SIEM Tool

Group Members:

Arjun C Santhosh	Roll No: CB.EN.U4CYS21010
G H Hem Sagar	Roll No: CB.EN.U4CYS21016
Madhav Harikumar	Roll No: CB.EN.U4CYS21038
Nishanth S	Roll No: CB.EN.U4CYS21050

TIFAC-CORE in Cyber Security
Amrita Vishwa Vidyapeetham, Coimbatore Campus

November 2024

Outline

1. Problem Statement
2. Objectives
3. Project Architecture
4. Current Status
5. Group Members' Contributions
6. Future Work
7. Screenshots and Results

Problem Statement

- Security teams face overwhelming volumes of complex security events, leading to alert fatigue and inefficiencies.
- Traditional methods struggle to deliver real-time threat detection and actionable insights.
- This increases the risk of delayed responses, operational inefficiencies, and potential breaches.

Objectives

1. **Centralized Log Collection**: Use Winlogbeat to collect logs from various sources and centralize them.
2. **Efficient Log Transportation**: Configure Kafka to ensure reliable and scalable log transportation.
3. **Real-time Log Correlation and Analysis**: Implement Apache Spark to correlate logs and detect threats in real time.
4. **User-friendly Dashboard**: Create a JavaScript-based dashboard for real-time visualization and alerting.
5. **Scalability**: Design the system to handle increasing log volume and complexity.
6. **Testing and Validation**: Conduct thorough testing and validation to ensure high accuracy and reliability in threat detection

Complete Project Architecture

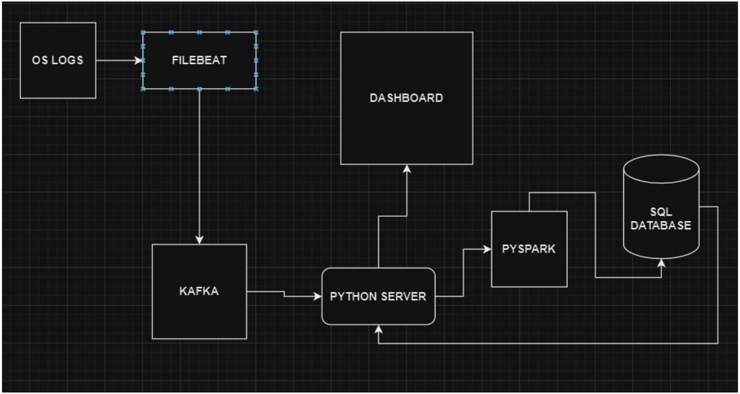


Figure: Project Architecture Diagram

Current Status

- **Completed Work (Overall):**
  - Interface design and implementation.
  - Core workflow setup.
  - Scalable architecture design.
- **Pending Work (Overall):**
  - Interface/Dashboard refinement.
  - Implementation of additional correlation functions.
  - Modularization of code.
  - System validation and testing.

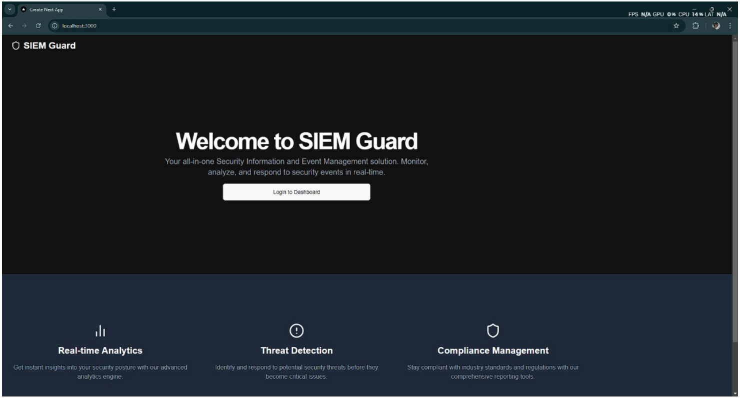
Group Members' Contributions

- **Arjun C Santhosh:**
  - Docker config file setup
  - Kafka setup
  - Pre-processor script for the logs from Kafka
  - Correlation function for RDP attack Detection
  - Front End UI
- **G H Hem Sagar:**
  - Correlation Engine Implementation and Database-Storage Integration
  - Reduced overhead for database operations
- **Madhav Harikumar:**
  - Pyspark Setup
  - Correlation functions and rule engine (Scripts) implementation
  - Simulating attacks on Windows machines to gather logs for correlation
- **Nishanth S:**
  - Created a flask server for receiving processed data from kafka
  - Simulated various attacks in SMB and privilege escalation, and gathered logs only for privilege escalation.

Planned Work for the Next Four Months

- **UI Performance Optimization:** Enhance and refine UI components to improve efficiency, responsiveness, and scalability.
- **Development of Additional Correlation Functions:** Expand the library of correlation functions to support advanced use cases.
- **Finalization and Maintenance of the SIEM Workflow:** Complete the remaining tasks in the Security Information and Event Management (SIEM) workflow and ensure its smooth operation and upkeep.

Home Page



Welcome to SIEM Guard

Your all-in-one Security Information and Event Management solution. Monitor, analyze, and respond to security events in real-time.

Real-time Analytics

Get instant insights into your security posture with our advanced analytics engine.

Threat Detection

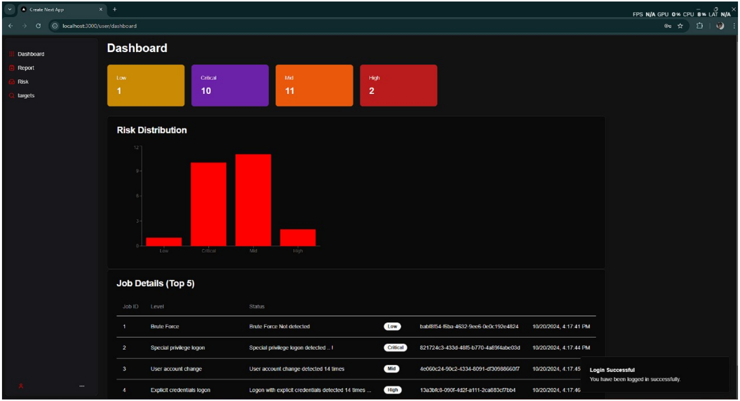
Identify and respond to potential security threats before they become critical issues.

Compliance Management

Stay compliant with industry standards and regulations with our comprehensive reporting tools.

Figure: Home Page

Dashboard



Dashboard

Low	Critical	Mid	High
1	10	11	2

Risk Distribution

Job Details (Top 5)

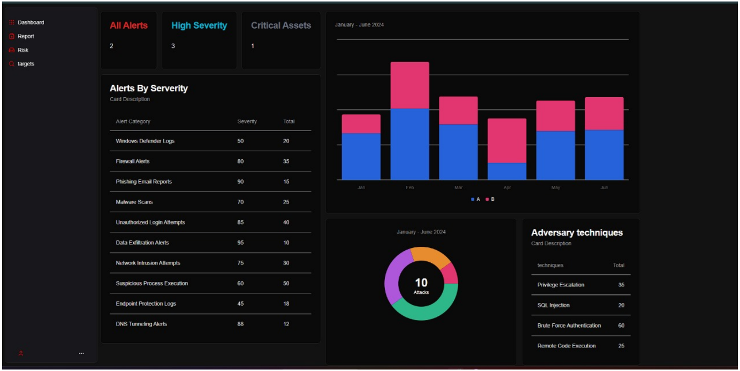
Job ID	Level	Status			
1	Brute Force	Brute Force Not detected	Low	babf8f54-f6ba-4632-9ee6-0e0c192e4824	10/20/2024, 4:17:41 PM
2	Special privilege logon	Special privilege logon detected .. !	Critical	821724c3-433d-48f5-b770-4a89f4abe03d	10/20/2024, 4:17:44 PM
3	User account change	User account change detected 14 times	Mid	4e060c24-90c2-4334-8091-df30988660f7	10/20/2024, 4:17:45
4	Explicit credentials logon	Logon with explicit credentials detected 14 times ...	High	13a3bfc8-090f-4d2f-a111-2ca883cf7bb4	10/20/2024, 4:17:46

Login Successful

You have been logged in successfully.

Figure: Dashboard

Risks Page



All Alerts 2

High Severity 3

Critical Assets 1

Alerts By Serverity

Card Description

Alert Category	Severity	Total
Windows Defender Logs	50	20
Firewall Alerts	80	35
Phishing Email Reports	90	15
Malware Scans	70	25
Unauthorized Login Attempts	85	40
Data Exfiltration Alerts	95	10
Network Intrusion Attempts	75	30
Suspicious Process Execution	60	50
Endpoint Protection Logs	45	18
DNS Tunneling Alerts	88	12

Adversary techniques

Card Description

techniques	Total
Privilege Escalation	35
SQL Injection	20
Brute Force Authentication	60
Remote Code Execution	25

Figure: Risks Page