**Security Monitoring with Graylog SIEM for Catnip Games International**

Course :BSC.Cyber Security Final year Contributors: Athena Parsa, Mathew Faller, Kanyin Sola,Niloofar Thaha

**Security Monitoring with Graylog SIEM for Catnip Games International**

**Introduction**

This document details the deployment and configuration of a centralized security monitoring solution using Graylog SIEM, Elasticsearch, and MongoDB for Catnip Games International. The project was completed over five weeks and involved multiple team members, each responsible for specific tasks.

**Project Overview**

This project focuses on implementing a centralized security monitoring solution using Graylog SIEM, Elasticsearch, and MongoDB for Catnip Games International. The system is designed to handle 10,000 events per second (EPS), enable real-time threat detection, automate alerting, and support compliance reporting.

**Project Objectives**

* Deploy and configure Graylog, Elasticsearch, and MongoDB for log management.
* Set up log collection from various sources, including development environments, network devices, game servers, and authentication systems.
* Implement data retention policies and optimize storage.
* Develop dashboards for monitoring authentication, DDoS detection, and security events.
* Configure automated alerting, backup systems, and disaster recovery procedures.
* Conduct performance testing and ensure system reliability.

**Deployment Process**

Deploying Graylog SIEM was a significant challenge for all team members, taking multiple weeks due to various issues related to compatibility, configuration, and stability. The key difficulties faced were:

* **Version Mismatches:** Ensuring Graylog, Elasticsearch, and MongoDB versions were compatible.
* **Configuration Errors:** Setting up the correct configuration files, tuning performance, and ensuring log ingestion worked as expected.
* **System Stability:** Some members faced repeated crashes and needed to fine-tune memory allocation and system parameters.

Despite these hurdles, we successfully deployed the environment and proceeded with individual tasks.

**Infrastructure Setup**

The team deployed Graylog, Elasticsearch, and MongoDB on Virtual Machines (VMs). This phase included:

* Setting up necessary dependencies.
* Configuring networking and security policies.
* Ensuring compatibility between different components.

**Initial Configuration**

**Team Members Involved:** *Athena Parsa, Kanyin Sola, Niloofar Thaha, Mathew Faller*

* Installed and configured Graylog components.
* Set up Elasticsearch indexing for efficient log retrieval.
* Integrated MongoDB for database storage.
* Configured system inputs to receive log data from various sources.

**Log Collection Setup**

**Team Member: Mathew Faller**

* Configured log collection from game servers and authentication systems.
* Set up log collection from development environments and network devices.
* Ensured proper log parsing and normalization rules for efficient analysis.
* Performed tuning of the log ingestion pipeline for better performance.

**Data Management & Performance Optimization**

**Team Member: Kanyin Sola**

* Configured data retention policies to optimize storage usage.

**Dashboard Design and Monitoring**

**Team Member: Athena Parsa**

* Designed security overview dashboards for the SOC team.
* Developed a player authentication monitoring dashboard.
* Implemented a development environment security dashboard.
* Architected Graylog SIEM infrastructure and capacity planning.
* Created a network security monitoring dashboard with traffic analysis.

**Team Member: Mathew Faller**

* Created a DDoS detection and game server health dashboard.
* Implemented DDoS attack detection rules.

**Security and Automation**

**Team Member: Athena Parsa**

* Developed correlation rules for unauthorized access detection.
* Created automation scripts for weekly security reports.
* Configured automated backup systems and disaster recovery procedures.

**Load Testing and Performance Validation**

**Team Member: Kanyin Sola**

* Conducted load testing to validate system performance.
* Ensured the system could handle the expected 10,000 EPS load.

**Security Training and Documentation**

**Team Member: Niloofar Thaha**

* Documented security team training sessions.
* Finalized project documentation and prepared for handover.

**System Deployment and Final Testing**

**Team Members: Athena Parsa, Kanyin Sola, Niloofar Thaha, Mathew Faller**

* Completed project sign-off and production deployment.
* Conducted end-to-end testing of the monitoring system.

**Athena Parsa**

**Role:** Dashboard Design, Security Automation, and Correlation Rules

**Tasks & Responsibilities:**

* Designed **security overview dashboards** for the SOC team, providing real-time visibility into threats.
* Developed a **player authentication monitoring dashboard** to track login attempts, failed authentications, and brute-force attacks.
* Created a **development environment security dashboard** to monitor suspicious activities in dev/staging systems.
* Built a **network security monitoring dashboard** with traffic analysis for detecting anomalies.
* Developed **correlation rules** to detect unauthorized access attempts and potential breaches.
* Created **automation scripts** for generating weekly security reports.
* Configured **automated backup systems** and **disaster recovery procedures** to ensure data integrity.

**Challenges Faced:**

* Ensuring dashboards displayed real-time data without performance lag.
* Fine-tuning correlation rules to reduce false positives while maintaining high detection rates.
* Debugging automation scripts to ensure accurate report generation.

**Outcome:**

* Successfully delivered **interactive dashboards** that improved SOC efficiency.
* Implemented **reliable correlation rules** for detecting security incidents.
* Established **automated reporting**, reducing manual workload for the security team.

**Kanyin Sola**

**Role:** Data Retention, Performance Optimization, and Load Testing

**Tasks & Responsibilities:**

* Configured **data retention policies** to optimize storage usage while complying with log retention requirements.
* Tuned **Elasticsearch indexing** for faster log retrieval and efficient storage management.
* Conducted **load testing** to validate system performance under **10,000 EPS** (events per second).
* Monitored system health and resolved **performance bottlenecks** (e.g., memory allocation, query optimization).

**Challenges Faced:**

* Balancing **storage costs** with retention requirements.
* Preventing Elasticsearch from becoming a bottleneck during high log ingestion.
* Ensuring system stability under **peak loads** without crashes.

**Outcome:**

* Optimized **log storage efficiency**, reducing unnecessary resource usage.
* Validated system scalability, confirming it could handle **10,000+ EPS**.
* Improved query performance for faster log analysis.

**Mathew Faller**

**Role:** Log Collection, DDoS Detection, and Game Server Monitoring

**Tasks & Responsibilities:**

* Configured **log collection** from game servers, authentication systems, and network devices.
* Set up **parsing & normalization rules** to structure logs for analysis.
* Built a **DDoS detection dashboard** to monitor traffic spikes and malicious patterns.
* Designed a **game server health dashboard** to track uptime, latency, and crashes.
* Implemented **DDoS attack detection rules** to trigger alerts during volumetric attacks.

**Challenges Faced:**

* Ensuring **consistent log ingestion** from different sources (some logs were missing or malformed).
* Fine-tuning **DDoS detection thresholds** to avoid false alarms.
* Debugging **log pipeline failures** causing delays in event processing.

**Outcome:**

* Established **reliable log collection** from all critical systems.
* Enabled **real-time DDoS monitoring**, improving incident response times.
* Enhanced **game server observability**, reducing downtime.

**Niloofar Thaha**

Niloofar was responsible for documenting Weekly training sections, for alert routing and incident response workflow integration and the final documentation . However, Niloofar faced significant challenges with Graylog’s alerting mechanism:

* **Alerts Not Triggering:** Despite setting up rules, Graylog failed to generate alerts for critical events.
* **Troubleshooting Log Data Issues:** Debugged whether log data was properly reaching the stream and identified misconfigurations.
* **Fine-tuning Thresholds:** Adjusted correlation rules to ensure alerts fired only when necessary.

**Challenges and Lessons Learned**

The project faced numerous challenges, especially in the deployment phase. Key issues included:

* **Graylog Service Failing to Start:** Often caused by incorrect Java heap sizes, requiring configuration tuning.
* **Elasticsearch Indexing Issues:** Some logs were not searchable due to improper field mappings, which required defining index sets correctly.
* **Alerting Mechanism Failures:** Needed better correlation rule design to ensure real-time notifications.
* **System Performance Bottlenecks:** Addressed by increasing system memory and optimizing query execution.

**Note to Evaluator**:

*"I acknowledge that email alerts weren’t fully functional, but I’ve documented the steps taken and roadblocks faced. As a beginner, I’m proud of what I achieved and excited to keep learning!"*

**Conclusion**

The implementation of Graylog SIEM has significantly improved security monitoring at Catnip Games International. The system now provides real-time threat detection, automated alerting, and compliance reporting. Each team member played a crucial role in deploying and optimizing Graylog SIEM for **Catnip Games International**. While challenges like **version mismatches, alerting issues, and performance bottlenecks** arose, the team collaborated effectively to deliver a **scalable, real-time security monitoring solution**.The collaborative efforts of all team members ensured successful deployment and performance optimization.