AWS Security by Design

소개

AWS 기반 보안, 규정 준수 및 감사 자동화

솔루션

2015년 10월

고지 사항

이 문서는 정보 제공 목적으로만 제공됩니다. 본 문서의 발행일 당시 AWS의 현재 제품 및 관행을 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

Security by Design(SbD)은 고객이 AWS 계정 설계를 정형화하고, 보안 제어를 자동화하고, 감사를 간소화하도록 해주는 보안 보장 접근법입니다.

본 백서에서는 Security by Design의 개념을 설명하고, 여러 산업계에 대규모의 보안 및 규정 준수를 유지하기 위한 4단계 접근법을 소개하며, AWS 고객이 AWS 환경에 보안을 적용하는 데 사용할 수 있는 리소스에 대해 알아보고, 제어가 작동 중인지 확인하는 방법에 대해 소개합니다.

서문

SbD는 여러 산업계, 표준 및 보안 기준 전체에서 대규모의 보안 및 규정 준수를 유지하기 위한 4단계 접근법을 포괄합니다. 보안 감사가 과거 소급적으로 적용하는 반면, SbD는 AWS IT 관리 프로세스 전체에서 보안 제어를 선제적으로 구축할 수 있는 기능을 제공하는, 체계적인 보안 보장 접근법입니다.

SbD는 여러 산업계, 표준 및 보안 기준 전체에서 대규모의 보안 및 규정 준수를 유지하기 위한 4단계 접근법을 포괄합니다. AWS SbD는 AWS 고객 환경 내에 있는 모든 것에 대한 보안을 설계함으로써 모든 단계에서 보안 및 규정 준수 기능을 설계하는 것입니다. 여기에는 권한관리, 로깅, 허가된 머신 이미지 사용강제, 신뢰 관계, 변경 이력관리, 암호화 적용 등이 포함됩니다. SbD를 사용하면 고객이 AWS 계정의 프런트 엔드 구조를 자동화하여 계정에 보안 및 규정 기준을 안정적으로 적용할 수 있습니다.

AWS 환경에서의 보안

AWS 인프라는 고객 개인 정보 및 분리와 관련하여 강력한 보안을 수행하면서도 가장 높은 수준의 가용성을 제공하도록 설계되었습니다. AWS 클라우드에서 시스템을 배포할 때는 AWS 및 고객이 보안 책임을 공동으로 부담합니다. AWS는 기반 인프라에 대한 보안을 담당하는 반면, 사용자는 AWS에 배포된 IT 리소스에 대한 보안을 담당합니다.

AWS를 사용하면 관리자의 시스템 사용을 간소화하고 AWS 환경의 감사를 보다 단순화 및 보안함으로써 고객 플랫폼에서 보안 제어 적용을 정형화할 수 있습니다.

AWS 보안에는 다음과 같은 두 가지 측면이 있습니다.

> AWS 환경에서의 보안. 보안에 구축하여 사용할 수 있는 구성 및 기능이 AWS 계정 자체에 들어 있습니다. 자격 증명, 로깅 기능, 암호화 기능, 시스템 사용 및 네트워크 설정 규칙은 모두 사용자가 관리하는 AWS 환경에 이미 들어 있습니다.
>
> 호스트 및 애플리케이션의 보안. 운영 체제, 디스크에 저장된 데이터베이스 및 고객이 관리하는 애플리케이션에도 보안 설정이 필요합니다. 이는 AWS 고객이 관리하기 나름입니다. 고객이 오늘날 온프레미스 환경에서 사용하는 보안 프로세스, 도구 및 기술은 모두 AWS에도 들어 있습니다.

여기에서 설명하는 Security by Design 접근법은 주로 AWS 환경에 적용됩니다. AWS 클라우드 작동에 대해 중앙 액세스, 가시성 및 투명성을 제공하여 AWS의 모든 서비스, 데이터 및 애플리케이션에 대해 완벽한 보안을 설계할 수 있는 가능성을 높여줍니다.

Security by Design: 개요

SbD를 사용하면 고객이 기본 구조를 자동화하여 AWS 환경의 보안 및 규정 준수를 안정적으로 개발할 수 있으므로 과거 항목을 제어하는 IT에 대해 규정 준수에 맞지 않는 항목을 적발하기 쉽습니다. 보안에 대한 클라우드 인프라 접근법에 보안 되고 반복 가능한 접근법을 만듦으로써 고객은 특정 인프라 제어 요소를 캡처, 보호 및 제어할 수 있습니다. 이러한 요소는 AWS Identify and Access Management(IAM), AWS Key Management Services(KMS) 및 AWS CloudTrail의 설계를 사전 정의하고 제한하는 등, IT 요소의 보안 규정 준수 프로세스 구축을 가능케 합니다.

SbD는 Quality by Design(QbD)의 일반 개념을 동일하게 계승합니다. Quality by Design은 품질 전문가인 Joseph M. Juran이 *Juran on Quality by Design*에서 처음으로 설명한 개념입니다. 품질 및 혁신을 염두한 설계는 Juran Trilogy의 3가지 보편적인 프로세스 중 하나로, 여기서 Juran은 새 제품, 서비스 및 프로세스에서 돌파구를 찾는 데 필요한 항목에 대해 설명합니다. QbD 접근법으로 이동하는 제조업체들은 주로, 사후 품질 확인을 주요 품질 제어 방법으로 사용하던 방식에서 제조 프로세스상에서 품질이 *기본적으로* 보장되도록 하는 방식으로 전환합니다.

QbD 개념과 마찬가지로, Security by Design은 시스템 설계를 통해 안정적인 방식으로 계획, 실행 및 유지 관리될 수 있으며, AWS의 기술 구축 역사를 통틀어 확장 가능하고 안정적인 실시간 보안을 보장합니다. 보안과 관련된 현재 문제만을 해결하는 데 급급한 감사 기능에 의존하는 것은 안정적이거나 확장 가능한 방식이 아닙니다.

Security by Design 접근법

SbD에는 AWS에서 실행되는 애플리케이션, 서비스, 운영 체제 및 AWS 인프라용으로 구현된 보안 제어의 조작화 및 감사, 기초 제어 자동화, 상속 기능 등이 들어 있습니다. 이 표준화되고, 자동화되고, 반복할 수 있는 아키텍처는 일반 사용 사례, 보안 표준 및 감사 요구 사항용으로 여러 산업계 및 워크로드에 대해 배포될 수 있습니다.

다음의 4단계 접근법을 따라 AWS 계정에 보안 및 규정 준수를 구축하는 것이 좋습니다.

- **1단계 – 요구 사항 확인.** 정책에 대해 간략히 설명하고, AWS에서 상속한 제어를 문서화하고, AWS 환경에서 소유하고 동작하는 제어를 문서화하여, AWS IT 환경에서 적용하고자 하는 보안 규칙을 결정합니다.

- **2단계 – 요구 사항 및 구현 조건에 맞는 "골드 환경" 구축.** 암호화 요구 사항(S3 객체에 대해 서버 측 암호화 설정), 리소스에 대한 권한(특정 환경에 적용할 역할), 허가할 컴퓨팅 이미지(허가한 서버의 골드 이미지 기반) 및 설정해야 하는 로깅 종류(사용할 수 있는 모든 리소스에 CloudTrail 사용 설정 등)와 같은 AWS 구성 값 양식으로 필요한 구성을 정의합니다. AWS는 구성 옵션의 완전한 세트(정기적으로 릴리스되고 있는 새로운 서비스 포함)를 제공하므로, 사용자의 고유 환경에서 활용할 수 있는 일부 템플릿이 제공됩니다. 이러한 보안 템플릿(AWS CloudFormation 템플릿 형식)에는 시스템적으로 설정할 수 있는 보다 포괄적인 규칙 세트가 들어 있습니다. AWS는 여러 보안 프레임워크(예: FISMA, PCI, HIPAA, FFIEC 및 CJIS)를 준수하는 보안 규칙을 제공하는 템플릿을 개발하였습니다. 이 사전 패키징된 산업별 템플릿 솔루션은 “AWS GoldBase 템플릿”이라는 템플릿 모음으로 고객에게 제공됩니다.

  “골드 환경”을 만드는 방법에 대한 추가 정보는 AWS 숙련 아키텍트, AWS 전문가 서비스 및 파트너의 IT 전환 리더 등으로부터 얻을 수 있습니다. 이러한 팀은 사용자 측 직원과 함께 작업하고 팀을 감사함으로써 타사 감사를 지원하면서 고품질 보안 고객 환경을 제공하는 데 중점을 둡니다.

- **3단계 – 템플릿 사용 설정.** 서비스 카탈로그를 설정하고 카탈로그에 템플릿을 사용하도록 설정합니다. 이 단계는 신규 구축 환경에 "골드 환경"을 사용하도록 설정하고, "골드 환경" 보안 규칙에 맞지 않는 환경은 만들 수 없도록 하는 단계입니다. 이렇게 하면 제어의 나머지 고객 계정 보안 구성을 효과적으로 조작할 수 있으므로 감사에 대비할 수 있습니다.

- **4단계 – 검증 작업 수행.** 서비스 카탈로그 및 "골드 환경" 템플릿을 통해 AWS를 구축하면 감사 대비 환경이 만들어집니다. 템플릿에서 정의한 규칙을 감사 지침으로 사용할 수 있습니다. AWS Config를 사용하면 환경의 현재 상태를 캡처할 수 있으며, 그런 다음 사용자의 "골드 환경" 규칙과 비교해 볼 수 있습니다. 또한, 보안된 "읽기 액세스" 권한을 통해 감사 증거 수집 기능과, 증거 모음을 자동으로 감사하는 고유 스크립트를 함께 제공합니다. 고객은 기존의 수동 관리 제어체계로부터, 설계 및 범위 지정이 제대로 된다면, 제어가 언제나 100% 작동하는(기존 감사방식은 샘플링 방식이나 특정 시점 검토 방식을 사용하는 것과 비교하면) 기술적으로 진보된 수준의 제어환경으로 전환할 수 있습니다.

이러한 기술적 감사는 사전 감사 지침, 고객 감사자에 대한 지원 및 교육에 의해 개선될 수 있으므로 감사 담당자가 AWS 클라우드가 제공하는 고유한 감사 자동화 기능을 이해하고 있어야 합니다.

Security by Design의 결과

SbD 아키텍처는 다음과 같은 목표를 달성하도록 만들어졌습니다.

- 수정 권한이 없는 사용자가 재정의할 수 없는 강제 기능 생성.
- 안정적인 제어 작업 구축.
- 지속적인 실시간 감사 가능.
- 거버넌스 정책을 스크립팅하는 기술.

이에 따라 고객의 보안 보장, 거버넌스, 보안 및 규정 준수 기능을 갖춘 자동화된 환경이 탄생하였습니다. 고객은 이제 이전에 작성한 정책, 표준 및 규정을 안정적으로 구현할 수 있게 되었습니다. 강제로 적용할 수 있는 보안 및 규정 준수를 만들 수 있으므로 AWS 고객 환경에 대한 기능적으로 안정된 거버넌스 모델을 만들 수 있습니다.

SbD 접근법 세부 사항

1단계 – 요구 사항 확인

먼저 보안 제어 합리화 작업을 수행합니다. 현재 고객 아키텍처에 최적화되어 운영중인 제어를 식별하고, 기존 AWS 인증내역,, 승인 및 보고서로 부터도 참조할 내역을 식별하여 보안 Controls Implementation Matrix(CIM)를 생성할 수 있습니다. 이는 보안 요구 사항과 상관없이 모든 AWS 환경에서 구현되어야 합니다. 이 단계를 마치면 고객 특정 맵(예: AWS Control Framework)이 만들어져 AWS 서비스 전반에서 대규모로 보안 및 규정 준수를 구축할 수 있는 보안 설정 방법이 제공됩니다.

CIM을 통해 기능 및 리소스를 특정 보안 제어 요구 사항에 매핑할 수 있습니다. 보안, 규정 준수 및 감사 담당자는 이러한 문서를 참조하여 AWS의 자격 및 승인 시스템을 보다 효율적으로 개선할 수 있습니다. 이 매트릭스에는 AWS 고객 환경에 대한 보안 제어 "위험 완화" 조건을 만족하는 제어 구현 참조 아키텍처 및 증거 예제가 들어 있습니다.

Control	Title	Type	Implementation
AC-2 (1)	Automated System Account Management	System Specific	The IAM service supports management of users and user permissions at the infrastructure layer and provides: Central control of users and security credentials, user access, and user capabilities to create and manage AWS resources.
AC-2 (2)	Removal Of Temporary / Emergency Accounts	System Specific	IAM supports the capability to grant temporary security credentials with a defined expiration for access to AWS resources. Refer to the Temporary Credentials Guide. http://docs.aws.amazon.com/STS/latest/UsingSTS/Welcome.html
AC-2 (4)	Automated Audit Actions	System Specific	In this architecture, S3 bucket logging is enabled on the developer bucket. CloudTrail logging of all API activity is enabled.
AC-2.a	Account Management	System Specific	In this architecture, the following IAM groups are available to support common infrastructure personnel functions : ISSOadmin, ISSOreadonly, SysAdmin, SecurityAnalysts.
AC-2.c	Account Management	System Specific	In this architecture, the ISSOadmin and SysAdmin groups are for various levels of

그림 1: NIST SP 800-53 버전 4 제어 보안 제어 매트릭스

- ### 제공되는 보안 서비스(상속)
  고객은 자신의 업계 및 AWS 관련 자격증, 증명 및/또는 보고서(예: PCI, FedRAMP, ISO 등)를 기반으로 AWS에서 보안 제어 요소를 참조 및 상속할 수 있습니다. 제어 상속성은 AWS에서 제공하는 자격증 및 보고서에 따라 달라질 수 있습니다.
- ### 양자간 서비스 보안(공유)
  양자간 서비스 보안 제어는 AWS 및 고객 모두가 호스트 운영 체제와 게스트 운영 체제 내에서 구현하는 제어를 말합니다. 이러한 제어에는 기술적, 운영적 및 관리적(예: IAM, 보안 그룹, 구성 관리 등) 제어가 포함되는데, 경우에 따라 부분적으로 상속(예: 내결함성)될 수도 있습니다. 예: AWS는 각 리전 내의 여러 가용 영역뿐 아니라 여러 지리적 리전 내에 데이터 센터를 구축하여 시스템 사고 시 최대의 안정성을 제공합니다. 고객은 고객의 고유한 내결함성 요구 사항을 만족하기 위해 분리된 가용 영역을 아키텍처함으로써 이러한 기능을 활용할 수 있습니다.
- ### 서비스 특정 보안(고객)
  고객 제어는 자신이 AWS에 구축하는 시스템 및 서비스를 기반으로 이루어질 수 있습니다. 또한, IAM, 보안 그룹 및 정의된 구성 관리 프로세스와 같은 여러 양자간 서비스 제어를 활용할 수도 있습니다.
- ### 최적화 IAM, 네트워크 및 운영 체제(OS) 제어
  이 제어는 조직이 선도 보안 모범 사례, 업계 요구 사항 및/또는 보안 표준을 기반으로 구축해야 하는 보안 제어 구현 또는 보안 개선 사항입니다. 일반적으로 여러 표준 및 서비스를 아우르는 이러한 제어는 AWS CloudFormation 템플릿 및 서비스 카탈로그를 사용하여, 정의된 "골드 환경"의 일부로 스크립팅될 수 있습니다.

2단계 – "골드 환경" 구축

이 단계는 사용자가 AWS가 제공하는 광범위한 보안 및 감사 서비스와 기능을 서로 연결하고, 보안, 규정 준수 및 감사 담당자에게 보안 및 규정 준수 환경을 구성하는 간단한 방법을 제공하도록 해줍니다. 이를 통해 환경을 보다 안전하고 감사 가능한 상태로 만드는 방식으로 서비스를 조정할 수 있습니다.

- ### 액세스 관리
  사용자, 그룹 및 역할을 만들고(개발자, 테스터 또는 관리자처럼) 이들에게 AWS 클라우드 리소스에 액세스하는 고유의 자격 증명을 제공합니다.

- ## 네트워크 분할
  클라우드에 서브넷을 설정하여 다른 환경으로부터 격리해야 하는 환경을 분리합니다. 예를 들어 개발 환경을 생산 환경으로부터 분리한 다음, 네트워크 ACL을 구성하여 이들 간에 트래픽을 라우팅하는 방법을 제어해야 하는 경우 사용할 수 있습니다. 고객은 또한 개별 관리 환경을 설정하여 생산 리소스에 대한 직접 액세스를 제한하는 용도로 접속 호스트를 사용하여 보안 무결성을 보장할 수 있습니다.

- ## 리소스 제약 조건 및 모니터링
  최신 보안 패치와 함께 Amazon Elastic Compute Cloud(EC2) 인스턴스 사용과 관련된 보안 강화 게스트 운영 체제 및 서비스를 확립하고, 데이터 백업을 수행하고, 백신 및 침입 감지 도구를 설치합니다. 모니터링, 로깅 및 알림 경보를 구축합니다.

- ## 데이터 암호화
  클라우드에 데이터나 객체가 저장되어 있을 때 이를 업로드하기 전에 클라우드 측이나 클라이언트 측에서 자동적으로 암호화합니다.

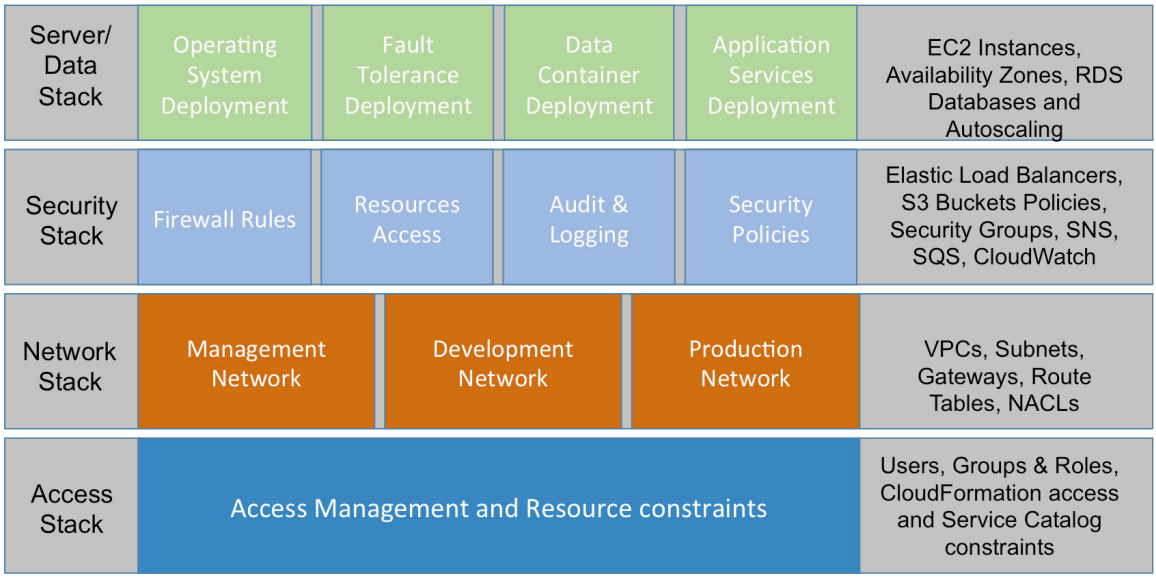

그림 3: AWS 자동화(예: CloudFormation)

AWS GoldBase 소개

AWS GoldBase는 특정 보안/규정 준수 요구 사항 내에서 사전 점검되고 자동화된 참조 아키텍처를 제공합니다. 관련 예가 다음 섹션에 나열되어 있습니다. AWS 기반 애플리케이션 구축의 의미에서, 규정 준수는 보안되고 가용성 있고 확장 가능한 기술 개념을 포함합니다. 이러한 설계는 모듈성 기능을 제공하여 필요 시 서브셋을 구축하도록 해줍니다. 또한, 여러 사용 사례에 대해 템플릿을 재사용할 수 있도록 해줍니다. AWS GoldBase *사용 사례 패키지*는 기준 CloudFormation 템플릿으로 구성되는데, 사용자는 이를 고객 환경 내 배포용으로 사용자 지정할 수 있습니다.

AWS GoldBase 리소스 패키지에는 다음이 포함됩니다.

- 보안 제어 구현 매트릭스 설명서
- 아키텍처 다이어그램
- AWS CloudFormation 템플릿
- 산업 규정 준수 템플릿(PCI, NIST 800-53, HIPAA, FFIEC 및 CJIS)
- 사용 설명서 및 구축 지침

자세한 내용은 "AWS GoldBase 소개" 백서 또는 "GoldBase 구현 설명서"를 참조하십시오.

3단계 – 템플릿 사용 설정

"골드 환경"을 만든 후에는 AWS에서 이를 사용할 수 있도록 설정해야 합니다. 서비스 카탈로그를 설정하여 이를 수행할 수 있습니다. 서비스 카탈로그를 설정하면 계정에 액세스하는 모든 사용자가 만들어진 CloudFormation 템플릿을 사용하여 자신의 환경을 만들어야 합니다. 사용자가 환경을 사용할 때마다 이러한 "골드 환경" 규칙이 모두 적용됩니다. 이렇게 하면 제어의 나머지 고객 계정 보안 구성을 효과적으로 조작할 수 있으므로 감사에 대비할 수 있습니다.

4단계 – 검증 작업 수행

이 단계의 목표는 AWS 고객이 일반적으로 용인되는 공공 감사 표준을 기준으로 독립적인 감사를 지원할 수 있도록 하는 것입니다. 감사 표준은 AWS 고객 환경 내에서 구축된 시스템을 감사할 때 달성해야 할 감사 품질 및 목표 수치를 제공합니다.

AWS는 규정을 준수하지 않는 인스턴스가 실제로 있는지 여부를 감지하는 도구를 제공합니다. AWS Config는 아키텍처의 현재 시점 설정정보를 제공합니다. AWS Config Rules를 활용할 수도 있는데, 이는 환경 간 제어의 스위핑 확인을 실행하기 위한 허용 조건으로 골드 환경을 사용하도록 강제할 수 있습니다. 이를 통해 암호화하지 않는 사용자, 인터넷에 포트를 공개한 사용자, VPC 외부에 데이터베이스가 있는 사용자를 감지할 수 있습니다. AWS 환경에 있는 모든 AWS 리소스의 측정 가능 특성은 모두 확인할 수 있습니다.

스위핑 감사 기능은 처음에 골드 환경을 기반으로 설정되지 않은 AWS 계정에서 작업하는 경우 특히 유용합니다. 또한, 골드 환경을 통해 만들었든 아니든 만들어진 방식과 상관없이 전체 계정을 확인하도록 해줍니다. AWS Config Rules를 사용하면 이를 지속적으로 모니터할 수 있으며 규정을 준수하고 있는 IT 리소스 및 그렇지 않은 IT 리소스가 항상 콘솔에 표시됩니다. 또한, 아주 잠깐 동안이더라도 사용자가 규정을 준수하고 있지 않은 경우 이를 알려줍니다. 이렇게 되면 특정 시점 및 특정 기간 감사가 매우 효과적이 됩니다.

산업 종류에 따라 감사 절차가 다르므로 AWS 고객은 산업 종류별로 제공되는 감사 지침을 검토해야 합니다. 가능한 경우 "클라우드를 잘아는" 감사 조직에 문의하여 AWS에서 제공하는 고유한 감사 자동화 기능을 이해하는 것이 좋습니다. 감사자에게 AWS 리소스 감사 경험이 있는지를 확인하고, 없는 경우 AWS에서 강의식 수업(6시간 소요, 실습 포함)을 통해 AWS 서비스 감사 방법에 대한 여러 가지 교육 옵션을 제공하고 있습니다. 자세한 내용은 awsaudittraining@amazon.com에 문의하십시오.

또한, AWS는 보안된 읽기 액세스를 통해 여러 감사 증거 수집 기능과 증거 모음을 자동으로 감사하는 고유 API(Application Programming Interface) 스크립트를 함께 제공합니다. 이를 통해 감사자는 샘플링 방법으로 테스트할 때와 비교해 100% 감사 테스팅을 수행할 수 있습니다.

SbD: 시작하는 방법

다음은 사용자 및 사용자 팀이 빠르게 시작하도록 지원하는 몇 가지 기초 리소스입니다.

- "Auditing your AWS Architecture"에서 자습형 교육을 수강합니다. 이 교육은 감사자 및 보안 제어 소유자에게 특히 유용한 구성 옵션을 비롯하여 AWS 기능 및 인터페이스를 손에 익힐 수 있게 해줍니다.
- "AWS GoldBase 소개" 백서를 읽고 자신이 사용할 수 있는 업계 템플릿을 이해합니다.
- 자신의 환경에서 템플릿을 수정, 문서화 및 구현하는 방법에 대한 자세한 지침을 솔루션 아키텍트나 계정 담당자에게 문의합니다.
- 다음과 같이 사용자에게 제공되는 추가 관련 리소스를 참조합니다.
    - Amazon Web Services: 보안 프로세스 개요
    - AWS 사용 감사에 대한 소개 백서
    - Federal Financial Institutions Examination Council(FFIEC) – 감사 설명서
    - SEC – 사이버 보안 이니셔티브 감사 설명서
    - CJIS 보안 정책 감사 설명서

참고 문헌

- AWS 규정 준수 센터: http://aws.amazon.com/compliance
- AWS Security by Design: http://aws.amazon.com/compliance/security-by-design
- AWS Security by Design 백서: https://do.awsstatic.com/whitepapers/compliance/Intro_to_Security_by Design.pdf
- AWS 보안 센터: http://aws.amazon.com/security
- FedRAMP FAQ: http://aws.amazon.com/compliance/fedramp
- 위험 및 규정 준수 백서: https://do.awsstatic.com/whitepapers/compliance/AWS_Risk_and_ Compliance_Whitepaper.pdf
- 보안 모범 사례 백서: https://do.awsstatic.com/whitepapers/aws-security-best-practices.pdf
- AWS 제품 개요: http://aws.amazon.com/products/
- AWS 영업 및 비즈니스 개발: https://aws.amazon.com/compliance/contact/
- AWS에서의 정부 및 교육 기관 https://aws.amazon.com/government-education/
- AWS Professional Services https://aws.amazon.com/professional-services