



## **Task 02: Security Operations Center (SOC) Internship Task: Security Alert Monitoring & Incident Response Simulation**

---

**Track Code:** FUTURE\_CS\_02

**Intern Name:** Vaibhav Malhotra

---

- **OBJECTIVE:**

Monitor security alerts, analyze potential threats, and simulate incident response — just like a SOC analyst in a real company. Secondly, Identify suspicious activities such as failed logins, unusual IP addresses, or malware alerts

- **Skills Gained:**

- > Basic log analysis and alert triage
- > Understanding of SIEM tools and dashboards
- > Incident classification and escalation process
- > Cybersecurity terminology and threat identification
- > Effective incident communication and reporting

- **Tools Used:**

1. Splunk Free Trial
2. Sample Alert Logs (provided by Internship mentors)
3. MS-Word (Incident Report)

# SPLUNK SIEM TOOL

## **SIEM: Security Information and Event Management**

---

Is a cybersecurity solution that gathers and analyzes security data from various sources within an IT environment to detect, analyze, and respond to threats. It combines Security Information Management (SIM) and Security Event Management (SEM) to provide a comprehensive view of an organization's security posture

## **SPLUNK APP:**

---

Splunk App are the applications which monitor web servers, analyze network security, or manage applications. They consist of various knowledge objects like saved searches, reports, alerts, dashboards, and datasets, along with other configurations like lookups and event types.

## **SPL: SEARCH PROCESSING LANGUAGE**

---

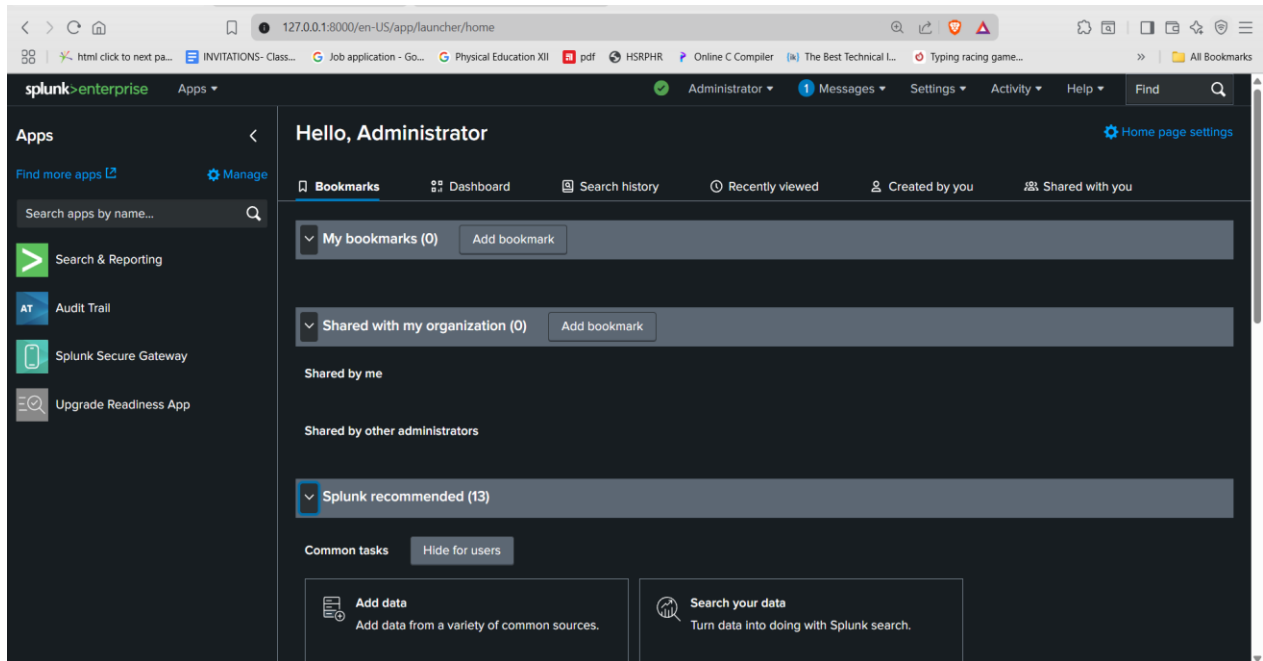
Is a query language used to search, analyze, and visualize data within the Splunk platform. It's not a traditional programming language, but rather a way to interact with and manipulate data stored in Splunk's indexes.

---

---

# Security Incident Report

## Splunk Enterprise >:



## The log data:

The screenshot displays a list of log events in Splunk. The table has columns for 'Time' and 'Event'. The events are filtered by 'host = LAPTOP-PCRSSHHO' and 'sourcetype = implog'. The events show various actions such as 'malware detected', 'file accessed', 'login success', and 'login failed'.

Time	Event
7/3/25 9:10:14.000 AM	2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior
7/3/25 9:10:14.000 AM	2025-07-03 09:10:14   user=bob   ip=198.51.100.42   action=file accessed
7/3/25 9:07:14.000 AM	2025-07-03 09:07:14   user=veve   ip=203.0.113.77   action=login success
7/3/25 9:02:14.000 AM	2025-07-03 09:02:14   user=david   ip=203.0.113.77   action=login failed
7/3/25 8:42:14.000 AM	2025-07-03 08:42:14   user=veve   ip=172.16.0.3   action=file accessed
7/3/25 8:42:14.000 AM	2025-07-03 08:42:14   user=charlie   ip=203.0.113.77   action=file accessed
7/3/25 8:31:14.000 AM	2025-07-03 08:31:14   user=veve   ip=203.0.113.77   action=file accessed
7/3/25 8:30:14.000 AM	2025-07-03 08:30:14   user=veve   ip=172.16.0.3   action=login success
7/3/25 8:21:14.000 AM	2025-07-03 08:21:14   user=david   ip=172.16.0.3   action=connection attempt
7/3/25 8:20:14.000 AM	2025-07-03 08:20:14   user=charlie   ip=192.168.1.101   action=connection attempt
7/3/25 8:00:14.000 AM	2025-07-03 08:00:14   user=alice   ip=198.51.100.42   action=login success
7/3/25 7:57:14.000 AM	2025-07-03 07:57:14   user=david   ip=10.0.0.5   action=file accessed
7/3/25 7:51:14.000 AM	2025-07-03 07:51:14   user=veve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature
7/3/25 7:46:14.000 AM	2025-07-03 07:46:14   user=bob   ip=10.0.0.5   action=login success

Format Show: 20 Per Page View List			< Prev 1 2 3 Next >			
Hide Fields All Fields						
SELECTED FIELDS						
host 1						
source 1						
sourcetype 1						
INTERESTING FIELDS						
action 4						
date_hour 6						
date_minute 33						
date_month 1						
date_second 1						
date_week 1						
date_year 1						
index 1						
ip 5						
linecount 1						
punct 3						
splunk_server 1						
threat 5						
timestamp 1						
user 5						
+ Extract New Fields						
Time Event						
7/3/25 7:18:14.000 AM			2025-07-03 07:18:14   user=bob   ip=203.0.113.77   action=file accessed			
7/3/25 7:02:14.000 AM			2025-07-03 07:02:14   user=alice   ip=203.0.113.77   action=login failed			
7/3/25 6:21:14.000 AM			2025-07-03 06:21:14   user=alice   ip=203.0.113.77   action=login success			
7/3/25 6:13:14.000 AM			2025-07-03 06:13:14   user=charlie   ip=10.0.0.5   action=connection attempt			
7/3/25 6:10:14.000 AM			2025-07-03 06:10:14   user=david   ip=203.0.113.77   action=file accessed			
7/3/25 6:01:14.000 AM			2025-07-03 06:01:14   user=bob   ip=172.16.0.3   action=file accessed			
7/3/25 5:49:14.000 AM			2025-07-03 05:49:14   user=charlie   ip=192.168.1.101   action=connection attempt			
7/3/25 5:48:14.000 AM			2025-07-03 05:48:14   user=bob   ip=10.0.0.5   action=malware detected   threat=Trojan Detected			
7/3/25 5:45:14.000 AM			2025-07-03 05:45:14   user=david   ip=172.16.0.3   action=malware detected   threat=Trojan Detected			
7/3/25 5:44:14.000 AM			2025-07-03 05:44:14   user=bob   ip=198.51.100.42   action=file accessed			
7/3/25 5:42:14.000 AM			2025-07-03 05:42:14   user=eve   ip=203.0.113.77   action=malware detected   threat=Trojan Detected			
7/3/25 5:33:14.000 AM			2025-07-03 05:33:14   user=david   ip=198.51.100.42   action=file accessed			
7/3/25 5:30:14.000 AM			2025-07-03 05:30:14   user=eve   ip=192.168.1.101   action=malware detected   threat=Trojan Detected			
7/3/25 5:27:14.000 AM			2025-07-03 05:27:14   user=david   ip=203.0.113.77   action=connection attempt			

## Security Alerts and logs (Malware Detected):

Format Show: 20 Per Page View List			< Prev 1 2 Next >			
Hide Fields All Fields						
SELECTED FIELDS						
host 1						
source 1						
sourcetype 2						
INTERESTING FIELDS						
action 1						
date_hour 4						
date_minute 10						
date_month 1						
date_second 1						
date_week 1						
date_year 1						
index 1						
ip 5						
linecount 1						
punct 2						
splunk_server 1						
threat 5						
timestamp 1						
user 5						
+ Extract New Fields						
Time Event						
7/3/25 8:10:14.000 AM			2025-07-03 08:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior			
7/3/25 7:51:14.000 AM			2025-07-03 07:51:14   user=eve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature			
7/3/25 7:51:14.000 AM			2025-07-03 07:51:14   user=eve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature			
7/3/25 7:45:14.000 AM			2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected			
7/3/25 7:45:14.000 AM			2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected			
7/3/25 5:48:14.000 AM			2025-07-03 05:48:14   user=bob   ip=10.0.0.5   action=malware detected   threat=Trojan Detected			
7/3/25 5:48:14.000 AM			2025-07-03 05:48:14   user=bob   ip=10.0.0.5   action=malware detected   threat=Trojan Detected			
7/3/25 5:45:14.000 AM			2025-07-03 05:45:14   user=david   ip=172.16.0.3   action=malware detected   threat=Trojan Detected			
7/3/25 5:45:14.000 AM			2025-07-03 05:45:14   user=david   ip=172.16.0.3   action=malware detected   threat=Trojan Detected			

Format Show: 20 Per Page View List			< Prev 1 2 Next >			
Hide Fields All Fields						
SELECTED FIELDS						
host 1						
source 1						
sourcetype 2						
INTERESTING FIELDS						
action 1						
date_hour 4						
date_minute 10						
date_month 1						
date_second 1						
date_week 1						
date_year 1						
index 1						
ip 5						
linecount 1						
punct 2						
splunk_server 1						
threat 5						
timestamp 1						
user 5						
+ Extract New Fields						
Time Event						
7/3/25 4:19:14.000 AM			2025-07-03 04:19:14   user=alice   ip=198.51.100.42   action=malware detected   threat=Rootkit Signature			
7/3/25 4:19:14.000 AM			2025-07-03 04:19:14   user=alice   ip=198.51.100.42   action=malware detected   threat=Rootkit Signature			

The screenshot shows a Splunk search interface with the following search query:

```
index=main source="imp-log.txt" "malware detected" | rex "user={<user>\\w+}"  
| rex "ip={<ip>\\d+\\.\\d+\\.\\d+\\.\\d+}"  
| rex "action={<action>[\\w+]}"  
| rex "threat={<threat>.+}"  
| eval severity=case(  
  match(threat, "Rootkit"), "Critical",  
  match(threat, "Ransomware"), "Critical",  
  match(threat, "Worm"), "High",  
  match(threat, "Trojan"), "High",  
  match(threat, "Spyware"), "Medium",  
  1==1, "Low"  
)  
| table _time user ip threat severity  
| sort -_time
```

The results table shows 22 events. The first two events are highlighted with a red border:

_time	user	ip	threat	severity
2025-07-03 04:19:14	alice	198.51.100.42	Rootkit Signature	Critical
2025-07-03 04:19:14	alice	198.51.100.42	Rootkit Signature	Critical

## Rootkit Signature

User: Alice

Time: 4:19:14

Date: 2025-7-3

IP address: 198.51.100.42

Threat: Rootkit Signature

Severity: Critical

- Difficult to detect, likely system compromise
- Rootkit allows persistent, stealthy access to a system.

The screenshot shows a Splunk search interface with the same search query as the first image:

```
index=main source="imp-log.txt" "malware detected" | rex "user={<user>\\w+}"  
| rex "ip={<ip>\\d+\\.\\d+\\.\\d+\\.\\d+}"  
| rex "action={<action>[\\w+]}"  
| rex "threat={<threat>.+}"  
| eval severity=case(  
  match(threat, "Rootkit"), "Critical",  
  match(threat, "Ransomware"), "Critical",  
  match(threat, "Worm"), "High",  
  match(threat, "Trojan"), "High",  
  match(threat, "Spyware"), "Medium",  
  1==1, "Low"  
)  
| table _time user ip threat severity  
| sort -_time
```

The results table shows 22 events. The first two events are highlighted with a red border:

_time	user	ip	threat	severity
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware Behavior	Critical
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware Behavior	Critical

## Ransomware Behaviour

**User:** BOB

**Time:** 9:10:14

**Date:** 2025-7-3

**IP Address:** 172.16.0.3

**Severity:** Critical

Repeated twice at the same timestamp — likely indicating:

1. Duplicate ingestion
2. Or high-priority detection by multiple systems

**Risk:** Encryption of files, lateral movement.

_time ↕	user ↕	ip ↕	threat ↕	severity ↕
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware Behavior	Critical
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware Behavior	Critical
2025-07-03 07:51:14	eve	10.0.0.5	Rootkit Signature	Critical
2025-07-03 07:51:14	eve	10.0.0.5	Rootkit Signature	Critical
2025-07-03 07:45:14	charlie	172.16.0.3	Trojan Detected	High
2025-07-03 07:45:14	charlie	172.16.0.3	Trojan Detected	High
2025-07-03 05:48:14	bob	10.0.0.5	Trojan Detected	High
2025-07-03 05:48:14	bob	10.0.0.5	Trojan Detected	High
2025-07-03 05:45:14	david	172.16.0.3	Trojan Detected	High
2025-07-03 05:45:14	david	172.16.0.3	Trojan Detected	High
2025-07-03 05:42:14	eve	203.0.113.77	Trojan Detected	High

## Trojan Detected

**User:** Charlie

**Time:** 07:45:14

**Date:** 2025-7-3

**IP Address:** 172.16.0.3

**Severity:** High

- Suggests shared asset or machine may be infected with multiple threats.
  - **Risk:** Command-and-control, data theft.
-

## Failed Login Attempts:

#	Time	Event
>	7/3/25 9:02:14.000 AM	2025-07-03 09:02:14   user=david   ip=203.0.113.77   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = imp_log
>	7/3/25 9:02:14.000 AM	2025-07-03 09:02:14   user=david   ip=203.0.113.77   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = imp_log
>	7/3/25 9:02:14.000 AM	2025-07-03 09:02:14   user=david   ip=203.0.113.77   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = implogs
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14   user=alice   ip=203.0.113.77   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = imp_log
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14   user=alice   ip=203.0.113.77   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = imp_log
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14   user=alice   ip=203.0.113.77   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = implogs
>	7/3/25 4:47:14.000 AM	2025-07-03 04:47:14   user=bob   ip=10.0.0.5   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = imp_log
>	7/3/25 4:47:14.000 AM	2025-07-03 04:47:14   user=bob   ip=10.0.0.5   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = imp_log
>	7/3/25 4:47:14.000 AM	2025-07-03 04:47:14   user=bob   ip=10.0.0.5   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = implogs
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14   user=bob   ip=172.16.0.3   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = imp_log
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14   user=charlie   ip=198.51.100.42   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = imp_log
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14   user=bob   ip=172.16.0.3   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = imp_log
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14   user=bob   ip=172.16.0.3   action=login failed host = LAPTOP-PCRSSH10   source = imp-log.txt   sourcetype = implogs

User	IP	Attempts	Risk
Bob	10.0.0.5, 172.16.0.3	2	Medium
Charlie	198.51.100.42	1	Medium
Alice	203.0.113.77	1	Medium
David	203.0.113.77	1	Medium

## Impact Assessment:

AREA	IMPACT DESCRIPTION
User affected	bob, alice, david, charlie, eve
System affected	10.0.0.5, 172.16.0.3, 198.51.100.42, 203.0.113.77
Threat Types	Ransomware behaviour, Trojan, Rootkit
Data Risk	Possible unauthorized access or data encryption
Persistence Risk	Rootkits could allow long-term stealth access

## Root Cause:

---

1. Malware entered the network through either email, USB, or external login attempts.
2. Users logged in from suspicious IPs before or after malware activity.
3. The shared IP **172.16.0.3** was used by two infected users and shows signs of being the infection hub → Bob and Charlie.

## Mitigation & Remediation Actions:

---

1. Isolated affected systems: **172.16.0.3** and **10.0.0.5**
2. Disabled user accounts: bob, charlie, eve
3. Alerted IT and SOC teams for rapid response

## Suggested Next Steps:

---

ACTIONS	PRIORITY
Full malware and rootkit scan on endpoints	High
Review access logs and login history	High
Reimage infected machines	High
Patch systems and update antivirus tools	Medium
Reset passwords for affected users	High
Create Splunk alerts for malware + failed logins	High

---



## **Stakeholder Communication:**

---

On July 3, 2025, a coordinated malware campaign targeting multiple internal users was detected via Splunk. Affected users include bob, charlie, and alice, with malware types ranging from trojans to ransomware. We are taking immediate containment steps and will conduct a full investigation and system patching. IT is advised to prioritize remediation, while users are urged not to access suspicious links or files until the incident is closed.

— **SOC Analyst, Future Interns Security Team**