AWS 클라우드 채택 프레임워크

보안 관점

2016년 6월

고지 사항

이 문서는 정보 제공 목적으로만 제공됩니다. 본 문서의 발행일 당시 AWS의 현재 제품 및 실행 방법을 설명하며, 예고 없이 변경될 수 있습니다. 고객은 본 문서에 포함된 정보나 AWS 제품 또는 서비스의 사용을 독립적으로 평가할 책임이 있으며, 각 정보 및 제품은 명시적이든 묵시적이든 어떠한 종류의 보증 없이 "있는 그대로" 제공됩니다. 본 문서는 AWS, 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 보증, 표현, 계약 약속, 조건 또는 보증을 구성하지 않습니다. 고객에 대한 AWS의 책임 및 채무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

목차

요약

Amazon Web Services(AWS) 클라우드 채택 프레임워크[1](CAF)에는 클라우드 컴퓨팅으로 마이그레이션하는 과정에서 조직의 다양한 부분을 조정하기 위한 지침이 나와 있습니다. CAF 지침은 클라우드 기반 IT 시스템 구현과 관련된 여러 중점 영역으로 분류되어 있습니다. 이러한 중점 영역을 *관점*이라고 하며, 각 관점은 *구성 요소*로 더 세분화됩니다. 7개의 각 CAF 관점에 대한 백서가 있습니다.

이 백서에서는 각 환경에서 AWS를 사용할 때 기존 보안 제어에 대한 지침 및 프로세스의 통합에 중점을 둔 보안 관점을 다룹니다.

소개

AWS에서의 보안은 간단합니다. 모든 AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다. AWS와 파트너는 가시성, 감사 효율성, 제어 효율성 및 민첩성을 중심으로 보안 목표를 달성하는 데 도움이 되는 수백 개의 도구와 기능을 제공합니다. 따라서 자본을 지출하지 않고도 온프레미스 환경보다 훨씬 저렴한 운영 비용으로 필요한 보안을갖출 수 있습니다.

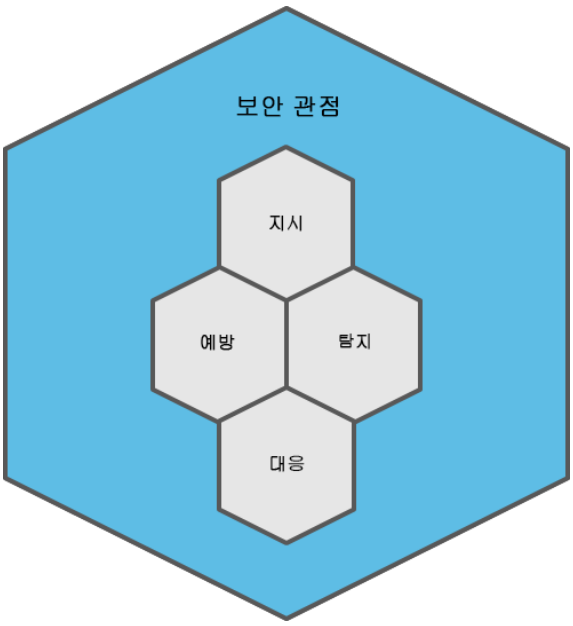

그림 1: AWS CAF 보안 관점

보안 관점 목표는 조직에 적합한 제어를 선택하고 구현할 수 있도록 지원하는 것입니다. 그림 1과 같이, 보안 관점의 구성 요소는 조직의 보안 문화를 변화시킬 수 있는 원칙을 구성합니다. 이 백서에서는 각 구성 요소에 대해 취할 수 있는 구체적인 조치와 진행 상태를 평가하는 수단에 대해 논의합니다.

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

클라우드에서의 보안 구현은 결코 낯설지 않습니다. 보안을 대규모로 보다 민첩하고 신속하게 저렴한 비용으로 실행한다고 해서 기존의 정보 보안 원칙이 무용지물이 되는 것은 아닙니다.

이 백서에서는 네 가지 보안 관점 구성 요소를 다룬 후, 클라우드로 전환하는 동안 각 환경에서 강력한 보안 기반을 유지하기 위해 취할 수 있는 조치에 대해 살펴봅니다.

- 클라우드에서의 **보안 전략**을 정의합니다. 전환을 시작할 때 조직의 비즈니스 목표, 위험 관리에 대한 접근 방식, 클라우드가 제공하는 기회의 수준을 고려해야 합니다.
- 보안, 개인 정보 보호, 규정 준수 및 위험 관리 기능을 개발하고 구현하기 위한 **보안 프로그램**을 제공합니다. 처음에는 범위가 방대하게 보일 수 있으므로, 조직이 클라우드에서의 보안을 통합적으로 다룰 수 있도록 하나의 구조를 만들어야 합니다. 또한 프로그램 개발에 따라 기능이 성숙해지도록 구현 과정에서 반복적인 개발이 가능해야 합니다. 이렇게 하면 보안 구성 요소는 조직의 나머지 클라우드 채택 작업에 대한 기폭제가 될 수 있습니다.

- 지속적으로 성숙해지고 향상되는 강력한 **보안 작업** 기능을 개발합니다. 보안을 구축하고 구현하는 일은 계속되는 과정입니다. 엄격하게 운영하는 동시에 새로운 기능을 계속해서 구축함으로써 보안을 지속적으로 개선해 나가는 것이 좋습니다.

AWS의 보안 이점

AWS에서 가장 우선순위가 높은 것이 클라우드 보안입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

AWS 클라우드의 장점은 고객이 보안 환경을 유지하면서 확장 및 혁신을 이룰 수 있다는 것입니다. 고객은 사용한 서비스에 대한 비용만 지불하면 됩니다. 즉 선결제 금액 없이 온프레미스 환경보다 낮은 비용으로 필요한 보안을 갖출 수 있습니다.

이 단원에서는 AWS 플랫폼의 몇 가지 보안 이점에 대해 논의합니다.

보안을 위한 설계

AWS 클라우드 인프라는 AWS 데이터 센터에서 운영되며 보안에 가장 민감한 고객의 요구 사항을 충족하도록 설계되었습니다. AWS 인프라는 고객의 개인 정보를 보호하기 위한 강력한 보안 조치를 실시하면서 높은 가용성을 제공하도록 설계되었습니다. 모든 데이터는 보안이 철저한 AWS 데이터 센터에 저장됩니다. Amazon VPC에 구축된 네트워크 방화벽과 AWS WAF의 웹 애플리케이션 방화벽 기능을 통해 프라이빗 네트워크를 만들고 인스턴스와 애플리케이션에 대한 액세스를 제어할 수 있습니다.

AWS 클라우드에 시스템을 배포하면 AWS는 보안 책임을 고객과 분담함으로써 고객을 지원합니다. AWS는 보안 설계 원칙을 적용하여 기본 인프라를 설계하며, 고객은 AWS에 배포된 워크로드에 대해 고유의 보안 아키텍처를 구현할 수 있습니다.

높은 수준의 자동화

AWS는 보안 도구를 목적에 맞게 빌드하고, 고유의 환경, 크기 및 글로벌 요구 사항에 맞게 이를 조정합니다. 보안 도구를 처음부터 새로 빌드하기 때문에 AWS는 보안 전문가가 일반적으로 시간을 소비하는 많은 일상적인 작업을 자동화할 수 있습니다. 따라서 AWS 보안 전문가는 AWS 클라우드 환경의보안을 강화하기 위한 조치에 더 많은 시간을 투자할 수 있습니다. 또한 고객은 종합적인 API 및 도구 세트를 사용하여 보안 엔지니어링 및 운영 기능을 자동화합니다. 이미 실행 중인 인기 있는 소프트웨어 개발 방법을 사용하여 자격 증명 관리, 네트워크 보안 및 데이터 보호, 모니터링 기능을 완전히 자동화하고 제공할 수 있습니다. 고객은 자동화된 접근 방식으로 보안 문제에 대응합니다. 사람이 직접 보안 위치를 모니터링하고 이벤트에 대응하는 대신 AWS 서비스를 사용하여 자동화하면 시스템에서 상태를 모니터링하고 검토하고 대응할 수 있습니다.

고가용성

AWS는 여러 지리적 리전에 데이터 센터를 구축하고 있습니다. 복원성을 제공하기 위해 리전 내에는 여러 가용 영역이 있습니다. AWS는 여분의 대역폭을 갖춘 데이터 센터를 설계하기 때문에 대규모 중단이 발생할 경우 트래픽을 로드 밸런싱하고 나머지 사이트에 라우팅하여 고객에게 미치는 영향을 최소화할 수 있는 충분한 용량이 있습니다. 또한 고객은 이 다중 리전, 다중 AZ 전략을 활용하여 분산된 낮은 비용으로 복원성 높은 애플리케이션을 빌드하고, 데이터를 쉽게 복제 및 백업하며, 비즈니스 전반에 걸쳐 글로벌 보안 제어를 일관적으로 배포합니다.

엄격한 인증

AWS 환경은 전 세계 인증 기관으로부터 지속적인 감사와 인증을 받습니다. 따라서 고객의 규정 준수 부문 중 일부가 이미 충족되어 있습니다. AWS가 준수하는 보안 규정 및 표준에 대한 자세한 내용은 AWS 클라우드 규정 준수[2] 웹 페이지를 참조하십시오. AWS는 특정 정부, 산업 및 회사 보안 표준과 규제를 충족할 수 있도록 AWS 클라우드 인프라가 광범위한 글로벌 보안 표준 목록의 요구 사항을 어떻게 충족하는지에 대해 설명하는 인증 보고서를 제공합니다. AWS 계정 담당자에게 문의하여 규정 준수 보고서를 받을 수 있습니다. 고객은 제어 기능을 실제로 직접 유지하는 것 외에도 AWS에서 운영하는 많은 제어 기능을 자체 규정 준수 및 인증 프로그램으로 상속하여 보안을 유지하고 실행하는 비용을 절감할 수 있습니다. 강력한 기반이 확립된 상태에서 민첩성, 복원성 및 확장성을 위해 워크로드의 보안을 자유롭게 최적화할 수 있습니다.

이 백서의 나머지 부분에서는 보안 관점의 각 구성 요소를 소개합니다. 이러한 구성 요소를 사용하여 클라우드로 성공적으로 전환하는 데 필요한 보안 목표를 탐색할 수 있습니다.

지시 구성 요소

AWS 보안 관점의 지시 구성 요소는 AWS로 마이그레이션할 때 보안 접근 방식을 계획하는 데 도움이 되는 지침을 제시합니다. 계획을 효과적으로 수립하기 위한 핵심은 보안 환경을 구현하고 운영하는 담당자에게 제시할 지침을 정의하는 것입니다. 정보에는 필요한 제어와 이 제어를 작동하는 방법을 결정하기 위한 방향이 제시되어 있어야 합니다. 고려해야 할 초기 영역에는 다음 항목이 포함됩니다.

- **계정 거버넌스** - 조직이 AWS 계정을 관리하기 위한 프로세스와 절차를 구축할 수 있도록 안내합니다. 정의할 영역에는 계정 인벤토리를 수집하고 유지 관리하는 방법, 시행되는 계약 및 수정 조항, AWS 계정을 생성할 때 적용할 기준 등이 포함됩니다. 모든 초기 설정이 적절하고 명확한 소유권이 확립되도록 계정을 일관적인 방식으로 생성하기 위한 프로세스를 개발합니다.

- **계정 소유권 및 계약 정보** - 조직 전반에서 사용되는 AWS 계정에 대해 적절한 거버넌스 모델을 설정하고 각 계정의 연락처 정보를 유지 관리하는 방법을 계획합니다. 개별 이메일 주소보다는 이메일 그룹과 연결된 AWS 계정을 생성합니다. 그러면 한 그룹의 사람들이 계정 활동에 대한 AWS의 정보를 모니터링하고 대응할 수 있습니다. 또한 내부 직원이 변경될 때 복원성이 제공되며 보안 책임을 배정하는 방법도 제공됩니다. 보안 팀을 보안 접점으로 등록하여 시간이 중요한 통신을 신속하게 처리합니다.

- **제어 프레임워크** - 산업 표준 제어 프레임워크를 설정하거나 적용하고 예상 보안 수준에서 AWS 서비스를 통합하기 위해 수정 또는 추가 사항이 필요한지를 결정합니다. 규정 준수 매핑 연습을 수행하여 규정 준수 요구 사항과 보안 제어에 AWS 서비스 사용이 어떻게 반영될지를 확인합니다.

- **제어 소유권** - AWS 웹 사이트에서 AWS 책임 분담 모델[3] 정보를 검토하여 제어 소유권을 수정해야 하는지 확인합니다. 책임 배정 매트릭스(RACI 차트)를 검토하고 AWS 환경에서 운영되는 제어의 소유권을 포함하도록 업데이트합니다.

- **데이터 분류** - 현재 데이터 분류를 검토하고 AWS 환경에서 그러한 분류를 관리할 방법과 적절한 제어 방식을 결정합니다.

- **변경 및 자산 관리** - AWS에서 변경 및 자산 관리를 수행할 방법을 결정합니다. 존재할 자산, 사용할 시스템, 시스템을 안전하게 관리할 방법을 결정하기 위한 수단을 마련합니다. 이 항목은 기존 구성 관리 데이터베이스(CMDB)와 통합할 수 있습니다. 필요한 보안 수준에서 식별 및 관리 작업을 수행할 수 있도록 명명 및 태깅을 위한 실행 방식을 마련합니다. 이 접근 방식을 사용하여 식별 및 제어에 사용되는 메타데이터를 정의하고 추적할 수 있습니다.

- **데이터 지역성** - 데이터가 상주할 수 있는 위치에 대한 기준을 검토하여 리전 전반에 걸쳐 AWS 서비스의 구성과 사용을 관리하기 위해 필요한 제어를 결정합니다. AWS 고객은 콘텐츠가 호스팅될 AWS 리전을 선택합니다. 이렇게 하면 특정한 지리적 요구 사항이 있는 고객이 선택한 위치에서 환경을 설정할 수 있습니다. 고객은 두 개 이상의 리전에 콘텐츠를 복제 및 백업할 수 있지만, AWS는 고객이 선택한 리전 이외의 장소로 고객의 콘텐츠를 이동하지 않습니다.

- **최소 권한 액세스** - 최소 권한 및 강력한 인증 원칙을 기반으로 하는 조직 보안 문화를 확립합니다. 모든 AWS 계정과 연결된 민감한 자격 증명 및 키 구성 요소에 대한 액세스를 보호하는 프로토콜을 구현합니다. 클라우드 채택에 관여하는 소프트웨어 엔지니어, 운영 직원 및 기타 직무를 기관에 위임하는 방식에 대한 기대 사항을 설정합니다.
- **보안 작업 지침 및 실행서** - 시간이 경과하더라도 조직이 참조할 수 있는 지속성 있는 가드 레일을 만들기 위한 보안 패턴을 정의합니다. 자동화를 통한 실행 과정을 실행서로 구현하고, 인간이 관여하는 개입을 적절하게 문서화합니다.

고려 사항

- 각 에코시스템에 맞는 맞춤형 AWS 책임 분담 모델을 만듭니다.
- 계정의 모든 작업자에 대한 보호 체계의 일부로 강력한 인증을 사용합니다.
- 애플리케이션 팀의 보안 소유권 문화를 장려합니다.
- AWS에 서비스가 포함되도록 데이터 분류 모델을 확장합니다.
- 개발자, 운영 및 보안 팀 목표와 직무를 통합합니다.
- AWS에서 서비스를 관리하는 데 사용되는 계정을 명명 및 추적하기 위한 전략을 만듭니다.
- 팀에서 모니터링할 수 있도록 전화 및 이메일 그룹을 중앙 집중화합니다.

예방 구성 요소

AWS 보안 관점의 예방 구성 요소는 AWS를 통해 또는 조직 내부에서 보안 인프라를 구현하기 위한 지침을 제공합니다.
올바른 제어 세트 구현의 핵심은 보안 팀이 민첩하고 확장 가능한 환경인 AWS에서 엔터프라이즈를 보호하기 위해 필수적인 자동화 및 배포 기술을 구축하는 데 필요한 자신감과 역량을 갖출 수 있도록 지원하는 것입니다.

지시 구성 요소를 사용하여 필요한 제어와 지침을 결정한 다음 예방 구성 요소를 사용하여 제어를 효과적으로 운영하는 방법을 결정합니다. AWS는 제어 구현 참조로 사용할 수 있는 AWS 서비스 활용 및 워크로드 배포 패턴의 모범 사례에 대한 지침을 정기적으로 제공합니다. AWS 보안 센터, 블로그, 최신 AWS Summit 및 re:Invent 컨퍼런스 보안 추적 비디오를 참조하십시오.

다음 영역을 고려하여 현재 보안 아키텍처 및 실행에 어떤 변경이(있는 경우) 필요한지 결정하십시오. 그러면 AWS 채택 전략을 원활하고 계획적으로 추진해 나가는 데 도움이 됩니다.

- **자격 증명 및 액세스** - AWS 사용을 조직의 인력 수명 주기는 물론 인증 및 권한 부여 소스에 통합합니다. 적절한 사용자 및 그룹과 관련된 세부적인 정책 및 역할을 생성합니다. 자동화를 통해서만 중요한 변경을 허용하고, 원치 않는 변경을 방지하거나 자동으로 롤백하는 가드 레일을 생성합니다. 이 조치를 수행하면 프로덕션 시스템과 데이터에 사람이 액세스하는 빈도가 줄어듭니다.
- **인프라 보호** - 지시 구성 요소를 사용하여 확인된 필요에 맞게 트러스트 경계, 시스템 보안 구성 및 유지 관리(예: 확정 및 패치), 기타 적절한 정책 적용 지점(예: 보안 그룹, AWS WAF, Amazon API Gateway) 등의 보안 기준을 구현합니다.
- **데이터 보호** - 적절한 보안 조치를 활용하여 전송 중인 데이터와 미사용 데이터를 보호합니다. 보안 조치에는 객체에 대한 세부적인 액세스 제어, 데이터 암호화에 사용되는 암호화 키 생성 및 제어, 적절한 암호화 또는 토큰화 방법 선택, 무결성 확인, 적절한 데이터 보존 등이 포함됩니다.

고려 사항

- 보안을 코드로 처리하여 조직을 보호하기 위한 확장성과 민첩성을 갖출 수 있는 방식으로 보안 인프라를 배포하고 확인할 수 있도록 합니다.
- 가드 레일과 실제 기본값을 생성하고 템플릿과 모범 사례를 코드로 제공합니다.
- 조직에서 매우 반복적이거나 특히 민감한 보안 기능에 활용할 수 있는 보안 서비스를 구축합니다.
- 작업자를 정의한 다음 AWS 서비스와 상호 작용하는 환경에 대한 스토리보드를 작성합니다.
- AWS Trusted Advisor 도구를 사용하여 AWS 보안 태세를 지속적으로 평가하고, AWS Well Architected 검토를 고려합니다.
- 최소 요건의 보안 기준을 설정하고, 보호 중인 워크로드에 대한 보호 수준을 지속적으로 반복하여 향상합니다.

탐지 구성 요소

AWS CAF 보안 관점의 탐지 구성 요소는 조직의 보안 태세를 보다 잘 파악하기 위한 지침을 제공합니다. AWS CloudTrail, 서비스별 로그 및 API/CLI 반환 값과 같은 서비스를 사용하여 풍부한 데이터와 정보를 수집할 수 있습니다. 이러한 정보 소스를 확장 가능한 플랫폼으로 수집하여 로그 관리 및 모니터링, 이벤트 관리, 테스트, 인벤토리/감사 등에 활용하면 자신감 있는 운영 보안에 필요한 투명성과 운영 민첩성을 갖출 수 있습니다.

- **로깅 및 모니터링** - AWS는 AWS 환경에서 발생하는 사건을 거의 실시간으로 파악하기 위해 활용할 수 있는 기본 로깅 및 서비스를 제공합니다. 이러한 도구를 사용하여 기존 로깅 및 모니터링 솔루션에 통합할 수 있습니다. 보안 관련 활동의 완벽한 해결을 위해 로깅 및 모니터링 소스의 출력을 IT 조직의 워크플로우에 심층적으로 통합합니다.
- **보안 테스트** - AWS 환경을 테스트하여 정의된 보안 표준이 충족되는지 확인합니다. 테스트를 통해 특정 이벤트가 발생할 때 시스템이 예상대로 응답하는지 확인하여 실제 이벤트에 더 잘 대비할 수 있습니다. 보안 테스트의 예에는 취약성 검사, 침투 테스트, 표준을 준수하고 있음을 증명하기 위한 오류 주입 등이 있습니다. 목표는 제어가 예상대로 응답하는지 확인하는 것입니다.
- **자산 인벤토리** - 어떤 워크로드를 배포했으며 운영 중인지를 알면 보안 표준에 따라 요구되는 예상 보안 거버넌스 수준에서 환경이 작동 중인지 모니터링하고 확인할 수 있습니다.
- **변경 탐지** - 예방 제어의 보안 기준을 이용하려면 이러한 제어가 변경되는 시기도 알아야 합니다. 보안 구성과 현재 상태 간의 차이를 확인하기 위한 조치를 구현합니다.

고려 사항

- AWS 환경에서 캡처, 모니터링 및 분석할 로깅 정보를 결정합니다.
- 기존 보안 운영 센터(SOC) 비즈니스 기능이 AWS 보안 모니터링 및 관리를 기존 실행에 통합하는 방식을 결정합니다.
- 해당 AWS 절차에 따라 취약성 검사 및 침투 테스트를 지속적으로 수행합니다.

대응 구성 요소

AWS CAF 보안 관점의 대응 구성 요소는 조직의 보안 태세 중 대응 부분에 대한 지침을 제공합니다. AWS 환경을 기존 보안 태세에 통합한 다음 대응이 필요한 작업을 준비하고 시뮬레이션하면 발생하는 인시던트에 대응하기 위한 준비를 더 잘 갖출 수 있습니다.

자동화된 인시던트 대응 및 복구 기능을 갖추고 재해 복구 부분의 업무 부담을 경감하면 보안 팀이 대응보다는 과학수사 및 근본 원인을 분석하는 데 집중할 수 있습니다. 보안 태세를 조정하는 일부로 다음과 같은 몇 가지 사항을 고려해야 합니다.

- **인시던트 대응** - 인시던트 중에는 이벤트를 포함시키고 알려진 정상 상태로 돌아가는 것이 대응 계획의 중요한 요소입니다. 예를 들어, AWS Config 규칙 및 AWS Lambda 응답기 스크립트를 사용하여 해당 기능의 여러 측면을 자동화하면 인터넷 속도로 대응을 확장할 수 있습니다. 현재 인시던트 대응 프로세스를 검토하고 AWS 자산에 대해 자동화된 대응 및 복구를 운영하고 관리할지 여부 및 방법을 결정합니다. 최대한 빠르게 대응하려면 보안 운영 센터의 기능을 AWS API와 긴밀히 통합해야 합니다. 이렇게 하면 AWS 클라우드 채택을 위한 보안 모니터링 및 관리 기능이 제공됩니다.
- **보안 인시던트 대응 시뮬레이션** - 이벤트를 시뮬레이션하여 시행 중인 제어와 프로세스가 예상대로 반응하는지 확인할 수 있습니다. 이 접근 방식을 사용하면 인시던트가 발생할 때 효과적으로 복구하고 대응할 수 있는지 확인할 수 있습니다.
- **과학수사** - 대부분의 경우 기존 과학수사 도구를 AWS 환경에서도 사용할 수 있습니다. 과학수사 팀은 리전 전체에 도구를 자동으로 배포할 수 있는 기능과 Amazon Simple Storage Service(S3), Amazon Elastic Block Store(EBS), Amazon Kinesis, Amazon DynamoDB, Amazon Relational Database Service(RDS), Amazon RedShift, Amazon Elastic Compute Cloud(EC2) 등과 같이 비즈니스에 중요한 애플리케이션의 기반이 되는 강력하고 확장 가능한 서비스를 사용하여 방대한 양의 데이터를 마찰 없이 빠르게 수집할 수 있는 기능에서 이점을 얻게 됩니다.

고려 사항

- AWS 환경을 인식하도록 인시던트 대응 프로세스를 업데이트합니다.
- AWS의 서비스를 활용하여 자동화 및 기능 선택을 통해 배포를 과학수사적으로 준비합니다.
- 견고성 및 확장성을 보장할 수 있도록 대응을 자동화합니다.
- AWS의 서비스를 데이터 수집 및 분석에 사용하여 조사를 지원합니다.
- 보안 인시던트 대응 시뮬레이션을 통해 인시던트 대응 기능을 확인합니다.

전환 과정 수행 – 전략 정의

현재 보안 전략을 검토하여 전략의 각 부분이 클라우드 채택 이니셔티브의 일부로 수행되는 변경에서 이점을 얻을 수 있는지 확인합니다. 비즈니스에 허용할 수 있는 위험 수준, 규제 및 규정 준수 목표를 달성하기 위한 접근 방식, 보호해야 할 대상 및 보호할 방법에 대한 정의 등을 기준으로 AWS 클라우드 채택 전략을 매핑합니다. 표 1에 특정 이니셔티브와 작업 흐름에 매핑된 원칙 세트를 명시하는 보안 전략의 예가 나와 있습니다.

원칙	작업 예
코드형 인프라. 게이트가 아닌 가드레일을 설계합니다.	보안 팀의 코드 및 자동화 기술을 향상하고 DevSecOps로 이동합니다. 우수한 동작을 목표로 구동을 설계합니다.
클라우드를 사용하여 클라우드를 보호합니다.	클라우드에서 보안 도구를 빌드, 작동 및 관리합니다.
최신 상태를 유지하고, 안전하게 실행합니다.	새로운 보안 기능을 이용하고, 패치 및 교체를 자주 수행합니다.
지속적인 액세스 이용을 줄입니다.	역할 카탈로그를 설정하고, 비밀 서비스를 통해 KMI를 자동화합니다.
전체적인 가시성.	OS 및 앱 로그를 사용하여 AWS 로그와 메타데이터를 집계합니다.
심층 분석.	BI 및 분석을 통해 보안 데이터 웨어하우스를 구현합니다.
확장 가능한 인시던트 대응(IR).	책임 분담 프레임워크를 위해 IR 및 과학수사 표준 운영 절차(SOP)를 업데이트합니다.
자동 복구.	수정 및 알려진 정상 상태로의 복원을 자동화합니다.

표 1: 보안 전략 예

전략이 진화함에 따라 타사 보증 프레임워크 및 조직 보안 요구 사항에 따른 반복과, AWS로 전환하는 과정을 안내하는 위험 관리 프레임워크로의 통합을 시작해야 합니다. 일반적으로 효과적인 실행 방법은 클라우드에서 워크로드의 필요와 AWS에서 제공하는 보안 기능에 대한 이해 향상에 따라 규정 준수 매핑도 진화하도록 하는 것입니다.

전략의 또 한 가지 핵심 요소는 각 에코시스템에 특정한 책임 분담 모델을 매핑하는 것입니다. AWS와 공유하는 매크로 관계 외에도 내부 조직의 책임 분담과 파트너에게 배정하는 책임도 살펴봐야 합니다. 기업은 책임 분담 모델을 제어 프레임워크, RACI(책임, 해명, 자문, 정보) 모델, 위험 레지스터라는 세 가지 주요 영역으로 분류할 수 있습니다. 제어 프레임워크는 비즈니스의 보안 측면이 어떻게 작동할 것으로 예상되는지 및 위험을 관리하기 위해 어떤 제어가 시행되는지를 설명합니다. RACI를 사용하여 프레임워크에서 제어를 책임지는 사람을 식별하고 배정할 수 있습니다. 마지막으로 위험 레지스터를 사용하여 적절한 소유권이 없는 제어를 캡처합니다. 식별된 나머지 위험에 우선 순위를 지정하고, 위험을 해결하기 위해 시행되는 새로운 작업 흐름 및 이니셔티브에 맞게 위험 처리를 조정합니다.

이러한 책임 분담을 매핑하면 운영을 자동화하고 보안, 규정 준수, 위험 관리 커뮤니티에서 중요 작업자 간의 워크플로우를 개선할 새로운 가능성을 모색할 수 있습니다. 그림 2에 확장된 책임 분담 모델의 예가 나와 있습니다.

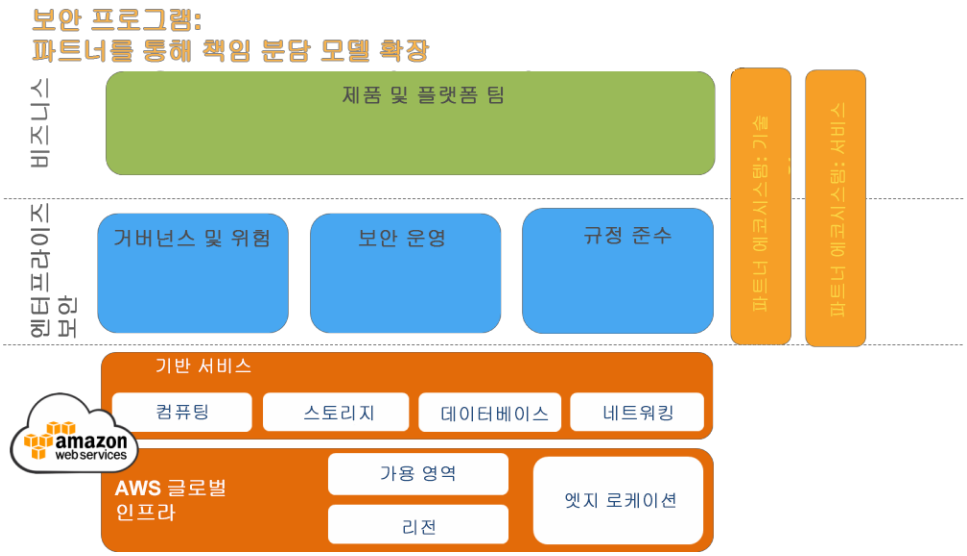

그림 2: 책임 분담 모델 예

고려 사항

- 클라우드에서 보안을 구현하기 위한 조직의 접근 방식을 다루는 맞춤형 전략을 수립합니다.
- 모든 전략의 기본 테마로 자동화를 촉진합니다.
- 먼저 클라우드에 대한 접근 방식을 명확하게 규정합니다.
- 가드 레일을 정의하여 민첩성과 유연성을 증진합니다.
- 클라우드 내 정보 보안에 대한 조직의 접근 방식을 정의하는 간단한 연습으로 전략을 실행합니다.
- 전략이 무엇인지 규정하는 동시에 신속하게 반복합니다. 목표는 핵심 작업을 추진하는 기본 원칙 세트를 설정하는 것이며, 전략은 그 자체로 끝이 아닙니다. 신속하게 행동하며 자발적으로 채택하고 진화해야 합니다.
- 특정 솔루션을 제시하는 전략보다는 보안에 이상적인 문화를 제시하고 설계 결정에 필요한 정보를 제공하는 전략적 원칙을 정의합니다.

전환 과정 수행 – 프로그램 제공

전략이 마련되면 이제 실행에 옮겨 보안 조직을 탈바꿈하고 클라우드 전환 과정을 보호하기 위한 구현을 시작합니다. 다양한 옵션과 기능을 선택할 수 있지만, 구현 작업을 장기간 지속해서는 안 됩니다. 다양한 기능이 함께 작동하는 방식을 설계하고 구현하는 이 프로세스는 새로운 작업을 빠르게 익히고 요구 사항에 가장 적합한 설계를 반복하는 방법을 학습하기 위한 기회이기도 합니다. 실제 구현에서 조기에 학습한 다음, 학습하는 동안 작은 변화를 이용하여 채택하고 진화해야 합니다.

그림 3: AWS CAF 보안 에픽

구현에 도움이 되는 CAF 보안 에픽을 사용할 수 있습니다(그림 3 참조). 보안 에픽은 스프린트 중 작업할 수 있는 사용자 사례(사용 사례 및 침해 사례) 그룹으로 구성됩니다. 이러한 각 에픽에는 점점 더 복잡해지는 요구 사항을 처리하고 견고성을 계층화하는 여러 반복이 있습니다. 민첩한 사용을 권장하지만, 다른 프레임워크를 사용하여 제공을 구조화하고 우선 순위를 지정하는 데 도움이 되는 일반적인 작업 흐름이나 주제로 에픽을 처리할 수도 있습니다. 제안되는 구조는 구현을 안내하는 다음 10가지 보안 에픽(그림 4)으로 구성됩니다.

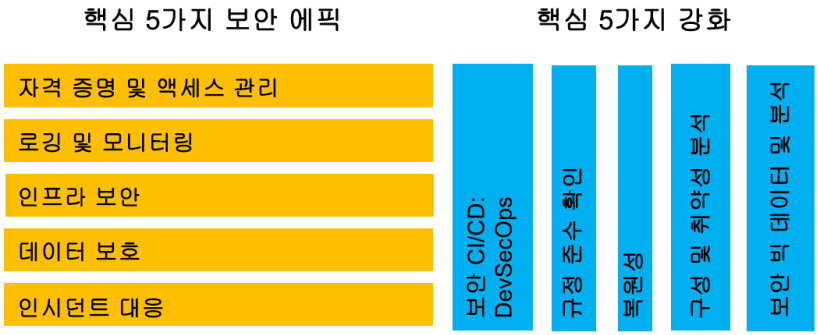

그림 4: AWS 10가지 보안 에픽

핵심 5가지

다음 5개의 에픽은 과정을 시작하기 위한 기반이므로 조기에 고려해야 하는 핵심 제어 및 기능 범주입니다.

- **IAM** — AWS Identity and Access Management(IAM)는 AWS 배포의 중추를 형성합니다. 리소스를 프로비저닝하거나 오케스트레이션하려면 먼저 클라우드에서 계정을 설정하고 권한을 부여받아야 합니다. 일반적인 자동화 사례에는 권한 매핑/부여/감사, 비밀 자료 관리, 의무와 최소 권한 액세스의 분리 적용, 적시 권한 관리, 장기 자격 증명 의존도 감소 등이 포함될 수 있습니다.

- **로깅 및 모니터링** – AWS 서비스는 플랫폼과의 상호 작용을 모니터링하는 데 도움이 되는 풍부한 로깅 데이터를 제공합니다. 구성 선택을 기반으로 한 AWS 서비스의 성능과, 공통의 참조 프레임을 생성하기 위한 OS 및 애플리케이션 로그 수집 기능도 제공합니다. 일반적인 자동화 사례에는 로그 집계, 임계값/경보/알림, 강화, 검색 플랫폼, 시각화, 이해관계자 액세스, 폐쇄형 루프 조직 대응을 시작하기 위한 워크플로우 및 티켓팅이 포함될 수 있습니다.

- **인프라 보안** – 코드형 인프라를 처리할 때 보안 인프라는 역시 코드로 배포해야 하는 첫 번째 티어 워크로드가 됩니다. 이러한 접근 방식을 통해 AWS 서비스를 프로그래밍 방식으로 구성하고 AWS Marketplace 파트너의 보안 인프라 또는 직접 설계한 솔루션을 배포할 수 있습니다. 일반적인 자동화 사례에는 각 요구 사항에 맞게 AWS 서비스를 구성하기 위한 사용자 지정 템플릿 생성, 보안 아키텍처 패턴 및 보안 작업 실행을 코드로 구현, AWS 서비스의 사용자 지정 보안 솔루션 제작, 블루/그린 배포와 같은 패치 관리 전략 사용, 노출되는 공격 영역 최소화, 배포 효과 확인 등이 포함될 수 있습니다.

- **데이터 보호** – 중요한 데이터를 보호하는 것은 정보 시스템 구축 및 운영의 중요 부분이므로 AWS는 수명 주기 전반에 걸쳐 데이터를 보호하기 위한 강력한 옵션이 포함된 서비스와 기능을 제공합니다. 일반적인 자동화 사례에는 워크로드 배치 결정, 태깅 스키마 구현, VPN 및 TLS/SSL 연결과 같이 사용 중인 데이터를 보호하기 위한 메커니즘 구성(AWS Certificate Manager 포함), 인프라의 적절한 티어에서 암호화를 통해 미사용 데이터를 보호하기 위한 메커니즘 구성, AWS Key Management Service(AWS KMS) 구현/통합 사용, AWS CloudHSM 배포, 토큰화 체계 생성, AWS Marketplace 파트너 솔루션 구현 및 운영 등이 포함될 수 있습니다.

- **인시던트 대응** – 인시던트 관리 프로세스의 여러 측면을 자동화하면 안정성이 개선되고 대응 속도가 향상되며 작업 후 검토에서 더 쉽게 평가할 수 있는 환경이 생성됩니다. 일반적인 자동화 사례에는 환경의 특정 변경에 대응하는 AWS Lambda 기능 "대응 담당자" 사용, 자동 조정 이벤트 오케스트레이션, 의심되는 시스템 구성 요소 격리, 적시 조사 도구 배포, 폐쇄형 루프 조직 대응을 종료하고 학습하기 위한 워크플로우 및 티켓팅 생성 등이 포함될 수 있습니다.

핵심 강화

이 다섯 가지 에픽은 가용성, 자동화 및 감사를 통해 지속적인 운영 우수성을 추진하는 테마를 나타냅니다. 이러한 에픽을 각 스프린트에 신중하게 통합해야 합니다. 추가 초점이 필요한 경우 에픽을 고유의 에픽으로 처리할 수 있습니다.

- **복원성** – 높은 가용성, 운영 지속성, 견고성 및 복원성, 재해 복구는 AWS를 이용하여 클라우드를 배포하는 이유입니다. 일반적인 자동화 사례에는 다중 AZ 및 다중 리전 배포 사용, 사용 가능한 공격 대상 영역 변경, 공격을 흡수하기 위한 리소스 할당 조정 및 이동, 노출된 리소스 보호, 시스템 운영 연속성을 확인하기 위한 고의적인 리소스 오류 도입 등이 포함될 수 있습니다.

- **규정 준수 확인** – 규정 준수를 보안 프로그램으로 완전히 통합하면 규정 준수가 확인란 연습이나 배포 후 발생하는 오버레이로 바뀌는 것을 방지할 수 있습니다. 이 에픽은 다른 에픽을 통해 생성된 규정 준수 아티팩트를 통합하고 합리화하는 플랫폼을 제공합니다. 일반적인 자동화 사례에는 규정 준수 요구 사항에 매핑된 보안 단위 테스트 생성, 규정 준수 증거 수집을 지원하기 위한 서비스 및 워크로드 설계, 증거 기능에서 규정 준수 알림 및 시각화 파이프라인 생성, 지속적인 모니터링, 규정 준수 도구 작성을 지향하는 DevSecOps 팀 생성 등이 포함될 수 있습니다.

- **보안 CI/CD(DevSecOps)** – 신뢰할 수 있는 확인된 지속적 통합 및 지속적 배포 도구 체인을 통해 소프트웨어 공급망에 대한 신뢰를 구축하는 것은 클라우드로 마이그레이션할 때 성숙한 보안 운영 실행을 유지하기 위한 방법입니다. 일반적인 자동화 사례에는 도구 체인 강화 및 패치 적용, 도구 체인에 대한 최소 권한 액세스, 프로덕션 프로세스의 로깅 및 모니터링, 보안 통합/배포 시각화, 코드 무결성 확인 등이 포함될 수 있습니다.

- **구성 및 취약성 분석** – 구성 및 취약성 분석은 AWS에서 제공하는 확장성, 민첩성 및 자동화에서 많은 이점을 얻을 수 있습니다. 일반적인 자동화 사례에는 AWS Config 사용 및 고객 AWS Config Rules 생성, Amazon CloudWatch 이벤트 및 AWS Lambda를 사용하여 변경 탐지에 대응, Amazon Inspector 구현, AWS Marketplace에서 지속적인 모니터링 솔루션 선택 및 배포, 트리거된 검사 배포, CI/CD 도구 체인에 평가 도구 통합 등이 포함될 수 있습니다.

- **보안 빅 데이터 및 예측 분석** - 보안 운영은 비즈니스의 다른 측면과 마찬가지로 빅 데이터 서비스 및 솔루션에서 이점을 얻습니다. 빅 데이터를 활용하면 더 시기 적절한 방식으로 더 깊이 있는 이해를 얻을 수 있으므로, 민첩성을 향상하고 확장 시 보안 태세를 반복할 수 있습니다. 일반적인 자동화 사례에는 보안 데이터 레이크 생성, 분석 파이프라인 개발, 보안 결정을 추진하기 위한 가시성 생성, 자율 대응을 위한 피드백 메커니즘 설정 등이 포함될 수 있습니다.

이 구조를 정의한 후 구현 계획을 세부적으로 작성할 수 있습니다. 시간 경과에 따른 기능 변경과 개선 기회를 지속적으로 확인합니다. 위의 테마와 기능 범주는 민첩 방법론에서 에픽으로 처리할 수 있으며 사용 사례 및 침해 사례를 포함하여 광범위한 사용자 사례가 포함됩니다. 여러 스프린트를 사용하면 비즈니스 속도 및 요구에 따라 조정할 수 있는 유연성을 유지하면서 성숙도를 향상할 수 있습니다.

스프린트 시리즈 예

다음과 같은 방법으로 단기 준비 기간을 포함하여 2주 단위의 스프린트 6개로 이루어진 샘플 세트(12주의 한 분기 동안 추진되는 에픽 그룹)를 구성합니다. 접근 방식은 최소 요건 프로덕션 기능(MVP)으로 진행할 때 리소스 가용성, 우선 순위, 각 기능에 필요한 성숙도 수준에 따라 달라집니다.

- **스프린트 0** - 보안 맵 작성: 규정 준수 매핑, 정책 매핑, 초기 위협 모델 검토, 위험 레지스트리 설정, 사용 및 침해 사례 백로그 구축, 보안 에픽 계획
- **스프린트 1** - IAM, 로깅 및 모니터링
- **스프린트 2** - IAM, 로깅 및 모니터링, 인프라 보호
- **스프린트 3** - IAM, 로깅 및 모니터링, 인프라 보호
- **스프린트 4** - IAM, 로깅 및 모니터링, 인프라 보호, 데이터 보호
- **스프린트 5** - 데이터 보호, 보안 운영 자동화, 인시던트 대응 계획/도구 작성, 복원성
- **스프린트 6** - 보안 운영 자동화, 인시던트 대응, 복원성

규정 준수 확인의 핵심 요소는 보안 및 규정 준수 단위 테스트 사례를 통해 확인을 각 스프린트에 통합한 다음 프로덕션 프로세스로 승격하는 것입니다. 명시적 규정 준수 확인 기능이 필요한 경우 해당 사용자 사례에 특히 중점을 두도록 스프린트를 설정할 수 있습니다. 시간이 경과하면 반복을 활용하여 지속적인 확인과 해당되는 경우 편차의 자동 수정 구현을 달성할 수 있습니다.

전체적인 접근 방식의 목표는 MVP 또는 기준이 무엇이며 각 영역의 첫 번째 스프린트에 무엇이 매핑되는지를 명확하게 정의하는 것입니다. 초기 단계에서는 최종 목표가 분명하게 정의되지 않을 수 있지만, 초기 스프린트의 명확한 로드맵이 생성됩니다. 타이밍, 경험 및 반복을 통해 점차 개선하여 최종 상태를 각 조직에 적합하게 조정할 수 있습니다. 실제로 최종 상태는 계속 변할 수 있지만 결국 프로세스는 점점 더 빠른 속도로 지속적인 개선으로 이어집니다. 이 접근 방식은 장기 일정과 높은 자본 지출을 기반으로 하는 빅뱅 접근 방식보다 더 효과적이고 더 경제적일 수 있습니다.

약간 더 깊이 있게 살펴본다면, IAM의 첫 번째 스프린트는 계정 구조 정의 및 핵심 모범 사례 세트 구현으로 구성될 수 있습니다. 두 번째 스프린트는 연동을 구현할 수 있습니다. 세 번째 스프린트는 여러 계정에 맞게 계정 관리를 확장할 수 있습니다. 이러한 초기 스프린트 하나 이상에 걸쳐 진행될 수 있는 IAM 사용자 사례에는 다음과 같은 사례가 포함될 수 있습니다.

"액세스 관리자로서, 권한 있는 액세스와 연동 자격 증명 제공자 신뢰 관계를 관리하기 위한 초기 사용자 세트를 생성하려고 합니다."

"액세스 관리자로서, 기존 기업 디렉터리에 있는 사용자를 AWS 플랫폼의 기능 역할 또는 액세스 권한 세트에 매핑하려고 합니다."

"액세스 관리자로서, 대화형 사용자가 AWS 콘솔을 통해 수행하는 모든 상호 작용에 멀티 팩터 인증을 적용하려고 합니다."

이 예에서 다음과 같은 로깅 및 모니터링 사용자 사례는 하나 이상의 초기 스프린트에 걸쳐 진행될 수 있습니다.

"보안 운영 분석가로서, 모든 AWS 리전 및 AWS 계정에 대해 플랫폼 수준의 로깅을 수신하려고 합니다."

"보안 운영 분석가로서, 모든 플랫폼 수준 로그가 모든 AWS 리전 및 계정에서 하나의 공유 위치로 전달되도록 하려고 합니다."

"보안 운영 분석가로서, IAM 정책을 사용자, 그룹 또는 역할에 연결하는 작업에 대해 알림을 수신하려고 합니다."

기능을 병렬 또는 직렬 방식으로 빌드하고 보안 기능 사용자 사례를 전체 제품 백로그에 포함시켜 유연성을 유지할 수 있습니다. 또한 사용자 사례를 보안 중심의 DevOps 팀으로 분할할 수도 있습니다. 이러한 결정을 정기적으로 다시 검토하여 시간 경과에 따라 조직의 필요에 맞게 제공을 조정할 수 있습니다.

고려 사항

- 기존 제어 프레임워크를 검토하여 필수 보안 표준을 충족할 수 있도록 AWS 서비스를 운영할 방법을 결정합니다.
- 작업자를 정의한 다음 AWS 서비스와 상호 작용하는 환경에 대한 스토리보드를 작성합니다.
- 첫 번째 스프린트와 초기의 상위 수준 장기 목표를 정의합니다.
- 최소 요건의 보안 기준을 설정하고, 보호 중인 워크로드와 데이터에 대한 보호 수준을 지속적으로 반복하여 향상합니다.

전환 과정 수행 – 강력한 보안 운영 개발

인프라가 코드인 환경에서는 보안을 코드로 처리해야 합니다. 보안 운영 구성 요소는 보안의 근본 원리를 코드로 전달하고 운용하기 위한 방법을 제공합니다.

- 클라우드를 사용하여 클라우드를 보호합니다.
- 보안 인프라는 클라우드 인식형이어야 합니다.
- API를 사용하여 보안 기능을 서비스로 노출합니다.
- 보안 및 규정 준수를 확장할 수 있도록 모든 기능을 자동화합니다.

이러한 거버넌스 모델을 실용화하기 위해 사업 부문은 주로 DevOps 팀을 구성하여 인프라 및 비즈니스 소프트웨어를 빌드하고 배포합니다. 보안을 DevOps 문화 또는 실행(DevSecOps라고도 함)에 통합하여 거버넌스 모델의 핵심 원리를 확장할 수 있습니다. 다음 원칙을 중심으로 팀을 구성합니다.

- 보안 팀은 DevOps 문화 및 행동을 수용합니다.
- 개발자는 보안 운영을 자동화하기 위해 사용되는 코드에 공개적으로 기여합니다.
- 보안 운영 팀에 애플리케이션 코드의 테스트 및 자동화에 참여할 권한을 부여합니다.
- 팀은 빠르고 빈번한 배포를 보장합니다. 더 작게 변경하여 더 빈번하게 배포하면 운영 위험을 줄이고 보안 전략을 신속하게 진행할 수 있습니다.

통합 개발, 보안 및 운영 팀은 다음과 같은 세 가지 핵심 임무를 공유합니다.

- 지속적인 통합/지속적인 배포 도구 체인을 강화합니다.
- 도구 체인을 통과하는 동안 복원성 있는 소프트웨어 개발을 지원하고 증진합니다.
- 도구 체인을 통해 모든 보안 인프라 및 소프트웨어를 배포합니다.

최신 보안 사례에 따라 변경(있는 경우)을 결정하면 원활한 AWS 채택 전략을 계획하는 데 도움이 됩니다.

결론

AWS 채택 과정을 시작할 때는 각 환경의 AWS 부분을 포함하도록 보안 태세를 업데이트해야 합니다. 이 보안 관점 백서는 AWS에서 운영할 경우 보안 태세에 제공되는 이점을 활용하기 위한 접근 방식을 규범적으로 안내합니다. AWS 웹 사이트에서 훨씬 더 많은 보안 정보를 확인할 수 있습니다. 이 사이트에는 보안 기능에 대한 자세한 설명과 일반적인 구현을 위한 더 세부적인 규범적 지침이 나와 있습니다. AWS 채택 이니셔티브를 준비할 때 보안 팀의 다양한 구성원이 검토해야 할 포괄적인 보안 중심 콘텐츠 목록[4]도 준비되어 있습니다.

부록 A: AWS CAF 보안 관점 전반에서 진행 상황 추적

이 부록에서 논의하는 핵심 보안 프로그램과 보안 에픽 진행 모델을 사용하여 AWS CAF 보안 관점의 구현 진행 상황과 성숙도를 평가할 수 있습니다. 프로그램과 진행 모델을 프로젝트 계획에 사용하여 구현의 견고성을 평가하거나 단순히 앞으로의 방향에 대한 대화를 추진하기 위한 수단으로 사용할 수도 있습니다.

핵심 보안 프로그램

핵심 보안 프로그램은 올바른 궤도를 유지하는 데 도움이 되는 이정표입니다. 여기서는 미처리, 처리 중, 완료라는 세 가지 값으로 구성된 평가 모델을 사용합니다.

- 클라우드 보안 전략 [미처리, 처리 중, 완료]
- 이해관계자 통신 계획 [미처리, 처리 중, 완료]
- 보안 맵 작성 [미처리, 처리 중, 완료]
- 책임 분담 모델 문서화 [미처리, 처리 중, 완료]
- 보안 운영 지침 및 실행서 [미처리, 처리 중, 완료]
- 보안 에픽 계획 [미처리, 처리 중, 완료]
- 보안 인시던트 대응 시뮬레이션 [미처리, 처리 중, 완료]

보안 에픽 진행 모델

보안 에픽 진행 모델은 이 문서에서 설명한 10가지 보안 에픽 구현의 진행 상황을 평가하는 데 도움이 됩니다. 0(영)부터 3까지의 평가 모델을 사용하여 견고성을 평가합니다. 자격 증명 및 액세스 관리 에픽과 로깅 및 모니터링 에픽에 대한 예를 제공했으므로 이 진행이 어떻게 작동하는지를 볼 수 있었습니다.

핵심 5가지 보안 에픽

0- 처리되지 않음

1- 아키텍처 및 계획에서 처리됨

2- 최소 요건 구현

3- 엔터프라이즈 준비 프로덕션 구현

보안 에픽	0	1	2	3
ID 및 액세스 관리	예: 온프레미스와 AWS 자격 증명 간에 관계가 없습니다.	예: 인력 수명 주기 자격 증명 관리에 대한 접근 방식이 정의됩니다. IAM 아키텍처가 문서화됩니다. 직무가 IAM 정책 필요에 매핑됩니다.	예: 아키텍처에서 정의한 대로 IAM을 구현했습니다. 일부 직무에 매핑되는 IAM 정책을 구현했습니다. IAM 구현이 확인되었습니다.	예: IAM 수명 주기 워크플로우의 자동화.
로깅 및 모니터링	예: AWS를 활용하여 로깅 및 모니터링 솔루션을 제공하지 않았습니다.	예: 로그 집계, 모니터링, 보안 이벤트 관리 프로세스로의 통합을 위한 접근 방식이 정의됩니다.	예: 플랫폼 수준 및 서비스 수준 로깅이 활성화되고 중앙 집중화됩니다.	예: 보안 관련 이벤트가 보안 워크플로우와 인시던트 관리 프로세스 및 시스템에 심층적으로 통합됩니다.
인프라 보안				
데이터 보호				
인시던트 관리				

핵심 5가지 강화

0- 처리되지 않음

1- 아키텍처 및 계획에서 처리됨

2- 최소 요건 구현

3- 엔터프라이즈 준비 프로덕션 구현

보안 에픽	0	1	2	3
복원성				
DevSecOps				
규정 준수 확인				
구성 및 취약성 관리				
보안 빅 데이터				

CAF 분류 및 용어

클라우드 채택 프레임워크(CAF)는 AWS가 이전의 고객 참여에서 얻은 지침과 모범 사례를 캡처하기 위해 만든 프레임워크입니다. AWS CAF *관점*은 조직 내 클라우드 기반 IT 시스템 구현과 관련된 중점 영역을 나타냅니다. 예를 들어, 보안 관점은 AWS 환경으로 이동할 때 기존 보안 제어를 평가하고 강화하기 위한 지침과 프로세스를 제공합니다.

각 CAF 관점은 구성 요소 및 활동으로 구성됩니다. *구성 요소*는 주의해야 할 특정 측면을 나타내는 관점의 하위 영역입니다. 이 백서에서는 보안 관점의 구성 요소를 살펴봅니다. *활동*은 조직이 클라우드로 이동하여 클라우드 기반 솔루션을 지속적으로 운영하기 위해 사용할 수 있는 실행 가능한 계획을 수립하기 위한 규범적 지침을 추가로 제공합니다.

예를 들어, *지시*는 보안 관점의 구성 요소 중 하나이며, 각 에코시스템에 맞게 AWS 책임 분담 모델을 조정하는 작업이 해당 구성 요소 내의 활동일 수 있습니다.

클라우드 채택 프레임워크(CAF)와 클라우드 채택 방법론(CAM)을 결합하여 AWS 클라우드로 전환하는 과정에서 지침으로 사용할 수 있습니다.

참고

[1] https://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

[2] https://aws.amazon.com/compliance/

[3] https://aws.amazon.com/compliance/shared-responsibility-model/

[4] https://aws.amazon.com/security/security-resources/