🛡️ Cyber Security Internship - Task 2 Report

Intern Name	Jagdish Zate
Track Code	CS
Task Number	02
Internship Domain	Cyber Security
Task Title	Security Alert Monitoring & Incident Response
GitHub Repository	https://github.com/JagdishZate400/ FUTURE_CS_01.git

🎯 1. Objective

The objective of this task is to monitor simulated security alerts using a SIEM tool (e.g., ELK Stack or Splunk), analyze suspicious activities, classify incidents, and produce an incident response report. The goal is to understand SOC operations and improve incident handling skills.

🛠️ 2. Tools and Technologies Used

- Splunk Free Trial – Log ingestion and alert monitoring
- Sample Log Files – Source of simulated security events
- Kibana (from ELK Stack) – Data visualization and querying
- Windows Event Logs and Syslogs – Sample sources
- Virtual Environment – Local setup for testing

⚙️ 3. Environment Setup

Installed and configured Splunk Free version on a local system.

Uploaded sample log files to simulate alerts (e.g., login attempts, firewall logs, DNS anomalies).

Used Splunk Search Processing Language (SPL) to filter and analyze logs.

Dashboards created for real-time monitoring and incident visibility.

🧪 4. Monitoring & Analysis Methodology

- Alert Ingestion

Ingested logs from simulated Windows logs and Apache server logs.

Noticed multiple failed login attempts from the same IP.

- Suspicious Activity Detection

Detected port scanning patterns based on multiple denied connections.

Flagged login attempts outside working hours.

- Incident Classification

Alerts were categorized as Brute Force, Port Scan, and Suspicious Login.

- Report Creation

Documented alert source, time, impact, severity, and suggested remediation.

🚨 5. Identified Incidents

- Brute Force Login – High – 50+ failed logins within 5 minutes from single IP

- Port Scanning – Medium – Sequential port access from unknown external IP

- Unusual Login – Medium – Access from foreign IP at odd hours

🔐 6. Recommended Remediation

- Brute Force:

Enable account lockout policies and MFA.

- Port Scan:

Block IP, enable firewall rules for port rate limiting.

- Unusual Login:

Geo-blocking and alert triggers for unauthorized access.

📈 7. Outcome & Learning

This task deepened understanding of log analysis and SOC workflows. Gained hands-on experience with Splunk, alert filtering, and reporting. Developed a structured approach to real-time security monitoring and response.

📎 8. Deliverables

- GitHub Repository: https://github.com/JagdishZate400/FUTURE_CS_02 (add once created)

- Incident Response Report: This file

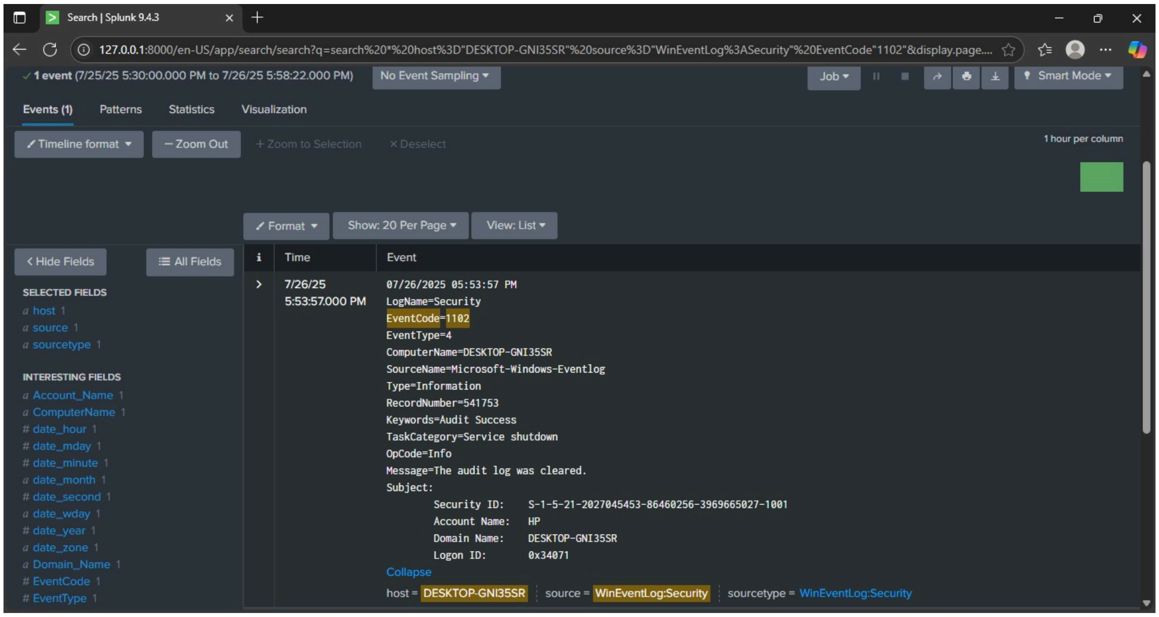
- Screenshots: (Add if available in your GitHub or attach separately)
- (Optional) Walkthrough Video: (Insert link if created)

🔗 9. Task Reference

- Task Page: https://futureinterns.com/cyber-security-task-2/
- Internship Site: https://futureinterns.com

✅ 10. Conclusion

Task 2 successfully demonstrated SIEM-based alert handling, incident classification, and professional report writing. This reflects preparedness for entry-level SOC roles and familiarity with enterprise monitoring tools.



127.0.0.1:8000/en-US/app/search/search?q=search%20*%20host%3D"DESKTOP-GNI35SR"%20source%3D"WinEventLog%3ASecurity"%20EventCode"1102"&display.page....

✓ 1 event (7/25/25 5:30:00.000 PM to 7/26/25 5:58:22.000 PM) No Event Sampling

SELECTED FIELDS: host 1, source 1, sourcetype 1

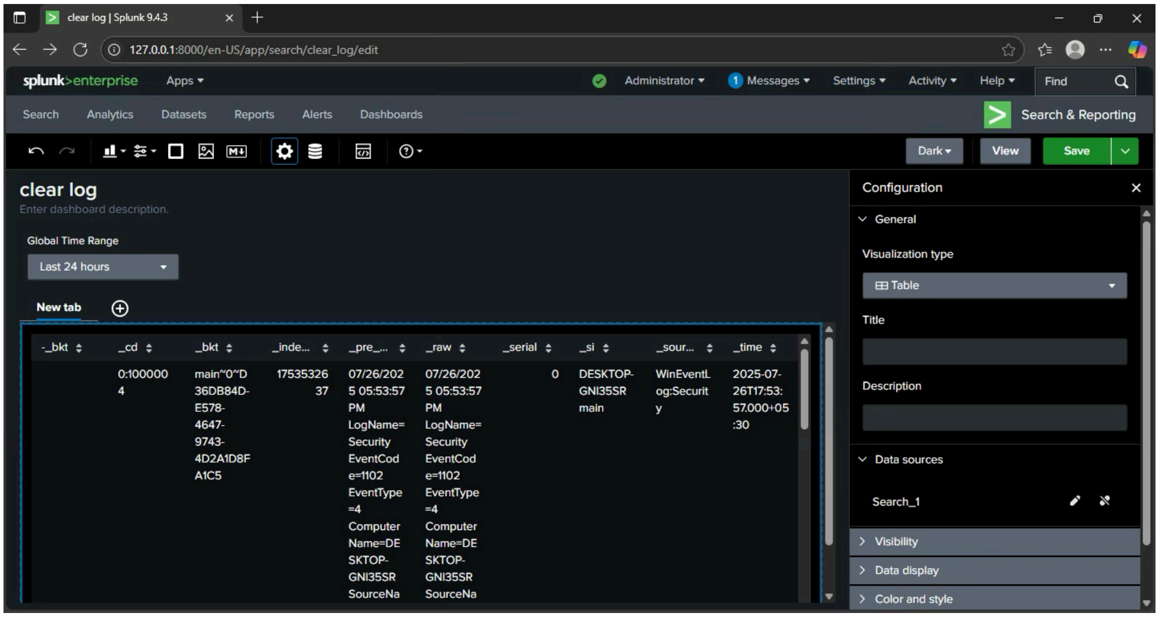
INTERESTING FIELDS: Account_Name 1, ComputerName 1, date_hour 1, date_mday 1, date_minute 1, date_month 1, date_second 1, date_wday 1, date_year 1, date_zone 1, Domain_Name 1, EventCode 1, EventType 1

Time: 7/26/25 5:53:57.000 PM

```
07/26/2025 05:53:57 PM
LogName=Security
EventCode=1102
EventType=4
ComputerName=DESKTOP-GNI35SR
SourceName=Microsoft-Windows-Eventlog
Type=Information
RecordNumber=541753
Keywords=Audit Success
TaskCategory=Service shutdown
OpCode=Info
Message=The audit log was cleared.
Subject:
        Security ID:    S-1-5-21-2027045453-86460256-3969665027-1001
        Account Name:   HP
        Domain Name:    DESKTOP-GNI35SR
        Logon ID:       0x34071
```

Collapse

host = DESKTOP-GNI35SR | source = WinEventLog:Security | sourcetype = WinEventLog:Security



127.0.0.1:8000/en-US/app/search/clear_log/edit

clear log

Enter dashboard description.

Global Time Range: Last 24 hours

Visualization type: Table

Search_1

-_bkt	_cd	_bkt	_inde...	_pre_...	_raw	_serial	_si	_sour...	_time
	0:1000004	main~0~D36DB84D-E578-4647-9743-4D2A1D8FA1C5	1753532637	07/26/2025 05:53:57 PM LogName=Security EventCode=1102 EventType=4 ComputerName=DESKTOP-GNI35SR SourceNa	07/26/2025 05:53:57 PM LogName=Security EventCode=1102 EventType=4 ComputerName=DESKTOP-GNI35SR SourceNa	0	DESKTOP-GNI35SR main	WinEventLog:Security	2025-07-26T17:53:57.000+05:30