IBM Innovation Center for Education

PHEMESOFT Software That Matters
TRUSTED DELIVERY PARTNER for IBM ICE

YENEPOYA (DEEMED TO BE UNIVERSITY)

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) INTEGRATION

Low-Level-Design

WORKING OF SEIM TOOLS

BACHELOR OF COMPUTER APPLICATION

CYBER SECURITY , ETHICAL HACKING , DIGITAL FORENSIC

2023-2026

SUBMITTED BY :

- Mohammed Shaan K- 23BCCED019 - 25154@yenepoya.edu.in - +91 8075909711
- Sreelakshmi Sreejith - 23BCCED033 - 25858@yenepoya.edu.in - +91 7511103331
- Akshitha K - 23BCCED006 - 26185@yenepoya.edu.in - +91 9074579508
- Neha Sreejith - 23BCCED025 - 25169@yenepoya.edu.in - +91 7025504075
- Prajwal M - 23BCCED026 - 26870@yenepoya.edu.in - +91 8089672524
- Rajih Ali P P - 23BCCED027 - 26893@yenepoya.edu.in - +91 9995590963

IBM Innovation Center for Education

PHEMESOFT Software That Matters

TRUSTED DELIVERY PARTNER for IBM ICE

GUIDED BY

MR.SHASHANK

Table of Content

1. Introduction

● **Purpose of the SIEM tool**

Real-Time Monitoring: SEIM tools continuously monitor security events and logs from various sources within an organization, providing real-time visibility into potential security threats.

SEIM tools are essential for enhancing an organization's cybersecurity strategy by providing visibility, improving incident response, and ensuring compliance.

● **Importance of SIEM tool**

Enhanced Security Posture: SEIM tools provide organizations with a comprehensive view, allowing them to identify vulnerabilities and threats quickly.

Real-Time Threat Detection: These tools enable real-time monitoring and alerting, which helps in the immediate detection of suspicious activities or potential breaches.

Centralized Log Management: SEIM tools aggregate logs and security data from multiple sources, making it easier for security teams to analyse and correlate events.

● Overview of the system development

SEIM (Security Information and Event Management) tools are developed through several key steps:

- **Requirements Gathering**: Identify what features stakeholders need, like log collection and real-time monitoring.
- **Architecture Design**: Create a scalable system architecture for data flow and processing.
- **Technology Selection**: Choose programming languages, databases, and frameworks suitable for the tool.

- **Data Collection**: Implement methods to gather logs from various sources and normalize them.

- **Event Correlation**: Develop algorithms to correlate events and detect security incidents, possibly using machine learning.

- **User Interface**: Build an intuitive dashboard for monitoring and reporting.

- **Testing**: Conduct unit, integration, and performance testing to ensure reliability.

- **Deployment**: Set up production environments and implement CI/CD for updates.

- **Monitoring and Maintenance**: Continuously monitor system health and gather user feedback for improvements.

- **Compliance**: Ensure the tool meets regulatory standards and regularly update it.

2. Scope of SIEM tool

- **What are the several key aspects of SIEM tool?**
  - **Log Management**: Collecting, storing, and managing logs from various sources like servers, firewalls, and applications.
  - **Real-Time Monitoring**: Continuously monitoring network traffic and system activities to identify suspicious behaviour as it happens.

- **Event Correlation**: Analyzing and correlating different logs and events to detect patterns that may indicate security threats.

- **Incident Response**: Providing tools and workflows for responding to detected security incidents, including alerts and automated responses.

● **Limitations and exclusions**

SEIM tools have several limitations and exclusions, including:

- **Data Overload**: They can generate a large volume of alerts, making it challenging for security teams to prioritize and respond effectively.

- **False Positives**: SEIM tools may produce false alarms, leading to alert fatigue among analysts and potentially missing real threats.

- **Integration Challenges**: Integrating with diverse data sources and existing security tools can be complex and time-consuming.

3.Intended Audience

● **Target audience for SIEM tool**

- **IT Security Teams**: Professionals responsible for monitoring and managing security incidents within an organization.

- **CISOs and Security Managers**: Senior leaders who need comprehensive visibility into security posture and incident response capabilities.

- **Compliance Officers**: Individuals focused on ensuring adherence to regulations and standards such as GDPR, HIPAA, or PCI DSS, who require audit trails and reporting.

4. System Overview

- **Data preprocessing**:- Data preprocessing in the context of a SEIM (Security Information and Event Management) tool involves several steps to prepare raw data for analysis and ensure that it can be effectively used for security monitoring and incident response. Here's a detailed overview of the data preprocessing steps typically involved:

- **Data Collection**: Gather data from various sources such as servers, network devices, applications, and security devices. This data can include logs, alerts, and events.

- **Data Normalization**: Convert data from different formats into a consistent format. This is important because different devices and applications may log information differently. Normalization helps in standardizing the data for easier analysis.

- **Model selection**:- Model selection for a SEIM tool involves defining objectives, collecting relevant data, selecting important features, choosing appropriate algorithms, training and validating the models, evaluating their performance using metrics, implementing the best model, and continuously improving it with new data. This ensures effective threat detection and response.

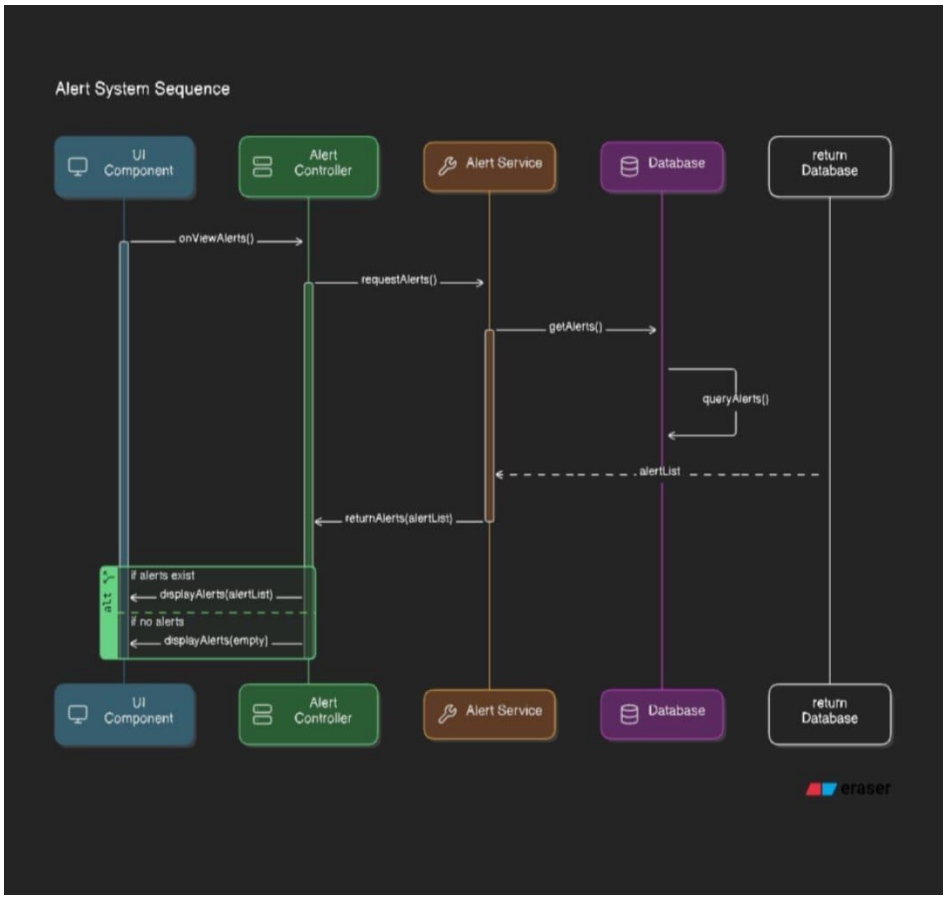
- **Evaluation metrics:-**

1) SEIM tool evaluation metrics include:

1. Accuracy: Overall correctness of predictions.
2. Precision: True positives among all positive predictions.
3. Recall: True positives among actual positives.
4. F1 Score: Balance between precision and recall.
5. True Positive Rate (TPR): Proportion of actual positives correctly identified.
6. False Positive Rate (FPR): Proportion of actual negatives incorrectly identified as positives.
7. ROC Curve: Graphical representation of TPR vs. FPR.
8. AUC-ROC: Measures the ability to discriminate between classes.
9. Mean Time to Detect (MTTD): Average time to detect incidents.
10. Mean Time to Respond (MTTR): Average time to respond to incidents.

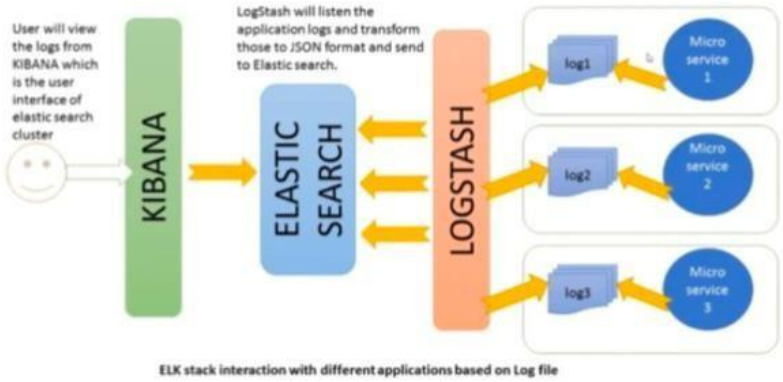
2) These metrics help assess the effectiveness of a SEIM tool in detecting and responding to security threats.

5. LOW LEVEL SYSTEM DIAGRAM SEQUENCE DIAGRAM:



6. DATA DESIGN

- **SIEM tool ELK stack is an example.**



ELK stack interaction with different applications based on Log file

ELK Stack points are:

1. **Elasticsearch**: For storing and searching data.
2. **Logstash**: For collecting and processing data from various sources.
3. **Kibana**: For visualizing data and creating dashboards.
4. **Scalability**: Can handle large data volumes and scale easily.
5. **Real-time Processing**: Supports real-time data analysis.
6. **Open Source**: Free to use with community support.

These make ELK Stack effective for data analysis and monitoring.

7.Model Development

Delection of deep learning models

- **Recurrent Neural Networks (RNNs)** ○ Use Case: Time series analysis, such as analyzing logs and detecting anomalies over time. ○ Advantages: Effective for sequential data and can capture temporal dependencies in event logs
- **Long Short-Term Memory Networks (LSTMs)**

o Use Case: Detecting patterns in sequences of security events or logs. o Advantages: Overcome the vanishing gradient problem, making them suitable for longer sequences.

- **Convolutional Neural Networks (CNNs)** o Use Case: Analyzing network traffic and intrusion detection. o Advantages: Can extract spatial features from data representations, useful for identifying patterns in multidimensional data.

- ❖ **Autoencoders** o Use Case: Anomaly detection by learning to reconstruct normal behavior. o Advantages: Can effectively learn representations of data and identify deviations from the norm.

8.Training and Evaluation

Training process

1. Define Objectives
   • Identify what you want to achieve with the SIEM tool, such as threat detection, compliance reporting, incident response, etc.

2. Data Collection
   • Log Sources: Integrate various data sources (e.g., firewalls, IDS/IPS, servers, applications) to collect logs and events. • Data Normalization: Ensure that incoming data is standardized for easier analysis.
3. Baseline Establishment
   • Analyze normal network behavior to establish a baseline. This helps in identifying anomalies later.
4. Rule and Alert Configuration
   • Create and configure correlation rules based on known attack patterns and behaviors. • Set up alert thresholds for different types of events to prioritize responses.

5. Machine Learning Models (if applicable)
   • If using advanced SIEMs with machine learning capabilities, train models on historical data to identify patterns of normal and malicious behavior.

6. Testing and Tuning
   • Run the SIEM in a testing environment to validate the rules and alerts. • Fine-tune the rules and thresholds based on false positives and negatives.

9.Validation and Testing procedure

Validation and testing of a SEIM tool involve several key steps:
1.**Requirements Verification**: Ensure the SEIM tool meets the specified security requirements and compliance standards.
2**. Data Integration Testing**: Test the tool's ability to collect and integrate data from various sources like logs, servers, and applications.
3**.Functionality Testing**:Verify that all features, such as alerting, reporting, and dashboard functionalities, work as intended.
4**.Performance Testing**: Assess the tool's performance under different loads to ensure it can handle the expected volume of data without lag.
5**.Incident Response Testing**: Simulate security incidents to evaluate the tool's ability to detect, alert, and respond effectively.
6**.User Acceptance Testing (UAT):** Gather feedback from end-users to ensure the tool meets their needs and is user-friendly.
These steps help ensure that the SEIM tool is effective, reliable, and ready for deployment.

10.CONCLUSION

In conclusion, a SEIM tool is essential for organizations to enhance their security posture. It provides real-time monitoring, threat detection, and incident response capabilities by aggregating and analyzing security data from various sources. By utilizing advanced analytics, machine learning, and threat intelligence, SEIM tools help in identifying potential security incidents quickly, allowing for timely responses to mitigate risks. Overall, implementing a SEIM tool is a crucial step in protecting an organization's assets and ensuring compliance with security regulations.

11.REFERENCE:

Here are some references you can explore for more information on SEIM tools:

1. Books:
- "Security Information and Event Management (SIEM) Implementation" by David Miller
2. Online Articles:
- "What is SIEM? A Complete Guide" on various cybersecurity websites like Splunk or IBM.
- "Understanding the Role of SIEM in Security Operations" on industry blogs.
3. Research Papers:
- Papers on platforms like IEEE Xplore or ResearchGate discussing the effectiveness and implementation of SEIM tools.
4. Vendor Documentation:
- Documentation from leading SEIM tool providers like Splunk, IBM QRadar, and ArcSight for detailed insights and use cases. Blogs on cybersecurity websites like SecurityIntelligence, Tripwire, or DarkReading.