Security Monitoring with Graylog SIEM for Catnip Games International

# 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:  
- Introduce the fundamentals of SIEM systems and Graylog deployment.  
- Learn about log aggregation and collection processes.

Training Content:  
- SIEM Overview: Introduction to SIEM concepts, its importance in cybersecurity, and how it aids in detecting and responding to security incidents.  
- Graylog Overview: Understanding Graylog as a SIEM platform, its architecture, components (Graylog server, Elasticsearch, MongoDB), and functionality.  
- Log Collection: Setting up log collection from Linux game servers, authentication systems, and network devices.  
- Log Parsing: Techniques for log normalization and structuring logs for analysis.

Hands-on Activity:  
- Deploy Graylog in a test environment.  
- Set up log collection from a sample Linux server and configure basic log parsing.

Expected Outcomes:  
- Participants will understand SIEM concepts and be able to deploy Graylog and collect logs from test systems.

## Week 2: Configuring Dashboards and Log Visualization

Objective:  
- Learn to create custom dashboards and visualize security logs effectively.

Training Content:  
- Graylog Dashboards: Steps to build real-time security dashboards in Graylog.  
- Data Visualization: Best practices for displaying security metrics, identifying suspicious activities, and visualizing system health.  
- Key Metrics: Learn how to visualize security data like failed login attempts, DDoS indicators, and access patterns.

Hands-on Activity:  
- Create custom dashboards to monitor game server health and security events.  
- Add widgets to display critical metrics for security analysis.

Expected Outcomes:  
- Participants will be able to design interactive dashboards with real-time security insights and metrics.

## Week 3: Implementing Automated Alerts and Correlation Rules

Objective:  
- Understand how to configure correlation rules and automated alerting for real-time threat detection.

Training Content:  
- Correlation Rules: Guide on how to create rules to detect specific security threats like brute-force login attempts or DDoS attacks.  
- Automated Alerts: Setting up email or Slack notifications for automatic alerts on suspicious activities.  
- Incident Response: Introduction to best practices for responding to security incidents triggered by alerts.

Hands-on Activity:  
- Create correlation rules to detect brute-force login attempts and unusual access patterns.  
- Configure automated alerting systems for notifications via email or Slack.

Expected Outcomes:  
- Participants will be able to set up correlation rules and automated alerting to detect and respond to security incidents.

## Week 4: Automating Reports and Ensuring Compliance

Objective:  
- Learn to automate security report generation and ensure compliance with regulatory standards.

Training Content:  
- Automated Report Generation: Introduction to scripting with Python to automate weekly security report generation.  
- Compliance Reporting: Overview of regulatory requirements (e.g., GDPR) and how they relate to security reporting.  
- Report Templates: Learn how to create templates for security audit and compliance reports.

Hands-on Activity:  
- Develop a Python script to automate the generation of weekly security reports.  
- Configure automated compliance reports for GDPR and other security audits.

Expected Outcomes:  
- Participants will be able to automate the creation of security and compliance reports.

## Week 5: Performance Optimization and Failover Setup

Objective:  
- Ensure the system can handle the required event volume and meets high availability standards.

Training Content:  
- Performance Tuning: Methods for tuning Graylog to handle 10,000 events per second and provide sub-5-second query responses.  
- High Availability: Best practices for setting up failover to ensure system availability and meet the 99.9% uptime requirement.  
- Storage Management: Learn about managing storage for hot/cold data and ensuring no data loss.

Hands-on Activity:  
- Benchmark Graylog performance and optimize configurations to handle high volumes of data.  
- Set up failover configurations to guarantee high availability.

Expected Outcomes:  
- Participants will be able to optimize Graylog for performance and set up failover systems to ensure high availability.

## 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:  
- Continuously improve security skills and ensure smooth knowledge transfer.

Training Content:  
- Continuous Learning: Importance of staying updated on new security threats and Graylog updates.  
- Post-Deployment Support: Training on monitoring system health, scaling infrastructure, and addressing new threats.  
- Cross-Team Collaboration: Effective teamwork practices for maintaining security operations.

Expected Outcomes:  
- Participants will be equipped to handle post-deployment tasks, continue learning, and work effectively across teams.

## 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.