CWL
CyberWarFare Labs

Multi-Cloud Blue Team Analyst (MCBTA)

@CyberWarFare Labs

Multi-Cloud Blue Team Analyst (MCBTA) Architecture

AWS

Azure

GCP

Centralized Logging

Multi-Cloud Detection Engineers

- Threat Hunting
- Incident Investigation
- Pro-Active Monitoring

CWL
CyberWarFare Labs

I. Multi Cloud Blue Teaming 101

II. Centralised Logging & Monitoring Architecture Deployment

III. Mastering Multi-Cloud Security

3.1 AWS & Its services

- 3.1.1 Introduction to AWS security
- 3.1.2 AWS logs & its types
  - 3.1.2.1 CloudTrail Logs
  - 3.1.2.2 CloudWatch Logs
  - 3.1.2.3 VPC Flow Logs & Route 53 Resolver Query Logs
  - 3.1.2.4 Amazon S3 Access Logs
- 3.1.3 Logging & Monitoring : AWS
- 3.1.4 Filebeta integration

III. Mastering Multi-Cloud Security

3.2 Azure & Its services

- 3.2.1 Introduction to Azure security
- 3.2.2 Azure logs & its types
  - 3.2.2.1 Activity Logs
  - 3.2.2.2 Audit Logs
  - 3.2.2.3 Sign-in Logs
  - 3.2.2.4 Application Logs
  - 3.2.2.5 Unified Audit Logs [UAL]
- 3.2.3 Logging & Monitoring : Azure
- 3.2.4 Filebeta integration

III. Mastering Multi-Cloud Security

3.3 GCP & Its services

- 3.3.1 Introduction to GCP security
- 3.3.2 GCP logs & its types
  - 3.3.2.1 Audit Logs
  - 3.3.2.2 Application Logs
  - 3.3.2.3 Security Logs
  - 3.3.2.4 Networking Logs
- 3.3.3 Logging & Monitoring : GCP
- 3.3.4 Filebeta integration

IV. Deploying And Configuring Investigation Lab

4.1 Blueprint for Investigation Lab Deployment

4.2 Deployment Overview

4.3 Implementation Requirements and Specifications

V. Investigating Threats Across Multi-Cloud

5.1 AWS

5.1.1 Critical S3 Data Loss: Unexpected Bucket Deletion Event

5.1.2 Suspicious IAM Instance Profile Provisioning in AWS

5.1.3 Unauthorized IAM Policy Modification Detected

5.1.4 Suspicious Lambda Function Execution Identified

5.1.5 Suspicious Cross-Account Trust Relationship Identified

V. Investigating Threats Across Multi-Cloud

5.2 Azure

5.2.1 Security Alert: Unusual LISTKEYS Request Activity Logged

5.2.2 Unapproved Network Security Group Configuration Detected

5.2.3 Enumeration of Azure Container Resources

5.2.4 Potential Secret Exfiltration from Azure Key Vault Identified

5.2.5 Suspicious Update to App Registration Credentials Detected

V. Investigating Threats Across Multi-Cloud

5.3 GCP

5.3.1 Potential Data Exfiltration: Unapproved File Copy from GCP Bucket

5.3.2 Suspicious Service Account Impersonation

5.3.3 Suspicious IAM Role Assignment Detected

5.3.4 Abnormal Bucket Object Creation Activity Identified

5.3.5 Suspicious Service Account Secret Creation Activity Identified

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live