aws training and certification

AWS 공인 보안 - 전문 분야
AWS Certified Security – Specialty
(SCS-C01) 시험 샘플 문항

1) 회사의 VPC 및 KMS 간 통신은 AWS 네트워크 내에서 모두 주고받아야 하며 퍼블릭 서비스 엔드포인트를 사용해서는 안 된다고 기업 클라우드 보안 정책에 명시되어 있습니다.

다음 작업 중 이 요구 사항을 가장 잘 충족하는 조합은 무엇입니까? (2개를 선택하십시오.)

A) 회사의 VPC 종단점 ID를 참조하는 AWS KMS 키 정책에 `aws:sourceVpce` 조건을 추가한다.
B) VPC에서 VPC 인터넷 게이트웨이를 제거하고 VPC에 가상 프라이빗 게이트웨이를 추가하여 직접 퍼블릭 인터넷 연결을 차단한다.
C) 프라이빗 DNS가 활성화된 AWS KMS에 대한 VPC 종단점을 생성한다.
D) KMS 키 가져오기 기능을 사용하여 VPN을 통해 AWS KMS 키를 안전하게 전송한다.
E) AWS KMS 키 정책에 `"aws:SourceIp": "10.0.0.0/16"` 조건을 추가한다.

2) 애플리케이션 팀에서 두 가지 애플리케이션으로 솔루션을 설계 중입니다. 보안 팀은 이 애플리케이션 중 하나가 민감한 데이터로 로그를 생성하기 때문에 서로 다른 두 장소에서 애플리케이션 로그를 캡처하려 합니다.

최소한의 위험과 노력으로 요구 사항을 충족할 수 있는 솔루션은 무엇입니까?

A) Amazon CloudWatch Logs를 사용하여 모든 로그를 캡처하고, 로그 파일을 분석하는 AWS Lambda 함수를 작성하고, 민감한 데이터를 다른 로그로 이동한다.
B) 각 애플리케이션에 하나씩 로그 그룹을 두 개로 하여 Amazon CloudWatch Logs를 사용하고, AWS IAM 정책을 사용하여 로그 그룹에 대한 액세스를 필요에 따라 제어한다.
C) 로그를 파일 하나로 집계하고, Amazon CloudWatch Logs를 사용하고, 그런 다음 CloudWatch 지표 필터 두 개를 설계하여 로그에서 민감한 데이터를 필터링한다.
D) Amazon EC2 인스턴스의 로컬 스토리지에 민감한 데이터 로그를 저장하는 애플리케이션에 로직을 추가하고, Amazon EC2 인스턴스에 로그인하여 민감한 로그를 안전한 위치로 이동하는 배치 스크립트를 작성한다.

3) 보안 엔지니어는 3티어 보안 그룹 애플리케이션에 대해 보안 그룹 규칙을 설정해야 합니다.

- **프레젠테이션 티어 - 사용자가 웹을 통하여 액세스하고, 보안 그룹 `presentation-sg`가 보호함**
- **로직 티어 - 프레젠테이션 티어에서 HTTPS를 통해 액세스되는 RESTful API로, 보안 그룹 `logic-sg`가 보호함**
- **데이터 티어 - 로직 티어에서 포트 1433을 통해 액세스되는 SQL Server 데이터베이스로, 보안 그룹 `data-sg`가 보호함**

이 애플리케이션의 보안과 기능을 보장하려면 다음 보안 그룹 규칙을 어떻게 조합해야 합니까? (3개를 선택하십시오.)

A) `presentation-sg`: 0.0.0.0/0에서 포트 80 및 포트 443 허용
B) `data-sg`: `presentation-sg`에서 포트 1433 허용
C) `data-sg`: `logic-sg`에서 포트 1433 허용
D) `presentation-sg`: `data-sg`에서 포트 1433 허용
E) `logic-sg`: `presentation-sg`에서 포트 443 허용
F) `logic-sg`: 0.0.0.0/0에서 포트 443 허용

4) 보안 엔지니어가 제품 팀과 함께 AWS에서 웹 애플리케이션을 빌드하는 중입니다. 이 애플리케이션은 Amazon S3를 사용하여 정적 콘텐츠를 호스팅하고, Amazon API Gateway를 사용하여 RESTful 서비스를 제공하고, 백엔드 데이터 스토어로 Amazon DynamoDB를 사용합니다. SAML 자격 증명 공급자를 통해 노출되는 디렉터리에 이미 사용자가 존재합니다.

사용자가 웹 애플리케이션에 인증하고 API를 호출할 수 있도록 하려면 이 엔지니어는 다음 작업을 어떻게 조합하여 수행해야 합니까? (3개를 선택하십시오.)

A) AWS Lambda를 사용하여 사용자 지정 권한 부여 서비스를 생성한다.
B) Amazon Cognito 사용자 풀 속성에 속성을 매핑하도록 Amazon Cognito에서 SAML 자격 증명 공급자를 구성한다.
C) 신뢰 당사자로 Amazon Cognito 사용자 풀 속성을 추가하도록 SAML 자격 증명 공급자를 생성한다.
D) 소셜 로그인 공급자를 통합하도록 Amazon Cognito 자격 증명 풀을 생성한다.
E) DynamoDB를 업데이트하여 사용자 이메일 주소 및 암호를 저장한다.
F) API Gateway를 업데이트하여 Amazon Cognito 사용자 풀 권한 부여자를 사용한다.

5) AWS에서 웹 애플리케이션을 호스팅하고 Amazon S3 버킷을 사용하여 이미지를 저장하는 회사가 있습니다. 사용자는 버킷에서 객체를 읽을 수 있어야 합니다. 보안 엔지니어는 다음 버킷 정책을 작성하여 퍼블릭 읽기 액세스를 부여했습니다.

```
{
   "ID":"Policy1502987489630",
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1502987487640",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":"arn:aws:s3:::appbucket",
         "Principal":"*"
      }
   ]
}
```

하지만 객체 읽기를 시도하면 다음과 같은 오류가 표시됩니다. "Action does not apply to any resource(s) in statement."

오류를 해결하려면 엔지니어는 어떻게 해야 합니까?

A) PutBucketPolicy 권한을 적용하여 IAM 권한을 변경한다.
B) 정책에 버킷 이름과 동일한 이름이 있는지 확인한다. 없으면 동일한 이름을 만든다.
C) `resource` 섹션을 `"arn:aws:s3:::appbucket/*"`로 변경한다.
D) `s3:ListBucket` 작업을 추가한다.

6) 어떤 회사에서 데이터베이스 호스트를 자체 VPC에 배치하고, 애플리케이션 티어 및 웹 티어가 포함된 다른 VPC에 VPC 피어링을 설정하기로 결정했습니다. 애플리케이션 서버는 데이터베이스에 연결할 수 없습니다.

문제를 해결하려면 어떤 네트워크 문제 해결 단계를 따라야 합니까? (2개를 선택하십시오.)

A) 애플리케이션 서버가 프라이빗 서브넷 또는 퍼블릭 서브넷에 있는지 확인한다.
B) 애플리케이션 서브넷의 라우팅 테이블에서 VPC 피어링 연결에 대한 경로를 확인한다.
C) 데이터베이스 서브넷의 NACL에서 인터넷의 트래픽을 허용하는 규칙을 확인한다.
D) 데이터베이스 보안 그룹에서 애플리케이션 서버의 트래픽을 허용하는 규칙을 확인한다.
E) 데이터베이스 VPC에 인터넷 게이트웨이가 있는지 확인한다.

7) 보안 엔지니어가 Amazon DynamoDB 테이블에서 항목을 검색하는 새로운 AWS Lambda 함수를 테스트할 때, 이 함수가 Amazon CloudWatch Logs에 어떤 데이터도 기록하지 않는 것을 확인했습니다.

다음 정책은 Lambda 함수가 맡은 역할에 할당되었습니다.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Dynamo-1234567",
         "Action": [
            "dynamodb:GetItem"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
}
```

이 함수가 제대로 기록할 수 있도록 하기 위해 추가해야 하는 최소 권한 정책은 무엇입니까?

A)
```
{
   "Sid": "Logging-12345",
   "Resource": "*",
   "Action": [
      "logs:*"
   ],
   "Effect": "Allow"
}
```

B)
```
{
   "Sid": "Logging-12345",
   "Resource": "*",
   "Action": [
      "logs:CreateLogStream"
   ],
   "Effect": "Allow"
}
```

C)
```
{
   "Sid": "Logging-12345",
   "Resource": "*",
   "Action": [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
   ],
   "Effect": "Allow"
}
```

D)
```
{
   "Sid": "Logging-12345",
```

```
      "Resource": "*",
      "Action": [
         "logs:CreateLogGroup",
         "logs:CreateLogStream",
         "logs:DeleteLogGroup",
         "logs:DeleteLogStream",
         "logs:getLogEvents",
         "logs:PutLogEvents"
      ],
      "Effect": "Allow"
   }
```

8) 한 회사에서 Amazon S3에서 데이터 레이크를 구축하고 있습니다. 이 데이터는 민감한 정보를 담은 작은 파일 수백만 개로 구성되어 있습니다. 보안 팀에는 이 아키텍처에 대한 다음과 같은 요구 사항이 있습니다.

- **전송 중 데이터를 암호화해야 합니다.**
- **저장 상태의 데이터를 암호화해야 합니다.**
- **프라이빗 버킷이어야 하지만, 실수로 퍼블릭으로 설정하더라도 데이터는 비밀로 유지되어야 합니다.**

이러한 요구 사항을 충족하는 단계 조합은 무엇입니까? (2개를 선택하십시오.)

A) S3 버킷에서 Amazon S3 관리형 암호화 키(SSE-S3)와 서버 측 암호화를 사용하여 AES-256 암호화를 활성화한다.

B) S3 버킷에서 AWS KMS 관리형 암호화 키(SSE-KMS)와 서버 측 암호화를 사용하여 기본 암호화를 활성화한다.

C) `PutObject` 요청에 `aws:SecureTransport`가 포함되지 않은 경우, 거부가 포함된 버킷 정책을 추가한다.

D) `aws:SourceIp`가 있는 버킷 정책을 추가하여 사내 인트라넷에서만 업로드 및 다운로드를 허용한다.

E) Amazon Macie를 활성화하여 데이터 레이크의 S3 버킷을 모니터링하고 변경 사항에 대해 조치를 취한다.

9) 보안 엔지니어는 모든 회사 계정에서 모든 API 호출을 수집하고, 온라인으로 유지하고, 90일간 즉시 분석에 사용할 수 있도록 해야 합니다. 규정 준수를 위해 이 데이터는 7년간 복원 가능해야 합니다.

확장성 있고 경제적인 방법으로 이 보존 요구 사항을 충족하려면 어떤 단계를 따라야 합니까?

A) 모든 계정에서 버전 관리가 활성화된 중앙 집중식 Amazon S3 버킷에 로깅하도록 AWS CloudTrail 로깅을 활성화한다. 데이터를 매일 Amazon Glacier로 이동하고 90일 후 데이터가 만료되도록 수명 주기 정책을 설정한다.

B) 모든 계정에서 S3 버킷에 로깅하도록 AWS CloudTrail 로깅을 활성화한다. 각 버킷의 데이터가 7년 후 만료되도록 수명 주기 정책을 설정한다.

C) 모든 계정에서 Amazon Glacier에 로깅하도록 AWS CloudTrail 로깅을 활성화한다. 데이터가 7년 후 만료되도록 수명 주기 정책을 설정한다.

D) 모든 계정에서 중앙 집중식 Amazon S3 버킷에 로깅하도록 AWS CloudTrail 로깅을 활성화한다. 데이터를 90일 후에 Amazon Glacier로 이동하고 7년 후 데이터가 만료되도록 수명 주기 정책을 설정한다.

10) 보안 엔지니어는 어떤 사용자의 액세스 키가 GitHub에서 발견되었다는 정보를 입수했습니다. 엔지니어는 이 액세스 키를 더 이상 사용할 수 없게 하고, 권한이 없는 활동을 이 액세스 키로 수행했는지 평가해야 합니다.

이러한 작업을 수행하려면 어떤 단계를 따라야 합니까?

A) 해당 사용자의 IAM 권한을 검토하고, 인식할 수 없거나 권한이 없는 리소스를 삭제한다.

B) 해당 사용자를 삭제하고, 모든 리전에서 Amazon CloudWatch Logs를 검토하고, 침해 사례를 보고한다.

C) 해당 사용자의 키를 삭제 또는 교체하고, 모든 리전에서 AWS CloudTrail logs를 검토하고, 인식할 수 없거나 권한이 없는 리소스를 삭제한다.

D) GitHub 제출 항목에서 이 키를 제거하고, 키를 교체하고, 시작된 인스턴스를 재배포하도록 해당 사용자에게 지시한다.

답

1) A, C - IAM 정책은 VPC 종단점을 통한 경우를 제외하고 다음 조건 문으로 AWS KMS에 대한 액세스를 거부할 수 있습니다.

```
"Condition": {
   "StringNotEquals": {
      "aws:sourceVpce": "vpce-0295a3caf8414c94a"
   }
}
```

프라이빗 DNS 이름 활성화 옵션을 선택하면 표준 AWS KMS DNS 호스트 이름(https://kms.<region>.amazonaws.com)이 VPC 종단점으로 확인됩니다.

2) B - 특정 Amazon CloudWatch Logs 로그 그룹에 로그를 보내도록 각 애플리케이션의 로그를 구성할 수 있습니다.

3) A, C, E - n-티어 아키텍처에서는 각 티어의 보안 그룹이 해당 보안 그룹의 트래픽만 전송할 수 있도록 허용합니다. 프레젠테이션 티어는 인터넷에서 들어오는 HTTP 및 HTTPS 트래픽을 엽니다. 보안 그룹은 상태가 저장되므로 인바운드 규칙만 있으면 됩니다.

4) B, C, F - Amazon Cognito는 SAML 어설션을 수신할 때 SAML 속성을 사용자 풀 속성에 매핑할 수 있어야 합니다. 자격 증명 공급자로부터 SAML 어설션을 받도록 Amazon Cognito를 구성할 때, Amazon Cognito가 해당 자격 증명 공급자의 신뢰 당사자로 구성되었는지 확인해야 합니다. Amazon API Gateway는 구성 단계에서 Amazon Cognito로부터 전달되는 권한 부여를 인식할 수 있어야 합니다.

5) C - `resource` 섹션은 작업 유형과 일치해야 합니다. ARN은 객체 작업이므로 끝에 /*가 포함되도록 변경합니다. 자세한 내용은 https://aws.amazon.com/blogs/security/writing-iam-policies-how-to-grant-access-to-an-amazon-s3-bucket/에서 확인하십시오.

6) B, D - 피어링 연결을 통해 서로 라우팅하도록 각 VPC의 라우팅 테이블을 구성해야 합니다. 또한 상대방 VPC의 애플리케이션 서버 보안 그룹에서 보내는 요청을 데이터베이스가 수락하도록 보안 그룹에 규칙을 추가해야 합니다.

7) C - Amazon CloudWatch Logs에 로깅하는 데 필요한 기본 Lambda 권한에는 `CreateLogGroup`, `CreateLogStream` 및 `PutLogEvents`가 포함됩니다.

8) B, C - KMS를 사용하는 버킷 암호화는 버킷이 퍼블릭 상태인 경우뿐 아니라 디스크가 도난당한 경우도 보호할 수 있습니다. AWS 외부 사용자가 AWS KMS 키를 사용하려면 권한을 부여받아야 하기 때문입니다. HTTPS는 전송 중인 데이터를 보호합니다.

9) D - Amazon Glacier로 전환하는 수명 주기 정책을 사용하면 모든 요구 사항이 충족되며 비용 효율적입니다.

10) C - 키를 제거하고 악의적인 활동이 일어나는 환경에 대해 감사를 실시합니다.

