AWS Certified Security - Specialty (SCS-C03) 시험 안내서

서론

AWS Certified Security - Specialty (SCS-C03) 시험은 클라우드 솔루션 보안을 담당하는 개인을 대상으로 합니다. 이 시험은 응시자가 AWS 제품 및 서비스 보안에 대한 지식을 효과적으로 입증할 수 있는 능력을 검증합니다.

또한 이 시험에서는 응시자가 다음 작업을 완료할 수 있는지 확인합니다.

- 전문적 데이터 분류 및 AWS 데이터 보호 메커니즘에 대한 적용
- 데이터 암호화 방법 및 AWS 암호화 메커니즘 구현
- 안전한 인터넷 프로토콜을 준수하도록 AWS 메커니즘 구현
- AWS 보안 서비스 및 기능을 사용하여 안전한 프로덕션 환경 확보
- 일련의 애플리케이션 요구 사항을 충족하기 위해 비용과 보안, 배포 복잡성 간에 균형 있는 의사 결정 가능
- 보안 운영 및 위험에 대한 이해

대상 응시자 설명

대상 응시자는 클라우드 솔루션 보안 분야에서 3~5 년에 준하는 경력을 보유하고 있어야 합니다.

AWS 지식 추천

대상 응시자는 다음과 같은 AWS 관련 지식이 있어야 합니다.

- AWS 공동 책임 모델 및 적용
- 규모에 맞는 자격 증명 관리
- 다수 계정 거버넌스
- 소프트웨어 공급망 위험 관리
- 보안 인시던트 방지 및 대응 전략
- 클라우드의 취약성 관리
- 규모에 맞는 방화벽 규칙 개발(계층 3~7 에 해당)
- 인시던트의 근본 원인 분석
- 감사에 대응한 경험

- 로깅 및 모니터링 전략
- 저장 및 전송 중 모두에 대한 데이터 암호화 방법론
- 백업 전략을 포함한 재해 복구 제어

대상 응시자의 시험 범위에 해당하지 않는 직무 관련 작업

다음 목록에는 대상 응시자가 수행할 수 있을 것으로 예상되지 않는 직무 관련 작업이 나와 있습니다. 이 목록에 모든 사항이 포함된 것은 아닙니다. 다음 작업은 시험 범위에 해당하지 않습니다.

- 암호화 알고리즘 설계
- 패킷 수준에서 트래픽 분석
- 전체 클라우드 배포 아키텍팅
- 최종 사용자 컴퓨팅 리소스 관리
- 기계 학습 모델 훈련

부록 A 를 참고하여 시험 범위에 해당하는 AWS 서비스 및 기능 목록, 시험 범위가 아닌 AWS 서비스 및 기능 목록을 확인하시기 바랍니다.

시험 콘텐츠

답안 유형

시험에는 다음과 같은 다양한 유형의 문항이 포함됩니다.

- **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.
- **순서 배열:** 지정된 작업을 완료하기 위한 3~5 개의 응답 목록이 있습니다. 정답을 선택하고 정답을 올바른 순서로 배치해야 문항에 배정된 점수를 받을 수 있습니다.
- **매치:** 3~7 개의 프롬프트 목록과 일치하는 응답 목록이 있습니다. 문항에 배정된 점수를 받으려면 모든 쌍을 정확하게 매칭해야 합니다.

답하지 않은 문항은 오답으로 채점됩니다. 추측에 따른 불이익은 없습니다. 시험에는 점수에 반영되는 50 개의 문항이 포함되어 있습니다 [1].

채점되지 않는 콘텐츠

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

시험 결과

AWS Certified Security - Specialty (SCS-C03) 시험은 합격 또는 불합격이 결정되는 시험입니다. AWS 전문가가 자격증 분야 모범 사례 및 가이드라인에 따라 설정한 최소 표준을 기준으로 시험 점수를 매깁니다.

시험 결과는 100 점에서 1,000 점까지 환산한 점수로 알려드립니다. 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 사용합니다. 즉, 각 섹션에서 합격 점수를 얻지 않아도 괜찮습니다. 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.

---

[1] 시험의 베타 버전에는 적용되지 않습니다. 베타 시험 전반에 대한 자세한 내용은 AWS Certification 웹사이트에서 확인할 수 있습니다.

내용 개요

이 시험 안내서에서는 시험의 가중치, 콘텐츠 도메인 및 태스크를 제공합니다. 이 안내서에서는 시험 내용의 전체 목록을 제공하지 않습니다.

시험의 콘텐츠 도메인과 가중치는 다음과 같습니다.

- 콘텐츠 도메인 1: 탐지(채점 대상 콘텐츠의 16%)
- 콘텐츠 도메인 2: 인시던트 대응(채점 대상 콘텐츠의 14%)
- 콘텐츠 도메인 3: 인프라 보안(채점 대상 콘텐츠의 18%)
- 콘텐츠 도메인 4: ID 및 액세스 관리(채점 대상 콘텐츠의 20%)
- 콘텐츠 도메인 5: 데이터 보호(채점 대상 콘텐츠의 18%)
- 콘텐츠 도메인 6: 보안 기반 및 거버넌스(채점 대상 콘텐츠의 14%)

콘텐츠 도메인 1: 탐지

작업 1.1: AWS 계정이나 조직용 모니터링 및 경보 솔루션을 설계하고 구현합니다.

기술 1.1.1: 워크로드를 분석하여 모니터링 요구 사항을 결정합니다.
기술 1.1.2: 워크로드 모니터링 전략을 설계하고 구현합니다. 예: 리소스 상태 확인 구성
기술 1.1.3: 보안 및 모니터링 이벤트를 집계합니다.
기술 1.1.4: 지표, 알림 및 대시보드를 만들어 이상 데이터와 이벤트를 탐지합니다.
예: Amazon GuardDuty, Amazon Security Lake, AWS Security Hub, Amazon Macie
기술 1.1.5: 자동화 기능을 만들고 관리하여 정기적인 평가와 조사를 수행합니다.
예: AWS Config 준수 팩, Security Hub, AWS Systems Manager State Manager 배포

작업 1.2: 로깅 솔루션을 설계하고 구현합니다.

기술 1.2.1: 요구 사항에 따라 로그 수집과 스토리지를 확보할 소스를 식별합니다.
기술 1.2.2: AWS 서비스 및 애플리케이션에 대한 로깅을 구성합니다. 예: 조직의 AWS CloudTrail 추적 구성, 전용 Amazon CloudWatch 로깅 계정 만들기, Amazon CloudWatch Logs 에이전트 구성
기술 1.2.3: 로그 스토리지 및 로그 데이터 레이크(예: Security Lake)를 구현하고 서드 파티 보안 도구와 통합합니다.

기술 1.2.4: AWS 서비스를 사용하여 로그를 분석합니다. 예: CloudWatch Logs Insights, Amazon Athena, Security Hub 조사 결과
기술 1.2.5: AWS 서비스를 사용하여 로그를 정규화하고, 구문 분석하고, 상관 관계를 분석합니다. 예: Amazon OpenSearch Service, AWS Lambda, Amazon Managed Grafana
기술 1.2.6: 네트워크 설계, 위협 및 공격을 기반으로 적절한 로그 소스를 결정하고 구성합니다. 예: VPC 흐름 로그, 전송 게이트웨이 흐름 로그, Amazon Route 53 Resolver 로그

작업 1.3: 보안 모니터링, 로깅 및 경보 솔루션의 문제를 해결합니다.

기술 1.3.1: 리소스의 기능, 권한 및 구성을 분석합니다. 예: Lambda 함수 로깅, Amazon API Gateway 로깅, 상태 확인, Amazon CloudFront 로깅
기술 1.3.2: 리소스의 잘못된 구성 문제를 해결합니다. 예: CloudWatch 에이전트 구성 문제 해결, 누락된 로그 문제 해결

콘텐츠 도메인 2: 인시던트 대응

작업 2.1: 인시던트 대응 계획을 설계 및 테스트합니다.

기술 2.1.1: 보안 인시던트에 대응하기 위한 대응 계획 및 런북을 설계하고 구현합니다. 예: Systems Manager OpsCenter, Amazon SageMaker AI 노트북
기술 2.1.2: AWS 서비스 특성과 기능을 사용하여 인시던트에 대비할 서비스를 구성합니다. 예: 액세스 프로비저닝, 보안 도구 배포, 영향 범위 최소화, AWS Shield Advanced 보호 기능 구성
기술 2.1.3: 인시던트 대응 계획의 효과를 테스트하고 확인하기 위한 절차를 권장합니다. 예: AWS Fault Injection Service, AWS Resilience Hub
기술 2.1.4: AWS 서비스를 사용하여 자동으로 인시던트를 해결합니다. 예: Systems Manager, Amazon EC2 용 Automated Forensics Orchestrator, AWS Step Functions, Amazon Application Recovery Controller, Lambda 함수

작업 2.2: 보안 이벤트에 대응합니다.

기술 2.2.1: 관련 시스템과 애플리케이션 로그를 포렌식 아티팩트로 캡처하고 저장합니다.
기술 2.2.2: 애플리케이션과 AWS 서비스 전반의 보안 이벤트 로그를 검색하고 상관 관계를 분석합니다.
기술 2.2.3: AWS 보안 서비스의 조사 결과를 확인하여 이벤트의 범위와 영향을 평가합니다.

기술 2.2.4: 위협을 억제하고 근절하여 영향을 받는 리소스에 대응하고 리소스를 복구합니다. 예: 네트워크 격리 제어 구현, 백업 복원

기술 2.2.5: 근본 원인 분석을 수행하는 방법을 설명합니다. 예: Amazon Detective

콘텐츠 도메인 3: 인프라 보안

작업 3.1: 네트워크 엣지 서비스의 보안 제어를 설계, 구현하고 문제를 해결합니다.

기술 3.1.1: 예상되는 위협과 공격을 기반으로 엣지 보안 전략을 정의하고 선택합니다.

기술 3.1.2: 적절한 네트워크 엣지 보호 기능을 구현합니다. 예: CloudFront 헤더, AWS WAF, AWS IoT 정책, OWASP 상위 10 개 위협에 대한 보호, Amazon S3 크로스 오리진 리소스 공유(CORS), Shield Advanced

기술 3.1.3: 요구 사항을 기반으로 AWS 엣지 제어 및 규칙을 설계하고 구현합니다. 예: 지리, 지리적 위치, 속도 제한, 클라이언트 핑거프린팅

기술 3.1.4: AWS 엣지 서비스 및 서드 파티 서비스와의 통합을 구성합니다. 예: 개방형 사이버 보안 스키마 프레임워크(OCSF) 형식으로 데이터 수집, 서드 파티 WAF 규칙 사용

작업 3.2: 컴퓨팅 워크로드에 대한 보안 제어를 설계, 구현하고 문제를 해결합니다.

기술 3.2.1: 강화된 Amazon EC2 AMI 와 컨테이너 이미지를 설계 및 구현하여 컴퓨팅 워크로드를 보호하고 보안 제어 기능을 내장합니다. 예: Systems Manager, EC2 Image Builder

기술 3.2.2: 인스턴스 프로파일, 서비스 역할 및 실행 역할을 적절하게 적용하여 컴퓨팅 워크로드를 승인합니다.

기술 3.2.3: 컴퓨팅 리소스를 스캔하여 알려진 취약성을 찾습니다. 예: Amazon Inspector 를 사용하여 컨테이너 이미지와 Lambda 함수 스캔, GuardDuty 를 사용하여 컴퓨팅 런타임 모니터링

기술 3.2.4: 업데이트 프로세스를 자동화하고 지속적인 확인 기능을 통합하여 컴퓨팅 리소스 전체에 패치를 배포해 안전하고 규정을 준수하는 환경을 유지합니다.
예: Systems Manager Patch Manager, Amazon Inspector

기술 3.2.5: 컴퓨팅 리소스에 대한 보안 관리 액세스를 구성합니다.
예: Systems Manager Session Manager, EC2 Instance Connect

기술 3.2.6: 파이프라인 내에서 취약성을 발견하고 해결하기 위한 보안 도구를 구성합니다.
예: Amazon Q Developer, Amazon CodeGuru 보안

기술 3.2.7: 생성형 AI 애플리케이션용 보호 및 가드레일을 구현합니다.
예: LLM 애플리케이션 보호용 생성형 AI OWASP 상위 10 개 적용

작업 3.3: 네트워크 보안 제어를 설계하고 문제를 해결합니다.

기술 3.3.1: 필요 시 네트워크 트래픽을 허용하거나 차단하기 위한 적절한 네트워크 제어를 설계하고 문제를 해결합니다. 예: 보안 그룹, 네트워크 ACL, AWS Network Firewall
기술 3.3.2: 하이브리드 네트워크와 멀티 클라우드 네트워크 간의 보안 연결을 설계합니다.
예: AWS Site-to-Site VPN, AWS Direct Connect, MAC 보안(MACsec)
기술 3.3.3: 하이브리드 환경과 AWS 간의 통신에 맞는 보안 워크로드 요구 사항을 결정하고 구성합니다. 예: AWS Verified Access 사용
기술 3.3.4: 보안 요구 사항을 기반으로 네트워크 세분화를 설계합니다. 예: 북부/남부 및 동부/서부 트래픽 보호, 격리된 서브넷
기술 3.3.5: 불필요한 네트워크 액세스를 식별합니다. 예: AWS Verified Access, Network Access Analyzer, Amazon Inspector 네트워크 연결성 조사 결과

콘텐츠 도메인 4: Identity and Access Management

작업 4.1: 인증 전략을 설계, 구현하고 문제를 해결합니다.

기술 4.1.1: 사용자, 애플리케이션 및 시스템 인증용 자격 증명 솔루션을 설계하고 설정합니다. 예: AWS IAM Identity Center, Amazon Cognito, 다중 인증(MFA), 자격 증명 제공업체(IdP) 통합
기술 4.1.2: 임시 자격 증명을 발급하는 메커니즘을 구성합니다.
예: AWS Security Token Service(AWS STS), Amazon S3 의 미리 서명된 URL
기술 4.1.3: 인증 문제를 해결합니다. 예: CloudTrail, Amazon Cognito, IAM Identity Center 권한 세트, AWS Directory Service

작업 4.2: 권한 부여 전략을 설계, 구현하고 문제를 해결합니다.

기술 4.2.1: 사용자, 애플리케이션 및 시스템 액세스에 대한 권한 부여 제어를 설계하고 평가합니다. 예: Amazon Verified Permissions, IAM 경로, IAM 역할 Anywhere, 크로스 계정 액세스를 위한 리소스 정책, IAM 역할 신뢰 정책
기술 4.2.2: 속성 기반 액세스 제어(ABAC) 및 역할 기반 액세스 제어(RBAC) 전략을 설계합니다. 예: 태그 또는 속성을 기반으로 리소스 액세스 구성

기술 4.2.3: 최소 권한의 원칙에 따라 IAM 정책을 설계, 해석 및 구현합니다. 예: 권한 범위, 세션 정책

기술 4.2.4: 인증 실패를 분석하여 원인이나 영향을 확인합니다. 예: IAM 정책 시뮬레이터, IAM Access Analyzer

기술 4.2.5: 리소스, 서비스 또는 엔터티에 부여된 의도하지 않은 권한, 인증 또는 상위 권한을 조사하고 수정합니다. 예: IAM Access Analyzer

콘텐츠 도메인 5: 데이터 보호

작업 5.1: 전송 중인 데이터에 대한 제어를 설계하고 구현합니다.

기술 5.1.1: 리소스에 접근하기 위해 연결할 때 암호화가 필요한 메커니즘을 설계하고 구성합니다. 예: Elastic Load Balancing(ELB) 보안 정책 구성, TLS 구성 적용

기술 5.1.2: 리소스에 안전하게 비공개로 액세스할 수 있는 메커니즘을 설계하고 구성합니다. 예: AWS PrivateLink, VPC 엔드포인트, AWS Client VPN, AWS Verified Access

기술 5.1.3: 전송 중인 리소스 간에 암호화를 설계하고 구성합니다.
예: Amazon EMR, Amazon Elastic Kubernetes Service(Amazon EKS), SageMaker AI, Nitro 암호화에서 노드 간 암호화 구성

작업 5.2: 저장 시 데이터에 대한 제어를 설계하고 구현합니다.

기술 5.2.1: 특정 요구 사항에 따라 저장 시 데이터 암호화를 설계, 구현 및 구성합니다.
예: AWS CloudHSM 또는 AWS Key Management Service(AWS KMS) 등의 적절한 암호화 키 서비스 선택, 클라이언트측 암호화 또는 서버 측 암호화 등의 적절한 암호화 유형 선택

기술 5.2.2: 데이터 무결성을 보호하는 메커니즘을 설계하고 구성합니다.
예: S3 객체 잠금, S3 Glacier 저장소 잠금, 버전 관리, 디지털 코드 서명, 파일 유효성 확인

기술 5.2.3: 데이터에 대한 자동 수명 주기 관리 및 보존 솔루션을 설계합니다.
예: S3 수명 주기 정책, S3 객체 잠금, Amazon Elastic File System(Amazon EFS) 수명 주기 정책, Amazon FSx for Lustre 백업 정책

기술 5.2.4: 안전한 데이터 복제 및 백업 솔루션을 설계 및 구성합니다.
예: Amazon Data Lifecycle Manager, AWS Backup, 랜섬웨어 보호, AWS DataSync

작업 5.3: 기밀 데이터, 자격 증명, 보안 암호, 암호화 키 자료를 보호하기 위한 제어 기능을 설계 및 구현합니다.

기술 5.3.1: 자격 증명과 보안 암호의 관리 방식과 회전 기능을 설계합니다.
예: AWS Secrets Manager
기술 5.3.2: 가져온 키 자료를 관리하고 사용합니다. 예: 가져온 키 자료를 관리 및 회전, 외부 키 저장소를 관리 및 구성
기술 5.3.3: 가져온 키 자료와 AWS 에서 생성한 키 자료 간의 차이점을 설명합니다.
기술 5.3.4: 민감한 데이터를 마스킹합니다. 예: CloudWatch Logs 데이터 보호 정책, Amazon Simple Notification Service(SNS) 메시지 데이터 보호
기술 5.3.5: 단일 AWS 리전이나 여러 리전에서 암호화 키와 인증서를 만들고 관리합니다.
예: AWS KMS 고객 관리형 AWS KMS 키, AWS Private Certificate Authority

콘텐츠 도메인 6: 보안 기반 및 거버넌스

작업 6.1: AWS 계정을 중앙에서 배포하고 관리하기 위한 전략을 개발합니다.

기술 6.1.1: AWS Organizations 을 사용하여 조직을 배포하고 구성합니다.
기술 6.1.2: 새 환경 및 기존 환경에서 AWS Control Tower 를 구현 및 관리하고 필요 시 선택할 수 있는 제어 및 사용자 지정 제어 기능을 배포합니다.
기술 6.1.3: 조직 정책을 구현하여 권한을 관리합니다. 예: SCP, RCP, AI 서비스 비동의 정책, 선언적 정책
기술 6.1.4: 보안 서비스를 한곳에서 관리합니다. 예: 위임된 관리자 계정
기술 6.1.5: AWS 계정 루트 사용자 자격 증명을 관리합니다. 예: 멤버 계정의 루트 액세스 중앙 집중화, MFA 관리, 비상용 우회 절차

작업 6.2: 클라우드 리소스를 안전하고 일관성 있게 배포할 수 있는 전략을 구현합니다.

기술 6.2.1: 코드형 인프라(IaC)를 사용하여 계정 전체에 클라우드 리소스를 일관성 있고 안전하게 배포합니다. 예: CloudFormation 스택 세트, 서드 파티 IaC 도구, CloudFormation Guard, cfn-lint
기술 6.2.2: 태그를 사용하여 AWS 리소스를 그룹화하여 관리합니다. 예: 부서, 비용 센터, 환경별로 그룹화

기술 6.2.3: 중앙 집중화된 소스에서 정책 및 구성을 배포하고 적용합니다.
예: AWS Firewall Manager
기술 6.2.4: AWS 계정 전체에서 리소스를 안전하게 공유합니다.
예: AWS Service Catalog, AWS Resource Access Manager(AWS RAM)

작업 6.3: AWS 리소스의 규정 준수 여부를 평가합니다.

기술 6.3.1: 규정 비준수 AWS 리소스를 탐지 및 해결하고 알림을 전송하는 규칙을 만들거나 사용합니다. 예: AWS Config 를 사용하여 경보를 집계하고 규정 비준수 리소스를 해결하는 Security Hub
기술 6.3.2: AWS 감사 서비스를 사용하여 증거를 수집하고 정리합니다. 예: AWS Audit Manager, AWS Artifact
기술 6.3.3: AWS 서비스를 사용하여 아키텍처가 AWS 보안 모범 사례를 준수하는지 평가합니다. 예: AWS Well-Architected Framework 도구

부록 A

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 순서는 시험에서의 상대적 가중치 또는 중요도를 의미하지 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. 일부 서비스는 시험 범위에 포함되지 않는 관계로 많은 서비스가 이 목록에서 제외되어 있습니다. 그러나 서비스의 보안 관련 사항은 시험 범위에 포함됩니다. 예를 들어 이 시험에는 S3 버킷 복제의 설정 단계에 대한 문항은 포함되어 있지 않습니다. 하지만 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.

분석:

- Amazon Athena
- Amazon OpenSearch Service

애플리케이션 통합:

- Amazon Simple Notification Service(SNS)
- AWS Step Functions

컴퓨팅:

- Amazon API Gateway
- Amazon EC2(예: EC2 Image Builder, EC2 Instance Connect)
- Amazon Elastic Kubernetes Service(Amazon EKS)
- Amazon EMR
- AWS Lambda
- Amazon Data Lifecycle Manager

개발자 도구

- AWS Fault Injection Service

사물 인터넷(IoT)

- AWS IoT Core

기계 학습:

- Amazon Bedrock
- Amazon CodeGuru Security
- Amazon Q Business
- Amazon Q Developer
- Amazon SageMaker AI

AWS 의 관리 및 거버넌스:

- AWS CloudFormation
- AWS CloudTrail
- AWS CloudTrail Lake
- Amazon CloudWatch
- AWS Config
- AWS Control Tower
- Amazon Managed Grafana
- AWS Organizations
- AWS Resilience Hub

- AWS Resource Access Manager(AWS RAM)
- AWS Service Catalog
- AWS Systems Manager
- AWS Trusted Advisor
- AWS 사용자 알림
- AWS Well-Architected Tool

네트워킹 및 콘텐츠 전송:

- Amazon Application Recovery Controller
- Amazon VPC
    - Network Access Analyzer
    - 네트워크 ACL
    - 보안 그룹
    - VPC 엔드포인트
    - AWS Site-to-Site VPN
    - 흐름 로그
    - VPC 엔드포인트
    - AWS Verified Access
- AWS Client VPN
- Amazon CloudFront
- Amazon Verified Permissions
- Amazon Route 53(예: Route 53 Resolver DNS Firewall)
- AWS Direct Connect
- Elastic Load Balancing(ELB)
- Network Access Analyzer
- AWS Transit Gateway

보안, 자격 증명 및 규정 준수:

- AWS Artifact
- AWS Audit Manager
- AWS Certificate Manager(ACM)

- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Amazon EC2 용 Automated Forensics Orchestrator
- Amazon GuardDuty
- AWS IAM Identity Center
- AWS Identity and Access Management(AWS IAM)
- Amazon Inspector
- AWS Key Management Service(AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Private Certificate Authority
- AWS Secrets Manager
- AWS Security Hub
- Amazon Security Lake
- AWS Security Token Service(AWS STS)
- AWS Shield
- AWS Shield Advanced
- AWS WAF

스토리지 및 데이터 관리:

- Amazon S3
- AWS Backup
- AWS DataSync
- Amazon Elastic File System(Amazon EFS)(예: EFS 수명 주기 정책)
- Amazon FSx for Lustre

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. 시험 대상의 직무와 전혀 관련이 없는 AWS 제품 및 서비스는 다음 목록에서 제외됩니다.

애플리케이션 통합:

- Amazon Managed Workflows for Apache Airflow(Amazon MWAA)

보안, 자격 증명 및 규정 준수:

- AWS Payment Cryptography

부록 B: SCS-C02 및 SCS-C03 비교

일대일 비교

다음 표에는 SCS-C02 시험(2025 년 12 월 1 일까지 사용) 및 SCS-C03 시험(2025 년 12 월 2 일부터 사용)의 도메인은 물론 각 도메인에서 채점되는 문항의 비율이 나와 있습니다.

SCS-C02 도메인	SCS-C03 도메인
도메인 1: 위협 탐지 및 인시던트 대응(14%)	콘텐츠 도메인 1: 탐지(채점 대상 콘텐츠의 16%)
도메인 2: 보안 로깅 및 모니터링(18%)	콘텐츠 도메인 2: 인시던트 대응(14%)
도메인 3: 인프라 보안(20%)	콘텐츠 도메인 3: 인프라 보안(18%)
도메인 4: Identity and Access Management(16%)	콘텐츠 도메인 4: Identity and Access Management(20%)
도메인 5: 데이터 보호(18%)	콘텐츠 도메인 5: 데이터 보호(18%)
도메인 6: 관리 및 보안 거버넌스(14%)	콘텐츠 도메인 6: 보안 기반 및 거버넌스(14%)

SCS-C03 에 추가된 내용

작업 2.2.3 에는 다음 내용이 추가되었습니다.

- 2.2.3 AWS 보안 서비스의 조사 결과를 확인하여 이벤트의 범위와 영향을 평가합니다.

작업 3.1.4 에는 다음 내용이 추가되었습니다.

- 3.1.4 AWS 엣지 서비스 및 서드 파티 서비스와의 통합을 구성합니다. 예: 개방형 사이버 보안 스키마 프레임워크(OCSF) 형식으로 데이터 수집, 서드 파티 WAF 규칙 사용

작업 3.2.7 에는 다음 내용이 추가되었습니다.

- 3.2.7 생성형 AI 애플리케이션용 보호 및 가드레일을 구현합니다. 예: LLM 애플리케이션 보호용 생성형 AI OWASP 상위 10 개 적용

작업 5.1.3 에는 다음 내용이 추가되었습니다.

- 5.1.3 전송 중인 리소스 간에 암호화를 설계하고 구성합니다. 예: Amazon EMR, Amazon Elastic Kubernetes Service(Amazon EKS), SageMaker AI, Nitro 암호화에서 노드 간 암호화 구성

작업 5.3.3 에는 다음 내용이 추가되었습니다.

- 5.3.3 가져온 키 자료와 AWS 에서 생성한 키 자료 간의 차이점을 설명합니다.

작업 5.3.4 에는 다음 내용이 추가되었습니다.

- 5.3.4 민감한 데이터를 마스킹합니다. 예: CloudWatch Logs 데이터 보호 정책, Amazon Simple Notification Service(SNS) 메시지 데이터 보호

작업 5.3.5 에는 다음 내용이 추가되었습니다.

- 5.3.5 단일 AWS 리전이나 여러 리전에서 암호화 키와 인증서를 만들고 관리합니다. 예: AWS KMS 고객 관리형 AWS KMS 키, AWS Private Certificate Authority

SCS-C03 에서 삭제된 내용

작업 6.4 에서 다음 내용이 제거되었습니다.

- 아키텍처 검토 및 비용 분석을 통해 보안 관련 허점을 식별합니다.

작업 1.1 에서 다음 내용이 제거되었습니다.

- AWS 보안 조사 결과 형식(ASFF)

작업 1.3 에서 다음 내용이 제거되었습니다.

- AWS 보안 인시던트 대응 가이드

작업 2.5 에서 다음 내용이 제거되었습니다.

- 로그 형식 및 구성 요소(예: CloudTrail 로그)

작업 3.3 에서 다음 내용이 제거되었습니다.

- 호스트 기반 보안(예: 방화벽, 강화)
- 호스트 기반 보안 메커니즘 활성화(예: 호스트 기반 방화벽)

작업 3.4 에서 다음 내용이 제거되었습니다.

- 연결성을 분석하는 방법(예: VPC Reachability Analyzer 및 Amazon Inspector 사용)
- 기본 TCP/IP 네트워킹 개념(예: UDP 및 TCP 비교, 포트, Open Systems Interconnection(OSI) 모델, 네트워크 운영 체제 유틸리티)
- 네트워크 연결 문제 식별, 해석 및 우선 순위 지정(예: Amazon Inspector 네트워크 연결성 사용)

작업 4.2 에서 다음 내용이 제거되었습니다.

- 정책의 구성 요소 및 영향(예: 보안 주체, 작업, 리소스, 조건)

작업 5.1 에서 다음 내용이 제거되었습니다.

- TLS 개념
- 프라이빗 VIF 와 퍼블릭 VIF 를 사용한 크로스 리전 네트워킹 설계

작업 5.2 에서 다음 내용이 제거되었습니다.

- S3 정적 웹 사이트 호스팅을 구성합니다.

SCS-C03 에서 재분류된 내용

SCS-C02 에서 SCS-C03 으로 전환하는 과정에서 다음과 같이 주요 콘텐츠 개편 작업이 진행되었습니다.

SCS-C02 도메인 1 과 2 가 다음과 같이 재구성되었습니다.

- '위협 탐지 및 인시던트 대응'과 '보안 로깅 및 모니터링'은 이제 다음과 같이 분류됩니다.
  - 도메인 1: 탐지
  - 도메인 2: 인시던트 대응

도메인 6 의 이름이 SCS-C03 이름으로 변경되었습니다.

- '관리 및 보안 거버넌스'에서 '보안 기반 및 거버넌스'로 변경

다음 작업 설명이 재분류되었습니다.

SCS-C02 작업 설명 1.1 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.1 AWS 계정이나 조직용 모니터링 및 경보 기능을 설계하고 구현합니다.
- 1.2 로깅을 설계 및 구현합니다.
- 2.1 인시던트 대응 계획을 설계 및 테스트합니다.
- 2.2 보안 이벤트에 대응합니다.

SCS-C02 작업 설명 1.2 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.1 AWS 계정이나 조직용 모니터링 및 경보 기능을 설계하고 구현합니다.
- 1.2 로깅을 설계 및 구현합니다.

SCS-C02 작업 설명 1.3 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 2.1 인시던트 대응 계획을 설계 및 테스트합니다.
- 2.2 보안 이벤트에 대응합니다.

SCS-C02 작업 설명 2.1 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.1 AWS 계정이나 조직용 모니터링 및 경보 기능을 설계하고 구현합니다.

SCS-C02 작업 설명 2.2 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.1 AWS 계정이나 조직용 모니터링 및 경보 기능을 설계하고 구현합니다.
- 1.2 로깅을 설계 및 구현합니다.
- 1.3 보안 모니터링, 로깅, 경보 관련 문제를 해결합니다.

SCS-C02 작업 설명 2.3 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.2 로깅을 설계 및 구현합니다.

SCS-C02 작업 설명 2.4 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.2 로깅을 설계 및 구현합니다.
- 1.3 보안 모니터링, 로깅, 경보 관련 문제를 해결합니다.

SCS-C02 작업 설명 2.5 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.2 로깅을 설계 및 구현합니다.

SCS-C02 작업 설명 3.1 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.2 로깅을 설계 및 구현합니다.
- 3.1 네트워크 엣지 서비스의 보안 제어를 설계, 구현하고 문제를 해결합니다.

SCS-C02 작업 설명 3.2 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.2 로깅을 설계 및 구현합니다.
- 3.3 네트워크 보안 제어를 설계하고 문제를 해결합니다.
- 5.1 전송 중인 데이터에 대한 제어를 설계하고 구현합니다.
- 6.2 클라우드 리소스를 안전하고 일관성 있게 배포할 수 있는 전략을 구현합니다.

SCS-C02 작업 설명 3.3 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 3.2 컴퓨팅 워크로드에 대한 보안 제어를 설계, 구현하고 문제를 해결합니다.
- 5.3 기밀 데이터, 자격 증명, 보안 암호, 암호화 키 자료를 보호하기 위한 제어 기능을 설계 및 구현합니다.

SCS-C02 작업 설명 3.4 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.2 로깅을 설계 및 구현합니다.
- 3.3 네트워크 보안 제어를 설계하고 문제를 해결합니다.

SCS-C02 작업 설명 4.1 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 4.1 인증 전략을 설계, 구현하고 문제를 해결합니다.

SCS-C02 작업 설명 4.2 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 4.2 권한 부여 전략을 설계, 구현하고 문제를 해결합니다.

SCS-C02 작업 설명 5.1 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 3.2 컴퓨팅 워크로드에 대한 보안 제어를 설계, 구현하고 문제를 해결합니다.
- 3.3 네트워크 보안 제어를 설계하고 문제를 해결합니다.
- 5.1 전송 중인 데이터에 대한 제어를 설계하고 구현합니다.

SCS-C02 작업 설명 5.2 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 4.2 권한 부여 전략을 설계, 구현하고 문제를 해결합니다.
- 5.2 저장 시 데이터에 대한 제어를 설계하고 구현합니다.

SCS-C02 작업 설명 5.3 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 5.2 저장 시 데이터에 대한 제어를 설계하고 구현합니다.

SCS-C02 작업 설명 5.4 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 5.2 저장 시 데이터에 대한 제어를 설계하고 구현합니다.
- 5.3 기밀 데이터, 자격 증명, 보안 암호, 암호화 키 자료를 보호하기 위한 제어 기능을 설계 및 구현합니다.

SCS-C02 작업 설명 6.1 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 4.2 권한 부여 전략을 설계, 구현하고 문제를 해결합니다.
- 6.1 AWS 계정을 중앙에서 배포하고 관리하기 위한 전략을 개발합니다.

SCS-C02 작업 설명 6.2 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 6.2 클라우드 리소스를 안전하고 일관성 있게 배포할 수 있는 전략을 구현합니다.

SCS-C02 작업 설명 6.3 은 SCS-C03 에서 다음 작업에 포함됩니다.

- 1.1 AWS 계정이나 조직용 모니터링 및 경보 기능을 설계하고 구현합니다.
- 5.2 저장 시 데이터에 대한 제어를 설계하고 구현합니다.
- 6.3 AWS 리소스의 규정 준수 여부를 평가합니다.

SCS-C02 작업 설명 6.4 는 SCS-C03 에서 다음 작업에 포함됩니다.

- 2.1 인시던트 대응 계획을 설계 및 테스트합니다.
- 1.1 AWS 계정이나 조직용 모니터링 및 경보 기능을 설계하고 구현합니다.
- 6.3 AWS 리소스의 규정 준수 여부를 평가합니다.

설문 조사

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