Team Name: SOC DOCS (Team 2)

Important Links

Copy of Developing a Cloud-based SOC (The Project Outline from Class)

GitHub Link: https://github.com/TEAM-2-SOC-Implemenation

Trello Link:https://trello.com/invite/b/Mb6AtLsK/ATTIea0596196333e148f0f427446b46f52981997592/soc-team-2

Sprint 1 | Project Plan and Requirements

Team Contact Info/Roles

Mario Register (Team Leader): mario.register1988@gmail.com
Giovanni Garcia Flores (Project Manager): Giovanni.Garcia162@gmail.com
Pedro Gomez (Technical Lead): pg842032@gmail.com
Matthew Escalera (Technical Lead): matthew.escalera08@gmail.com

Sprint Schedule

Sprint 1 / Project Planning & Requirements Gathering

(Week 1-2): Monday, April 15 - Monday, April 29 (Wednesday May 1 Extension)

- **Deliverables:**
    - Project Plan: Define project goals, scope, target audience, success metrics (e.g., reduced alert fatigue, faster incident response times), and a detailed 10-week sprint schedule.
    - Requirements Document: Research and document security data sources (logs, network traffic, endpoint data) to be ingested into the SOC platform.
    - High-Level Architecture Design: Outline the cloud platform services and security tools needed for the core functionalities of the SOC.

Sprint 2 / Secure Cloud Infrastructure & Access Control

(Week 3-4): Monday, April 29 - Monday, May 13 (Wednesday, May 15 Extension)

- **Technical Documentation:**
    - Secure Cloud Network Design: Define a secure virtual network architecture within the cloud platform to segregate SOC components and manage data access. Optimally all components will exist on one VPC with the tool's respective public and private subnets within one or two availability zones for any anticipated failures.
    - Identity and Access Management (IAM): Implement granular access control policies using IAM roles to restrict access to SOC functionalities based on user privileges. We will use the AWS IAM Management service to exemplify a regular user vs an admin user. Will be used as a demo piece for introducing a high/low level security environment for users accessing the SOC platform.

Sprint 3 / Security Data Collection & Aggregation

(Week 5-6): Monday, May 13 - Monday, May 27 (Wednesday, May 29 Extension)

- **Technical Documentation:**
  - Security Data Ingestion Pipelines: Design and implement automated data ingestion pipelines to collect security data from various sources (firewalls, intrusion detection systems, endpoint security agents) into a centralized log management platform. Amazon Kinesis Firehose will be our primary log ingestion pipeline, AWS Lambda for automated log ingestion process.
  - Log Management & Normalization: Configure the log management platform to normalize and enrich logs for efficient analysis and threat detection. Splunk Cloud for a centralized log analysis platform that ingests security data from Kineses Firehose. Splunk Cloud offers powerful search, indexing, and data processing capabilities, allowing you to normalize and enrich logs from various sources into a consistent format for efficient analysis and threat detection.
  - OpenSearch Service (successor to Amazon Elasticsearch Service) can be used as an alternative or complementary log management and analytics platform, particularly for log data that requires high-performance search and analysis capabilities.
  - Kibana offers powerful features for log normalization, such as creating custom log parsers, defining data mappings, and applying data transformations to ensure consistent log formats for efficient analysis and threat detection. Serves as a general dashboard for the SOC platform as well.

Sprint 4 / Security Automation & Alert Correlation

(Week 7-8): Monday, May 27 - Monday, June 10 (Wednesday, June 12 Extension)

- **Technical Documentation:**
    - Security Automation Playbooks: Develop playbooks within AWS Lambda to automate repetitive tasks in the incident response workflow.

  Examples of playbooks include:

- User account isolation upon suspicious login attempts.
- Automated malware scanning and remediation on infected endpoints.
- Escalation procedures for high-severity incidents.
    - Threat Detection & Alert Correlation: Implement rules within Splunk Cloud to correlate security events from various sources (firewalls, endpoints, AWS services).
    - Utilize machine learning models within Splunk Cloud to identify anomalies and potential threats based on historical data and threat intelligence.
    - Configure Splunk Cloud to generate high-fidelity alerts based on correlated events and threat detection rules. This reduces alert fatigue for security analysts by focusing on the most critical events.

Sprint 5 / User Interface & Security Monitoring

(Week 9-10): Monday, June 10 - Monday, June 24 (Wednesday, June 26 Extension)

- **Technical Documentation:**
    - User-Friendly SOC Interface Design: Design a dashboard in Splunk Cloud tailored for security analysts.

  - Utilize clear visualizations (charts, graphs) to represent security events, incidents, and overall security posture.
  - Implement intuitive search and filtering capabilities for efficient incident investigation.
  - Consider integrating interactive elements (drill-down menus) for deeper analysis.

  - Continuous Security Monitoring: Configure Splunk Cloud for continuous log ingestion and analysis.
  - Define real-time threat detection rules within Splunk Cloud based on threat intelligence and best practices.
  - Leverage Amazon GuardDuty for continuous threat monitoring within the AWS environment.
  - Integrate vulnerability scanning results from Amazon Inspector into Splunk Cloud for continuous vulnerability management.
- **Technical Documentation:**
  - Testing Report & Security Baseline: Conduct penetration testing and vulnerability assessments of the SOC platform itself to identify and address potential security weaknesses.
  - Test the functionality of the SOC platform, including log ingestion, analysis, alert generation, and response capabilities.
  - Establish a security baseline for the SOC platform, documenting its configuration, security controls, and expected performance metrics.

- This baseline will serve as a reference point for ongoing monitoring and optimization of the SOC platform's security posture.

- Knowledge Transfer & Handover Package: Develop comprehensive documentation for the SOC platform, including user guides, configuration manuals, and best practices for security analysts.
- Conduct training sessions for the security team, covering the functionalities of the SOC platform, incident response procedures, and threat intelligence analysis.
- Ensure clear handover of knowledge and responsibilities for operating and maintaining the SOC platform.

Project Goal

The primary goal of the project is to establish a scalable and automated Security Operations Center (SOC) on AWS to centralize security monitoring, incident detection, and response capabilities. Secondary goals include improving security posture and reducing response times to security incidents

Scope

The project will focus on designing, deploying, and configuring the SOC infrastructure on AWS, including the selection and integration of appropriate AWS services and security tools. It will not include extensive customization or integration with on-premises systems.

Target Audience

The SOC platform will primarily serve security operations professionals, IT security teams, and security analysts within an organization.

Success Metrics

Reduction in alert fatigue by at least 30% within six months of SOC deployment.
Increase incident response times by 20%

Achievement of an average incident response time of less than 15 minutes for critical security events.

Improvement in security visibility with centralized monitoring and reporting capabilities.

Streamline incident response workflows through automation playbooks and improve overall response efficiency.

Architecture Design

Data Sources:

- **Network Security Devices (pfSense firewall):** This acts as your first line of defense, filtering and monitoring network traffic for suspicious activity. Logs from pfSense can be ingested into your SOC platform.
- **Cloud Infrastructure Logs (VPC Flow Logs, DNS Logs, CloudTrail Logs):** These logs provide valuable insights into activities within your AWS environment. Kinesis Firehose will collect and pre-process these logs.

Log Ingestion and Preprocessing:

- **Amazon Kinesis Firehose:** Acts as a streaming data delivery service, collecting logs from various sources (pfSense, CloudTrail, etc.) and preparing them for further analysis by Splunk Cloud.

Log Management and Analysis:

- **Splunk Cloud (SIEM):** This is the central hub for your SOC, receiving preprocessed logs from Kinesis Firehose. Splunk Cloud analyzes these logs for security events, anomalies, and potential threats. It also integrates with your chosen threat intelligence feed (ETOpen) to enrich its threat detection capabilities.

Threat Detection and Vulnerability Assessment:

- **Amazon GuardDuty:** This managed threat detection service continuously monitors your AWS environment for malicious activity using threat intelligence. It works seamlessly with Splunk Cloud, potentially triggering alerts if it detects suspicious activity.
- **Amazon Inspector:** This service helps you identify vulnerabilities and exposures in your Amazon EC2 instances. It scans instances for known vulnerabilities and misconfigurations, reporting findings to Splunk Cloud for further analysis.

Security Orchestration, Automation, and Response (SOAR):

- **AWS Lambda (Automated Responses):** This serverless compute service allows you to create custom functions (automations) for repetitive tasks. For example, upon a high-severity threat alert from Splunk Cloud, a Lambda function could automatically quarantine an infected instance.

- **AWS Security Hub (Optional):** This service acts as a central repository for security findings from various AWS services like GuardDuty and Inspector. While optional, Security Hub can be used for centralized investigation and response, potentially feeding its findings back to Splunk Cloud for analyst review.

Security Visualization:

- **Kibana (integrated with Splunk Cloud):** This is a data visualization tool that provides real-time dashboards and reports. You can use Kibana to visualize security metrics, trends, and alerts generated by Splunk Cloud, offering a clear view of your security posture.

Threat Intelligence Feed:

- **Emerging Threats Open (ETOpen) - Open Source Tool:** This provides valuable threat intelligence data to Splunk Cloud. By integrating ETOpen, Splunk can leverage this data to improve its detection capabilities and identify emerging threats more effectively.

IAM Roles with Least Privilege:

- **IAM (Identity and Access Management):** This service ensures secure access control by assigning roles with least privilege to users and resources. This minimizes the potential damage if a security breach occurs.

How They Work Together:

1. **Log Collection:** Logs are generated from various data sources (pfSense, AWS services) and collected by Kinesis Firehose.
2. **Log Preprocessing and Delivery:** Kinesis Firehose preprocesses logs and delivers them to Splunk Cloud.

3. **Log Analysis and Threat Detection:** Splunk Cloud analyzes the logs and leverages threat intelligence (ETOpen) to identify potential threats and vulnerabilities.
4. **Alert Generation:** If suspicious activity is detected, Splunk Cloud generates security alerts.
5. **Investigation and Response:** Security analysts investigate alerts in Splunk Cloud and determine appropriate responses.
6. **Automation (Optional):** AWS Lambda functions (based on pre-defined rules) can be triggered for automated responses to high-severity alerts (e.g., quarantining infected instances).
7. **Centralized Findings (Optional):** Security Hub can act as a central repository for findings from GuardDuty, Inspector, and potentially Splunk Cloud, aiding in comprehensive investigation.
8. **Security Visualization:** Kibana provides real-time visualizations of security data from Splunk Cloud, offering situational awareness for the security team.

Alternative: AWS OpenSearch Service

While we've chosen Splunk Cloud for log analysis, AWS offers OpenSearch Service as an alternative. OpenSearch is an open-source search and analytics engine that works well with Kibana for visualization.

This breakdown highlights how these tools work together to create a comprehensive SOC platform for your AWS environment.

Research

- **Optimizing your SOC's threat coverage and data value:** https://m.youtube.com/watch?v=YD6QCEVDw20 (This video by Securonix discusses optimizing data ingestion for threat coverage and highlights the importance of accurate data intake for effective SOC operations.)

- **Live Demo: Get Faster Time-to-Value Across Your SOC Workflow with Hunters SOC Platform:** https://m.youtube.com/watch?v=YD6QCEVDw20 (This Hunters SOC Platform demo showcases how their platform connects to various data sources and emphasizes the importance of data readiness for analysis.)

- **Upgrade your SOC from log collection to true threat detection & response:** https://m.youtube.com/watch?v=YD6QCEVDw20 (This Microsoft and CyberProof discussion focuses on transitioning from basic log collection to true threat detection and response. While not directly addressing ingestion requirements, it highlights the importance of comprehensive data collection for effective SOC functionality.)

- **AWS re:Inforce 2022 - Using AWS security services to build your cloud security operations baseline -**
  ▶ AWS re:Inforce 2022 - Using AWS security services to build your cloud sec…
  (An AWS conference that explains GuardDuty and Security Hub in detail as it relates to building a cloud security operation).

- **SOC GUIDE** https://github.com/cyb3rxp/awesome-soc/blob/main/README.md