aws training and certification

AWS Certified Security – Specialty (SCS-C01) 시험 안내서

소개

AWS Certified Security – Specialty (SCS-C01) 시험은 보안 역할을 수행하는 개인을 대상으로 합니다. 이 시험은 응시자가 AWS 플랫폼 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 이상의 프로덕션 배포 경험을 바탕으로 구축된 컴피턴시
- 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 5 년의 IT 보안 경험이 있어야 합니다. 또한 대상 응시자는 AWS 워크로드 보안에 대해 2 년 이상의 실무 경험이 있어야 합니다.

AWS 지식 권장 사항

대상 응시자는 다음과 같은 지식이 있어야 합니다.

- AWS 공동 책임 모델 및 해당 애플리케이션
- AWS 에서 워크로드에 대한 보안 제어
- 로깅 및 모니터링 전략
- 클라우드 보안 위협 모델
- 패치 관리 및 보안 자동화
- 서드 파티 도구 및 서비스로 AWS 보안 서비스를 강화하는 방법
- BCP 및 백업을 포함한 재해 복구 제어
- 암호화

- 액세스 제어
- 데이터 보존

대상 응시자가 갖추지 않아도 되는 것은 무엇입니까?

다음은 대상 응시자가 수행하지 않아도 될 것으로 예상되는 관련 작업 태스크의 목록입니다(전체 목록은 아님). 다음 항목은 시험 범위에 포함되지 않는 것으로 간주됩니다.

- 구성 생성 또는 쓰기
- 구현(SysOps)
- 특정 언어(예: Perl 또는 Java)로 스크립팅 시연

시험에서 다룰 수 있는 특정 도구 및 기술에 대한 자세한 목록과 범위 포함 여부가 표시된 AWS 서비스 목록은 부록을 참조하십시오.

시험 콘텐츠

응답 유형

이 시험의 문항은 두 가지 유형으로 제공됩니다.

- **선다형:** 정답 1 개와 오답 3 개(정답 이외의 답)가 있습니다.
- **다답형:** 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 있습니다.

채점 대상이 아닌 콘텐츠

시험에는 점수에 반영되지 않아 채점 대상이 아닌 15 개의 문항이 포함되어 있습니다. AWS 는 채점 대상이 아닌 질문에 대한 응시자 성과 정보를 수집하여 추후 채점 대상 질문으로 사용할 수 있도록 이러한 질문을 평가합니다. 이러한 채점 대상이 아닌 질문은 시험에서 식별되지 않습니다.

시험 결과

AWS Certified Security – Specialty (SCS-C01) 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 기준의 스케일링된 점수로 채점됩니다. 합격 최소 점수는 750 점입니다. 응시자의 점수는 전반적인 시험 성적과 합격 여부를 보여줍니다. 스케일링된 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. 이 정보는 시험 성적에 대한 일반적인 피드백을 제공하기 위한 것입니다. 시험은 보상 점수 모델을 사용하므로 각 섹션에서 합격 점수를 얻을 필요는 없습니다. 전체 시험에만 합격하면 됩니다.

시험의 섹션마다 특정 가중치가 적용되므로 일부 섹션은 다른 섹션보다 문항 수가 많습니다. 표에는 응시자의 장단점을 보여주는 일반 정보가 포함되어 있습니다. 섹션 레벨 피드백을 검토할 때 주의하시기 바랍니다.

콘텐츠 개요

이 시험 가이드는 시험의 가중치, 테스트 영역 및 목표를 제공하며, 이 시험에 대한 종합적인 콘텐츠 목록은 아닙니다. 하지만 시험을 준비하는 데 도움이 되는 각 목표에 대한 추가 배경 정보가 있습니다. 다음 표에는 주요 콘텐츠 영역과 가중치가 나열되어 있습니다. 이 표는 추가 배경 정보가 포함되어 있는 전체 시험 콘텐츠 개요 앞에 나옵니다. 각 영역의 백분율은 채점되는 콘텐츠만 나타냅니다.

영역	시험 비율(%)
영역 1: 사고 대응	12%
영역 2: 로깅 및 모니터링	20%
영역 3: 인프라 보안	26%
영역 4: Identity and Access Management	20%
영역 5: 데이터 보호	22%
합계	**100%**

영역 1: 사고 대응

1.1 특정 AWS 침해 알림에서 손상이 의심되는 인스턴스 또는 유출 액세스 키를 진단합니다.

- 특정 EC2 인스턴스에 대한 AWS 침해 보고서에 따라 포렌식 조사의 일환으로 인스턴스를 안전하게 격리합니다.
- 보고된 인스턴스와 관련된 로그를 분석하여 위반을 확인하고 관련 데이터를 수집합니다.
- 추후 심층적인 분석이나 법적 규정 준수를 위해 의심되는 인스턴스에서 메모리 덤프를 캡처합니다.

1.2 사고 대응 전략에 관련 AWS 서비스가 포함되어 있는지 확인합니다.

- 기본 보안 구성에 변경 사항이 있는지 확인합니다.
- 목록에 사고 대응을 지원하는 서비스, 프로세스 또는 절차가 생략되는지 확인합니다.
- 문제 해결을 위한 서비스, 프로세스, 절차를 제시합니다.

1.3 자동 알림 구성을 확인하고 보안 관련 사고와 새로운 문제에 대한 가능한 조치 방안을 실행합니다.

- 신규/변경/제거 리소스에 대한 적합성 평가를 자동화합니다.
- 일반적인 인프라 구성 오류에 대해 규칙 기반 알림을 적용합니다.
- 이전 보안 사고를 검토하고 기존 시스템의 개선 사항을 제시합니다.

영역 2: 로깅 및 모니터링

2.1 보안 모니터링 및 알림을 설계 및 구현합니다.

- 아키텍처를 분석하고 모니터링 요구 사항 및 모니터링 통계 소스를 식별합니다.
- 아키텍처를 분석하여 모니터링 및 알림을 자동화하는 데 사용할 수 있는 AWS 서비스를 판단합니다.
- 사용자 지정 애플리케이션 모니터링에 대한 요구 사항을 분석하고 이를 달성할 수 있는 방법을 판단합니다.
- 자동화 도구/스크립트를 설정하여 정기적인 감사를 수행합니다.

2.2 보안 모니터링 및 알림 문제를 해결합니다.

- 알려진 이벤트가 예상된 알림 없이 발생한 경우, 서비스 기능 및 구성을 분석하고 문제를 해결합니다.
- 알려진 이벤트가 예상된 알림 없이 발생한 경우, 권한을 분석하고 문제를 해결합니다.
- 사용자 지정 애플리케이션이 애플리케이션 통계를 보고하지 않는 경우, 구성을 분석하고 문제를 해결합니다.
- 시스템 및 사용자 활동의 감사 추적을 검토합니다.

2.3 로깅 솔루션을 설계하고 구현합니다.

- 아키텍처를 분석하고 로그 수집을 위한 로깅 요구 사항 및 소스를 식별합니다.
- AWS 모범 사례에 따라 요구 사항을 분석하고 내구성이 강하고 안전한 로그 스토리지를 구현합니다.
- 아키텍처를 분석하여 로그 수집 및 분석을 자동화하는 데 사용할 수 있는 AWS 서비스를 판단합니다.

2.4 로깅 솔루션 문제 해결

- 로그가 없는 경우 잘못된 구성을 확인하고 문제 해결 단계를 정의합니다.
- 로깅 액세스 권한을 분석하여 잘못된 구성을 확인하고 문제 해결 단계를 정의합니다.
- 보안 정책 요구 사항에 따라 올바른 로그 수준, 유형 및 소스를 판단합니다.

영역 3: 인프라 보안

3.1 AWS 의 엣지 보안을 설계합니다.

- 특정 워크로드에 대해 공격 대상 영역을 평가하여 최소화합니다.
- 공격 영향 범위를 줄입니다(예: 계정 및 리전 기반으로 애플리케이션 배포).
- 적합한 AWS 및/또는 WAF, CloudFront 및 Route 53 과 같은 서드 파티 엣지 서비스를 선택하여 DDoS 공격으로부터 보호하거나 애플리케이션 수준 공격을 필터링합니다.
- 애플리케이션에 대한 일련의 엣지 보호 요구 사항이 있는 경우 메커니즘을 평가하여 규정 준수 위반을 방지 및 감지하고 필요한 변경 사항을 제시합니다.
- WAF 규칙을 테스트하여 악성 트래픽이 차단되는지 확인합니다.

3.2 보안 네트워크 인프라를 설계하고 구현합니다.

- 불필요한 네트워크 포트 및 프로토콜을 비활성화합니다.
- 일련의 엣지 보호 요구 사항이 있는 경우 애플리케이션의 보안 그룹과 NACL 이 규정을 준수하는지 평가하고 필요한 변경 사항을 제시합니다.
- 보안 요구 사항에 따라 필요한 수신/송신 액세스를 최소로 허용하는 네트워크 세분화(예: 보안 그룹 및 NACL)에 대해 결정합니다.
- VPN 또는 Direct Connect 의 사용 사례를 확인합니다.
- VPC Flow Logs 를 활성화하기 위한 사용 사례를 확인합니다.
- VPC 의 네트워크 인프라에 대한 설명에 따라 보안 운영을 위한 서브넷과 게이트웨이 사용을 분석합니다.

3.3 보안 네트워크 인프라 문제 해결

- 네트워크 트래픽 흐름이 거부되는 위치를 확인합니다.
- 특정 구성에 따라 보안 그룹과 NACL 이 올바르게 구현되었는지 확인합니다.

3.4 호스트 기반 보안 설계 및 구현

- 특정 보안 요구 사항에 따라 Inspector, SSM 을 포함하여 호스트 기반 보호 기능을 설치 및 구성합니다.
- iptables 와 같은 호스트 기반 방화벽을 사용할 시기를 결정합니다.
- 호스트 강화 및 모니터링 방법을 제시합니다.

영역 4: Identity and Access Management

4.1 AWS 리소스에 액세스할 수 있도록 확장 가능한 권한 부여 및 인증 시스템을 설계하고 구현합니다.

- 워크로드에 대한 특정 설명에 따라 AWS 서비스에 대한 액세스 제어 구성을 분석하고 위험을 줄이는 권장 사항을 제시합니다.
- 조직에서 AWS 계정을 관리하는 방법에 대한 설명에 따라 루트 사용자의 보안을 확인합니다.
- 조직의 규정 준수 요구 사항에 따라 사용자 정책 및 리소스 정책의 적용 시기를 판단합니다.
- 조직의 정책 내에서 디렉터리 서비스를 IAM 에 연동할 시기를 판단합니다.
- 사용자, 그룹, 역할 및 정책을 포함하는 확장 가능한 권한 부여 모델을 설계합니다.
- 데이터 및 AWS 리소스의 개별 사용자를 식별하고 제한합니다.
- 정책을 검토하여 사용자/시스템이 책임 범위를 넘어서는 기능을 수행하지 못하도록 제한하고 책임을 적절하게 분리합니다.

4.2 AWS 리소스에 액세스하기 위한 권한 부여 및 인증 시스템 문제를 해결합니다.

- 사용자가 S3 버킷 콘텐츠에 액세스할 수 없는 문제를 조사합니다.
- 사용자가 역할을 다른 계정으로 전환할 수 없는 문제를 조사합니다.
- Amazon EC2 인스턴스에서 특정 AWS 리소스에 액세스할 수 없는 문제를 조사합니다.

영역 5: 데이터 보호

5.1 키 관리 및 사용을 설계 및 구현합니다.

- 특정 시나리오를 분석하여 적절한 키 관리 솔루션을 판단합니다.
- 일련의 데이터 보호 요구 사항이 있는 경우, 키 사용을 평가하고 필요한 변경 사항을 제시합니다.
- 키 손상 이벤트에 대한 영향 범위를 확인 및 제어하고 해당 사항을 포함하는 솔루션을 설계합니다.

5.2 키 관리 문제 해결

- KMS 키 부여와 IAM 정책의 차이점을 분석합니다.
- 특정 키에 대해 서로 다른 충돌 정책이 있는 경우 우선 순위를 추론합니다.
- 손상이 발생할 경우 사용자 또는 서비스의 사용 권한을 취소하는 시기와 방법을 판단합니다.

5.3 저장 데이터 및 전송 중인 데이터에 대한 데이터 암호화 솔루션을 설계하고 구현합니다.

- 일련의 데이터 보호 요구 사항이 있는 경우 워크로드의 저장 데이터 보안을 평가하고 필요한 변경 사항을 제시합니다.
- 특정 AWS 서비스에서만 사용할 수 있는 키에 대한 정책을 검증합니다.
- 태그 기반 데이터 분류를 통해 데이터의 규정 준수 상태를 구분하고 문제 해결을 자동화합니다.
- 다양한 전송 암호화 기술을 평가하고 적절한 방법(예: TLS, IPsec, 클라이언트 측 KMS 암호화)을 선택합니다.

부록

시험에서 다룰 수 있는 주요 도구, 기술 및 개념은 무엇입니까?

다음은 시험에서 다룰 수 있는 도구 및 기술 목록입니다(전체 목록은 아님). 이 목록은 변경될 수 있으며 시험에서 다루는 서비스, 기능 또는 기술의 일반적인 범위를 이해하는 데 도움이 됩니다. 이 목록에서 일반 도구 및 기술은 특별한 순서 없이 표시됩니다. AWS 서비스는 기본 기능에 따라 그룹화됩니다. 이러한 기술 중 일부는 시험에서 다른 기술보다 더 많이 다룰 수 있지만, 이 목록에서 순서 및 배치는 상대적인 비중이나 중요성을 나타내지 않습니다.

- AWS CLI
- AWS SDK
- AWS 관리 콘솔
- 네트워크 분석 도구(패킷 캡처 및 흐름 캡처)
- SSH/RDP
- Signature Version 4
- TLS
- 인증서 관리
- 코드형 인프라(IaC)

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.

관리 및 거버넌스:

- AWS Audit Manager
- AWS CloudTrail

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

네트워킹 및 콘텐츠 전송:

- Amazon Detective
- AWS Firewall Manager
- AWS Network Firewall
- AWS Security Hub
- AWS Shield
- Amazon VPC
    - VPC 엔드포인트
    - 네트워크 ACL
    - 보안 그룹
- AWS WAF

보안, 자격 증명 및 규정 준수:

- AWS Certificate Manager(ACM)
- AWS CloudHSM
- AWS Directory Service
- Amazon GuardDuty
- AWS Identity and Access Management(IAM)
- Amazon Inspector
- AWS Key Management Service(AWS KMS)
- Amazon Macie
- AWS Single Sign-On

대상 범위가 아닌 AWS 서비스 및 기능

다음은 시험에서 다루지 않는 AWS 서비스 및 기능의 목록입니다(전체 목록은 아님). 여기에 나열된 서비스와 기능이 시험 콘텐츠에서 제외되는 모든 AWS 서비스 및 기능을 나타내지는 않습니다. 시험의 대상 직무 역할과 전혀 관련이 없는 서비스 또는 기능은 관련성이 없는 것으로 간주되므로 이 목록에서 제외됩니다.

대상 범위가 아닌 AWS 서비스 및 기능에는 다음이 포함됩니다.

- 애플리케이션 개발 서비스
- IoT 서비스
- 기계 학습(ML) 서비스
- 미디어 서비스
- 마이그레이션 및 전송 서비스