Security Monitoring with Graylog SIEM for Catnip Games International

Name: Niloofar Thaha
Course :BSc.Cyber Security
Student ID: THA21540701

Weekly Training Documentation

This document outlines the weekly training sessions for the 'Security Monitoring with Graylog SIEM for Catnip Games International' project. The training program is designed to ensure all team members gain the necessary skills and knowledge to successfully deploy, manage, and optimize the security monitoring infrastructure, using Graylog SIEM, Elasticsearch, and Python automation. The training covers key aspects such as log collection, dashboard creation, automated alerting, incident detection, performance optimization, and reporting, aligning with the industry's best practices for security operations.

Week 1: Introduction to SIEM, Graylog Deployment, and Log Collection

Objective: The training will present basic concepts about SIEM systems together with information about Graylog deployment. Log aggregation combined with collection methods form an important part of the training.

Training Content:

-This section presents an introduction to SIEM fundamentals followed by explanations about its essential role in security operations as well as its role in monitoring security events.

- Graylog Overview: Understanding Graylog as a SIEM platform, its architecture, components (Graylog server, Elasticsearch, MongoDB), and functionality.

-Log Collection involves establishing log collection from Linux game servers and authentication systems and network devices and other devices.

- The normalization process in addition to log structure methods for analytical purposes.

Hands-on Activity:

-The installation of Graylog needs to take place within a testing infrastructure.

- Configure basic log parsing and implement log collection from one Linux server as part of the installation process.

Expected Outcomes:

The participants will master SIEM principles through Graylog deployment and test system log acquisition.

Week 2: Configuring Dashboards and Log Visualization

Objective: Security personnel should acquire skills to design their own dashboards alongside effective log security visualization methods.

Training Content:

- The training includes instructions to develop security dashboards that function real-time in Graylag.

- Security metrics need specialized display techniques which will demonstrate suspicious system behavior while showing network health through visual means.

-The course shows students how to graphically display security data which includes failed login attempts and DDoS indicators and access patterns.

Hands-on Activity:

-The purpose of this activity will guide users through creating custom dashboards that aid in tracking game server health together with security events.

-Parameters for security analysis can be displayed through added widgets within the system.

Expected Outcomes:

- The participants will acquire the ability to construct dashboards which present live security data and performance measurements to users.

Week 3: Implementing Automated Alerts and Correlation Rules

Objective: The user should learn to establish correlation rules and automated alert systems which help detect security threats in real-time.

Training Content:

- Guidelines to design security detection rules present in the section focus on brute-force login attempts and DDoS attacks detection.

-Alerts automatically send to email or Slack when suspicious activities occur after users set up notifications.

-Security incident response experts learn to handle incidents that arise because of alert activations.

Hands-on Activity:

- Users should establish correlation rules which detect brute-force login attacks together with unusual access behavior.
-Windows has a built-in feature for automated system notifications through email or the Slack application.

Expected Outcomes:

-Participation in this course will teach participants how to create correlation rules and establish automatic alerting that detects security incidents.

Week 4: Automating Reports and Ensuring Compliance

Objective: Security reports need automation to generate them and security teams should follow all regulatory requirements.

Training Content:

- Training demonstrates scripting fundamentals by introducing Python scripting which automatically generates week-to-week security reports.

-Security reporting receives an overview of regulatory requirements including GDPR so participants understand their relationship to security reporting.

- The training will instruct you to develop security audit and compliance report templates.

Hands-on Activity:

-The development of a Python script should create an automatic system for weekly security report creation.

- Automation settings should be designed to produce GDPR reports along with other security audit reports.

Expected Outcomes:

- The system will produce security and compliance reports automatically following participant configuration.

Week 5: Performance Optimization and Failover Setup

Objective: The system needs to process required event volumes at high availability standards.

Training Content:

-Graylog performance experts should establish methods which allow the system to process 10,000 events per second with query results delivered in under 5 seconds.#

- The system needs failover procedures which follow best practices to maintain system availability at 99.9% uptime.

-The training covers hot and cold data storage management as well as techniques to avoid data loss.

Hands-on Activity:

- The team will measure how Graylog performs before making adjustments to configuration settings that excel at managing high volumes of collected information.

- The implementation of failover systems will ensure the continuous operation of the system.

Expected Outcomes:

- Participants can achieve performance optimization to establish failover configurations which provide high availability for their Graylog implementation systems.

Week 6: Incident Detection, Testing, and Final Documentation

Objective: Test the complete system, validate performance, and prepare final documentation for project handover.

Training Content:
- Incident Detection and Response: Learn how to use Graylog to detect, analyze, and respond to incidents in real-time.
- Testing and Troubleshooting: Steps for conducting a full system test, troubleshooting common issues, and ensuring the setup meets all requirements.
- Documentation Best Practices: Guidance on writing clear technical documentation and post-deployment support procedures.

Hands-on Activity:
- Simulate security incidents (e.g., brute-force login, DDoS) and verify alerting and response workflows.
- Complete the final documentation, including configuration details, recovery procedures, and system usage guides.

Expected Outcomes:
- Participants will be able to manage incident detection workflows and provide comprehensive documentation for the system.

Ongoing Training & Knowledge Transfer

Objective: Staff members need to improve their security skills consistently while maintaining smooth knowledge transfer between individuals.

Training Content: Employees must maintain continuous learning because security threats together with Graylog updates require regular awareness. After Deployment Assistance Features include classes about inspecting system wellness in addition to infrastructure expansion abilities and threat management methods. Functional teamwork methods should be developed to maintain security operations between different teams.

Expected Outcomes: The training will teach participants to perform post-deployment work while maintaining their professional growth alongside effective teamwork.

Conclusion

By the end of the 6-week training program, all team members will have gained hands-on experience with key security operations tasks, including log collection, dashboard creation, automated alerting, incident response, and performance optimization. This training ensures that the team can effectively deploy, manage, and optimize the SIEM infrastructure for Catnip Games International, providing robust security monitoring for their gaming infrastructure.