HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

PROJECT 3

Implementing a SIEM System with the ELK Stack: Log Monitoring and Management

Student: Vũ Ngọc Quyền

Student ID: 20214971

Supervisor: Nguyễn Đức Toàn

School: Information and Communications Technology

HANOI, 2024

TABLE OF CONTENTS

1 Objective and Scope

Objective: The primary objective of this project is to design and implement a Security Information and Event Management (SIEM) system using the ELK Stack. The SIEM system should be capable of centralizing log data from various sources, analyzing security events, and providing actionable insights to detect and respond to potential security incidents. Another key objective is to integrate the MITRE ATT&CK framework to align threat detection capabilities with real-world adversary techniques.

Scope: The scope of this project covers the deployment and configuration of the ELK Stack (Elasticsearch, Logstash, and Kibana) for collecting and analyzing log data from Windows and Linux systems.

2 ELK stack

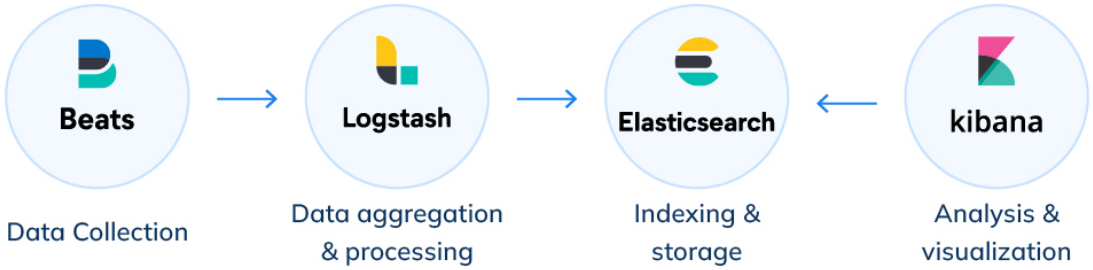

Fig. 1. ELK stack

The ELK Stack is an open-source suite of tools designed for real-time log management and analytics. It consists of three main components: Elasticsearch, Logstash, and Kibana, which work together to collect, store, and visualize data.

2.1 Elasticsearch

Elasticsearch is a RESTful distributed search engine. It basically provides distributed search capabilities via API and stores data in a NoSQL database. Elasticsearch allows you to perform and combine many types of searches: structured, unstructured, geo, and metric in the way you want.

It stores, indexes, and makes log data searchable in near real-time, providing scalability and efficient querying for large volumes of data in a SIEM system.

2.2 Logstash

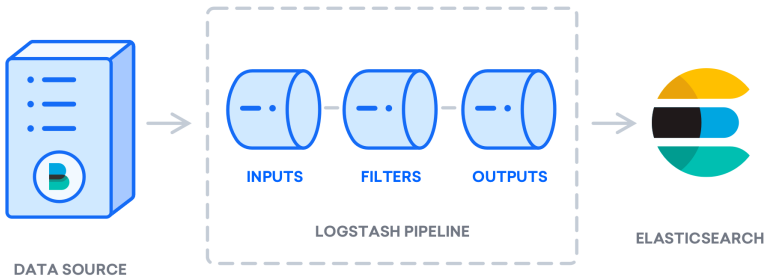

Fig. 2. Logstash Pipeline

Logstash collects and processes log data from multiple sources. It filters, enriches, and formats data before sending it to Elasticsearch for indexing, handling both structured and unstructured logs for security analysis.

2.3 Kibana

Kibana offers data visualization for the ELK Stack. It allows users to analyze and visualize log data through customizable dashboards, helping security teams track key metrics, detect anomalies, and respond to threats in real time.

2.4 Beats

The ELK Stack uses lightweight agents, known as Beats, to facilitate log collection from many systems. Beats are specialized data shippers that send logs and metrics to Logstash or Elasticsearch. Among the most commonly used Beats in a SIEM setup are Auditbeat, Filebeat, and Winlogbeat, each serving a unique role in collecting security-relevant data.

Auditbeat: Monitors Linux systems, capturing security-related events like file access and user activities. It's used to track system changes and suspicious behaviors through the Linux Audit framework.

Filebeat: Collects logs from various sources, such as system files and network devices, across Linux and Windows. It forwards this log data to Logstash or Elasticsearch for analysis, simplifying log collection and ensuring centralized storage.

Winlogbeat: Winlogbeat collects logs from Windows Event Logs, covering security events, application events, and system logs. One of its key features is its ability to integrate with Sysmon (System Monitor), a Windows system service that provides detailed information about process creation, network connections, file modifications, and other system activities.

3 MITRE ATT&CK Overview

The MITRE ATT&CK framework is a knowledge base of adversary tactics and techniques based on real-world observations of cyberattacks. It categorizes and organizes the various methods attackers use during different phases of a cyber intrusion, from initial access to execution, persistence, and data exfiltration.

3.1 Integrating MITRE ATT&CK

Incorporating MITRE ATT&CK into the ELK Stack allows for a more structured approach to threat detection. By mapping log events to ATT&CK techniques, analysts can correlate data with known attacker behavior patterns. For instance, specific log entries may indicate the use of a particular ATT&CK technique, such as a brute force attack or malware execution, allowing the SIEM system to trigger alerts based on real-world attack scenarios.

3.2 Benefits of Using MITRE ATT&CK

- Understanding threat: ATT&CK helps analysts understand the tactics behind detected events, making threat analysis more precise.
- Structured detection use cases: Analysts can design detection rules and alerts based on specific ATT&CK techniques, leading to more effective monitoring.
- Enhanced threat hunting capabilities: Security teams can use the ATT&CK framework as a reference when conducting proactive threat hunting activities.

By leveraging MITRE ATT&CK within the ELK Stack SIEM system, organizations gain deeper insights into the tactics and techniques employed by adversaries, improving their overall security posture.

4 System Architecture

Machine Type	Operation System	Installed Tools
Elasticsearch Server	Ubuntu Server 22.04	ElasticSearch, Kibana, Logstash
Log collector from Linux	Kali Linux	Filebeat, Syslog, Auditbeat
Log collector from Windows	Windows Server or Windows 10	Sysmon, Winlogbeat

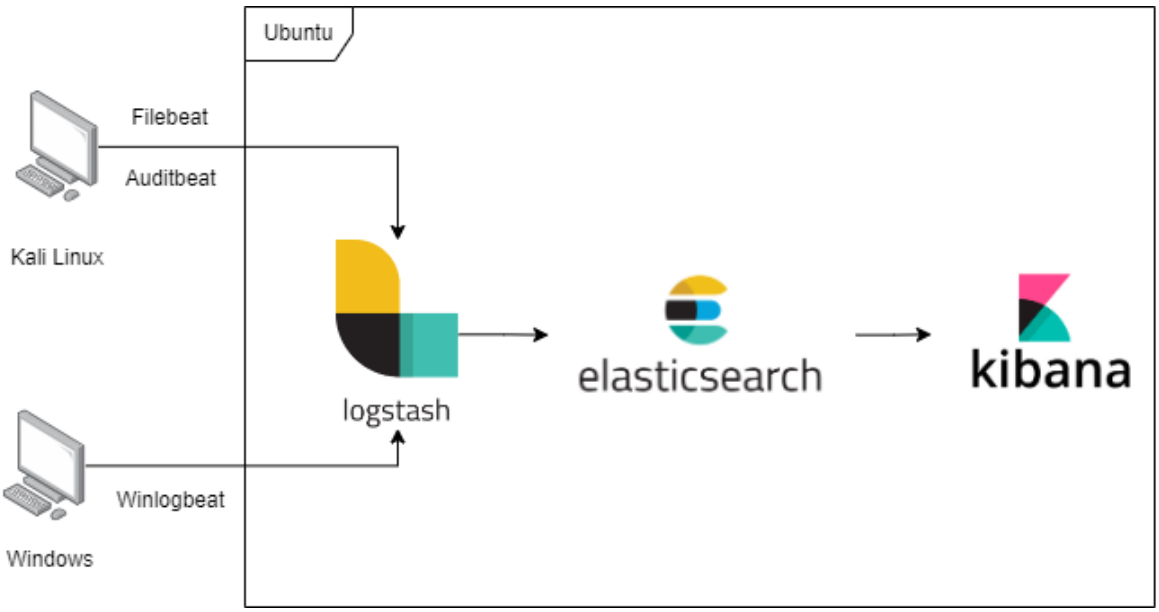

Fig. 3. System Architecture

5 Creating Alert Rules in a SIEM System

Establishing alert rules is essential for effective threat detection in a SIEM system. Here's a concise overview of the process, including testing with Atomic Red Team and Metasploit.

5.1 Identify Use Cases

Determine specific security scenarios to monitor, such as unauthorized access or unusual activity.

5.2 Define Alert Criteria

Set parameters that trigger alerts, including:

- Event Types: Specify relevant log types (e.g., login events).
- Thresholds: Define limits (e.g., more than five failed logins).
- Conditions: Outline when alerts should activate (e.g., logins from unknown IPs).

5.3 Implement Rules in the SIEM

Create rules using the SIEM's features, ensuring proper formatting to minimize false positives.

5.4 Test and Refine Rules

Use Atomic Red Team and Metasploit to simulate attacks and generate relevant logs. Monitor the results and refine rules as needed.

5.5 Monitor and Adjust

Continuously review alerts and adjust rules to adapt to changing threats and organizational needs

6 Demo

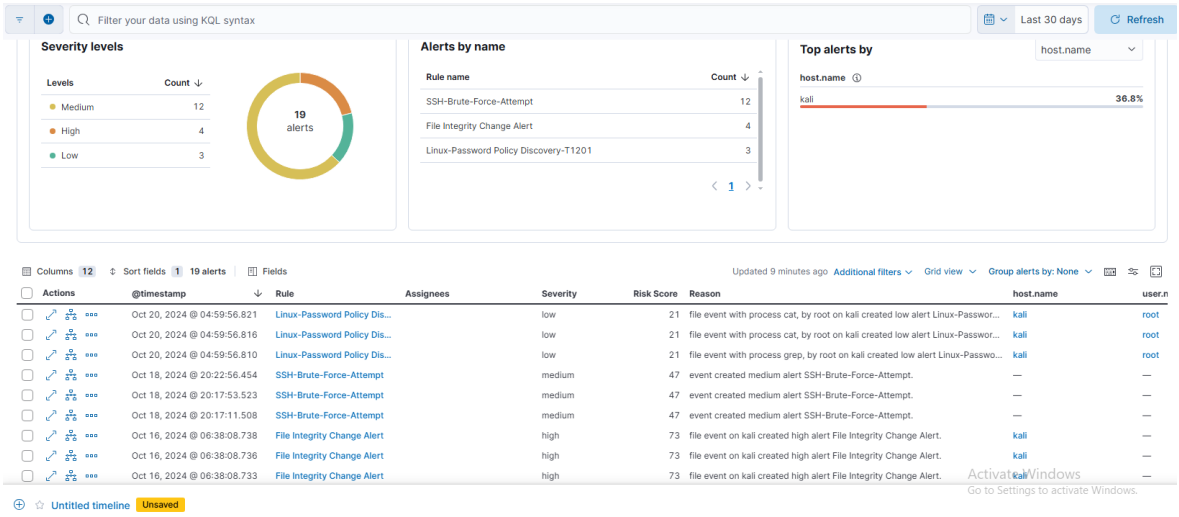

Fig. 4. Alert demo illustrating three rules applied to a Linux system.

- Linux - Password Policy Discovery - T1201:

  This rule detects attempts to gather information about password policies on Linux systems. Activities may include querying configuration files or using commands to check password rules.

- Linux - SSH Brute Force Attempt:

  This rule alerts on brute force attack attempts via the SSH protocol, where an attacker tries to gain access by testing multiple passwords in a short period.

- Linux - File Integrity Change Alert:

  This rule detects changes to system or application files. Monitoring file integrity helps identify unusual activities, such as attacks or intrusions on the system.