SOC Fundamentals and Operations

1. Log Management Fundamentals

Introduction

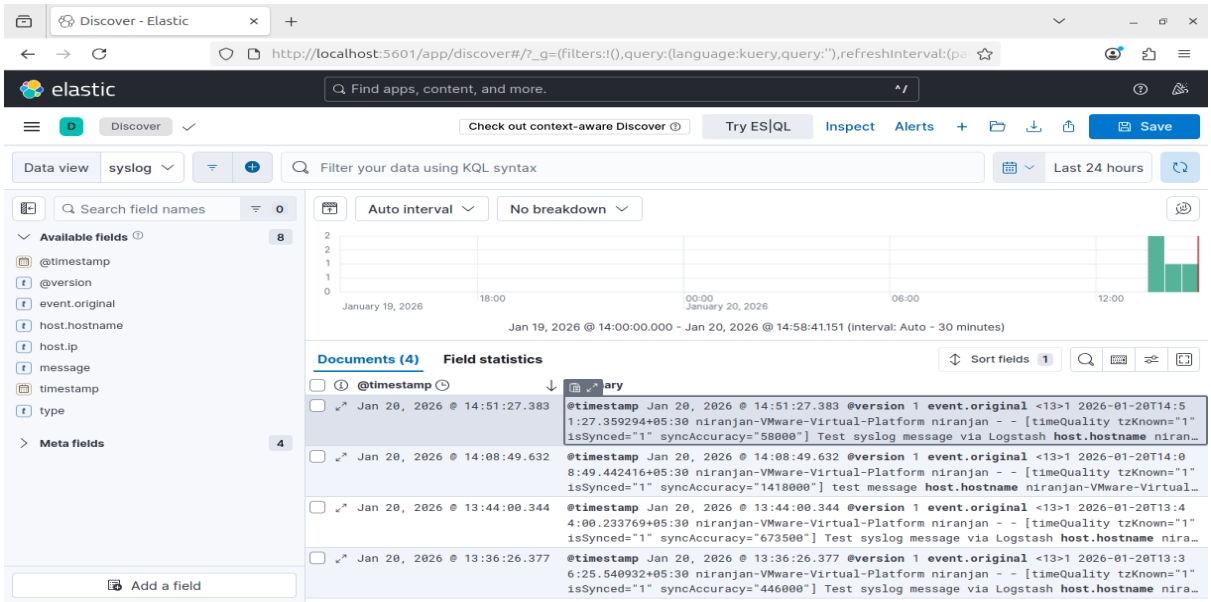
Log Management Fundamentals is the practice of collecting, standardizing, storing, and analysing logs from systems and applications to support security monitoring and troubleshooting. Logs such as Windows Event Logs, Syslog, and HTTP logs are collected using tools like Fluentd or Logstash, normalized into formats like JSON, and analyzed using query languages such as KQL to detect issues and security threats.

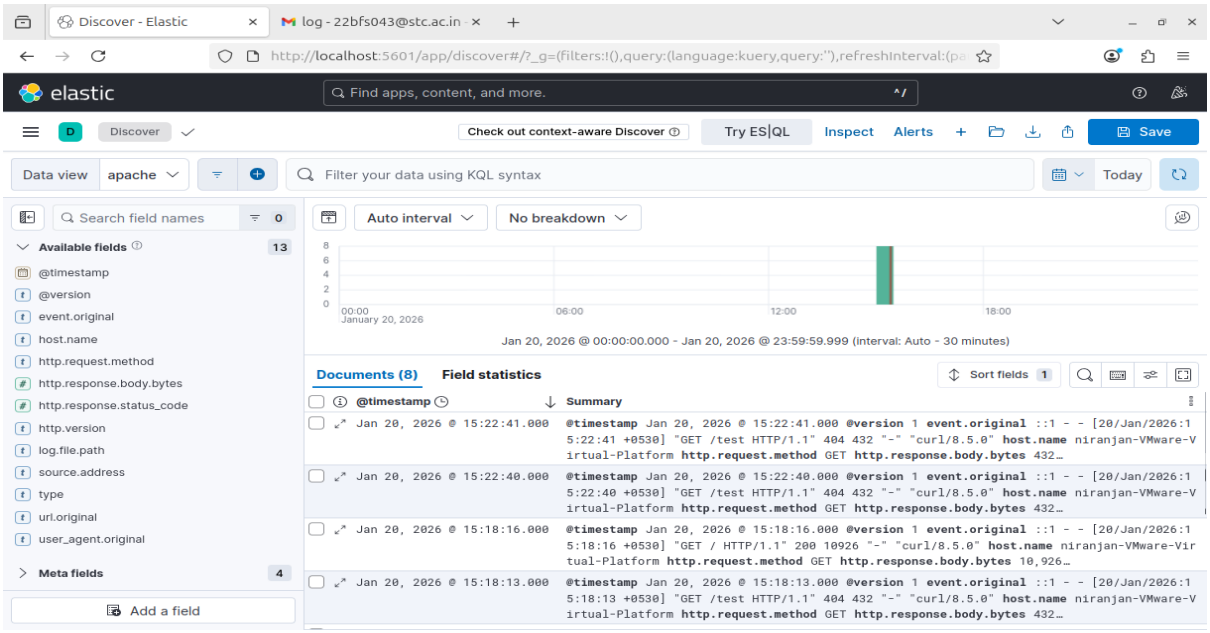
Methodology

- Collect Logs:- Install Logstash and Configure them to forward logs to the SIEM.
- Test by generating logs with logger"Text Message"
- Use a KQL query to find Event ID 4625 (failed logins)
- Use Logstash to convert an Apache access log to JSON. Save output to a file and check the format

Result

Successfully generated logs with logger"Text Message" , KQL Query Practice and converted an Apache access log to JSON





2. Security Tools Overview

Introduction

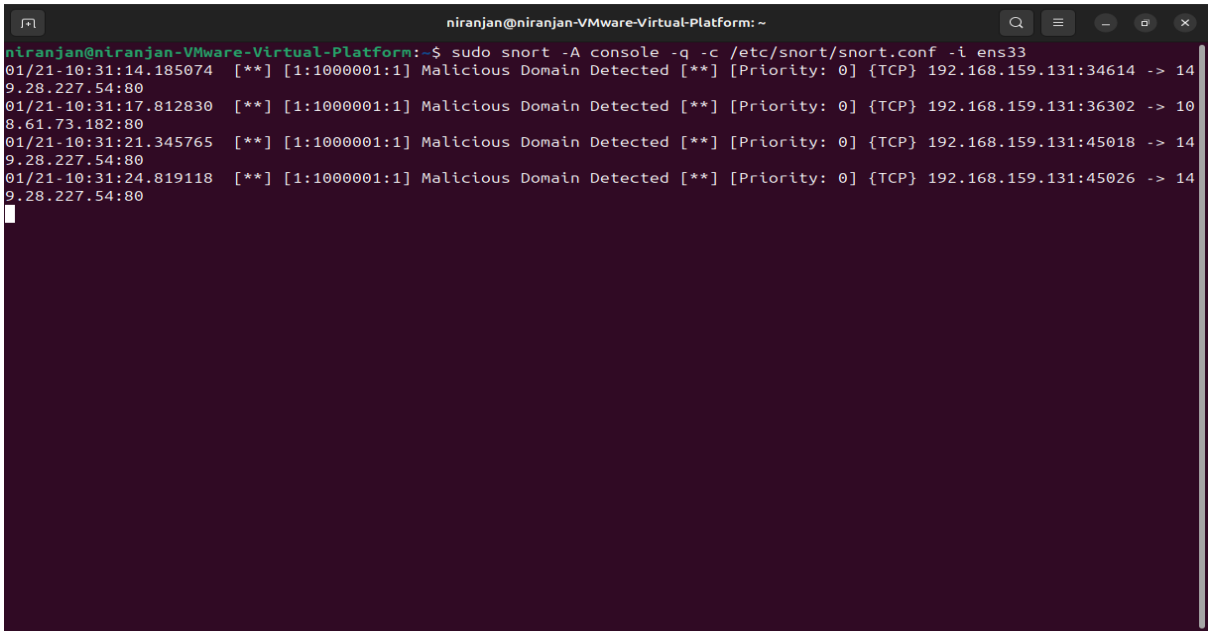
Security tools are essential for detecting, analyzing, and responding to cyber threats in a SOC environment. SIEM platforms (Splunk, QRadar) collect and correlate logs for centralized monitoring. EDR solutions (CrowdStrike) provide endpoint-level visibility to detect malicious activity. IDS/IPS tools like Snort monitor network traffic to detect or block attacks, while vulnerability scanners such as Nessus identify security weaknesses in systems before attackers can exploit them.

Methodology

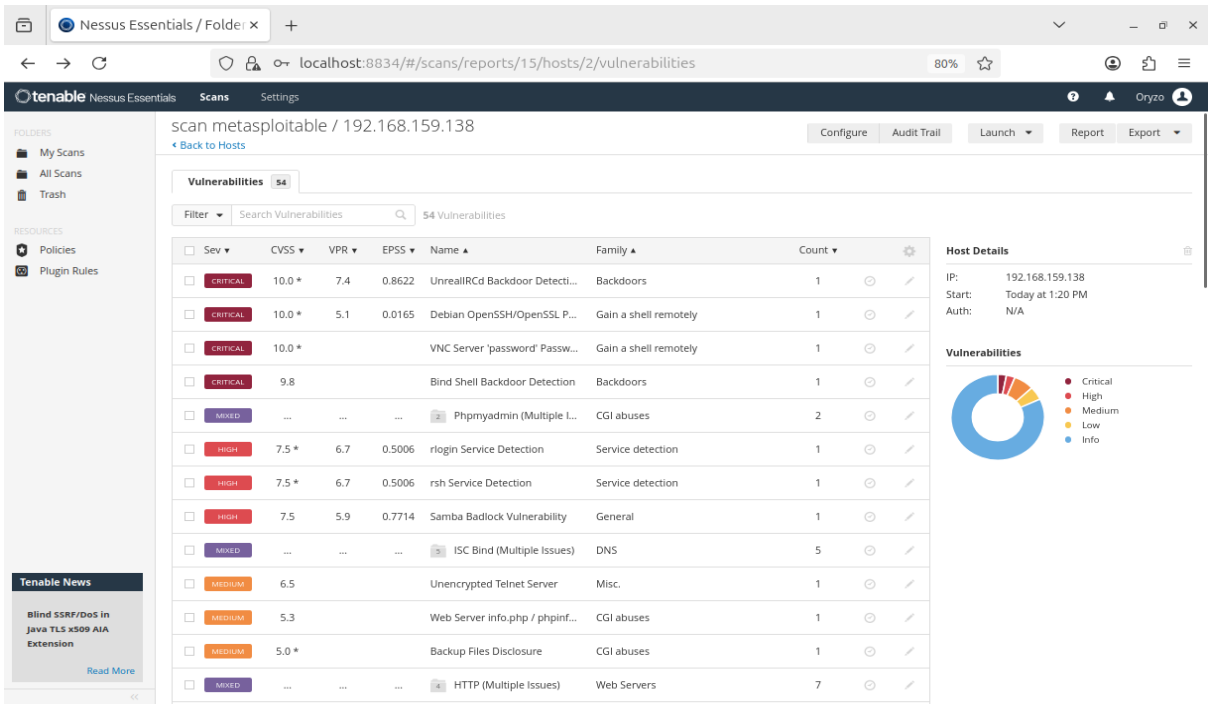
- Install snort and Write a rule to detect HTTP requests to "malicious.com"
- Rule used “alert tcp any any -> any 80 (msg:"Malicious Domain"; content:"malicious.com"; http_uri; sid:1000001;)”
- Test the rule using curl http://malicious.com
- Install Nessus Essentials on Ubuntu to scan vulnerabilities of Metasploitable2.
- Export the report and list the top 3 vulnerabilities by CVSS score.
- Install Osquery on Windows VM
- Query the list of running processes using SELECT * FROM processes; and simulate malicious activity by executing a harmless batch file to observe and analyze its process behavior.

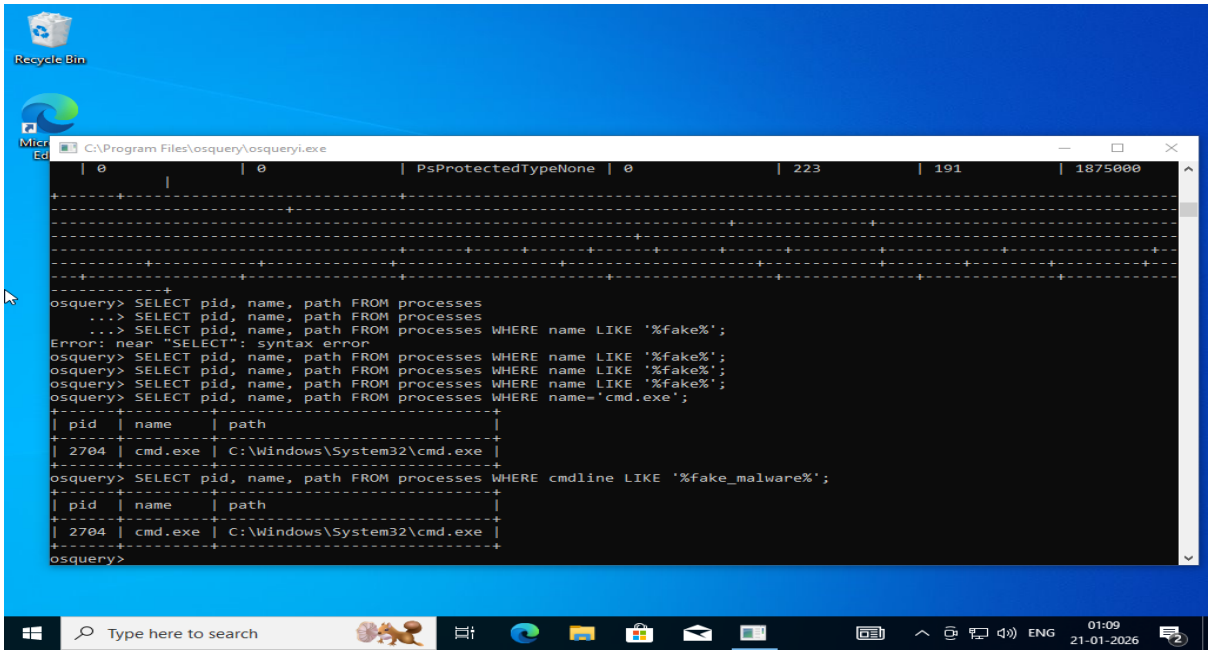
Result

Successfully detect HTTP requests to "malicious.com".



Reported the top 3 vulnerabilities by CVSS score.





3. Log Analysis

Introduction

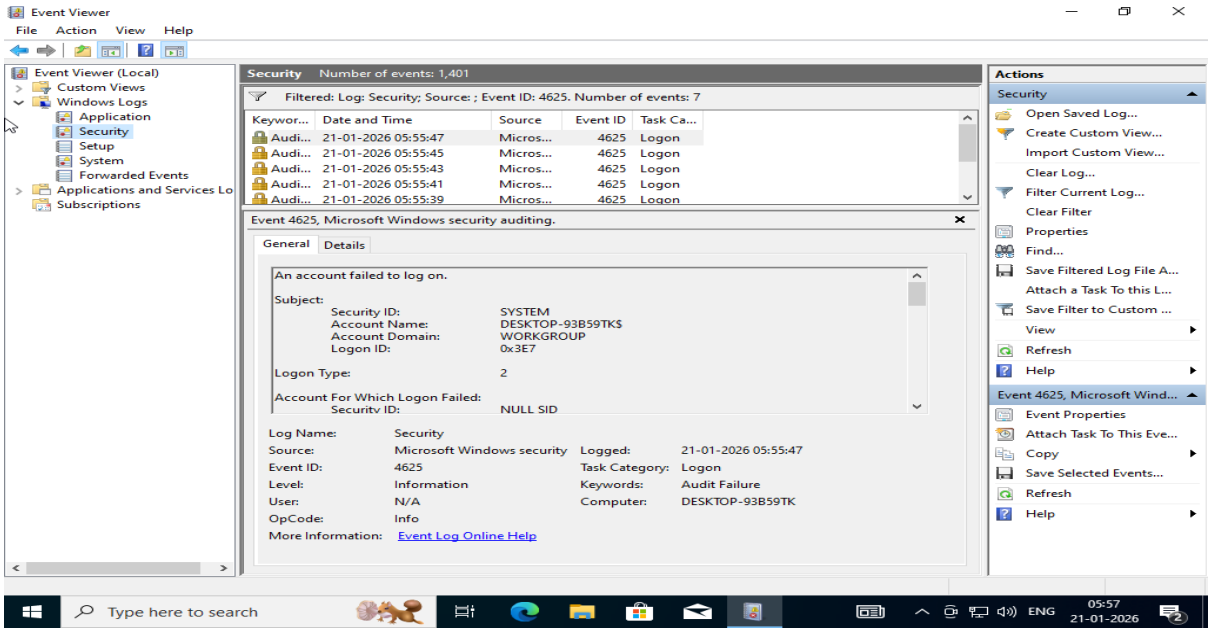
Log analysis involves examining system and application logs to detect suspicious activities and security incidents. By analyzing Windows Event Logs (such as failed logins and service creation events), analysts can identify threats like brute-force attacks. Browser history analysis helps uncover malicious or suspicious web activity by reviewing visited URLs. Using built-in tools like Windows Event Viewer and advanced third-party tools such as Eric Zimmerman's forensic utilities and SIEM platforms, analysts gain hands-on experience in detecting, validating, and documenting security events in a real-world SOC workflow.

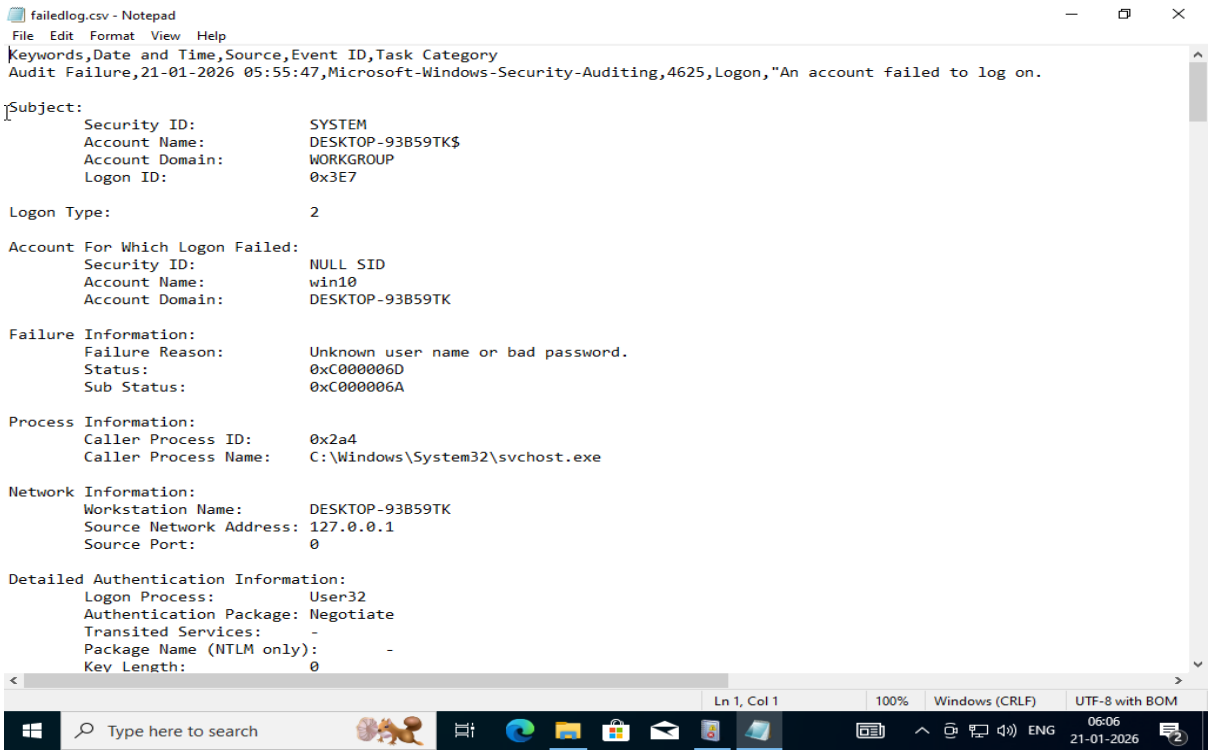
Methodology

- Event Generation :- Simulate security events by performing multiple failed login attempts and basic system changes.
- Open **Windows Event Viewer** and Filter **Security logs** for Event ID **4625** (failed login)
- Export filtered event logs to **CSV** using Event Viewer.
- Locate Chrome history files from the user profile on the VM.
- Use **Eric Zimmerman's tools (LECmd)** to parse browser history and extract visited URLs.
- Review parsed results to identify suspicious or test URLs (e.g., http://test.com).

Result

Successfully export filtered event logs to **CSV** using Event Viewer.





Document Security Events

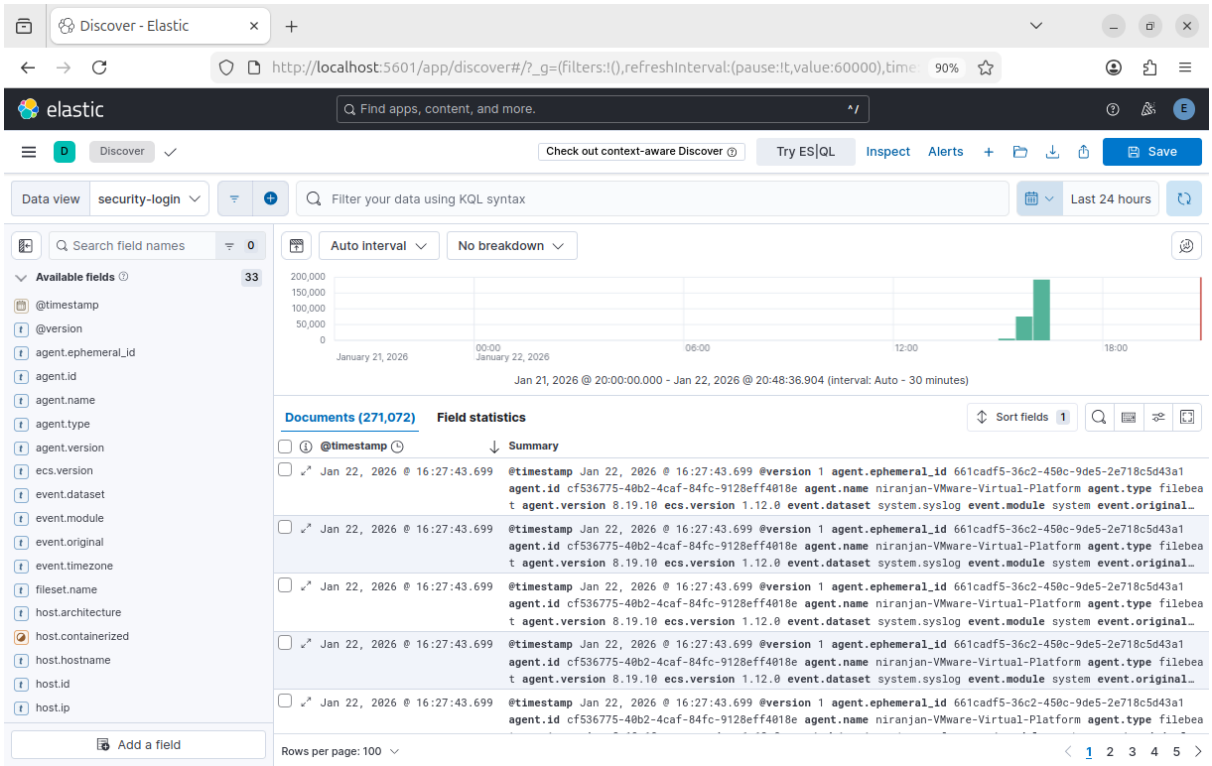
Introduction

Security event documentation is a critical SOC activity used to record, analyze, and respond to suspicious or malicious activities detected through monitoring tools such as Elastic SIEM. Proper documentation helps analysts track incidents, identify attack patterns, support incident response, and maintain an audit trail for future investigation and compliance.

Event Documentation

Login Activity Log (Mock Documentation)

- Date/Time: Jan 22, 2026 @ 16:27:43
- Source IP:192.168.159.133
- Event ID: System login event (Security Login dataset)
- Description: Login-related events collected from a ubuntu system and ingested into Elastic SIEM via Filebeat. Multiple login records observed within a short time frame, indicating potential authentication activity monitoring.
- Action Taken: Event reviewed and documented for baseline analysis. No immediate threat identified. Logs retained for further correlation and alert rule testing.



4. Set Up Monitoring Dashboards

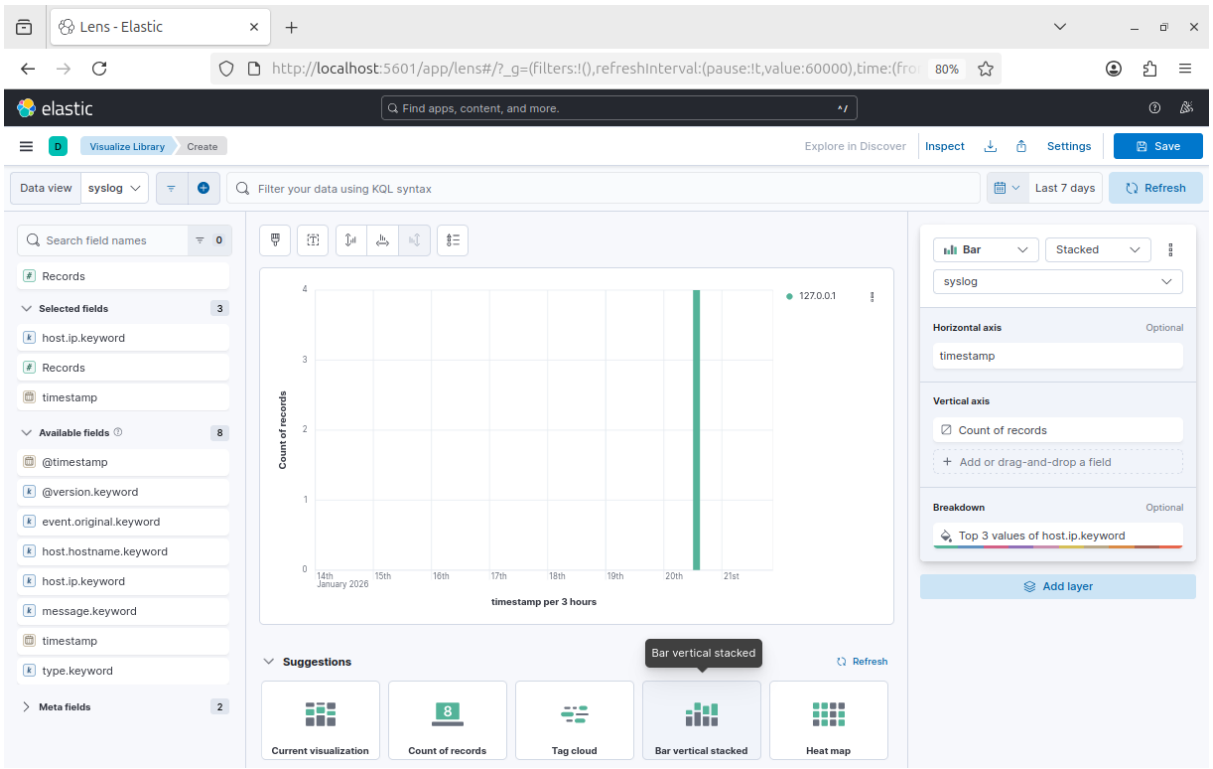
Introduction

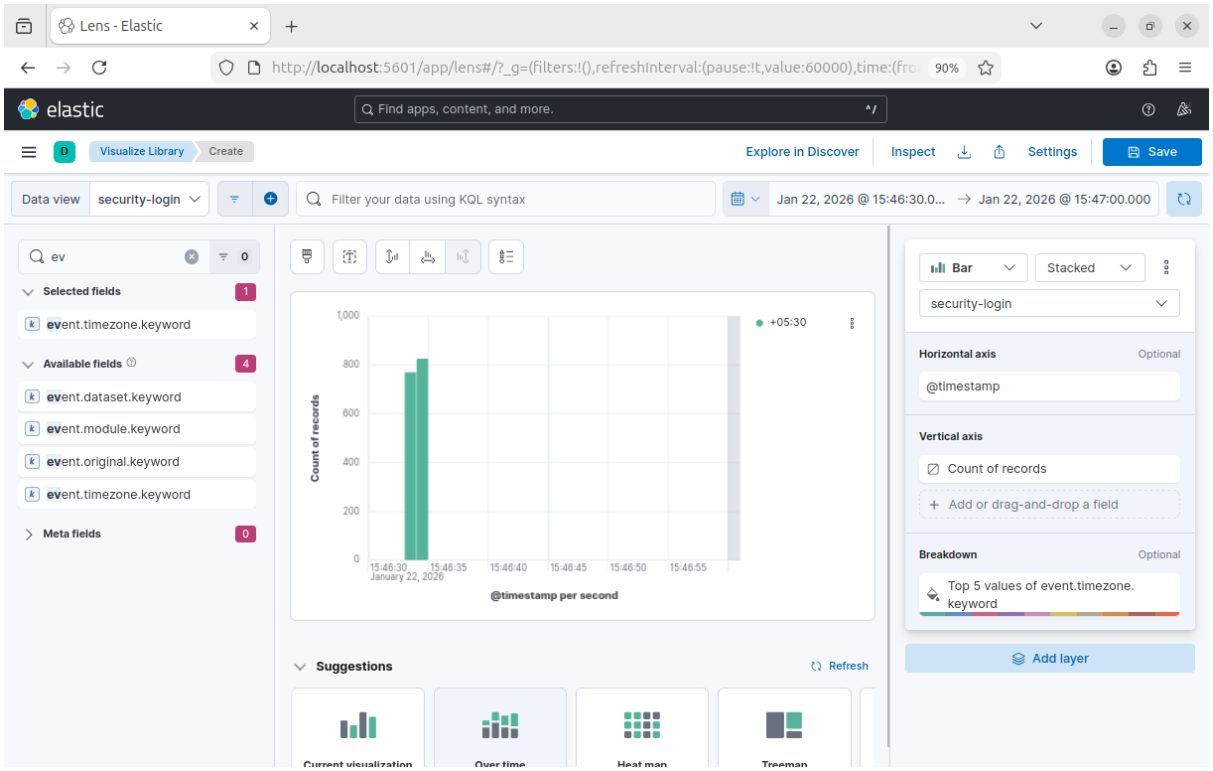
Monitoring dashboards in Kibana or Grafana provide a centralized and visual way to analyze security events in real time. By creating dashboards that display the top source IPs generating alerts and the frequency of critical event IDs, security analysts can quickly identify suspicious activity, detect attack patterns, and prioritize incident response actions effectively.

Methodology

- In Kibana create visualizations for Top 10 source IPs generating alerts.
- Use pre-built dashboards like sigma detection tools

Result





5. Configure Alert Rules

Introduction

Security alert rules are a core function of a SOC and SIEM platform. They help analysts automatically detect suspicious activities such as brute-force login attempts, reduce manual log monitoring, and enable faster incident response. In this task, Elastic SIEM and Wazuh are used to configure and validate alert rules for failed login attempts, simulating real-world attack scenarios and verifying the effectiveness of detection mechanisms.

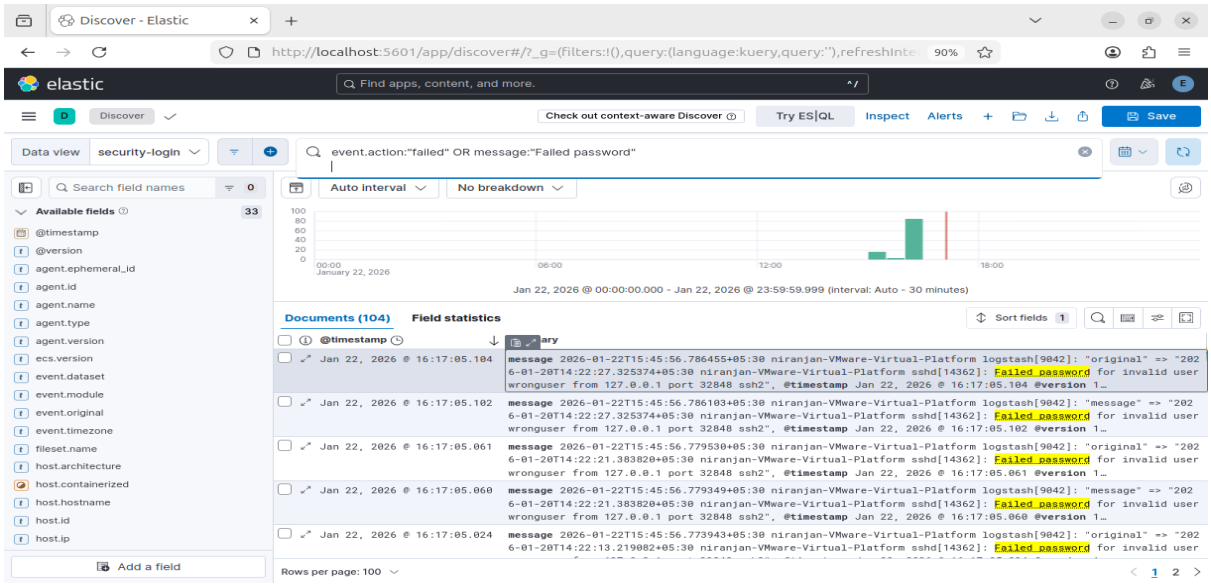
Methodology

- Elastic SIEM Alert Rule Configuration:- Create a detection rule in Elastic SIEM that specify “Rule: "Detect 5+ failed logins in 5 minutes" Index: security-login-* Condition: count > 5”
- Test with simulated failed SSH logins.
- Confirm that the alert is triggered when the defined threshold is exceeded and review alert details such as source IP, timestamp, and event count.

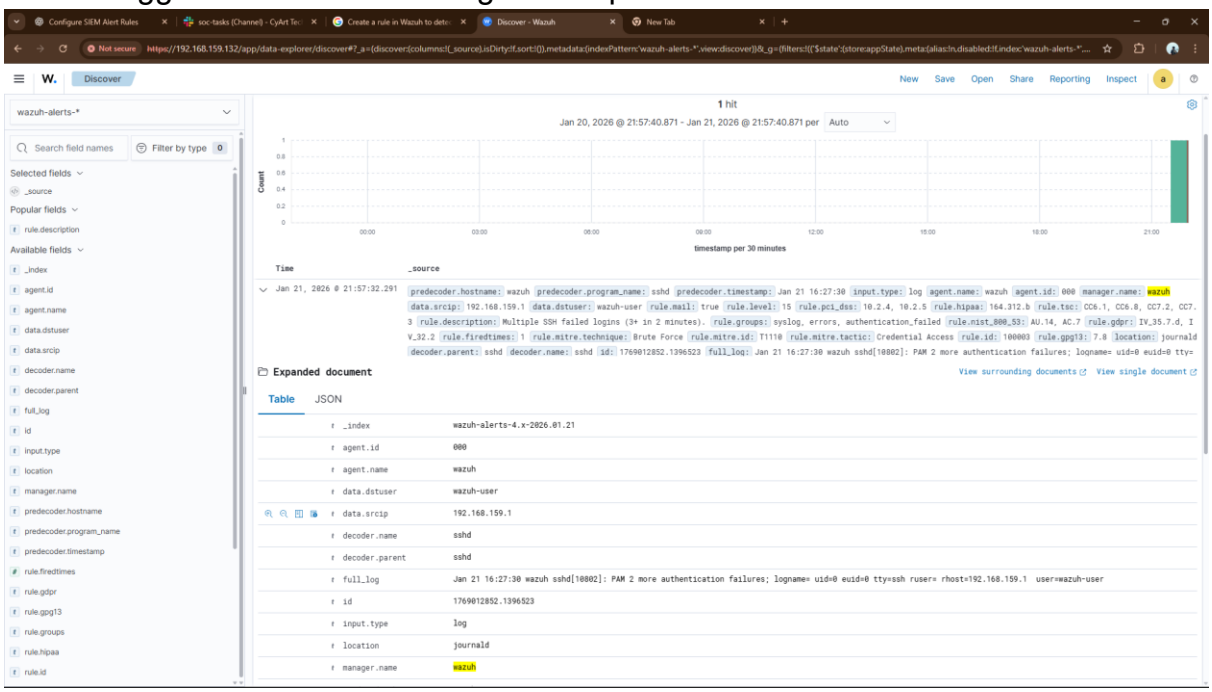
- Configure a custom Wazuh rule to detect three or more failed login attempts within two minutes using authentication failure logs.
- Repeat failed SSH login attempts and verify that the Wazuh rule generates alerts as expected.

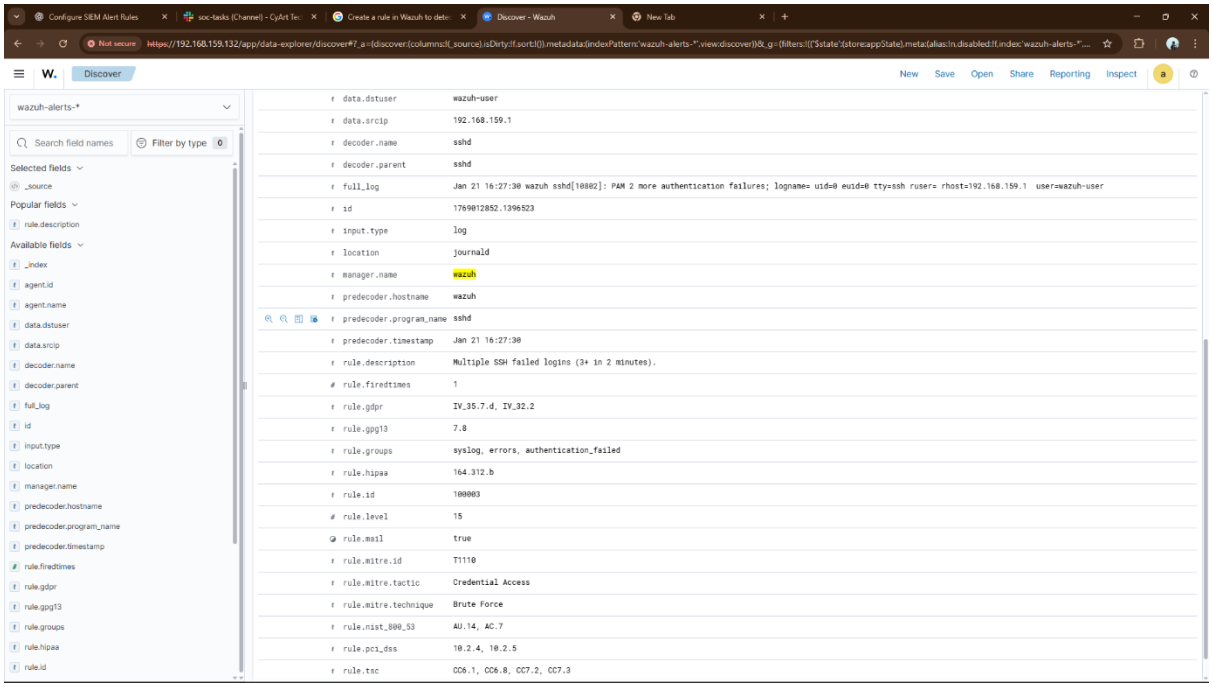
Result

Alert is triggered in Elastic SIEM



Alert is triggered for failed SSH login attempts in Wazuh





Conclusion

This study provides a solid understanding of SOC fundamentals by integrating theoretical concepts with practical security operations. Through hands-on experience with log analysis, SIEM monitoring, alert rule creation, and incident response workflows, learners develop the skills required to detect, investigate, and respond to security incidents. Overall, this approach prepares learners for real-world SOC environments by emphasizing structured processes, effective tools, and industry best practices.