aws training and certification

AWS Certified Security - Specialty(SCS-C02) 시험 안내서

서론

AWS Certified Security - Specialty(SCS-C02) 시험은 보안 역할을 수행하는 개인을 대상으로 합니다. 이 시험은 응시자가 AWS 제품 및 서비스 보안에 대한 지식을 효과적으로 입증할 수 있는 능력을 검증합니다.

시험은 응시자가 다음 사항을 갖추고 있는지도 검증합니다.

- 전문적 데이터 분류 및 AWS 데이터 보호 메커니즘에 대한 이해
- 데이터 암호화 방법 및 이를 구현하기 위한 AWS 메커니즘에 대한 이해
- 보안 인터넷 프로토콜 및 이를 구현하기 위한 AWS 메커니즘에 대한 이해
- 안전한 프로덕션 환경을 제공하기 위한 AWS 보안 서비스 및 서비스 기능에 대한 실무 지식
- AWS 보안 서비스 및 기능을 활용한 2 년 이상 프로덕션 배포 경험의 역량
- 일련의 애플리케이션 요구 사항을 충족하기 위해 비용, 보안 및 배포 복잡성과 관련하여 균형 있는 결정을 내릴 수 있는 능력
- 보안 운영 및 위험에 대한 이해

대상 응시자 설명

대상 응시자는 보안 솔루션의 설계 및 구현 분야에서 3–5 년의 경험이 있어야 합니다. 또한 대상 응시자는 AWS 워크로드 보안에 대해 최소 2 년의 실무 경험이 있어야 합니다.

권장되는 AWS 지식

대상 응시자는 다음과 같은 지식이 있어야 합니다.

- AWS 공동 책임 모델 및 해당 애플리케이션
- AWS 서비스 및 클라우드 솔루션 배포에 대한 일반 지식
- AWS 환경 및 워크로드에 대한 보안 제어
- 로깅 및 모니터링 전략
- 취약성 관리 및 보안 자동화
- AWS 보안 서비스를 서드 파티 도구와 통합하는 방법
- 백업 전략을 포함한 재해 복구 제어
- 암호화 및 키 관리

- Identity Access Management
- 데이터 보존 및 수명 주기 관리
- 보안 문제 해결 방법
- 다중 계정 거버넌스 및 조직 규정 준수
- 위협 감지 및 인시던트 대응 전략

대상 응시자의 시험 범위에 해당하지 않는 작업 태스크

다음 목록에는 대상 응시자가 수행할 수 있을 것으로 예상되지 않는 작업 태스크가 나와 있습니다. 이 목록에 모든 사항이 포함된 것은 아닙니다. 다음 태스크는 시험 범위에 해당하지 않습니다.

- 특정 언어(예: Python, Java)로 소프트웨어를 개발합니다.
- 규정 준수 여부를 확인합니다.
- 소프트웨어 개발 수명 주기를 관리합니다.
- 네트워크 토폴로지를 설계합니다.
- 전체 클라우드 배포를 아키텍팅합니다.
- 데이터 레지던시 요구 사항(예: 일반 데이터 보호 규정[GDPR])에 따라 스토리지 서비스를 구성합니다.

부록을 참고하여 시험에 출제될 수 있는 기술 및 개념 목록, 시험 범위에 해당하는 AWS 서비스 및 기능 목록, 시험 범위가 아닌 AWS 서비스 및 기능 목록을 확인하시기 바랍니다.

시험 콘텐츠

답안 유형

이 시험의 문항은 두 가지 유형으로 제공됩니다.

- **선다형:** 정답 1 개와 오답 3 개(정답 이외의 답)가 있습니다.
- **복수 응답형:** 5 개 이상의 응답 항목 중에 2 개 이상의 정답이 있습니다.

문장을 가장 잘 완성하거나 질문에 대한 답으로 가장 적합한 응답을 하나 이상 선택합니다. 정답 이외의 답 또는 오답은 지식이나 기술이 부족한 응시자가 선택할 가능성이 큰 응답 항목입니다. 정답 이외의 답은 일반적으로 콘텐츠 영역에 부합하여 맞아 보이는 응답입니다.

답을 하지 않은 문항은 오답으로 처리됩니다. 추측에 따른 불이익은 없습니다. 시험에는 점수에 반영되는 50 개의 문항이 포함되어 있습니다.

채점되지 않는 콘텐츠

시험에는 점수에 반영되지 않아 채점되지 않는 15 개의 문항이 포함되어 있습니다. AWS 는 채점되지 않는 문항에 대한 응시자 성적 정보를 수집하여 추후 채점 대상 문항으로 사용할 수 있도록 이러한 문항을 평가합니다. 이러한 채점되지 않는 질문은 시험에서 식별되지 않습니다.

시험 결과

AWS Certified Security - Specialty(SCS-C02) 시험은 합격 또는 불합격이 결정되는 시험입니다. AWS 전문가가 자격증 분야 모범 사례 및 지침에 따라 설정한 최소 표준을 기준으로 시험 점수를 매깁니다.

시험 결과는 100~1,000 점의 변환 점수로 보고됩니다. 합격 최소 점수는 750 점입니다. 응시자는 점수를 통해 전반적인 시험 성적과 합격 여부를 알 수 있습니다. 변환 점수 모델은 난이도가 조금씩 다를 수 있는 여러 시험 형식에 걸쳐 점수를 균등하게 조정하는 데 도움이 됩니다.

점수 보고서에는 섹션 레벨별로 성적 분류표가 포함될 수 있습니다. 시험은 보상 점수 모델을 사용하므로 각 섹션에서 합격 점수를 얻을 필요는 없으며, 전체 시험에만 합격하면 됩니다.

시험의 섹션마다 특정 가중치가 적용되므로 일부 섹션은 다른 섹션보다 문항 수가 많습니다. 분류표에는 응시자의 장단점을 강조하여 보여주는 일반 정보가 포함되어 있습니다. 섹션별 피드백을 파악할 때 주의하시기 바랍니다.

내용 개요

이 시험 안내서에서는 시험의 가중치, 콘텐츠 도메인 및 태스크 설명 자료를 제공합니다. 이 안내서에서 시험 내용의 전체 목록을 제공하지는 않습니다. 그러나 각 태스크 설명에 관한 추가 맥락 정보를 사용하여 시험을 준비하는 데 참고할 수 있습니다.

시험의 콘텐츠 도메인과 가중치는 다음과 같습니다.

- 도메인 1: 위협 감지 및 사고 대응(채점 대상 콘텐츠의 14%)
- 도메인 2: 보안 로깅 및 모니터링(채점 대상 콘텐츠의 18%)
- 도메인 3: 인프라 보안(채점 대상 콘텐츠의 20%)
- 도메인 4: Identity and Access Management(채점 대상 콘텐츠의 16%)
- 도메인 5: 데이터 보호(채점 대상 콘텐츠의 18%)
- 도메인 6: 관리 및 보안 거버넌스(채점 대상 콘텐츠의 14%)

도메인 1: 위협 감지 및 인시던트 대응

태스크 설명 1.1: 인시던트 대응 계획 설계 및 구현.

관련 지식:

- 인시던트 대응을 위한 AWS 모범 사례
- 클라우드 인시던트
- 인시던트 대응 계획에서의 역할 및 책임
- AWS 보안 검색 형식(ASFF)

기술:

- 침해 대응을 위한 자격 증명 무효화 및 회전 전략 구현[예: AWS Identity and Access Management(IAM) 및 AWS Secrets Manager 사용]
- AWS 리소스 격리
- 보안 인시던트 대응을 위한 플레이북 및 실행서 설계 및 구현
- 보안 서비스 배포(예: AWS Security Hub, Amazon Macie, Amazon GuardDuty, Amazon Inspector, AWS Config, Amazon Detective, AWS Identity and Access Management Access Analyzer)
- 네이티브 AWS 서비스 및 서드 파티 서비스와의 통합 구성(예: Amazon EventBridge 및 ASFF 사용)

태스크 설명 1.2: AWS 서비스를 사용하여 보안 위협 및 이상 감지.

관련 지식:

- 위협을 감지하는 AWS 관리형 보안 서비스
- 여러 서비스에서 데이터를 결합하기 위한 이상 및 상관 관계 기법
- 이상을 식별하기 위한 시각화
- 보안 발견 사항을 중앙 집중화하기 위한 전략

기술:

- 보안 서비스의 발견 사항 평가(예: GuardDuty, Security Hub, Macie, AWS Config, IAM Access Analyzer)
- AWS 서비스 전반의 보안 위협 검색 및 상관 관계 파악(예: Detective 사용)
- 보안 이벤트 검증을 위한 쿼리 수행(예: Amazon Athena 사용)
- 이상 활동을 탐지하기 위한 지표 필터 및 대시보드 생성(예: Amazon CloudWatch 사용)

태스크 설명 1.3: 손상된 리소스 및 워크로드에 대응.

관련 지식:

- AWS 보안 인시던트 대응 가이드
- 리소스 격리 메커니즘
- 근본 원인 분석 기법
- 데이터 캡처 메커니즘
- 이벤트 검증을 위한 로그 분석

기술:

- AWS 서비스를 사용한 문제 해결 자동화(예: AWS Lambda, AWS Step Functions, EventBridge, AWS Systems Manager 실행서, Security Hub, AWS Config)
- 손상된 리소스에 대응(예: Amazon EC2 인스턴스 격리)
- 근본 원인 분석을 위한 조사 및 분석(예: Detective 사용)
- 손상된 리소스에서 관련 포렌식 데이터 캡처[예: Amazon Elastic Block Store(Amazon EBS) 볼륨 스냅샷, 메모리 덤프]
- 보안 이벤트와 관련된 상황별 정보에 대한 Amazon S3 의 로그 쿼리(예: Athena 사용)
- 포렌식 아티팩트 보호 및 보존(예: S3 객체 잠금, 격리된 포렌식 계정, S3 수명 주기 및 S3 복제 사용)
- 인시던트에 대비한 서비스 준비 및 인시던트 발생 후 서비스 복구

도메인 2: 보안 로깅 및 모니터링

태스크 설명 2.1: 보안 이벤트 해결을 위한 모니터링 및 경고 설계 및 구현.

관련 지식:

- 이벤트를 모니터링하고 경보를 제공하는 AWS 서비스(예: CloudWatch, EventBridge)
- 경고를 자동화하는 AWS 서비스[예: Lambda, Amazon Simple Notification Service(Amazon SNS), Security Hub]
- 지표와 기준을 모니터링하는 도구(예: GuardDuty, Systems Manager)

기술:

- 모니터링 요구 사항 및 보안 모니터링용 데이터 소스를 식별하기 위한 아키텍처 분석
- 모니터링 요구 사항을 결정하기 위한 환경 및 워크로드 분석
- 비즈니스 및 보안 요구 사항을 기반으로 환경 모니터링 및 워크로드 모니터링 설계

- 정기적인 감사를 수행하기 위한 자동화된 도구 및 스크립트 설정(예: Security Hub 에서 사용자 지정 인사이트 생성)
- 경고를 생성하는 지표 및 임계값 정의

태스크 설명 2.2: 보안 모니터링 및 알림 문제를 해결합니다.

관련 지식:

- 모니터링 서비스 구성(예: Security Hub)
- 보안 이벤트를 나타내는 관련 데이터

기술:

- 가시성 또는 경고를 제공하지 않은 이벤트 발생 후 서비스 기능, 권한 및 리소스 구성 분석
- 통계를 보고하지 않는 사용자 지정 애플리케이션의 구성 분석 및 문제 해결
- 보안 요구 사항에 맞게 조정하기 위한 로깅 및 모니터링 서비스 평가

태스크 설명 2.3: 로깅 솔루션을 설계하고 구현합니다.

관련 지식:

- 로깅 기능을 제공하는 AWS 서비스 및 기능(예: VPC 흐름 로그, DNS 로그, AWS CloudTrail, Amazon CloudWatch Logs)
- 로깅 기능의 속성(예: 로그 수준, 유형, 세부 사항)
- 로그 대상 및 수명 주기 관리(예: 보존 기간)

기술:

- 서비스 및 애플리케이션에 대한 로깅 구성
- 로그 수집을 위한 로깅 요구 사항 및 소스 식별
- AWS 모범 사례 및 조직 요구 사항에 따른 로그 스토리지 및 수명 주기 관리 구현

태스크 설명 2.4: 로깅 솔루션 문제를 해결합니다.

관련 지식:

- 데이터 소스(예: 로그 수준, 유형, 세부 사항, 주기, 적시성, 불변성)를 제공하는 AWS 서비스의 기능 및 사용 사례
- 로깅 기능을 제공하는 AWS 서비스 및 기능(예: VPC 흐름 로그, DNS 로그, CloudTrail, CloudWatch Logs)
- 로깅에 필요한 액세스 권한

기술:

- 잘못된 구성을 식별하고 로깅에 필요한 액세스 권한 부재에 대한 문제 해결 단계 결정(예: 읽기/쓰기 권한, S3 버킷 권한, 퍼블릭 액세스 및 무결성 관리)
- 로그 누락의 원인 파악 및 문제 해결 단계 수행

태스크 설명 2.5: 로그 분석 솔루션를 설계합니다.

관련 지식:

- 캡처된 로그를 분석하는 서비스 및 도구(예: Athena, CloudWatch Logs 필터)
- AWS 서비스의 로그 분석 기능(예: CloudWatch Logs Insights, CloudTrail 인사이트, Security Hub 인사이트)
- 로그 형식 및 구성 요소(예: CloudTrail 로그)

기술:

- 이상 및 알려진 위협을 나타내는 로그 패턴 식별
- 로그 정규화, 파싱 및 상관 관계 지정

도메인 3: 인프라 보안

태스크 설명 3.1: 엣지 서비스를 위한 보안 제어의 설계 및 구현.

관련 지식:

- 엣지 서비스의 보안 기능(예: AWS WAF, 로드 밸런서, Amazon Route 53, Amazon CloudFront, AWS Shield)
- 일반적인 공격, 위협 및 악용[예: Open Web Application Security Project(OWASP) Top 10, DDoS]
- 계층형 웹 애플리케이션 아키텍처

기술:

- 일반적인 사용 사례(예: 공개 웹 사이트, 서버리스 앱, 모바일 앱 백엔드)에 대한 엣지 보안 전략 정의
- 예상되는 위협 및 공격(예: OWASP Top 10, DDoS)을 기반으로 적절한 엣지 서비스 선택
- 예상되는 취약성 및 위험(예: 취약한 소프트웨어, 애플리케이션, 라이브러리)을 기반으로 적절한 보호 장치 선택
- 엣지 보안 서비스(예: AWS WAF 및 로드 밸런서를 사용하는 CloudFront)를 결합하여 방어 계층 정의
- 다양한 기준(예: 지리, 지리적 위치, 속도 제한)을 기반으로 엣지에 제한 적용

- 공격 여부를 표시하기 위해 엣지 서비스 주변에 로그, 지표 및 모니터링 활성화

태스크 설명 3.2: 네트워크 보안 제어 설계 및 구현.

관련 지식:

- VPC 보안 메커니즘(예: 보안 그룹, 네트워크 ACL, AWS Network Firewall)
- VPC 간 연결(예: AWS Transit Gateway, VPC 엔드포인트)
- 보안 원격 분석 소스(예: 트래픽 미러링, VPC 흐름 로그)
- VPN 기술, 용어 및 사용
- 온프레미스 연결 옵션(예: AWS VPN, AWS Direct Connect)

기술:

- 보안 요구 사항(예: 퍼블릭 서브넷, 프라이빗 서브넷, 민감한 VPC, 온프레미스 연결)을 기반으로 네트워크 세분화 구현
- 필요에 따라 네트워크 트래픽을 허용하거나 방지하는 네트워크 제어 설계(예: 보안 그룹, 네트워크 ACL 및 Network Firewall 사용)
- 데이터가 퍼블릭 인터넷에 연결되지 않도록 네트워크 흐름 설계(예: VPC 에서 Transit Gateway, VPC 엔드포인트 및 Lambda 사용)
- 네트워크 설계, 위협 및 공격(예: 로드 밸런서 로그, VPC 흐름 로그, 트래픽 미러링)을 기반으로 모니터링할 원격 분석 소스 결정
- 온프레미스 환경과 AWS 클라우드 간의 통신을 위한 중복성 및 보안 워크로드 요구 사항 결정(예: AWS VPN, DX 를 통한 AWS VPN 및 MACsec 사용)
- 불필요한 네트워크 액세스 식별 및 제거
- 요구 사항 변화에 따른 네트워크 구성 관리(예: AWS Firewall Manager 사용)

태스크 설명 3.3: 컴퓨팅 워크로드에 대한 보안 제어의 설계 및 구현.

관련 지식:

- EC2 인스턴스 프로비저닝 및 유지 관리(예: 패치, 검사, 스냅샷 및 AMI 생성, EC2 Image Builder 사용)
- IAM 인스턴스 역할 및 IAM 서비스 역할
- 컴퓨팅 워크로드의 취약성을 스캔하는 서비스[예: Amazon Inspector, Amazon Elastic Container Registry(Amazon ECR)]
- 호스트 기반 보안(예: 방화벽, 강화)

기술:

- 강화된 EC2 AMI 생성
- 컴퓨팅 워크로드를 승인하기 위해 인스턴스 역할 및 서비스 역할을 적절하게 적용

- EC2 인스턴스 및 컨테이너 이미지에 알려진 취약성이 있는지 스캔
- EC2 인스턴스 또는 컨테이너 이미지 전체에 패치 적용
- 호스트 기반 보안 메커니즘 활성화(예: 호스트 기반 방화벽)
- Amazon Inspector 발견 사항 분석 및 적절한 완화 기법 결정
- 보안 및 자격 증명을 컴퓨팅 워크로드에 안전하게 전달

태스크 설명 3.4: 네트워크 보안 문제 해결.

관련 지식:

- 연결성을 분석하는 방법(예: VPC Reachability Analyzer 및 Amazon Inspector 사용)
- 기본 TCP/IP 네트워킹 개념[예: UDP 및 TCP, 포트, Open Systems Interconnection(OSI) 모델, 네트워크 운영 체제 유틸리티]
- 관련 로그 소스를 읽는 방법(예: Route 53 로그, AWS WAF 로그, VPC 흐름 로그)

기술:

- 네트워크 연결 문제 식별, 해석 및 우선 순위 지정(예: Amazon Inspector 네트워크 연결 가능성 사용)
- 원하는 네트워크 동작을 구현하기 위한 솔루션 결정
- 문제 식별을 위한 로그 소스 분석
- 문제 분석을 위한 트래픽 샘플 캡처(예: 트래픽 미러링 사용)

도메인 4: AWS Identity and Access Management

태스크 설명 4.1: AWS 리소스 인증의 설계, 구현 및 문제 해결.

관련 지식:

- 자격 증명을 생성하고 관리하는 방법 및 서비스[예: 페더레이션, 자격 증명 기관, AWS IAM Identity Center(AWS Single Sign-On), Amazon Cognito]
- 장기 및 임시 자격 증명 메커니즘
- 인증 문제를 해결하는 방법(예: CloudTrail, IAM Access Advisor 및 IAM 정책 시뮬레이터 사용)

기술:

- 요구 사항에 따라 인증 시스템을 통한 자격 증명 설정
- 멀티 팩터 인증(MFA) 사용

- AWS Security Token Service(AWS STS)를 사용하여 임시 자격 증명을 발급할 시기 결정

태스크 설명 4.2: AWS 리소스 권한 부여의 설계, 구현 및 문제 해결.

관련 지식:

- 다양한 IAM 정책(예: 관리형 정책, 인라인 정책, 자격 증명 기반 정책, 리소스 기반 정책, 세션 제어 정책)
- 정책의 구성 요소 및 영향(예: 보안 주체, 작업, 리소스, 조건)
- 권한 부여 문제를 해결하는 방법(예: CloudTrail, IAM Access Advisor 및 IAM 정책 시뮬레이터 사용)

기술:

- 속성 기반 액세스 제어(ABAC) 및 역할 기반 액세스 제어(RBAC) 전략 구축
- 주어진 요구 사항 및 워크로드에 대한 IAM 정책 유형 평가
- IAM 정책이 환경 및 워크로드에 미치는 영향 해석
- 환경 전반에 최소 권한의 원칙 적용
- 적절한 업무 분리 시행
- 원인 또는 결과를 파악하기 위한 액세스 또는 권한 부여 오류 분석
- 의도하지 않은 상태에서 리소스, 서비스 또는 엔터티에 부여된 권한 또는 권한 부여 조사

도메인 5: 데이터 보호

태스크 설명 5.1: 전송 중인 데이터에 기밀성과 무결성을 제공하는 제어의 설계 및 구현.

관련 지식:

- TLS 개념
- VPN 개념(예: IPsec)
- 안전한 원격 액세스 방법(예: Systems Manager Session Manager 를 통한 SSH, RDP)
- Systems Manager Session Manager 개념
- TLS 인증서가 다양한 네트워크 서비스 및 리소스(예: CloudFront, 로드 밸런서)에서 작동하는 방식

기술:

- AWS 와 온프레미스 네트워크 간의 보안 연결 설계(예: DX 및 VPN 게이트웨이 사용)
- 리소스에 연결할 때 암호화를 요구하는 메커니즘 설계[예: Amazon RDS, Amazon Redshift, CloudFront, Amazon S3, Amazon DynamoDB, 로드 밸런서, Amazon Elastic File System(Amazon EFS), Amazon API Gateway]
- AWS API 호출을 위한 TLS 요구(예: Amazon S3 사용)
- 보안 연결을 통해 트래픽을 전달하는 메커니즘 설계(예: Systems Manager 및 EC2 Instance Connect 사용)
- 프라이빗 VIF 와 퍼블릭 VIF 를 사용한 리전 간 네트워킹 설계

태스크 설명 5.2: 저장된 데이터에 기밀성과 무결성을 제공하는 제어의 설계 및 구현.

관련 지식:

- 암호화 기술 선택(예: 클라이언트 측, 서버 측, 대칭, 비대칭)
- 무결성 검사 기법(예: 해싱 알고리즘, 디지털 서명)
- 리소스 정책[예: DynamoDB, Amazon S3 및 AWS Key Management Service(AWS KMS)]
- IAM 역할 및 정책

기술:

- 인증된 사용자에 대한 액세스를 제한하는 리소스 정책 설계(예: S3 버킷 정책, DynamoDB 정책)
- 무단 퍼블릭 액세스를 방지하는 메커니즘 설계(예: S3 퍼블릭 액세스 차단, 퍼블릭 스냅샷 및 퍼블릭 AMI 방지)
- 저장 중인 데이터의 암호화를 활성화하기 위한 서비스 구성[예: Amazon S3, Amazon RDS, DynamoDB, Amazon Simple Queue Service(Amazon SQS), Amazon EBS, Amazon EFS]
- 수정을 방지하여 데이터 무결성을 보호하는 메커니즘 설계(예: S3 객체 잠금, KMS 키 정책, S3 Glacier 저장소 잠금 및 AWS Backup 저장소 잠금 사용)
- 관계형 데이터베이스를 위한 AWS CloudHSM 을 사용하여 저장 중 암호화 설계(예: Amazon RDS, RDS 사용자 지정, EC2 인스턴스의 데이터베이스)
- 비즈니스 요구 사항에 따른 암호화 기술 선택

태스크 설명 5.3: 저장된 데이터의 수명 주기를 관리하기 위한 제어의 설계 및 구현.

관련 지식:

- 수명 주기 정책
- 데이터 보존 표준

기술:

- 필요한 보존 기간 동안 데이터를 보존하기 위한 S3 수명 주기 메커니즘 설계(예: S3 객체 잠금, S3 Glacier 저장소 잠금, S3 수명 주기 정책)
- AWS 서비스 및 리소스에 대한 자동 수명 주기 관리 설계[예: Amazon S3, EBS 볼륨 스냅샷, RDS 볼륨 스냅샷, AMI, 컨테이너 이미지, CloudWatch 로그 그룹, Amazon Data Lifecycle Manager)
- AWS 서비스 전반에 걸친 AWS Backup 의 일정 및 보존 수립

태스크 설명 5.4: 자격 증명, 비밀 및 암호화 키 자료를 보호하기 위한 제어의 설계 및 구현.

관련 지식:

- Secrets Manager
- Systems Manager Parameter Store
- 대칭 키 및 비대칭 키의 사용 및 관리(예: AWS KMS)

기술:

- 워크로드에 대한 비밀의 관리 및 회전 설계(예: 데이터베이스 액세스 자격 증명, API 키, IAM 액세스 키, AWS KMS 고객 관리 키)
- 키 사용을 인증된 사용자로 제한하는 KMS 키 정책 설계
- 고객이 제공한 키 자료를 가져오고 제거하는 메커니즘 수립

도메인 6: 관리 및 보안 거버넌스

태스크 설명 6.1: AWS 계정을 중앙에서 배포하고 관리하기 위한 전략의 개발.

관련 지식:

- 다중 계정 전략
- 관리 위임을 허용하는 Managed Services
- 정책으로 정의된 가드레일
- 루트 계정 모범 사례
- 교차 계정 역할

기술:

- AWS Organizations 배포 및 구성
- AWS Control Tower 배포 시기 및 방법 결정(예: 성공적인 배포를 위해 비활성화해야 하는 서비스)
- 정책 시행을 위한 기술 솔루션으로 SCP 를 구현(예: 루트 계정 사용 제한, AWS Control Tower 의 제어 구현)
- 중앙 집중식 보안 서비스 관리 및 발견 사항 집계(예: 관리 위임 및 AWS Config 애그리게이터 사용)
- AWS 계정 루트 사용자 자격 증명 보호

태스크 설명 6.2: 클라우드 리소스를 위한 안전하고 일관된 배포 전략의 구현.

관련 지식:

- 코드형 인프라(IaC)를 사용한 배포 모범 사례(예: AWS CloudFormation 템플릿 강화 및 드리프트 감지)
- 태깅 모범 사례
- AWS 서비스의 중앙 집중식 관리, 배포 및 버전 관리
- AWS 인프라에 대한 가시성 및 제어

기술:

- CloudFormation 을 사용하여 클라우드 리소스를 일관되고 안전하게 배포
- 다중 계정 태깅 전략 구현 및 적용
- 승인된 AWS 서비스의 포트폴리오 구성 및 배포(예: AWS Service Catalog 사용)
- 관리를 위해 AWS 리소스를 여러 그룹으로 구성
- 정책 시행을 위한 Firewall Manager 배포
- AWS 계정 간에 리소스를 안전하게 공유[예: AWS Resource Access Manager(AWS RAM) 사용]

태스크 설명 6.3: AWS 리소스의 규정 준수 평가.

관련 지식:

- AWS 서비스를 사용한 데이터 분류
- AWS 리소스 구성을 측정, 감사 및 평가하는 방법(예: AWS Config 사용)

기술:

- Macie 를 사용하여 민감한 데이터 식별
- 규정을 준수하지 않는 AWS 리소스 탐지를 위한 AWS Config 규칙 생성
- Security Hub 및 AWS Audit Manager 를 사용하여 증거 수집 및 구성

태스크 설명 6.4: 아키텍처 검토 및 비용 분석을 통해 보안 허점 식별.

관련 지식:

- 이상 식별을 위한 AWS 비용 및 사용
- 공격 대상 영역을 줄이기 위한 전략
- AWS Well-Architected Framework

기술:

- 리소스 사용률 및 추세를 기반으로 이상 식별
- AWS 서비스 및 도구를 사용하여 미사용 리소스 식별(예: AWS Trusted Advisor, AWS Cost Explorer)
- AWS Well-Architected Tool 을 사용하여 보안 허점 파악

부록

시험에 출제될 수 있는 기술 및 개념

다음 목록에는 시험에 출제될 수 있는 기술 및 개념이 포함되어 있습니다. 이 목록에 모든 사항이 포함된 것은 아니며 변경될 수 있습니다. 이 목록에 나와 있는 다음 항목의 배치와 순서가 시험에서의 상대적 가중치 또는 중요도를 의미하지는 않습니다.

- AWS CLI
- AWS SDK
- AWS Management Console
- 보안 원격 액세스
- 인증서 관리
- 코드형 인프라(IaC)

시험 범위에 포함되는 AWS 서비스 및 기능

참고: 보안은 모든 AWS 서비스에 영향을 줍니다. 전체 서비스가 범위에 포함되지 않으므로 많은 서비스가 이 목록에 표시되지 않습니다. 그러나 서비스의 보안에 관련된 사항은 범위에 포함됩니다. 예를 들어 이 시험에는 S3 버킷 복제의 설정 단계에 대한 문항은 없지만 S3 버킷 정책 구성에 대한 문항은 있을 수 있습니다.

다음 목록에는 시험 범위에 해당하는 AWS 서비스 및 기능이 나와 있습니다. 이 목록에 모든 사항이 포함된 것은 아니며 변경될 수 있습니다. AWS 제품 및 서비스는 주요 기능에 따라 다음과 같은 카테고리로 분류됩니다.

AWS 의 관리 및 거버넌스:

- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- AWS Organizations
- AWS Systems Manager
- AWS Trusted Advisor

네트워킹 및 콘텐츠 전송:

- Amazon VPC
  - Network Access Analyzer
  - 네트워크 ACL
  - 보안 그룹
  - VPC 엔드포인트

보안, 자격 증명 및 규정 준수:

- AWS Audit Manager
- AWS Certificate Manager(ACM)
- AWS CloudHSM
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Amazon GuardDuty
- AWS IAM Identity Center(AWS Single Sign-On)
- AWS Identity and Access Management(IAM)
- Amazon Inspector
- AWS Key Management Service(AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Security Hub
- AWS Shield
- AWS WAF

시험 범위가 아닌 **AWS** 서비스 및 기능

다음 목록에는 시험 범위가 아닌 AWS 서비스 및 기능이 나와 있습니다. 이 목록에 모든 사항이 포함된 것은 아니며 변경될 수 있습니다. 시험의 대상 작업 역할과 전혀 관련이 없는 AWS 제품 및 서비스는 다음 목록에서 제외됩니다.

블록체인:

- Amazon Managed Blockchain
- Amazon Quantum Ledger Database(Amazon QLDB)

비즈니스 애플리케이션:

- Alexa for Business
- Amazon Chime
- Amazon Chime SDK
- Amazon Connect
- Amazon Honeycode
- Amazon Pinpoint
- AWS Supply Chain
- AWS Wickr
- Amazon WorkDocs

최종 사용자 컴퓨팅:

- Amazon AppStream 2.0

미디어 서비스:

- Amazon Elastic Transcoder
- AWS Elemental Appliances and Software
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- Amazon Interactive Video Service(Amazon IVS)
- Amazon Kinesis Video Streams
- Amazon Nimble Studio

마이그레이션 및 전송:

- AWS Application Discovery Service
- AWS Application Migration Service
- AWS Database Migration Service(AWS DMS)
- 마이그레이션 평가기
- AWS Migration Hub
- AWS Transfer Family

퀀텀 테크놀로지:

- Amazon Braket

로보틱스:

- AWS RoboMaker

인공위성:

- AWS Ground Station

설문 조사

이 시험 안내서가 도움이 되었나요? 설문 조사에 참여하여 의견을 공유해 주시기 바랍니다.