Logs and Auditing

4.3 Given a Scenario, Implement Identity and Access Management

Description

- In this episode, we will explore the concept and practice of auditing our systems, also referred to as "Logging and Monitoring". We will learn why logging and monitoring is important from a security perspective as well as look into some common practices associated with auditing. We will also explore a few logging solutions from both AWS and Azure.

Resources

- N/A

Learning Objectives

- Explain why logging, auditing, monitoring is important for cybersecurity
- List and describe common practices associated with logging/monitoring

Notes

- Why logging and monitoring is important
- Common practices associated with logging and monitoring
    - Centralized Log Management
    - Alerting
        - Set up alerts to notify your team of suspicious activity or threshold breaches
    - Automated Responses
        - Automate responses to certain alerts using tools like AWS Lambda or Azure Logic Apps
    - Compliance
        - Use built-in tools to ensure compliance with industry standards and regulatory requirements
- AWS Logging
    - AWS CloudWatch
        - Monitors resources and apps
        - Look through the dashboard and options
    - AWS CloudTrail
        - Monitors user activity and API usage
    - AWS Config
        - Monitor configurations of your AWS resources
    - AWS Security Hub
        - Centralized security logging
    - AWS Guard Duty
        - Intelligent threat detection service
            - Continuously monitors for malicious or unauthorized behavior
    - AWS Inspector
        - Automated security assessment service for EC2 instances
            - Checks for vulnerabilities and deviations from best practices
    - AWS Detective
        - Collects logs for use in security analysis

- Azure Logging
    - Azure Monitor
        - Logging system that collects, analyzes, and acts on telemetry data from Azure and on-premises environments
    - Azure Security Center
        - Security monitoring and mangement system
            - Provides threat protection across Azure and on-premises data centers
    - Microsoft Sentinel
        - Cloud-based SIEM solution
            - Utilizes built-in AI to help analyze large volumes of data across an enterprise
            - Detection
            - Investigation
            - Response
            - Threat Hunting