



# SOC Fundamentals and Operations

## 1. Log Management Fundamentals

### Introduction

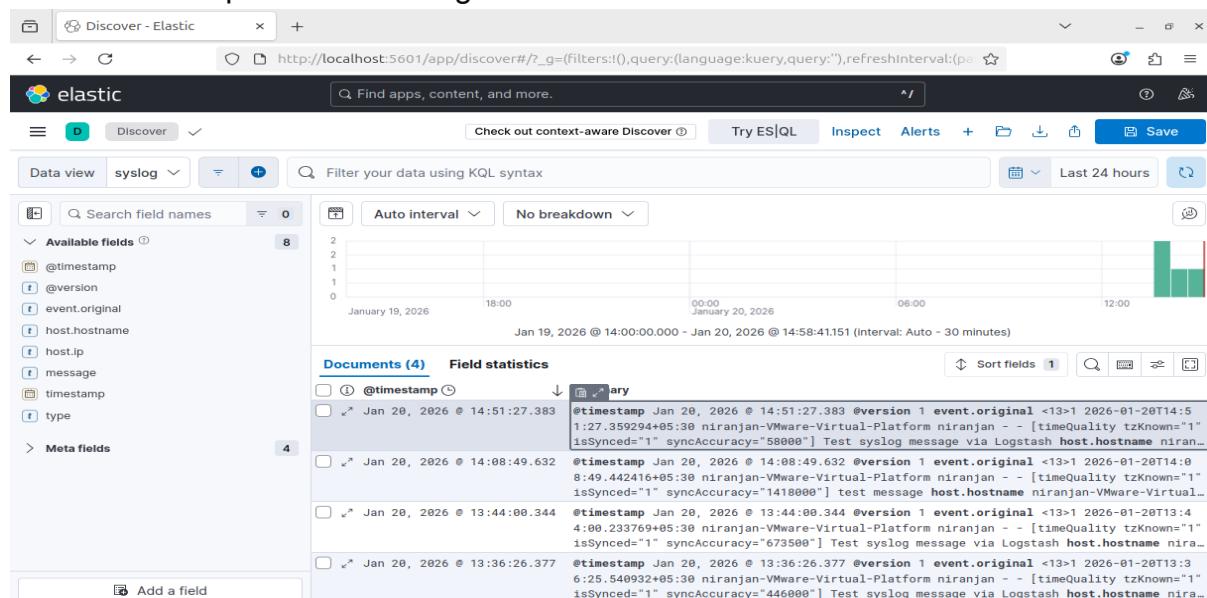
Log Management Fundamentals is the practice of collecting, standardizing, storing, and analysing logs from systems and applications to support security monitoring and troubleshooting. Logs such as Windows Event Logs, Syslog, and HTTP logs are collected using tools like Fluentd or Logstash, normalized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

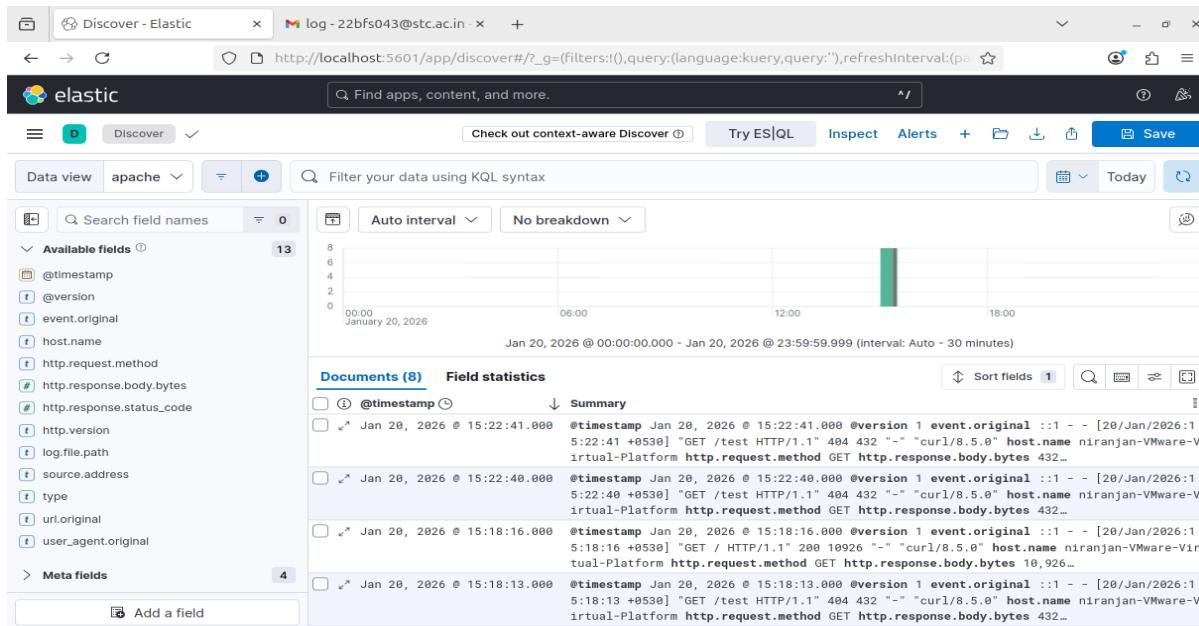
### Methodology

- 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](http://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

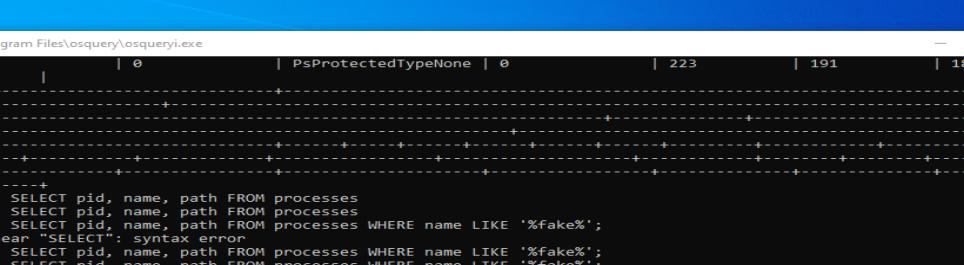
Successfully detect HTTP requests to "[malicious.com](#)".

```
niranjan@niranjan-VMware-Virtual-Platform:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i ens33
01/21-10:31:14.185074 [**] [1:1000001:1] Malicious Domain Detected [**] [Priority: 0] {TCP} 192.168.159.131:34614 -> 14
9.28.227.54:80
01/21-10:31:17.812830 [**] [1:1000001:1] Malicious Domain Detected [**] [Priority: 0] {TCP} 192.168.159.131:36302 -> 10
8.61.73.182:80
01/21-10:31:21.345765 [**] [1:1000001:1] Malicious Domain Detected [**] [Priority: 0] {TCP} 192.168.159.131:45018 -> 14
9.28.227.54:80
01/21-10:31:24.819118 [**] [1:1000001:1] Malicious Domain Detected [**] [Priority: 0] {TCP} 192.168.159.131:45026 -> 14
9.28.227.54:80
```

Reported the top 3 vulnerabilities by CVSS score.

The screenshot shows the Tenable Nessus Essentials interface. The main window displays a list of 54 vulnerabilities found on the host 192.168.159.138. The vulnerabilities are listed in a table with columns for Severity (CVSS), Name, Family, and Count. A pie chart in the bottom right corner shows the distribution of vulnerability types: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (light green). The interface includes a sidebar with Folders (My Scans, All Scans, Trash), Policies, and Plugin Rules. A news section at the bottom left mentions "Blind SSRF/DoS in Java TLS x509 AIA Extension".

Severity	CVSS	VPR	EPSS	Name	Family	Count
Critical	10.0 *	7.4	0.8622	UnrealRCd Backdoor Detection	Backdoors	1
Critical	10.0 *	5.1	0.0165	Debian OpenSSH/OpenSSL P...	Gain a shell remotely	1
Critical	10.0 *			VNC Server 'password' Passw...	Gain a shell remotely	1
Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1
Mixed	...	...	...	Phpmmyadmin (Multiple I...	CGI abuses	2
High	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
High	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1
High	7.5	5.9	0.7714	Samba Badlock Vulnerability	General	1
Mixed	...	...	...	ISC Bind (Multiple Issues)	DNS	5
Medium	6.5			Unencrypted Telnet Server	Misc.	1
Medium	5.3			Web Server info.php / phpinf...	CGI abuses	1
Medium	5.0 *			Backup Files Disclosure	CGI abuses	1
Mixed	...	...	...	HTTP (Multiple Issues)	Web Servers	7



```
C:\Program Files\osquery\osqueryi.exe
| 0 | 0 | PsProtectedTypeNone | 0 | 223 | 191 | 1875000
+---+---+-----+---+---+
osquery> SELECT pid, name, path FROM processes
...-> SELECT pid, name, path FROM processes
...-> SELECT pid, name, path FROM processes WHERE name LIKE '%fake%';
Error: near "SELECT": syntax error
osquery> SELECT pid, name, path FROM processes WHERE name LIKE '%fake%';
osquery> SELECT pid, name, path FROM processes WHERE name LIKE '%fake%';
osquery> SELECT pid, name, path FROM processes WHERE name LIKE '%fake%';
osquery> SELECT pid, name, path FROM processes WHERE name='cmd.exe';
+---+ | pid | name | path |
+---+ | 2704 | cmd.exe | C:\Windows\System32\cmd.exe |
+---+ | pid | name | path |
osquery> SELECT pid, name, path FROM processes WHERE cmdline LIKE '%fake_malware%';
+---+ | pid | name | path |
+---+ | 2704 | cmd.exe | C:\Windows\System32\cmd.exe |
+---+ | osquery>
```

### 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.

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists 'Event Viewer (Local)', 'Custom Views', 'Windows Logs' (with 'Security' selected), 'Application', 'Setup', 'System', 'Forwarded Events', 'Applications and Services Log', and 'Subscriptions'. The main pane displays a table of events under the heading 'Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 7'. The table columns are 'Keyword...', 'Date and Time', 'Source', 'Event ID', and 'Task Ca...'. Seven entries for event ID 4625 (Logon) on 21-01-2026 at 05:55:47 are listed. A detailed view of the first entry is shown in a modal window titled 'Event 4625, Microsoft Windows security auditing.' The modal shows the 'General' tab with the message 'An account failed to log on.' and the 'Details' tab with logon information: Subject (Security ID: SYSTEM, Account Name: DESKTOP-93B59TK\$, Account Domain: WORKGROUP, Logon ID: 0x3E7), Logon Type: 2, and Account For Which Logon Failed (Security ID: NULL SID). Below this, event properties are listed: Log Name: Security, Source: Microsoft Windows security, Event ID: 4625, Task Category: Logon, Level: Information, User: N/A, OpCode: Info, and More Information: [Event Log Online Help](#). The right pane is titled 'Actions' and contains a list of options: Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Clear Filter, Properties, Find..., Save Filtered Log File A..., Attach a Task To this L..., Save Filter to Custom ..., View, Refresh, Help, and Event 4625, Microsoft Wind... (expanded to show Event Properties, Attach Task To This Eve..., Copy, Save Selected Events..., Refresh, and Help).

The screenshot shows a Notepad window displaying the contents of 'failedlog.csv'. The file contains a header row with 'Keywords, Date and Time, Source, Event ID, Task Category' and a single data row: 'Audit Failure, 21-01-2026 05:55:47, Microsoft-Windows-Security-Auditing, 4625, Logon, "An account failed to log on..'. Below this, detailed log information is presented in key-value pairs:

```
Subject:
  Security ID: SYSTEM
  Account Name: DESKTOP-93B59TK$
  Account Domain: WORKGROUP
  Logon ID: 0x3E7

Logon Type: 2

Account For Which Logon Failed:
  Security ID: NULL SID
  Account Name: win10
  Account Domain: DESKTOP-93B59TK

Failure Information:
  Failure Reason: Unknown user name or bad password.
  Status: 0xC000006D
  Sub Status: 0xC000006A

Process Information:
  Caller Process ID: 0x2a4
  Caller Process Name: C:\Windows\System32\svchost.exe

Network Information:
  Workstation Name: DESKTOP-93B59TK
  Source Network Address: 127.0.0.1
  Source Port: 0

Detailed Authentication Information:
  Logon Process: User32
  Authentication Package: Negotiate
  Transited Services: -
  Package Name (NTLM only): -
  Key Length: 0
```

## Document Security Events

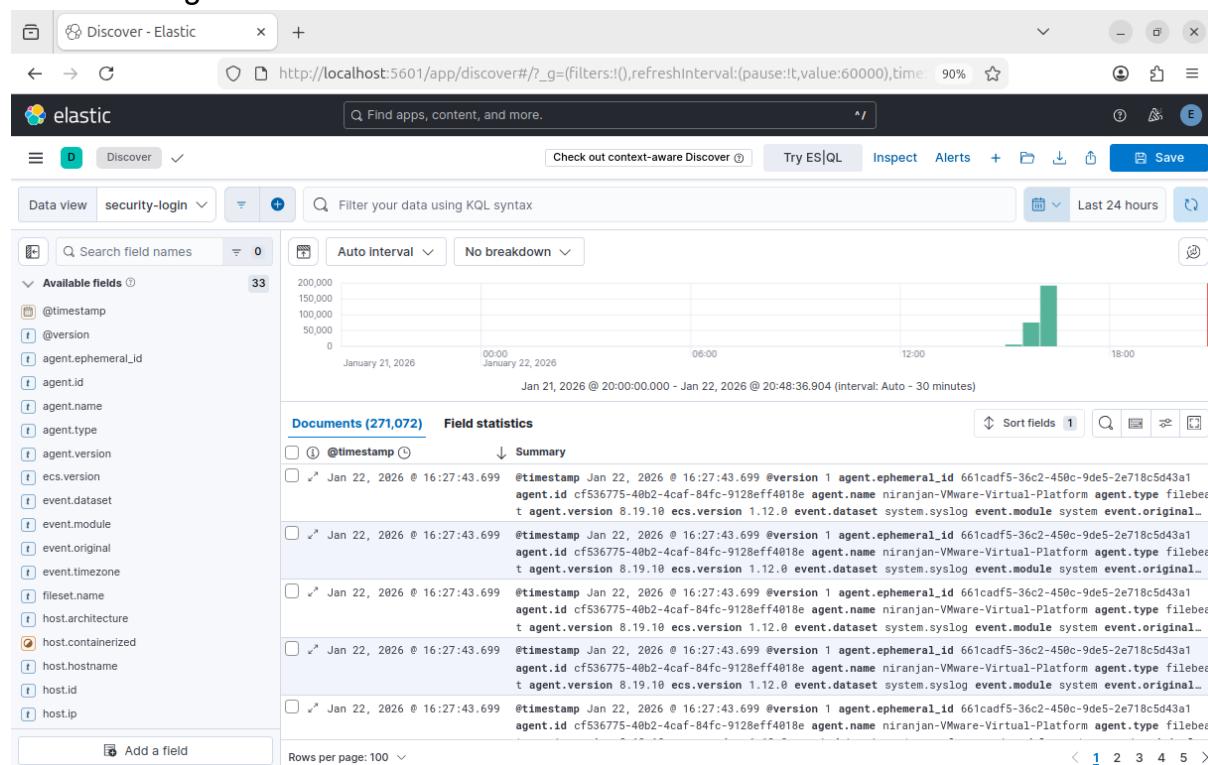
### Introduction

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

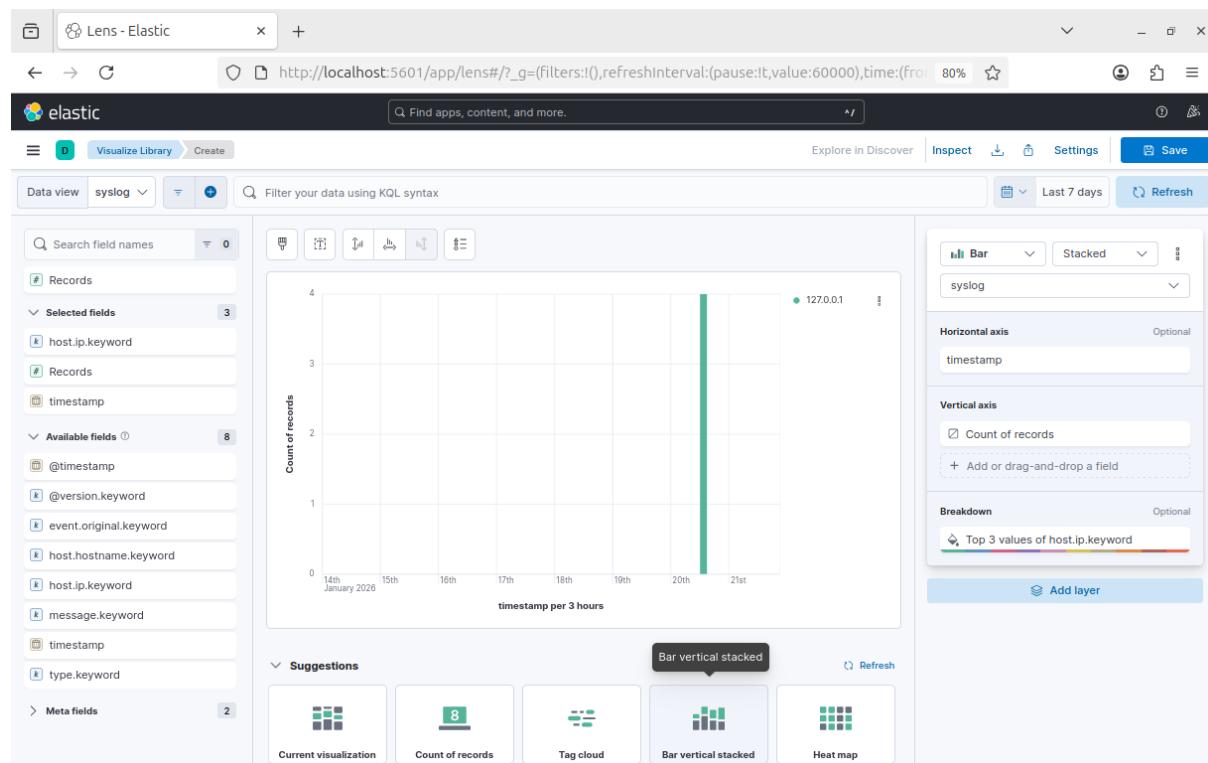
### Introduction

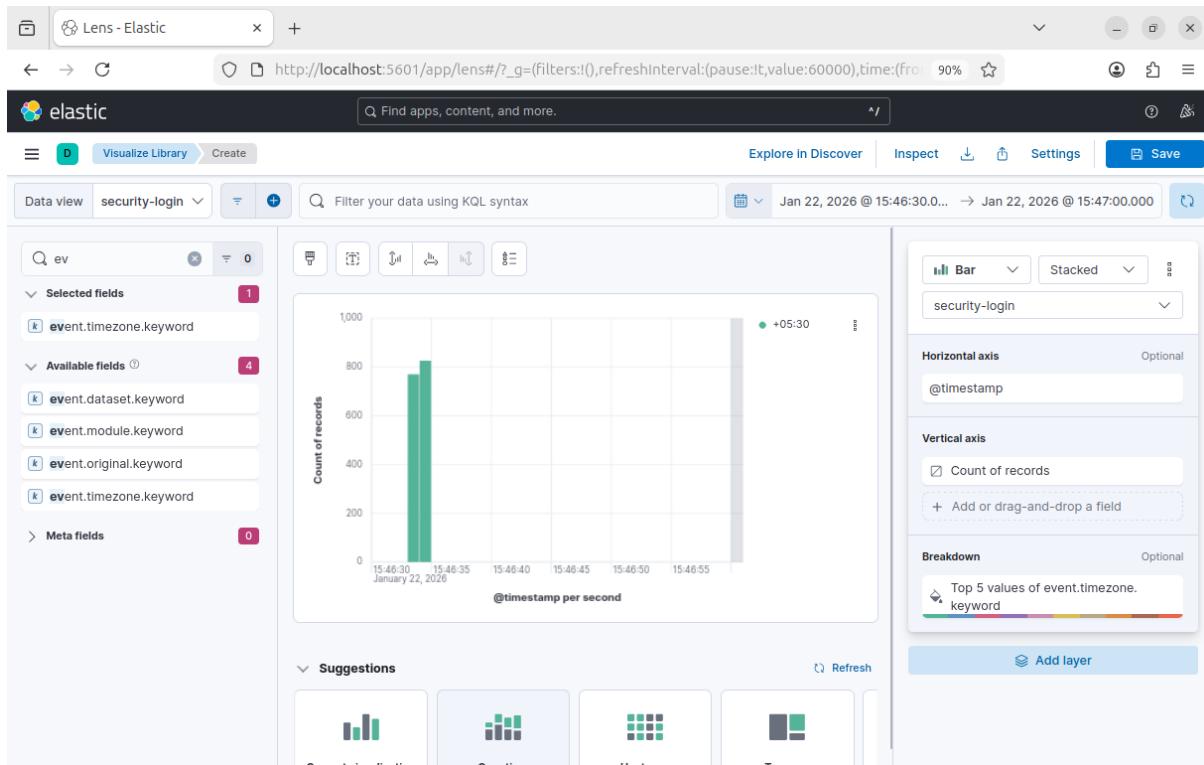
Monitoring dashboards in Kibana or Grafana provide a centralized and visual way to analyze security events in real time. By creating dashboards that display the top source IPs generating alerts and the frequency of critical event IDs, security analysts can quickly identify suspicious activity, detect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

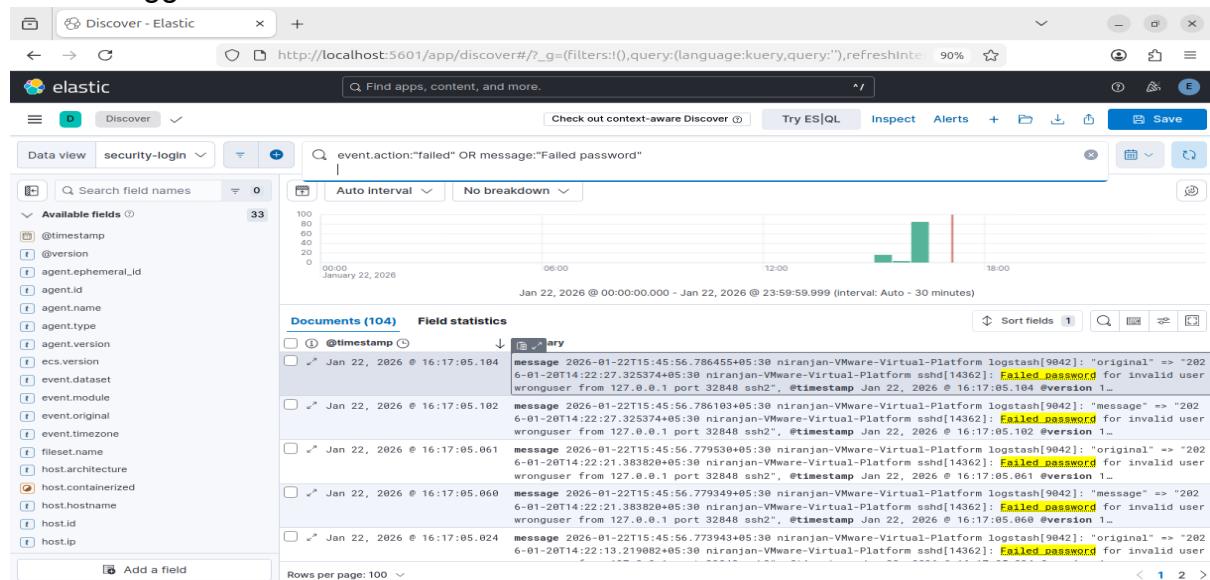
- **Elastic SIEM Alert Rule Configuration:-** Create a detection rule in Elastic SIEM that specify "Rule: "Detect 5+ failed logins in 5 minutes" Index: security-login-\* Condition: count > 5"
- Test with simulated failed SSH logins.
- Confirm that the alert is triggered when the defined threshold is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



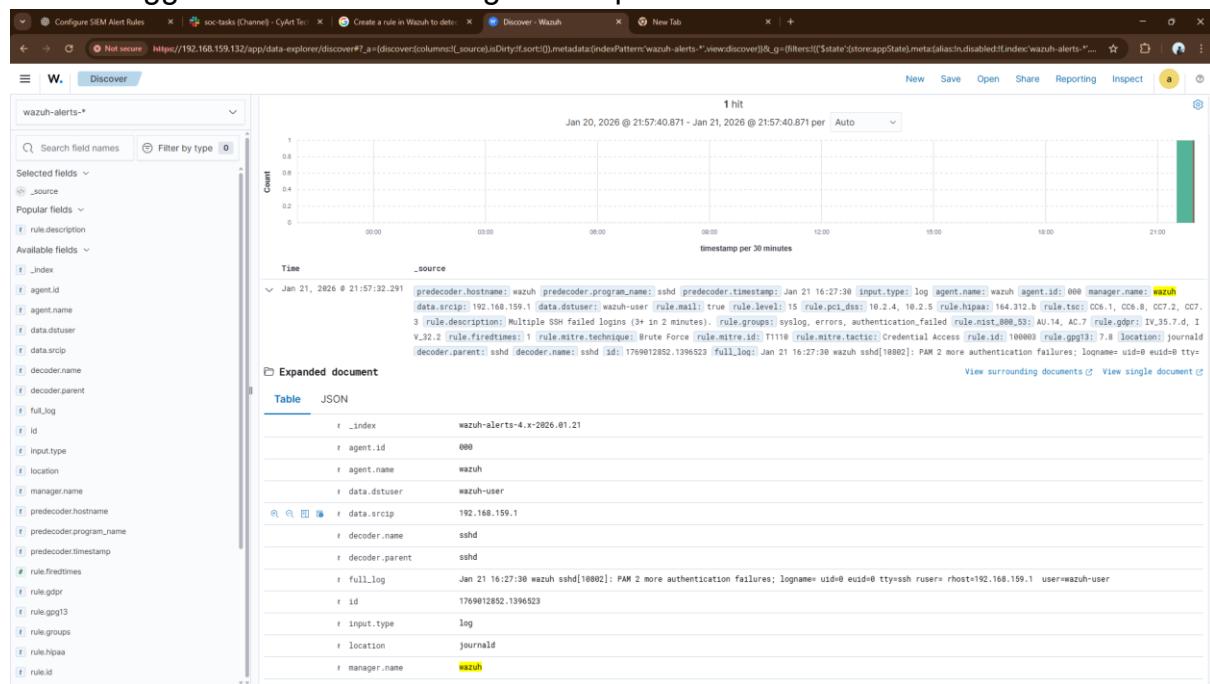
- Configure a custom Wazuh rule to detect three or more failed login attempts within two minutes using authentication failure logs.
- Repeat failed SSH login attempts and verify that the Wazuh rule generates alerts as expected.

## Result

Alert is triggered in Elastic SIEM



Alert is triggered for failed SSH login attempts in Wazuh





	wazuh-alerts-*	
Selected fields	↳ _source	
Popular fields	↳ rule.description	
Available fields	↳ _index	
	↳ agent.id	
	↳ agent.name	
	↳ data.dstuser	wazuh-user
	↳ data.srcip	192.168.159.1
	↳ decoder.name	sshd
	↳ decoder.parent	sshd
	↳ full_log	Jan 21 16:27:30 wazuh sshd[10882]: PAN 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.159.1 user=wazuh-user
	↳ id	1799012852,1996523
	↳ input.type	log
	↳ location	journald
	↳ manager.name	wazuh
	↳ predecoder.hostname	wazuh
	↳ predecoder.program.name	sshd
	↳ predecoder.timestamp	Jan 21 16:27:30
	↳ rule.description	Multiple SSH failed logins (3+ in 2 minutes).
	↳ rule.firetimes	1
	↳ rule.gdpr	IV_35.7_d, IV_32.2
	↳ rule.gpg13	7.8
	↳ rule.groups	syslog, errors, authentication_failed
	↳ rule.hipaa	164.312.b
	↳ rule.id	100003
	↳ rule.level	15
	↳ rule.mail	true
	↳ rule.mitre.id	T110
	↳ rule.mitre.tactic	Credential Access
	↳ rule.mitre.technique	Brute Force
	↳ rule.nist_800_53	AU.14, AC.7
	↳ rule.pci_dss	10.2.4, 10.2.5
	↳ rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3

## 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.



CYART

inquiry@cyart.io

www.cyart.io