AWS Security 5 EPICs

박병화
Security Consultant
AWS Professional Services

AWS Professional Services

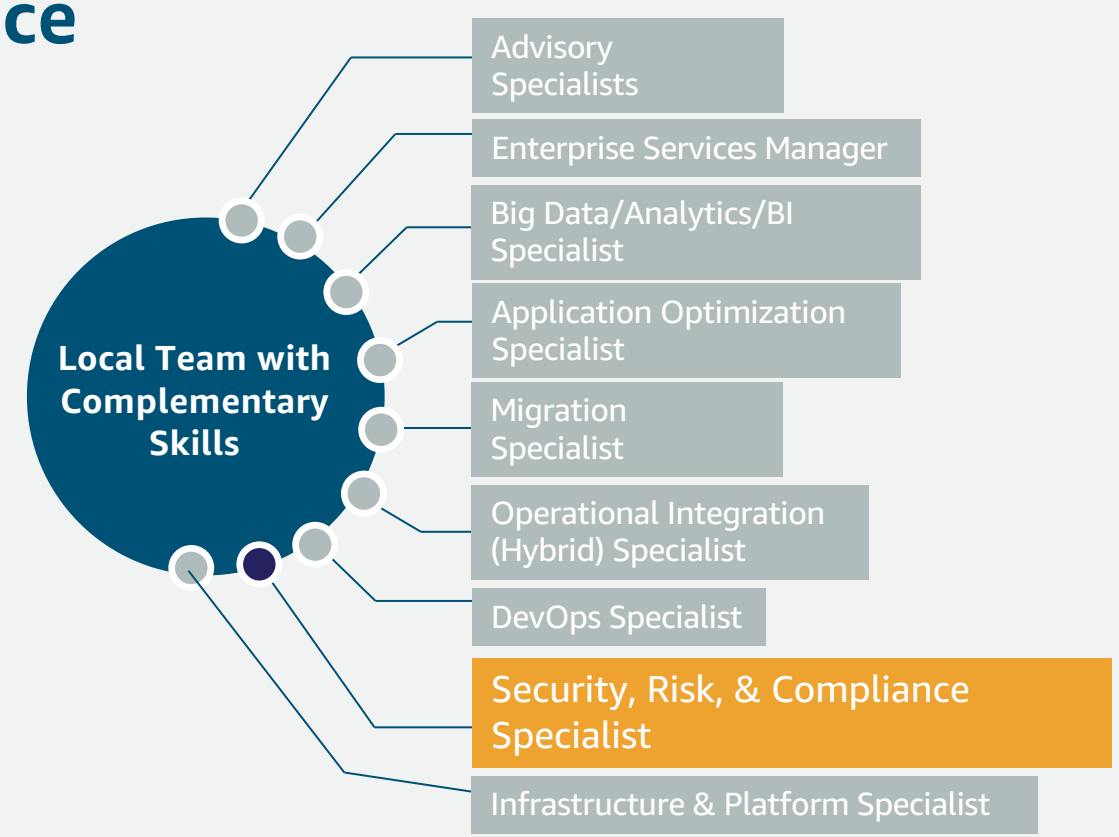
AWS Professional Services - 목표

Security, Risk, & Compliance Practice

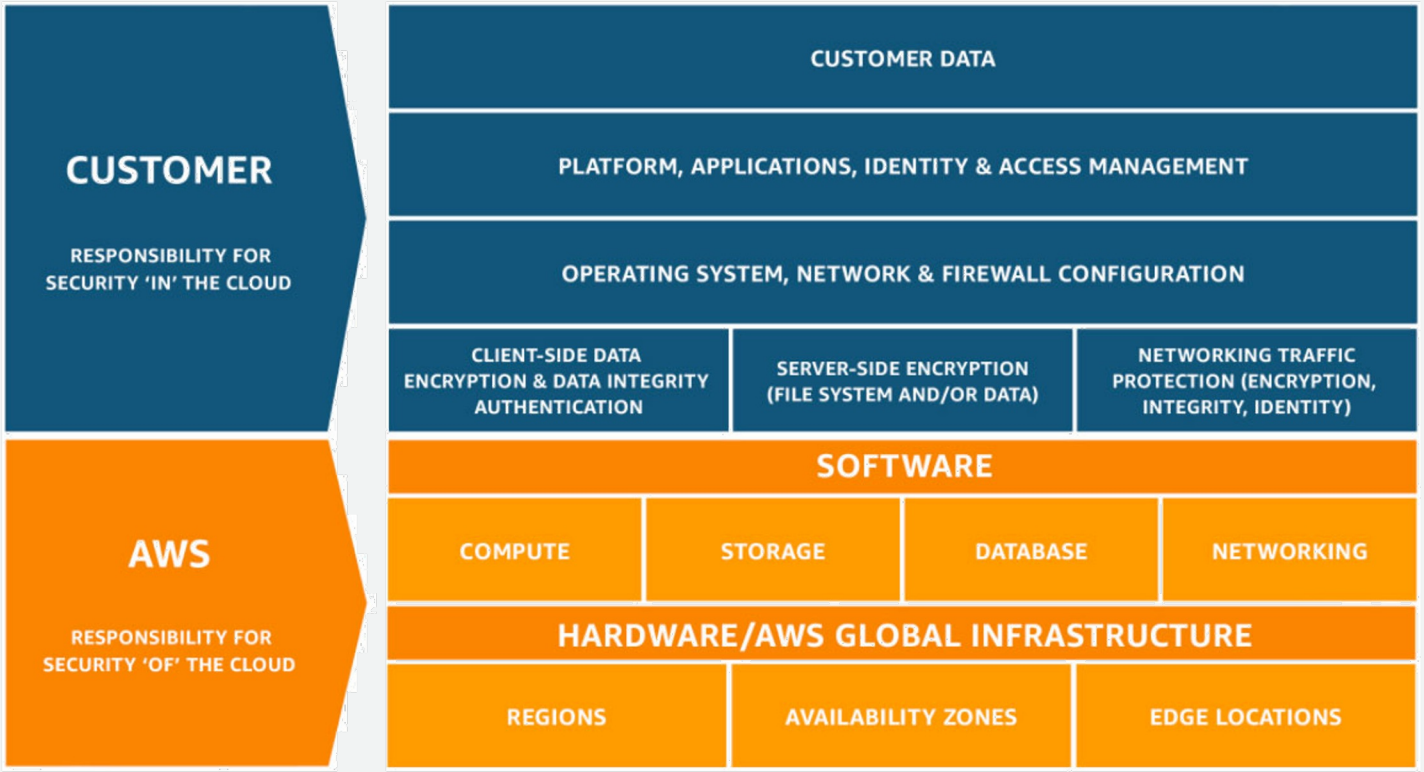
"**고객**과 **파트너**가 클라우드 채택과 혁신을 안전하게 **가속화할 수 있는 자신감과 기술 역량을 구축할 수 있도록 지원**합니다."

How

공유 책임 모델을 운영하고, 보안 **모범 사례, 방법론** 및 위험을 효과적으로 관리하는 솔루션을 제공합니다.



보안은 AWS와 고객의 공동 책임입니다.

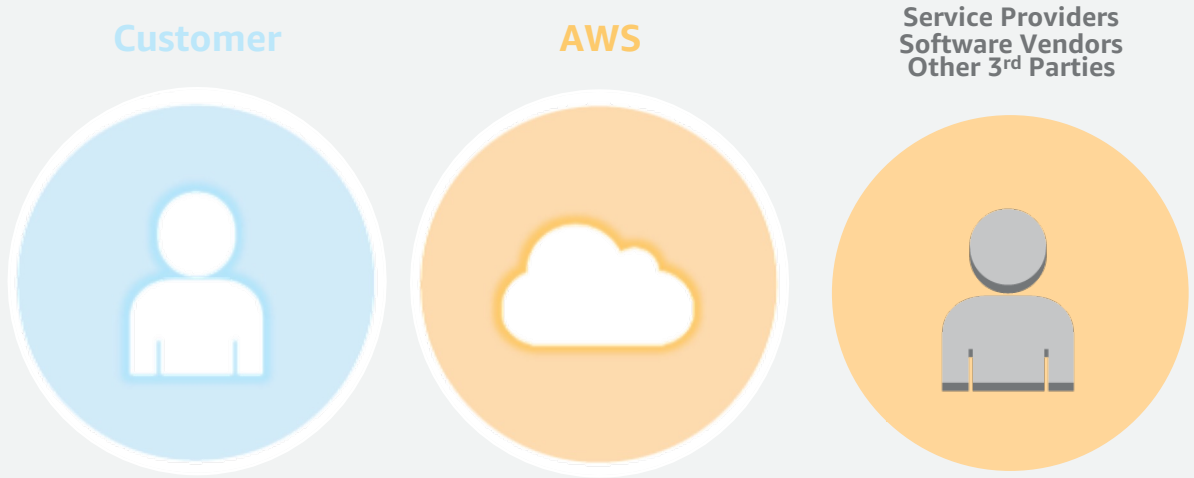


고객은
클라우드**에서(in)**
보안을 책임집니다.

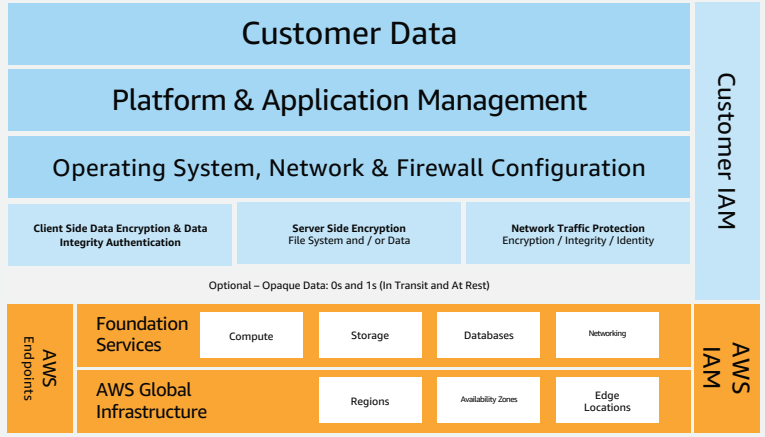
AWS는
클라우드**의(of)**
보안을 책임집니다.

왜 함께 일해야 할까요?

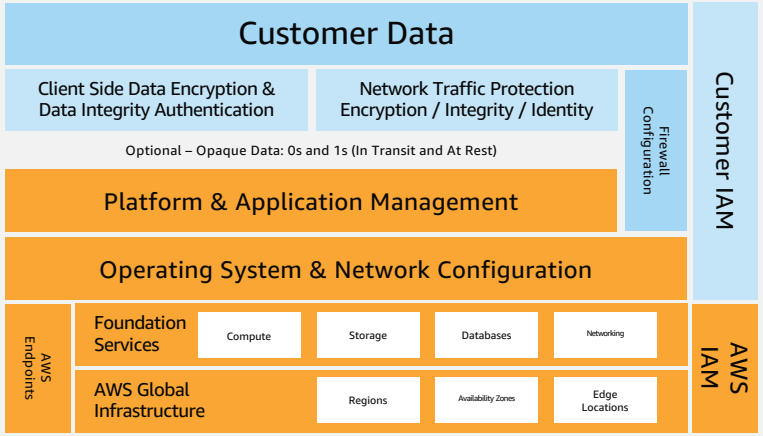
공유 책임은
정적(Static)이지
않습니다.



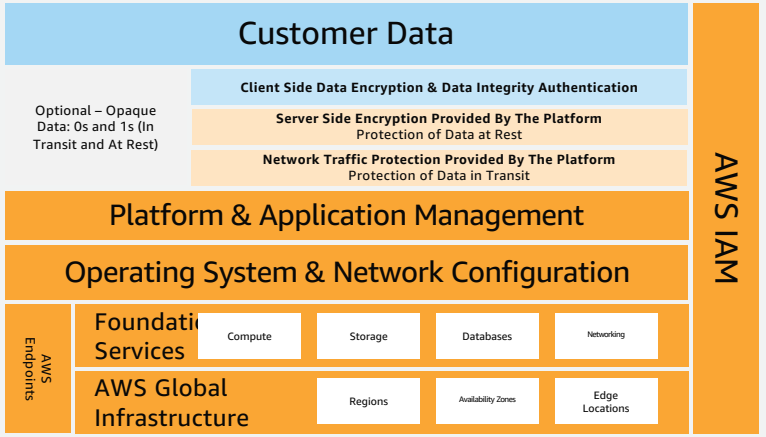
Infrastructure Services



Container Services



Abstracted Services

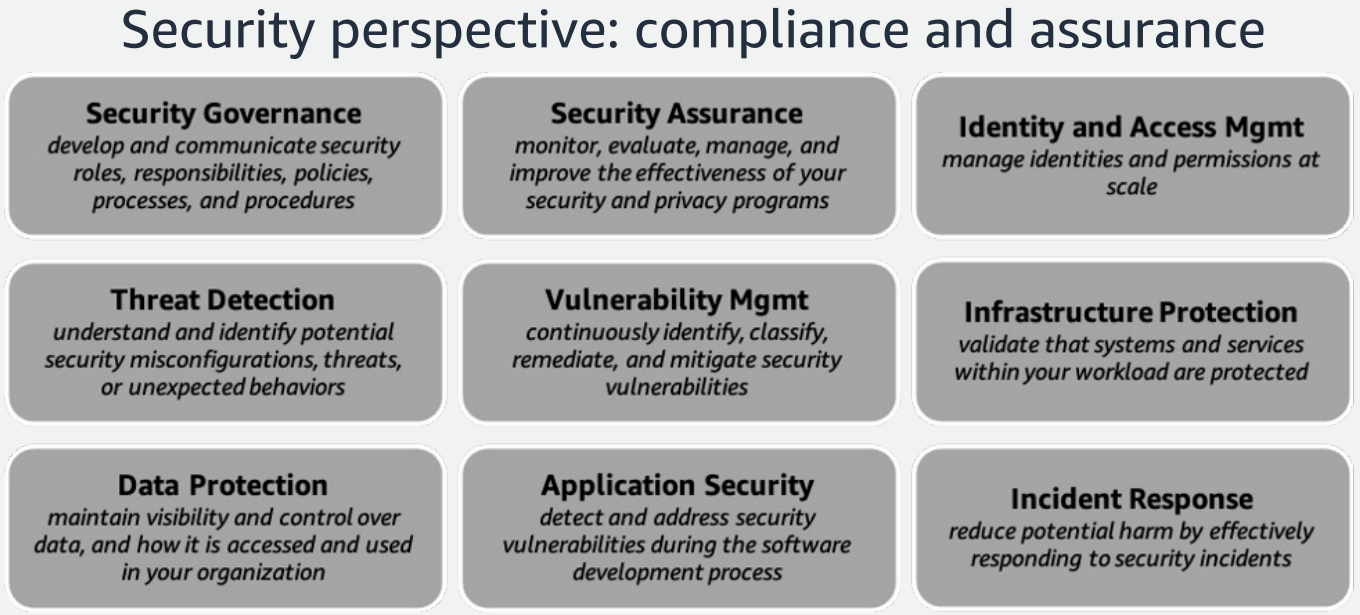


https://aws.amazon.com/compliance/shared-responsibility-model/

Security EPICs이란?

EPICs란 무엇인가요?

AWS Security EPICs은 기업 혁신을 위한 고객의 클라우드 보안 여정을 제시하는 전술적 규범 지침이 포함된 전략적 계획

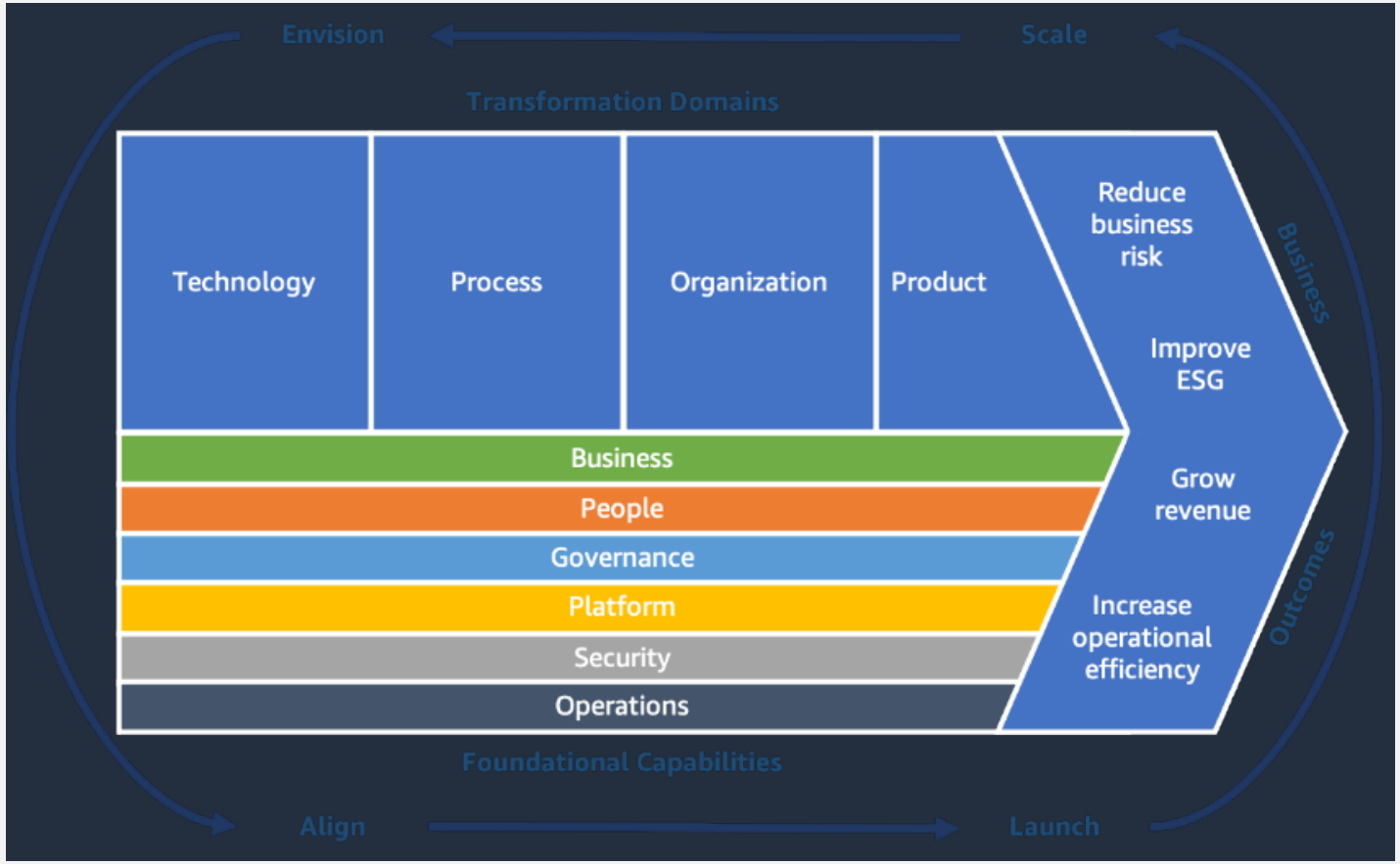


The *security* perspective helps you achieve the confidentiality, integrity, and availability of your data and cloud workloads. It comprises nine capabilities shown in the following figure. Common stakeholders include CISO, CCO, internal audit leaders, and security architects and engineers.

최종 목표는 요구 사항이 진화함에 따라 고객이 보안 프로그램을 지속적으로 반복하고 궁극적으로 지속적인 메커니즘을 유지함으로써, 비즈니스 결과를 가속화할 수 있도록, 그리고 프로세스에서 자급자족할 수 있도록 기술 세트를 개발하는 것입니다.

AWS Cloud Adoption Framework (AWS CAF)

AWS 클라우드 채택 프레임워크(AWS CAF)는 AWS 경험과 모범 사례를 활용하여 고객, 현장 및 파트너 팀이 혁신 기회를 식별하고 우선순위를 지정하고 클라우드 준비 상태를 평가 및 개선할 수 있도록 하는 클라우드 혁신을 위한 공유 정신 모델을 설정하기 위한 메커니즘입니다. 혁신 로드맵을 반복적으로 발전시킵니다.



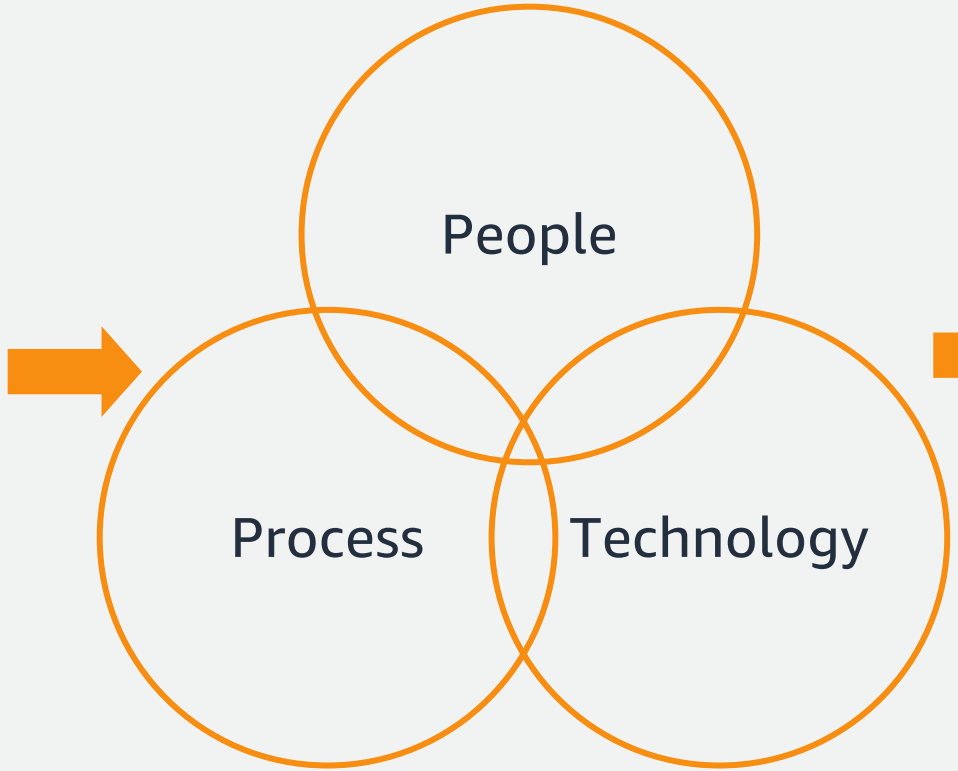
출처: https://aws.amazon.com/professional-services/CAF/

핵심 기반에 있는 보안

AWS Cloud Adoption Framework (CAF) – Security Epics의 발상지

AWS Cloud Adoption Framework (CAF)

Business Capability Focused	**Business** Value Realization
	People Roles and Readiness
	Governance Prioritization and Control
Technical Capability Focused	**Security** Risk and Compliance
	Platform Applications and Infrastructure
	Operations Hybrid and Dynamic



Expected Outcomes

- **Access control**
- Monitoring & **detective capabilities**
- Secure **infrastructure**
- Data classification
- **Encryption** strategy
- Cloud **Incident Response**
- **Security automation**
- Governance
- **Compliance & Policies**
- Risk Management

*not an exhaustive list

Reference: “The Security Perspective of the AWS Cloud Adoption Framework” Whitepaper https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

Security 5 EPICs – 각 pillar별 핵심 기능들

Identity & access management

Identity Mgmt. at scale

Federation

Access rights

Access limitations

Account level access security (ie: root)

Local account level authentication

Role based access control

Account Hierarchy

Detective controls

Org & Account level visibility

Service level visibility

Node level visibility

Retention requirements

Centralized log Ingestion (SIEM Integration)

Traffic log collection

Build foundation for automation

Infrastructure protection

VPC patterns

Hybrid Connectivity; Direct Connect/VPN

Network security (Security Groups, NACLs, etc.)

DDoS mitigation

Web App Firewalls

Configuration Mgmt. (ie: AMI Bakery)

Designing for security, elasticity & availability

Data protection

Encryption strategy

KMS Playbooks & Runbooks

Key & secrets management

Encryption at rest

Encryption in transit

Integrity validation

Incident response

Alerting

Investigations

Cloud IR Procedures & Playbooks

Preparation (IAM, AMI's, etc..)

Automated response & remediation

Containment

Forensics

Simulations

Security 5 EPICs – 식별 및 접근 제어

Identity & access management

AWS Identity & Access Management (IAM)

AWS Single Sign-On

AWS Directory Service

Amazon Cognito

AWS Organizations

AWS Resource Access Manager

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.

Security 5 EPICs – 탐지 컨트롤

Detective controls

AWS Security Hub

Amazon GuardDuty

AWS Config

AWS CloudTrail

Amazon CloudWatch

VPC Flow Logs

Amazon Macie

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.

Security 5 EPICs – 인프라 보안

Infrastructure protection

AWS Systems Manager

AWS Shield

AWS WAF – Web application firewall

AWS Firewall Manager

Amazon Inspector

Amazon Virtual Private Cloud (VPC)

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.

Security 5 EPICs – 데이터 보호

Data protection

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

Amazon Macie

AWS Secrets Manager

Server-Side Encryption

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.

Security 5 EPICs – 침해사고 대응

Incident response

AWS Config Rules

AWS Lambda

Amazon EC2 Systems Manager

Detective

침해사고 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.

감사합니다!