ECSA Cohort 21: Checkride 시나리오

A. Landing zone Mini Project

BACKGROUND

현재 고객은 대규모 클라우드 마이그레이션을 위한 기반을 마련하기 위해 랜딩존 프로젝트를 수행하고자 합니다. 이미 몇 개의 AWS 계정으로 시범적인 서비스를 운영하고 있으며 향후 본격적인 클라우드 전환을 시작하게 되면 점차적으로 늘어나는 AWS 계정에 대한 보안 거버넌스를 체계적으로 유지할 수 있어야 합니다.

REQUIREMENTS

고객사는 비즈니스 민첩성과 클라우드 거버넌스를 동시에 달성할 수 있도록 다중 계정 (Multi-Account) 전략을 채택하기로 하였으며, AWS Control Tower 기반의 랜딩존을 구축해야 합니다. 고객이 제시한 요구사항은 아래와 같습니다.

1. MULTI-ACCOUNT 구조 (5점)

- 랜딩존 초기에는 운영계 서비스 1개, 개발계 서비스 1개로 AWS Account를 생성하여 운영하고자 합니다.
- AWS Best Practice 기반으로 아래와 같은 AWS 조직 구조 (Organizational Structure)를 구성하고자 하며 각 OU (Organizational Unit)의 운영 방안에 대하여 타당성을 검토 후 적용하고자 합니다.
    - Security OU
        - Audit Account
        - Log Archive Account
    - Infrastructure OU
    - Workloads_Prod OU
        - Prod_Service1 Account
    - Workloads_Dev OU
        - Dev_Service1 Account
    - Exceptions OU
    - Suspended OU
    - Policy Staging OU
    - Transitional OU
- 생성된 AWS Account ID (12자리 숫자)를 아래에 기재합니다.
    - Management Account:
    - Audit Account:
    - Log Archive Account
    - Prod_Service1 Account:
    - Dev_Service1 Account:

2. 회사 클라우드 보안규정 준수 (40점)

- 신규 AWS Account를 발급할 때에는 본 보안 규정을 만족할 수 있도록 해야 합니다.
- 신규 AWS Account 생성 후, 수작업으로 인한 보안 설정 누락을 방지하기 위해 가급적 자동화로 구현합니다.
- 최대한 보안 규정을 강제적으로 적용할 수 있도록 하며, 강제 적용이 힘들 경우에는 효율적으로 규정 위반 내용을 탐지하고 식별할 수 있어야 합니다.

- 신규 Account 발급 시, 회사 클라우드 보안 규정이 어떻게 자동으로 적용될 수 있는지 설명할 수 있어야 합니다.
- 보안 규정 준수를 위한 컨트롤 (가드레일)이 정상적으로 동작하는지를 고객에게 시연할 수 있어야 합니다.
- 모든 보안 로그 (CloudTrail, Config로 한정)는 최소 5년을 보관하도록 설정을 변경합니다.
- Control Tower 컨트롤 (가드레일) 적용
    - 업계 규정 및 회사 규정 상, 서울 및 버지니아 리전 등 2개의 리전만 사용하고 이 외 리전은 사용을 금지합니다.
    - 운영환경 (Prod_Service1)은 Root 사용자의 작업을 금지합니다.
    - 운영환경 (Prod_Service1)은 Root 사용자의 Access Key 생성을 금지합니다.
    - 운영환경 (Prod_Service1)은 잘 알려진 TCP 포트 (FTP, RDP, SSH 등)에 대해 공개 오픈이 되어 있는지를 탐지할 수 있어야 합니다. — **SSH 공개 오픈에 대한 Non-compliant 상태 구현 (VPC 및 EC2 생성 필요)**
    - 운영환경 (Prod_Service1)은 S3 Bucket Versioning을 사용하도록 탐지할 수 있어야 합니다. — **Non-compliant 상태 구현 필요**
    - 운영환경 (Prod_Service1)은 IAM User(사용자)에 대해 MFA 설정여부를 탐지할 수 있어야 합니다. — **변경내용이 즉시 반영되지 않으므로, Non-compliant 구현은 하지 않아도 됨)**
    - 개발환경 (Dev_Service1)은 Ingress 인터넷 연결을 차단해야 합니다.
- 추가적인 예방 (Preventive) 컨트롤 (가드레일) 적용 (SCP) — Organizations에 직접 적용하며 2개의 Workloads_Prod, Workloads_Dev OU에 적용함 (실제 프로젝트 시에는 CfCT, AFC, CloudFormation StackSet으로 구현하는 영역)
    - Organizations 내의 계정이 임의로 탈퇴를 하지 못하도록 금지합니다.
    - VPC Flow Logs의 삭제를 금지합니다.
    - KMS Key 삭제를 금지합니다.
    - Organizations 외부 계정과의 리소스 공유를 금지합니다.
- 추가적인 탐지 컨트롤 (가드레일) 적용 (AWS Config) — Prod_Service1 Account에 직접 수작업으로 적용하되, Multi-Account에 적용할 수 있는 방안을 설명할 수 있어야 합니다.
    - 모든 IAM User의 패스워드 규칙은 아래 규정을 만족해야 합니다. — Non-compliant 상태 구현
        - AWS 서비스 사용 시 접속하는 모든 IAM 사용자에 적용해야 함
        - 최소 길이 8자 이상
        - 특수문자, 숫자, 영문 대/소문자를 최소 1개씩 포함
        - 패스워드 최대 사용기간은 90일
        - 패스워드 재사용 금지 횟수 8개
    - 모든 EBS 및 EFS 서비스가 암호화 되어 있는지 탐지하도록 합니다. — Non-compliant 상태 구현

3. AWS IAM IDENTITY CENTER (SINGLE SIGN-ON) (15점)

- 여러 AWS Account에 동일한 ID로 접속할 수 있도록 AWS IAM Identity Center를 구성합니다.
- MFA를 활성화 합니다.
- 회사의 팀별 권한은 아래와 같이 설정합니다.
    - CCoE: 전체 AWS Account의 관리자 (Administrator) 권한 부여
        - User: ecsa_admin
        - Group: ecsa_admingroup
    - 서비스 운영팀: Prod_Service1, Dev_Service1 Account에 PowerUser 권한 부여
        - User: ecsa_svc
        - Group: ecsa_svcgroup
    - 관제팀: Prod_Service1, Dev_Service1 Account에 ReadOnly 권한 부여
        - User: ecsa_cert

        - Group: ecsa_certgroup
    - 관제팀은 1.1.1.0/24 IP 대역에서 접속했을 때만 정상적인 조회업무가 가능하도록 정책을 설정합니다. 단, 관제팀이 사용하는 Permission-set (권한 세트)는 Default로 제공되는 것을 사용하지 말고 별도로 생성하여 구성합니다.

4. 보안서비스 (40점)

- WAF (25점)
    - WAF 테스트용 VPC는 운영환경의 Prod_Service1 계정에 임의로 생성합니다. (AZ1, AZ3 사용)
        - Public Subnet 2개, Private Subnet 2개 구성
        - NAT Gateway 생성하지 않음
    - WAF 검증용 DVWA EC2 인스턴스 1개를 Private Subnet에 구성합니다.
        - DVWA 서버 구성은 AWS AMI 서비스에서 community 버전에서 DVWA를 검색하여 생성합니다.
    - DVWA 인스턴스 1개만을 가지는 Target Group을 생성합니다. 그리고 테스트용 ALB (Application Laod Balancer)를 Public Subnet에 생성합니다.
    - WAF를 생성된 ALB에 연동하여 구성합니다. ALB의 DNS 주소로 접속하여 DVWA 로그인 페이지가 정상적으로 표시되는지를 확인합니다.
        - DVWA 로그인 URL: http://ALB-DNS-NAME/dvwa
    - XSS 및 SQL Injection 등의 OWASP Top 10 주요 침해 시나리오를 수립하고 WAF가 방어하는 체계를 시연합니다.
        - SQL Injection: 'OR 1=1 #', XSS: <script>alert(document.cookie)</script>
    - 당사는 별도로 자체 black-ip-list를 보유하고 있지 않는 관계로 별도 관리하고 싶지는 않으나, 외부의 나쁜 평판의 IP 리스트로부터 트래픽 유입 차단을 하고자 합니다.
    - 특정 국가 IP (예: US) 로부터 Request가 유입될 경우, Block 하며 별도의 커스텀 응답 페이지 출력합니다. (예: Your request is not allowed. — Security Team)
    - WAF에서 발생하는 로그는 CloudWatch Logs에 저장 (저장 주기는 1개월)하며, 차단/탐지 로그만 로깅 (허용 로그는 남기지 않음)합니다.
- GuardDuty (10점)
    - 회사는 효율적인 AWS 서비스의 보안 모니터링을 위해 GuardDuty를 사용하기로 하였습니다.
    - Audit Account에서 전체 Organization의 GuardDuty를 통합적으로 관리할 수 있도록 설정합니다.
    - 향후 생성되는 모든 Account들이 자동으로 GuardDuty에 등록되도록 설정합니다.
    - GuardDuty의 Sample Findings를 임의로 발생시켜서 향후 탐지될 수 있는 유형에 대해 검토합니다.
    - GuardDuty에서 탐지된 내용들을 특정 S3 Bucket에 저장하도록 구성합니다.
- SecurityHub (5점)
    - Audit Account에서 전체 Organization의 SecurityHub를 통합 관리합니다.
    - 운영 및 개발 환경에서 AWS Foundational Security Best Practices Standard를 준수하는지 확인하고, 이에 대한 결과를 검토합니다.
    - 향후 생성되는 모든 Account들이 자동으로 SecurityHub에 등록되도록 설정합니다.

B. 네트워크 보안

BACKGROUND

고객은 ECSA Module1을 통해 기본 랜딩존 환경을 구축하여 Multi-Account 전략 실행의 기반을 마련하였습니다. 이제 본격적인 네트워크 아키텍처 설계와 탄력적이고 확장 가능한 네트워크 보안 체계를 구축하고자 합니다.

REQUIREMENTS

네트워크 설계/구성

- Management 계정에 접속하여, Infrastructure OU 내에 Network 계정 및 SharedService 계정을 추가로 생성합니다.
    - 계정 (Account) 2개 신규 생성 후, SSO Permission Set 할당을 통해 관리자 권한으로 접속할 수 있도록 설정합니다. (AWS IAM Identity Center 서비스를 통해 접속)
- PPT 혹은 draw.io 등의 도구를 써서 본인이 설계한 네트워크 아키텍처를 작성하고 CIDR은 참조 Workshop 혹은 Blog와 다르게 본인만의 CIDR 대역으로 재설계 합니다.
    - 참조 Workshop: https://catalog.us-east-1.prod.workshops.aws/workshops/d071f444-e854-4f3f-98c8-025fa0d1de2f/en-US/lab-three
    - 참조 Workshop: https://catalog.workshops.aws/networkfirewall/en-US/setup/centralmodel
    - 참조 Blog: https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/
- 네트워크 아키텍처 설계 시, 가급적으로 Multi-AZ로 구성을 권고하지만 개인별 난이도를 고려하여 업무용 VPC (운영/개발) 및 SharedServices VPC는 Single AZ로 구성해도 됩니다. (TGW Appliance 모드 관련 구현 내용과 관련됨)
- 네트워크 아키텍처 다이어그램에는 VPC가 어떤 AWS Account에 속해 있는지 표현하여 주시기 바랍니다.
- 아키텍처 다이어그램은 1/23(목)까지 아래 이메일로 전송하여 주시기 바랍니다.
    - 제출 파일 제목: ECSA-Cohort21-[회사명]-[이름]
    - 제출 이메일 주소: bhpark@amazon.com, hjinsung@amazon.com

고객 요구사항

- 고객은 운영환경 (Prod_Service1 계정)과 개발환경 (Dev_Service1 계정)을 모두 보유하고 있으며, 각 환경의 트래픽 허용/차단 정책은 다음과 같습니다.
    - 운영환경 (Prod_Service1 계정)
        - 개발환경 (Dev)과의 통신은 기본적으로 차단합니다.
        - 외부 인터넷으로부터의 접근 (Inbound)은 허용합니다. (분산형 또는 중앙집중형 Ingress 구현)
        - 외부 인터넷으로부터의 접근 시에 WAF 또는 Network Firewall 서비스를 통한 경계 보안 구성이 필요합니다.
    - 개발환경 (Dev_Service1 계정)
        - 운영환경 (Prod)과의 통신은 기본적으로 차단합니다.
        - 외부 인터넷으로부터의 접근 (Inbound)은 기본적으로 차단합니다.
    - 공통사항
        - SharedServices 계정의 VPC는 운영, 개발 환경과의 양방향 모두 접근 가능하여야 합니다.
        - 모든 환경의 인스턴스가 외부 인터넷 접속 (Outbound) 시에는 네트워크 계정의 Centralized Egress VPC를 통해 통신되도록 구성합니다.
        - 고객은 EC2 접속을 위한 별도의 키관리를 하지 않으려고 합니다. 따라서 EC2 인스턴스 접속은 Session Manager를 사용합니다.
        - Session Manager는 Endpoint 서비스를 사용하지 않고, Centralized Egress VPC를 경유하여, 아웃바운드 인터넷을 통해 서비스 되어야 합니다. (하단의 네트워크 방화벽 아웃바운드 정책에서 *.amazon.com 도메인 허용 확인)
- 네트워크 계정을 활용하여 서로 다른 환경 간의 연결성 (Connectivity)을 제공할 수 있어야 합니다. VPC 추가 시에도 기존 VPC 설정 변경을 최소화하여 유연하게 네트워크 구성이 가능하도록 해야 합니다.
    - Multi-Account 환경에서는 네트워크 계정에서 Transit Gateway (TGW)를 생성하고 이를 Resource Access Manager (RAM)을 통해 Organization 또는 Organizational Unit (OU)에 TGW를 공유를 구성합니다.
        - Management 계정에 접속

        - TGW를 Organizations 내에서 RAM을 통해 공유되도록 RAM 서비스를 미리 Organizations에서 “Trusted Access” 활성화를 해야 합니다.
        - Organizations - Services - RAM 선택하여 Trusted Access 활성화
        - Resource Access Manager - Settings에서 Enable sharing with AWS Organization 활성화
    - 네트워크 (Network) 계정에 접속
        - Resource Access Manager > Shared by me: Resource shares > Create resource share
        - Resource type에 TGW를 선택하여 생성된 TGW를 선택
        - Organizations 내에서만 공유하되 Organizations 전체 혹은 특정 OU들에 대해서 공유 설정
  - Multi-Account 환경에서는 TGW Attachment는 각 계정 (Prod_Service1, Dev_Service1, SharedServices, Network 등)에서 생성하여 TGW에 Attach한 후, 네트워크 계정에서 이를 Accept 해 줘야 합니다. (단, TGW 생성 시 Configure cross-account sharing options에서 ‘Auto accept shared attachments를 활성화한 경우 제외. 해당 설정 시 자동으로 Accept 수행됨)
- 보안 서비스
  - AWS Network Firewall
    - 방화벽은 고가용성을 위해 2개의 가용성 존 (Availability Zone)에 구성하며 네트워크 계정에서 통합 관리합니다.
    - 기본 deny any any 정책을 준수하며, 아래와 같이 White-list 기반의 허용 정책을 구성합니다. (허용된 정책 외에는 통신 불가)
    - 트래픽 확인을 위하여 로깅 설정
    - 아래 요구사항을 반영하여 방화벽 Ingress/Egress 정책(5 Tuples, Domain)을 적용해 주시기 바랍니다.

	Protocol	Source IP	Source Port	Destination IP	Destination Port	Logging 여부
1	ICMP	운영 환경		Any		Yes
2	HTTPS	운영/개발 환경		www.naver.com	443	Yes
3	HTTPS	운영/개발 환경		*.amazon.com	443	Yes

[OPTIONAL] 필수는 아니지만, 구성시 가산점

- (Optional + 30점) Audit을 위해 보안 솔루션들의 logging 집중화
  - 보안 서비스들의 로그를 Log Archive 계정의 S3에서 Centralized logging하여 관리하며, 저장 주기 1년입니다.
  - 연동할 보안 서비스들은 GuardDuty, WAF, Network Firewall 입니다.

참고사항

	구분	리소스	1일 예상비용	2일 예상 비용
1	Multi-Account	Config	1,000원 미만	2,000
2	클라우드 보안규정	Config	1,000원 미만	2,000
3	IAM Identity Center	External IdP(optional)	Okta Developer 기준 무료	0
4	네트워크 구성	Transit Gateway	4개 Attachment 시, 6,000원 (VPC Attachment당 1,500원 내외)	12,000
5		NAT Gateway	Network Firewall과 함께 사용 시, 해당 시간당 및 처리 비용 무료 (방화벽 엔드포인트 및 처리비용으로 대체)	0
6	보안서비스	WAF	1 ACL, 2 Managed Rule 기준 일 1,000원 미만	2,000
7		Network Firewall	2개 엔드포인트 사용시, 22,000원 (엔드포인트 당 일 11,000원 내외)	44,000

** 상기 비용은 수강생이 구현하는 아키텍처에 따라 상이하므로 충분히 비용을 모니터링하면서 구현하시기를 권장드립니다. 특히, Network Firewall 및 Transit Gateway 비용을 감안하면서 구현하시기 바랍니다.

- 본 Checkride 과제 내용은 수업시간에 다루지 않은 내용도 포함되어 있을 수 있으며, 수강생은 AWS Docs 및 공식 Blog, Knowledge Center 등의 검색을 통해서 구현할 수 있습니다.
- Checkride가 종료된 후에는 모든 리소스를 순차적으로 삭제하며, 생성한 역순으로 삭제하시면 됩니다.
- AWS Docs, 공식 블로그, Knowledge Center, 워크샵 가이드 자료
    - https://docs.aws.amazon.com/
    - https://aws.amazon.com/ko/blogs/tech/
    - https://aws.amazon.com/ko/blogs/korea/
    - https://repost.aws/knowledge-center
    - 워크샵 URL
        - AWS General Immersion Day — Basic
            - https://catalog.us-east-1.prod.workshops.aws/workshops/f3a3e2bd-e1d5-49de-b8e6-dac361842e76/en-US/basic-modules
        - AWS IAM Workshop
            - https://catalog.us-east-1.prod.workshops.aws/workshops/dd23d392-bea4-483c-aefd-f62ed73f936d/en-US
        - AWS KMS Workshop
            - https://catalog.us-east-1.prod.workshops.aws/workshops/a5e4d4c2-9a7c-4753-8af5-c89cff42cc32/ko-KR
        - 위협 탐지 및 대응 (AWS GuardDuty, Inspector, Security Hub)
            - https://catalog.us-east-1.prod.workshops.aws/workshops/b25772b2-6b30-4061-b0d1-012357335af9/ko-KR
        - Security Hub Workshop
            - https://catalog.workshops.aws/vulnerabilitymanagement/en-US/1-containers
        - Prowler Workshop
            - https://catalog.us-east-1.prod.workshops.aws/workshops/b1cdc52b-eb11-44ed-8dc8-9dfe5fb254f5/en-US/build/quicksight
        - AWS WAF (Web Application Firewall)
            - https://catalog.us-east-1.prod.workshops.aws/workshops/bbaefbc2-bb4b-4332-aa36-4047e31c4972/ko-KR
        - AWS Network Firewall
            - https://catalog.us-east-1.prod.workshops.aws/workshops/d071f444-e854-4f3f-98c8-025fa0d1de2f/en-US
        - GWLB (GateWay Load Balancer)
            - https://whchoi98.gitbook.io/aws-gwlb
        - EKS
            - https://catalog.workshops.aws/eks-immersionday/en-US/introduction
        - Control Tower
            - https://catalog.us-east-1.prod.workshops.aws/workshops/1242b940-6f02-4d39-8ef2-2796370be864/ko-KR/
        - 그 밖에 워크샵 검색방법
            - https://workshops.aws/ 에서 검색, 또는 Google에서 'aws *서비스명* workshop' (예, aws *fargate* workshop) 을 검색