

# **Capstone Project: Design and Implementation of a Cloud-based Security Information and Event Management System (SIEM)**

Jose Rodriguez, Jesus Ayala, D'Andre Walden, Jasmine Melton  
TKH- The Knowledge House  
10-week Duration  
May 2024

## **Abstract**

This document presents the design and implementation of a cloud-based Security Information and Event Management (SIEM) system, developed as a capstone project over a 10-week period. The primary goal is to create a scalable and automated SIEM solution on a cloud platform (such as AWS, Azure, or GCP) to enhance an organization's security monitoring, incident detection, and response capabilities.

Five biweekly sprints that each concentrate on important SIEM system components make up the project's organizational structure. Project planning and requirements collecting are the first steps in the process. Next, a secure cloud infrastructure is designed and access controls are put in place. The development of security automation and alarm correlation mechanisms, the gathering and aggregation of security data, and the design of an intuitive user interface for ongoing security monitoring are all covered in later stages.

The project's main results include increased security visibility throughout the company, quicker incident reaction times, and a decrease in alert fatigue through efficient automation. In addition, the document offers suggestions for maintaining threat intelligence integration, continuous improvement tactics, and constant security training as means of guaranteeing the SIEM system's long-term viability.

With the help of this capstone project, the security team will have a strong, cloud-based SIEM platform that will improve the organization's overall security posture and consolidate security operations.

# Table of Contents

<b><u>Abstract.....</u></b>	<b><u>0</u></b>
<b><u>Project Overview.....</u></b>	<b><u>2</u></b>
Requirements Gathering Report.....	3
Required Documents.....	3
Additional Recommendations.....	3
<b><u>Success Metrics.....</u></b>	<b><u>4</u></b>
<b><u>Project Planning &amp; Requirements Gathering (Sprint 1: Week 1-2).....</u></b>	<b><u>4</u></b>
Project Plan.....	4
Requirements Document.....	4
High-Level Architecture Design.....	4
<b><u>Secure Cloud Infrastructure &amp; Access Control (Sprint 2: Week 3-4).....</u></b>	<b><u>5</u></b>
Visual Network Topology Overview.....	7
Network Architecture Overview.....	7
IAM Policies Overview.....	10
Multi-Factor Authentication (MFA).....	10
Implementation Details.....	11
<b><u>Security Data Collection &amp; Aggregation (Sprint 3: Week 5-6).....</u></b>	<b><u>12</u></b>
1. Design of Ingestion Pipelines:.....	13
Documentation and Automation:.....	14
Log Management & Normalization.....	14
<b><u>Security Automation &amp; Alert Correlation ( Sprint 4: Week 7-8).....</u></b>	<b><u>14</u></b>
Appendices.....	21
<b><u>User Interface &amp; Security Monitoring (Sprint 5: Week 9-10).....</u></b>	<b><u>24</u></b>
<b><u>Conclusion &amp; Resources .....</u></b>	<b><u>38</u></b>

# Introduction

## Project Overview

This project involves creating a cloud-based SIEM system to help organizations monitor their security, detect potential threats, and respond quickly to incidents. The system centralizes all security information to make it easier to manage and improve overall security. In Sprint 1, the focus is on establishing a solid foundation for the SIEM implementation project, including defining project goals, gathering requirements, and outlining the high-level architecture design.

For real-time updates on project tasks, progress, and collaboration, please refer to our Trello project board:

Trello Project Manager

<https://trello.com/invite/b/tgLHkUSF/ATTI3ad31a70d5845a23d363b6a999056f30F71F3F9E/siemcapstone-project>

Feel free to explore the board for task details, timelines, and team communications related to our SIEM system implementation.

## Project Goal

To build a scalable and automated SIEM system using cloud services like AWS, Azure, or GCP, enhancing an organization's ability to monitor security, detect threats, and respond to incidents efficiently.

## Requirements Gathering Report

The specified security data sources that the SIEM system on AWS will be collecting are listed in detail in the requirements gathering report. This includes security logs from other AWS services used, Amazon GuardDuty findings, Amazon S3 access logs, Amazon VPC flow logs, and AWS CloudTrail trails.

## High-Level Architecture Design Outline

The High-Level Architecture Design provides a blueprint for the necessary cloud services and security tools required for the SIEM system. This includes:

- Selection of a cloud SIEM service (e.g., AWS Security Hub, Amazon Kinesis Firehose with Splunk Cloud) based on further research and evaluation.
- Utilization of Amazon S3 for scalable and cost-effective log storage within the SIEM system architecture.
- Implementation of AWS CloudWatch Logs for initial log collection and filtering, integrated with the selected SIEM service for streamlined data ingestion and analysis.
- Definition of IAM policies and user setup with least privilege access for secure AWS resource management.

### **Required Documents**

- Conduct research to identify and document the various security data sources your SIEM system will collect logs from on AWS.
- Create a comprehensive Requirements Document outlining specific AWS security sources for log collection and system functionalities.

### **Additional Recommendations**

- Utilize project management tools (e.g., Trello, GitHub Project) for task management, progress tracking, and document sharing within the project team.
- Schedule regular team meetings to discuss progress, address roadblocks, and ensure alignment on project objectives.

## **Target Audience**

The system is designed for Security Operations Professionals, Security Analysts, and IT Security Teams.

## **Success Metrics**

- **Reduced Alert Fatigue:** Decrease the number of unnecessary security alerts.
- **Faster Incident Response Times:** Improve the speed of responding to security incidents.
- **Improved Security Visibility:** Enhance visibility into security issues across the organization.

## **Project Planning & Requirements Gathering (Sprint 1: Week 1-2)**

## Project Plan

The project plan outlines the goals, scope, and success criteria. It identifies stakeholders and provides a detailed 10-week schedule.

## Requirements Document

The requirements document identifies the types of security data needed, such as logs from firewalls and servers, and outlines the functionalities the SIEM system must have.

## High-Level Architecture Design

The high-level design identifies the necessary cloud services and security tools required for the SIEM system.

### Sprint 1: Project Planning & Requirements Gathering (Week 1-2)

- ☒ **Project Plan**
  - ☒ Define project goals, scope, and objectives.
  - ☒ Identify target audience and success metrics.
  - ☒ Create a detailed 10-week sprint schedule.
  - ☒ Document stakeholder expectations and deliverables.
- ☒ **Requirements Document**
  - ☒ Research and document security data sources.
  - ☒ Identify logs, network traffic, and endpoint data for ingestion.
  - ☒ Determine data retention requirements and compliance needs.
- ☒ **High-Level Architecture Design**
  - ☒ Outline cloud platform services for SIEM deployment.
  - ☒ Define core functionalities of the SIEM system.
  - ☒ Determine integration with existing security tools.
- ☒ **Milestone:** Completion of project plan.
- ☒ **Deliverable:** Project plan document.

## Secure Cloud Infrastructure & Access Control (Sprint 2: Week 3-4)

### Secure Cloud Network Design

The secure cloud network design defines a virtual network architecture within the chosen cloud platform to ensure data segregation and access control for SIEM components. This section outlines the network topology, subnets, security groups, and routing configurations necessary to establish a secure environment.

### Identity and Access Management (IAM)

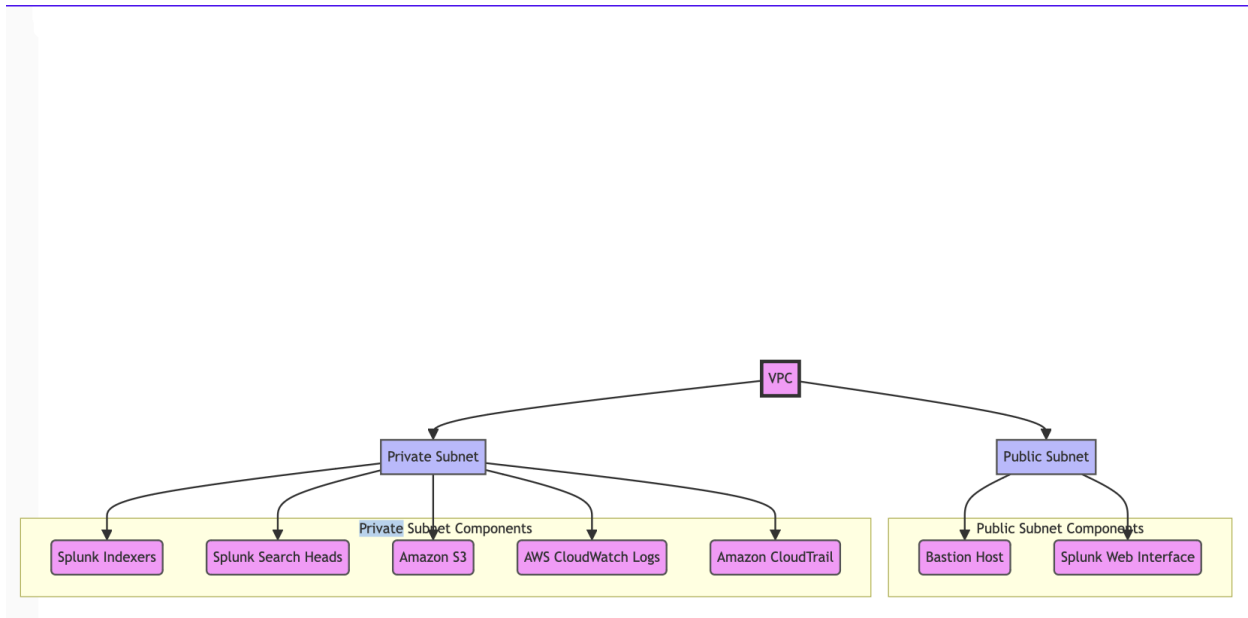
The IAM section focuses on implementing granular access control policies using IAM roles within the cloud platform. Access to SIEM functionalities is restricted based on user roles and privileges to ensure least privilege access and reduce the risk of unauthorized access or data breaches.

### Sprint 2: Secure Cloud Infrastructure & Access Control (Week 3-4)

- ☒ Secure Cloud Network Design
  - ☒ Design a secure virtual network architecture.
  - ☒ Segregate SIEM components within the cloud platform.
  - ☒ Implement network security controls (e.g., security groups, ACLs).
- ☒ Identity and Access Management (IAM)
  - ☒ Define IAM roles and permissions.
  - ☒ Configure IAM policies for granular access control.
  - ☒ Ensure least privilege access for users and services.
- ☒ **Milestone:** Secure cloud infrastructure and access control design finalized.
- ☒ **Deliverable:** Technical documentation for secure cloud infrastructure and access control.

## Visual Network Topology Overview

The following diagram depicts the network topology designed for our SIEM (Security Information and Event Management) system implementation. This architecture is configured to ensure secure and efficient communication among key components hosted within our cloud environment.



## Network Architecture Overview

### Virtual Private Cloud (VPC) Configuration:

To guarantee appropriate data segregation and access control, our SIEM system is installed inside a Virtual Private Cloud (VPC) on the selected cloud platform AWS. This VPC is split into separate public and private subnets.

- **Public Subnet Deployment:**
  - **Bastion Host:** Located in the public subnet, the bastion host acts as a secure gateway for authorized administrators to access private SIEM resources via SSH.

This deployment enhances the security posture by providing controlled and monitored access to internal components.

- **Splunk Web Interface (Front-end):** The Splunk web interface, utilized for SIEM dashboarding and log visualization, is hosted within the public subnet. This allows authorized users to access SIEM functionalities conveniently via web browsers after establishing a secure connection through the bastion host.
- **Private Subnet Deployment:**
  - **Splunk Indexers and Search Heads:** Splunk indexers, serving as the log storage and indexing engine, along with search heads for log processing and querying, are deployed within the private subnet. This configuration ensures that sensitive SIEM components are shielded from direct external access, enhancing overall system security.

### **Additional Log Storage and Management:**

- **Amazon S3 for Long-Term Log Storage:** ( Private Subnet)
  - Amazon S3 is utilized as a scalable and cost-effective solution for long-term storage and archival of log data generated by the SIEM system. This allows for retention of historical logs while optimizing storage costs and scalability.
- **AWS CloudWatch Logs Integration:**( Private Subnet)
  - AWS CloudWatch Logs plays a crucial role in aggregating, monitoring, and forwarding logs generated by various AWS services and SIEM components.
  - CloudWatch Logs seamlessly integrates with Amazon S3, allowing for the archival and storage of log data for compliance, auditing, and long-term analysis purposes within the SIEM ecosystem.
- **Amazon CloudTrail for Auditing and Monitoring:** (Private Subnet)
  - Amazon CloudTrail provides detailed logging of API calls and activities within your AWS environment, offering audit trails for compliance, security analysis, and troubleshooting. CloudTrail logs can be integrated with CloudWatch Logs and stored in Amazon S3, providing comprehensive visibility and monitoring capabilities across the SIEM infrastructure.



## Security Features and Access Control:

Our cloud network design incorporates robust security measures to safeguard SIEM infrastructure and log data:

- **Bastion Host Security:**
  - The bastion host acts as a secure entry point into the VPC, enforcing strict access controls through SSH authentication and IP whitelisting, limiting exposure to internal resources.
- **Network Security Controls:**
  - **Security Groups:** Applied to control inbound and outbound traffic flow, security groups define specific rules governing access to SIEM components, ensuring only authorized communication.
  - **Network ACLs:** Operating at the subnet level, network ACLs provide an additional layer of defense by filtering traffic based on predetermined rules, bolstering overall network security.
- **Encryption Mechanisms:**
  - **SSL/TLS Encryption:** Data transmitted within our SIEM infrastructure is secured using industry-standard encryption protocols (SSL/TLS), both in transit and at rest, ensuring data integrity and confidentiality.

## Connectivity and Operational Flow:

Our network architecture facilitates efficient connectivity and operational workflows:

- **Authorized User Interaction:**
  - Administrators establish secure SSH connections to the bastion host from external networks, leveraging encrypted communications for accessing SIEM resources securely.
- **User Access to Kibana:**
  - Upon connecting to the bastion host, users can seamlessly access the Kibana front-end interface via web browsers, enabling intuitive log visualization and analysis functionalities.
- **Log Processing Pipeline:**
  - Logstash processes log data sourced from various endpoints and applications, forwarding enriched logs to Elasticsearch for indexing and storage, forming the backbone of our SIEM data pipeline.

## IAM Implementation for SIEM Access Control

The IAM (Identity and Access Management) policies implemented for our SIEM (Security Information and Event Management) system focus on enforcing granular access control to secure resources and functionalities within the cloud platform. This ensures that users and components have appropriate permissions based on their roles and privileges, following the principle of least privilege to minimize potential security risks.

### IAM Policies Overview

1. **VPC (Virtual Private Cloud) Policy:** Defines access controls related to VPC resources, such as subnets, route tables, and network gateways.
2. **EC2 (Elastic Compute Cloud) Policy:** Specifies permissions for EC2 instances hosting SIEM components, controlling actions like instance launching, modification, and termination.
3. **S3 (Amazon Simple Storage Service) Policy:** Governs access to S3 buckets used for log storage and archival within the SIEM system, regulating object-level permissions and data management.
4. **GuardDuty Policy:** Manages access to Amazon GuardDuty, which provides threat detection and monitoring capabilities, ensuring appropriate monitoring of security events.
5. **CloudTrail Policy:** Controls access to AWS CloudTrail, enabling logging and auditing of API calls and account activity for compliance and security analysis purposes.

### Multi-Factor Authentication (MFA)

- **Enhanced Security with MFA:** Multi-Factor Authentication (MFA) is enabled for IAM users accessing SIEM functionalities, adding an extra layer of security beyond standard username and password authentication.
- **MFA Implementation:** IAM policies enforce the use of MFA for accessing critical SIEM resources and performing privileged operations, reducing the risk of unauthorized access even in the event of compromised credentials.

### Implementation Details

- **IAM Roles and Permissions:** IAM roles are assigned to users, applications, or services involved in SIEM operations, granting only necessary permissions to perform specific tasks.

- **Least Privilege Access:** Policies are designed to enforce the principle of least privilege, limiting access to SIEM functionalities based on the minimum permissions required for operational tasks.
- **Continuous Monitoring and Compliance:** IAM policies are regularly reviewed and updated to align with security best practices and compliance requirements, ensuring ongoing protection of SIEM resources and data.

By implementing these IAM policies, we establish a robust access control framework that enhances the security posture of our SIEM system, mitigating the risk of unauthorized access and data breaches.

## Security Data Collection & Aggregation (Sprint 3: Week 5-6)

- Security Data Ingestion Pipelines: Design and implement data ingestion.
- Log Management & Normalization: Configure log management platform.

### Sprint 3: Security Data Collection & Aggregation (Week 5-6)

- ☒ **Security Data Ingestion Pipelines:**
  - ☒ Design automated data ingestion pipelines to collect security data from various sources.
  - ☒ Implement ingestion pipelines for firewalls, intrusion detection systems, endpoint security agents, etc.
  - ☒ Ensure pipelines are scalable and reliable for continuous data collection.
- ☒ **Log Management & Normalization:**
  - ☒ Configure the log management platform for centralized storage of collected security data.
  - ☒ Normalize and enrich logs to standardize formats and enhance data analysis capabilities.
  - ☒ Implement normalization rules to ensure consistency across different log sources.
- ☒ **Milestone:** Completion of security data collection and aggregation setup.
- ☒ **Deliverable:** Technical documentation for security data collection and aggregation.

For the SIEM system to acquire thorough and timely security data from several sources, security data intake pipeline design and execution are essential. The architecture and procedures used to set up these pipelines are described in this section:

## 1. Design of Ingestion Pipelines:

- **Source Identification:**
  - Determine the primary sources of security data, including application logs, intrusion detection systems (IDS), firewalls, and endpoint security agents.
    - **Cloud service logs** (AWS CloudTrail, VPC Flow Logs, GuardDuty)
    - **On-premises security appliances** (e.g., firewalls, intrusion detection/prevention systems)
      - Firewalls: AWS Network Firewall
      - Intrusion Detection/Prevention Systems (IDS/IPS): AWS GuardDuty; Snort IDS/IPS; Suricata
    - **Endpoint security agents** (e.g., antivirus, EDR solutions)
      - Antivirus Solutions: AWS Systems Manager
    - **Application and server logs**
- **Ingestion Tools:**
  - Data from various sources can be gathered, parsed, and transformed using Splunk, then indexed and analyzed within the Splunk environment.
    - Utilize **Splunk** Forwarders to collect and process logs from various sources.
    - Forward processed logs to **Splunk Indexers** for indexing.
    - Store raw and processed logs in **Amazon S3** for archival purposes.
    - Ensure secure data transmission (e.g., encryption in transit and at rest) and access control for the ingestion pipelines.
- **Data Flow ( Data Transformation and Enrichment):**
  - Configure Splunk to handle data flow from various sources. Each pipeline is designed to handle specific kinds of security events and logs.
  - Parsing and structuring log data. Splunk Forwarders parse and structure log data before sending it to Splunk Indexers.
  - Enriching data with contextual information (e.g., IP geolocation, threat intelligence).
  - Normalize data formats for consistent analysis within the Splunk environment.

## Monitoring and Alerting:

Set up warning and monitoring systems for the data ingestion pipelines to identify and address problems such as:

- Pipeline failures or bottlenecks.
- Data loss or corruption.
- Security incidents or unauthorized access attempts.

## Documentation and Automation:

Record the configurations of the data ingestion pipeline, including the data sources, transformations, and enrichment stages.

- Utilize Infrastructure as Code (IaC) solutions such as AWS CloudFormation or Terraform to automate the deployment and management of the ingestion pipelines.
- Ensure that the IaC templates include provisions for setting up Splunk Forwarders, Indexers, and any required AWS services (e.g., S3 for log storage).

## Log Management & Normalization

Effective log management and normalization are critical for both threat detection and data analysis. This section explains the steps taken to configure the log management platform and standardize logs within the SIEM system:

### 1. Log Management Platform Configuration

A log management platform should be chosen and set up for centralized log analysis, storage, and visualization. Choices consist of:

- **Splunk:** For storing, indexing, and searching log data
- **Amazon S3:** For storing raw and processed logs.
- **Splunk Dashboard:** For visualizing and analyzing logs stored in Splunk.

### Configuration:

- Install and configure Splunk components (Forwarders, Indexers, Search Heads).

- Set up data inputs and indexes within Splunk for various log sources.
- Integrate Amazon S3 for long-term log storage and archival.

## 2. Log Normalization

To standardize the format and structure of logs from various sources and facilitate effective analysis and correlation, apply log normalization techniques.

- Use **Splunk's Data Onboarding** capabilities to extract relevant fields and map them to a common schema.
- Consider adopting industry-standard log formats or schemas (e.g., Common Event Format, Elastic Common Schema) for better interoperability.

### Log Indexing and Search:

#### Splunk Indexing:

- Set up Splunk so that the enhanced and normalized log data can be efficiently indexed and searched.
- Implement appropriate indexing strategies, such as time-based or field-based indexing, to optimize search performance and storage utilization.
- Utilize Splunk's **Indexer Clustering** for scalability and high availability.

### Access Control and Auditing:

- Use granular access control techniques to limit user roles and responsibilities-based access to log data.
- Configure **Splunk Role-based Access Control (RBAC)** to enforce access policies.
- Enable auditing and logging of user activities within the log management platform for security and compliance purposes.
- Use **Splunk's Audit Logs** to monitor and review user actions.

**Documentation and Knowledge Transfer:** Record the data formats, enrichment rules, and indexing strategies used in the log management and normalization operations.

- Document Splunk configurations, including data inputs, parsing rules, and index settings.
- Provide training and knowledge transfer sessions to ensure that security analysts and other stakeholders can effectively utilize the log management platform.
- Develop user manuals, training materials, and conduct hands-on workshops.

## Security Automation & Alert Correlation (Sprint 4: Week 7-8)

- **Technical Documentation:**

- Security Automation Playbooks: Develop automated playbooks.
- Threat Detection & Alert Correlation: Implement rules and ML models.

### Sprint 4: Security Automation & Alert Correlation (Week 7-8)

- ☒ **Security Automation Playbooks:**

- ☒ Develop automated playbooks using SOAR tools for incident response workflows.
- ☒ Define response actions for common security incidents and automate their execution.
- ☒ Test and validate automation playbooks to ensure effectiveness and reliability.

- ☒ **Threat Detection & Alert Correlation:**

- ☒ Implement rules and machine learning models for threat detection.
- ☒ Configure alert correlation logic to identify potential threats and reduce false positives.
- ☒ Fine-tune detection rules based on feedback and threat intelligence.

- ☒ **Milestone:** Security automation and alert correlation mechanisms implemented.

- ☒ **Deliverable:** Technical documentation for security automation and alert correlation.

## Security Automation Playbooks

**Objective:** To develop and implement security automation playbooks using AWS Security Hub and establish robust threat detection and alert correlation mechanisms within the SIEM system.

## 2.1 SOAR Tool Selection and Integration

### SOAR Tool Selection and Integration

- Tool Chosen: AWS Security Hub
- Integration Process:
  - Integrated AWS Security Hub with our Security Operations Center (SOC) infrastructure.
  - Connected AWS Security Hub to other AWS services such as AWS Lambda for automated response actions and AWS SNS for notifications.
- Challenges and Resolutions:
  - Challenge: Initial difficulties in configuring AWS Lambda triggers.
  - Resolution: Conducted additional training and utilized AWS documentation to properly configure the triggers.

## 2.2 Incident Response Playbooks

### Incident Response Playbooks

- Overview: Developed incident response playbooks using AWS Security Hub.
- Incident Types Covered:
  - Phishing Attempts:
    - Isolate affected systems
    - Notify users
    - Analyze email headers
  - Malware Infections:
    - Quarantine infected devices
    - Run antivirus scans
    - Notify IT security team
  - Unauthorized Access:



- Block access
  - Notify security operations center (SOC)
  - Investigate access logs
- Data Exfiltration:
  - Terminate data transfers
  - Notify data protection officer
  - Review audit logs
- Workflow and Automation Steps:
  - Automated workflows in AWS Security Hub trigger predefined response actions.
  - AWS Lambda automates actions such as isolating compromised instances or sending notifications via AWS SNS.
- Best Practices and Industry Standards:
  - Incorporated security best practices and industry standards like NIST and MITRE ATT&CK into playbook development.

## 2.3 Playbook Testing and Validation

### Playbook Testing and Validation

- Testing Procedures:
  - Created test cases to simulate various security incidents.
  - Verified that playbooks execute the correct response actions.
- Validation Metrics:
  - Effectiveness Metrics:
    - Response time
    - Success rate of automated actions
  - Feedback Loop:
    - Collected feedback from security analysts after testing.
    - Adjusted playbooks based on feedback and observed performance.
- Security Measures:
  - Ensured playbooks are secure and do not introduce any vulnerabilities or risks

## **2.4 Incident Response Playbook**

### **2.4.1 Introduction**

- Purpose: This playbook provides a standardized approach to responding to cybersecurity incidents.
- Scope: Applicable to all types of cybersecurity incidents affecting the organization's systems, data, and networks.

### **2.4.2 Roles and Responsibilities**

Incident Response Team (IRT): A group responsible for managing and coordinating the incident response.

- Incident Commander: Jesus Ayala
- Technical Lead: Jose Rodriguez
- Communications Lead: Jasmine Melton
- Legal/Compliance Officer: D'Andre Walden
- IT Support: Heimdall-SIEM Team

### **2.4.3 Incident Identification and Reporting**

- Detection: Continuous monitoring of systems using tools such as IDS/IPS, SIEM, and antivirus software.
- Reporting:
  - Any suspicious activity must be reported immediately to the IRT.
  - Use the incident reporting form (Appendix A).

### **2.4.4 Incident Classification**

- Low: Minor incidents with minimal impact (e.g., spam emails).
- Medium: Incidents with potential moderate impact (e.g., malware infection).
- High: Severe incidents with significant impact (e.g., data breach).

### **2.4.5 Initial Response**

- Containment:
  - Isolate affected systems to prevent further damage.
  - Implement network segmentation if necessary.
- Communication:
  - Notify stakeholders (internal and external) as per the communication plan.
  - Document all actions and decisions.

### **2.4.6 Investigation**

- Evidence Collection:
  - Preserve logs, system images, and any relevant data.
  - Follow chain of custody procedures.
- Analysis:
  - Determine the root cause of the incident.
  - Identify affected systems and data.

### **2.4.7 Eradication**

- Remove malware or other malicious code.
- Apply patches and updates.
- Verify that the threat has been eliminated.

### **2.4.8 Recovery**

- Restore systems to normal operations.
- Validate the integrity of restored systems and data.
- Monitor systems for any signs of recurring incidents.

### **2.4.9 Post-Incident Activities**

- Lessons Learned:

- Conduct a post-incident review meeting.
- Document findings and areas for improvement.
- Reporting:
  - Prepare an incident report (Appendix B).
- Updates:
  - Update policies and procedures based on lessons learned.

### 3. Appendices

- Appendix A: Incident Reporting Form
- Appendix B: Incident Report Template
- Appendix C: Contact Information for Incident Response Team

#### Appendix A: Incident Reporting Form

Field	Description
Date/Time	June 16, 2024, 10:20 UTC
Reporter Name	Jose Rodriguez
Reporter Contact	rodriguezjosemg@gmail.com
Incident Description	An alert was raised for several unauthorized login attempts to the AWS Management Console from an IP address in a different region during normal monitoring in AWS Security Hub. The user account jasmine.melton was the focus of the login attempts. When a successful login attempt was made after multiple unsuccessful attempts, there were worries that the user's credentials might have been compromised.
Affected Systems	- AWS Management Console - EC2 Instances - S3 Buckets
Initial Actions Taken	- Disabled the affected AWS IAM user account (jasmine.melton). - Blocked the suspicious IP address using AWS Network ACLs. - Triggered an immediate password reset for the compromised account. - Preserved CloudTrail logs and CloudWatch metrics for further investigation. -

	Notified the Incident Response Team (IRT), including Jesus Ayala, D'Andre Walden, and Jasmine Melton, to begin a coordinated response. <b>For AWS Config Error:</b> - Updated the S3 bucket policy to grant necessary permissions to AWS Config. Verified and specified the S3 key prefix in AWS Config settings. Configured the KMS key and ensured necessary permissions were granted.
Error Message	<b>Error message for AWS Config while trying to send logs to central bucket:</b> <i>Error: Insufficient delivery policy to S3 bucket: heimdall-central-bucket, unable to write to bucket, provided S3 key prefix is 'null', provided KMS key is 'null'.</i>

## Appendix B: Incident Report Template

Field	Description
Incident ID	INC-20240610-001
Date/Time of Detection	June 10, 2024, 10:20 UTC
Detected By	Jose Rodriguez
Incident Description	An alert was raised for several unauthorized login attempts to the AWS Management Console from an IP address in a different region during normal monitoring in AWS Security Hub. The user account jasmine.melton was the focus of the login attempts. When a successful login attempt was made after multiple unsuccessful attempts, there were worries that the user's credentials might have been compromised.
Impact Assessment	Access to sensitive data-containing S3 buckets and vital EC2 instances was possible for the compromised account. To avoid any data exfiltration and system compromise, quick action was needed..
Root Cause Analysis	The event was linked to a successful phishing attempt that obtained the user's credentials. Unintentionally, the user clicked on a malicious link and gave their login credentials on a phony

	Amazon login screen.
Actions Taken	<ul style="list-style-type: none"> <li>- Disabled the affected AWS IAM user account (jasmine.melton).</li> <li>- Blocked the suspicious IP address using AWS Network ACLs.</li> <li>- Triggered an immediate password reset for the compromised account.</li> <li>- Preserved CloudTrail logs and CloudWatch metrics for further investigation.</li> <li>- Conducted a full scan of systems for additional compromises.</li> <li>- Notified all relevant stakeholders and initiated a comprehensive review of access logs.</li> <li>- Addressed AWS Config error by updating the S3 bucket policy to allow sufficient permissions for writing logs.</li> </ul>
Recommendations	<ul style="list-style-type: none"> <li>- Implement multi-factor authentication (MFA) for all user accounts.</li> <li>- Conduct regular security awareness training to help users recognize phishing attempts.</li> <li>- Enhance monitoring and alerting for suspicious login activities.</li> <li>- Review and update incident response playbooks to include recent lessons learned.</li> </ul>
Prepared By	Jose Rodriguez
Reviewed By	Jesus Ayala

### Appendix C: Contact Information for Incident Response Team

Name	Role	Contact Information	Role Description
Jesus Ayala	Incident Commander / Security Data Engineer	Jesus.ayala.c13@gmail.com	<p>Coordinates incident response activities, ensuring thorough documentation and reporting.</p> <p>Design and implementation of data ingestion pipelines, log processes management, and leads incident response efforts as Commander.</p>
Jose Rodriguez	Technical Lead / Cloud Infrastructure Architect	rodriguezjosemg@gmail.com	<p>Designs and implements secure cloud infrastructure for the SIEM system, configuring virtual network architecture within the cloud platform and implementing granular IAM policies to control SIEM access.</p>

			Ensures the infrastructure supports scalability, high availability, and robust security measures..
Jasmine Melton	Communications Lead / Project Manager	jmelton09251@gmail.com	<p>Manages internal and external communications during incidents, updates stakeholders, and documents actions.</p> <p>Develop automated security playbooks using SOAR tools. Implement incident response workflows.</p>
D'Andre Walden	Legal-Compliance Officer / Threat Detection and Analysis Specialist	dandre.walden@gmail.com	<p>Ensures compliance with legal and regulatory requirements, develops and maintains security policies.</p> <p>Develop and refine correlation rules in the SIEM system for threat detection, integrate threat intelligence feeds and indicators of compromise (IoCs), conduct threat analysis, and refine detection rules for accuracy.</p>
Heimdall-SIEM Team	IT Support		Provides technical support and assists with maintaining the SIEM system and related infrastructure.

### 3. Threat Detection & Alert Correlation

#### 3.1 SIEM Solution and Data Sources

##### SIEM Solution and Data Sources

- **SIEM Solution Implemented:** AWS Security Hub
- **Data Sources Integrated:**
  - Logs
  - Network traffic
  - Endpoint data

- **Data Normalization and Enrichment:**
  - Normalized and enriched collected data for effective analysis and correlation.

## 3.2 Correlation Rules and Threat Detection

### Correlation Rules and Threat Detection

- **Correlation Rules Developed:**
  - Identified potential threats using developed correlation rules.
- **Rule Development Techniques:**
  - Pattern matching
  - Statistical analysis
  - Machine learning models
- **Incorporation of Threat Intelligence:**
  - Integrated threat intelligence feeds and indicators of compromise (IoCs) into correlation rules.
- **Tuning and Refinement:**
  - Regularly reviewed and updated correlation rules to reduce false positives and improve detection accuracy.

## 3.3 Alert Prioritization and Triage

### Alert Prioritization and Triage

- **Process Implemented:**
  - Alert prioritization and triage process in SOC.
- **Criteria for Severity Levels:**
  - Asset criticality
  - Threat level
  - Confidence score
- **Integration with Incident Response:**
  - Integrated alert prioritization with incident response playbooks and workflows.



- **Examples of High-Fidelity Alerts:**
  - Provided examples of high-fidelity alerts and corresponding actions taken.

## **User Interface & Security Monitoring (Sprint 5: Week 9-10)**

- **Technical Documentation:**
  - SIEM Interface Design: Develop a user-friendly dashboard.
  - Continuous Security Monitoring: Configure SIEM for real-time threat detection.

### **Sprint 5: User Interface & Security Monitoring (Week 9-10)**

- ☒ **User-Friendly SIEM Interface Design:**
  - ☒ Design and develop a user-friendly dashboard for security analysts.
  - ☒ Incorporate visualization tools for easy interpretation of security events.
  - ☒ Ensure the interface is intuitive and responsive for efficient workflow management.
- ☒ **Continuous Security Monitoring:**
  - ☒ Configure the SIEM solution for continuous monitoring of security events.
  - ☒ Implement real-time threat detection capabilities to identify security incidents promptly.
  - ☒ Set up alerts and notifications for proactive threat response.
- ☒ **Milestone:** Completion of SIEM system development and testing.
- ☒ **Deliverable:** Comprehensive documentation and training materials.

## **User-Friendly SIEM Interface Design Document**

### **1. Introduction**

The design concepts, wireframes, and mockups for our SIEM system's user-friendly dashboard are described in this document. The objective is to develop a user-friendly and effective interface that security analysts may use to track, examine, and react to security incidents.

#### **1. User Personas and Use Cases**

## User Personas

1. **Security Analyst:**
  - **Role:** Monitors security alerts, investigates incidents, and responds to threats.
  - **Needs:** Quick access to alerts, detailed event logs, and investigation tools.
2. **Security Manager:**
  - **Role:** Oversees security operations, reviews incident reports, and ensures compliance.
  - **Needs:** High-level summaries, compliance reports, and team performance metrics.
3. **IT Administrator:**
  - **Role:** Manages IT infrastructure, ensures system uptime, and supports the security team.
  - **Needs:** System health checks, configuration changes, and maintenance logs.

## Use Cases

1. **Real-Time Monitoring:**
  - **Description:** Security analysts need to monitor security events in real-time.
  - **Tasks:** View alerts, filter logs, and drill down into event details.
2. **Incident Investigation:**
  - **Description:** Analysts investigate security incidents to determine the cause and impact.
  - **Tasks:** Access historical data, analyze event correlations, and generate incident reports.
3. **Compliance Reporting:**
  - **Description:** Security managers generate compliance reports to meet regulatory requirements.
  - **Tasks:** Generate and review reports, ensure data retention, and audit trails.

## 3. Information Architecture and Navigation Flow

### Information Architecture

- **Home Dashboard:**
  - Overview of key metrics (total alerts, resolved incidents, active threats).
  - Quick access widgets (recent alerts, top threats, system health).
- **Alerts:**
  - List of all alerts with filtering options.
  - Detailed view for each alert.
- **Investigations:**

- Tools for incident investigation (log search, event correlation, network diagrams).
- Timeline of incidents and their resolutions.
- **Reports:**
  - Generate and view compliance and performance reports.
  - Export options (PDF, CSV).
- **Settings:**
  - Configuration settings for the SIEM system.
  - User management and permissions.

### Navigation Flow

- **Main Menu:** Home, Alerts, Investigations, Reports, Settings.
- **Sub-Menus:** Contextual based on the selected main menu item.

## 4. Visual Design Guidelines

### Color Schemes

- **Primary Colors:** Blue (#007BFF), White (FFFFFF), Gray (#6C757D).
- **Alert Colors:** Red (#DC3545) for critical, Orange (#FFC107) for warning, Green (#28A745) for resolved.

### Typography

- **Primary Font:** Arial, sans-serif.
- **Headings:** Bold, 16-24px.
- **Body Text:** Regular, 12-14px.

### Icons

- **Source:** Font Awesome or similar.
- **Usage:** Use consistent icons for similar actions (e.g., edit, delete, view details).

## 5. Dashboard Layout and Components

### Layout

- **Header:** Contains the logo, user profile, and notification icons.
- **Sidebar:** Main navigation menu.
- **Main Content Area:** Displays the selected dashboard view (e.g., alerts, investigations).

### Components

- **Widgets:** Mini-dashboards for quick metrics (e.g., total alerts, active threats).

- **Charts:** Bar charts, line graphs, and pie charts for visualizing data trends.
- **Tables:** Detailed lists with sorting and filtering options.
- **Forms:** Input forms for settings and configurations.

## 6. Interaction Design

### Filtering

- **Functionality:** Allow users to filter alerts and logs based on criteria (e.g., time range, severity).
- **UI Elements:** Dropdowns, date pickers, and search boxes.

### Drill-Downs

- **Functionality:** Enable users to click on items (e.g., alerts) to view detailed information.
- **UI Elements:** Expandable rows, modals, and new pages.

### Contextual Menus

- **Functionality:** Provide quick actions (e.g., mark as resolved, assign to analyst) via right-click or hover menus.
- **UI Elements:** Pop-up menus, tooltips.

## 7. Accessibility and Usability Considerations

- **Accessibility:** Ensure the interface is accessible to users with disabilities (e.g., screen reader support, keyboard navigation).
- **Usability:** Conduct user testing to ensure the interface is intuitive and easy to use. Apply feedback to improve user experience.

## 8. Front-End Code Repository

- **Repository:** [GitHub Repository Link]
- **Structure:** Organized by folders (e.g., HTML, CSS, JavaScript).
- **Documentation:** README file with setup instructions, coding standards, and contribution guidelines.

## 9. User Testing Report

### Methodology

- **Participants:** Security analysts and IT administrators.
- **Tasks:** Monitor alerts, investigate incidents, generate reports.

### Findings

- **Positive Feedback:** Users found the dashboard intuitive and visually appealing.
- **Areas for Improvement:** Some users suggested adding more filter options and improving load times for large datasets.

### Recommendations

- **Implement:** Additional filtering capabilities and optimize data loading performance.
- **Iterate:** Continuously gather user feedback and iterate on the design.

## 2. Continuous Security Monitoring

### 2.1 Monitoring Architecture Diagram

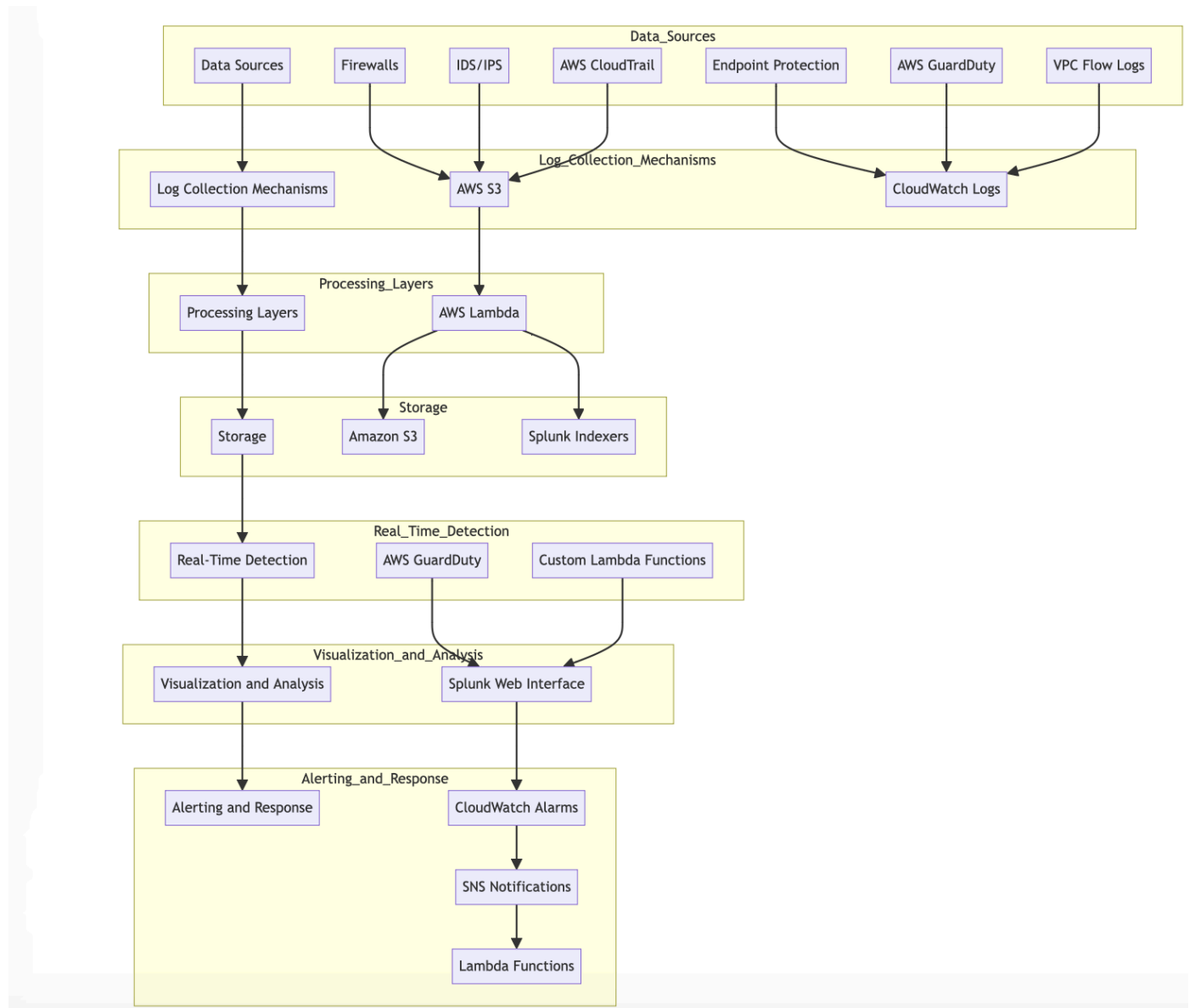
- **Diagram Overview:** The architecture for continuous security monitoring, detailing data sources, log collection mechanisms, and real-time threat detection components.

### Components:

1. **Data Sources:** Firewalls, IDS/IPS, Endpoint Protection, Cloud Services (AWS CloudTrail, AWS GuardDuty, VPC Flow Logs)
2. **Log Collection Mechanisms:** AWS S3, CloudWatch Logs
3. **Processing Layers:** AWS Lambda for log processing
4. **Storage:** Centralized log storage in Amazon S3, Splunk Indexers for indexing and search
5. **Real-Time Detection:** Amazon GuardDuty, Custom Lambda functions for additional threat detection
6. **Visualization and Analysis:** Splunk Web Interface for dashboards and visualizations
7. **Alerting and Response:** CloudWatch Alarms, SNS for notifications, Lambda for automated responses

### Visual Network Topology Overview

The following diagram depicts the network topology designed for our SIEM (Security Information and Event Management) system implementation with Splunk. This architecture is configured to ensure secure and efficient communication among key components hosted within our AWS cloud environment. The design incorporates public and private subnets, secure access controls, and integration with AWS services for log storage and monitoring.



## 2.2 Data Source Integration Guide

### Integrating Firewalls:

- **Configuration:** Enable log forwarding to an S3 bucket or directly to CloudWatch Logs.
- **Parser:** Use a Lambda function to parse firewall logs and send them to Splunk.

### Integrating IDS/IPS:

- **Configuration:** Configure IDS/IPS to forward logs to an S3 bucket or CloudWatch Logs.
- **Parser:** Use a Lambda function to parse IDS/IPS logs and send them to Splunk.

### Integrating Endpoint Protection:

- **Configuration:** Enable log forwarding from endpoint protection software to an S3 bucket or CloudWatch Logs.
- **Parser:** Use a Lambda function to parse endpoint protection logs and send them to Splunk.

### Integrating Cloud Services:

- **AWS CloudTrail:**
  - **Configuration:** Enable CloudTrail and configure it to send logs to an S3 bucket.
  - **Parser:** Use a Lambda function to parse CloudTrail logs and send them to Splunk.
- **AWS GuardDuty:**
  - **Configuration:** Enable GuardDuty and configure it to send findings to CloudWatch Events.
  - **Parser:** Use a Lambda function to parse GuardDuty findings and send them to Splunk.
- **VPC Flow Logs:**
  - **Configuration:** Enable VPC Flow Logs and configure them to send logs to an S3 bucket or CloudWatch Logs.
  - **Parser:** Use a Lambda function to parse VPC Flow Logs and send them to Splunk.

## 2.3 Threat Detection Rules and Correlation Engines

### Threat Detection Rules:

- **Rule 1: Suspicious Login Activity:**
  - **Description:** Detects multiple failed login attempts followed by a successful login.
  - **Logic:** If more than 5 failed login attempts are followed by a successful login within 10 minutes, generate an alert.
  - **Implementation:** Use Splunk's search processing language (SPL) to query and analyze CloudTrail logs for this pattern.
- **Rule 2: Data Exfiltration:**
  - **Description:** Detects large data transfers that may indicate data exfiltration.
  - **Logic:** If data transfer exceeds a threshold within a short period, generate an alert.

- **Implementation:** Use Splunk queries and custom alerting mechanisms to monitor VPC Flow Logs for large data transfers.

### Correlation Engines:

- **Engine 1: Anomaly Detection:**
  - **Description:** Uses machine learning to detect anomalies in network traffic and user behavior.
  - **Models:** Anomaly detection models trained on historical data.
  - **Implementation:** Splunk's Machine Learning Toolkit (MLTK) applies these models to real-time data for anomaly detection.
- **Engine 2: Event Correlation:**
  - **Description:** Correlates events from different data sources to identify complex attack patterns.
  - **Logic:** Uses predefined correlation rules to link related events across multiple logs.
  - **Implementation:** Splunk's correlation search capabilities are used to correlate events and trigger alerts based on defined rules.

## 2.4 Alerting and Notification Configuration

### Configuring Alerts and Notifications:

1. **Splunk Alerts:**
  - **Configuration:** Set up alerts within Splunk for key security metrics and detected threats.
  - **Example:** Create an alert for anomalous login activities detected in Splunk.
    - **Trigger Condition:** More than 5 failed login attempts followed by a successful login within 10 minutes.
    - **Action:** Trigger an alert to the designated security team.
2. **Splunk Notifications:**
  - **Configuration:** Configure notifications within Splunk to notify security teams in real-time.
  - **Channels:** Utilize email and SMS notifications for immediate alert dissemination.
  - **Example:**
    - **Notification Channels:** security-team@example.com, +1234567890
    - **Event:** Notify on detection of critical security incidents
3. **Incident Response Workflows:**
  - **Integration:** Integrate Splunk alerts with automation tools like AWS Lambda for rapid incident response.
  - **Example:** Automatically initiate isolation of a compromised system based on Splunk alert triggers.
    - **Automation Script:** Lambda function triggered by Splunk alert for suspicious activity.
4. **Escalation Procedures:**



- **Configuration:** Define escalation paths for critical alerts to ensure timely response.
- **Example:** Escalate unacknowledged alerts to senior security personnel after a designated time frame.
  - **Procedure:** Notify on-call analyst initially; escalate to security manager if not acknowledged within 10 minutes.

### 3. Testing Report & Security Baseline

#### 3.1 Test Plan and Test Cases

**Test Plan Overview:** The test plan outlines the testing strategy, scenarios, and cases to validate the SIEM platform functionalities, security posture, and alert correlation rules.

#### Test Scenarios:

1. **Log Ingestion:** Validate correct ingestion of logs from various sources into Splunk.
2. **Real-Time Threat Detection:** Validate the effectiveness of real-time threat detection mechanisms in Splunk.
3. **Log Processing:** Ensure that AWS Lambda processes logs accurately and sends them to Splunk.
4. **Data Storage:** Verify that logs are stored correctly in Amazon S3 and indexed in Splunk.
5. **Visualization and Analysis:** Confirm that Splunk dashboards display data correctly and enable effective analysis.
6. **Alerting and Response:** Validate that Splunk alerts trigger notifications and automated responses appropriately.

Test Case ID	Test Scenario	Description	Expected Result
TC01	Log Ingestion	Verify logs are ingested from firewalls	Logs appear in Splunk and Amazon S3 bucket
TC02	Log Ingestion	Verify logs are ingested from IDS/IPS	Logs appear in Splunk and Amazon S3 bucket
TC03	Real-Time Threat Detection	Simulate a threat and verify GuardDuty detection	GuardDuty generates a finding and sends alert
TC04	Real-Time Threat Detection	Trigger a custom Lambda function for a simulated threat	Lambda function processes the threat and sends alert
TC05	Log Processing	Verify Lambda processes logs and	Logs appear in Splunk

		sends to Splunk	
TC06	Data Storage	Verify logs are stored in Amazon S3	Logs are present in the specified S3 bucket
TC07	Data Storage	Verify logs are indexed in Splunk	Logs are searchable in Splunk
TC08	Visualization and Analysis	Verify alternative visualization tool for log data	Logs are displayed correctly in the alternative visualization tool
TC09	Alerting and Response	Trigger a CloudWatch Alarm and verify SNS notification	SNS sends a notification email/SMS
TC10	Alerting and Response	Trigger a CloudWatch Alarm and verify Lambda response	Lambda function executes the configured response action

### 3.2 Test Execution Report

**Test Execution Overview:** This section documents the results of the executed test cases, noting any issues or defects identified and their resolutions.

#### Execution Results:

Test Case ID	Description	Result	Issues/Defects Identified	Resolution
TC01	Verify logs are ingested from firewalls	Passed	None	N/A
TC02	Verify logs are ingested from IDS/IPS	Passed	None	N/A
TC03	Simulate a threat and verify GuardDuty detection	Passed	None	N/A
TC04	Trigger a custom Lambda function for a simulated	Failed	Lambda function not triggering correctly	Updated Lambda trigger configuration

	threat			
TC05	Verify Lambda processes logs and sends to Splunk	Passed	None	N/A
TC06	Verify logs are stored in Amazon S3	Passed	None	N/A
TC07	Verify logs are indexed in Splunk	Passed	None	N/A
TC08	Verify alternative visualization tool for log data	Passed	None	N/A
TC09	Trigger a CloudWatch Alarm and verify SNS notification	Passed	None	N/A
TC10	Trigger a CloudWatch Alarm and verify Lambda response	Failed	Lambda function response delayed	Optimized Lambda function and reduced execution time

**Summary:** Overall, the majority of test cases passed successfully. Issues identified were promptly resolved, and the SIEM platform operates as expected. Follow-up tests confirmed that all resolutions were effective.

### 3.3 Security Baseline Document

**Security Baseline Overview:** The security baseline defines acceptable security configurations, hardening guidelines, and best practices for the SIEM platform and its underlying infrastructure. It ensures that the system adheres to security policies and protects against threats.

#### Security Configurations:

1. **AWS Account Security:**
  - Enable MFA for all IAM users.
  - Use IAM roles instead of root accounts for administrative tasks.
  - Regularly rotate IAM access keys.
2. **S3 Bucket Security:**
  - Enable bucket versioning and logging.
  - Apply bucket policies to restrict access.

- Enable default encryption for all objects stored in S3.
- 3. **Network Security:**
  - Use VPC to isolate resources.
  - Apply security groups and NACLs to control inbound and outbound traffic.
  - Enable VPC Flow Logs for monitoring network traffic.
- 4. **Data Encryption:**
  - Encrypt data at rest using AWS KMS.
  - Encrypt data in transit using SSL/TLS.
  - Use secure protocols for data transfer.
- 5. **Logging and Monitoring:**
  - Enable CloudTrail to log all API activity.
  - Configure CloudWatch for monitoring and alerting.
  - Ensure GuardDuty is enabled for threat detection.
- 6. **Instance Security:**
  - Regularly update and patch EC2 instances.
  - Use Amazon Inspector for vulnerability assessments.
  - Implement least privilege access for applications and services.
- 7. **Compliance and Auditing:**
  - Conduct regular security audits and assessments.
  - Ensure compliance with industry standards (e.g., PCI-DSS, HIPAA).
  - Maintain detailed logs and records for audit purposes.

#### **Hardening Guidelines:**

- Disable unnecessary services and ports.
- Remove default passwords and accounts.
- Apply the principle of least privilege for all users and services.
- Regularly review and update security configurations.

#### **Best Practices:**

- Regularly back up critical data and configurations.
- Implement incident response and disaster recovery plans.
- Train staff on security awareness and best practices.
- Stay informed about new threats and vulnerabilities.

## **4. Knowledge Transfer & Handover Package**

### **4.1 User Manual**

**Overview:** This manual provides detailed instructions for the installation, configuration, and operation of the SIEM platform. It includes step-by-step instructions, screenshots, and troubleshooting tips.

## Sections:

- **Installation:**
  - System requirements.
  - Installation steps for the SIEM components (AWS CloudTrail, GuardDuty, VPC Flow Logs, AWS Config, Splunk).
- **Configuration:**
  - Configuring data sources.
  - Setting up AWS services for integration with Splunk.
  - Configuring alerting and notifications in Splunk.
- **Operation:**
  - Using the Splunk interface for log analysis.
  - Monitoring and investigating alerts in Splunk.
  - Generating and viewing reports using Splunk capabilities.
- **Troubleshooting:**
  - Common issues specific to Splunk and their solutions.
  - How to collect logs and troubleshoot for support.

## 4.2 Training Materials

**Overview:** Develop comprehensive training materials to facilitate knowledge transfer to the security team. This includes presentations, videos, and interactive tutorials.

### Materials:

- **Presentations:** Slide decks covering the overview of the SIEM system, key features, and how to use the interface.
- **Videos:** Step-by-step video tutorials demonstrating the installation, configuration, and usage of the SIEM platform.
- **Interactive Tutorials:** Hands-on labs and exercises to practice using the SIEM system.

## 4.3 Deployment and Maintenance Guide

**Overview:** This guide provides a comprehensive outline of the deployment process, system requirements, backup and recovery procedures, and ongoing maintenance tasks for the SIEM platform.

### Sections:

- **Deployment:**
  - Detailed deployment steps.
  - Pre-deployment checklist.
  - Post-deployment verification.
- **System Requirements:**
  - Hardware and software requirements.
  - Network requirements.

- **Backup and Recovery:**
  - Backup strategies and schedules.
  - Recovery procedures.
- **Maintenance:**
  - Regular maintenance tasks.
  - Monitoring and health checks.
  - Updating and patching the system.

## 4.4 Source Code Documentation

**Overview:** Document the source code of the SIEM platform, including inline comments, architecture diagrams, and API documentation to facilitate future development and maintenance.

**Sections:**

- **Inline Comments:** Ensure all source code is well-commented.
- **Architecture Diagrams:** Visual representations of the system architecture.
- **API Documentation:** Detailed documentation of any APIs used or created, including endpoints, request/response formats, and usage examples.

## 4.5 Handover Checklist



**Overview:** Create a checklist to ensure a smooth transition of the SIEM platform to the security team. This includes any outstanding tasks, known issues, and future enhancement plans.

**Checklist:**


- ☐ All documentation is complete and reviewed.
  - ☐ Training materials are created and distributed.
  - ☐ User manual is reviewed and accessible.
  - ☐ Deployment and maintenance guide is complete.
  - ☐ Source code is documented and checked into the repository.
  - ☐ All test cases are executed and passed.
  - ☐ Outstanding tasks are identified and assigned.
  - ☐ Known issues are documented with mitigation plans.
  - ☐ Future enhancement plans are outlined.
-

# Resources

## Capstone Project Documents

1.  Capstone Project 2024 - Final Deliverables
2. <https://docs.google.com/document/d/1VpPdi99zy8kB56csmfv-fbbFWc6TWT71yUpo73TLi3s/edit#heading=h.ae289x9ezy7e>
3.  TKH\_SIEM\_CAPSTONE\_Project\_TEAM2\_TechDoc

## Related Articles and Tutorials

- <https://www.linkedin.com/pulse/how-create-siem-solution-similar-elastic-search-stack-ahmed-hassan/>
-  Logstash Elasticsearch Kibana Tutorial | Logstash pipeline & input, output config...
- [Build Your Own SIEM Stack with Open Source Tools Series | by SOCFortress | Medium](#)

## Documentation and Guides

- [Elasticsearch: The Official Distributed Search & Analytics Engine | Elastic](#)
- [Kibana: Explore, Visualize, Discover Data | Elastic](#)
- [Logstash: Collect, Parse, Transform Logs | Elastic](#)
- [What is ELK stack? - Elasticsearch, Logstash, Kibana Stack Explained - AWS](#)

## Specific Tutorials and Configurations

- Logstash Netflow Module Documentation
-  AWS OpenSearch Service | Kibana Dashboard | Setup Elastic Search On AWS

## Tools and Software:

- Mermaid.live - Online tool for generating diagrams using Mermaid syntax, including network topology diagrams for technical documentation.