캔하고 감지한 정책 위반을 보고(또는 수정 조치 수행)하여 보안 및 규정 준수를 유지하는 데 도움이 됩니다. Systems Manager를 개별 멤버 AWS 계정 (예: 애플리케이션 계정)의 적절한 배포와 페어링하면 인스턴스 인벤토리 데이터 수집을 조정하고 패치 및 보안 업데이트와 같은 자동화를 중앙 집중화할 수 있습니다.

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory라고도 하는를 AWS Managed Microsoft AD사용하면 디렉터리 인식 워크로드 및 AWS 리소스에서 관리형 Active Directory를 사용할 수 있습니다 AWS. AWS Managed Microsoft AD 를 사용하여 Windows Server용 Amazon EC2, Linux용 Amazon EC2 및 SQL Server용 Amazon RDS인스턴스를 도메인에 조인하고 Active Directory AWS 사용자 및 그룹과 함께 Amazon WorkSpaces와 같은 최종 사용자 컴퓨팅(EUC) 서비스를 사용할 수 있습니다. Amazon WorkSpaces

AWS Managed Microsoft AD 를 사용하면 기존 Active Directory를 로 확장 AWS 하고 기존 온프레미스 사용자 자격 증명을 사용하여 클라우드 리소스에 액세스할 수 있습니다. 또한 가용성이 높은 온프레미스 Active Directory를 실행하고 유지 관리하는 복잡성 없이 온프레미스 사용자, 그룹, 애플리케이션 및 시스템을 관리할 수 있습니다. 기존 컴퓨터, 랩톱 및 프린터를 AWS Managed Microsoft AD 도메인에 조인할 수 있습니다.

AWS Managed Microsoft AD 는 Microsoft Active Directory를 기반으로 하며 기존 Active Directory에서 클라우드로 데이터를 동기화하거나 복제할 필요가 없습니다. 그룹 정책 객체(GPOs), 도메인 신뢰, 세분화된 암호 정책, 그룹 관리형 서비스 계정(gMSAs), 스키마 확장, Kerberos 기반 Single Sign-On과 같은 익숙한 Active Directory 관리 도구 및 기능을 사용할 수 있습니다. Active Directory 보안 그룹을 사용하여 관리 작업을 위임하고 액세스 권한을 부여할 수도 있습니다.

다중 리전 복제를 사용하면 여러에 단일 AWS Managed Microsoft AD 디렉터리를 배포하고 사용할 수 있습니다 AWS 리전. 따라서 Microsoft Windows 및 Linux 워크로드를 전 세계에 더 쉽고 비용 효율적으로 배포하고 관리할 수 있습니다. 자동화된 다중 리전 복제 기능을 사용하면 애플리케이션이 최적의 성능을 위해 로컬 디렉터리를 사용하는 동안 복원력이 향상됩니다.

AWS Managed Microsoft AD 는 클라이언트 및 서버 역할 모두에서 LDAPS라고도 하는 SSL/TLS를 통한 LDAP(Lightweight Directory Access Protocol)를 지원합니다. 서버 역할을 할 때 AWS Managed Microsoft AD 는 포트 636(SSL) 및 389(TLS)를 통해 LDAPS를 지원합니다. AWS기반 Active Directory Certificate Services(AD CS) 인증 기관(CA)의 AWS Managed Microsoft AD 도메인 컨트롤러에 인증서를 설치하여 서버 측 LDAPS 통신을 활성화합니다. 클라이언트 역할을 할 때는 포트 636(SSL)을 통해 LDAPS를 AWS Managed Microsoft AD 지원합니다. 서버 인증서 발급자의 CA 인증서를에 등록하여 클라이언트 측 LDAPS 통신을 활성화 AWS한 다음 디렉터리에서 LDAPS를 활성화할 수 있습니다.

AWS SRA에서 Directory Service 는 공유 서비스 계정 내에서 여러 AWS 멤버 계정의 Microsoft 인식 워크로드에 대한 도메인 서비스를 제공하는 데 사용됩니다.

> 설계 고려 사항
>
> IAM Identity Center를 사용하고를 자격 증명 소스 AWS Managed Microsoft AD 로 선택하여 온프레미스 Active Directory 사용자에게 기존 Active Directory 자격 증명으로 AWS Management Console 및 AWS Command Line Interface (AWS CLI)에 로그인할 수 있는 액세스 권한을 부여할 수 있습니다. 이를 통해 사용자는 로그인 시 할당된 역할 중 하나를 수임하고 역할에 대해 정의된 권한에 따라 리소스에 액세스하고 조치를 취할 수 있습니다. 다른 옵션은를 사용하여 사용자가 IAM 역할을 수임할 수 AWS Managed Microsoft AD 있도록 하는 것입니다.

IAM Identity Center

AWS SRA는에서 지원하는 위임된 관리자 기능을 사용하여 IAM Identity Center 관리의 대부분을 공유 서비스 계정에 AWS IAM Identity Center 위임합니다. 이렇게 하면 조직 관리 계정에 액세스해야 하는 사용자 수를 제한하는 데 도움이 됩니다. 조직 관리 계정 내에서 프로비저닝된 권한 세트 관리를 포함하여 특정 작업을 수행하려면 조직 관리 계정에서 IAM Identity Center를 활성화해야 합니다.

공유 서비스 계정을 IAM Identity Center의 위임된 관리자로 사용하는 주된 이유는 Active Directory 위치입니다. Active Directory를 IAM Identity Center ID 소스로 사용하려는 경우 IAM Identity Center 위임된 관리자 계정으로 지정한 멤버 계정에서 디렉터리를 찾아야 합니다. AWS SRA에서 공유 서비스 계정은를 호스팅 AWS Managed Microsoft AD하므로 계정이 IAM Identity Center의 위임된 관리자가 됩니다.

IAM Identity Center는 한 번에 단일 멤버 계정을 위임된 관리자로 등록할 수 있도록 지원합니다. 멤버 계정은 관리 계정의 자격 증명으로 로그인할 때만 등록할 수 있습니다. 위임을 활성화하려면 IAM Identity Center 설명서에 나열된 사전 조건을 고려해야 합니다. 위임된 관리자 계정은 대부분의 IAM Identity Center 관리 작업을 수행할 수 있지만 IAM Identity Center 설명서에 나열된 몇 가지 제한이 있습니다. IAM Identity Center의 위임된 관리자 계정에 대한 액세스는 엄격하게 제어되어야 합니다.

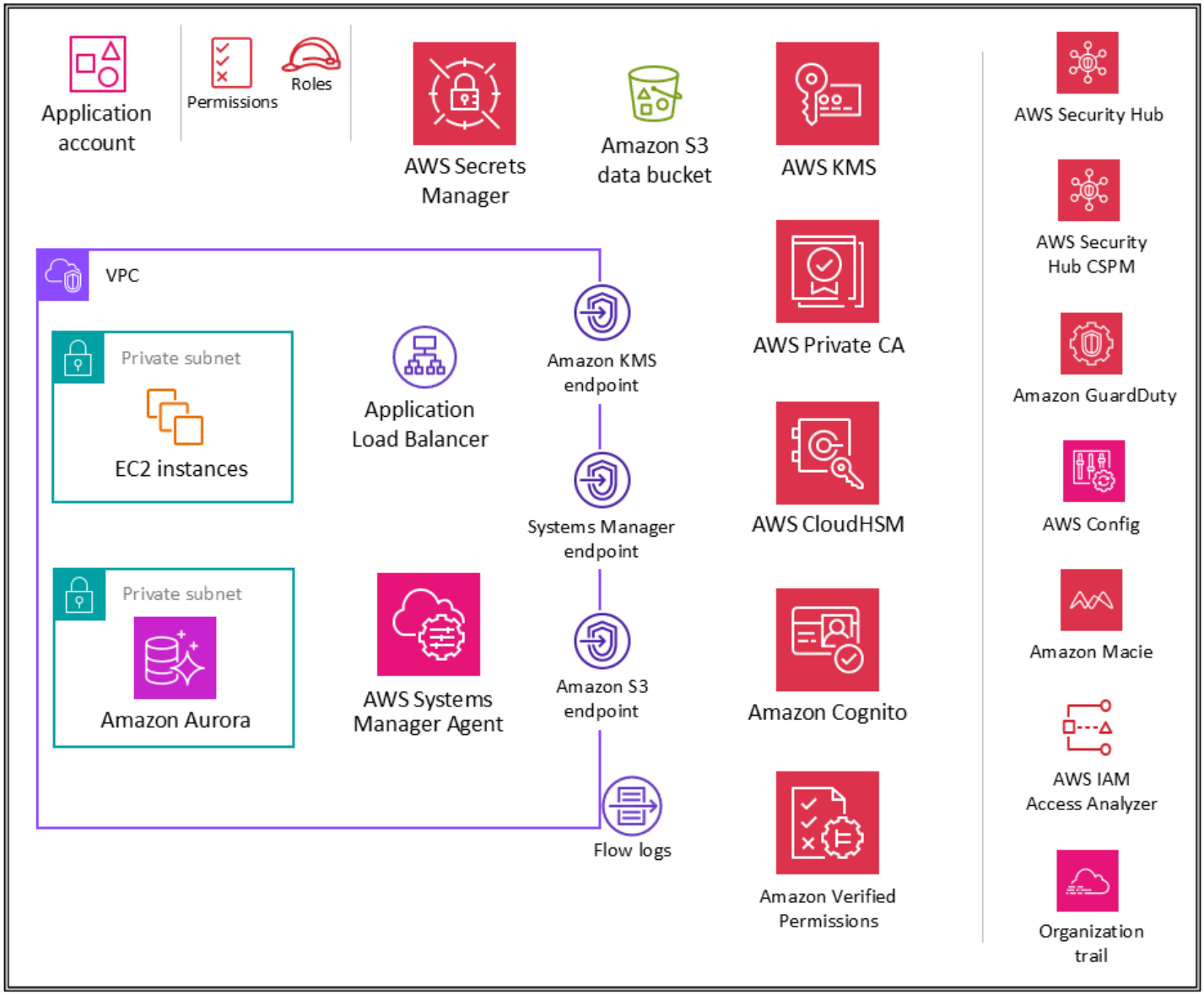
> 설계 고려 사항
>
> - IAM Identity Center ID 소스를 다른 소스에서 Active Directory로 변경하거나 Active Directory에서 다른 소스로 변경하려는 경우 디렉터리는 IAM Identity Center 위임된 관리자 계정(소유자)에 있어야 합니다. 그렇지 않으면 관리 계정에 있어야 합니다.

- 다른 계정의 전용 VPC AWS Managed Microsoft AD 내에서를 호스팅한 다음 AWS Resource Access Manager (AWS RAM)를 사용하여이 다른 계정의 서브넷을 위임된 관리자 계정과 공유할 수 있습니다. 이렇게 하면 AWS Managed Microsoft AD 인스턴스가 위임된 관리자 계정에서 제어되지만 네트워크 관점에서 다른 계정의 VPC에 배포된 것처럼 작동합니다. 이는 AWS Managed Microsoft AD 인스턴스가 여러 개 있고 워크로드가 실행 중인에 로컬로 배포하고 단일 계정을 통해 중앙에서 관리하려는 경우에 유용합니다.
- 정기적인 자격 증명 및 액세스 관리 활동을 수행하는 전용 자격 증명 팀이 있거나 자격 증명 관리 기능을 다른 공유 서비스 기능과 분리하기 AWS 계정 위한 엄격한 보안 요구 사항이 있는 경우 자격 증명 관리 전용를 호스팅할 수 있습니다. 이 시나리오에서는이 계정을 IAM Identity Center의 위임된 관리자로 지정하고 AWS Managed Microsoft AD 디렉터리도 호스팅합니다. 단일 공유 서비스 계정 내에서 세분화된 IAM 권한을 사용하여 ID 관리 워크로드와 기타 공유 서비스 워크로드 간에 동일한 수준의 논리적 격리를 달성할 수 있습니다.
- IAM Identity Center는 현재 다중 리전 지원을 제공하지 않습니다. (다른 리전에서 IAM Identity Center를 활성화하려면 먼저 현재 IAM Identity Center 구성을 삭제해야 합니다.) 또한 계정 세트마다 다른 자격 증명 소스 사용을 지원하지 않거나 조직의 다른 부분(즉, 위임된 여러 관리자) 또는 다른 관리자 그룹에 권한 관리를 위임할 수 없습니다. 이러한 기능이 필요한 경우 IAM 페더레이션을 사용하여 외부의 ID 제공업체(IdP) 내에서 사용자 ID를 관리하고 이러한 외부 사용자 ID에 계정의 AWS 리소스를 사용할 수 있는 권한을 AWS 부여할 수 있습니다. IAM은 OpenID Connect(OIDC) 또는 SAML 2.0과 호환되는 IdPs를 지원합니다. 가장 좋은 방법은 Active Directory Federation Service(AD FS), Okta, Azure Active Directory(Azure AD) 또는 Ping Identity와 같은 타사 자격 증명 공급자와의 SAML 2.0 페더레이션을 사용하여 사용자가에 로그인 AWS Management Console 하거나 AWS API 작업을 호출할 수 있는 Single Sign-On 기능을 제공하는 것입니다. IAM 페더레이션 및 자격 증명 공급자에 대한 자세한 내용은 IAM 설명서의 SAML 2.0 기반 페더레이션 정보를 참조하세요.

워크로드 OU – 애플리케이션 계정

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

다음 다이어그램은 (애플리케이션 자체와 함께) 애플리케이션 계정에 구성된 AWS 보안 서비스를 보여줍니다.



애플리케이션 계정은 엔터프라이즈 애플리케이션을 실행하고 유지하기 위해 기본 인프라와 서비스를 호스팅합니다. 애플리케이션 계정 및 워크로드 OU는 몇 가지 주요 보안 목표를 제공합니다. 먼저 각 애플리케이션에 대해 별도의 계정을 생성하여 워크로드 간에 경계와 제어를 제공하므로 역할, 권한, 데이터 및 암호화 키를 가져오는 문제를 방지할 수 있습니다. 애플리케이션 팀에 다른 사용자에게 영향을 주지 않고 자체 인프라를 관리할 수 있는 광범위한 권한을 부여할 수 있는 별도의 계정 컨테이너를 제공하려고 합니다. 다음으로 보안 운영 팀이 보안 데이터를 모니터링하고 수집할 수 있는 메커니즘을 제공하여 보호 계층을 추가합니다. 보안 팀이 구성하고 모니터링하는 계정 보안 서비스(Amazon GuardDuty, AWS Config AWS Security Hub CSPM,,, Amazon EventBridge, IAM Access Analyzer)의 조직 추적 및 로컬 배포를 사용합니다. 마지막으로 엔터프라이즈가 제어를 중앙에서 설정할 수 있도록 합니다. 애플리케이션 계정을 적절한 서비스 권한, 제약 조건 및 가드레일을 상속하는 워크로드 OU의 멤버로 만들어 더 광범위한 보안 구조에 맞게 조정합니다.

설계 고려 사항

조직에서는 비즈니스 애플리케이션이 두 개 이상 있을 수 있습니다. 워크로드 OU는 프로덕션 환경과 비프로덕션 환경을 포함하여 대부분의 비즈니스별 워크로드를 수용하기 위한 것입니다. 이러한 워크로드는 상용 off-the-shelf품(COTS) 애플리케이션과 자체적으로 개발된 사용자 지정 애플리케이션 및 데이터 서비스를 혼합한 것일 수 있습니다. 개발 환경과 함께 다양한 비즈니스 애플리케이션을 구성하는 패턴은 거의 없습니다. 한 가지 패턴은 프로덕션, 스테이징, 테스트 및 개발과 같은 개발 환경에 따라 하위 OUs를 여러 개 확보하고 이러한 OU AWS 계정에서 서로 다른 애플리케이션과 관련된 별도의 하위 OUs를 사용하는 것입니다. 또 다른 일반적인 패턴은 애플리케이션당 별도의 하위 OUs를 만든 다음 개별 개발 환경에 별도의 하위 OU AWS 계정 를 사용하는 것입니다. 정확한 OU 및 계정 구조는 애플리케이션 설계와 해당 애플리케이션을 관리하는 팀에 따라 달라집니다. 환경별 제어이든 애플리케이션별 제어이든 적용하려는 보안 제어를 고려합니다. 이러한 제어를 OUs에서 SCPs로 구현하는 것이 더 쉽기 때문입니다. 워크로드 지향 OUs 구성에 대한 추가 고려 사항은 AWS 백서 여러 계정을 사용하여 환경 구성의 애플리케이션 OUs 섹션을 참조하세요. AWS

애플리케이션 VPC

애플리케이션 계정의 Virtual Private Cloud(VPC)에는 인바운드 액세스(모델링 중인 간단한 웹 서비스의 경우)와 아웃바운드 액세스(애플리케이션 요구 사항 또는 AWS 서비스 요구 사항의 경우)가 모두 필요합니다. 기본적으로 VPC 내의 리소스는 서로 라우팅할 수 있습니다. 두 개의 프라이빗 서브넷이 있습니다. 하나는 EC2 인스턴스(애플리케이션 계층)를 호스팅하는 서브넷이고 다른 하나는 Amazon Aurora(데이터베이스 계층)를 호스팅하는 서브넷입니다. 애플리케이션 계층 및 데이터베이스 계층과 같은 다양한 계층 간의 네트워크 세분화는 인스턴스 수준에서 트래픽을 제한하는 VPC 보안 그룹을 통해 수행됩니다. 복원력을 위해 워크로드는 2개 이상의 가용 영역에 걸쳐 있으며 영역당 2개의 서브넷을 활용합니다.

설계 고려 사항

트래픽 미러링을 사용하여 EC2 인스턴스의 탄력적 네트워크 인터페이스에서 네트워크 트래픽을 복사할 수 있습니다. 그런 다음 콘텐츠 검사, 위협 모니터링 또는 문제 해결을 위해 트래픽을 out-of-band 보안 및 모니터링 어플라이언스로 전송할 수 있습니다. 예를 들어 VPC에서 나가는 트래픽 또는 소스가 VPC 외부에 있는 트래픽을 모니터링할 수 있습니다. 이 경우 VPC 내에서 전달되는 트래픽을 제외한 모든 트래픽을 미러링하여 단일 모니터링 어플라이언스로 전송합니다. Amazon VPC 흐름 로그는 미러링된 트래픽을 캡처하지 않으며, 일반적으로 패킷 헤더에서만 정보를 캡처합니다. 트래픽 미러링은 페이로드를 포함한 실제 트래픽 콘텐츠를 분석할 수

있도록 하여 네트워크 트래픽에 대한 심층적인 인사이트를 제공합니다. 민감한 워크로드의 일부로 작동하거나 문제 발생 시 자세한 진단이 필요할 것으로 예상되는 EC2 인스턴스의 탄력적 네트워크 인터페이스에만 트래픽 미러링을 활성화합니다.

VPC 엔드포인트

VPC 엔드포인트는 확장성 및 안정성뿐만 아니라 또 다른 보안 제어 계층을 제공합니다. 이를 사용하여 애플리케이션 VPC를 다른에 연결합니다 AWS 서비스. (애플리케이션 계정에서 AWS SRA는 AWS KMS AWS Systems Manager및 Amazon S3에 대해 VPC 엔드포인트를 사용합니다.) 엔드포인트는 가상 디바이스입니다. 수평으로 확장된 고가용성 중복 VPC 구성 요소입니다. 네트워크 트래픽에 가용성 위험이나 대역폭 제약을 발생시키지 않고 VPC의 인스턴스와 서비스 간에 통신할 수 있습니다. VPC 엔드포인트를 사용하여 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 연결 AWS PrivateLink 없이 에서 제공하는 지원되는 AWS 서비스 및 VPC 엔드포인트 서비스에 VPC를 비공개로 연결할 수 있습니다 AWS Direct Connect . VPC의 인스턴스는 다른 인스턴스와 통신하는 데 퍼블릭 IP 주소가 필요하지 않습니다 AWS 서비스. VPC와 다른 VPC 간의 트래픽 AWS 서비스 은 Amazon 네트워크를 벗어나지 않습니다.

VPC 엔드포인트 사용의 또 다른 이점은 엔드포인트 정책 구성을 활성화하는 것입니다. VPC 엔드포인트 정책은 엔드포인트를 만들거나 수정 시 엔드포인트에 연결하는 IAM 리소스 정책입니다. 엔드포인트를 생성할 때 IAM 정책을 연결하지 않으면는 서비스에 대한 전체 액세스를 허용하는 기본 IAM 정책을 AWS 연결합니다. 엔드포인트 정책은 IAM 사용자 정책 또는 서비스별 정책(예: S3 버킷 정책)을 무시하거나 교체하지 않습니다. 엔드포인트에서 지정된 서비스로의 액세스를 제어하기 위한 별도의 IAM 정책입니다. 이렇게 하면 보안 AWS 주체가 리소스 또는 서비스와 통신할 수 있는 또 다른 제어 계층이 추가됩니다.

Amazon EC2

애플리케이션을 구성하는 Amazon EC2 인스턴스는 인스턴스 메타데이터 서비스(IMDSv2) 버전 2를 사용합니다. IMDSv2는 IMDS에 액세스하려는 데 사용할 수 있는 네 가지 유형의 취약성, 즉 웹 사이트 애플리케이션 방화벽, 개방형 역방향 프록시, 서버 측 요청 위조(SSRF) 취약성, 개방형 계층 3 방화벽 및 NATs에 대한 보호를 추가합니다. 자세한 내용은 블로그 게시물 EC2 인스턴스 메타데이터 서비스가 향상된 개방형 방화벽, 역방향 프록시 및 SSRF 취약성에 대한 심층 방어 추가를 참조하세요.

별도의 VPCs(계정 경계의 하위 집합)를 사용하여 워크로드 세그먼트별로 인프라를 격리합니다. 서브넷을 사용하여 단일 VPC 내의 애플리케이션 티어(예: 웹, 애플리케이션 및 데이터베이스)를 격리합니다. 인터넷에서 직접 액세스하면 안 되는 경우 프라이빗 서브넷을 인스턴스에 사용합니다. 인터넷 게이트웨이를 사용하지 않고 프라이빗 서브넷에서 Amazon EC2 API를 호출하려면를 사용합니다 AWS

PrivateLink. 보안 그룹을 사용하여 인스턴스에 대한 액세스를 제한합니다. VPC 흐름 로그를 사용하여 인스턴스에 도달하는 트래픽을 모니터링합니다. 의 기능인 UseSession Manager AWS Systems Manager를 사용하여 인바운드 SSH 포트를 열고 SSH 키를 관리하는 대신 원격으로 인스턴스에 액세스합니다. 운영 체제 및 데이터에 별도의 Amazon Elastic Block Store(Amazon EBS) 볼륨을 사용합니다. 생성한 새 EBS 볼륨 및 스냅샷 복사본의 암호화를 적용하도록를 구성할 AWS 계정 수 있습니다.

> 구현 예제
>
> AWS SRA 코드 라이브러리는 Amazon EC2에서 기본 Amazon EBS 암호화의 샘플 구현을 제공합니다. 조직의 각 내에서 계정 수준 기본 Amazon EBS 암호화 AWS 계정 AWS 리전를 활성화하는 방법을 보여줍니다 AWS .

AWS Nitro Enclaves

AWS Nitro Enclaves는 EC2 인스턴스에서 격리된 실행 환경인 엔클레이브를 생성할 수 있는 Amazon EC2 기능입니다. Enclaves는 별도의 강화되고 매우 제한적인 가상 시스템입니다. 단일 상위 EC2 인스턴스의 CPU와 메모리는 격리된 엔클레이브로 분할됩니다. 각 엔클레이브는 독립 커널을 실행합니다. 엔클레이브는 상위 인스턴스와의 안전한 로컬 소켓 연결만 제공합니다. 영구 스토리지, 대화형 액세스 또는 외부 네트워킹이 없습니다. 사용자는 엔클레이브로 SSH할 수 없으며, 상위 인스턴스의 프로세스, 애플리케이션 또는 사용자(루트 또는 관리자)가 엔클레이브 내의 데이터 및 애플리케이션에 액세스할 수 없습니다. EC2 인스턴스 내에서 개인 식별 정보(PII), 의료, 금융 및 지적 재산 데이터와 같은 가장 민감한 데이터를 보호할 수 있습니다. Nitro Enclaves를 사용하면 외부 서비스와의 통합에 대해 걱정하는 대신 애플리케이션에 집중할 수 있습니다. Nitro Enclaves에는 승인된 코드만 실행되고 있는지 확인할 수 있도록 소프트웨어에 대한 암호화 증명이 포함되어 있으며, 엔클레이브만 민감한 자료에 액세스할 수 AWS KMS 있도록와 통합됩니다. 이렇게 하면 가장 민감한 데이터 처리 애플리케이션의 공격 표면적을 줄일 수 있습니다. Nitro Enclaves 사용에 따른 추가 비용은 없습니다.

암호화 증명은 엔클레이브의 자격 증명을 증명하는 데 사용되는 프로세스입니다. 증명 프로세스는 Nitro Hypervisor를 통해 수행됩니다. Nitro Hypervisor는 엔클레이브가 다른 타사 또는 서비스에 자격 증명을 증명할 수 있도록 서명된 증명 문서를 생성합니다. 증명 문서에는 엔클레이브의 퍼블릭 키, 엔클레이브 이미지 및 애플리케이션의 해시 등과 같은 엔클레이브의 주요 세부 정보가 포함되어 있습니다.

Nitro Enclaves용 AWS Certificate Manager (ACM)를 사용하면 Nitro Enclaves가 있는 EC2 인스턴스에서 실행되는 웹 애플리케이션 및 웹 서버에 퍼블릭 및 프라이빗 SSL/TLS 인증서를 사용할 수 있습니다. SSL/TLS 인증서는 네트워크 통신을 보호하고 인터넷을 통해 웹 사이트의 ID와 프라이빗 네트워크의 리소스를 설정하는 데 사용됩니다. Nitro Enclaves용 ACM은 SSL/TLS 인증서를 구매, 업로드 및

갱신하는 데 시간이 많이 걸리고 오류가 발생하기 쉬운 수동 프로세스를 제거합니다. Nitro Enclaves용 ACM은 보안 프라이빗 키를 생성하고, 인증서와 해당 프라이빗 키를 엔클레이브에 배포하고, 인증서 갱신을 관리합니다. Nitro Enclaves용 ACM을 사용하면 인증서의 프라이빗 키가 엔클레이브에서 격리된 상태로 유지되므로 인스턴스와 해당 사용자가 액세스할 수 없습니다. 자세한 내용은AWS Certificate Manager Nitro Enclaves 설명서의 Nitro Enclaves용 섹션을 참조하세요.

Application Load Balancers

Application Load Balancer는 들어오는 애플리케이션 트래픽을 여러 가용 영역의 EC2 인스턴스 등 여러 대상에 분산합니다. AWS SRA에서 로드 밸런서의 대상 그룹은 애플리케이션 EC2 인스턴스입니다. AWS SRA는 HTTPS 리스너를 사용하여 통신 채널이 암호화되도록 합니다. Application Load Balancer는 서버 인증서를 사용하여 프런트 엔드 연결을 종료한 다음 대상에 전송하기 전에 클라이언트의 요청을 복호화합니다.

AWS Certificate Manager (ACM)은 기본적으로 Application Load Balancer와 통합되며, AWS SRA는 ACM을 사용하여 필요한 X.509(TLS 서버) 퍼블릭 인증서를 생성하고 관리합니다. Application Load Balancer 보안 정책을 통해 프런트 엔드 연결에 TLS 1.2 및 강력한 암호를 적용할 수 있습니다. 자세한 내용은 Elastic Load Balancing 설명서를 참조하십시오.

설계 고려 사항

- Application Load Balancer에서 프라이빗 TLS 인증서가 필요한 엄격한 내부 애플리케이션과 같은 일반적인 시나리오의 경우이 계정 내의 ACM을 사용하여에서 프라이빗 인증서를 생성할 수 있습니다 AWS Private CA. AWS SRA에서 ACM 루트 프라이빗 CA는 보안 도구 계정에서 호스팅되며 보안 도구 계정 섹션의 앞부분에서 설명한 대로 전체 AWS 조직 또는 최종 엔터티 인증서를 발급 AWS 계정 하는 특정와 공유할 수 있습니다.
- 퍼블릭 인증서의 경우 ACM을 사용하여 해당 인증서를 생성하고 자동 교체를 포함하여 관리할 수 있습니다. 또는 SSL/TLS 도구를 사용하여 인증서 서명 요청(CSR)을 생성하고, 인증 기관(CA)이 서명한 CSR을 가져와 인증서를 생성한 다음, 인증서를 ACM으로 가져오거나 Application Load Balancer와 함께 사용할 수 있도록 인증서를 IAM에 업로드하여 자체 인증서를 생성할 수 있습니다. 인증서를 ACM으로 가져오는 경우 인증서의 만료 날짜를 모니터링하고 만료되기 전에 인증서를 갱신해야 합니다.
- 추가 방어 계층을 위해 Application Load Balancer를 보호하는 AWS WAF 정책을 배포할 수 있습니다. 엣지 정책, 애플리케이션 정책, 심지어 프라이빗 또는 내부 정책 적용 계층이 있으면 통신 요청의 가시성이 향상되고 통합 정책 적용이 제공됩니다. 자세한 내용은 블로그 게시물 용 를 사용하여 심층 방어 배포를 참조 AWS Managed Rules 하세요 AWS WAF.

AWS Private CA

AWS Private Certificate Authority (AWS Private CA)는 애플리케이션 계정에서 Application Load Balancer와 함께 사용할 프라이빗 인증서를 생성하는 데 사용됩니다. Application Load Balancer가 TLS를 통해 보안 콘텐츠를 제공하는 일반적인 시나리오입니다. 이렇게 하려면 Application Load Balancer에 TLS 인증서를 설치해야 합니다. 엄격하게 내부인 애플리케이션의 경우 프라이빗 TLS 인증서가 보안 채널을 제공할 수 있습니다.

AWS SRA에서 AWS Private CA 는 Security Tooling 계정에서 호스팅되고를 사용하여 애플리케이션 계정과 공유됩니다 AWS RAM. 이렇게 하면 애플리케이션 계정의 개발자가 공유 프라이빗 CA에서 인증서를 요청할 수 있습니다. 조직 전체 또는 전체에서 CAs 공유 AWS 계정 하면 모든에서 중복 CAs를 생성하고 관리하는 데 드는 비용과 복잡성을 줄일 수 있습니다 AWS 계정. ACM을 사용하여 공유 CA에서 프라이빗 인증서를 발급하면 인증서가 요청 계정에서 로컬로 생성되고 ACM은 전체 수명 주기 관리 및 갱신을 제공합니다.

Amazon Inspector –

AWS SRA는 Amazon Inspector를 사용하여 Amazon Elastic Container Registry(Amazon ECR)에 있는 EC2 인스턴스 및 컨테이너 이미지를 자동으로 검색하고 스캔하여 소프트웨어 취약성 및 의도하지 않은 네트워크 노출이 있는지 확인합니다.

Amazon Inspector는이 계정의 EC2 인스턴스에 취약성 관리 서비스를 제공하기 때문에 애플리케이션 계정에 배치됩니다. 또한 Amazon Inspector는 EC2 인스턴스와 주고받는 원치 않는 네트워크 경로를 보고합니다.

멤버 계정의 Amazon Inspector는 위임된 관리자 계정에서 중앙에서 관리합니다. AWS SRA에서 보안 도구 계정은 위임된 관리자 계정입니다. 위임된 관리자 계정은 조사 결과 데이터와 조직 구성원에 대한 특정 설정을 관리할 수 있습니다. 여기에는 모든 멤버 계정에 대한 집계된 조사 결과 세부 정보 보기, 멤버 계정에 대한 스캔 활성화 또는 비활성화, AWS 조직 내에서 스캔한 리소스 검토가 포함됩니다.

> 설계 고려 사항
>
> 의 기능인 Patch Manager AWS Systems Manager를 사용하여 온디맨드 패치를 트리거하여 Amazon Inspector 제로데이 또는 기타 중요한 보안 취약성을 해결할 수 있습니다. 패치 관리자는 일반적인 패치 적용 일정을 기다릴 필요 없이 이러한 취약성을 패치하는 데 도움이 됩니다. 문제 해결은 Systems Manager Automation 실행서를 사용하여 수행됩니다. 자세한 내용은 Amazon Inspector 및를 AWS 사용하여에서 취약성 관리 및 문제 해결 자동화 AWS Systems Manager라는 두 부분으로 구성된 블로그 시리즈를 참조하세요.

AWS Systems Manager

AWS Systems Manager는 여러의 운영 데이터를 보고 AWS 리소스 전반의 운영 작업을 AWS 서비스 자동화하는 데 사용할 수 있는 입니다 AWS 서비스 . 자동화된 승인 워크플로 및 실행서를 사용하면 인적 오류를 줄이고 AWS 리소스에 대한 유지 관리 및 배포 작업을 간소화할 수 있습니다.

Systems Manager는 이러한 일반 자동화 기능 외에도 다양한 예방, 탐지 및 대응 보안 기능을 지원합니다. AWS Systems Manager 에이전트(SSM 에이전트)는 EC2 인스턴스, 온프레미스 서버 또는 가상 머신(VM)에 설치 및 구성할 수 있는 Amazon 소프트웨어입니다. SSM Agent를 사용하면 Systems Manager가 이러한 리소스를 업데이트, 관리 및 구성할 수 있습니다. Systems Manager는 이러한 관리형 인스턴스를 스캔하고 패치, 구성 및 사용자 지정 정책에서 감지한 위반을 보고(또는 수정 조치 수행)하여 보안 및 규정 준수를 유지하는 데 도움이 됩니다.

AWS SRA는 Systems Manager의 기능인 Session Manager를 사용하여 대화형 브라우저 기반 셸 및 CLI 환경을 제공합니다. 이를 통해 인바운드 포트를 열거나, 접속 호스트를 유지 관리하거나, SSH 키를 관리할 필요 없이 안전하고 감사 가능한 인스턴스를 관리할 수 있습니다. AWS SRA는 Systems Manager의 기능인 Patch Manager를 사용하여 운영 체제와 애플리케이션 모두에 대한 EC2 인스턴스에 패치를 적용합니다.

또한 AWS SRA는 Systems Manager의 기능인 Automation을 사용하여 Amazon EC2 인스턴스 및 기타 AWS 리소스의 일반적인 유지 관리 및 배포 작업을 간소화합니다. 자동화를 통해 노드 한 개 이상에 대한 상태 변경(승인 자동화 사용), 일정에 따른 노드 상태 관리와 같은 일반 IT 태스크를 간소화할 수 있습니다. Systems Manager에는 태그를 사용해 대규모 인스턴스 그룹을 대상으로 설정하는 기능과 사용자가 정의한 한계에 따라 변경 사항을 롤아웃하는 작업을 지원하는 속도 제어 기능이 있습니다. Automation은 골든 Amazon Machine Image(AMIs) 생성 및 연결할 수 없는 EC2 인스턴스 복구와 같은 복잡한 작업을 간소화하기 위한 원클릭 자동화를 제공합니다. 또한 해당 역할에 직접 권한을 부여하지 않고도 IAM 역할에 특정 런북에 대한 액세스 권한을 부여하여 특정 기능을 수행할 수 있습니다. 예를 들어 패치 업데이트 후 IAM 역할에 특정 EC2 인스턴스를 다시 시작할 수 있는 권한이 있지만 해당 역할에 직접 권한을 부여하지 않으려는 경우 대신 Automation 런북을 생성하고 런북만 실행할 수 있는 권한을 역할에 부여할 수 있습니다.

설계 고려 사항

- Systems Manager는 올바르게 작동하기 위해 EC2 인스턴스 메타데이터를 사용합니다. Systems Manager는 인스턴스 메타데이터 서비스(IMDSv1 및 IMDSv2) 버전 1 또는 버전 2를 사용하여 인스턴스 메타데이터에 액세스할 수 있습니다.
- SSM 에이전트는 Amazon EC2 메시지, Systems Manager 및 Amazon S3와 같은 다양한 AWS 서비스 및 리소스와 통신해야 합니다. 이 통신이 이루어지려면 서브넷에 아웃바운드

인터넷 연결 또는 적절한 VPC 엔드포인트 프로비저닝이 필요합니다. AWS SRA는 SSM 에이전트에 VPC 엔드포인트를 사용하여 다양한에 대한 프라이빗 네트워크 경로를 설정합니다 AWS 서비스.

- Automation을 사용하여 조직의 나머지 부서와 모범 사례를 공유할 수 있습니다. 런북에서 리소스 관리를 위한 모범 사례를 생성하고 AWS 리전 및 그룹 간에 런북을 공유할 수 있습니다. 런북 파라미터에 허용되는 값을 제한할 수도 있습니다. 이러한 사용 사례의 경우 보안 도구 또는 공유 서비스와 같은 중앙 계정에서 Automation 런북을 생성하고 AWS 조직의 나머지 부분과 공유해야 할 수 있습니다. 일반적인 사용 사례에는 패치 및 보안 업데이트를 중앙에서 구현하고, VPC 구성 또는 S3 버킷 정책의 드리프트를 수정하고, EC2 인스턴스를 대규모로 관리하는 기능이 포함됩니다. 구현 세부 정보는 Systems Manager 설명서를 참조하세요.

Amazon Aurora

AWS SRA에서 Amazon Aurora와 Amazon S3는 논리적 데이터 계층을 구성합니다. Aurora는 MySQL 및 PostgreSQL과 호환되는 완전 관리형 관계형 데이터베이스 엔진입니다. EC2 인스턴스에서 실행 중인 애플리케이션은 필요에 따라 Aurora 및 Amazon S3와 통신합니다. Aurora는 DB 서브넷 그룹 내의 데이터베이스 클러스터로 구성됩니다.

설계 고려 사항

많은 데이터베이스 서비스와 마찬가지로 Aurora에 대한 보안은 세 가지 수준에서 관리됩니다. Aurora DB 클러스터 및 DB 인스턴스에서 Amazon Relational Database Service(RDS) 관리 작업을 수행할 수 있는 사용자를 제어하려면 IAM을 사용합니다. VPC에서 Aurora DB 클러스터용 DB 인스턴스의 클러스터 엔드포인트 및 포트에 대한 연결을 열 수 있는 디바이스 및 EC2 인스턴스를 제어하려면 VPC 보안 그룹을 사용합니다. Aurora DB 클러스터에 대한 로그인 및 권한을 인증하려면 MySQL 또는 PostgreSQL의 독립형 DB 인스턴스와 동일한 접근 방식을 취하거나 Aurora MySQL 호환 버전에 IAM 데이터베이스 인증을 사용할 수 있습니다. 이 후자의 접근 방식을 사용하면 IAM 역할과 인증 토큰을 사용하여 Aurora MySQL 호환 DB 클러스터에 인증합니다.

Amazon S3

Amazon S3는 업계 최고의 확장성, 데이터 가용성, 보안 및 성능을 제공하는 객체 스토리지 서비스입니다. 이는 구축된 많은 애플리케이션의 데이터 백본이며 민감한 데이터를 보호하는 데 AWS적절한 권한 및 보안 제어가 중요합니다. Amazon S3에 권장되는 보안 모범 사례는 블로그 게시물의 설명서, 온

라인 기술 강연 및 심층 분석을 참조하세요. https://aws.amazon.com/blogs/storage/protect-amazon-s3-buckets-using-access-analyzer-for-s3/ 가장 중요한 모범 사례는 S3 버킷에 대한 지나치게 허용적인 액세스(특히 퍼블릭 액세스)를 차단하는 것입니다.

AWS KMS

AWS SRA는 키 관리에 권장되는 배포 모델을 보여줍니다. 여기서는 암호화할 리소스 AWS 계정 와 동일한 내에 AWS KMS key 있습니다. 이러한 이유로 AWS KMS 는 보안 도구 계정에 포함되는 것 외에도 애플리케이션 계정에서 사용됩니다. 애플리케이션 계정에서 AWS KMS 는 애플리케이션 리소스와 관련된 키를 관리하는 데 사용됩니다. 키 정책을 사용하여 로컬 애플리케이션 역할에 키 사용 권한을 부여하고 키 관리자에 대한 관리 및 모니터링 권한을 제한하여 업무 분리를 구현할 수 있습니다.

> 설계 고려 사항
>
> 분산 모델에서 AWS KMS 주요 관리 책임은 애플리케이션 팀에 있습니다. 그러나 중앙 보안 팀은 다음과 같은 중요한 암호화 이벤트의 거버넌스 및 모니터링을 담당할 수 있습니다.
>
> - KMS 키의 가져온 키 구성 요소의 만료 날짜가 가까워졌습니다.
> - KMS 키의 키 구성 요소가 자동으로 교체되었습니다.
> - AKMS 키가 삭제되었습니다.
> - 복호화 실패율이 높습니다.

AWS CloudHSM

AWS CloudHSM는에서 관리형 하드웨어 보안 모듈(HSMs)을 제공합니다 AWS 클라우드. 이를 통해 액세스를 제어하는 FIPS 140-2 레벨 3 검증 HSMs AWS 을 사용하여에서 자체 암호화 키를 생성하고 사용할 수 있습니다. AWS CloudHSM 를 사용하여 웹 서버의 SSL/TLS 처리를 오프로드할 수 있습니다. 이렇게 하면 웹 서버의 부담이 줄어들고 웹 서버의 프라이빗 키를에 저장하여 보안을 강화할 수 있습니다 AWS CloudHSM. 마찬가지로 네트워크 계정의 인바운드 VPC에 AWS CloudHSM 에서 HSM을 배포하여 발급 인증 기관 역할을 해야 하는 경우 프라이빗 키를 저장하고 인증서 요청에 서명할 수 있습니다.

> 설계 고려 사항
>
> FIPS 140-2 레벨 3에 대한 엄격한 요구 사항이 있는 경우 기본 KMS 키 스토어를 AWS KMS 사용하는 대신 AWS CloudHSM 클러스터를 사용자 지정 키 스토어로 사용하도록를 구성할

수도 있습니다. 이렇게 AWS 서비스 하면 KMS 키를 보호하는 HSMs을 책임지는 동시에 데이터를 암호화하는 AWS KMS 와 간의 통합의 이점을 누릴 수 있습니다. 이렇게 하면 제어 중인 단일 테넌트 HSMs과 사용 및 통합의 용이성이 결합됩니다 AWS KMS. 인프라를 관리 AWS CloudHSM 하려면 퍼블릭 키 인프라(PKI)를 사용하고 HSMs.

AWS Secrets Manager

AWS Secrets Manager는 애플리케이션, 서비스 및 IT 리소스에 액세스하는 데 필요한 자격 증명(보안 암호)을 보호하는 데 도움이 됩니다. 이 서비스를 사용하면 수명 주기 동안 데이터베이스 자격 증명, API 키 및 기타 보안 암호를 효율적으로 교체, 관리 및 검색할 수 있습니다. 코드의 하드 코딩된 자격 증명을 Secrets Manager에 대한 API 호출로 대체하여 프로그래밍 방식으로 보안 암호를 검색할 수 있습니다. 이렇게 하면 보안 암호가 코드에 더 이상 존재하지 않으므로 코드를 검사하는 사람이 보안 암호를 손상시키지 않도록 할 수 있습니다. 또한 Secrets Manager를 사용하면 환경(개발, 사전 프로덕션, 프로덕션) 간에 애플리케이션을 이동할 수 있습니다. 코드를 변경하는 대신 환경에서 적절하게 이름이 지정되고 참조된 보안 암호를 사용할 수 있는지 확인할 수 있습니다. 이렇게 하면 코드를 테스트한 후 변경 사항과 인적 상호 작용을 줄이면서 다양한 환경에서 애플리케이션 코드의 일관성과 재사용 가능성을 높일 수 있습니다.

Secrets Manager를 사용하면 세분화된 IAM 정책 및 리소스 기반 정책을 사용하여 보안 암호에 대한 액세스를 관리할 수 있습니다. 를 사용하여 관리하는 암호화 키로 암호를 암호화하여 보안 암호를 보호할 수 있습니다 AWS KMS. 또한 Secrets Manager는 중앙 집중식 감사를 위해 AWS 로깅 및 모니터링 서비스와 통합됩니다.

Secrets Manager는 AWS KMS keys 및 데이터 키를 사용한 봉투 암호화를 사용하여 각 보안 암호 값을 보호합니다. 보안 암호를 생성할 때 AWS 계정 및 리전에서 대칭 고객 관리형 키를 선택하거나 Secrets Manager에 관리 AWS 형 키를 사용할 수 있습니다.

보안 암호를 모니터링하여 변경 사항을 기록하는 것이 가장 좋습니다. 이렇게 하면 예상치 못한 사용 또는 변경 사항을 조사할 수 있습니다. 원치 않는 변경 사항은 롤백할 수 있습니다. Secrets Manager는 현재 조직 및 활동을 모니터링할 수 AWS 서비스 있는 두 가지를 지원합니다 AWS CloudTrail AWS Config. CloudTrail은 Secrets Manager 콘솔의 호출 및 Secrets Manager API에 대한 코드 호출을 포함하여 Secrets Manager에 대한 모든 API 호출을 이벤트로 캡처합니다. 또한 CloudTrail은에 보안 또는 규정 준수 영향을 미치 AWS 계정 거나 운영 문제를 해결하는 데 도움이 될 수 있는 기타 관련(비 API) 이벤트를 캡처합니다. 여기에는 특정 보안 암호 교체 이벤트 및 보안 암호 버전 삭제가 포함됩니다.는 Secrets Manager에서 보안 암호에 대한 변경 사항을 추적하고 모니터링하여 탐지 제어를 제공할 AWS Config 수 있습니다. 이러한 변경 사항에는 보안 암호의 설명, 교체 구성, 태그, KMS 암호화 키 또는 보안 암호 교체에 사용되는 AWS Lambda 함수와 같은 다른 AWS 소스와의 관계가 포함됩니다. 구성 및

규정 준수 변경 알림을 수신하는 Amazon EventBridge를 구성 AWS Config하여 알림 또는 수정 작업을 위해 특정 보안 암호 이벤트를 라우팅할 수도 있습니다.

AWS SRA에서 Secrets Manager는 애플리케이션 계정에 위치하여 로컬 애플리케이션 사용 사례를 지원하고 사용에 가까운 보안 암호를 관리합니다. 여기서 인스턴스 프로파일은 애플리케이션 계정의 EC2 인스턴스에 연결됩니다. 그런 다음 인스턴스 프로파일이 보안 암호를 검색할 수 있도록 Secrets Manager에서 별도의 보안 암호를 구성할 수 있습니다. 예를 들어 적절한 Active Directory 또는 LDAP 도메인에 조인하고 Aurora 데이터베이스에 액세스할 수 있습니다. Secrets Manager는 Amazon RDS DB 인스턴스 또는 다중 AZ DB 클러스터를 생성, 수정 또는 복원할 때 사용자 자격 증명을 관리하기 위해 Amazon RDS와 통합됩니다. 이렇게 하면 키 생성 및 교체를 관리하고 코드의 하드 코딩된 자격 증명을 Secrets Manager에 대한 프로그래밍 방식 API 호출로 대체할 수 있습니다.

> 설계 고려 사항
>
> 일반적으로 보안 암호가 사용될 위치와 가장 가까운 계정에서 Secrets Manager를 구성하고 관리합니다. 이 접근 방식은 사용 사례에 대한 현지 지식을 활용하고 애플리케이션 개발 팀에 속도와 유연성을 제공합니다. 추가 제어 계층이 적절할 수 있는 엄격하게 제어되는 정보의 경우 보안 도구 계정의 Secrets Manager에서 보안 암호를 중앙에서 관리할 수 있습니다.

Amazon Cognito

Amazon Cognito를 사용하면 웹 및 모바일 앱에 사용자 가입, 로그인 및 액세스 제어를 빠르고 효율적으로 추가할 수 있습니다. Amazon Cognito는 수백만 명의 사용자로 확장되며 SAML 2.0 및 OpenID Connect를 통해 Apple, Facebook, Google 및 Amazon과 같은 소셜 자격 증명 공급자와 엔터프라이즈 자격 증명 공급자와의 로그인을 지원합니다. Amazon Cognito의 두 가지 주요 구성 요소는 사용자 풀과 자격 증명 풀입니다. 사용자 풀은 애플리케이션 사용자에게 가입 및 로그인 옵션을 제공하는 사용자 디렉터리입니다. 자격 증명 풀을 사용하면 사용자에게 다른에 대한 액세스 권한을 부여할 수 있습니다 AWS 서비스. 자격 증명 풀과 사용자 풀을 별도로 또는 함께 사용할 수 있습니다. 일반적인 사용 시나리오는 Amazon Cognito 설명서를 참조하세요.

Amazon Cognito는 사용자 가입 및 로그인을 위한 사용자 지정 가능한 기본 제공 UI를 제공합니다. Amazon Cognito용 Android, iOS 및 JavaScript SDKs 사용하여 앱에 사용자 가입 및 로그인 페이지를 추가할 수 있습니다. Amazon Cognito Sync는 애플리케이션 관련 사용자 데이터의 디바이스 간 동기화를 지원하는 AWS 서비스 및 클라이언트 라이브러리입니다.

Amazon Cognito는 저장된 데이터와 전송 중인 데이터의 다중 인증 및 암호화를 지원합니다. Amazon Cognito 사용자 풀은 애플리케이션의 사용자 계정에 대한 액세스를 보호하는 데 도움이 되는 고급 보

안 기능을 제공합니다. 이러한 고급 보안 기능은 위험 기반 적응형 인증 및 손상된 자격 증명의 사용으로부터 보호합니다.

설계 고려 사항

- AWS Lambda 함수를 생성한 다음 Lambda 트리거를 사용하여 사용자 가입, 확인 및 로그인(인증)과 같은 사용자 풀 작업 중에 해당 함수를 트리거할 수 있습니다. 인증 문제 추가, 사용자 마이그레이션 및 확인 메시지 사용자 지정을 수행할 수 있습니다. 일반적인 작업 및 사용자 흐름은 Amazon Cognito 설명서를 참조하세요. Amazon Cognito는 Lambda 함수를 동기식으로 호출합니다.
- Amazon Cognito 사용자 풀을 사용하여 작은 멀티 테넌트 애플리케이션을 보호할 수 있습니다. 멀티 테넌트 설계의 일반적인 사용 사례는 워크로드를 실행하여 애플리케이션의 여러 버전 테스트를 지원하는 것입니다. 멀티 테넌트 설계는 여러 데이터 집합으로 단일 애플리케이션을 테스트하는 데에도 클러스터 리소스를 완전하게 사용할 수 있도록 해준다는 점에서 유용합니다. 그러나 테넌트 수와 예상 볼륨이 관련 Amazon Cognito 서비스 할당량과 일치하는지 확인합니다. 이러한 할당량은 애플리케이션의 모든 테넌트 간에 공유됩니다.

Amazon Verified Permissions

Amazon Verified Permissions는 빌드하는 애플리케이션에 대한 확장 가능한 권한 관리 및 세분화된 권한 부여 서비스입니다. 개발자와 관리자는 역할 및 속성과 함께 특별히 구축된 보안 우선 오픈 소스 정책 언어인 Cedar를 사용하여 보다 세분화된 컨텍스트 인식 정책 기반 액세스 제어를 정의할 수 있습니다. 개발자는 권한 부여를 외부화하고 정책 관리 및 관리를 중앙 집중화하여 더 안전한 애플리케이션을 더 빠르게 구축할 수 있습니다. Verified Permissions에는 수백만 개의 권한으로 확장되는 스키마 정의, 정책 설명 문법 및 자동화된 추론이 포함되어 있으므로 기본 거부 및 최소 권한의 원칙을 적용할 수 있습니다. 이 서비스에는 권한 부여 결정 및 작성자 정책을 테스트하는 데 도움이 되는 평가 시뮬레이터 도구도 포함되어 있습니다. 이러한 기능을 사용하면 제로 트러스트 객체를 지원하는 심층적이고 세분화된 권한 부여 모델을 쉽게 배포할 수 있습니다. Verified Permissions는 정책 스토어의 권한을 중앙 집중화하고 개발자가 이러한 권한을 사용하여 애플리케이션 내의 사용자 작업을 승인하는 데 도움이 됩니다.

API를 통해 애플리케이션을 서비스에 연결하여 사용자 액세스 요청을 승인할 수 있습니다. 각 권한 부여 요청에 대해 서비스는 관련 정책을 검색하고 해당 정책을 평가하여 사용자, 역할, 그룹 멤버십 및 속성과 같은 컨텍스트 입력을 기반으로 사용자가 리소스에 대한 작업을 수행할 수 있는지 여부를 결정합니다. 정책 관리 및 권한 부여 로그를 전송하도록 Verified Permissions를 구성하고 연결할 수 있습니다 AWS CloudTrail. Amazon Cognito를 자격 증명 스토어로 사용하는 경우 Verified Permissions와 통합

하고 Amazon Cognito가 애플리케이션의 권한 부여 결정에 반환하는 ID 및 액세스 토큰을 사용할 수 있습니다. Amazon Cognito 토큰을 Verified Permissions에 제공합니다.이 권한은 토큰에 포함된 속성을 사용하여 보안 주체를 나타내고 보안 주체의 권한을 식별합니다. 이 통합에 AWS 대한 자세한 내용은 블로그 게시물Simplifying fine-grained authorization with Amazon Verified Permissions and Amazon Cognito를 참조하세요.

Verified Permissions는 정책 기반 액세스 제어(PBAC)를 정의하는 데 도움이 됩니다. PBAC는 정책으로 표현되는 권한을 사용하여 애플리케이션의 리소스에 액세스할 수 있는 사용자를 결정하는 액세스 제어 모델입니다. PBAC는 역할 기반 액세스 제어(RBAC)와 속성 기반 액세스 제어(ABAC)를 결합하여 보다 강력하고 유연한 액세스 제어 모델을 제공합니다. PBAC와 Verified Permissions를 사용하여 권한 부여 모델을 설계하는 방법에 대해 자세히 알아보려면 AWS 블로그 게시물 Amazon Verified Permissions를 사용한 애플리케이션 개발 시 정책 기반 액세스 제어를 참조하세요.

AWS SRA에서 Verified Permissions는 Amazon Cognito와의 통합을 통해 애플리케이션에 대한 권한 관리를 지원하기 위해 애플리케이션 계정에 있습니다.

계층형 방어

애플리케이션 계정은가 AWS 활성화하는 계층화된 방어 보안 주체를 설명할 수 있는 기회를 제공합니다. AWS SRA에 표시된 간단한 예제 애플리케이션의 코어를 구성하는 EC2 인스턴스의 보안을 고려하면 계층형 방어에서 함께 AWS 서비스 작동하는 방식을 확인할 수 있습니다. 이 접근 방식은이 가이드 앞부분의 조직 전체에 AWS 보안 서비스 적용 섹션에 설명된 대로 보안 서비스의 구조적 관점에 부합합니다. AWS

- 가장 안쪽 계층은 EC2 인스턴스입니다. 앞서 언급했듯이 EC2 인스턴스에는 기본적으로 또는 옵션으로 많은 기본 보안 기능이 포함되어 있습니다. 예를 들어 IMDSv2, Nitro 시스템 및 Amazon EBS 스토리지 암호화가 있습니다.
- 두 번째 보호 계층은 EC2 인스턴스에서 실행되는 운영 체제 및 소프트웨어에 중점을 둡니다. Amazon Inspector 및와 같은 서비스를 AWS Systems Manager 사용하면 이러한 구성을 모니터링, 보고 및 수정 조치를 취할 수 있습니다. Amazon Inspector는 소프트웨어에 취약성이 있는지 모니터링하고 Systems Manager는 관리형 인스턴스의 패치 및 구성 상태를 스캔한 다음 지정한 수정 조치를 보고하고 수행하여 보안 및 규정 준수를 유지하는 데 도움이 됩니다.
- 인스턴스와 이러한 인스턴스에서 실행되는 소프트웨어는 AWS 네트워킹 인프라에 있습니다. Amazon VPC의 보안 기능을 사용하는 것 외에도 AWS SRA는 VPC 엔드포인트를 사용하여 VPC AWS 서비스와 지원되는 간에 프라이빗 연결을 제공하고 네트워크 경계에 액세스 정책을 배치하는 메커니즘을 제공합니다.

- EC2 인스턴스, 소프트웨어, 네트워크, IAM 역할 및 리소스의 활동 및 구성은 Amazon GuardDuty AWS Security Hub CSPM, AWS Security Hub, AWS CloudTrail AWS Config, IAM Access Analyzer, Amazon Macie와 같은 AWS 계정중점 서비스별로 추가로 모니터링됩니다.
- 마지막으로 애플리케이션 계정 외에도는 다른 계정과 공유되는 리소스를 제어하는 AWS RAM 데 도움이 되며, IAM 서비스 제어 정책은 AWS 조직 전체에 일관된 권한을 적용하는 데 도움이 됩니다.

보안을 위한 AI/ML

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

인공 지능 및 기계 학습(AI/ML)은 비즈니스를 혁신하고 있습니다. AI/ML은 20년 이상 Amazon에 중점을 두어 왔으며, 보안 서비스를 AWS포함하여 고객이와 함께 사용하는 많은 기능은 AI/ML에 의해 구동됩니다. 이렇게 하면 보안 또는 애플리케이션 개발 팀이 AI/ML에 대한 전문 지식을 갖추지 AWS 않고도를 안전하게 구축할 수 있으므로 차별화된 가치가 기본적으로 생성됩니다.

AI는 기계와 시스템이 인텔리전스와 예측 기능을 얻을 수 있는 고급 기술입니다. AI 시스템은 소비하거나 훈련된 데이터를 통해 과거 경험을 통해 학습합니다. ML은 AI의 가장 중요한 측면 중 하나입니다. ML은 컴퓨터가 명시적으로 프로그래밍되지 않고 데이터에서 학습할 수 있는 기능입니다. 기존 프로그래밍에서 프로그래머는 프로그램이 컴퓨터 또는 머신에서 작동하는 방식을 정의하는 규칙을 작성합니다. ML에서 모델은 데이터에서 규칙을 학습합니다. ML 모델은 데이터에서 숨겨진 패턴을 검색하거나 훈련 중에 사용되지 않은 새 데이터를 정확하게 예측할 수 있습니다. AI/ML을 여러 번 AWS 서비스 사용하여 방대한 데이터 세트에서 학습하고 보안 추론을 수행합니다.

- Amazon Macie는 ML 및 패턴 일치를 사용하여 민감한 데이터를 검색하고 보호하는 데 도움이 되는 데이터 보안 서비스입니다. Macie는 이름, 주소, 신용 카드 번호와 같은 금융 정보와 같은 개인 식별 정보(PII)를 포함하여 점점 증가하는 대규모 민감한 데이터 유형 목록을 자동으로 감지합니다. 또한 Amazon Simple Storage Service(Amazon S3)에 저장된 데이터에 대한 지속적인 가시성을 제공합니다. Macie는 다양한 유형의 데이터 세트에 대해 훈련된 자연어 처리(NLP) 및 ML 모델을 사용하여 기존 데이터를 이해하고 비즈니스 크리티컬 데이터의 우선 순위를 지정하기 위해 비즈니스 가치를 할당합니다. 그런 다음 Macie는 민감한 데이터 조사 결과를 생성합니다.
- Amazon GuardDuty는 ML, 이상 탐지 및 통합 위협 인텔리전스를 사용하여 악의적인 활동 및 무단 동작을 지속적으로 모니터링하여 AWS 계정사용자, 인스턴스, 서버리스 및 컨테이너 워크로드, 사용자, 데이터베이스 및 스토리지를 보호하는 위협 탐지 서비스입니다. GuardDuty는 잠재적으로 악의적인 사용자 활동을 변칙적이지만 정상적인 운영 동작과 구분하는 데 매우 효과적인 ML 기술을 통합합니다 AWS 계정. 이 기능은 계정 내에서 API 호출을 지속적으로 모델링하고 확률적 예측을 통합하여 매우 의심스러운 사용자 동작을 보다 정확하게 격리하고 경고합니다. 이 접근 방식은 검색, 초기 액세스, 지속성, 권한 에스컬레이션, 방어 회피, 자격 증명 액세스, 영향 및 데이터 유출을 포함하여 알려진 위협 전술과 관련된 악의적인 활동을 식별하는 데 도움이 됩니다. GuardDuty가 기계 학습을 사용하는 방법에 대해 자세히 알아보려면 AWS re:Inforce 2023 breakout sessionDeveloping new findings using machine learning in Amazon GuardDuty(TDR310)를 참조하세요.

입증 가능한 보안

AWS 는 수학 로직을 사용하여 인프라에 대한 중요한 질문에 답하고 잠재적으로 데이터를 노출할 수 있는 잘못된 구성을 감지하는 자동화된 추론 도구를 개발합니다. 이 기능을 입증 가능한 보안이라고 합니다. 클라우드와 클라우드의 보안에 대한 더 높은 보장을 제공하기 때문입니다. 입증 가능한 보안은 컴퓨터 시스템에 논리적 공제를 적용하는 AI의 특정 분야인 자동 추론을 사용합니다. 예를 들어 자동화된 추론 도구는 정책 및 네트워크 아키텍처 구성을 분석하고 취약한 데이터를 노출할 가능성이 있는 의도하지 않은 구성이 없음을 입증할 수 있습니다. 이 접근 방식은 클라우드의 중요한 보안 특성에 대해 가능한 최고 수준의 보장을 제공합니다. 자세한 내용은 AWS 웹 사이트의 보호 가능한 보안 리소스를 참조하세요. 다음 AWS 서비스 및 기능은 현재 자동화된 추론을 사용하여 애플리케이션에 대해 증명할 수 있는 보안을 달성하는 데 도움이 됩니다.

- Amazon Verified Permissions는 사용자가 빌드하는 애플리케이션을 위한 확장 가능한 권한 관리 및 세분화된 권한 부여 서비스입니다. Verified Permissions는 자동화된 추론 및 차등 테스트를 사용하여 구축된 액세스 제어를 위한 오픈 소스 언어인 Cedar를 사용합니다. Cedar는 권한을 어떤 리소스에 액세스해야 하는지 설명하는 정책으로 정의하는 언어입니다. 또한 이러한 정책을 평가하기 위한 사양이기도 합니다. Cedar 정책을 사용하여 애플리케이션의 각 사용자가 수행할 수 있는 작업과 액세스할 수 있는 리소스를 제어합니다. Cedar 정책은 사용자가 리소스에 대해 작업할 수 있는지 여부를 결정하는permitorforbid 문입니다. 정책은 리소스와 연결되며 여러 정책을 리소스에 연결할 수 있습니다. 금지 정책은 권한 정책을 재정의합니다. 애플리케이션 사용자가 리소스에 대한 작업을 수행하려고 하면 애플리케이션은 Cedar 정책 엔진에 권한 부여를 요청합니다. Cedar는 해당 정책을 평가하고 `ALLOW` 또는 `DENY` 결정을 반환합니다. Cedar는 모든 유형의 보안 주체 및 리소스에 대한 권한 부여 규칙을 지원하고, 역할 기반 및 속성 기반 액세스 제어를 허용하며, 정책을 최적화하고 보안 모델을 검증하는 데 도움이 되는 자동화된 추론 도구를 통한 분석을 지원합니다.
- AWS Identity and Access Management Access Analyzer는 권한 관리를 간소화하는 데 도움이 됩니다. 이 기능을 사용하여 세분화된 권한을 설정하고, 의도한 권한을 확인하고, 미사용 액세스를 제거하여 권한을 세분화할 수 있습니다. IAM Access Analyzer는 로그에 캡처된 액세스 활동을 기반으로 세분화된 정책을 생성합니다. 또한 정책을 작성하고 검증하는 데 도움이 되는 100개 이상의 정책 검사를 제공합니다. IAM Access Analyzer는 증명 가능한 보안을 사용하여 액세스 경로를 분석하고 리소스에 대한 퍼블릭 및 크로스 계정 액세스에 대한 포괄적인 조사 결과를 제공합니다. 이 도구는 IAM 정책을 동등한 논리적 문으로 변환하고 문제에 대해 범용 및 특수 논리적 솔버(만족성 모듈로 이론) 제품군을 실행하는 Zelkova를 기반으로 구축되었습니다. IAM Access Analyzer는 정책의 내용에 따라 정책이 허용하는 행동 클래스를 특성화하기 위해 점점 더 구체적인 쿼리가 있는 Zelkova를 정책에 반복적으로 적용합니다. 분석기는 액세스 로그를 검사하여 외부 엔터티가 신뢰 영역 내의 리소스에 액세스했는지 여부를 확인하지 않습니다. 리소스 기반 정책이 리소스에 대한 액세스를 허용할 때 외부 엔터티에서 리소스에 액세스하지 않았더라도 결과를 생성합니다. 만족도 모듈로 이론에 대한 자세한 내용은 만족도 핸드북의 만족도 모듈로 이론을 참조하세요.*

- Amazon S3 퍼블릭 액세스 차단은 버킷 및 객체의 퍼블릭 액세스로 이어질 수 있는 구성 오류를 차단할 수 있는 Amazon S3의 기능입니다. 액세스 포인트, 버킷, 계정 및 AWS 조직(계정의 기존 버킷과 새 버킷 모두에 영향을 미침)에 대해 Amazon S3 퍼블릭 액세스 차단을 활성화할 수 있습니다. 액세스 제어 목록(ACL), 버킷 정책 또는 둘 다를 통해 버킷 및 객체에 퍼블릭 액세스 권한이 부여됩니다. 지정된 정책 또는 ACL이 퍼블릭으로 간주되는지 여부는 Zelkova 자동 추론 시스템을 사용하여 결정합니다. Amazon S3는 Zelkova를 사용하여 각 버킷 정책을 확인하고 권한이 없는 사용자가 버킷을 읽거나 쓸 수 있는지 경고합니다. 버킷에 퍼블릭으로 플래그가 지정된 경우 일부 퍼블릭 요청은 버킷에 액세스할 수 있습니다. 버킷에 퍼블릭이 아닌 것으로 플래그가 지정된 경우 모든 퍼블릭 요청이 거부됩니다. Zelkova는 IAM 정책을 정확하게 수학적으로 표현하므로 이러한 결정을 내릴 수 있습니다. 각 정책에 대한 공식을 생성하고 해당 공식에 대한 이론을 증명합니다.
- Amazon VPC Network Access Analyzer는 리소스에 대한 잠재적 네트워크 경로를 이해하고 의도하지 않은 잠재적 네트워크 액세스를 식별하는 데 도움이 되는 Amazon VPC의 기능입니다. Network Access Analyzer를 사용하면 네트워크 세분화를 확인하고, 인터넷 접근성을 식별하고, 신뢰할 수 있는 네트워크 경로 및 네트워크 액세스를 확인할 수 있습니다. 이 기능은 자동 추론 알고리즘을 사용하여 패킷이 네트워크의 리소스 간에 취할 수 있는 AWS 네트워크 경로를 분석합니다. 그런 다음 아웃바운드 및 인바운드 트래픽 패턴을 정의하는 네트워크 액세스 범위와 일치하는 경로에 대한 조사 결과를 생성합니다. Network Access Analyzer는 네트워크 구성의 정적 분석을 수행합니다. 따라서 이 분석의 일환으로 네트워크에서 패킷이 전송되지 않습니다.
- Amazon VPC Reachability Analyzer는 AWS 네트워크에서 연결을 디버깅, 이해 및 시각화할 수 있는 Amazon VPC의 기능입니다. Reachability Analyzer는 Virtual Private Cloud(VPC)에서 소스 리소스와 대상 리소스 간의 연결을 테스트할 수 있는 구성 분석 도구입니다. 대상에 도달할 수 있는 경우 Reachability Analyzer는 소스와 대상 간의 가상 네트워크 경로에 대한 hop-by-hop 세부 정보를 생성합니다. 대상에 연결할 수 없는 경우 Reachability Analyzer는 차단 구성 요소를 식별합니다. Reachability Analyzer는 소스와 대상 간에 네트워크 구성 모델을 구축하여 자동화된 추론을 사용하여 실행 가능한 경로를 식별합니다. 그런 다음 구성을 기반으로 연결 가능성을 확인합니다. 패킷을 보내거나 데이터 영역을 분석하지 않습니다.

* Biere, A. M. Heule, H. van Maaren 및 T. Walsh. 2009. 만족도 핸드북. IOS Press, NLD.

보안 아키텍처 구축 - 단계별 접근 방식

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

AWS SRA에서 권장하는 다중 계정 보안 아키텍처는 설계 프로세스 초기에 보안을 주입하는 데 도움이 되는 기본 아키텍처입니다. 각 조직의 클라우드 여정은 고유합니다. 클라우드 보안 아키텍처를 성공적으로 발전시키려면 원하는 대상 상태를 구상하고, 현재 클라우드 준비 상태를 이해하고, 격차를 줄이기 위해 애자일 접근 방식을 채택해야 합니다. AWS SRA는 보안 아키텍처에 대한 참조 대상 상태를 제공합니다. 점진적으로 변환하면 원거리 예측의 필요성을 최소화하면서 가치를 빠르게 입증할 수 있습니다.

AWS Cloud Adoption Framework (AWS CAF)는 구상, 정렬, 시작 및 확장이라는 네 가지 반복 및 증분 클라우드 변환 단계를 권장합니다. 시작 단계에 진입하고 프로덕션 환경에서 파일럿 이니셔티브를 제공하는 데 집중할 때는 강력한 보안 아키텍처를 확장 단계의 기반으로 구축하는 데 집중해야 합니다. 그래야만 비즈니스 크리티컬 워크로드를 자신 있게 마이그레이션하고 운영할 수 있는 기술적 역량을 갖추게 됩니다. 이 단계별 접근 방식은 스타트업, 비즈니스를 확장하려는 중소기업 또는 새 사업부를 인수하거나 인수 합병을 진행 중인 기업에 적용됩니다. AWS SRA를 사용하면 보안 기준 아키텍처를 달성할 수 있으므로에서 확장하는 조직 전체에 보안 제어를 균일하게 적용할 수 있습니다 AWS Organizations. 기준 아키텍처는 여러 AWS 계정 및 서비스로 구성됩니다. 계획 및 구현은 기준 보안 아키텍처를 설정하는 더 큰 목표에 도달하기 위해 더 작은 마일스톤을 반복할 수 있도록 다단계 프로세스여야 합니다. 이 섹션에서는 구조화된 접근 방식을 기반으로 클라우드 여정의 일반적인 단계를 설명합니다. 이러한 단계는 AWS Well-Architected Framework 보안 설계 원칙에 부합합니다.

1단계: OU 및 계정 구조 구축

강력한 보안 기반을 구축하기 위한 사전 조건은 잘 설계된 AWS 조직 및 계정 구조입니다. 이 가이드의 SRA 구성 요소 섹션에서 설명한 대로 여러를 사용하면 다양한 비즈니스 및 보안 기능을 설계별로 분리하는 AWS 계정 데 도움이 됩니다. 처음에는 불필요한 작업처럼 보일 수 있지만 빠르고 안전하게 확장하는 데 도움이 되는 투자입니다. 또한이 섹션에서는 AWS Organizations 를 사용하여 여러를 관리하는 방법과 신뢰할 수 있는 액세스 및 위임된 관리자 기능을 사용하여 이러한 여러 계정 AWS 서비스 에서를 중앙에서 관리하는 AWS 계정방법을 설명합니다.

이 가이드의 앞부분에 설명된 AWS Control Tower 대로를 사용하여 랜딩 존을 오케스트레이션할 수 있습니다. 현재 단일를 사용하는 경우 가능한 한 빨리 여러 계정으로 마이그레이션하기 위해 여러 로 전환 AWS 계정 가이드를 AWS 계정참조하세요. 예를 들어, 스타트업 회사가 현재 단일에서 제품을 구상

하고 프로토타이핑하는 경우 시장에서 제품을 출시하기 전에 다중 계정 전략을 채택하는 것을 고려해야 AWS 계정합니다. 마찬가지로 소규모, 중형 및 엔터프라이즈 조직은 초기 프로덕션 워크로드를 계획하는 즉시 다중 계정 전략을 구축하기 시작해야 합니다. 파운데이션 OUs 및 로 시작한 AWS 계정다음 워크로드 관련 OUs 및 계정을 추가합니다.

SRA에 제공된 것 이상의 AWS 계정 및 OU 구조 권장 사항은 중소기업을 위한 다중 계정 전략 블로그 게시물을 참조하세요 AWS . OU 및 계정 구조를 마무리할 때 서비스 제어 정책(SCPs), 리소스 제어 정책(RCPs) 및 선언적 정책을 사용하여 적용하려는 조직 전체의 상위 수준 보안 제어를 고려하세요.

> 설계 고려 사항
>
> OU 및 계정 구조를 설계할 때 회사의 보고 구조를 복제하지 마십시오. OUs는 워크로드 함수와 워크로드에 적용되는 공통 보안 제어 세트를 기반으로 해야 합니다. 처음부터 전체 계정 구조를 설계하려고 하지 마세요. 기본 OUs에 집중한 다음 필요에 따라 워크로드 OUs 추가합니다. OUs 간에 계정을 이동하여 설계 초기 단계에서 대체 접근 방식을 실험할 수 있습니다. 그러나 이로 인해 OU 및 계정 경로를 기반으로 하는 SCPs, RCPs, 선언적 정책 및 IAM 조건에 따라 논리적 권한 관리에 약간의 오버헤드가 발생할 수 있습니다.

> 구현 예제
>
> AWS SRA 코드 라이브러리는 계정 대체 연락처의 샘플 구현을 제공합니다. 이 솔루션은 조직 내 모든 계정에 대한 결제, 작업 및 보안 대체 연락처를 설정합니다.

2단계: 강력한 자격 증명 기반 구현

여러을 생성하는 즉시 팀에 해당 계정 내의 AWS 리소스에 대한 액세스 권한을 부여 AWS 계정해야 합니다. 자격 증명 관리에는 직원 자격 증명과 액세스 관리, 고객 자격 증명https://aws.amazon.com/identity/customer-identities/과 액세스 관리(CIAM)라는 두 가지 일반적인 범주가 있습니다. 인력 IAM은 직원 및 자동화된 워크로드가 작업을 수행하기 AWS 위해에 로그인해야 하는 조직을 위한 것입니다. CIAM은 조직의 애플리케이션에 대한 액세스를 제공하기 위해 사용자를 인증하는 방법이 조직에 필요한 경우에 사용됩니다. 팀이 애플리케이션을 구축하고 마이그레이션할 수 있도록 먼저 인력 IAM 전략이 필요합니다. 인간 또는 기계 사용자에게 액세스 권한을 제공하려면 항상 IAM 사용자 대신 IAM 역할을 사용해야 합니다. 조직 관리 및 공유 서비스 계정 AWS IAM Identity Center 내에서를 사용하여에 대한 Single Sign-On(SSO) 액세스를 중앙에서 관리하는 방법에 대한 AWS SRA 지침을 따릅니다 AWS 계정. 또한이 지침은 IAM Identity Center를 사용할 수 없는 경우 IAM 페더레이션을 사용하기 위한 설계 고려 사항을 제공합니다.

IAM 역할을 사용하여 AWS 리소스에 대한 사용자 액세스를 제공하는 경우이 가이드의 보안 도구 및 조직 관리 섹션에 설명된 대로 IAM Access Analyzer 및 IAM 액세스 어드바이저를 사용해야 합니다. ??? 이러한 서비스는 최소 권한을 달성하는 데 도움이 되며, 이는 올바른 보안 태세를 구축하는 데 도움이 되는 중요한 예방 제어입니다.

> 설계 고려 사항
>
> 최소 권한을 달성하기 위해 자격 증명과 자격 증명이 제대로 작동하는 데 필요한 권한 간의 관계를 정기적으로 검토하고 이해하는 프로세스를 설계합니다. 학습하면서 이러한 권한을 미세 조정하고 가능한 최소 권한으로 점진적으로 줄입니다. 확장성을 위해 이는 중앙 보안 팀과 애플리케이션 팀 간의 공동 책임입니다. 리소스 기반 정책, 권한 경계, 속성 기반 액세스 제어 및 세션 정책과 같은 기능을 사용하면 애플리케이션 소유자가 세분화된 액세스 제어를 정의할 수 있습니다.

> 구현 예제
>
> AWS SRA 코드 라이브러리는이 단계에 적용되는 두 가지 샘플 구현을 제공합니다.
>
> - IAM 암호 정책은 사용자가 공통 규정 준수 표준에 맞게 계정 암호 정책을 설정합니다.
> - Access Analyzer는 위임된 관리자 계정 내에서 조직 수준 분석기를 구성하고 각 계정 내에서 계정 수준 분석기를 구성합니다.

3단계: 추적성 유지

사용자가에 액세스 AWS 하고 구축을 시작하면 누가 무엇을 언제 어디서 하고 있는지 알고 싶을 것입니다. 또한 잠재적인 보안 구성 오류, 위협 또는 예상치 못한 동작에 대한 가시성이 필요합니다. 보안 위협을 더 잘 이해하면 적절한 보안 제어의 우선 순위를 지정할 수 있습니다. 활동을 모니터링 AWS 하려면 Log Archive 계정 내에서 로그를 AWS CloudTrail 사용하고 중앙 집중화하여 조직 추적을 설정하기 위한 AWS SRA 권장 사항을 따르세요. 보안 이벤트 모니터링의 경우 AWS Security Hub CSPM보안 도구 계정 섹션에 설명된 대로 AWS Config, Amazon GuardDuty 및 Amazon Security Lake를 사용합니다.

설계 고려 사항

새 로그 사용을 시작할 때 서비스에 대한 서비스별 로그를 AWS 서비스활성화하고 중앙 로그 리포지토리의 일부로 저장해야 합니다.

구현 예제

AWS SRA 코드 라이브러리는이 단계에 적용되는 다음과 같은 샘플 구현을 제공합니다.

- Organization CloudTrail은 조직 추적을 생성하고에서 구성한 CloudTrail의 중복을 줄이기 위해 데이터 이벤트(예: Amazon S3 및 AWS Lambda)를 구성하도록 기본값을 설정합니다 AWS Control Tower. 이 솔루션은 관리 이벤트를 구성하는 옵션을 제공합니다.
- AWS Config Control Tower 관리 계정을 사용하면 관리 계정 AWS Config 에서 리소스 규정 준수를 모니터링할 수 있습니다.
- 적합성 팩 조직 규칙은 조직 내 계정 및 지정된 리전에 적합성 팩을 배포합니다.
- AWS Config 애그리게이터는 Audit 계정 이외의 멤버 계정에 관리를 위임하여 애그리게이터를 배포합니다.
- Security Hub CSPM Organization은 조직 내 계정 및 관리 리전의 위임된 관리자 계정 내에서 Security Hub CSPM을 구성합니다.
- GuardDuty Organization은 조직 내 계정의 위임된 관리자 계정 내에서 GuardDuty를 구성합니다.

4단계: 모든 계층에 보안 적용

이때 다음을 수행해야 합니다.

- 에 대한 적절한 보안 제어입니다 AWS 계정.
- SCPs, RCPs, 선언적 정책 및 최소 권한 IAM 역할 및 정책을 통해 정의된 예방 제어를 포함하는 잘 정의된 계정 및 OU 구조입니다.
- 를 사용하여 AWS 활동을 로깅하고 AWS CloudTrail, , AWS Security Hub CSPM Amazon GuardDuty를 사용하여 보안 이벤트를 감지하고, Amazon Security Lake AWS Config를 사용하여 보안을 위해 특별히 구축된 데이터 레이크에서 고급 분석을 수행하는 기능입니다.

이 단계에서는 AWS 조직 전체에 보안 서비스 적용 섹션에 설명된 대로 AWS 조직의 다른 계층에 보안을 적용하도록 계획합니다. 네트워크 계정 섹션에 설명된 대로 (AWS Shield AWS Firewall Manager AWS Network Firewall AWS Certificate Manager ACM), Amazon CloudFront AWS WAF, Amazon Route 53 및 Amazon VPC와 같은 서비스를 사용하여 네트워킹 계층에 대한 보안 제어를 구축할 수 있습니다. 기술 스택을 아래로 이동할 때 워크로드 또는 애플리케이션 스택과 관련된 보안 제어를 적용합니다. 애플리케이션 계정 섹션에 설명된 대로 VPC 엔드포인트, Amazon Inspector AWS Systems Manager AWS Secrets Manager, 및 Amazon Cognito를 사용합니다.

설계 고려 사항

심층 방어(DiD) 보안 제어를 설계할 때 조정 요소를 고려하세요. 중앙 보안 팀은 대역폭을 확보하거나 모든 애플리케이션이 환경에서 작동하는 방식을 완전히 이해하지 못합니다. 애플리케이션 팀이 애플리케이션에 적합한 보안 제어를 식별하고 설계할 수 있도록 지원합니다. 중앙 보안 팀은 애플리케이션 팀을 지원하는 데 적합한 도구와 상담을 제공하는 데 집중해야 합니다. 가 보안에 대한 보다 왼쪽 이동 접근 방식을 채택하는 AWS 데 사용하는 조정 메커니즘을 이해하려면 블로그 게시물 How AWS built the Security Guardians program, a mechanism to distribution security ownership을 참조하세요.

구현 예제

AWS SRA 코드 라이브러리는이 단계에 적용되는 다음과 같은 샘플 구현을 제공합니다.

- EC2 기본 EBS 암호화는 제공된 AWS KMS key 내에서 기본값을 사용하도록 Amazon EC2의 기본 Amazon EBS 암호화를 구성합니다 AWS 리전.
- S3 Block Account Public Access는 조직 내 계정에 대해 Amazon S3의 계정 수준 퍼블릭 액세스 차단(BPA) 설정을 구성합니다.
- Firewall Manager는 조직 내 계정에 대한 보안 그룹 정책 및 AWS WAF 정책을 구성하는 방법을 보여줍니다.
- Inspector Organization은 조직 내 계정 및 관리 리전에 대해 위임된 관리자 계정 내에서 Amazon Inspector를 구성합니다.

5단계: 전송 중 및 저장 데이터 보호

비즈니스 및 고객 데이터는 보호해야 하는 중요한 자산입니다. AWS 는 이동 및 저장 데이터를 보호하기 위한 다양한 보안 서비스와 기능을 제공합니다. 네트워크 계정 섹션에 설명된 AWS Certificate

Manager대로 Amazon CloudFront를와 함께 사용하여 인터넷을 통해 수집된 이동 중인 데이터를 보호합니다. 내부 네트워크 내에서 이동 중인 데이터의 경우 애플리케이션 계정 섹션에 설명된 대로 Application Load Balancer를와 함께 사용합니다. AWS KMS 및는 저장 데이터를 보호하기 위한 암호화 키 관리를 제공하는 데 AWS CloudHSM 도움이 됩니다. AWS Private Certificate Authority ???

6단계: 보안 이벤트 준비

IT 환경을 운영할 때 보안 정책 위반 또는 보안 제어 실패를 나타내는 IT 환경의 일상적인 운영 변경 사항인 보안 이벤트가 발생합니다. 보안 이벤트를 최대한 빨리 인식하려면 적절한 추적성이 중요합니다. 보안 이벤트가 에스컬레이션되기 전에 적절한 조치를 취할 수 있도록 이러한 보안 이벤트를 분류하고 대응할 준비를 하는 것도 마찬가지로 중요합니다. 준비는 보안 이벤트를 빠르게 분류하여 잠재적 영향을 이해하는 데 도움이 됩니다.

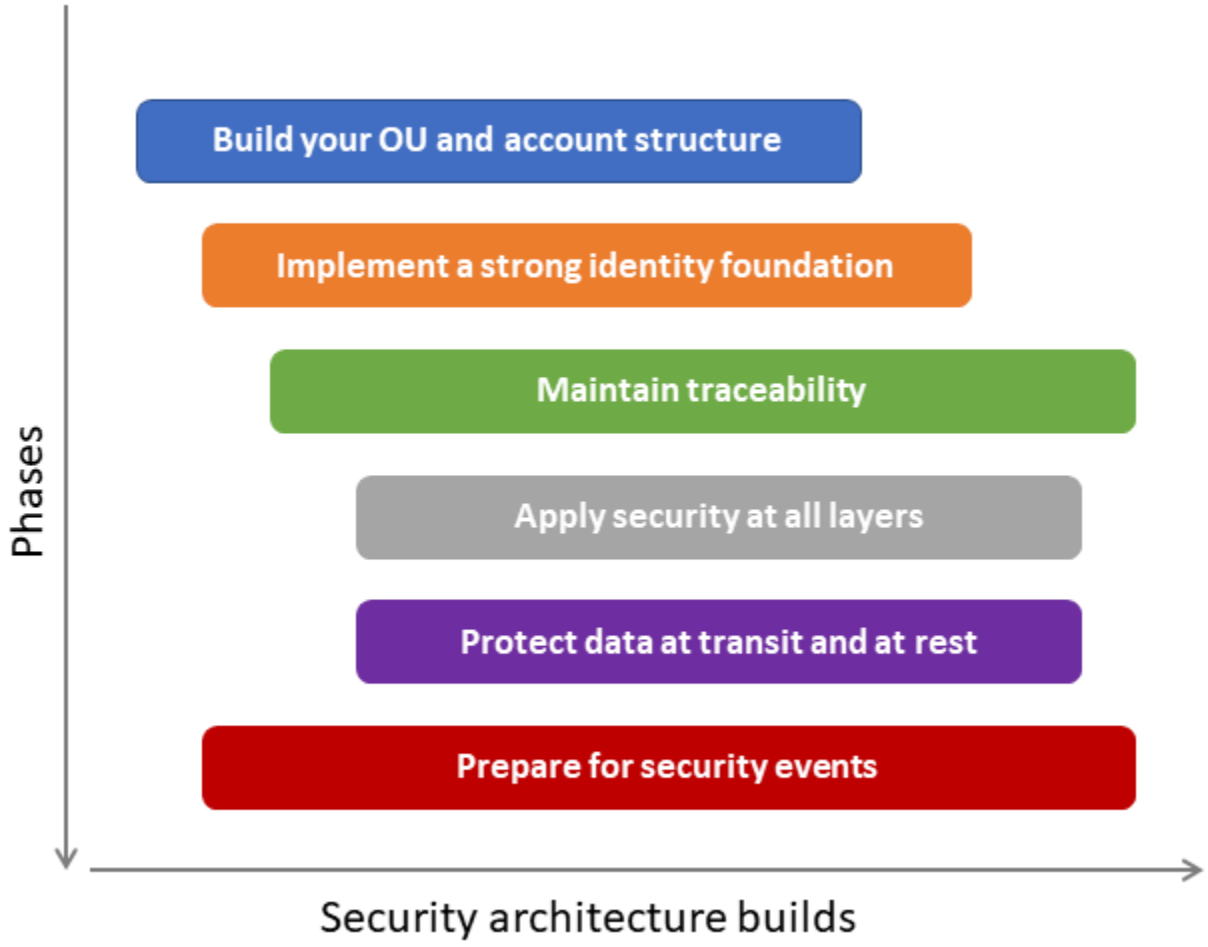
AWS SRA는 보안 도구 계정의 설계와 모든 보안 서비스 내의 공통 보안 서비스 배포를 통해 조직 전체에서 보안 이벤트를 감지할 수 있는 기능을 AWS 계정 제공합니다. 보안 도구 계정 내의 Amazon Detective는 보안 이벤트를 분류하고 근본 원인을 식별하는 데 도움이 됩니다. AWS 보안 조사 중에 관련 로그를 검토하여 인시던트의 전체 범위와 타임라인을 기록하고 이해할 수 있어야 합니다. 관심 있는 특정 작업이 발생할 때 알림 생성에도 로그가 필요합니다. AWS SRA는 모든 보안 및 운영 로그의 변경 불가능한 저장을 위해 중앙 로그 아카이브 계정을 권장합니다. CloudWatch 로그 그룹에 저장된 데이터에 대해 CloudWatch Logs Insights를 사용하고 Amazon S3에 저장된 데이터에 대해 Amazon Athena 및 Amazon OpenSearch Service를 사용하여 로그를 쿼리할 수 있습니다. CloudWatch Amazon S3 Amazon Security Lake를 사용하여 AWS 환경, 서비스형 소프트웨어(SaaS) 공급자, 온프레미스 및 기타 클라우드 공급자의 보안 데이터를 자동으로 중앙 집중화할 수 있습니다. AWS SRA에 설명된 대로 Security Tooling 계정 또는 모든 전용 계정에서 구독자를 설정하여 조사를 위해 해당 로그를 쿼리합니다.

AWS 보안 인시던트 대응는 보안 인시던트 대응, 조사 및 문제 해결을 자동화하는 데 도움이 됩니다. 보안 이벤트에 빠르고 일관되게 대응할 수 있도록 사전 구축된 플레이북과 워크플로를 제공합니다. 사전 대응 기능이 활성화되면 Security Incident Response가 Security Hub CSPM 및 GuardDuty와 통합되어 보안 조사 결과가 감지되면 응답 워크플로를 자동으로 트리거합니다. 이 서비스는 AWS 조직 전체에서 인시던트 대응 프로세스를 표준화하고 자동화하는 데 도움이 됩니다. 추가 지원이 필요한 경우 서비스 지원 사례를 열어 고객 인시던트 대응 팀(CIRT)에 AWS 문의할 수 있습니다.

> 설계 고려 사항
>
> - 클라우드 여정이 시작될 때부터 보안 이벤트를 감지하고 대응할 준비를 시작해야 합니다. 제한된 리소스를 더 잘 활용하려면 보안 이벤트를 감지할 때 관련 AWS 리소스의 중요도에 따

라 분류 및 응답의 우선순위를 지정할 수 있도록 리소스에 데이터 및 비즈니스 중요도를 할당합니다.

- 이 단원에서 설명한 대로 클라우드 보안 아키텍처를 빌드하는 단계는 본질적으로 순차적입니다. 그러나 다음 단계를 시작하기 전에 한 단계가 완전히 완료될 때까지 기다릴 필요는 없습니다. 클라우드 보안 태세를 발전시키면서 여러 단계에서 동시에 작업을 시작하고 각 단계를 발전시키는 반복적인 접근 방식을 채택하는 것이 좋습니다. 다양한 단계를 거치면 설계가 진화합니다. 다음 다이어그램에 표시된 제안된 시퀀스를 특정 요구 사항에 맞게 조정하는 것이 좋습니다.



구현 예제

AWS SRA 코드 라이브러리는 계정에 관리를 위임하여 Amazon Detective 를 자동으로 활성화 하고(예: 감사 또는 보안 도구) 기존 및 향후 AWS Organizations 계정에 대해 Detective를 구성하는 Detective Organization의 샘플 구현을 제공합니다.

AWS SRA 모범 사례 체크리스트

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

이 섹션에서는이 가이드 전체에 자세히 설명된 AWS SRA 모범 사례를 보안 아키텍처 버전을 빌드할 때 따를 수 있는 체크리스트로 추출합니다 AWS. 이 목록을 가이드 검토를 대체하는 것이 아니라 참조 지점으로 사용합니다. 체크리스트는 별로 그룹화됩니다 AWS 서비스. AWS SRA 모범 사례 체크리스트를 기준으로 기존 AWS 환경을 프로그래밍 방식으로 검증하려면 SRA Verify를 사용할 수 있습니다.

SRA Verify는 여러 AWS 계정 및 리전에서 조직의 AWS SRA 조정을 평가하는 데 도움이 되는 보안 평가 도구입니다. AWS SRA 지침에 따라 구현을 검증하는 자동 검사를 제공하여 AWS SRA 권장 사항에 직접 매핑됩니다. 이 도구를 사용하면 보안 서비스가 참조 아키텍처에 따라 올바르게 구성되었는지 확인할 수 있습니다.이 도구는 AWS 환경이 보안 모범 사례를 따르도록 세부 조사 결과와 실행 가능한 수정 단계를 제공합니다. SRA Verify는 조직 감사(보안 도구) 계정 AWS CodeBuild 에서 실행되도록 설계되었습니다. SRA Verify 라이브러리를 사용하여 로컬에서 실행하거나 확장할 수도 있습니다.

> **Note**
>
> SRA Verify에는 여러 서비스에 대한 검사가 포함되어 있지만 AWS SRA의 모든 고려 사항에 대한 검사가 포함되어 있지 않을 수 있습니다. 자세한 내용은 AWS SRA 라이브러리의 가이드를 참조하세요.

AWS Organizations

- AWS Organizations 는 모든 기능에서 활성화됩니다.
- 서비스 제어 정책(SCPs)은 IAM 보안 주체에 대한 액세스 제어 지침을 정의하는 데 사용됩니다.
- 리소스 제어 정책(RCPs)은 AWS 리소스에 대한 액세스 제어 지침을 정의하는 데 사용됩니다.
- 선언적 정책은 조직 전체에서 지정된에 대해 원하는 구성을 중앙 AWS 서비스 에서 선언하고 적용하는 데 사용됩니다.
- 파운데이션 서비스를 제공하는 멤버 계정을 그룹화하기 위해 세 가지 기본 OUs(보안, 인프라 및 워크로드)가 생성됩니다.
- 보안 도구 계정은 보안 OU 아래에 생성됩니다. 이 계정은 AWS 보안 서비스 및 기타 타사 보안 도구에 대한 중앙 집중식 관리를 제공합니다.

- 로그 아카이브 계정은 보안 OU 아래에 생성됩니다. 이 계정은 AWS 서비스 및 애플리케이션 로그의 엄격하게 제어되는 중앙 로그 리포지토리를 제공합니다.
- 네트워크 계정은 인프라 OU에서 생성됩니다. 이 계정은 애플리케이션과 더 광범위한 인터넷 간의 게이트웨이를 관리합니다. 개별 애플리케이션 워크로드, 보안 및 기타 인프라에서 네트워킹 서비스, 구성 및 작업을 격리합니다.
- 공유 서비스 계정은 인프라 OU에서 생성됩니다. 이 계정은 여러 애플리케이션과 팀이 결과를 제공하는 데 사용하는 서비스를 지원합니다.
- 애플리케이션 계정은 워크로드 OU에서 생성됩니다. 이 계정은 엔터프라이즈 애플리케이션을 실행하고 유지하기 위해 기본 인프라와 서비스를 호스팅합니다. 이 가이드는 표현을 제공하지만 실제로는 애플리케이션, 개발 환경 및 기타 보안 고려 사항으로 구분된 여러 OUs 및 멤버 계정이 있습니다.
- 모든 멤버 계정의 결제, 운영 및 보안에 대한 대체 연락처 정보가 구성됩니다.

AWS CloudTrail

- 조직 추적은 관리 계정 및 조직의 모든 멤버 계정에서 CloudTrail 관리 이벤트를 제공할 수 AWS 있도록 구성됩니다.
- 조직 추적은 다중 리전 추적으로 구성됩니다.
- 조직 추적은 글로벌 리소스에서 이벤트를 캡처하도록 구성됩니다.
- 특정 데이터 이벤트를 캡처하기 위한 추가 추적은 민감한 AWS 리소스 활동을 모니터링하기 위해 필요에 따라 구성됩니다.
- Security Tooling 계정은 조직 추적의 위임된 관리자로 설정됩니다.
- 조직 추적은 모든 새 멤버 계정에 대해 자동으로 활성화되도록 구성됩니다.
- 조직 추적은 로그 아카이브 계정에서 호스팅되는 중앙 집중식 S3 버킷에 로그를 게시하도록 구성됩니다.
- 조직 추적에는 로그 파일의 무결성을 확인하기 위한 로그 파일 검증이 활성화되어 있습니다.
- 조직 추적은 로그 보존을 위해 CloudWatch Logs와 통합됩니다.
- 조직 추적은 고객 관리형 키를 사용하여 암호화됩니다.
- Log Archive 계정의 로그 리포지토리에 사용되는 중앙 S3 버킷은 고객 관리형 키로 암호화됩니다.
- Log Archive 계정의 로그 리포지토리에 사용되는 중앙 S3 버킷은 변경 불가능을 위해 S3 객체 잠금으로 구성됩니다.
- Log Archive 계정의 로그 리포지토리에 사용되는 중앙 S3 버킷에 대해 버전 관리가 활성화됩니다.
- Log Archive 계정의 로그 리포지토리에 사용되는 중앙 S3 버킷에는 리소스 Amazon 리소스 이름(ARN)을 통한 조직 추적에 의해서만 객체 업로드를 제한하는 리소스 정책이 정의되어 있습니다.

AWS Security Hub CSPM

- Security Hub CSPM은 모든 멤버 계정과 관리 계정에 대해 활성화됩니다.
- AWS Config 는 Security Hub CSPM의 사전 조건으로 모든 멤버 계정에 대해 활성화됩니다.
- Security Tooling 계정은 Security Hub CSPM의 위임된 관리자로 설정됩니다.
- Amazon GuardDuty 및 Amazon Detective에는 원활한 서비스 통합을 위해 Security Hub CSPM과 동일한 위임된 관리자 계정이 있습니다.
- 중앙 구성은 여러 AWS 계정 및에서 Security Hub CSPM을 설정하고 관리하는 데 사용됩니다 AWS 리전.
- 모든 OU 및 멤버 계정은 Security Hub CSPM의 위임된 관리자가 중앙에서 관리하는 것으로 지정됩니다.
- Security Hub CSPM은 모든 새 멤버 계정에 대해 자동으로 활성화됩니다.
- Security Hub CSPM은 새 표준 구성에 대해 자동으로 활성화됩니다.
- 모든 리전의 Security Hub CSPM 조사 결과는 단일 홈 리전으로 집계됩니다.
- 모든 멤버 계정의 Security Hub CSPM 조사 결과는 Security Tooling 계정 내에서 집계됩니다.
- Security Hub CSPM의 AWS 기본 모범 사례(FSBP) 표준은 모든 멤버 계정에 대해 활성화됩니다.
- Security Hub CSPM의 CIS AWS 파운데이션 벤치마크 표준은 모든 멤버 계정에 대해 활성화됩니다.
- 기타 Security Hub CSPM 표준은 해당하는 경우 활성화됩니다.
- Security Hub CSPM 자동화 규칙은 리소스 컨텍스트로 조사 결과를 보강하는 데 사용됩니다.
- Security Hub CSPM 자동 응답 및 문제 해결 기능은 특정 결과에 대해 자동 작업을 수행하는 사용자 지정 EventBridge 규칙을 생성하는 데 사용됩니다.

AWS Config

- AWS Config 레코더는 모든 멤버 계정과 관리 계정에 대해 활성화됩니다.
- AWS Config 레코더는 모든 리전에서 활성화됩니다.
- AWS Config 전송 채널 S3 버킷은 로그 아카이브 계정에서 중앙 집중화됩니다.
- AWS Config 위임된 관리자 계정은 보안 도구 계정으로 설정됩니다.
- AWS Config 에는 조직 집계자가 설정되어 있습니다. 애그리게이터에는 모든 리전이 포함됩니다.
- AWS Config 적합성 팩은 위임된 관리자 계정의 모든 멤버 계정에 균일하게 배포됩니다.

- AWS Config 규칙 결과는 Security Hub CSPM으로 자동 전송됩니다.

Amazon GuardDuty

- GuardDuty 감지기는 모든 멤버 계정과 관리 계정에 대해 활성화됩니다.
- GuardDuty 감지기는 모든 리전에서 활성화됩니다.
- GuardDuty 감지기는 모든 새 멤버 계정에 대해 자동으로 활성화됩니다.
- GuardDuty 위임된 관리는 보안 도구 계정으로 설정됩니다.
- CloudTrail 관리 이벤트, VPC 흐름 로그 및 Route 53 Resolver DNS 쿼리 로그와 같은 GuardDuty 기본 데이터 소스가 활성화됩니다.
- GuardDuty S3 보호가 활성화되었습니다.
- EBS 볼륨에 대한 GuardDuty 맬웨어 보호가 활성화되어 있습니다.
- S3용 GuardDuty 맬웨어 보호가 활성화되었습니다.
- GuardDuty RDS 보호가 활성화되었습니다.
- GuardDuty Lambda 보호가 활성화되었습니다.
- GuardDuty EKS 보호가 활성화되었습니다.
- GuardDuty EKS 런타임 모니터링이 활성화되어 있습니다.
- GuardDuty 확장 위협 탐지가 활성화되었습니다.
- GuardDuty 결과는 보존을 위해 로그 아카이브 계정의 중앙 S3 버킷으로 내보내집니다.

IAM

- IAM 사용자는 사용되지 않습니다.
- 멤버 계정에 대한 루트 액세스의 중앙 집중식 관리가 적용됩니다.
- 관리 계정에 대한 중앙 집중식 권한 루트 사용자 작업은 위임된 관리자로부터 적용됩니다.
- 중앙 집중식 루트 액세스 관리는 보안 도구 계정에 위임됩니다.
- 모든 멤버 계정 루트 자격 증명이 제거됩니다.
- 모든 멤버 및 관리 AWS 계정 암호 정책은 조직의 보안 표준에 따라 설정됩니다.
- IAM 액세스 어드바이저는 IAM 그룹, 사용자, 역할 및 정책에 대해 마지막으로 사용된 정보를 검토하는 데 사용됩니다.

- 권한 경계는 IAM 역할에 대해 가능한 최대 권한을 제한하는 데 사용됩니다.

IAM Access Analyzer

- IAM Access Analyzer는 모든 멤버 계정과 관리 계정에 대해 활성화됩니다.
- IAM Access Analyzer 위임된 관리자는 보안 도구 계정으로 설정됩니다.
- IAM Access Analyzer 외부 액세스 분석기는 모든 리전에서 신뢰하는 조직 영역으로 구성됩니다.
- IAM Access Analyzer 외부 액세스 분석기는 모든 리전에서 계정 신뢰 영역으로 구성됩니다.
- IAM Access Analyzer 내부 액세스 분석기는 모든 리전에서 신뢰하는 조직 영역으로 구성됩니다.
- IAM Access Analyzer 내부 액세스 분석기는 모든 리전에서 계정 신뢰 영역으로 구성됩니다.
- 현재 계정에 대한 IAM Access Analyzer 미사용 액세스 분석기가 생성됩니다.
- 현재 조직에 대한 IAM Access Analyzer 미사용 액세스 분석기가 생성됩니다.

Amazon Detective

- Detective는 모든 멤버 계정에 대해 활성화됩니다.
- Detective는 모든 새 멤버 계정에 대해 자동으로 활성화됩니다.
- Detective는 모든 리전에서 활성화됩니다.
- Detective 위임된 관리자는 보안 도구 계정으로 설정됩니다.
- Detective, GuardDuty 및 Security Hub CSPM 위임 관리자는 동일한 보안 도구 계정으로 설정됩니다.
- Detective는 원시 로그의 저장 및 분석을 위해 Security Lake와 통합됩니다.
- Detective는 결과를 수집하기 위해 GuardDuty와 통합됩니다.
- Detective는 분석을 위해 Amazon EKS 감사 로그를 수집하고 있습니다.
- Detective는 분석을 위해 Security Hub CSPM 로그를 수집하고 있습니다.

AWS Firewall Manager

- Firewall Manager 보안 정책이 설정되어 있습니다.
- Firewall Manager 위임된 관리자는 보안 도구 계정으로 설정됩니다.
- AWS Config 는 사전 조건으로 활성화됩니다.

- OU, 계정 및 리전별로 범위가 제한된 여러 Firewall Manager 관리자가 설정됩니다.
- Firewall Manager AWS WAF 보안 정책이 정의됩니다.
- Firewall Manager AWS WAF 중앙 집중식 로깅 정책이 정의됩니다.
- Firewall Manager Shield Advanced 보안 정책이 정의됩니다.
- Firewall Manager 보안 그룹 보안 정책이 정의됩니다.

Amazon Inspector –

- Amazon Inspector는 모든 멤버 계정에 대해 활성화됩니다.
- Amazon Inspector는 모든 새 멤버 계정에 대해 자동으로 활성화됩니다.
- Amazon Inspector 위임된 관리자는 보안 도구 계정으로 설정됩니다.
- Amazon Inspector EC2 취약성 스캔이 활성화되었습니다.
- Amazon Inspector ECR 이미지 취약성 스캔이 활성화되어 있습니다.
- Amazon Inspector Lambda 함수 및 계층 취약성 스캔이 활성화됩니다.
- Amazon Inspector Lambda 코드 스캔이 활성화되었습니다.
- Amazon Inspector 코드 보안 스캔이 활성화되어 있습니다.

Amazon Macie

- Macie는 해당 멤버 계정에 대해 활성화됩니다.
- Macie는 적용 가능한 새 멤버 계정에 대해 자동으로 활성화됩니다.
- Macie 위임 관리자는 보안 도구 계정으로 설정됩니다.
- Macie 조사 결과는 로그 아카이브 계정의 중앙 S3 버킷으로 내보내집니다.
- Macie 조사 결과를 저장하는 S3 버킷은 고객 관리형 키로 암호화됩니다.
- Macie 정책 및 분류 정책은 Security Hub CSPM에 게시됩니다.

Amazon Security Lake

- Security Lake 조직 구성이 활성화되어 있습니다.
- Security Lake 위임된 관리자는 보안 도구 계정으로 설정됩니다.
- 새 멤버 계정에 대해 Security Lake 조직 구성이 활성화됩니다.

- Security Tooling 계정은 로그 분석을 수행하기 위한 데이터 액세스 구독자로 설정됩니다.
- Security Tooling 계정은 로그 분석을 수행하기 위한 데이터 쿼리 구독자로 설정됩니다.
- 모든 또는 지정된 활성 멤버 계정에서 Security Lake에 대해 CloudTrail 관리 로그 소스가 활성화됩니다.
- 모든 또는 지정된 활성 멤버 계정에서 Security Lake에 대해 VPC 흐름 로그 소스가 활성화됩니다.
- 모든 또는 지정된 활성 멤버 계정에서 Security Lake에 대해 Route 53 로그 소스가 활성화됩니다.
- S3 로그 소스에 대한 CloudTrail 데이터 이벤트는 모든 또는 지정된 활성 멤버 계정의 Security Lake에 대해 활성화됩니다.
- Lambda 실행 로그 소스는 모든 또는 지정된 활성 멤버 계정의 Security Lake에 대해 활성화됩니다.
- 모든 또는 지정된 활성 멤버 계정에서 Security Lake에 대해 Amazon EKS 감사 로그 소스가 활성화됩니다.
- Security Hub 결과 로그 소스는 모든 또는 지정된 활성 멤버 계정의 Security Lake에 대해 활성화됩니다.
- 모든 또는 지정된 활성 멤버 계정에서 Security Lake에 대해 AWS WAF 로그 소스가 활성화됩니다.
- 위임된 관리자 계정의 Security Lake SQS 대기열은 고객 관리형 키로 암호화됩니다.
- 위임된 관리자 계정의 Security Lake SQS 배달 못한 편지 대기열은 고객 관리형 키로 암호화됩니다.
- Security Lake S3 버킷은 고객 관리형 키로 암호화됩니다.
- Security Lake S3 버킷에는 Security Lake에 의한 직접 액세스만 제한하는 리소스 정책이 있습니다.

AWS WAF

- 모든 CloudFront 배포가 연결됩니다 AWS WAF.
- 모든 Amazon API Gateway REST APIs 연결됩니다 AWS WAF.
- 모든 Application Load Balancer가 연결되어 있습니다 AWS WAF.
- All AWS AppSync GraphQL APIs와 연결됩니다 AWS WAF.
- 모든 Amazon Cognito 사용자 풀이 연결되어 있습니다 AWS WAF.
- 모든 AWS App Runner 서비스가와 연결되어 있습니다 AWS WAF.
- 모든 AWS Verified Access 인스턴스가와 연결되어 있습니다 AWS WAF.
- 모든 AWS Amplify 애플리케이션이와 연결됩니다 AWS WAF.
- AWS WAF 로깅이 활성화되었습니다.
- AWS WAF 로그는 로그 아카이브 계정의 S3 버킷에 중앙 집중화됩니다.

AWS Shield Advanced

- Shield Advanced 구독이 활성화되고 퍼블릭 리소스가 있는 모든 애플리케이션 계정에 대해 자동 갱신으로 설정됩니다.
- Shield Advanced는 모든 CloudFront 배포에 대해 구성됩니다.
- Shield Advanced는 모든 Application Load Balancer에 대해 구성됩니다.
- Shield Advanced는 모든 Network Load Balancer에 대해 구성됩니다.
- Shield Advanced는 모든 Route 53 호스팅 영역에 대해 구성됩니다.
- Shield Advanced는 모든 탄력적 IP 주소에 대해 구성됩니다.
- Shield Advanced는 모든 Global Accelerator에 대해 구성됩니다.
- CloudWatch 경보는 Shield Advanced로 보호되는 CloudFront 및 Route 53 리소스에 대해 구성됩니다.
- Shield 대응 팀(SRT) 액세스가 구성되어 있습니다.
- Shield Advanced 사전 대응이 활성화되어 있습니다.
- Shield Advanced 선제적 참여 고객 응대가 구성되어 있습니다.
- Shield Advanced 보호 리소스에는 사용자 지정 AWS WAF 규칙이 구성되어 있습니다.
- Shield Advanced 보호 리소스에는 자동 애플리케이션 계층 DDoS 완화가 활성화되어 있습니다.

AWS 보안 인시던트 대응

- AWS 보안 인시던트 대응은 전체 AWS 조직에 대해 활성화됩니다.
- AWS 보안 인시던트 대응 위임된 관리자가 보안 도구 계정으로 설정됩니다.
- 사전 대응 및 알림 분류 워크플로가 활성화됩니다.
- AWS 고객 인시던트 대응 팀(CIRT) 격리 작업이 승인됩니다.

AWS Audit Manager

- Audit Manager는 모든 멤버 계정에 대해 활성화됩니다.
- 새 멤버 계정에 대해 Audit Manager가 자동으로 활성화됩니다.
- Audit Manager 위임된 관리자는 보안 도구 계정으로 설정됩니다.
- AWS Config 는 Audit Manager의 사전 조건으로 활성화됩니다.
- 고객 관리형 키는 Audit Manager에 저장된 데이터에 사용됩니다.

- 기본 평가 보고서 대상이 구성됩니다.

IAM 리소스

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

AWS Identity and Access Management (IAM)은 기존 아키텍처 다이어그램에 포함된 서비스가 아니지만 AWS 조직의 모든 측면 AWS 계정, 및에 적용됩니다 AWS 서비스. 먼저 IAM 엔터티를 생성하고 권한을 부여 AWS 서비스 하지 않으면를 배포할 수 없습니다. IAM에 대한 전체 설명은이 문서의 범위를 벗어나지만이 섹션에서는 모범 사례 권장 사항 및 추가 리소스에 대한 포인터에 대한 중요한 요약을 제공합니다.

- IAM 모범 사례는 AWS 설명서의 IAM의 보안 모범 사례, 보안 블로그의 IAM 문서, AWS re:Invent 프레젠테이션을 참조하세요. AWS
- AWS Well-Architected 보안 원칙은 권한 가드레일 정의, 최소 권한 액세스 권한 부여, 퍼블릭 및 크로스 계정 액세스 분석, 리소스를 안전하게 공유, 지속적인 권한 감소, 긴급 액세스 프로세스 설정 등 권한 관리 프로세스의 주요 단계를 간략하게 설명합니다.
- 다음 표와 함께 제공되는 참고 사항은 사용 가능한 IAM 권한 정책 유형과 보안 아키텍처에서 이를 사용하는 방법에 대한 권장 지침의 개략적인 개요를 제공합니다. 자세한 내용은 AWS 적절한 IAM 정책 조합을 선택하는 방법에 대한 re:Invent 2020 동영상을 참조하세요.

사용 사례 또는 정책	효과	에서 관리	용도	와 관련됨	영향	에 배포됨
서비스 제어 정책 (SCP)	제한	플랫폼 또는 보안 팀과 같은 중앙 팀 [1]	가드레일, 거버넌스	조직, OU, 계정	조직, OU 및 계정의 모든 보안 주체	조직 관리 계정 [2]
리소스 제어 정책 (RCPs)	제한	플랫폼 또는 보안 팀과 같은 중앙 팀 [1]	가드레일, 거버넌스	조직, OU, 계정	멤버 계정의 리소스 [12]	조직 관리 계정 [2]
기준 계정 자동화 정책(플랫폼	권한 부여 및 제한	플랫폼, 보안 또는 IAM 팀과	(기준) 워크로드가 아닌 자동화	단일 계정 [4]	멤버 계정 내에서 자동화에 사	멤버 계정

이 계정을 운영하는 데 사용하는 IAM 역할)		같은 중앙 팀 [1]	역할에 대한 권한 [3]		용되는 보안 주체	
기본 인적 정책(사용자에게 작업을 수행할 수 있는 권한을 부여하는 IAM 역할)	권한 부여 및 제한	플랫폼, 보안 또는 IAM 팀과 같은 중앙 팀 [1]	인적 역할에 대한 권한 [5]	단일 계정 [4]	페더레이션 보안 주체 [5] 및 IAM 사용자 [6]	멤버 계정
권한 경계(권한 있는 개발자가 다른 보안 주체에게 할당할 수 있는 최대 권한)	제한	플랫폼, 보안 또는 IAM 팀과 같은 중앙 팀 [1]	애플리케이션 역할에 대한 가드레일(적용해야 함)	단일 계정 [4]	이 계정의 애플리케이션 또는 워크로드에 대한 개별 역할 [7]	멤버 계정
애플리케이션에 대한 시스템 역할 정책(개발자가 배포한 인프라에 연결된 역할)	권한 부여 및 제한	개발자에게 위임 [8]	애플리케이션 또는 워크로드에 대한 권한 [9]	단일 계정	이 계정의 보안 주체	멤버 계정
리소스 정책	권한 부여 및 제한	개발자에게 위임 [8,10]	리소스에 대한 권한	단일 계정	계정의 보안 주체 [11]	멤버 계정

중앙 루트 사용자 관리	권한 부여 및 제한	플랫폼, 보안 또는 IAM 팀과 같은 중앙 팀 [1]	멤버 계정 루트 사용자를 대규모로 중앙에서 관리	Organization	멤버 계정의 모든 루트 사용자	조직 관리 계정, 위임된 관리자 계정

테이블의 참고 사항:

1. 기업은 이러한 독립 제어의 책임을 나누고 서로의 정책을 피어 리뷰하는 많은 중앙 집중식 팀(예: 클라우드 플랫폼, 보안 운영 또는 ID 및 액세스 관리 팀)을 보유하고 있습니다. 테이블의 예제는 자리 표시자입니다. 기업에 가장 효과적인 업무 분리를 결정해야 합니다.
2. SCPs 사용하려면 내의 모든 기능을 활성화해야 합니다 AWS Organizations.
3. 파이프라인, 배포 도구, 모니터링 도구(예: AWS Lambda 및 AWS Config 규칙) 및 기타 권한에 대한 권한과 같은 자동화를 활성화하려면 일반적으로 일반적인 기준 역할 및 정책이 필요합니다. 이 구성은 일반적으로 계정이 프로비저닝될 때 전달됩니다.
4. 이는 단일 계정의 리소스(예: 역할 또는 정책)와 관련이 있지만 AWS CloudFormation StackSets를 사용하여 여러 계정에 복제하거나 배포할 수 있습니다.
5. 중앙 팀이 모든 멤버 계정에 배포하는 기본 인적 역할 및 정책의 핵심 세트를 정의합니다(대개 계정 프로비저닝 중에). 플랫폼 팀의 개발자, IAM 팀 및 보안 감사 팀을 예로 들 수 있습니다.
6. 가능하면 자격 증명 페더레이션(로컬 IAM 사용자 대신)을 사용합니다.
7. 권한 경계는 위임된 관리자가 사용합니다. 이 IAM 정책은 최대 권한을 정의하고 다른 정책(리소스에 대한 모든 작업을 허용하는 "*:*" 정책 포함)을 재정의합니다. 기준 인적 정책에는 역할(예: 워크로드 성능 역할)을 생성하고 정책을 연결하기 위한 조건으로 권한 경계가 필요합니다. SCPs와 같은 추가 구성은 권한 경계의 연결을 적용합니다.
8. 이는 충분한 가드레일(예: SCPs 및 권한 경계)이 배포되었다고 가정합니다.
9. 이러한 선택적 정책은 계정 프로비저닝 중에 또는 애플리케이션 개발 프로세스의 일부로 제공될 수 있습니다. 이러한 정책을 생성하고 연결할 수 있는 권한은 애플리케이션 개발자의 자체 권한에 의해 관리됩니다.
10. 로컬 계정 권한 외에도 중앙 집중식 팀(예: 클라우드 플랫폼 팀 또는 보안 운영 팀)은 종종 일부 리소스 기반 정책을 관리하여 교차 계정 액세스를 활성화하여 계정을 운영합니다(예: 로깅을 위해 S3 버킷에 대한 액세스 제공).
11. 리소스 기반 IAM 정책은 모든 계정의 모든 보안 주체를 참조하여 리소스에 대한 액세스를 허용하거나 거부할 수 있습니다. 익명 보안 주체를 참조하여 퍼블릭 액세스를 활성화할 수도 있습니다.

12RCPs의 하위 집합에 대한 리소스에 적용됩니다 AWS 서비스. 자세한 내용은 설명서의 RCPs를 AWS 서비스 지원하는 목록을 참조하세요. AWS Organizations

IAM 자격 증명에 잘 설명된 작업 세트에 필요한 권한만 있는지 확인하는 것은 악의적이거나 의도하지 않은 권한 침해 위험을 줄이는 데 중요합니다. 최소 권한 모델을 설정하고 유지하려면 초과 권한을 지속적으로 업데이트, 평가 및 완화하기 위한 의도적인 계획이 필요합니다. 다음은 해당 계획에 대한 몇 가지 추가 권장 사항입니다.

- 조직의 거버넌스 모델과 설정된 위험 선호도를 사용하여 특정 가드레일과 권한 경계를 설정합니다.
- 지속적인 반복 프로세스를 통해 최소 권한을 구현합니다. 이 연습은 일회성 연습이 아닙니다.
- SCPs 사용하여 실행 가능한 위험을 줄입니다. 이는 좁은 대상 제어가 아닌 광범위한 가드레일입니다.
- 권한 경계를 사용하여 IAM 관리를 더 안전한 방식으로 위임합니다.
  - 위임된 관리자가 자신이 생성하는 역할 및 사용자에게 적절한 IAM 경계 정책을 연결해야 합니다.
- defense-in-depth 접근 방식(자격 증명 기반 정책과 함께)으로 리소스 기반 IAM 정책을 사용하여 리소스에 대한 광범위한 액세스를 거부합니다.
- IAM Access Advisor, AWS CloudTrail IAM Access Analyzer 및 관련 도구를 사용하여 부여된 과거 사용량 및 권한을 정기적으로 분석합니다. 명백한 초과 권한을 즉시 해결합니다.
- 별표를 와일드카드로 사용하여 모든 리소스를 표시하는 대신 해당하는 경우 특정 리소스에 대한 광범위한 작업의 범위를 지정합니다.
- 요청에 따라 IAM 정책 예외를 빠르게 식별, 검토 및 승인하는 메커니즘을 구현합니다.

AWS SRA용 코드 리포지토리 예제

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

AWS SRA에서 지침을 구축하고 구현하는 데 도움이 되도록 https://github.com/aws-samples/aws-security-reference-architecture-examples 코드형 인프라(IaC) 리포지토리가이 가이드와 함께 제공됩니다. 이 리포지토리에는 개발자와 엔지니어가이 문서에 제시된 몇 가지 지침 및 아키텍처 패턴을 배포하는 데 도움이 되는 코드가 포함되어 있습니다. 이 코드는 AWS 전문 서비스 컨설턴트의 고객 직접 경험을 바탕으로 작성되었습니다. 템플릿은 본질적으로 일반적입니다. 템플릿의 목표는 완전한 솔루션을 제공하는 대신 구현 패턴을 설명하는 것입니다. AWS 서비스 구성 및 리소스 배포는 의도적으로 매우 제한적입니다. 환경 및 보안 요구 사항에 맞게 이러한 솔루션을 수정하고 조정해야 할 수 있습니다.

AWS SRA 코드 리포지토리는 AWS CloudFormation 및 Terraform 배포 옵션을 모두 포함하는 코드 샘플을 제공합니다. 솔루션 패턴은 두 가지 환경을 지원합니다. 하나는를 필요로 AWS Control Tower 하고 다른 하나는를 사용하지 AWS Organizations 않고 사용합니다 AWS Control Tower. 가 필요한이 리포지토리의 솔루션은 및 Customizations for AWS Control Tower (CfCT)를 사용하여AWS Control Tower환경 내에 배포 AWS CloudFormation되고 테스트 AWS Control Tower 되었습니다. 필요하지 않은 솔루션은를 사용하여 AWS Organizations환경 내에서 테스트 AWS Control Tower 되었습니다 AWS CloudFormation. CfCT 솔루션은 고객이 AWS 모범 사례를 기반으로 안전한 다중 계정 AWS 환경을 빠르게 설정하는 데 도움이 됩니다. 계정 및 리소스 생성을 통해 초기 보안 기준을 구현하면서 안전하고 확장 가능한 워크로드를 실행하기 위한 환경 설정을 자동화하여 시간을 절약할 수 있습니다. AWS Control Tower 또한는 다중 계정 아키텍처, ID 및 액세스 관리, 거버넌스, 데이터 보안, 네트워크 설계 및 로깅을 시작할 수 있는 기준 환경을 제공합니다. AWS SRA 리포지토리의 솔루션은이 문서에 설명된 패턴을 구현하기 위한 추가 보안 구성을 제공합니다.

다음은 AWS SRA 리포지토리의 솔루션 요약입니다. 각 솔루션에는 세부 정보가 포함된 `README.md` 파일이 포함되어 있습니다.

- CloudTrail Organization 솔루션은 조직 관리 계정 내에 조직 추적을 생성하고 Audit 또는 Security Tooling 계정과 같은 멤버 계정에 관리를 위임합니다. 이 추적은 Security Tooling 계정에서 생성된 고객 관리형 키로 암호화되며 로그 아카이브 계정의 S3 버킷에 로그를 전송합니다. 선택적으로 Amazon S3 및 AWS Lambda 함수에 대해 데이터 이벤트를 활성화할 수 있습니다. 조직 추적은 멤버 계정이 구성을 수정하지 못하도록 하면서 조직의 모든 AWS 계정 에 AWS 대한 이벤트를 로깅합니다.
- GuardDuty Organization 솔루션은 Security Tooling 계정에 관리를 위임하여 Amazon GuardDuty를 활성화합니다. 모든 기존 및 향후 AWS 조직 계정에 대해 보안 도구 계정 내에서 GuardDuty를 구성

합니다. 또한 GuardDuty 결과는 KMS 키로 암호화되어 로그 아카이브 계정의 S3 버킷으로 전송됩니다.

- Security Hub CSPM Organization 솔루션은 Security Tooling 계정에 관리를 위임하여 Security Hub CSPM을 구성합니다. 모든 기존 및 향후 AWS 조직 계정에 대해 Security Tooling 계정 내에서 Security Hub CSPM을 구성합니다. 또한 솔루션은 모든 계정 및 리전에서 활성화된 보안 표준을 동기화하고 Security Tooling 계정 내에서 리전 애그리게이터를 구성하기 위한 파라미터를 제공합니다. Security Tooling 계정 내에서 Security Hub CSPM을 중앙 집중화하면 보안 표준 규정 준수 및 AWS 서비스 및 타사 AWS Partner 통합의 조사 결과를 교차 계정 보기로 확인할 수 있습니다.
- Inspector 솔루션은 조직의 모든 계정 및 관리 리전에 대해 위임된 관리자(보안 도구) 계정 내에서 Amazon Inspector를 AWS 구성합니다.
- Firewall Manager 솔루션은 Security Tooling 계정에 관리를 위임하고 AWS Firewall Manager 보안 그룹 정책 및 여러 AWS WAF 정책으로 Firewall Manager를 구성하여 보안 정책을 구성합니다. 보안 그룹 정책에는 솔루션에서 배포하는 VPC(기존 또는 솔루션에서 생성) 내에서 허용되는 최대 보안 그룹이 필요합니다.
- Macie Organization 솔루션은 Security Tooling 계정에 관리를 위임하여 Amazon Macie를 활성화합니다. 모든 기존 및 향후 AWS 조직 계정에 대해 보안 도구 계정 내에서 Macie를 구성합니다. Macie는 KMS 키로 암호화된 중앙 S3 버킷으로 검색 결과를 보내도록 추가로 구성됩니다.
- AWS Config:
  - Config Aggregator 솔루션은 Security Tooling 계정에 관리를 위임하여 AWS Config 집계자를 구성합니다. 그런 다음 솔루션은 AWS 조직의 모든 기존 및 향후 계정에 대해 Security Tooling 계정 내의 AWS Config 집계자를 구성합니다.
  - 적합성 팩 조직 규칙 솔루션은 관리를 보안 도구 계정에 위임 AWS Config 규칙 하여 배포합니다. 그런 다음 조직의 모든 기존 및 향후 계정에 대해 위임된 관리자 계정 내에 AWS 조직 적합성 팩을 생성합니다. 솔루션은 암호화 및 키 관리 적합성 팩 운영 모범 사례 샘플 템플릿을 배포하도록 구성되어 있습니다.
  - AWS Config Control Tower Management Account 솔루션은 AWS Control Tower 관리 계정 AWS Config 에서 AWS Config 를 활성화하고 그에 따라 Security Tooling 계정 내의 애그리게이터를 업데이트합니다. 이 솔루션은 템플릿을 사용하여를 AWS Control Tower CloudFormation 참조 AWS Config 로 활성화하여 AWS 조직의 다른 계정과의 일관성을 보장합니다.
- IAM:
  - Access Analyzer 솔루션은 Security Tooling 계정에 관리를 위임하여 IAM Access Analyzer를 활성화합니다. 그런 다음 조직의 모든 기존 및 향후 계정에 대해 Security Tooling 계정 내에서 AWS 조직 수준 IAM Access Analyzer를 구성합니다. 또한 솔루션은 모든 멤버 계정 및 리전에 IAM Access Analyzer를 배포하여 계정 수준 권한 분석을 지원합니다.

  - IAM 암호 정책 솔루션은 AWS 조직의 모든 계정 내에서 암호 정책을 업데이트 AWS 계정 합니다. 솔루션은 업계 규정 준수 표준에 맞게 암호 정책 설정을 구성하기 위한 파라미터를 제공합니다.
- EC2 기본 EBS 암호화 솔루션은 각 AWS 계정 및 조직 내에서 계정 수준의 기본 Amazon EBS 암호화 AWS 리전 를 AWS 활성화합니다. 생성한 새 EBS 볼륨 및 스냅샷의 암호화를 적용합니다. 예를 들어 Amazon EBS는 인스턴스를 시작할 때 생성되는 EBS 볼륨과 암호화되지 않은 스냅샷에서 복사하는 스냅샷을 암호화합니다.
- S3 Block Account Public Access 솔루션은 AWS 계정 AWS 조직의 각 내에서 Amazon S3 계정 수준 설정을 활성화합니다. Amazon S3 퍼블릭 액세스 차단 기능은 액세스 포인트, 버킷 및 계정에 대한 설정을 제공하여 Amazon S3 리소스에 대한 퍼블릭 액세스를 관리하는 데 도움을 줍니다. 기본적으로 새 버킷, 액세스 포인트 및 객체는 퍼블릭 액세스를 허용하지 않습니다. 그러나 사용자는 퍼블릭 액세스를 허용하도록 버킷 정책, 액세스 포인트 정책 또는 객체 권한을 수정할 수 있습니다. Amazon S3 퍼블릭 액세스 차단 설정은 이러한 리소스에 대한 퍼블릭 액세스를 제한할 수 있도록 이러한 정책 및 권한을 재정의합니다.
- Detective Organization 솔루션은 계정(예: 감사 또는 보안 도구 계정)에 관리를 위임하고 모든 기존 및 향후 AWS Organizations 계정에 대해 Detective를 구성하여 Amazon Detective 활성화를 자동화합니다.
- Shield Advanced 솔루션은의 배포를 자동화 AWS Shield Advanced 하여의 애플리케이션에 향상된 DDoS 보호를 제공합니다 AWS.
- AMI Bakery Organization 솔루션은 표준 강화 Amazon Machine Image(AMI) 이미지를 구축하고 관리하는 프로세스를 자동화하는 데 도움이 됩니다. 이를 통해 AWS 인스턴스 전반의 일관성과 보안을 보장하고 배포 및 유지 관리 작업을 간소화할 수 있습니다.
- 패치 관리자 솔루션은 여러에서 패치 관리를 간소화하는 데 도움이 됩니다 AWS 계정. 이 솔루션을 사용하여 모든 관리형 인스턴스에서 AWS Systems Manager 에이전트(SSM 에이전트)를 업데이트하고 Windows 및 Linux 태그가 지정된 인스턴스에서 중요하고 중요한 보안 패치 및 버그 수정을 스캔하고 설치할 수 있습니다. 또한 솔루션은 새의 생성을 감지 AWS 계정 하고 해당 계정에 솔루션을 자동으로 배포하도록 기본 호스트 관리 구성 설정을 구성합니다.

기여자

기본 작성자:

- Avik Mukherjee, AWS 선임 보안 SA

기여자:

- Jason Hurst, AWS CIRT 선임 보안 조사자
- Abhishek Panday, AWS 책임 제품 관리자 – 기술
- Itay Meller, AWS 선임 전문가 SA
- Jonathan VanKim, AWS 보안 주체 SA
- Josh Du Lac, AWS 엔터프라이즈 보안 전략가
- James Thompson, AWS 선임 솔루션 아키텍트
- Jeremy Girven, AWS Specialist SA
- Rodney Underkoffler, AWS Specialist Senior SA
- Farhan Farooq, AWS 선임 솔루션 아키텍트
- Prashob Krishnan, AWS 기술 계정 관리자
- Meg Peddada, AWS 선임 보안 컨설턴트
- Ashwin Phadke, AWS 선임 솔루션 아키텍트
- Sowjanya Rajavaram, AWS 수석 보안 SA
- Tomek Jakubowski, AWS 선임 컨설턴트
- Arun Thomas, AWS 선임 솔루션 아키텍트
- Ross Warren, AWS 제품 솔루션 아키텍트
- Scott Conklin, AWS 선임 컨설턴트
- Ilya Epshteyn, 자격 증명 솔루션 AWS 선임 관리자
- Michael Haken, AWS 책임 기술자
- Mehial Mendrin, AWS 선임 컨설턴트
- Christopher Evensen, AWS 선임 기술 계정 관리자

검토:

- Eric Rose, AWS 보안 주체 SA
- Manoj Kumar, AWS Delivery Consultant

기술 작성:

- Handan Selamoglu, AWS 선임 기술 작성자

부록: AWS 보안, 자격 증명 및 규정 준수 서비스

간단한 설문 조사에 참여하여 AWS 보안 참조 아키텍처(AWS SRA)의 미래에 영향을 미칩니다.

소개 또는 재교육은 클라우드에서 워크로드와 애플리케이션을 보호하는 데 도움이 되는 목록은 웹 사이트의 보안, 자격 증명 및 규정 준수를 AWS 참조하세요. AWS AWS 서비스 이러한 서비스는 데이터 보호, 자격 증명 및 액세스 관리, 네트워크 및 애플리케이션 보호, 위협 탐지 및 지속적 모니터링, 규정 준수 및 데이터 개인 정보 보호의 5가지 범주로 그룹화됩니다.

데이터 보호 - 무단 액세스로부터 데이터, 계정 및 워크로드를 보호하는 데 도움이 되는 서비스를 AWS 제공합니다.

- Amazon Macie - 기계 학습 기반 보안 기능으로 민감한 데이터를 검색, 분류 및 보호합니다.
- AWS KMS - 데이터를 암호화하는 데 사용되는 키를 생성하고 제어합니다.
- AWS CloudHSM-에서 하드웨어 보안 모듈(HSMs)을 관리합니다 AWS 클라우드.
- AWS Certificate Manager -에 사용할 SSL/TLS 인증서를 프로비저닝, 관리 및 배포합니다 AWS 서비스.
- AWS Secrets Manager - 수명 주기 동안 데이터베이스 자격 증명, API 키 및 기타 보안 암호를 교체, 관리 및 검색합니다.

ID 및 액세스 관리 - AWS ID 서비스를 사용하면 ID, 리소스 및 권한을 대규모로 안전하게 관리할 수 있습니다.

- IAM - AWS 서비스 및 리소스에 대한 액세스를 안전하게 제어합니다.
- IAM Identity Center - 여러 AWS 계정 및 비즈니스 애플리케이션에 대한 SSO 액세스를 중앙에서 관리합니다.
- Amazon Cognito - 웹 및 모바일 애플리케이션에 사용자 가입, 로그인 및 액세스 제어를 추가합니다.
- AWS Directory Service -에서 관리형 Microsoft Active Directory를 사용합니다 AWS 클라우드.
- AWS RAM - AWS 리소스를 간단하고 안전하게 공유합니다.
- AWS Organizations - 여러에 대한 정책 기반 관리를 구현합니다 AWS 계정.
- Amazon Verified Permissions - 사용자 지정 애플리케이션에서 확장 가능하고 세분화된 권한 및 권한 부여를 관리합니다.

네트워크 및 애플리케이션 보호 - 이러한 범주의 서비스를 사용하면 조직 전체의 네트워크 제어 지점에서 세분화된 보안 정책을 적용할 수 있습니다. AWS 서비스 는 트래픽을 검사하고 필터링하여 호스트 수준, 네트워크 수준 및 애플리케이션 수준 경계에서 무단 리소스 액세스를 방지하는 데 도움이 됩니다.

- AWS Shield - 관리형 DDoS 보호 AWS 로에서 실행되는 웹 애플리케이션을 보호합니다.
- AWS WAF - 일반적인 웹 악용으로부터 웹 애플리케이션을 보호하고 가용성과 보안을 보장합니다.
- AWS Firewall Manager - 중앙 위치에서 AWS 계정 및 애플리케이션 간에 AWS WAF 규칙을 구성하고 관리합니다.
- AWS Systems Manager - OS 패치를 적용하고, 보안 시스템 이미지를 생성하고, 보안 운영 체제를 구성하도록 Amazon EC2 및 온프레미스 시스템을 구성 및 관리합니다.
- Amazon VPC - 정의한 가상 네트워크에서 AWS 리소스를 시작할 수 AWS 있는 논리적으로 격리된 섹션을 프로비저닝합니다.
- AWS Network Firewall - VPCs.
- Amazon Route 53 DNS 방화벽 - VPCs에서 아웃바운드 DNS 요청을 보호합니다.
- AWS Verified Access - 가상 프라이빗 네트워크(VPNs) 없이 애플리케이션에 대한 보안 액세스를 제공합니다.
- Amazon VPC Lattice service-to-service 연결, 보안 및 모니터링을 간소화합니다.

위협 탐지 및 지속적인 모니터링 - AWS 모니터링 및 탐지 서비스는 AWS 환경 내에서 잠재적 보안 인시던트를 식별하는 데 도움이 되는 지침을 제공합니다.

- AWS Security Hub CSPM - 보안 알림을 보고 관리하고 중앙 위치에서 규정 준수 검사를 자동화합니다.
- AWS Security Hub - 보안 조사 결과를 상호 연관시키고 보강하여 계정 및 전체에서 중요한 보안 문제의 우선순위를 지정합니다 AWS 리전.
- Amazon GuardDuty - 지능형 위협 탐지 및 지속적인 모니터링을 통해 AWS 계정 및 워크로드를 보호합니다.
- Amazon Inspector - 보안 평가를 자동화하여 배포된 애플리케이션의 보안 및 규정 준수를 개선합니다 AWS.
- AWS Config - AWS 리소스 구성을 기록하고 평가하여 규정 준수 감사, 리소스 변경 추적 및 보안 분석을 활성화합니다.
- AWS Config 규칙 - 리소스 격리, 추가 데이터로 이벤트 강화 또는 알려진 정상 상태로 구성 복원과 같은 환경 변경에 대응하여 자동으로 조치를 취하는 규칙을 생성합니다.

- AWS 보안 인시던트 대응 - 사전 구축된 플레이북 및 워크플로를 사용하여 보안 인시던트 대응, 조사 및 문제 해결을 자동화합니다.
- AWS CloudTrail - 사용자 활동 및 API 사용량을 추적하여에 대한 거버넌스, 운영 및 위험 감사를 활성화합니다 AWS 계정.
- Amazon Detective - 보안 데이터를 분석하고 시각화하여 잠재적 보안 문제의 근본 원인을 신속하게 파악합니다.
- AWS Lambda - 서버를 프로비저닝하거나 관리하지 않고도 코드를 실행하여 인시던트에 대한 프로그래밍되고 자동화된 대응을 확장할 수 있습니다.

규정 준수 및 데이터 개인 정보 보호 - 규정 준수 상태를 포괄적 AWS 으로 파악하고 비즈니스가 따르는 AWS 모범 사례 및 업계 표준에 따라 자동화된 규정 준수 검사를 사용하여 환경을 지속적으로 모니터링합니다.

- AWS Artifact - 무료 셀프 서비스 포털을 사용하여 AWS 보안 및 규정 준수 보고서에 대한 온디맨드 액세스를 얻고 온라인 계약을 선택합니다.
- AWS Audit Manager - AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 평가하는 방법을 간소화합니다.

문서 이력

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

변경 사항	설명	날짜
콘텐츠 재구성 및 업데이트	• Security Hub 및 AWS Nitro Enclaves에 대한 지침이 추가되었습니다. • 핵심 아키텍처에 초점을 맞추도록 AWS SRA를 재구성하고 심층 분석 섹션을 자격 증명 관리, 경계 보안, 사이버 포렌식, 생성형 AI 및 IoT에 대한 별도의 가이드로 이동했습니다. • AWS CloudTrail,, Amazon Detective AWS Config,, Amazon GuardDuty AWS Firewall Manager, IAM Access Analyzer, Amazon Security Lake AWS Shield Advanced및에 대한 추가 세부 정보를 포함하도록 기존 지침을 업데이트했습니다 AWS Audit Manager. Amazon GuardDuty	2025년 12월 22일
주요 업데이트	• 새로운 IAM 중앙 집중식 루트 사용자 액세스 관리, 리소스 제어 정책(RCPs) 및 선언적 정책에 대한 정보가 추가되었습니다.	2025년 8월 29일

	• 새 Security Hub CSPM에 대한 Security Hub CSPM 참조를 업데이트했습니다. • Amazon GuardDuty 및 Security Hub CSPM에 대한 새로운 서비스 기능이 포함되었습니다. • AWS 보안 인시던트 대응 서비스 지침이 추가되었습니다. • machine-to-machine 자격 증명 관리를 위한 VPC Lattice를 포함하도록 IAM 심층 분석 지침을 업데이트했습니다. • 새로운 심층 분석 지침인 IoT용 SRA가 추가되었습니다.	
추가 및 설명	• 보안 도구 계정 섹션에서 지침을 업데이트했습니다 AWS KMS . • 고객 자격 증명 관리 섹션에서 API Gateway 권한 부여에 대한 정보를 확장했습니다. • OU 및 계정 설계에 대한 설계 고려 사항을 추가하도록 생성형 AI 섹션을 업데이트했습니다. • AWS SRA 코드 리포지토리 섹션에서 새 패치 관리 솔루션에 대한 정보가 추가되었습니다.	2024년 9월 12일

주요 업데이트	• 심층 분석 아키텍처 지침에 대한 두 섹션, 즉 Amazon Bedrock을 사용한 생성형 AI와 자격 증명 관리를 추가했습니다. • AWS Identity and Access Management Access Analyzer, Amazon Detective, Amazon Inspector, AWS Artifact, AWS Config, Amazon Security Lake, AWS Security Hub CSPM및 Amazon CloudFront 섹션을 새로운 서비스 기능으로 업데이트했습니다. • 새로운 Terraform 배포 옵션과 AWS Shield Advanced 및 AMI Bakery 솔루션 추가를 포함하도록 AWS SRA 코드 리포지토리 섹션을 업데이트했습니다.	2024년 6월 7일

주요 업데이트	• Amazon Verified Permissions 및 Amazon VPC Lattice에 대한 아키텍처 지침을 추가하도록 네트워크 계정 AWS Verified Access및 애플리케이션 계정 섹션을 업데이트했습니다. • 보안 기능을 기반으로 심층 분석 아키텍처 지침을 추가했습니다. • AI/ML을 AWS 서비스 사용하여 더 나은 보안 결과를 제공하는 방법에 대한 새로운 지침이 추가되었습니다. • 단계별 방식으로 보안 아키텍처를 계획하는 방법에 대한 지침이 추가되었습니다.	2023년 11월 4일
Security Lake 추가	Amazon Security Lake와 관련된 설계 지침을 추가하도록 보안 도구 계정 및 로그 아카이브 계정 섹션을 업데이트했습니다.	2023년 9월 22일
마이너 업데이트	• 새로운 AWS 서비스 기능과 모범 사례를 반영하도록 기존 지침을 업데이트했습니다. • AWS CloudTrail AWS IAM Identity Center및 엣지 보안에 대한 아키텍처 지침이 업데이트되었습니다.	2023년 5월 10일

설문 조사	조직에서 AWS SRA를 사용하는 방법을 더 잘 이해하기 위해 간단한 설문 조사를 추가했습니다.	2022년 12월 14일
참조 아키텍처 다이어그램의 소스 파일	AWS 보안 참조 아키텍처 섹션에서이 가이드의 아키텍처 다이어그램을 편집 가능한 PowerPoint 형식으로 제공하는 다운로드 파일을 추가했습니다.	2022년 11월 17일
보안 기반 섹션 업데이트	보안 기반 섹션에서 Well-Architected Framework 원칙 및 보안 설계 원칙에 대한 정보를 업데이트했습니다.	2022년 9월 27일
주요 추가 및 업데이트	• AWS SRA 및 주요 구현 지침을 사용하는 방법에 대한 정보가 추가되었습니다. • AWS Artifact, Amazon Inspector, Amazon Route 53 AWS RAM,, AWS Control Tower AWS Audit Manager, Directory Service, Amazon Cognito 및 Network Access Analyzer와 AWS 서비스 같은 추가에 대한 아키텍처 지침이 추가되었습니다. • 새로운 AWS 서비스 기능과 모범 사례를 반영하도록 기존 지침을 업데이트했습니다.	2022년 7월 25일
一	최초 게시	2021년 6월 23일

AWS 권장 가이드 용어집

다음은 AWS 권장 가이드에서 제공하는 전략, 가이드 및 패턴에서 일반적으로 사용되는 용어입니다. 용어집 항목을 제안하려면 용어집 끝에 있는 피드백 제공 링크를 사용하십시오.

숫자

7가지 전략

애플리케이션을 클라우드로 이전하기 위한 7가지 일반적인 마이그레이션 전략 이러한 전략은 Gartner가 2011년에 파악한 5가지 전략을 기반으로 하며 다음으로 구성됩니다.

- 리팩터링/리아키텍트 - 클라우드 네이티브 기능을 최대한 활용하여 애플리케이션을 이동하고 해당 아키텍처를 수정함으로써 민첩성, 성능 및 확장성을 개선합니다. 여기에는 일반적으로 운영 체제와 데이터베이스 이식이 포함됩니다. 예: 온프레미스 Oracle 데이터베이스를 Amazon Aurora PostgreSQL 호환 에디션으로 마이그레이션합니다.
- 리플랫포밍(리프트 앤드 리셰이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 AWS 클라우드의 Amazon Relational Database Service(Amazon RDS) for Oracle로 마이그레이션합니다.
- 재구매(드롭 앤드 숍) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com으로 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 AWS 클라우드클라우드의 EC2 인스턴스에 있는 Oracle로 마이그레이션합니다.
- 재배치(하이퍼바이저 수준의 리프트 앤 시프트) - 새 하드웨어를 구매하거나, 애플리케이션을 다시 작성하거나, 기존 운영을 수정하지 않고도 인프라를 클라우드로 이동합니다. 온프레미스 플랫폼에서 동일한 플랫폼의 클라우드 서비스로 서버를 마이그레이션합니다. 예: Microsoft Hyper-V 애플리케이션을 로 마이그레이션합니다 AWS.
- 유지(보관) - 소스 환경에 애플리케이션을 유지합니다. 대규모 리팩터링이 필요하고 해당 작업을 나중으로 연기하려는 애플리케이션과 비즈니스 차원에서 마이그레이션할 이유가 없어 유지하려는 레거시 애플리케이션이 여기에 포함될 수 있습니다.
- 사용 중지 - 소스 환경에서 더 이상 필요하지 않은 애플리케이션을 폐기하거나 제거합니다.

A

ABAC

속성 기반 액세스 제어를 참조하세요.

추상화된 서비스

관리형 서비스를 참조하세요.

ACID

원자성, 일관성, 격리성, 내구성을 참조하세요.

능동-능동 마이그레이션

양방향 복제 도구 또는 이중 쓰기 작업을 사용하여 소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되고, 두 데이터베이스 모두 마이그레이션 중 연결 애플리케이션의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 이 방법은 일회성 전환이 필요한 대신 소규모의 제어된 배치로 마이그레이션을 지원합니다. 더 유연하지만 액티브 패시브 마이그레이션보다 더 많은 작업이 필요합니다.

능동-수동 마이그레이션

소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되지만 소스 데이터베이스만 연결 애플리케이션의 트랜잭션을 처리하고 데이터는 대상 데이터베이스로 복제되는 데이터베이스 마이그레이션 방법입니다. 대상 데이터베이스는 마이그레이션 중 어떤 트랜잭션도 허용하지 않습니다.

집계 함수

행 그룹에서 작동하고 그룹에 대한 단일 반환 값을 계산하는 SQL 함수입니다. 집계 함수의 예로 `SUM` 및 `MAX`가 있습니다.

AI

인공 지능을 참조하세요.

AIOps

인공 지능 운영을 참조하세요.

익명화

데이터세트에서 개인 정보를 영구적으로 삭제하는 프로세스입니다. 익명화는 개인 정보 보호에 도움이 될 수 있습니다. 익명화된 데이터는 더 이상 개인 데이터로 간주되지 않습니다.

안티 패턴

솔루션이 다른 솔루션보다 비생산적이거나 비효율적이거나 덜 효과적이어서 반복되는 문제에 자주 사용되는 솔루션입니다.

애플리케이션 제어

맬웨어로부터 시스템을 보호하기 위해 승인된 애플리케이션만 사용하도록 허용하는 보안 접근 방식입니다.

애플리케이션 포트폴리오

애플리케이션 구축 및 유지 관리 비용과 애플리케이션의 비즈니스 가치를 비롯하여 조직에서 사용하는 각 애플리케이션에 대한 세부 정보 모음입니다. 이 정보는 포트폴리오 탐색 및 분석 프로세스의 핵심이며 마이그레이션, 현대화 및 최적화할 애플리케이션을 식별하고 우선순위를 정하는 데 도움이 됩니다.

인공 지능

컴퓨터 기술을 사용하여 학습, 문제 해결, 패턴 인식 등 일반적으로 인간과 관련된 인지 기능을 수행하는 것을 전문으로 하는 컴퓨터 과학 분야입니다. 자세한 내용은 What is Artificial Intelligence?를 참조하십시오.

인공 지능 운영(AIOps)

기계 학습 기법을 사용하여 운영 문제를 해결하고, 운영 인시던트 및 사용자 개입을 줄이고, 서비스 품질을 높이는 프로세스입니다. AWS 마이그레이션 전략에서 AIOps가 사용되는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

비대칭 암호화

한 쌍의 키, 즉 암호화를 위한 퍼블릭 키와 복호화를 위한 프라이빗 키를 사용하는 암호화 알고리즘입니다. 퍼블릭 키는 복호화에 사용되지 않으므로 공유할 수 있지만 프라이빗 키에 대한 액세스는 엄격히 제한되어야 합니다.

원자성, 일관성, 격리성, 내구성(ACID)

오류, 정전 또는 기타 문제가 발생한 경우에도 데이터베이스의 데이터 유효성과 운영 신뢰성을 보장하는 소프트웨어 속성 세트입니다.

ABAC(속성 기반 액세스 제어)

부서, 직무, 팀 이름 등의 사용자 속성을 기반으로 세분화된 권한을 생성하는 방식입니다. 자세한 내용은 AWS Identity and Access Management (IAM) 설명서의 용 ABAC AWS를 참조하세요.

신뢰할 수 있는 데이터 소스

가장 신뢰할 수 있는 정보 소스로 간주되는 기본 버전의 데이터를 저장하는 위치입니다. 익명화, 편집 또는 가명화와 같은 데이터 처리 또는 수정의 목적으로 신뢰할 수 있는 데이터 소스의 데이터를 다른 위치로 복사할 수 있습니다.

가용 영역

다른 가용 영역의 장애로부터 격리 AWS 리전 되고 동일한 리전의 다른 가용 영역에 저렴하고 지연 시간이 짧은 네트워크 연결을 제공하는 내의 고유한 위치입니다.

AWS 클라우드 채택 프레임워크(AWS CAF)

조직이 클라우드로 성공적으로 전환 AWS 하기 위한 효율적이고 효과적인 계획을 개발하는 데 도움이 되는의 지침 및 모범 사례 프레임워크입니다. AWS CAF는 지침을 비즈니스, 사람, 거버넌스, 플랫폼, 보안 및 운영이라는 6가지 중점 영역으로 구성합니다. 비즈니스, 사람 및 거버넌스 관점은 비즈니스 기술과 프로세스에 초점을 맞추고, 플랫폼, 보안 및 운영 관점은 전문 기술과 프로세스에 중점을 둡니다. 예를 들어, 사람 관점은 인사(HR), 직원 배치 기능 및 인력 관리를 담당하는 이해관계자를 대상으로 합니다. 이러한 관점에서 AWS CAF는 성공적인 클라우드 채택을 위해 조직을 준비하는 데 도움이 되는 인력 개발, 교육 및 커뮤니케이션에 대한 지침을 제공합니다. 자세한 내용은 AWS CAF 웹사이트와 AWS CAF 백서를 참조하세요.

AWS 워크로드 검증 프레임워크(AWS WQF)

데이터베이스 마이그레이션 워크로드를 평가하고, 마이그레이션 전략을 권장하고, 작업 견적을 제공하는 도구입니다. AWS WQF는 AWS Schema Conversion Tool (AWS SCT)에 포함되어 있습니다. 데이터베이스 스키마 및 코드 객체, 애플리케이션 코드, 종속성 및 성능 특성을 분석하고 평가 보고서를 제공합니다.

B

악성 봇

개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

BCP

비즈니스 연속성 계획을 참조하세요.

동작 그래프

리소스 동작과 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰입니다. Amazon Detective에서 동작 그래프를 사용하여 실패한 로그온 시도, 의심스러운 API 직접 호출 및 유사한 작업을 검사할 수 있습니다. 자세한 내용은 Detective 설명서의 Data in a behavior graph를 참조하십시오.

빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. 엔디안도 참조하세요.

바이너리 분류

바이너리 결과(가능한 두 클래스 중 하나)를 예측하는 프로세스입니다. 예를 들어, ML 모델이 “이 이메일이 스팸인가요, 스팸이 아닌가요?”, '이 제품은 책인가요, 자동차인가요?' 등의 문제를 예측해야 할 수 있습니다.

블룸 필터

요소가 세트의 멤버인지 여부를 테스트하는 데 사용되는 메모리 효율성이 높은 확률론적 데이터 구조입니다.

블루/그린(Blue/Green) 배포

동일하지만 별개의 두 환경을 생성하는 배포 전략입니다. 하나의 환경(파란색)에서 현재 애플리케이션 버전을 실행하고 새 애플리케이션 버전은 다른 환경(녹색)에서 실행합니다. 이 전략을 사용하면 영향을 최소화하면서 신속하게 롤백할 수 있습니다.

bot

인터넷을 통해 자동화된 태스크를 실행하고 인적 활동이나 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같이 유용하거나 이로운 봇도 있습니다. 악성 봇이라고 하는 다른 일부 봇은 개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

봇넷

맬웨어에 감염되고 봇 허더 또는 봇 운영자와 같은 단일 당사자가 제어하는 봇 네트워크입니다. 봇넷은 봇의 규모와 봇의 영향 범위를 확대하는 가장 잘 알려진 메커니즘입니다.

브랜치

코드 리포지토리의 포함된 영역입니다. 리포지토리에 생성되는 첫 번째 브랜치가 기본 브랜치입니다. 기존 브랜치에서 새 브랜치를 생성한 다음 새 브랜치에서 기능을 개발하거나 버그를 수정할 수 있습니다. 기능을 구축하기 위해 생성하는 브랜치를 일반적으로 기능 브랜치라고 합니다. 기능을 출시할 준비가 되면 기능 브랜치를 기본 브랜치에 다시 병합합니다. 자세한 내용은 About branches(GitHub 설명서)를 참조하십시오.

긴급 액세스 권한

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는에 액세스할 수 AWS 계정 있는 빠른 방법입니다. 자세한 내용은 AWS Well-Architected 지침의 Implement break-glass procedures 지표를 참조하세요.

브라운필드 전략

사용자 환경의 기존 인프라 시스템 아키텍처에 브라운필드 전략을 채택할 때는 현재 시스템 및 인프라의 제약 조건을 중심으로 아키텍처를 설계합니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

버퍼 캐시

가장 자주 액세스하는 데이터가 저장되는 메모리 영역입니다.

사업 역량

기업이 가치를 창출하기 위해 하는 일(예: 영업, 고객 서비스 또는 마케팅)입니다. 마이크로서비스 아키텍처 및 개발 결정은 비즈니스 역량에 따라 이루어질 수 있습니다. 자세한 내용은 백서의 AWS에서 컨테이너화된 마이크로서비스 실행의 비즈니스 역량 중심의 구성화 섹션을 참조하십시오.

비즈니스 연속성 계획(BCP)

대규모 마이그레이션과 같은 중단 이벤트가 운영에 미치는 잠재적 영향을 해결하고 비즈니스가 신속하게 운영을 재개할 수 있도록 지원하는 계획입니다.

C

CAF

AWS Cloud Adoption Framework를 참조하세요.

카나리 배포

최종 사용자에게 제공하는 느린 증분 릴리스 버전입니다. 확신이 들면 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

클라우드 혁신 센터를 참조하세요.

CDC

데이터 캡처 변경을 참조하세요.

변경 데이터 캡처(CDC)

데이터베이스 테이블과 같은 데이터 소스의 변경 내용을 추적하고 변경 사항에 대한 메타데이터를 기록하는 프로세스입니다. 대상 시스템의 변경 내용을 감사하거나 복제하여 동기화를 유지하는 등의 다양한 용도로 CDC를 사용할 수 있습니다.

카오스 엔지니어링

시스템의 복원력을 테스트하기 위해 의도적으로 장애나 중단 이벤트를 도입합니다. AWS Fault Injection Service (AWS FIS)를 사용하여 AWS 워크로드에 스트레스를 주고 응답을 평가하는 실험을 수행할 수 있습니다.

CI/CD

지속적 통합 및 지속적 전송을 참조하세요.

분류

예측을 생성하는 데 도움이 되는 분류 프로세스입니다. 분류 문제에 대한 ML 모델은 이산 값을 예측합니다. 이산 값은 항상 서로 다릅니다. 예를 들어, 모델이 이미지에 자동차가 있는지 여부를 평가해야 할 수 있습니다.

클라이언트측 암호화

대상이 데이터를 AWS 서비스 수신하기 전에 로컬에서 데이터를 암호화합니다.

클라우드 혁신 센터(CCoE)

클라우드 모범 사례 개발, 리소스 동원, 마이그레이션 타임라인 설정, 대규모 혁신을 통한 조직 선도 등 조직 전체에서 클라우드 채택 노력을 추진하는 다분야 팀입니다. 자세한 내용은 AWS 클라우드 엔터프라이즈 전략 블로그의 CCoE 게시물을 참조하세요.

클라우드 컴퓨팅

원격 데이터 스토리지와 IoT 디바이스 관리에 일반적으로 사용되는 클라우드 기술 클라우드 컴퓨팅은 일반적으로 엣지 컴퓨팅 기술에 연결되어 있습니다.

클라우드 운영 모델

IT 조직에서 하나 이상의 클라우드 환경을 구축, 성숙화 및 최적화하는 데 사용되는 운영 모델입니다. 자세한 내용은 클라우드 운영 모델 구축을 참조하십시오.

클라우드 채택 단계

조직이 AWS 클라우드로 마이그레이션할 때 일반적으로 거치는 4단계는 다음과 같습니다.

- 프로젝트 - 개념 증명 및 학습 목적으로 몇 가지 클라우드 관련 프로젝트 실행
- 기반 – 클라우드 채택 확장을 위한 기초 투자(예: 랜딩 존 생성, CCoE 정의, 운영 모델 구축)
- 마이그레이션 - 개별 애플리케이션 마이그레이션
- Re-invention - 제품 및 서비스 최적화와 클라우드 혁신

이러한 단계는 Stephen Orban이 블로그 게시물 The Journey Toward Cloud-First and the Stages of Adoption on the AWS 클라우드 Enterprise Strategy 블로그에서 정의했습니다. AWS 마이그레이션 전략과 어떤 관련이 있는지에 대한 자세한 내용은 마이그레이션 준비 가이드를 참조하세요.

CMDB

구성 관리 데이터베이스를 참조하세요.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반적인 클라우드 리포지토리로 GitHub 또는 Bitbucket Cloud가 포함됩니다. 코드의 각 버전을 브랜치라고 합니다. 마이크로서비스 구조에서 각 리포지토리는 단일 기능 전용입니다. 단일 CI/CD 파이프라인은 여러 리포지토리를 사용할 수 있습니다.

콜드 캐시

비어 있거나, 제대로 채워지지 않았거나, 오래되었거나 관련 없는 데이터를 포함하는 버퍼 캐시입니다. 주 메모리나 디스크에서 데이터베이스 인스턴스를 읽어야 하기 때문에 성능에 영향을 미치며, 이는 버퍼 캐시에서 읽는 것보다 느립니다.

콜드 데이터

거의 액세스되지 않고 일반적으로 과거 데이터인 데이터. 이런 종류의 데이터를 쿼리할 때는 일반적으로 느린 쿼리가 허용됩니다. 이 데이터를 성능이 낮고 비용이 저렴한 스토리지 계층 또는 클래스로 옮기면 비용을 절감할 수 있습니다.

컴퓨터 비전(CV)

기계 학습을 사용하여 디지털 이미지 및 비디오와 같은 시각적 형식에서 정보를 분석하고 추출하는 AI 필드입니다. 예를 들어 Amazon SageMaker AI는 CV에 대한 이미지 처리 알고리즘을 제공합니다.

구성 드리프트

워크로드의 경우 구성이 예상되는 상태에서 변경됩니다. 이로 인해 워크로드가 규정을 준수하지 않을 수 있으며, 이는 일반적으로 점진적이고 의도되지 않은 작업입니다.

구성 관리 데이터베이스(CMDB)

하드웨어 및 소프트웨어 구성 요소와 해당 구성을 포함하여 데이터베이스와 해당 IT 환경에 대한 정보를 저장하고 관리하는 리포지토리입니다. 일반적으로 마이그레이션의 포트폴리오 탐색 및 분석 단계에서 CMDB의 데이터를 사용합니다.

규정 준수 팩

규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 AWS Config 규칙 및 수정 작업 모음입니다. YAML 템플릿을 사용하여 적합성 팩을 AWS 계정 및 리전 또는 조직 전체에 단일 엔터티로 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 적합성 팩을 참조하세요.

지속적 통합 및 지속적 전달(CI/CD)

소프트웨어 릴리스 프로세스의 소스, 빌드, 테스트, 스테이징 및 프로덕션 단계를 자동화하는 프로세스입니다. CI/CD는 일반적으로 파이프라인으로 설명됩니다. CI/CD를 통해 프로세스를 자동화하고, 생산성을 높이고, 코드 품질을 개선하고, 더 빠르게 제공할 수 있습니다. 자세한 내용은 지속적 전달의 이점을 참조하십시오. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 지속적 전달(Continuous Delivery)과 지속적인 개발을 참조하십시오.

CV

컴퓨터 비전을 참조하세요.

D

저장 데이터

스토리지에 있는 데이터와 같이 네트워크에 고정되어 있는 데이터입니다.

데이터 분류

중요도와 민감도를 기준으로 네트워크의 데이터를 식별하고 분류하는 프로세스입니다. 이 프로세스는 데이터에 대한 적절한 보호 및 보존 제어를 결정하는 데 도움이 되므로 사이버 보안 위험 관리 전략의 중요한 구성 요소입니다. 데이터 분류는 AWS Well-Architected Framework의 보안 원칙 구성 요소입니다. 자세한 내용은 데이터 분류를 참조하십시오.

데이터 드리프트

프로덕션 데이터와 ML 모델 학습에 사용된 데이터 간의 상당한 차이 또는 시간 경과에 따른 입력 데이터의 의미 있는 변화. 데이터 드리프트는 ML 모델 예측의 전반적인 품질, 정확성 및 공정성을 저하시킬 수 있습니다.

전송 중 데이터

네트워크를 통과하고 있는 데이터입니다. 네트워크 리소스 사이를 이동 중인 데이터를 예로 들 수 있습니다.

데이터 메시

중앙 집중식 관리 및 거버넌스를 통해 분산되고 탈중앙화된 데이터 소유권을 제공하는 아키텍처 프레임워크입니다.

데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. 에서 데이터를 최소화하면 개인 정보 보호 위험, 비용 및 분석 탄소 발자국을 줄일 AWS 클라우드 수 있습니다.

데이터 경계

신뢰할 수 있는 자격 증명만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스하도록 하는 데 도움이 되는 AWS 환경의 예방 가드레일 세트입니다. 자세한 내용은 데이터 경계 구축을 참조하세요 AWS.

데이터 사전 처리

원시 데이터를 ML 모델이 쉽게 구문 분석할 수 있는 형식으로 변환하는 것입니다. 데이터를 사전 처리한다는 것은 특정 열이나 행을 제거하고 누락된 값, 일관성이 없는 값 또는 중복 값을 처리함을 의미할 수 있습니다.

데이터 출처

라이프사이클 전반에 걸쳐 데이터의 출처와 기록을 추적하는 프로세스(예: 데이터 생성, 전송, 저장 방법).

데이터 주체

데이터를 수집 및 처리하는 개인입니다.

데이터 웨어하우스

분석과 같은 비즈니스 인텔리전스를 지원하는 데이터 관리 시스템입니다. 데이터 웨어하우스에는 보통 많은 양의 기록 데이터가 포함되며 일반적으로 쿼리 및 분석에 사용됩니다.

데이터 정의 언어(DDL)

데이터베이스에서 테이블 및 객체의 구조를 만들거나 수정하기 위한 명령문 또는 명령입니다.

데이터베이스 조작 언어(DML)

데이터베이스에서 정보를 수정(삽입, 업데이트 및 삭제)하기 위한 명령문 또는 명령입니다.

DDL

데이터 정의 언어를 참조하세요.

딥 앙상블

예측을 위해 여러 딥 러닝 모델을 결합하는 것입니다. 딥 앙상블을 사용하여 더 정확한 예측을 얻거나 예측의 불확실성을 추정할 수 있습니다.

딥 러닝

여러 계층의 인공 신경망을 사용하여 입력 데이터와 관심 대상 변수 간의 매핑을 식별하는 ML 하위 분야입니다.

심층 방어

네트워크와 그 안의 데이터 기밀성, 무결성 및 가용성을 보호하기 위해 컴퓨터 네트워크 전체에 일련의 보안 메커니즘과 제어를 신중하게 계층화하는 정보 보안 접근 방식입니다. 이 전략을 채택하면 AWS Organizations 구조의 여러 계층에 여러 제어를 AWS추가하여 리소스를 보호할 수 있습니다. 예를 들어, 심층 방어 접근 방식은 다단계 인증, 네트워크 세분화 및 암호화를 결합할 수 있습니다.

위임된 관리자

에서 AWS Organizations호환되는 서비스는 AWS 멤버 계정을 등록하여 조직의 계정을 관리하고 해당 서비스에 대한 권한을 관리할 수 있습니다. 이러한 계정을 해당 서비스의 위임된 관리자라고 합니다. 자세한 내용과 호환되는 서비스 목록은 AWS Organizations 설명서의 AWS Organizations와 함께 사용할 수 있는 AWS 서비스를 참조하십시오.

배포

대상 환경에서 애플리케이션, 새 기능 또는 코드 수정 사항을 사용할 수 있도록 하는 프로세스입니다. 배포에는 코드 베이스의 변경 사항을 구현한 다음 애플리케이션 환경에서 해당 코드베이스를 구축하고 실행하는 작업이 포함됩니다.

개발 환경

환경을 참조하세요.

탐지 제어

이벤트 발생 후 탐지, 기록 및 알림을 수행하도록 설계된 보안 제어입니다. 이러한 제어는 기존의 예방적 제어를 우회한 보안 이벤트를 알리는 2차 방어선입니다. 자세한 내용은 AWS에서 보안 제어 구현의 탐지 제어를 참조하세요.

개발 가치 흐름 매핑 (DVSM)

소프트웨어 개발 라이프사이클에서 속도와 품질에 부정적인 영향을 미치는 제약 조건을 식별하고 우선 순위를 지정하는 데 사용되는 프로세스입니다. DVSM은 원래 린 제조 방식을 위해 설계된 가치 흐름 매핑 프로세스를 확장합니다. 소프트웨어 개발 프로세스를 통해 가치를 창출하고 이동하는 데 필요한 단계와 팀에 중점을 둡니다.

디지털 트윈

건물, 공장, 산업 장비 또는 생산 라인과 같은 실제 시스템을 가상으로 표현한 것입니다. 디지털 트윈은 예측 유지 보수, 원격 모니터링, 생산 최적화를 지원합니다.

차원 테이블

스타 스키마에서 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블을 말합니다. 차원 테이블 속성은 일반적으로 텍스트 필드나 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 보통 쿼리 제약, 필터링 및 결과 세트 레이블 지정에 사용됩니다.

재해

워크로드 또는 시스템이 기본 배포 위치에서 비즈니스 목표를 달성하지 못하게 방해하는 이벤트입니다. 이러한 이벤트는 자연재해, 기술적 오류, 의도하지 않은 구성 오류 또는 멀웨어 공격과 같은 사람의 행동으로 인한 결과일 수 있습니다.

재해 복구(DR)

재해로 인한 가동 중지 시간 및 데이터 손실을 최소화하기 위해 사용하는 전략 및 프로세스입니다. 자세한 내용은 AWS Well-Architected Framework의 Disaster Recovery of Workloads on AWS: Recovery in the Cloud를 참조하세요.

DML

데이터베이스 조작 언어를 참조하세요.

도메인 기반 설계

구성 요소를 각 구성 요소가 제공하는 진화하는 도메인 또는 핵심 비즈니스 목표에 연결하여 복잡한 소프트웨어 시스템을 개발하는 접근 방식입니다. 이 개념은 에릭 에반스에 의해 그의 저서인 도메인 기반 디자인: 소프트웨어 중심의 복잡성 해결(Boston: Addison-Wesley Professional, 2003)에서 소개되었습니다. Strangler Fig 패턴과 함께 도메인 기반 설계를 사용하는 방법에 대한 자세한 내용은 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

DR

재해 복구를 참조하세요.

드리프트 감지

기준이 되는 구성과의 편차 추적을 말합니다. 예를 들어 AWS CloudFormation 를 사용하여 시스템 리소스의 드리프트를 감지하거나를 사용하여 AWS Control Tower 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 랜딩 존의 변경 사항을 감지할 수 있습니다.

DVSM

개발 가치 흐름 매핑을 참조하세요.

E

EDA

탐색 데이터 분석을 참조하세요.

EDI

전자 데이터 교환을 참조하세요.

엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 엣지 컴퓨팅은 클라우드 컴퓨팅에 비해 보다 통신 지연 시간을 줄이고 응답 시간을 개선할 수 있습니다.

전자 데이터 교환(EDI)

조직 간 비즈니스 문서의 자동화된 교환을 나타냅니다. 자세한 내용은 전자 데이터 교환(EDI)이란 무엇인가요?를 참조하세요.

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 사이퍼텍스트로 변환하는 컴퓨팅 프로세스입니다.

암호화 키

암호화 알고리즘에 의해 생성되는 무작위 비트의 암호화 문자열입니다. 키의 길이는 다양할 수 있으며 각 키는 예측할 수 없고 고유하게 설계되었습니다.

엔디안

컴퓨터 메모리에 바이트가 저장되는 순서입니다. 빅 엔디안 시스템은 가장 중요한 바이트를 먼저 저장합니다. 리틀 엔디안 시스템은 가장 덜 중요한 바이트를 먼저 저장합니다.

엔드포인트

서비스 엔드포인트를 참조하세요.

엔드포인트 서비스

Virtual Private Cloud(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. 를 사용하여 엔드포인트 서비스를 생성하고 다른 AWS 계정 또는 AWS Identity and Access Management (IAM) 보안 주체에 권한을 AWS PrivateLink 부여할 수 있습니다. 이러한 계정 또는 보안 주체는 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 자세한 내용은 Amazon Virtual Private Cloud(VPC) 설명서의 엔드포인트 서비스 생성을 참조하십시오.

엔터프라이즈 리소스 계획(ERP)

엔터프라이즈의 주요 비즈니스 프로세스(예: 회계, MES, 프로젝트 관리)를 자동화하고 관리하는 시스템입니다.

봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service (AWS KMS) 설명서의 봉투 암호화를 참조하세요.

환경

실행 중인 애플리케이션의 인스턴스입니다. 다음은 클라우드 컴퓨팅의 일반적인 환경 유형입니다.

- 개발 환경 - 애플리케이션 유지 관리를 담당하는 핵심 팀만 사용할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. 개발 환경은 변경 사항을 상위 환경으로 승격하기 전에 테스트하는 데 사용됩니다. 이러한 유형의 환경을 테스트 환경이라고도 합니다.
- 하위 환경 - 초기 빌드 및 테스트에 사용되는 환경을 비롯한 애플리케이션의 모든 개발 환경입니다.
- 프로덕션 환경 - 최종 사용자가 액세스할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. CI/CD 파이프라인에서 프로덕션 환경이 마지막 배포 환경입니다.
- 상위 환경 - 핵심 개발 팀 이외의 사용자가 액세스할 수 있는 모든 환경입니다. 프로덕션 환경, 프로덕션 이전 환경 및 사용자 수용 테스트를 위한 환경이 여기에 포함될 수 있습니다.

에픽

애자일 방법론에서 작업을 구성하고 우선순위를 정하는 데 도움이 되는 기능적 범주입니다. 에픽은 요구 사항 및 구현 작업에 대한 개괄적인 설명을 제공합니다. 예를 들어, AWS CAF 보안 에픽에는 ID 및 액세스 관리, 탐지 제어, 인프라 보안, 데이터 보호 및 인시던트 대응이 포함됩니다. AWS 마이그레이션 전략의 에픽에 대한 자세한 내용은 프로그램 구현 가이드를 참조하십시오.

ERP

엔터프라이즈 리소스 계획을 참조하세요.

탐색 데이터 분석(EDA)

데이터 세트를 분석하여 주요 특성을 파악하는 프로세스입니다. 데이터를 수집 또는 집계한 다음 초기 조사를 수행하여 패턴을 찾고, 이상을 탐지하고, 가정을 확인합니다. EDA는 요약 통계를 계산하고 데이터 시각화를 생성하여 수행됩니다.

F

팩트 테이블

스타 스키마의 중앙 테이블입니다. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블은 측정값이 있는 열 및 차원 테이블에 대한 외래 키가 있는 열과 같이 두 가지 열 유형을 포함합니다.

빠른 실패

개발 수명 주기를 줄이기 위해 빈번한 증분 테스트를 사용하는 철학입니다. 애자일 접근 방식의 핵심입니다.

장애 격리 경계

에서 장애의 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역, AWS 리전 컨트롤 플레인 또는 데이터 플레인과 같은 AWS 클라우드경계입니다. 자세한 내용은 AWS 장애 격리 경계를 참조하세요.

기능 브랜치

브랜치를 참조하세요.

기능

예측에 사용하는 입력 데이터입니다. 예를 들어, 제조 환경에서 기능은 제조 라인에서 주기적으로 캡처되는 이미지일 수 있습니다.

기능 중요도

모델의 예측에 특성이 얼마나 중요한지를 나타냅니다. 이는 일반적으로 SHAP(Shapley Additive Descriptions) 및 통합 그레디언트와 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

기능 변환

추가 소스로 데이터를 보강하거나, 값을 조정하거나, 단일 데이터 필드에서 여러 정보 세트를 추출하는 등 ML 프로세스를 위해 데이터를 최적화하는 것입니다. 이를 통해 ML 모델이 데이터를 활용

할 수 있습니다. 예를 들어, 날짜 '2021-05-27 00:15:37'을 '2021년', '5월', '목', '15일'로 분류하면 학습 알고리즘이 다양한 데이터 구성 요소와 관련된 미묘한 패턴을 학습하는 데 도움이 됩니다.

퓨샷 프롬프팅

유사한 태스크를 수행하도록 요청하기 전에 LLM에 태스크와 원하는 출력을 보여주는 몇 가지 예제를 제공합니다. 이 기법은 모델이 프롬프트에 포함된 예제(샷)에서 학습하는 컨텍스트 내 학습을 적용합니다. 퓨샷 프롬프팅은 특정 형식 지정, 추론 또는 분야별 지식이 필요한 태스크에 효과적일 수 있습니다. 제로샷 프롬프팅도 참조하세요.

FGAC

세분화된 액세스 제어를 참조하세요.

세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

플래시컷 마이그레이션

단계적 접근 방식을 사용하는 대신 변경 데이터 캡처를 통해 지속적 데이터 복제를 사용하여 최단 시간에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

FM

파운데이션 모델을 참조하세요.

파운데이션 모델(FM)

일반화되고 레이블이 지정되지 않은 데이터의 대규모 데이터세트에서 훈련된 대규모 딥 러닝 신경망입니다. FM은 언어 이해, 텍스트 및 이미지 생성, 자연어 대화와 같은 다양한 일반 태스크를 수행할 수 있습니다. 자세한 내용은 파운데이션 모델이란?을 참조하세요.

G

생성형 AI

대량의 데이터에서 훈련되었으며 간단한 텍스트 프롬프트를 사용하여 이미지, 비디오, 텍스트, 오디오와 같은 새 콘텐츠와 아티팩트를 생성할 수 있는 AI 모델의 하위 세트입니다. 자세한 내용은 생성형 AI란 무엇인가요?를 참조하세요.

지리적 차단

지리적 제한을 참조하세요.

지리적 제한(지리적 차단)

Amazon CloudFront에서 특정 국가의 사용자가 콘텐츠 배포에 액세스하지 못하도록 하는 옵션입니다. 허용 목록 또는 차단 목록을 사용하여 승인된 국가와 차단된 국가를 지정할 수 있습니다. 자세한 내용은 CloudFront 설명서의 콘텐츠의 지리적 배포 제한을 참조하십시오.

Gitflow 워크플로

하위 환경과 상위 환경이 소스 코드 리포지토리의 서로 다른 브랜치를 사용하는 방식입니다. Gitflow 워크플로는 레거시로 간주되며 트렁크 기반 워크플로는 선호되는 현대적 접근 방식입니다.

골든 이미지

시스템 또는 소프트웨어의 새 인스턴스를 배포하기 위한 템플릿으로 사용되는 해당 시스템 또는 소프트웨어의 스냅샷입니다. 예를 들어 제조 분야에서는 골든 이미지를 사용하여 여러 디바이스에서 소프트웨어를 프로비저닝할 수 있으며 이를 통해 딥이스 제조 작업의 속도, 확장성 및 생산성을 개선할 수 있습니다.

브라운필드 전략

새로운 환경에서 기존 인프라의 부재 시스템 아키텍처에 대한 그린필드 전략을 채택할 때 브라운필드라고도 하는 기존 인프라와의 호환성 제한 없이 모든 새로운 기술을 선택할 수 있습니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

가드레일

조직 단위(OU) 전체에서 리소스, 정책 및 규정 준수를 관리하는 데 도움이 되는 중요 규칙입니다. 예방 가드레일은 규정 준수 표준에 부합하도록 정책을 시행하며, 서비스 제어 정책과 IAM 권한 경계를 사용하여 구현됩니다. 탐지 가드레일은 정책 위반 및 규정 준수 문제를 감지하고 해결을 위한 알림을 생성하며, 이는 AWS Config Amazon GuardDuty AWS Security Hub CSPM, , AWS Trusted Advisor Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

H

HA

고가용성을 참조하세요.

이기종 데이터베이스 마이그레이션

다른 데이터베이스 엔진을 사용하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Oracle에서 Amazon Aurora로) 이기종 마이그레이션은 일반적으로 리아키텍트 작업의 일부이며 스

키마를 변환하는 것은 복잡한 작업일 수 있습니다.AWS 는 스키마 변환에 도움이 되는 AWS SCT를 제공합니다.

높은 가용성(HA)

문제나 재해 발생 시 개입 없이 지속적으로 운영할 수 있는 워크로드의 능력. HA 시스템은 자동으로 장애 조치되고, 지속적으로 고품질 성능을 제공하고, 성능에 미치는 영향을 최소화하면서 다양한 부하와 장애를 처리하도록 설계되었습니다.

히스토리언 현대화

제조 산업의 요구 사항을 더 잘 충족하도록 운영 기술(OT) 시스템을 현대화하고 업그레이드하는 데 사용되는 접근 방식입니다. 히스토리언은 공장의 다양한 출처에서 데이터를 수집하고 저장하는 데 사용되는 일종의 데이터베이스입니다.

홀드아웃 데이터

기계 학습 모델을 훈련하는 데 사용되는 데이터세트에서 보류되는 레이블이 지정된 기록 데이터의 일부입니다. 홀드아웃 데이터를 사용하여 모델 예측을 홀드아웃 데이터와 비교해 모델 성능을 평가할 수 있습니다.

동종 데이터베이스 마이그레이션

동일한 데이터베이스 엔진을 공유하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Microsoft SQL Server에서 Amazon RDS for SQL Server로) 동종 마이그레이션은 일반적으로 리호스팅 또는 리플랫포밍 작업의 일부입니다. 네이티브 데이터베이스 유틸리티를 사용하여 스키마를 마이그레이션할 수 있습니다.

핫 데이터

자주 액세스하는 데이터(예: 실시간 데이터 또는 최근 번역 데이터). 일반적으로 이 데이터에는 빠른 쿼리 응답을 제공하기 위한 고성능 스토리지 계층 또는 클래스가 필요합니다.

핫픽스

프로덕션 환경의 중요한 문제를 해결하기 위한 긴급 수정입니다. 핫픽스는 긴급하기 때문에 일반적인 DevOps 릴리스 워크플로 외부에서 실행됩니다.

하이퍼케어 기간

전환 직후 마이그레이션 팀이 문제를 해결하기 위해 클라우드에서 마이그레이션된 애플리케이션을 관리하고 모니터링하는 기간입니다. 일반적으로 이 기간은 1~4일입니다. 하이퍼케어 기간이 끝나면 마이그레이션 팀은 일반적으로 애플리케이션에 대한 책임을 클라우드 운영 팀에 넘깁니다.

I

IaC

코드형 인프라를 참조하세요.

자격 증명 기반 정책

AWS 클라우드 환경 내에서 권한을 정의하는 하나 이상의 IAM 보안 주체에 연결된 정책입니다.

유휴 애플리케이션

90일 동안 평균 CPU 및 메모리 사용량이 5~20%인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하거나 온프레미스에 유지하는 것이 일반적입니다.

IIoT

산업용 사물 인터넷을 참조하세요.

변경 불가능한 인프라

기존 인프라를 업데이트, 패치 또는 수정하는 대신 프로덕션 워크로드에 대한 새 인프라를 배포하는 모델입니다. 변경 불가능한 인프라는 변경 가능한 인프라보다 본질적으로 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 AWS Well-Architected Framework의 변경 불가능한 인프라를 사용하여 배포 모범 사례를 참조하세요.

인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 외부에서 네트워크 연결을 수락, 검사 및 라우팅하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

증분 마이그레이션

한 번에 전체 전환을 수행하는 대신 애플리케이션을 조금씩 마이그레이션하는 전환 전략입니다. 예를 들어, 처음에는 소수의 마이크로서비스나 사용자만 새 시스템으로 이동할 수 있습니다. 모든 것이 제대로 작동하는지 확인한 후에는 레거시 시스템을 폐기할 수 있을 때까지 추가 마이크로서비스 또는 사용자를 점진적으로 이동할 수 있습니다. 이 전략을 사용하면 대규모 마이그레이션과 관련된 위험을 줄일 수 있습니다.

Industry 4.0

연결성, 실시간 데이터, 자동화, 분석 및 AI/ML의 발전을 통해 제조 프로세스의 현대화를 나타내기 위해 2016년에 Klaus Schwab에서 도입한 용어입니다.

인프라

애플리케이션의 환경 내에 포함된 모든 리소스와 자산입니다.

코드형 인프라(IaC)

구성 파일 세트를 통해 애플리케이션의 인프라를 프로비저닝하고 관리하는 프로세스입니다. IaC는 새로운 환경의 반복 가능성, 신뢰성 및 일관성을 위해 인프라 관리를 중앙 집중화하고, 리소스를 표준화하고, 빠르게 확장할 수 있도록 설계되었습니다.

산업용 사물 인터넷(IIoT)

제조, 에너지, 자동차, 의료, 생명과학, 농업 등의 산업 부문에서 인터넷에 연결된 센서 및 디바이스의 사용 자세한 내용은 산업용 사물 인터넷(IoT) 디지털 트랜스포메이션 전략 구축을 참조하십시오.

검사 VPC

AWS 다중 계정 아키텍처에서는 VPC(동일하거나 다른 AWS 리전), 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 관리하는 중앙 집중식 VPCs입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

사물 인터넷(IoT)

인터넷이나 로컬 통신 네트워크를 통해 다른 디바이스 및 시스템과 통신하는 센서 또는 프로세서가 내장된 연결된 물리적 객체의 네트워크 자세한 내용은 IoT란?을 참조하십시오.

해석력

모델의 예측이 입력에 따라 어떻게 달라지는지를 사람이 이해할 수 있는 정도를 설명하는 기계 학습 모델의 특성입니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

IoT

사물 인터넷을 참조하세요.

IT 정보 라이브러리(ITIL)

IT 서비스를 제공하고 이러한 서비스를 비즈니스 요구 사항에 맞게 조정하기 위한 일련의 모범 사례 ITIL은 ITSM의 기반을 제공합니다.

IT 서비스 관리(ITSM)

조직의 IT 서비스 설계, 구현, 관리 및 지원과 관련된 활동 클라우드 운영을 ITSM 도구와 통합하는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

ITIL

IT 정보 라이브러리를 참조하세요.

ITSM

IT 서비스 관리를 참조하세요.

L

레이블 기반 액세스 제어(LBAC)

사용자 및 데이터 자체에 각각 보안 레이블 값을 명시적으로 할당하는 필수 액세스 제어(MAC)를 구현한 것입니다. 사용자 보안 레이블과 데이터 보안 레이블 간의 교차 부분에 따라 사용자가 볼 수 있는 행과 열이 결정됩니다.

랜딩 존

랜딩 존은 확장 가능하고 안전한 잘 설계된 다중 계정 AWS 환경입니다. 조직은 여기에서부터 보안 및 인프라 환경에 대한 확신을 가지고 워크로드와 애플리케이션을 신속하게 시작하고 배포할 수 있습니다. 랜딩 존에 대한 자세한 내용은 안전하고 확장 가능한 다중 계정 AWS 환경 설정을 참조하십시오.

대규모 언어 모델(LLM)

방대한 양의 데이터에서 사전 훈련된 딥 러닝 AI 모델입니다. LLM은 질문에 대한 답변, 문서 요약, 텍스트를 다른 언어로 번역, 문장 완성과 같은 여러 태스크를 수행할 수 있습니다. 자세한 내용은 대규모 언어 모델(LLM)이란 무엇인가요?를 참조하세요.

대규모 마이그레이션

300대 이상의 서버 마이그레이션입니다.

LBAC

레이블 기반 액세스 제어를 참조하세요.

최소 권한

작업을 수행하는 데 필요한 최소 권한을 부여하는 보안 모범 사례입니다. 자세한 내용은 IAM 설명서의 최소 권한 적용을 참조하십시오.

리프트 앤드 시프트

7R을 참조하세요.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. 엔디안도 참조하세요.

LLM

대규모 언어 모델을 참조하세요.

하위 환경

환경을 참조하세요.

M

기계 학습(ML)

패턴 인식 및 학습에 알고리즘과 기법을 사용하는 인공 지능의 한 유형입니다. ML은 사물 인터넷(IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 기계 학습을 참조하십시오.

기본 브랜치

브랜치를 참조하세요.

맬웨어

컴퓨터 보안 또는 프라이버시를 위협하도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 방해하거나 민감한 정보를 유출하거나 무단 액세스 권한을 확보할 수 있습니다. 맬웨어의 예로 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

AWS 서비스 는 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하고, 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. 관리형 서비스의 예로 Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB가 있습니다. 이를 추상화된 서비스라고도 합니다.

제조 실행 시스템(MES)

원자재를 생산 현장에서 완제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

Migration Acceleration Program을 참조하세요.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 조정을 위해 결과를 검사하는 전체 프로세스입니다. 메커니즘은 작동 시 자체적으로 강화하고 개선하는 주기입니다. 자세한 내용은 AWS Well-Architected Framework의 메커니즘 구축을 참조하세요.

멤버 계정

조직의 일부인 관리 계정을 AWS 계정 제외한 모든 계정. AWS Organizations하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다.

MES

제조 실행 시스템을 참조하세요.

메시지 큐 원격 분석 전송(MQTT)

리소스 제약이 있는 IoT 디바이스에 대한 게시 및 구독 패턴을 기반으로 하는 경량 Machine-to-Machine(M2M) 통신 프로토콜입니다.

마이크로서비스

잘 정의된 API를 통해 통신하고 일반적으로 소규모 자체 팀이 소유하는 소규모 독립 서비스입니다. 예를 들어, 보험 시스템에는 영업, 마케팅 등의 비즈니스 역량이나 구매, 청구, 분석 등의 하위 영역에 매핑되는 마이크로 서비스가 포함될 수 있습니다. 마이크로서비스의 이점으로 민첩성, 유연한 확장, 손쉬운 배포, 재사용 가능한 코드, 복원력 등이 있습니다. 자세한 내용은 AWS 서버리스 서비스를 사용하여 마이크로서비스 통합을 참조하세요.

마이크로서비스 아키텍처

각 애플리케이션 프로세스를 마이크로서비스로 실행하는 독립 구성 요소를 사용하여 애플리케이션을 구축하는 접근 방식입니다. 이러한 마이크로서비스는 경량 API를 사용하여 잘 정의된 인터페이스를 통해 통신합니다. 애플리케이션의 특정 기능에 대한 수요에 맞게 이 아키텍처의 각 마이크로서비스를 업데이트, 배포 및 조정할 수 있습니다. 자세한 내용은 에서 마이크로서비스 구현을 참조하세요 AWS.

Migration Acceleration Program(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 초기 마이그레이션 비용을 상쇄하는 데 도움이 되는 컨설팅 지원, 교육 및 서비스를 제공하는 AWS 프로그램입니다. MAP에는 레거시 마이그레이션을 체계적인 방식으로 실행하기 위한 마이그레이션 방법론과 일반적인 마이그레이션 시나리오를 자동화하고 가속화하는 도구 세트가 포함되어 있습니다.

대규모 마이그레이션

애플리케이션 포트폴리오의 대다수를 웨이브를 통해 클라우드로 이동하는 프로세스로, 각 웨이브에서 더 많은 애플리케이션이 더 빠른 속도로 이동합니다. 이 단계에서는 이전 단계에서 배운 모범 사례와 교훈을 사용하여 팀, 도구 및 프로세스의 마이그레이션 팩토리를 구현하여 자동화 및 민첩한 제공을 통해 워크로드 마이그레이션을 간소화합니다. 이것은 AWS 마이그레이션 전략의 세 번째 단계입니다.

마이그레이션 팩토리

자동화되고 민첩한 접근 방식을 통해 워크로드 마이그레이션을 간소화하는 다기능 팀입니다. 마이그레이션 팩토리 팀에는 일반적으로 스프린트에서 일하는 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자, DevOps 전문가가 포함됩니다. 엔터프라이즈 애플리케이션 포트폴리오의 20~50%는 공장 접근 방식으로 최적화할 수 있는 반복되는 패턴으로 구성되어 있습니다. 자세한 내용은 이 콘텐츠 세트의 클라우드 마이그레이션 팩토리 가이드와 마이그레이션 팩토리에 대한 설명을 참조하십시오.

마이그레이션 메타데이터

마이그레이션을 완료하는 데 필요한 애플리케이션 및 서버에 대한 정보 각 마이그레이션 패턴에는 서로 다른 마이그레이션 메타데이터 세트가 필요합니다. 마이그레이션 메타데이터의 예로는 대상 서브넷, 보안 그룹 및 AWS 계정이 있습니다.

마이그레이션 패턴

사용되는 마이그레이션 전략, 마이그레이션 대상, 마이그레이션 애플리케이션 또는 서비스를 자세히 설명하는 반복 가능한 마이그레이션 작업입니다. 예: AWS Application Migration Service를 사용하여 Amazon EC2로 마이그레이션을 리호스팅합니다.

Migration Portfolio Assessment(MPA)

AWS 클라우드로 마이그레이션하는 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다. MPA는 상세한 포트폴리오 평가(서버 적정 규모 조정, 가격 책정, TCO 비교, 마이그레이션 비용 분석)와 마이그레이션 계획(애플리케이션 데이터 분석 및 데이터 수집, 애플리케이션 그룹화, 마이그레이션 우선순위 지정, 웨이브 계획)을 제공합니다. MPA 도구(로그인 필요)는 모든 AWS 컨설턴트와 APN 파트너 컨설턴트가 무료로 사용할 수 있습니다.

마이그레이션 준비 상태 평가(MRA)

AWS CAF를 사용하여 조직의 클라우드 준비 상태에 대한 인사이트를 얻고, 강점과 약점을 식별하고, 식별된 격차를 해소하기 위한 행동 계획을 수립하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 가이드를 참조하십시오. MRA는 AWS 마이그레이션 전략의 첫 번째 단계입니다.

마이그레이션 전략

워크로드를 AWS 클라우드로 마이그레이션하는 데 사용되는 접근 방식입니다. 자세한 내용은 이 용어집의 7R 항목과 조직을 동원하여 대규모 마이그레이션 가속화를 참조하세요.

ML

기계 학습을 참조하세요.

현대화

비용을 절감하고 효율성을 높이고 혁신을 활용하기 위해 구식(레거시 또는 모놀리식) 애플리케이션과 해당 인프라를 클라우드의 민첩하고 탄력적이고 가용성이 높은 시스템으로 전환하는 것입니다. 자세한 내용은 AWS 클라우드에서 애플리케이션을 현대화하기 위한 전략을 참조하세요.

현대화 준비 상태 평가

조직 애플리케이션의 현대화 준비 상태를 파악하고, 이점, 위험 및 종속성을 식별하고, 조직이 해당 애플리케이션의 향후 상태를 얼마나 잘 지원할 수 있는지를 확인하는 데 도움이 되는 평가입니다. 평가 결과는 대상 아키텍처의 청사진, 현대화 프로세스의 개발 단계와 마일스톤을 자세히 설명하는 로드맵 및 파악된 격차를 해소하기 위한 실행 계획입니다. 자세한 내용은 AWS 클라우드에서 애플리케이션의 현대화 준비 상태 평가를 참조하세요.

모놀리식 애플리케이션(모놀리식 유형)

긴밀하게 연결된 프로세스를 사용하여 단일 서비스로 실행되는 애플리케이션입니다. 모놀리식 애플리케이션에는 몇 가지 단점이 있습니다. 한 애플리케이션 기능에 대한 수요가 급증하면 전체 아키텍처 규모를 조정해야 합니다. 코드 베이스가 커지면 모놀리식 애플리케이션의 기능을 추가하거나 개선하는 것도 더 복잡해집니다. 이러한 문제를 해결하기 위해 마이크로서비스 아키텍처를 사용할 수 있습니다. 자세한 내용은 마이크로서비스로 모놀리식 유형 분해를 참조하십시오.

MPA

Migration Portfolio Assessment를 참조하세요.

MQTT

메시지 큐 원격 분석 전송을 참조하세요.

멀티클래스 분류

여러 클래스에 대한 예측(2개 이상의 결과 중 하나 예측)을 생성하는 데 도움이 되는 프로세스입니다. 예를 들어, ML 모델이 '이 제품은 책인가요, 자동차인가요, 휴대폰인가요?' 또는 '이 고객이 가장 관심을 갖는 제품 범주는 무엇인가요?'라고 물을 수 있습니다.

변경 가능한 인프라

프로덕션 워크로드에 대한 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework에서는 변경 불가능한 인프라를 모범 사례로 사용할 것을 권장합니다.

O

OAC

오리진 액세스 제어를 참조하세요.

OAI

오리진 액세스 ID를 참조하세요.

OCM

조직 변경 관리를 참조하세요.

오프라인 마이그레이션

마이그레이션 프로세스 중 소스 워크로드가 중단되는 마이그레이션 방법입니다. 이 방법은 가동 중지 증가를 수반하며 일반적으로 작고 중요하지 않은 워크로드에 사용됩니다.

OI

운영 통합을 참조하세요.

OLA

운영 수준 계약을 참조하세요.

온라인 마이그레이션

소스 워크로드를 오프라인 상태로 전환하지 않고 대상 시스템에 복사하는 마이그레이션 방법입니다. 워크로드에 연결된 애플리케이션은 마이그레이션 중에도 계속 작동할 수 있습니다. 이 방법은 가동 중지 차단 또는 최소화를 수반하며 일반적으로 중요한 프로덕션 워크로드에 사용됩니다.

OPC-UA

Open Process Communications - Unified Architecture(OPC-UA)를 참조하세요.

Open Process Communications - Unified Architecture(OPC-UA)

산업 자동화를 위한 Machine-to-Machine(M2M) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계에 관한 상호 운용성 표준을 제공합니다.

운영 수준 협약(OLA)

서비스 수준에 관한 계약(SLA)을 지원하기 위해 직무 IT 그룹이 서로에게 제공하기로 약속한 내용을 명확히 하는 계약입니다.

운영 준비 상태 검토(ORR)

인시던트 및 잠재적 장애의 범위를 이해, 평가 또는 예방하거나 줄이는 데 도움이 되는 질문 체크리스트 및 관련 모범 사례입니다. 자세한 내용은 AWS Well-Architected Framework의 운영 준비 상태 검토(ORR)를 참조하세요.

운영 기술(OT)

물리적 환경에서 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조 분야에서 OT 및 정보 기술(IT) 시스템의 통합은 Industry 4.0 트랜스포메이션의 주요 중점 사항입니다.

운영 통합(OI)

클라우드에서 운영을 현대화하는 프로세스로 준비 계획, 자동화 및 통합을 수반합니다. 자세한 내용은 운영 통합 가이드를 참조하십시오.

조직 트레일

조직 AWS 계정 내 모든에 대한 모든 이벤트를 로깅 AWS CloudTrail 하는에서 생성된 추적입니다 AWS Organizations. 이 트레일은 조직에 속한 각 AWS 계정 에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 CloudTrail 설명서의 Creating a trail for an organization을 참조하십시오.

조직 변경 관리(OCM)

사람, 문화 및 리더십 관점에서 중대하고 파괴적인 비즈니스 혁신을 관리하기 위한 프레임워크입니다. OCM은 변화 채택을 가속화하고, 과도기적 문제를 해결하고, 문화 및 조직적 변화를 주도함으로써 조직이 새로운 시스템 및 전략을 준비하고 전환할 수 있도록 지원합니다. AWS 마이그레이션 전략에서는 클라우드 채택 프로젝트에 필요한 변경 속도 때문에이 프레임워크를 인력 가속화라고 합니다. 자세한 내용은 사용 가이드를 참조하십시오.

오리진 액세스 제어(OAC)

CloudFront에서 Amazon Simple Storage Service(S3) 콘텐츠를 보호하기 위해 액세스를 제한하는 고급 옵션입니다. OAC는 AWS KMS (SSE-KMS)를 사용한 모든 서버 측 암호화 AWS 리전와 S3 버킷에 대한 동적 PUT 및 DELETE 요청에서 모든 S3 버킷을 지원합니다.

오리진 액세스 ID(OAI)

CloudFront에서 Amazon S3 콘텐츠를 보호하기 위해 액세스를 제한하는 옵션입니다. OAI를 사용하면 CloudFront는 Amazon S3가 인증할 수 있는 보안 주체를 생성합니다. 인증된 보안 주체는 특

정 CloudFront 배포를 통해서만 S3 버킷의 콘텐츠에 액세스할 수 있습니다. 더 세분화되고 향상된 액세스 제어를 제공하는 OAC도 참조하십시오.

ORR

운영 준비 상태 검토를 참조하세요.

OT

운영 기술을 참조하세요.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작된 네트워크 연결을 처리하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

P

권한 경계

사용자나 역할이 가질 수 있는 최대 권한을 설정하기 위해 IAM 보안 주체에 연결되는 IAM 관리 정책입니다. 자세한 내용은 IAM 설명서의 권한 경계를 참조하십시오.

개인 식별 정보(PII)

직접 보거나 다른 관련 데이터와 함께 짝을 지을 때 개인의 신원을 합리적으로 추론하는 데 사용할 수 있는 정보입니다. PII의 예로는 이름, 주소, 연락처 정보 등이 있습니다.

PII

개인 식별 정보를 참조하세요.

플레이북

클라우드에서 핵심 운영 기능을 제공하는 등 마이그레이션과 관련된 작업을 캡처하는 일련의 사전 정의된 단계입니다. 플레이북은 스크립트, 자동화된 런북 또는 현대화된 환경을 운영하는 데 필요한 프로세스나 단계 요약의 형태를 취할 수 있습니다.

PLC

프로그래밍 가능 로직 컨트롤러를 참조하세요.

PLM

제품 수명 주기 관리를 참조하세요.

정책

권한 정의(ID 기반 정책 참조), 액세스 조건 지정(리소스 기반 정책 참조), AWS Organizations 내 조직의 모든 계정에 대한 최대 권한 정의(서비스 제어 정책 참조)와 같은 작업을 수행할 수 있는 객체입니다.

다국어 지속성

데이터 액세스 패턴 및 기타 요구 사항을 기반으로 독립적으로 마이크로서비스의 데이터 스토리지 기술 선택. 마이크로서비스가 동일한 데이터 스토리지 기술을 사용하는 경우 구현 문제가 발생하거나 성능이 저하될 수 있습니다. 요구 사항에 가장 적합한 데이터 저장소를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다.

포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 상태 평가를 참조하십시오.

조건자

보통 `WHERE` 절에 있는 `true` 또는 `false`를 반환하는 쿼리 조건입니다.

푸시다운 조건자

전송 전에 쿼리의 데이터를 필터링하는 데이터베이스 쿼리 최적화 기법입니다. 이렇게 하면 관계형 데이터베이스에서 검색하고 처리해야 하는 데이터의 양이 줄고 쿼리 성능이 향상됩니다.

예방적 제어

이벤트 발생을 방지하도록 설계된 보안 제어입니다. 이 제어는 네트워크에 대한 무단 액세스나 원치 않는 변경을 방지하는 데 도움이 되는 1차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 Preventative controls를 참조하십시오.

보안 주체

작업을 수행하고 리소스에 액세스할 수 AWS 있는의 엔터티입니다. 이 엔터티는 일반적으로 , AWS 계정 IAM 역할 또는 사용자의 루트 사용자입니다. 자세한 내용은 IAM 설명서의 역할 용어 및 개념의 보안 주체를 참조하십시오.

개인 정보 보호 중심 설계

전체 개발 프로세스에서 개인 정보를 고려하는 시스템 엔지니어링에서의 접근 방식입니다.

프라이빗 호스팅 영역

Amazon Route 53에서 하나 이상의 VPC 내 도메인과 하위 도메인에 대한 DNS 쿼리에 응답하는 방법에 대한 정보가 담긴 컨테이너입니다. 자세한 내용은 Route 53 설명서의 프라이빗 호스팅 영역 작업을 참조하십시오.

선제적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 보안 제어입니다. 이러한 제어는 리소스를 프로비저닝하기 전에 리소스를 스캔합니다. 리소스가 제어를 준수하지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 제어 참조 가이드를 참조하고 보안 제어 구현의 사전 예방적 제어를 참조하세요. AWS

제품 수명 주기 관리(PLM)

설계, 개발 및 출시부터 성장 및 성숙도를 거쳐 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리를 나타냅니다.

프로덕션 환경

환경을 참조하세요.

프로그래밍 가능 로직 컨트롤러(PLC)

제조 분야에서 기계를 모니터링하고 제조 프로세스를 자동화하는 매우 안정적이고 적응력이 뛰어난 컴퓨터입니다.

프롬프트 체이닝

한 LLM 프롬프트의 출력을 다음 프롬프트의 입력으로 사용하여 더 나은 응답을 생성합니다. 이 기법은 복잡한 태스크를 하위 태스크로 나누거나 예비 응답을 반복적으로 세부 조정하거나 확장하는 데 사용됩니다. 이를 통해 모델 응답의 정확성과 관련성을 개선하고 보다 세분화되고 개인화된 결과를 얻을 수 있습니다.

가명화

데이터세트의 개인 식별자를 자리 표시자 값으로 바꾸는 프로세스입니다. 가명화는 개인 정보를 보호하는 데 도움이 될 수 있습니다. 가명화된 데이터는 여전히 개인 데이터로 간주됩니다.

게시/구독(pub/sub)

여러 마이크로서비스에서 비동기 통신을 지원하여 확장성과 응답성을 개선하는 패턴입니다. 예를 들어 마이크로서비스 기반 MES에서 마이크로서비스는 다른 마이크로서비스가 구독할 수 있는 채널에 이벤트 메시지를 게시할 수 있습니다. 시스템은 게시 서비스를 변경하지 않고도 새 마이크로서비스를 추가할 수 있습니다.

Q

쿼리 계획

SQL 관계형 데이터베이스 시스템의 데이터에 액세스하는 데 사용되는 명령어와 같은 일련의 단계입니다.

쿼리 계획 회귀

데이터베이스 서비스 최적화 프로그램이 데이터베이스 환경을 변경하기 전보다 덜 최적의 계획을 선택하는 경우입니다. 통계, 제한 사항, 환경 설정, 쿼리 파라미터 바인딩 및 데이터베이스 엔진 업데이트의 변경으로 인해 발생할 수 있습니다.

R

RACI 매트릭스

Responsible, Accountable, Consulted, Informed(RACI)를 참조하세요.

RAG

검색 증강 생성을 참조하세요.

랜섬웨어

결제가 완료될 때까지 컴퓨터 시스템이나 데이터에 대한 액세스를 차단하도록 설계된 악성 소프트웨어입니다.

RASCI 매트릭스

Responsible, Accountable, Consulted, Informed(RACI)를 참조하세요.

RCAC

행 및 열 액세스 제어를 참조하세요.

읽기 전용 복제본

읽기 전용 용도로 사용되는 데이터베이스의 사본입니다. 쿼리를 읽기 전용 복제본으로 라우팅하여 기본 데이터베이스의 로드를 줄일 수 있습니다.

리아키텍팅

7R을 참조하세요.

Recovery Point Objective(RPO)

마지막 데이터 복구 시점 이후 허용되는 최대 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 사이에 허용되는 데이터 손실로 간주되는 범위가 결정됩니다.

Recovery Time Objective(RTO)

서비스 중단과 서비스 복원 사이의 허용 가능한 지연 시간입니다.

리팩터링

7R을 참조하세요.

리전

지리적 영역의 AWS 리소스 모음입니다. 각 AWS 리전 는 내결함성, 안정성 및 복원력을 제공하기 위해 서로 격리되고 독립적입니다. 자세한 내용은 계정에서 사용할 수 있는 AWS 리전 지정을 참조하세요.

회귀

숫자 값을 예측하는 ML 기법입니다. 예를 들어, '이 집은 얼마에 팔릴까?'라는 문제를 풀기 위해 ML 모델은 선형 회귀 모델을 사용하여 주택에 대해 알려진 사실(예: 면적)을 기반으로 주택의 매매 가격을 예측할 수 있습니다.

리호스팅

7R을 참조하세요.

릴리스

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

7R을 참조하세요.

리플랫포밍

7R을 참조하세요.

재구매

7R을 참조하세요.

복원력

중단에 저항하거나 중단을 복구할 수 있는 애플리케이션의 기능입니다. 고가용성 및 재해 복구는 AWS 클라우드에서 복원력을 계획할 때 일반적인 고려 사항입니다. 자세한 내용은 AWS 클라우드 복원력을 참조하세요.

리소스 기반 정책

Amazon S3 버킷, 엔드포인트, 암호화 키 등의 리소스에 연결된 정책입니다. 이 유형의 정책은 액세스가 허용된 보안 주체, 지원되는 작업 및 충족해야 하는 기타 조건을 지정합니다.

RACI(Responsible, Accountable, Consulted, Informed) 매트릭스

마이그레이션 활동 및 클라우드 운영에 참여하는 모든 당사자의 역할과 책임을 정의하는 매트릭스입니다. 매트릭스 이름은 매트릭스에 정의된 책임 유형에서 파생됩니다. 실무 담당자 (R), 의사 결정권자 (A), 업무 수행 조언자 (C), 결과 통보 대상자 (I). 지원자는 (S) 선택사항입니다. 지원자를 포함하면 매트릭스를 RASCI 매트릭스라고 하고, 지원자를 제외하면 RACI 매트릭스라고 합니다.

대응 제어

보안 기준에서 벗어나거나 부정적인 이벤트를 해결하도록 설계된 보안 제어입니다. 자세한 내용은 AWS에서 보안 제어 구현의 대응 제어를 참조하세요.

retain

7R을 참조하세요.

사용 중지

7R을 참조하세요.

검색 증강 세대(RAG)

응답을 생성하기 전에 LLM이 훈련 데이터 소스 외부에 있는 신뢰할 수 있는 데이터 소스를 참조하는 생성형 AI 기술입니다. 예를 들어 RAG 모델은 조직의 지식 기반 또는 사용자 지정 데이터에 대한 시맨틱 검색을 수행할 수 있습니다. 자세한 내용은 검색 증강 생성(RAG)이란 무엇인가요?를 참조하세요.

교체

공격자가 자격 증명에 액세스하는 것을 더욱 어렵게 만들기 위해 보안 암호를 주기적으로 업데이트하는 프로세스입니다.

행 및 열 액세스 제어(RCAC)

액세스 규칙이 정의된 기본적이고 유연한 SQL 표현식을 사용합니다. RCAC는 행 권한과 열 마스크로 구성됩니다.

RPO

목표 복구 시점(RPO)을 참조하세요.

RTO

목표 복구 시간(RTO)을 참조하세요.

런북

특정 작업을 수행하는 데 필요한 일련의 수동 또는 자동 절차입니다. 일반적으로 오류율이 높은 반복 작업이나 절차를 간소화하기 위해 런북을 만듭니다.

S

SAML 2.0

많은 ID 제공업체(idP)에서 사용하는 개방형 표준입니다. 이 기능을 사용하면 연동 SSO(Single Sign-On)를 AWS Management Console 사용할 수 있으므로 사용자는 조직의 모든 사용자에 대해 IAM에서 사용자를 생성하지 않고도에 로그인하거나 AWS API 작업을 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 SAML 2.0 기반 페더레이션 정보를 참조하십시오.

SCADA

감독 제어 및 데이터 획득을 참조하세요.

SCP

서비스 제어 정책을 참조하세요.

보안 암호

에는 암호화된 형식으로 저장하는 암호 또는 사용자 자격 증명과 같은 AWS Secrets Manager기밀 또는 제한된 정보가 있습니다. 보안 암호 값과 메타데이터로 구성됩니다. 보안 암호 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 AWS Secrets Manager 설명서의 Secrets Manager 보안 암호란 무엇인가요?를 참조하세요.

보안 중심 설계

전체 개발 프로세스에서 보안을 고려하는 시스템 엔지니어링에서의 접근 방식입니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어는 예방, 감지, 대응, 선제적과 같은 기본적인 네 가지 보안 제어 유형으로 구분됩니다.

보안 강화

공격 표면을 줄여 공격에 대한 저항력을 높이는 프로세스입니다. 더 이상 필요하지 않은 리소스 제거, 최소 권한 부여의 보안 모범 사례 구현, 구성 파일의 불필요한 기능 비활성화 등의 작업이 여기에 포함될 수 있습니다.

보안 정보 및 이벤트 관리(SIEM) 시스템

보안 정보 관리(SIM)와 보안 이벤트 관리(SEM) 시스템을 결합하는 도구 및 서비스입니다. SIEM 시스템은 서버, 네트워크, 디바이스 및 기타 소스에서 데이터를 수집, 모니터링 및 분석하여 위협과 보안 침해를 탐지하고 알림을 생성합니다.

보안 응답 자동화

보안 이벤트에 자동으로 응답하거나 이를 해결하도록 설계된 사전 정의되고 프로그래밍된 작업입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 탐지 또는 대응 AWS 보안 제어 역할을 합니다. 자동화된 응답 작업의 예로 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치 적용 또는 자격 증명 교체 등이 있습니다.

서버 측 암호화

대상에서 데이터를 수신하는 AWS 서비스 에 의한 데이터 암호화.

서비스 제어 정책(SCP)

AWS Organizations에 속한 조직의 모든 계정에 대한 권한을 중앙 집중식으로 제어하는 정책입니다. SCP는 관리자가 사용자 또는 역할에 위임할 수 있는 작업에 대해 제한을 설정하거나 가드레일을 정의합니다. SCP를 허용 목록 또는 거부 목록으로 사용하여 허용하거나 금지할 서비스 또는 작업을 지정할 수 있습니다. 자세한 내용은 AWS Organizations 설명서의 서비스 제어 정책을 참조하세요.

서비스 엔드포인트

에 대한 진입점의 URL입니다 AWS 서비스. 엔드포인트를 사용하여 대상 서비스에 프로그래밍 방식으로 연결할 수 있습니다. 자세한 내용은 AWS 일반 참조의 AWS 서비스 엔드포인트를 참조하십시오.

서비스 수준에 관한 계약(SLA)

IT 팀이 고객에게 제공하기로 약속한 내용(예: 서비스 가동 시간 및 성능)을 명시한 계약입니다.

서비스 수준 지표(SLI)

오류 발생률, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정값입니다.

서비스 수준 목표(SLO)

서비스 수준 지표로 측정되는 서비스의 상태를 나타내는 목표 지표입니다.

공동 책임 모델

클라우드 보안 및 규정 준수를 AWS 위해와 공유하는 책임을 설명하는 모델입니다. AWS 는 클라우드의 보안을 담당하는 반면, 사용자는 클라우드의 보안을 담당합니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

SIEM

보안 정보 및 이벤트 관리 시스템을 참조하세요.

단일 장애점(SPOF)

애플리케이션을 중단시킬 수 있는 애플리케이션의 중요한 단일 구성 요소에서 발생하는 장애입니다.

SLA

서비스 수준 계약을 참조하세요.

SLI

서비스 수준 지표를 참조하세요.

SLO

서비스 수준 목표를 참조하세요.

분할 앤 시드 모델

현대화 프로젝트를 확장하고 가속화하기 위한 패턴입니다. 새로운 기능과 제품 릴리스가 정의되면 핵심 팀이 분할되어 새로운 제품 팀이 만들어집니다. 이를 통해 조직의 역량과 서비스 규모를 조정하고, 개발자 생산성을 개선하고, 신속한 혁신을 지원할 수 있습니다. 자세한 내용은 AWS 클라우드에서 애플리케이션을 현대화하기 위한 단계별 접근 방식을 참조하세요.

SPOF

단일 장애점을 참조하세요.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 더 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 데이터 웨어하우스에서 또는 비즈니스 인텔리전스 목적으로 사용하도록 설계되었습니다.

Strangler Fig 패턴

레거시 시스템을 폐기할 수 있을 때까지 시스템 기능을 점진적으로 다시 작성하고 교체하여 모놀리식 시스템을 현대화하기 위한 접근 방식. 이 패턴은 무화과 덩굴이 나무로 자라 결국 숙주를 압도하고 대체하는 것과 비슷합니다. Martin Fowler가 모놀리식 시스템을 다시 작성할 때 위험을 관리하는 방법으로 이 패턴을 도입했습니다. 이 패턴을 적용하는 방법의 예는 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

서브넷

VPC의 IP 주소 범위입니다. 서브넷은 단일 가용 영역에 상주해야 합니다.

감독 제어 및 데이터 획득(SCADA)

제조 분야에서 하드웨어와 소프트웨어를 사용하여 물리적 자산과 프로덕션 작업을 모니터링하는 시스템입니다.

대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

합성 테스트

사용자 상호 작용을 시뮬레이션하여 잠재적 문제를 감지하거나 성능을 모니터링하는 방식으로 진행되는 시스템 테스트입니다. Amazon CloudWatch Synthetics를 사용하여 이러한 테스트를 생성할 수 있습니다.

시스템 프롬프트

LLM에 컨텍스트, 명령 또는 지침을 제공하여 동작을 지시하는 기법입니다. 시스템 프롬프트는 컨텍스트를 설정하고 사용자와의 상호 작용을 위한 규칙을 설정하는 데 도움이 됩니다.

T

tags

AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색, 필터링할 수 있습니다. 자세한 내용은 AWS 리소스에 태그 지정을 참조하십시오.

대상 변수

지도 ML에서 예측하려는 값으로, 결과 변수라고도 합니다. 예를 들어, 제조 설정에서 대상 변수는 제품 결함일 수 있습니다.

작업 목록

런북을 통해 진행 상황을 추적하는 데 사용되는 도구입니다. 작업 목록에는 런북의 개요와 완료해야 할 일반 작업 목록이 포함되어 있습니다. 각 일반 작업에 대한 예상 소요 시간, 소유자 및 진행 상황이 작업 목록에 포함됩니다.

테스트 환경

환경을 참조하세요.

훈련

ML 모델이 학습할 수 있는 데이터를 제공하는 것입니다. 훈련 데이터에는 정답이 포함되어야 합니다. 학습 알고리즘은 훈련 데이터에서 대상(예측하려는 답)에 입력 데이터 속성을 매핑하는 패턴을 찾고, 이러한 패턴을 캡처하는 ML 모델을 출력합니다. 그런 다음 ML 모델을 사용하여 대상을 모르는 새 데이터에 대한 예측을 할 수 있습니다.

Transit Gateway

VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 AWS Transit Gateway 설명서의 전송 게이트웨이란 무엇입니까?를 참조하세요.

트렁크 기반 워크플로

개발자가 기능 브랜치에서 로컬로 기능을 구축하고 테스트한 다음 해당 변경 사항을 기본 브랜치에 병합하는 접근 방식입니다. 이후 기본 브랜치는 개발, 프로덕션 이전 및 프로덕션 환경에 순차적으로 구축됩니다.

신뢰할 수 있는 액세스

사용자를 대신하여 AWS Organizations 및 해당 계정에서 조직에서 작업을 수행하도록 지정하는 서비스에 대한 권한 부여. 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여 관리 작업을 수행합니다. 자세한 내용은 설명서의 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하세요 AWS Organizations .

튜닝

ML 모델의 정확도를 높이기 위해 훈련 프로세스의 측면을 여러 변경하는 것입니다. 예를 들어, 레이블링 세트를 생성하고 레이블을 추가한 다음 다양한 설정에서 이러한 단계를 여러 번 반복하여 모델을 최적화하는 방식으로 ML 모델을 훈련할 수 있습니다.

피자 두 판 팀

피자 두 판이면 충분한 소규모 DevOps 팀. 피자 두 판 팀 규모는 소프트웨어 개발에 있어 가능한 최상의 공동 작업 기회를 보장합니다.

U

불확실성

예측 ML 모델의 신뢰성을 저해할 수 있는 부정확하거나 불완전하거나 알려지지 않은 정보를 나타내는 개념입니다. 불확실성에는 두 가지 유형이 있습니다. 인식론적 불확실성은 제한적이고 불완전한 데이터에 의해 발생하는 반면, 우연한 불확실성은 데이터에 내재된 노이즈와 무작위성에 의해 발생합니다. 자세한 내용은 Quantifying uncertainty in deep learning systems 가이드를 참조하십시오.

차별화되지 않은 작업

애플리케이션을 만들고 운영하는 데 필요하지만 최종 사용자에게 직접적인 가치를 제공하거나 경쟁 우위를 제공하지 못하는 작업을 헤비 리프팅이라고도 합니다. 차별화되지 않은 작업의 예로는 조달, 유지보수, 용량 계획 등이 있습니다.

상위 환경

환경을 참조하세요.

V

정리

스토리지를 회수하고 성능을 향상시키기 위해 증분 업데이트 후 정리 작업을 수반하는 데이터베이스 유지 관리 작업입니다.

버전 제어

리포지토리의 소스 코드 변경과 같은 변경 사항을 추적하는 프로세스 및 도구입니다.

VPC 피어링

프라이빗 IP 주소를 사용하여 트래픽을 라우팅할 수 있게 하는 두 VPC 간의 연결입니다. 자세한 내용은 Amazon VPC 설명서의 VPC 피어링이란?을 참조하십시오.

취약성

시스템 보안을 손상시키는 소프트웨어 또는 하드웨어 결함입니다.

W

웜 캐시

자주 액세스하는 최신 관련 데이터를 포함하는 버퍼 캐시입니다. 버퍼 캐시에서 데이터베이스 인스턴스를 읽을 수 있기 때문에 주 메모리나 디스크에서 읽는 것보다 빠릅니다.

웜 데이터

자주 액세스하지 않는 데이터입니다. 이런 종류의 데이터를 쿼리할 때는 일반적으로 적절히 느린 쿼리가 허용됩니다.

창 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에서 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대적 위치를 기반으로 행 값에 액세스하는 등의 태스크를 처리하는 데 유용합니다.

워크로드

고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음입니다.

워크스트림

마이그레이션 프로젝트에서 특정 작업 세트를 담당하는 직무 그룹입니다. 각 워크스트림은 독립적이지만 프로젝트의 다른 워크스트림을 지원합니다. 예를 들어, 포트폴리오 워크스트림은 애플리케이션 우선순위 지정, 웨이브 계획, 마이그레이션 메타데이터 수집을 담당합니다. 포트폴리오 워크스트림은 이러한 자산을 마이그레이션 워크스트림에 전달하고, 마이그레이션 워크스트림은 서버와 애플리케이션을 마이그레이션합니다.

WORM

Write Once, Read Many(WORM)를 참조하세요.

WQF

AWS Workload Qualification Framework를 참조하세요.

Write Once Read Many(WORM)

데이터를 한 번 쓰고 데이터가 삭제되거나 수정되지 않도록 하는 스토리지 모델입니다. 권한 있는 사용자는 필요한 만큼 여러 번 데이터를 읽을 수 있지만 데이터를 변경할 수는 없습니다. 이 데이터 스토리지 인프라는 변경 불가능한 항목으로 간주됩니다.

Z

제로데이 익스플로잇

제로데이 취약성을 악용하는 공격(일반적으로 맬웨어)입니다.

제로데이 취약성

프로덕션 시스템의 명백한 결함 또는 취약성입니다. 위협 행위자는 이러한 유형의 취약성을 사용하여 시스템을 공격할 수 있습니다. 개발자는 공격의 결과로 취약성을 인지하는 경우가 많습니다.

제로샷 프롬프팅

태스크를 수행하기 위해 LLM에 명령을 제공하지만 안내에 도움이 되는 예제(샷)는 제공하지 않습니다. LLM은 사전 훈련된 지식을 사용하여 태스크를 처리해야 합니다. 제로샷 프롬프팅의 효과는 태스크의 복잡성과 프롬프트의 품질에 따라 달라집니다. 퓨샷 프롬프팅도 참조하세요.

좀비 애플리케이션

평균 CPU 및 메모리 사용량이 5% 미만인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하는 것이 일반적입니다.

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