Project Proposal: Creating SIEM (Security information and event management)

Done by: **D.James Chrishan - AS0509**

Project Title:

Building a Security Monitoring Lab with Elastic SIEM and Kali Linux

Executive Summary:

This project aims to create a hands-on security monitoring lab utilizing Elastic SIEM and a Kali Linux virtual machine (VM). The objective is to demonstrate the integration of Elastic SIEM for real-time monitoring, threat detection, and security event visualization using data forwarded from a Kali VM. By setting up this lab, the project provides a cost-effective, practical environment to enhance cybersecurity skills, enabling effective detection and response to security incidents.

Background and Rationale:

Effective security monitoring is essential for identifying and responding to cyber threats. Elastic SIEM is a robust platform that provides real-time security insights, but its potential is best realized through hands-on practice. Setting up a lab environment with Elastic SIEM and Kali Linux offers cybersecurity professionals a controlled space to simulate threats and gain proficiency in monitoring, analysis, and response. This project addresses the lack of accessible training labs for aspiring security analysts and emphasizes practical learning through simulated attacks and log analysis.

Objectives:

1. **Set up and configure Elastic SIEM** for security monitoring with a free trial Elastic Cloud account.
2. **Deploy and configure a Kali Linux VM** for log forwarding and threat simulation.

3. **Integrate Elastic Agent** to collect and forward security events from the VM to the SIEM.
4. **Simulate security events** using tools like Nmap to generate meaningful data for analysis.
5. **Create dashboards and alerts** in Elastic SIEM to visualize and monitor security incidents.
6. Provide a step-by-step guide for replication, enabling scalability of the lab for broader use.

SMART Objective:

1. **Specific:** Configure Elastic SIEM on a free trial Elastic Cloud account for real-time security monitoring and event analysis.
2. **Measurable:** Successfully deploy Elastic Agent on a Kali Linux VM to forward logs and validate data ingestion with at least three simulated security events.
3. **Achievable:** Utilize free tools such as Elastic Cloud, VirtualBox, and Kali Linux, following detailed configuration guides.
4. **Relevant:** Develop practical skills for cybersecurity professionals by setting up a replicable security monitoring lab.
5. **Time-bound:** Complete the setup, integration, and testing within two weeks from the start of the project.

Objective Summary:
"Implement Elastic SIEM on Elastic Cloud, configure a Kali Linux VM for log forwarding, and simulate three unique security events within two weeks to demonstrate seamless integration and monitoring capabilities."

SMART Research:

1. **Specific:** Study the impact of simulated attack scenarios (e.g., Nmap scans) on the ability of security professionals to detect and analyze threats.
2. **Measurable:** Assess improvement in security event analysis accuracy by comparing pre- and post-setup performance across five test scenarios.
3. **Achievable:** Use simulated attacks and Elastic SIEM dashboards to generate data and conduct analysis.

4. **Relevant:** Contribute to scalable, practical training methodologies for cybersecurity professionals.
5. **Time-bound:** Complete the research and compile findings within four weeks.

Research Summary:
"Evaluate the impact of simulated Nmap scans on security incident analysis accuracy and response times using Elastic SIEM within four weeks, aiming to quantify skill enhancements."

Scope:

Included:

- Setting up Elastic SIEM on Elastic Cloud.
- Installing and configuring Kali Linux as a VM.
- Generating and analyzing security events.
- Creating dashboards and alerts for monitoring.

Excluded:

- Integration with external log sources such as Windows or cloud platforms.
- Advanced customizations of Elastic SIEM features.

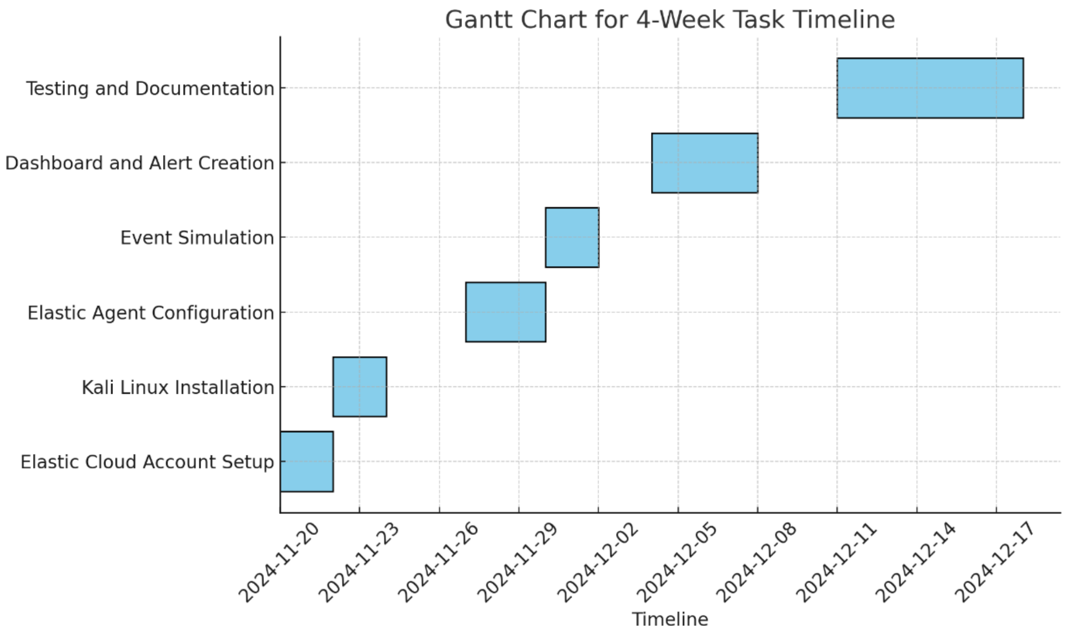
Methodology:

1. **Setup Phase:**
    - Register for Elastic Cloud and deploy an Elasticsearch instance.
    - Download and install Kali Linux on VirtualBox or VMware.
2. **Integration Phase:**
    - Install Elastic Agent on Kali VM and configure it to forward logs to the SIEM.
    - Verify successful data ingestion using basic log queries in Elastic SIEM.
3. **Event Generation:**
    - Simulate attacks using Nmap and analyze the logs in Elastic SIEM.

4. **Data Visualization:**
    - Create a dashboard to track security event trends.
5. **Alert Creation:**
    - Configure alerts for specific security incidents, such as Nmap scans.

Timeline:

Task name	**Start Date**	**Duration**
Elastic Cloud Account Setup	2024-11-20	2
Kali Linux Installation	2024-11-22	2
Elastic Agent Configuration	2024-11-27	3
Event Simulation	2024-11-30	2
Dashboard and Alert Creation	2024-12-04	4
Testing and Documentation	2024-12-11	7



Resources and Budget:

- **Hardware:** Laptop or PC with sufficient processing power and RAM (Existing resource).
- **Software:**
  - Elastic Cloud (Free Trial).
  - VirtualBox or VMware (Free).
  - Kali Linux VM (Free).
- **Personnel:** Cybersecurity Students (self-directed).
- **Budget:** $0 (leveraging free tools and platforms).

Risk Management:

1. **Risk:** Internet connectivity issues during Elastic Agent installation.
   - **Mitigation:** Verify connection with ping and use a stable network.

2. **Risk:** Delayed log ingestion in SIEM.
    - **Mitigation:** Allow sufficient time for data to populate; validate configurations.
3. **Risk:** Errors in agent configuration.
    - **Mitigation:** Re-run installation commands and cross-reference Elastic documentation.

Stakeholder Analysis:

- **Primary Stakeholder:** Security professionals and analysts seeking hands-on experience.
- **Secondary Stakeholder:** Organizations leveraging Elastic SIEM for threat detection and monitoring.
- **Engagement Plan:** Provide step-by-step documentation to ensure accessibility and usability.

Expected Outcomes and Impact:

- **Outcomes:** A fully operational security lab with Elastic SIEM monitoring simulated events.
- **Impact:** Enhanced practical skills in using Elastic SIEM for security monitoring, benefiting cybersecurity professionals and organizations.

Conclusion:

This project provides a practical, cost-effective solution for learning and practicing security monitoring with Elastic SIEM. By simulating real-world scenarios, it equips participants with the skills needed to detect, analyze, and respond to security threats effectively. The setup is scalable, enabling others to replicate and benefit from the lab environment, fostering broader adoption and skill development in the cybersecurity field.

References:

1. Elastic Security Deployment Guide.
   Elastic. (n.d.). *Elastic Security setup for monitoring threats*. Retrieved November 18, 2024, from https://www.elastic.co/guide/en/security
2. Kali Linux VM Installation guide.
   Offensive Security. (n.d.). *Kali Linux installation*. Kali Linux. Retrieved November 25, 2024, from https://www.kali.org/docs/installation/
3. Nmap guide
   Station X. (n.d.). *Nmap cheat sheet*. Station X. Retrieved November 25, 2024, from https://www.stationx.net/nmap-cheat-sheet/