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:

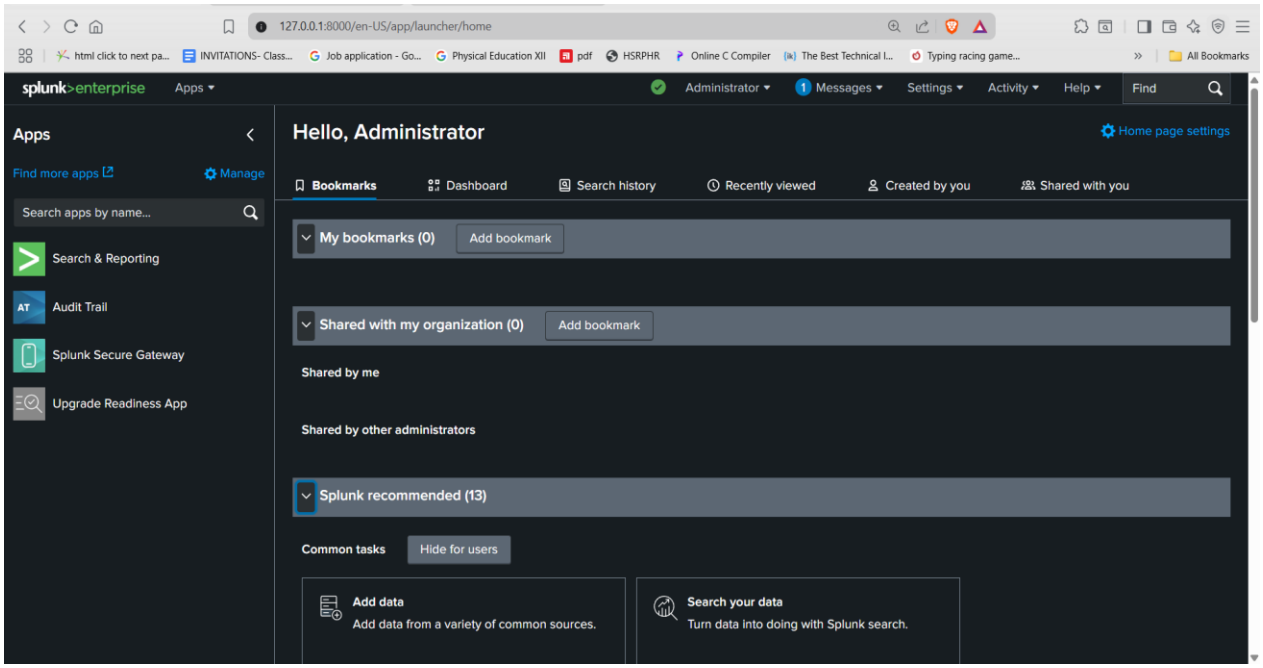
Splunk App are the applications which monitor web servers, analyze network security, or manage applications. They consist of various knowledge objects like saved searches, reports, alerts, dashboards, and datasets, along with other configurations like lookups and event types.

SPL: SEARCH PROCESSING LANGUAGE

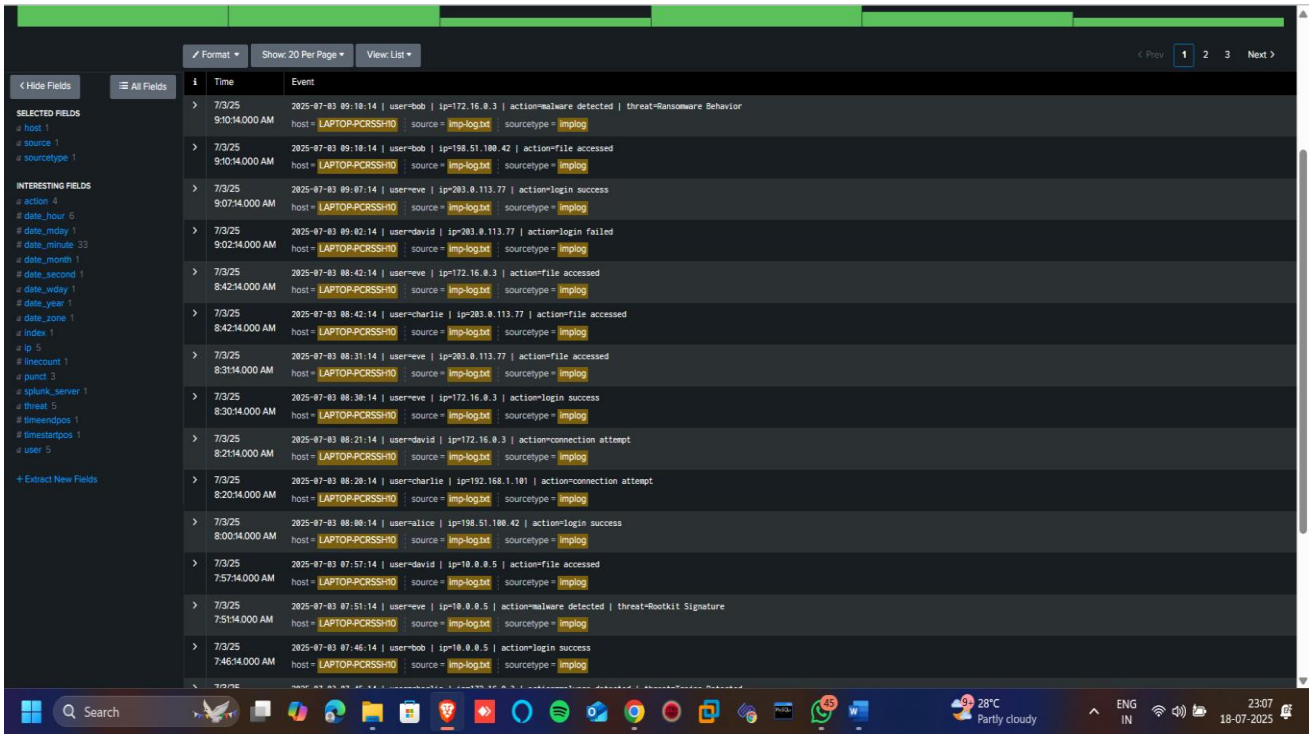
Is a query language used to search, analyze, and visualize data within the Splunk platform. It's not a traditional programming language, but rather a way to interact with and manipulate data stored in Splunk's indexes.

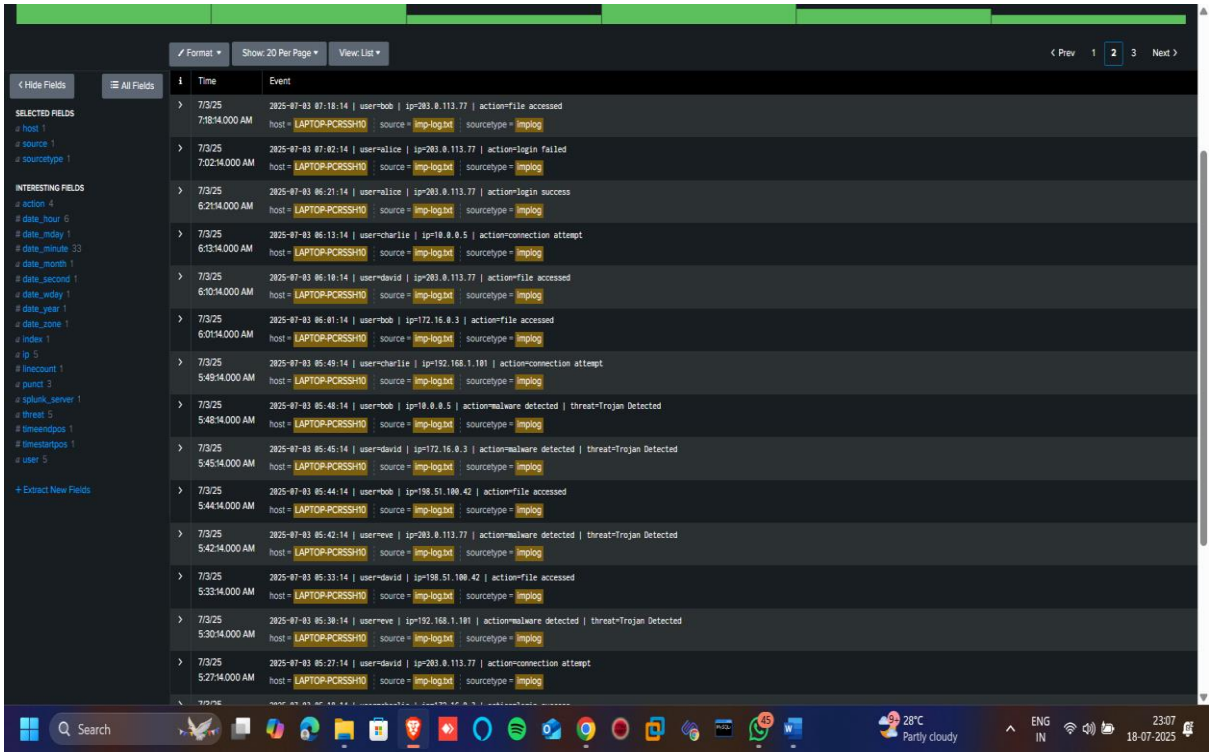
Security Incident Report

Splunk Enterprise >:

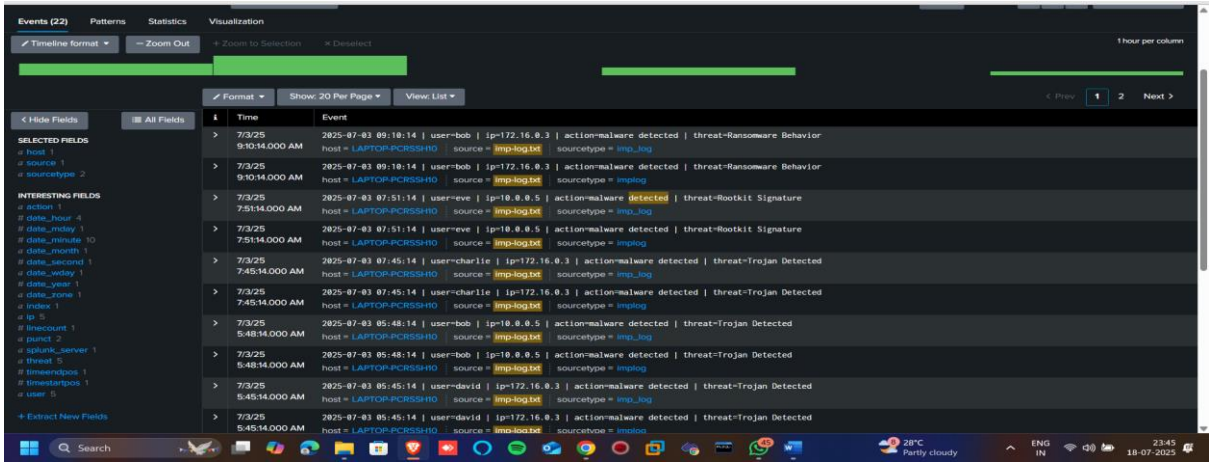


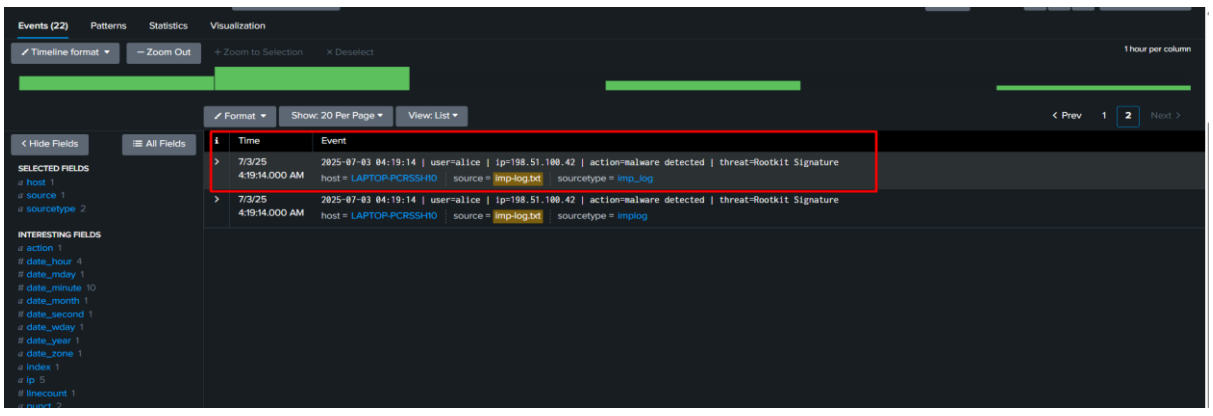
The log data:





Security Alerts and logs (Malware Detected):





Rootkit Signature

User: Alice

Time: 4:19:14

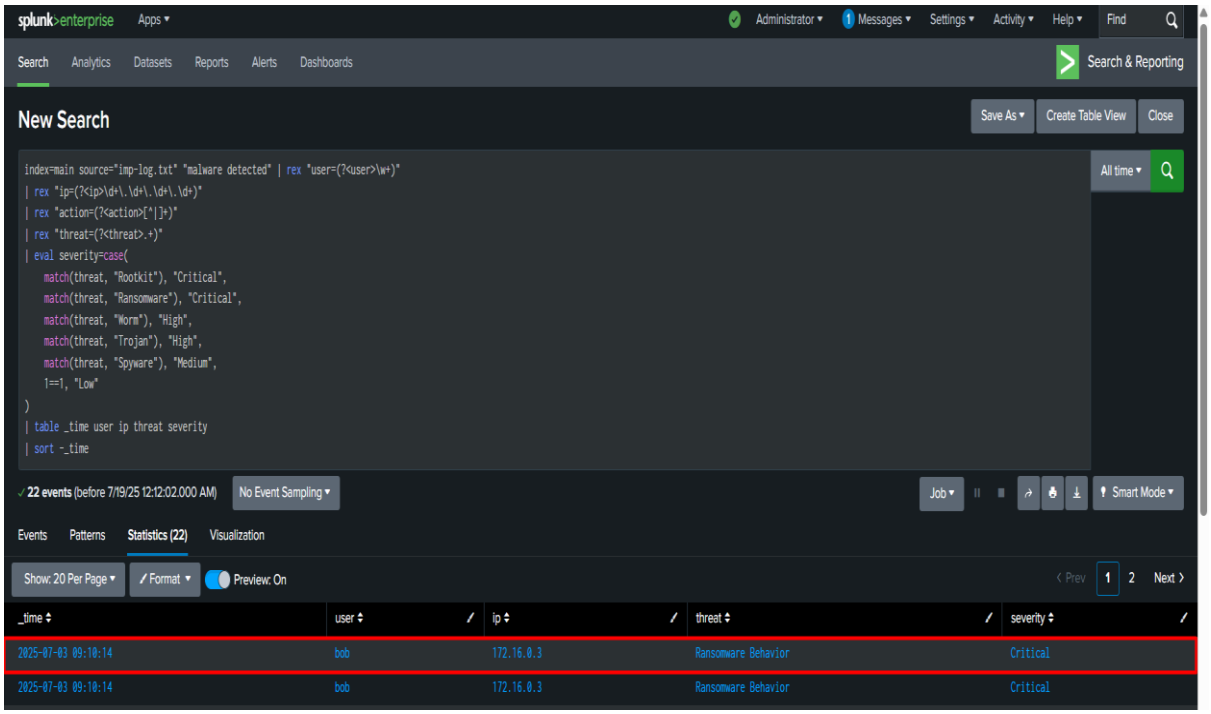
Date: 2025-7-3

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.



Ransomware Behaviour

User: BOB

Time: 9:10:14

Date: 2025-7-3

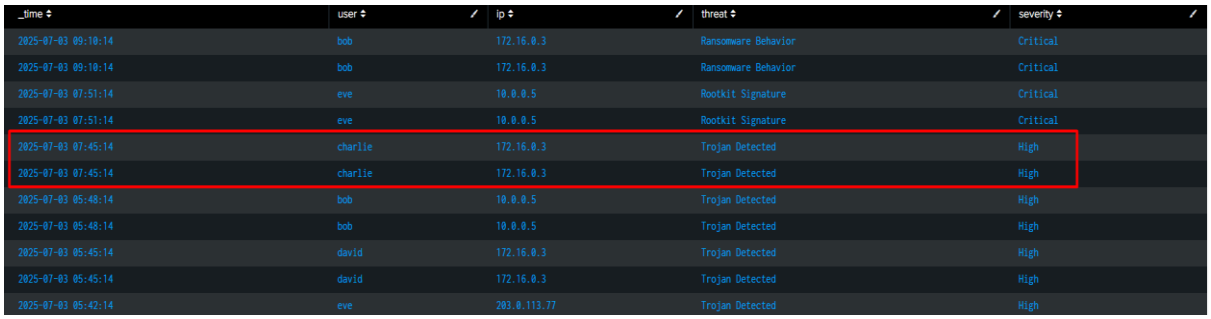
IP Address: 172.16.0.3

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

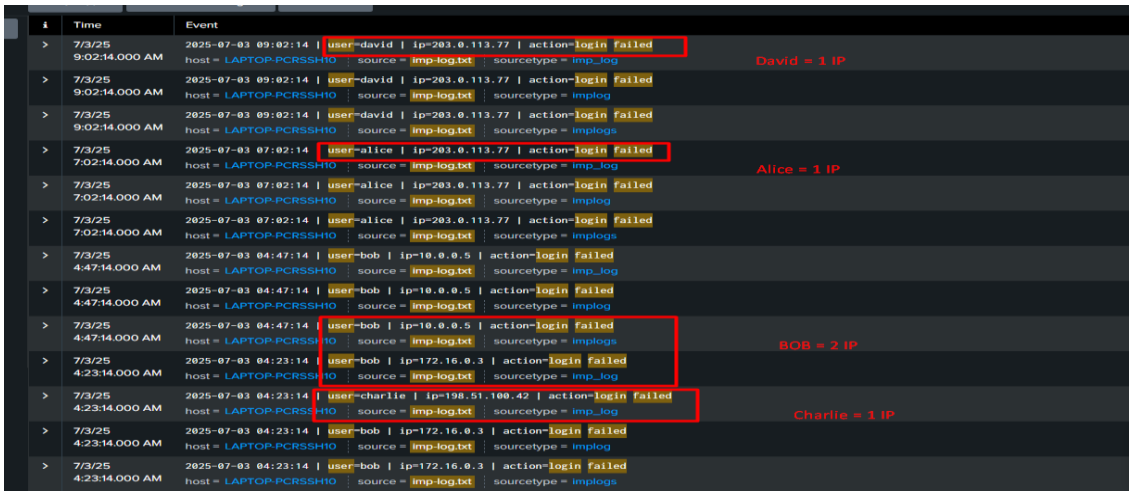
Date: 2025-7-3

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:



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**