SOC Log Monitoring & Visualization System

Name: Ahad Shaikh

Seat No: 31011224057

Subject: Software Engineering

Semester: IV

Security Monitoring

Real-time Visibility

Log Analysis

Visualization

Project Overview

A **SOC Log Monitoring & Visualization System** serves as the central nervous system for modern security operations, providing real-time visibility into organizational security posture.

A **centralized security monitoring platform** designed to support daily SOC operations by collecting, processing, and visualizing logs from diverse digital infrastructure components.

- Collects logs from multiple sources
- Normalizes log data for correlation
- Real-time security dashboards
- Advanced search capabilities
- Incident investigation tools
- Historical log storage

System Architecture

Problem Statement

Modern organizations face **increasing cyber threats** with expanding attack surfaces, creating an urgent need for centralized security monitoring.

Current log monitoring environments present significant challenges:

- Log data spread across multiple systems
- Different systems generate logs in different formats
- Manual monitoring is time-consuming and inefficient
- Important warning signs buried in large data volumes
- Delayed detection leads to delayed response
- Lack of visualization makes security posture unclear

Impact of Current Problems

- Missed Alerts
- Slow Investigations
- Inconsistent Security Responses
- Weak Defense
- Poor Compliance

Stakeholders

Identifying **stakeholders** is crucial in software engineering to ensure requirements align with operational needs and create solutions that deliver real value.

SOC Analysts

L1, L2, L3 Levels

Primary users who monitor, analyze, and investigate security events daily

- Real-time Monitoring
- Alert Review
- Log Analysis
- Incident Investigation

SOC Manager

Operations Oversight

Oversees daily operations and team performance

- Performance Metrics
- Compliance

System Admins

Technical Management

Handles configuration, integration, and maintenance

- Configuration
- User Management

IT Security Team

Incident Response

Acts on confirmed incidents to remediate threats

- Remediation
- Defense

Functional Requirements

Functional requirements define what a system must do, serving as the foundation for development and ensuring the final product meets stakeholder needs.

Data Collection & Processing

- Collect logs from multiple sources
- Support different log formats
- Normalize log data into standard format
- Secure centralized storage
- Real-time log ingestion

Visualization

- Interactive dashboards
- Dashboard customization
- Security metrics display

Analysis

- Search and filter logs
- Log correlation
- Time-based analysis
- Event-based analysis

Alerting

- Generate alerts for suspicious patterns
- Add investigation notes
- Incident tagging

Conclusion

Conclusions in software engineering **summarize key findings** and provide stakeholders with a clear understanding of project outcomes and next steps.

- Centralizes log monitoring across diverse infrastructure
- Provides essential visibility for security operations
- Enables efficient incident detection and response
- Serves diverse stakeholder needs across organization

This system forms a solid foundation for strengthening organizational cybersecurity posture and operational resilience

System Impact

Enhanced Security

Strengthened Cybersecurity Posture

Improved Decision Making