AWS 결정 가이드

AWS 보안, 자격 증명 및 거버넌스 서비스 선택

AWS 보안, 자격 증명 및 거버넌스 서비스 선택: AWS 결정 가이드

Table of Contents

AWS 보안, 자격 증명 및 거버넌스 서비스 선택

첫 번째 단계 수행

읽기 시간	27분	
용도	조직에 가장 적합한 AWS 보안, 자격 증명 및 거버넌스 서비스를 결정하는 데 도움이 됩니다.	
최종 업데이트 날짜	2024년 12월 30일	
적용되는 서비스	• AWS Artifact • AWS Audit Manager • AWS Certificate Manager • AWS CloudHSM • AWS CloudTrail • Amazon Cognito • AWS Config • AWS Control Tower • Amazon Detective • AWS Firewall Manager • Amazon GuardDuty • AWS IAM • AWS IAM Identity Center • Amazon Inspector	• AWS KMS • Amazon Macie • AWS Network Firewall • AWS Organizations • AWS Payment Cryptography • AWS Private CA • AWS RAM • AWS Secrets Manager • AWS Security Hub • Amazon Security Lake • AWS 보안 인시던트 대응 • AWS Shield • AWS WAF

소개

클라우드의 보안, 자격 증명 및 거버넌스는 데이터 및 서비스의 무결성과 안전을 달성하고 유지하는 데 중요한 구성 요소입니다. 이는 특히 더 많은 기업이 Amazon Web Services()와 같은 클라우드 제공업체로 마이그레이션할 때 관련이 있습니다AWS.

이 가이드는 요구 사항과 조직에 가장 적합한 AWS 보안, 자격 증명 및 거버넌스 서비스와 도구를 선택하는 데 도움이 됩니다.

먼저 보안, 자격 증명 및 거버넌스의 의미를 살펴보겠습니다.

- 클라우드 보안은 조치와 관행을 사용하여 위협으로부터 디지털 자산을 보호하는 것을 말합니다. 여기에는 데이터 센터의 물리적 보안과 온라인 위협으로부터 보호하기 위한 사이버 보안 조치가 모두 포함됩니다.는 암호화된 데이터 스토리지, 네트워크 보안 및 잠재적 위협의 지속적인 모니터링을 통해 보안을 AWS 우선시합니다.
- 자격 증명 서비스는 확장 가능한 방식으로 자격 증명, 리소스 및 권한을 안전하게 관리하는 데 도움이 됩니다.는 작업 인력 및 고객 대면 애플리케이션과 워크로드 및 애플리케이션에 대한 액세스 관리를 위해 설계된 자격 증명 서비스를 AWS 제공합니다.
- 클라우드 거버넌스는 조직이 모범 사례를 따르도록 안내하는 규칙, 프로세스 및 보고서 세트입니다. AWS 리소스 전반에 클라우드 거버넌스를 설정하고, 기본 제공 모범 사례 및 표준을 사용하고, 규정 준수 및 감사 프로세스를 자동화할 수 있습니다. 클라우드에서의 규정 준수란 데이터 보호 및 개인 정보 보호에 관한 법률과 규정을 준수하는 것을 말합니다. AWS 규정 준수 프로그램은와 일치하는 AWS 인증, 규정 및 프레임워크에 대한 정보를 제공합니다.

이 one-and-a-half분짜리 비디오는가 코어에서 강력한 보안을 AWS 구축하는 방법을 요약합니다.

AWS 보안, 자격 증명 및 거버넌스 서비스 이해

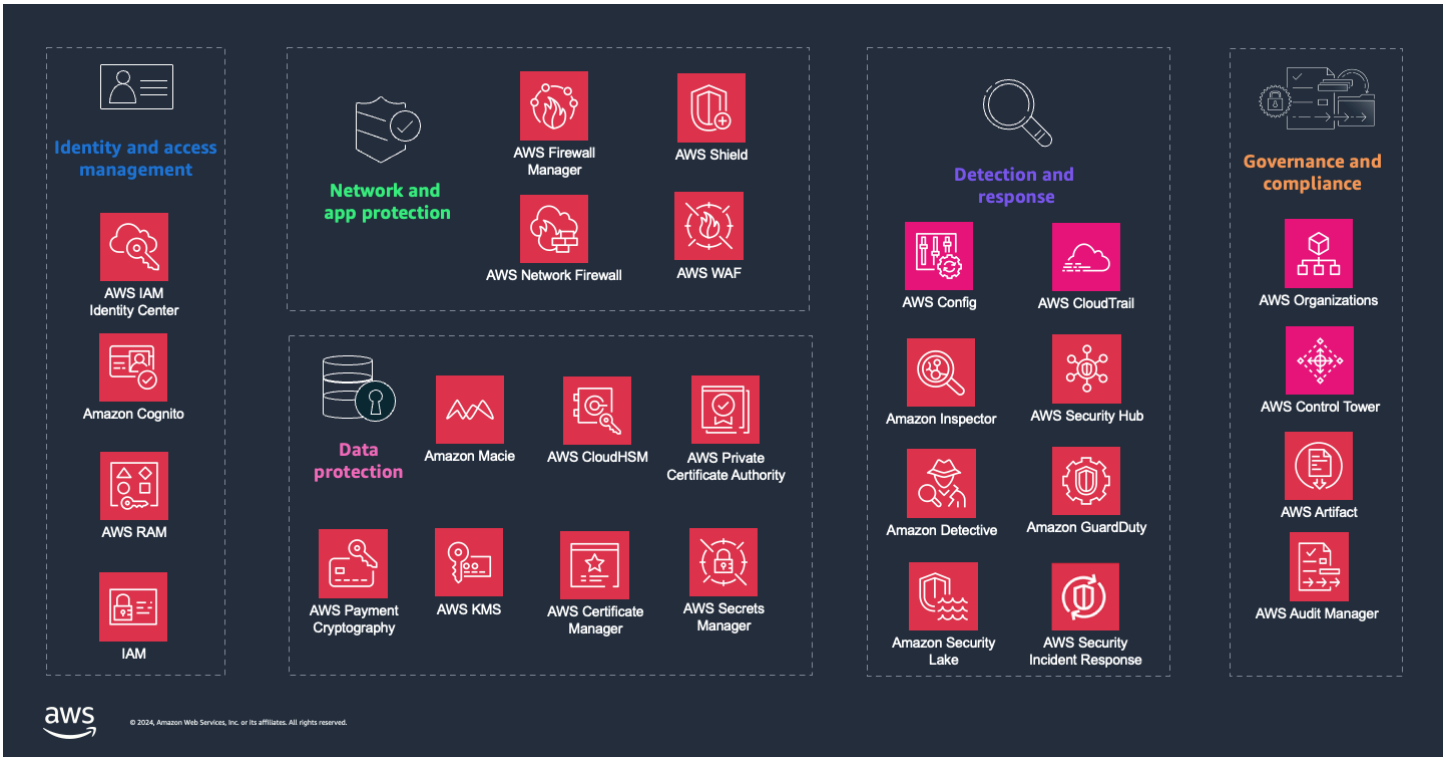
보안 및 규정 준수는 공동의 책임입니다.

AWS 보안, 자격 증명 및 거버넌스 서비스를 선택하기 전에 보안 및 규정 준수가 사용자와 간의 공동 책임임을 이해하는 것이 중요합니다 AWS.

이 공동 책임의 특성은 운영 부담을 줄이는 데 도움이 되며 배포에 대한 유연성과 제어를 제공합니다. 이러한 책임의 차별화를 일반적으로 클라우드의 보안 "of"와 클라우드의 보안 "in"이라고 합니다.

이 모델을 이해하면 사용 가능한 옵션 범위와 해당가 어떻게 AWS 서비스 일치하는지 이해할 수 있습니다.

AWS 도구와 서비스를 결합하여 워크로드를 보호할 수 있습니다.



이전 다이어그램에서 볼 수 있듯이는 클라우드에서 강력한 보안, 자격 증명 관리 및 거버넌스를 달성하고 유지하는 데 도움이 되는 5개 도메인의 도구와 서비스를 AWS 제공합니다. 이 5개 도메인 AWS 서비스 에서를 사용하여 다음을 수행할 수 있습니다.

- 데이터 및 환경을 보호하기 위한 다중 접근 방식 형성
- 진화하는 위협으로부터 클라우드 인프라 강화
- 엄격한 규제 표준 준수

AWS 보안 설명서를 포함하여 보안에 대한 자세한 내용은 AWS 보안 설명서를 AWS 서비스참조하세요.

다음 섹션에서는 각 도메인을 자세히 살펴봅니다.

AWS 자격 증명 및 액세스 관리 서비스 이해

AWS 보안의 핵심은 최소 권한의 원칙입니다. 개인과 서비스는 필요한 액세스 권한만 가집니다. AWS IAM Identity Center는 AWS 리소스에 AWS 서비스 대한 사용자 액세스를 관리하는 데 권장됩니다. 이 서비스를 사용하여 외부 자격 증명 공급자의 자격 증명을 포함하여 해당 계정 내의 계정 및 권한에 대한 액세스를 관리할 수 있습니다.

다음 표에는이 가이드에서 설명하는 자격 증명 및 액세스 관리 상품이 요약되어 있습니다.

AWS IAM Identity Center

AWS IAM Identity Center를 사용하면 자격 증명 소스를 연결하거나 사용자를 생성할 수 있습니다. 여러 AWS 계정 및 애플리케이션에 대한 인력 액세스를 중앙에서 관리할 수 있습니다.

Amazon Cognito

Amazon Cognito는 웹 및 모바일 앱이 기본 제공 사용자 디렉터리, 엔터프라이즈 디렉터리 및 소비자 자격 증명 공급자의 사용자를 인증하고 권한을 부여할 수 있는 자격 증명 도구를 제공합니다.

AWS RAM

AWS RAM를 사용하면 조직 전체 AWS 계정, 조직 내, IAM 역할 및 사용자와 리소스를 안전하게 공유할 수 있습니다.

IAM

IAM을 사용하면 AWS 워크로드 리소스에 대한 액세스를 안전하고 세분화된 제어가 가능합니다.

AWS 데이터 보호 서비스 이해

데이터 보호는 클라우드에서 매우 중요하며 데이터, 계정 및 워크로드를 보호하는 데 도움이 되는 서비스를 AWS 제공합니다. 예를 들어 전송 중 데이터와 저장 중 데이터를 모두 암호화하면 노출로부터 데이터를 보호하는 데 도움이 됩니다. AWS Key Management Service (AWS KMS) 및를 사용하면 데이터를 보호하는 데 사용하는 암호화 키를 생성하고 제어할 AWS CloudHSM 수 있습니다.

다음 표에는이 가이드에서 설명하는 데이터 보호 상품이 요약되어 있습니다.

Amazon Macie

Amazon Macie는 기계 학습 및 패턴 일치를 사용하여 민감한 데이터를 검색하고 관련 위험으로부터 자동으로 보호할 수 있습니다.

AWS KMS

AWS KMS는 데이터를 보호하는 데 사용하는 암호화 키를 생성하고 제어합니다.

AWS CloudHSM

AWS CloudHSM는 가용성이 높은 클라우드 기반 하드웨어 보안 모듈(HSMs 제공합니다.

AWS Certificate Manager

AWS Certificate Manager는 퍼블릭 및 프라이빗 SSL/TLS X.509 인증서와 키를 생성, 저장 및 갱신하는 복잡성을 처리합니다.

AWS Private CA

AWS Private CA를 사용하면 루트 및 하위 인증 기관(CAs.

AWS Secrets Manager

AWS Secrets Manager는 데이터베이스 자격 증명, 애플리케이션 자격 증명, OAuth 토큰, API 키 및 기타 보안 암호를 관리, 검색 및 교체하는 데 도움이 됩니다.

AWS Payment Cryptography

AWS Payment Cryptography는 결제 카드 산업(PCI) 표준에 따라 결제 처리에 사용되는 암호화 함수 및 키 관리에 대한 액세스를 제공합니다.

AWS 네트워크 및 애플리케이션 보호 서비스 이해

AWS 는 네트워크와 애플리케이션을 보호하기 위한 여러 서비스를 제공합니다. AWS Shield는 분산 서비스 거부(DDoS) 공격으로부터 보호하고 일반적인 웹 악용 공격으로부터 웹 애플리케이션을 보호하는 AWS WAF 데 도움이 됩니다.

다음 표에는이 안내서에서 설명하는 네트워크 및 애플리케이션 보호 상품이 요약되어 있습니다.

AWS Firewall Manager

AWS Firewall Manager는 보호를 위해 여러 계정 및 리소스에서 관리 및 유지 관리 작업을 간소화합니다.

AWS Network Firewall

AWS Network Firewall는 VPC와 함께 상태 저장 관리형 네트워크 방화벽 및 침입 탐지 및 방지 서비스를 제공합니다.

AWS Shield

AWS Shield는 네트워크, 전송 및 애플리케이션 계층의 AWS 리소스에 대한 DDoS 공격으로부터 보호합니다.

AWS WAF

AWS WAF는 보호된 웹 애플리케이션 리소스로 전달되는 HTTP(S) 요청을 모니터링할 수 있도록 웹 애플리케이션 방화벽을 제공합니다.

AWS 탐지 및 대응 서비스 이해

AWS 는 다중 계정 환경을 포함하여 환경 전반의 보안 작업을 간소화하는 데 도움이 AWS 되는 도구를 제공합니다. 예를 들어 지능형 위협 탐지에 Amazon GuardDuty를 사용할 수 있으며 Amazon Detective를 사용하여 로그 데이터를 수집하여 보안 결과를 식별하고 분석할 수 있습니다.는 여러 보안 표준을 AWS Security Hub 지원하고 보안 알림 및 규정 준수 상태에 대한 개요를 제공합니다 AWS 계정.는 보안 이벤트를 이해하고 대응하는 데 중요한 사용자 활동 및 애플리케이션 프로그래밍 인터페이스(API) 사용을 AWS CloudTrail 추적합니다.

다음 표에는이 가이드에서 설명하는 탐지 및 대응 상품이 요약되어 있습니다.

AWS Config

AWS Config는의 AWS 리소스 구성에 대한 자세한 보기를 제공합니다 AWS 계정.

AWS CloudTrail

AWS CloudTrail는 사용자, 역할 또는가 수행한 작업을 기록합니다 AWS 서비스.

AWS Security Hub

AWS Security Hub는의 보안 상태에 대한 포괄적인 보기를 제공합니다 AWS.

Amazon GuardDuty

Amazon GuardDuty는 사용자 AWS 계정, 워크로드, 런타임 활동 및 데이터에 악의적인 활동이 있는지 지속적으로 모니터링합니다.

Amazon Inspector

Amazon Inspector는 AWS 워크로드에서 소프트웨어 취약성 및 의도하지 않은 네트워크 노출을 검사합니다.

Amazon Security Lake

Amazon Security Lake는 AWS 환경, SaaS 공급자, 온프레미스 환경, 클라우드 소스 및 타사 소스의 보안 데이터를 데이터 레이크로 자동으로 중앙 집중화합니다.

Amazon Detective

Amazon Detective는 사용자가 보안 조사 결과 또는 의심스러운 활동의 근본 원인을 분석 및 조사하고 신속하게 식별하는 데 도움이 됩니다.

AWS Security Incident Response

AWS 보안 인시던트 대응

보안 인시던트를 복구하는 데 도움이 되는 지침을 신속하게 준비, 대응 및 받을 수 있습니다.

AWS 거버넌스 및 규정 준수 서비스 이해

AWS 는 보안, 운영, 규정 준수 및 비용 표준을 준수하는 데 도움이 되는 도구를 제공합니다. 예를 들어 AWS Control Tower를 사용하여 규범적 제어를 통해 다중 계정 환경을 설정하고 관리할 수 있습니다. 를 사용하면 조직 내 여러 계정에 대한 정책 기반 관리를 설정할 AWS Organizations수 있습니다.

AWS 또한는 규정 준수 상태를 포괄적으로 파악하고 조직이 따르는 AWS 모범 사례 및 업계 표준에 따라 자동화된 규정 준수 검사를 사용하여 환경을 지속적으로 모니터링합니다. 예를 들어 AWS Artifact는 규정 준수 보고서에 대한 온디맨드 액세스를 제공하고 증거 수집을 AWS Audit Manager 자동화하여 제어가 효과적으로 작동하는지 보다 쉽게 평가할 수 있습니다.

다음 표에는이 가이드에서 설명하는 거버넌스 및 규정 준수 상품이 요약되어 있습니다.

AWS Organizations

AWS Organizations를 사용하면 여러을 생성하고 중앙에서 관리하는 조직 AWS 계정 으로 통합할 수 있습니다.

AWS Control Tower

AWS Control Tower는 모범 사례를 기반으로 하는 AWS 다중 계정 환경을 설정하고 관리하는 데 도움이 됩니다.

AWS Artifact

AWS Artifact는 AWS 보안 및 규정 준수 문서의 온디맨드 다운로드를 제공합니다.

AWS Audit Manager

AWS Audit Manager

AWS 사용량을 지속적으로 감사하여 위험 및 규정 준수를 평가하는 방법을 간소화할 수 있습니다.

AWS 보안, 자격 증명 및 거버넌스 기준 고려

에서 올바른 보안, 자격 증명 및 거버넌스 서비스를 선택하는 것은 특정 요구 사항 및 사용 사례에 AWS 따라 달라집니다. AWS 보안 서비스를 채택하기로 결정하면 보안, 자격 증명 및 거버넌스 AWS 서비스 채택이 조직에 적합한지 결정하는 데 도움이 되는 의사 결정 트리가 제공됩니다. 또한 사용할 서비스에 대해 결정할 때 고려해야 할 몇 가지 기준이 있습니다.

Security requirements and threat landscape

조직의 특정 취약성 및 위협에 대한 포괄적인 평가를 수행합니다. 여기에는 개인 고객 정보, 재무 기록 또는 독점 비즈니스 데이터와 같이 처리하는 데이터 유형을 식별하는 작업이 포함됩니다. 각각과 관련된 잠재적 위험을 이해합니다.

애플리케이션 및 인프라 아키텍처를 평가합니다. 애플리케이션이 퍼블릭인지 여부와 애플리케이션이 처리하는 웹 트래픽의 종류를 결정합니다. 이는 웹 악용으로부터 AWS WAF 보호하기 위한와 같은 서비스의 필요성에 영향을 미칩니다. 내부 애플리케이션의 경우 비정상적인 액세스 패턴 또는 무단 배포를 식별할 수 있는 Amazon GuardDuty를 사용한 내부 위협 탐지 및 지속적인 모니터링의 중요성을 고려합니다.

마지막으로 기존 보안 태세의 정교함과 보안 팀의 전문 지식을 고려합니다. 팀에 리소스가 제한된 경우 더 많은 자동화 및 통합을 제공하는 서비스를 선택하면 팀에 부담을 주지 않고 효과적인 보안 강화를 제공할 수 있습니다. 서비스 예에는 AWS Shield DDoS 보호 및 중앙 집중식 보안 모니터링 AWS Security Hub 이 포함됩니다.

Compliance and regulatory requirements

일반 데이터 보호 규정(GDPR), 미국 HIPAA(Health Insurance Portability and Accountability Act of 1996) 또는 PCI DSS(Payment Card Industry Data Security Standard)와 같은 업계 또는 지리적 리전의 관련 법률과 표준을 식별합니다.

AWS 는 다양한 표준 준수를 관리하는 데 도움이 되는 AWS Config 및 AWS 아티팩트와 같은 서비스를 제공합니다. AWS Config를 사용하면 AWS 리소스 구성을 평가, 감사 및 평가할 수 있으므로 내부 정책 및 규제 요구 사항을 더 쉽게 준수할 수 있습니다. AWS Artifact는 AWS 규정 준수 문서에 대한 온디맨드 액세스를 제공하여 감사 및 규정 준수 보고를 지원합니다.

특정 규정 준수 요구 사항에 맞는 서비스를 선택하면 조직이 법적 요구 사항을 충족하고 데이터에 대한 안전하고 신뢰할 수 있는 환경을 구축하는 데 도움이 될 수 있습니다. 자세한 내용은 AWS 규정 준수 프로그램을 참조하세요.

Scalability and flexibility

조직의 성장 방식과 속도를 고려합니다. 보안 조치가 인프라에 따라 원활하게 확장되고 진화 AWS 서비스 하는 위협에 적응하는 데 도움이 되도록 선택합니다.

빠르게 확장할 수 있도록는 AWS Organizations 및 AWS IAM Identity Center를 AWS 서비스비롯한 다른 여러의 기능을 AWS Control Tower 조정하여 1시간 이내에 랜딩 존을 구축합니다. Control Tower는 사용자를 대신하여 리소스를 설정하고 관리합니다.

AWS 또한는 위협 탐지 및 웹 애플리케이션 보호를 위해 Amazon GuardDuty와 같은 애플리케이션의 트래픽 및 사용 패턴 AWS WAF 에 따라 자동으로 확장할 수 있는 많은 서비스를 설계합니다. 비즈니스가 확장되면 이러한 서비스는 수동 조정이나 병목 현상 없이 확장됩니다.

또한 비즈니스 요구 사항 및 위협 환경에 맞게 보안 제어를 사용자 지정할 수 있어야 합니다. 여러 계정에서 40개 이상의 서비스 리소스를 관리할 수 AWS Organizations있도록를 사용하여 계정을 관리하는 것이 좋습니다. 이를 통해 개별 애플리케이션 팀은 워크로드와 관련된 보안 요구 사항을 관리할 수 있는 유연성과 가시성을 확보하고 중앙 집중식 보안 팀에 거버넌스와 가시성을 제공할 수 있습니다.

확장성과 유연성을 고려하면 보안 태세가 견고하고 응답성이 뛰어나며 동적 비즈니스 환경을 지원할 수 있는지 확인할 수 있습니다.

Integration with existing systems

현재 작업을 중단하지 않고 개선하는 보안 조치를 고려합니다. 예를 들어 다음을 고려합니다.

- 에서 보안 데이터와 알림을 집계하고 기존 보안 정보 AWS 서비스 및 이벤트 관리(SIEM) 시스템과 함께 분석하여 워크플로를 간소화합니다.
- AWS 및 온프레미스 환경 모두에서 보안 위협 및 취약성에 대한 통합 보기를 생성합니다.
- AWS CloudTrail 를 기존 로그 관리 솔루션과 통합하여 AWS 인프라 및 기존 애플리케이션 전반의 사용자 활동 및 API 사용량을 포괄적으로 모니터링합니다.
- 리소스 사용률을 최적화하고 환경 전체에 보안 정책을 일관되게 적용할 수 있는 방법을 살펴봅니다. 이를 통해 보안 적용 범위의 격차 위험을 줄일 수 있습니다.

Cost and budget considerations

고려 중인 각 서비스의 요금 모델을 검토합니다. AWS API 호출 수, 처리된 데이터 양 또는 저장된 데이터 양과 같은 사용량에 따라 요금이 부과되는 경우가 많습니다. 예를 들어 Amazon GuardDuty는 위협 탐지를 위해 분석된 로그 데이터의 양을 기준으로 요금을 부과하는 반면 AWS WAF , 청구서는 배포된 규칙 수와 수신된 웹 요청 수를 기준으로 합니다.

예상 사용량을 예측하여 비용을 정확하게 예측합니다. 현재 요구 사항과 수요의 잠재적 증가 또는 급증을 모두 고려합니다. 예를 들어 확장성은의 주요 기능 AWS 서비스이지만 신중하게 관리하지 않으면 비용이 증가할 수도 있습니다. 를 사용하여 다양한 시나리오AWS Pricing Calculator를 모델링하고 해당 시나리오가 재무에 미치는 영향을 평가합니다.

관리 및 유지 관리에 필요한 시간 및 리소스와 같은 간접 비용과 직접 비용을 모두 포함하는 총 소유 비용(TCO)을 평가합니다. 관리형 서비스를 선택하면 운영 오버헤드를 줄일 수 있지만 가격이 높아질 수 있습니다.

마지막으로 위험 평가를 기반으로 보안 투자를 우선시합니다. 모든 보안 서비스가 인프라에 동일하게 중요한 것은 아니므로 위험을 줄이고 규정 준수를 보장하는 데 가장 중요한 영향을 미칠 영역에 예산을 집중하세요. 비용 효율성과 필요한 보안 수준의 균형을 맞추는 것이 성공적인 AWS 보안 전략의 핵심입니다.

Organizational structure and access needs

조직의 구조 및 운영 방식과 팀, 프로젝트 또는 위치에 따라 액세스 요구 사항이 어떻게 달라질 수 있는지 평가합니다. 이는 사용자 ID를 관리 및 인증하고, 역할을 할당하고, 환경 전체에서 액세스 제어를 적용하는 방법에 영향을 미칩니다 AWS . 최소 권한 적용 및 다중 인증(MFA) 요구와 같은 모범 사례를 구현합니다.

대부분의 조직은 다중 계정 환경이 필요합니다. 이러한 유형의 환경에 대한 모범 사례를 검토하고 및를 사용하여 구현 AWS Organizations AWS Control Tower 하는 것이 좋습니다.

고려해야 할 또 다른 측면은 자격 증명 및 액세스 키 관리입니다. IAM Identity Center를 사용하여 여러 AWS 계정 및 비즈니스 애플리케이션에서 액세스 관리를 중앙 집중화하면 보안과 사용자 편의성이 모두 향상됩니다. 조직의 계정 전체에서 액세스를 원활하게 관리하는 데 도움이 되도록 IAM Identity Center는와 통합됩니다 AWS Organizations.

또한 이러한 ID 및 액세스 관리 서비스가 기존 디렉터리 서비스와 통합되는 방식을 평가합니다. 기존 자격 증명 공급자가 있는 경우 SAML 2.0 또는 OpenID Connect(OIDC)를 사용하여 IAM Identity Center와 통합할 수 있습니다. 또한 IAM Identity Center는 디렉터리를 동기화된 상태로 유지하는 데 도움이 되는 SCIM(System for Cross-domain Identity Management) 프로비저닝을 지원합니다. 이렇게 하면 AWS 리소스에 액세스하는 동안 원활하고 안전한 사용자 환경을 보장할 수 있습니다.

AWS 보안, 자격 증명 및 거버넌스 서비스 선택

이제 보안 옵션 평가 기준을 알았으므로 조직 요구 사항에 적합한 AWS 보안 서비스를 선택할 준비가 되었습니다.

다음 표에서는 어떤 서비스가 어떤 상황에 최적화되어 있는지를 강조합니다. 테이블을 사용하여 조직 및 사용 사례에 가장 적합한 서비스를 결정할 수 있습니다.

Note

[1]와 통합 AWS Security Hub (전체 목록)
[2] Amazon GuardDuty와 통합(전체 목록)
[3] Amazon Security Lake와 통합(전체 목록)

AWS 자격 증명 및 액세스 관리 서비스 선택

적절한 개인에게 시스템, 애플리케이션 및 데이터에 대한 적절한 수준의 액세스 권한을 부여합니다.

언제 사용해야 하나요?	무엇에 최적화되어 있나요?	보안, 자격 증명 및 거버넌스 서비스
이러한 서비스를 사용하면 고객, 작업 인력 및 워크로드에 대한 액세스를 안전하게 관리하고 관리하는 데 도움이 됩니다.	자격 증명 소스를 연결하거나 사용자를 생성하는 데 도움이 됩니다. 여러 AWS 계정 및 애플리케이션에 대한 인력 액세스를 중앙에서 관리할 수 있습니다.	AWS IAM Identity Center
	웹 및 모바일 애플리케이션 사용자를 인증하고 권한을 부여하는 데 최적화되었습니다.	Amazon Cognito
	내에서 리소스를 안전하게 공유하도록 최적화되었습니다 AWS.	AWS RAM
	AWS 워크로드 리소스에 대한 액세스를 안전하고 세분화된 제어가 가능합니다.	IAM [1]

AWS 데이터 보호 서비스 선택

키 관리 및 민감한 데이터 검색부터 자격 증명 관리에 이르기까지 다양한 데이터 보호 및 보안 작업을 자동화하고 간소화합니다.

언제 사용해야 하나요?	무엇에 최적화되어 있나요?	데이터 보호 서비스
이러한 서비스를 사용하면 AWS 환경 내에 저장되고 처리되는 민감한 데이터의 기밀성, 무결성 및 가용성을 달성하고 유지하는 데 도움이 됩니다.	민감한 데이터를 검색하는 데 최적화되었습니다.	Amazon Macie [1]
	암호화 키에 최적화되었습니다.	AWS KMS
	HSMs.	AWS CloudHSM
	프라이빗 SSL/TLS X.509 인증서 및 키에 최적화되었습니다.	AWS Certificate Manager
	프라이빗 인증 기관 계층 구조 생성에 최적화되었습니다.	AWS Private CA
	데이터베이스 자격 증명, 애플리케이션 자격 증명, OAuth 토큰, API 키 및 기타 보안 암호에 최적화되었습니다.	AWS Secrets Manager
	PCI 표준에 따라 결제 처리에 사용되는 암호화 함수 및 키 관리에 대한 액세스를 제공하도록 최적화되었습니다.	AWS Payment Cryptography

AWS 네트워크 및 애플리케이션 보호 서비스 선택

일반적인 DDoS 및 애플리케이션 공격으로부터 인터넷 리소스를 중앙에서 보호합니다.

언제 사용해야 하나요?	무엇에 최적화되어 있나요?	네트워크 및 애플리케이션 보호 서비스
이러한 서비스를 사용하면 모든 네트워크 제어 지점에서 세부 보안 정책을 적용하는 데 도움이 됩니다.	방화벽 규칙을 중앙에서 구성하고 관리하는 데 최적화되었습니다.	AWS Firewall Manager [1]

언제 사용해야 하나요?	무엇에 최적화되어 있나요?	네트워크 및 애플리케이션 보호 서비스
	상태 저장 관리형 네트워크 방화벽과 침입 탐지 및 방지 서비스를 제공하는 데 최적화되었습니다.	AWS Network Firewall
	네트워크, 전송 및 애플리케이션 계층의 AWS 리소스에 대한 DDoS 공격으로부터 보호하는 데 최적화되었습니다.	AWS Shield
	웹 애플리케이션 방화벽을 제공하는 데 최적화되었습니다.	AWS WAF

AWS 탐지 및 대응 서비스 선택

보안 모범 사례를 조기에 통합하면서 보안 위험을 지속적으로 식별하고 우선순위를 지정합니다.

언제 사용해야 하나요?	무엇에 최적화되어 있나요?	탐지 및 대응 서비스
이러한 서비스를 사용하면 계정 전반의 보안 위험을 감지하고 이에 대응할 수 있으므로 워크로드를 대규모로 보호할 수 있습니다.	보안 검사를 자동화하고 AWS 및 타사 통합을 통해 보안 알림을 중앙 집중화하는 데 최적화되었습니다.	AWS Security Hub [2, 3]
	리소스 구성을 평가, 감사 및 평가하는 데 최적화되었습니다.	AWS Config [1]
	다른의 이벤트를 감사 추적 AWS 서비스 으로 로깅하도록 최적화되었습니다.	AWS CloudTrail
	지능형 위협 탐지 및 세부 보고에 최적화되었습니다.	Amazon GuardDuty [1]

언제 사용해야 하나요?	무엇에 최적화되어 있나요?	탐지 및 대응 서비스
	취약성 관리에 최적화되었습니다.	Amazon Inspector [1]
	보안 데이터를 중앙 집중화하도록 최적화되었습니다.	Amazon Security Lake [1]
	잠재적 보안 문제를 집계하고 요약하는 데 최적화되었습니다.	Amazon Detective [1, 2, 3]
	조사 결과를 분류하고, 보안 이벤트를 에스컬레이션하고, 즉각적인 주의가 필요한 사례를 관리하는 데 도움이 되도록 최적화되었습니다.	AWS 보안 인시던트 대응

AWS 거버넌스 및 규정 준수 서비스 선택

리소스 전반에 걸쳐 클라우드 거버넌스를 설정하고 규정 준수 및 감사 프로세스를 자동화합니다.

언제 사용해야 하나요?	무엇에 최적화되어 있나요?	거버넌스 및 규정 준수 서비스
이러한 서비스를 사용하면 사용 시 모범 사례를 구현하고 업계 표준을 충족하는 데 도움이 됩니다 AWS.	여러 계정 및 통합 결제를 중앙에서 관리하는 데 최적화되었습니다.	AWS Organizations
	AWS 보안 및 규정 준수 문서의 온디맨드 다운로드를 제공하는 데 최적화되었습니다.	AWS Artifact
	사용량 감사에 최적화되었습니다 AWS .	AWS Audit Manager [1]
	AWS 다중 계정 환경을 설정하고 관리하는 데 최적화되었습니다.	AWS Control Tower

AWS 보안, 자격 증명 및 거버넌스 서비스 사용

이제 각 AWS 보안, 자격 증명 및 거버넌스 서비스(및 지원 AWS 도구 및 서비스)가 수행하는 작업과 자신에게 적합할 수 있는 작업에 대해 명확하게 이해할 수 있습니다.

사용 가능한 각 AWS 보안, 자격 증명 및 거버넌스 서비스를 사용하고 자세히 알아보는 방법을 알아보기 위해 각 서비스의 작동 방식을 탐색하는 경로를 제공했습니다. 다음 섹션에서는 시작하는 데 도움이 되는 심층 설명서, 실습 자습서 및 리소스에 대한 링크를 제공합니다.

AWS ID 및 액세스 관리 서비스 사용

다음 표에는 시작하는 데 도움이 되도록 서비스별로 구성된 몇 가지 유용한 자격 증명 및 액세스 관리 리소스가 나와 있습니다.

AWS IAM Identity Center

- AWS IAM Identity Center 활성화

  IAM Identity Center를 활성화하고에서 사용을 시작합니다 AWS Organizations.

  가이드 살펴보기
- 기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스 구성

  기본 디렉터리를 자격 증명 소스로 사용하고 사용자 액세스를 설정하고 테스트합니다.

  지침으로 시작하기
- Active Directory를 자격 증명 소스로 사용

  Active Directory를 IAM Identity Center ID 소스로 사용하기 위한 기본 설정을 완료합니다.

  지침으로 시작하기
- Okta 및 IAM Identity Center를 사용하여 SAML 및 SCIM 구성

  Okta 및 IAM Identity Center와 SAML 연결을 설정합니다.

  지침으로 시작하기

Amazon Cognito

- Amazon Cognito 시작하기

  가장 일반적인 Amazon Cognito 작업에 대해 알아봅니다.

  가이드 살펴보기
- 자습서: 사용자 풀 생성

  사용자가 웹 또는 모바일 앱에 로그인할 수 있는 사용자 풀을 생성합니다.

  지침으로 시작하기
- 자습서: 자격 증명 풀 생성

  사용자가 액세스하기 위한 임시 AWS 자격 증명을 얻을 수 있도록 자격 증명 풀을 생성합니다 AWS 서비스.

  지침으로 시작하기
- Amazon Cognito 워크숍

  Amazon Cognito를 사용하여 가상의 반려 동물 저장소에 대한 인증 솔루션을 구축하는 방법을 연습합니다.

  지침으로 시작하기

AWS RAM

- 시작하기 AWS RAM

  AWS RAM 용어 및 개념에 대해 알아봅니다.

  가이드 살펴보기
- 공유 AWS 리소스 작업

  소유한 AWS 리소스를 공유하고 공유된 AWS 리소스에 액세스합니다.

  가이드 살펴보기
- AWS RAM에서 권한 관리

  관리형 권한과 고객 AWS 관리형 권한이라는 두 가지 유형의 관리형 권한에 대해 알아봅니다.

가이드 살펴보기

- AWS RAM을 사용하여 공유되는 리소스에 대한 세부 액세스 구성

  고객 관리형 권한을 사용하여 리소스 액세스를 사용자 지정하고 최소 권한의 모범 사례를 달성합니다.

  블로그 읽기

IAM

- IAM 시작하기

  를 사용하여 IAM 역할, 사용자 및 정책을 생성합니다 AWS Management Console.

  지침으로 시작하기
- 역할을 AWS 계정 사용하여 간에 액세스 권한 위임

  역할을 사용하여 사용자가 소유한 ProductionandDevelopment라는 다른 AWS 계정 의 리소스에 대한 액세스를 위임합니다.

  지침으로 시작하기
- 고객 관리형 정책 생성

  AWS Management Console 를 사용하여 고객 관리형 정책을 생성한 다음 해당 정책을의 IAM 사용자에게 연결합니다 AWS 계정.

  지침으로 시작하기
- 태그를 기반으로 AWS 리소스에 액세스할 수 있는 권한 정의

  보안 주체 태그가 있는 IAM 역할이 일치하는 태그가 있는 리소스에 액세스할 수 있도록 허용하는 정책을 생성하고 테스트합니다.

  지침으로 시작하기
- IAM의 보안 모범 사례

  IAM 모범 사례를 사용하여 AWS 리소스를 보호할 수 있습니다.

  가이드 살펴보기

AWS 데이터 보호 서비스 사용

다음 섹션에서는 데이터 보호를 설명하는 AWS 자세한 리소스에 대한 링크를 제공합니다.

Macie

- Amazon Macie 시작하기

  에 대해 Macie를 활성화하고 AWS 계정, Amazon S3 보안 태세를 평가하고, S3 버킷에서 민감한 데이터를 검색하고 보고하기 위한 키 설정 및 리소스를 구성합니다.

  가이드 살펴보기
- Amazon Macie를 사용한 데이터 보안 및 개인 정보 보호 모니터링

  Amazon Macie를 사용하여 Amazon S3 데이터 보안을 모니터링하고 보안 태세를 평가합니다.

  가이드 살펴보기
- Amazon Macie 조사 결과 분석

  Amazon Macie 조사 결과를 검토, 분석 및 관리합니다.

  가이드 살펴보기
- Amazon Macie 조사 결과를 사용하여 민감한 데이터 샘플 검색

  Amazon Macie를 사용하여 개별 조사 결과에서 보고된 민감한 데이터의 샘플을 검색하고 공개합니다.

  가이드 살펴보기
- Amazon Macie를 사용하여 민감한 데이터 검색

  Amazon S3 데이터 자산에서 민감한 데이터의 검색, 로깅 및 보고를 자동화합니다.

  가이드 살펴보기

AWS KMS

- 시작하기 AWS KMS

  생성부터 삭제까지 대칭 암호화 KMS 키를 관리합니다.

가이드 살펴보기

- 특수 목적 키

  대칭 암호화 KMS 키 외에도에서 AWS KMS 지원하는 다양한 유형의 키에 대해 알아봅니다.

  가이드 살펴보기

- 를 사용하여 저장 시 암호화 기능 확장 AWS KMS

  내에서 사용할 수 있는 저장 데이터 암호화 옵션에 대해 알아봅니다 AWS.

  워크숍 살펴보기

AWS CloudHSM

- 시작하기 AWS CloudHSM

  AWS CloudHSM 클러스터를 생성, 초기화 및 활성화합니다.

  가이드 살펴보기

- AWS CloudHSM 클러스터 관리

  AWS CloudHSM 클러스터 및 클러스터 관리의 다양한 관리 작업에 연결합니다.

  가이드 살펴보기

- 에서 HSM 사용자 및 키 관리 AWS CloudHSM

  클러스터의 HSMs에서 사용자 및 키를 생성합니다.

  가이드 살펴보기

- CloudHSM에서 TLS 오프로드와 함께 Amazon ECS를 사용하여 NGINX 웹 서비스 배포 자동화

  AWS CloudHSM 를 사용하여 클라우드에서 호스팅되는 웹 사이트의 프라이빗 키를 저장합니다.

  블로그 읽기

AWS Certificate Manager

- 퍼블릭 인증서 요청

AWS Certificate Manager (ACM) 콘솔 또는 AWS CLI 를 사용하여 퍼블릭 ACM 인증서를 요청합니다.

가이드 살펴보기

- 에 대한 모범 사례 AWS Certificate Manager

  현재 ACM 고객의 실제 경험을 기반으로 모범 사례를 알아봅니다.

  가이드 살펴보기

- 를 AWS Certificate Manager 사용하여 인증서 발급 제어를 적용하는 방법

  IAM 조건 키를 사용하여 사용자가 조직의 지침에 따라 TLS 인증서를 발급하거나 요청하는지 확인합니다.

  블로그 읽기

AWS Private CA

- AWS Private CA 배포 계획

  프라이빗 인증 기관을 생성하기 전에 사용할 AWS Private CA 준비를 합니다.

  가이드 살펴보기

- AWS Private CA 관리

  조직에서 내부적으로 사용할 수 있도록 루트 및 하위 인증 기관의 완전히 AWS 호스팅된 계층 구조를 생성합니다.

  가이드 살펴보기

- 인증서 관리

  를 사용하여 프라이빗 인증서 발급 AWS Private CA, 검색 및 나열과 같은 기본 인증서 관리 작업을 수행합니다.

  가이드 살펴보기

- AWS Private CA 워크숍

  사설 인증 기관의 다양한 사용 사례를 통해 실습 경험을 개발합니다.

워크숍 살펴보기

- 를 사용하여 Active Directory에서 인증서 프로비저닝을 간소화하는 방법 AWS Private CA

  AWS Private CA 를 사용하여 Microsoft Active Directory 환경 내에서 사용자 및 시스템에 대한 인증서를 보다 쉽게 프로비저닝할 수 있습니다.

  블로그 읽기

- 에서 DNS 이름 제약 조건을 적용하는 방법 AWS Private CA

  AWS Private CA 서비스를 사용하여 하위 CA에 DNS 이름 제약 조건을 적용합니다.

  블로그 읽기

AWS Secrets Manager

- AWS Secrets Manager 개념

  를 사용하여 프라이빗 인증서 발급 AWS Private CA, 검색 및 나열과 같은 기본 인증서 관리 작업을 수행합니다.

  가이드 살펴보기

- 에 대한 대체 사용자 교체 설정 AWS Secrets Manager

  데이터베이스 자격 증명이 포함된 보안 암호에 대해 대체 사용자 교체를 설정합니다.

  가이드 살펴보기

- Kubernetes에서 AWS Secrets Manager 보안 암호 사용

  Secrets and Configuration Provider(ASCP)를 사용하여 Secrets Manager의 AWS 보안 암호를 Amazon EKS 포드에 탑재된 파일로 표시합니다.

  가이드 살펴보기

AWS Payment Cryptography

- 시작하기 AWS Payment Cryptography

  키를 생성하고 다양한 암호화 작업에 사용합니다.

가이드 살펴보기

- AWS Payment Cryptography FAQs

  의 기본 사항을 이해합니다 AWS Payment Cryptography.

  FAQs 살펴보기

AWS 네트워크 및 애플리케이션 보호 서비스 사용

다음 표에는 AWS 네트워크 및 애플리케이션 보호를 설명하는 자세한 리소스에 대한 링크가 나와 있습니다.

AWS Firewall Manager

- AWS Firewall Manager 정책 시작하기

  AWS Firewall Manager 를 사용하여 다양한 유형의 보안 정책을 활성화합니다.

  가이드 살펴보기
- 를 사용하여 보안 그룹을 지속적으로 감사하고 제한하는 방법 AWS Firewall Manager

  AWS Firewall Manager 를 사용하여 보안 그룹을 제한하고 필요한 포트만 열려 있는지 확인합니다.

  블로그 읽기
- AWS Firewall Manager 를 사용하여 대규모로 보호 배포 AWS Organizations

  AWS Firewall Manager 를 사용하여에 보안 정책을 배포하고 관리합니다 AWS Organizations.

  블로그 읽기

AWS Network Firewall

- 시작하기 AWS Network Firewall

  기본 인터넷 게이트웨이 아키텍처를 사용하여 VPC용 AWS Network Firewall 방화벽을 구성하고 구현합니다.

  가이드 살펴보기

- AWS Network Firewall 워크숍

  인프라 코드를 사용하여 AWS Network Firewall 를 배포합니다.

  워크숍 살펴보기

- AWS Network Firewall 유연한 규칙 엔진 실습 – 1부

  AWS Network Firewall 에 데모를 배포 AWS 계정 하여 규칙 엔진과 상호 작용합니다.

  블로그 읽기

- AWS Network Firewall 유연한 규칙 엔진 실습 – 2부

  엄격한 규칙 순서로 방화벽 정책을 생성하고 하나 이상의 기본 작업을 설정합니다.

  블로그 읽기

- 용 배포 모델 AWS Network Firewall

  트래픽 경로에 추가할 수 AWS Network Firewall 있는 일반적인 사용 사례에 대한 배포 모델을 알아봅니다.

  블로그 읽기

- AWS Network Firewall VPC 라우팅 기능이 향상된 용 배포 모델

  향상된 VPC 라우팅 프리미티브를 사용하여 동일한 VPC의 서로 다른 서브넷에 있는 워크로드 AWS Network Firewall 간에를 삽입합니다.

  블로그 읽기

AWS Shield

- AWS Shield 작동 방식

  및 AWS Shield Advanced 가 네트워크 AWS Shield Standard 및 전송 계층(계층 3 및 4)과 애플리케이션 계층(계층 7)의 AWS 리소스에 대한 DDoS 공격으로부터 보호하는 방법을 알아봅니다.

  가이드 살펴보기

- 시작하기 AWS Shield Advanced

  Shield Advanced 콘솔 AWS Shield Advanced 을 사용하여를 시작합니다.

가이드 살펴보기

- AWS Shield Advanced 워크숍

  인터넷에 노출된 리소스를 DDoS 공격으로부터 보호하고, 인프라에 대한 DDoS 공격을 모니터링하고, 적절한 팀에 알립니다.

  워크숍 살펴보기

AWS WAF

- 시작하기 AWS WAF

  웹 요청을 필터링하는 규칙 및 규칙 그룹을 추가하여 웹 ACL을 설정 및 AWS WAF생성하고 Amazon CloudFront를 보호합니다.

  지침으로 시작하기

- Amazon CloudWatch AWS WAF Logs에서 로그 분석

  Amazon CloudWatch logs에 대한 기본 AWS WAF 로깅을 설정하고 로그의 데이터를 시각화하고 분석합니다.

  블로그 읽기

- Amazon CloudWatch 대시보드를 사용하여 AWS WAF 로그 시각화

  Amazon CloudWatch를 사용하여 CloudWatch 지표, Contributor Insights 및 Logs Insights를 사용하여 AWS WAF 활동을 모니터링하고 분석할 수 있습니다.

  블로그 읽기

AWS 탐지 및 대응 서비스 사용

다음 표에는 AWS 탐지 및 대응 서비스를 설명하는 자세한 리소스에 대한 링크가 나와 있습니다.

AWS Config

- 시작하기 AWS Config

  SDK를 설정하고 AWS Config 작업합니다. AWS SDKs

가이드 살펴보기

- 위험 및 규정 준수 워크숍

  AWS Config 및 AWS 관리형 Config 규칙을 사용하여 제어를 자동화합니다.

  워크숍 살펴보기
- AWS Config 규칙 개발 키트 라이브러리: 대규모 규칙 구축 및 운영

  규칙 개발 키트(RDK)를 사용하여 사용자 지정 AWS Config 규칙을 빌드하고 RDKLib와 함께 배포합니다.

  블로그 읽기

AWS CloudTrail

- 이벤트 기록 보기

  CloudTrail을 지원하는 서비스에 AWS 계정 대한의 AWS API 활동을 검토합니다.

  지침으로 시작하기
- 관리 이벤트를 로깅하는 추적 생성

  추적을 생성하여 모든 리전에서 관리 이벤트를 로깅합니다.

  지침으로 시작하기

AWS Security Hub

- 활성화 AWS Security Hub

  독립 실행형 계정으로 AWS Security Hub AWS Organizations 또는를 활성화합니다.

  가이드 살펴보기
- 크로스 리전 집계

  여러의 AWS Security Hub 조사 결과를 단일 집계 리전 AWS 리전 으로 집계합니다.

  가이드 살펴보기
- AWS Security Hub 워크숍

AWS Security Hub 및를 사용하여 AWS 환경의 보안 태세를 관리하고 개선하는 방법을 알아봅니다.

워크숍 살펴보기

- 세 가지 기본 Security Hub 사용 패턴 및 배포 방법

  가장 일반적인 세 가지 AWS Security Hub 사용 패턴과 조사 결과를 식별하고 관리하기 위한 전략을 개선하는 방법에 대해 알아봅니다.

  블로그 읽기

Amazon GuardDuty

- Amazon GuardDuty 시작하기

  Amazon GuardDuty를 활성화하고, 샘플 조사 결과를 생성하고, 알림을 설정합니다.

  자습서 살펴보기

- Amazon GuardDuty의 EKS 보호

  Amazon GuardDuty를 사용하여 Amazon Elastic Kubernetes Service(Amazon EKS) 감사 로그를 모니터링합니다.

  가이드 살펴보기

- Amazon GuardDuty의 Lambda 보호

  AWS Lambda 함수를 호출할 때 잠재적 보안 위협을 식별합니다.

  가이드 살펴보기

- GuardDuty Amazon RDS 보호

  Amazon GuardDuty를 사용하여 Amazon Aurora 데이터베이스에 대한 잠재적 액세스 위협에 대해 Amazon Relational Database Service(Amazon RDS) 로그인 활동을 분석하고 프로파일링합니다.

  가이드 살펴보기

- Amazon GuardDuty의 Amazon S3 보호 Amazon GuardDuty

GuardDuty를 사용하여 CloudTrail 데이터 이벤트를 모니터링하고 S3 버킷 내의 잠재적 보안 위험을 식별합니다.

가이드 살펴보기

- Amazon GuardDuty 및 Amazon Detective를 사용한 위협 탐지 및 대응

  Amazon GuardDuty 및 Amazon Detective의 기본 사항에 대해 알아봅니다.

  워크숍 살펴보기

Amazon Inspector

- Amazon Inspector 시작하기

  Amazon Inspector 스캔을 활성화하여 콘솔의 결과를 이해합니다.

  지침으로 시작하기

- Amazon Inspector를 사용한 취약성 관리

  Amazon Inspector를 사용하여 Amazon Elastic Container Registry(Amazon ECR)의 Amazon EC2 인스턴스 및 컨테이너 이미지에서 소프트웨어 취약성을 스캔합니다.

  워크숍 살펴보기

- Amazon Inspector를 사용하여 EC2 AMIs 스캔하는 방법

  여러를 사용하여 AMIs이 있는지 검사 AWS 서비스 하여 솔루션을 구축합니다.

  블로그 읽기

Amazon Security Lake

- Amazon Security Lake 시작하기

  Amazon Security Lake를 활성화하고 사용을 시작합니다.

  가이드 살펴보기

- 를 사용하여 여러 계정 관리 AWS Organizations

  여러에서 보안 로그 및 이벤트를 수집합니다 AWS 계정.

가이드 살펴보기

- Amazon Security Lake에서 Amazon OpenSearch Service에 게시한 이벤트를 수집, 변환 및 전달합니다.

  SecOps 팀이 사용할 수 있도록 Amazon Security Lake 데이터를 수집, 변환 및 Amazon OpenSearch Service에 전송합니다.

  블로그 읽기

- How to visualize Amazon Security Lake findings with QuickSight

  Amazon AthenaandQuickSight를 사용하여 Amazon Security Lake에서 데이터를 쿼리하고 시각화합니다.

  블로그 읽기

Amazon Detective

- Amazon Detective 용어 및 개념

  Amazon Detective를 이해하는 데 중요한 주요 용어 및 개념과 작동 방식을 알아봅니다.

  가이드 살펴보기

- Amazon Detective 설정

  Amazon Detective 콘솔, Amazon Detective API 또는에서 Amazon Detective를 활성화합니다 AWS CLI.

  가이드 살펴보기

- Amazon GuardDuty 및 Amazon Detective를 사용한 위협 탐지 및 대응

  Amazon GuardDuty 및 Amazon Detective의 기본 사항에 대해 알아봅니다.

  워크숍 살펴보기

AWS 거버넌스 및 규정 준수 서비스 사용

다음 표에는 거버넌스 및 규정 준수를 설명하는 자세한 리소스에 대한 링크가 나와 있습니다.

AWS Organizations

- 조직 생성 및 구성

  조직을 생성하고 두 개의 AWS 멤버 계정으로 구성합니다.

  지침으로 시작하기

- 에서 작동하는 서비스 AWS Organizations

  와 함께 사용할 수 있는 항목 AWS Organizations 과 조직 전체 수준에서 각 서비스를 사용할 AWS 서비스 때 얻을 수 있는 이점을 이해합니다.

  가이드 살펴보기

- 여러 계정을 사용하여 AWS 환경 구성

  전체 AWS 환경을 구성하기 위한 모범 사례 및 현재 권장 사항을 구현합니다.

  백서 읽기

AWS Artifact

- 시작하기 AWS Artifact

  보안 및 규정 준수 보고서를 다운로드하고, 법적 계약을 관리하고, 알림을 관리합니다.

  가이드 살펴보기

- 에서 계약 관리 AWS Artifact

  AWS Management Console 를 사용하여 계정 또는 조직의 계약을 검토, 수락 및 관리합니다.

  가이드 살펴보기

- 1 AWS 부 - AWS 감사 관리자 AWS Config및 AWS 아티팩트에서 감사 준비

  AWS 서비스 를 사용하면 감사에 사용되는 증거 수집을 자동화할 수 있습니다.

  블로그 읽기

AWS Audit Manager

- AWS Audit Manager 활성화

, Audit Manager API 또는를 사용하여 Audit Manager AWS Management Console를 활성화합니다 AWS CLI.

가이드 살펴보기

- 감사 소유자를 위한 자습서: 평가 생성

  Audit Manager 샘플 프레임워크를 사용하여 평가를 생성합니다.

  가이드 살펴보기

- 대리인을 위한 자습서: 컨트롤 세트 검토

  Audit Manager에서 감사 소유자가 공유한 컨트롤 세트를 검토합니다.

  가이드 살펴보기

AWS Control Tower

- 시작하기 AWS Control Tower

  규범적 모범 사례를 따르는 랜딩 존이라는 다중 계정 환경을 설정하고 시작합니다.

  가이드 살펴보기

- Amazon Bedrock 및를 사용한 계정 관리 현대화 AWS Control Tower

  보안 도구 계정을 프로비저닝하고 생성형 AI를 활용하여 AWS 계정 설정 및 관리 프로세스를 가속화합니다.

  블로그 읽기

- 를 사용하여 Well-Architected AWS GovCloud(미국) 환경 구축 AWS Control Tower

  조직 단위(OU) 및를 사용하여 AWS 워크로드 관리를 포함하여 AWS GovCloud(미국) 리전에서 거버넌스를 설정합니다 AWS 계정.OUs

  블로그 읽기

AWS 보안, 자격 증명 및 거버넌스 서비스 살펴보기

Editable architecture diagrams

참조 아키텍처 다이어그램

보안, 자격 증명 및 거버넌스 전략을 개발하는 데 도움이 되는 참조 아키텍처 다이어그램을 살펴보세요.

보안, 자격 증명 및 거버넌스 참조 아키텍처 살펴보기

Ready-to-use code

추천 솔루션

의 Security Insights AWS

Amazon Security Lake의 데이터를 시각화하여 보안 이벤트를 보다 신속하게 조사하고 대응할 수 있도록 지원하는 배포 AWS빌드된 코드입니다.

이 솔루션 살펴보기

AWS 솔루션

사전 구성되고 배포 가능한 솔루션과 이를 기반으로 구축된 구현 가이드를 살펴봅니다 AWS.

모든 AWS 보안, 자격 증명 및 거버넌스 솔루션 살펴보기

Documentation

보안, 자격 증명 및 거버넌스 백서

조직에 가장 적합한 보안, 자격 증명 및 거버넌스 서비스를 선택, 구현 및 사용하는 방법에 대한 추가 인사이트와 모범 사례를 알아보려면 백서를 살펴보세요.

보안, 자격 증명 및 거버넌스 백서 살펴보기

AWS 보안 블로그

특정 보안 사용 사례를 다루는 블로그 게시물을 살펴보세요.

AWS 보안 블로그 살펴보기

문서 기록

다음 표에서는이 결정 가이드의 중요한 변경 사항에 대해 설명합니다. 이 가이드의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
re:Invent 업데이트	AWS 보안 인시던트 대응 및 에 대한 정보가 추가되었습니다 AWS Payment Cryptography. AWS Identity and Access Management 및에 대한 서비스 정보가 업데이트되었습니다 AWS IAM Identity Center.	2024년 12월 30일
비디오 업데이트	re:Inforce 2024의 최근 번개 토크로 입문용 비디오를 업데이트했습니다.	2024년 6월 25일
거버넌스 서비스 추가	AWS CloudTrail AWS Control Tower, 및 추가를 포함하여 거버넌스를 포함하도록 문서의 범위를 넓혔습니다 AWS Organizations. 새 범위를 반영하도록 그래픽을 업데이트했습니다. 자격 증명에 대한 모범 사례를 명확히 했습니다. 문서 전반에 편집상 변경 사항을 적용했습니다.	2024년 6월 7일
최초 게시	가이드가 처음 게시되었습니다.	2024년 3월 21일

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