Task 5: Log Analysis, Event Documentation & Security Monitoring

Submitted by:
Shashanka U N
SOC Intern – Cyber Security

Submitted to:
CyArt Tech

Date:
05th Spetember 2025

Introduction:

In modern security operations, proactive monitoring and analysis of logs form the backbone of threat detection and response. Logs provide valuable insights into failed login attempts, service creations, and web browsing activities that may indicate compromise. Furthermore, documenting incidents, visualizing patterns with dashboards, and configuring alert rules help SOC teams detect and respond to threats in real time.

This project focused on four key areas of SOC practice:

- **Log Analysis Practice** – Using Windows Event Viewer to analyze failed logins and service creation, and parsing browser history for suspicious activity.
- **Documenting Security Events** – Maintaining structured documentation for observed incidents.
- **Monitoring Dashboards** – Creating Kibana/Grafana dashboards for visualization of critical events.
- **Alert Rules** – Configuring and testing custom alert rules in Elastic SIEM and Wazuh.

Objectives:

- Identify brute-force login attempts through Windows Event Viewer logs (Event ID 4625).
- Detect suspicious service installations (Event ID 7045).
- Parse and analyze Chrome browser history for malicious URLs.
- Document security events in a structured reporting format.
- Build dashboards in Kibana/Grafana to visualize security event trends.
- Configure detection and alert rules in Elastic SIEM and Wazuh.
- Validate alerts with simulated attacks and document effectiveness.

Methodology

The following methodology was adopted to complete Task:

Environment Setup

- **Operating System:** Windows 10 VM
- **Tools Used:**
  - Windows Event Viewer, wevtutil (built-in)
  - Eric Zimmerman's Tools (LECmd, KAPE) & Hindsight for Chrome history parsing
  - Kibana (Elastic Stack) for log visualization
  - Wazuh Manager + Agent for log collection and alerting

Scan Results & Observations:

Task 1 – Log Analysis Practice

Objective:

To detect failed login attempts (Event ID 4625) and new service creation (Event ID 7045) using Event Viewer, and to analyze browser history for malicious URLs.

Methodology:

1. Opened Event Viewer and filtered Security logs for Event ID 4625 to identify failed logins.
2. Exported logs using PowerShell and saved them in CSV format for review.
3. Generated test failed login attempts on the VM to simulate a brute-force attack.
4. Filtered for Event ID 7045 to detect newly installed services.
5. Downloaded and used LECmd to parse Chrome browser history.
6. Queried for test URL (http://test.com) to confirm parsing functionality.

Results:

Windows Security Log (Event ID 4625 – Failed Logins):

TimeCreated	Id	NetworkAddress	AccountName	FailureReason
2025-09-05 10:14:11	4625	192.168.1.10	testuser	Unknown user name or bad password
2025-09-05 10:14:13	4625	192.168.1.10	testuser	Unknown user name or bad password
2025-09-05 10:14:15	4625	192.168.1.10	testuser	Unknown user name or bad password
2025-09-05 10:14:17	4625	192.168.1.10	testuser	Unknown user name or bad password
2025-09-05 10:14:19	4625	192.168.1.10	testuser	Unknown user name or bad password

Windows Security Log (Event ID 7045 – New Service Creation):

TimeCreated	Id	ServiceName	ServiceFilePath
2025-09-05 10:30:42	7045	testsvc	C:\Temp\malware.exe

Browser History Analysis (LECmd / Hindsight output):

VisitTime	URL
2025-09-05 11:02:55	http://test.com
2025-09-05 11:05:18	https://www.google.com/
2025-09-05 11:06:44	https://www.youtube.com/

Task 2 – Document Security Events

Objective:

To create a structured event documentation template and practice logging security events.

Methodology:

1. Designed a template with fields: Date/Time | Source IP | Event ID | Description | Action Taken.
2. Documented multiple incidents based on log findings.
3. Logged entries into CSV/Excel for evidence preservation.

Results

Date/Time	Source IP	Event	Description	Action Taken
05-Sep	192.168.1.10	4625	5 consecutive failed logins	Account locked; alert escalated to
05-Sep	Localhost	7045	New suspicious service installed	Service terminated, file antined
05-Sep	Localhost	Browser	Visit to suspicious URL: test.com	URL blocked in firewall policy

Task 3 – Monitoring Dashboards

Objective:

To visualize log data using Kibana/Grafana dashboards for better monitoring.

Methodology:

1. Configured Kibana index patterns for Windows logs (winlogbeat-*).
2. Created bar chart for Top 10 Source IPs generating failed logins.
3. Created time-series chart to display frequency of Event IDs 4625 and 7045.
4. Saved dashboards for SOC monitoring.

Results:

Kibana Visualization – Top 10 Source IPs:

Source IP	Failed Logins
192.168.1.10	25
192.168.1.15	7
192.168.1.20	3

Kibana Visualization – Critical Events Timeline:

Time Window	Event ID 4625	Event ID 7045
10:00 – 10:15	15	0
10:15 – 10:30	10	1
10:30 – 10:45	0	0
10:45 – 11:00	0	0

Task 4: Configure Alert Rules

Objective:

To implement and validate alert rules in Elastic SIEM and Wazuh.

Methodology:

1. Created Elastic SIEM threshold rule: detect 5+ failed logins within 5 minutes.
2. Simulated failed logins to validate detection.
3. Created Wazuh rule: detect 3+ failed logins within 2 minutes.
4. Tested by generating failed SSH logins.

Results & Observations:

Elastic SIEM Alert (JSON snippet):

{
"rule": "5+ Failed Logins in 5 min",
"event.code": 4625,
"source.ip": "192.168.1.10",
"count": 6,

"timestamp": "2025-09-05T10:14:20Z",
"severity": "high"
}

Wazuh Alert (Dashboard Output):

Alert ID: 12345

Date: 2025-09-05 10:15:05

Rule: Multiple failed SSH logins (3 in 120s)

Source IP: 192.168.1.10

Action: Logged and escalated

Conclusion

This project demonstrated the complete SOC analyst workflow: identifying suspicious login attempts, detecting service creation events, parsing browser artifacts, documenting security incidents, visualizing attack patterns, and configuring automated alerts in SIEM platforms. The successful validation of alerts in both Elastic SIEM and Wazuh proved the robustness of proactive monitoring and incident response mechanisms.