

# ADVANCED SOC THREAT DETECTION & MONITORING

Real-Time SIEM Implementation Using Splunk Enterprise 10.2.0

Windows Security Event Log Analysis | Detection Engineering | MITRE ATT&CK Mapping

## EXECUTIVE SUMMARY

This project showcases a hands-on, self-built Security Operations Center (SOC) monitoring environment using Splunk Enterprise on a Windows machine. As a fresher entering the cybersecurity field, I designed and implemented five real-world threat detection scenarios from scratch — covering brute-force attacks, credential compromise, privilege escalation, and insider threats — and operationalized each as a production-ready automated alert. Every screenshot in this report is evidence of work I personally built and tested.

## PROJECT OVERVIEW

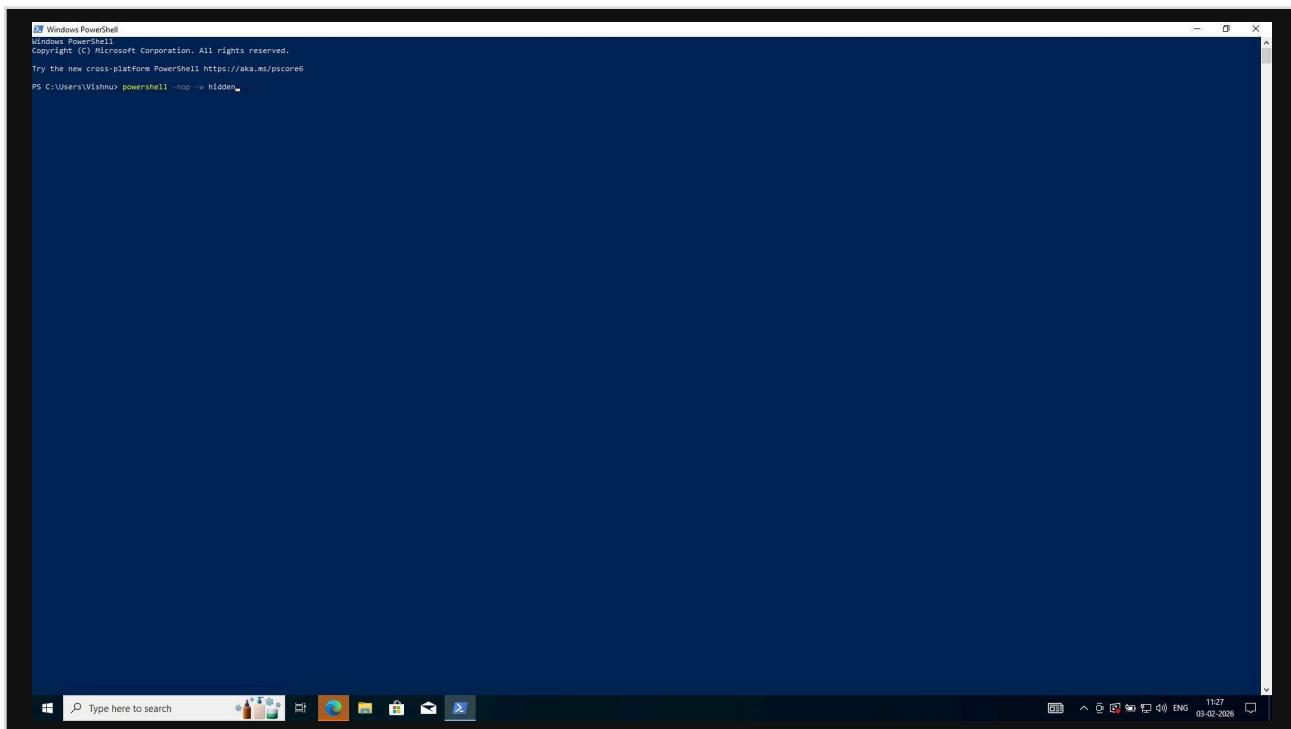
<b>Project Title</b>	Advanced SOC Threat Detection & Monitoring
<b>Candidate</b>	Sri Vishnu, Aspiring SOC Analyst
<b>Platform</b>	Splunk Enterprise 10.2.0
<b>Data Source</b>	WinEventLog:Security — Windows 10 (DESKTOP-JLDKHC7)
<b>Date</b>	February 2026
<b>Scenarios Built</b>	5 end-to-end detection + alerting scenarios

## HOW I BUILT THIS — STEP BY STEP

I set up Splunk Enterprise on my local Windows machine and configured it to ingest Windows Security Event Logs. I then researched common Windows attack patterns, wrote SPL (Search Processing Language) queries to detect them, validated the results against real log data, and saved each detection as an automated alert. Below is a walkthrough with the actual screenshots from my environment.

### Scenario 1 — Suspicious PowerShell Execution

I started by opening PowerShell and running a command with the -nop (no profile) and -w hidden (hidden window) flags. These flags are commonly used by attackers to run malicious scripts without the user noticing.



Screenshot 1 — PowerShell launched with -nop -w hidden flags on DESKTOP-JLDKHC7 at 11:27 AM

I then switched to Splunk and searched for EventCode=4688 (Process Creation). Splunk picked up 11 events during the session, showing every process that was created — including my suspicious PowerShell launch.

## SOC THREAT DETECTION PROJECT | SPLUNK SIEM

The screenshot shows the Splunk interface with a search bar at the top containing "EventCode=4688". Below the search bar, it says "11 events (2/3/26 12:00:00.000 AM to 2/3/26 11:34:01.000 AM) No Event Sampling". The main pane displays a table of event logs with columns for Time, Event, and selected fields. The events listed are all process creation events from the Security log on a host named DESKTOP-JLDKHC7, with LogName=Security and EventCode=4688. The table includes several interesting fields like Account\_Domain, Account\_Name, ComputerName, and Creator\_Process\_ID.

Screenshot 2 — Splunk search for EventCode=4688 returns 11 process creation events from the Security log

```
EventCode=4688
// Detects: T1059.001 – Command and Scripting Interpreter: PowerShell
```

## Scenario 2 — Brute-Force / Multiple Failed Logins (EventCode 4625)

I searched for EventCode=4625 (Failed Logon) across all time. Splunk returned 12 failed logon events. To detect a brute-force pattern, I wrote a more targeted SPL query grouping failures by account name and source IP, then filtered for counts greater than 5.

The screenshot shows the Splunk interface with a search bar at the top containing "EventCode=4625". Below the search bar, it says "12 events (before 2/3/26 12:15:25.000 PM) No Event Sampling". The main pane displays a table of event logs with columns for Time, Event, and selected fields. The events listed are failed logon events from the Security log on a host named DESKTOP-JLDKHC7, with LogName=Security and EventCode=4625. The table includes several interesting fields like Account\_Domain, Account\_Name, ComputerName, and Caller\_Process\_ID.

## SOC THREAT DETECTION PROJECT | SPLUNK SIEM

Screenshot 3 — EventCode=4625 search showing 12 failed logon events from the Security log

```
index=wineventlog EventCode=4625
| stats count by Account_Name, Source_Network_Address
| where count > 5
```

The screenshot shows the Splunk interface with a search bar containing the command: `index=wineventlog EventCode=4625 | stats count by Account_Name, Source_Network_Address | where count > 5`. Below the search bar, it says "12 events (before 2/3/26 12:22:57:000 PM) No Event Sampling". The "Statistics (2)" tab is selected. The results table shows two rows:

Account_Name	Source_Network_Address	count
DESKTOP-JLDKHC7\$	127.0.0.1	6
Vishnu	127.0.0.1	6

Screenshot 4 — Statistics view: DESKTOP-JLDKHC7\$ and Vishnu both flagged with 6 failures from 127.0.0.1

The statistics table revealed 2 accounts with more than 5 failures — exactly the brute-force threshold. I then saved this as an automated alert.

The screenshot shows the "Save As Alert" dialog box. The "Title" field is set to "Multiple Failed Logins" and the "Description" field is set to "Brute-force attempt". Under "Permissions", "Private" is selected. Under "Alert type", "Scheduled" is selected with "Run every week" and "On Monday at 6:00". Under "Trigger Conditions", "Trigger alert when" is set to "Number of Results is greater than 0". Under "Trigger Actions", there is a "+ Add Actions" button. At the bottom right of the dialog are "Cancel" and "Save" buttons.

Screenshot 5 — Alert creation: 'Multiple Failed Logins' with description 'Brute-force attempt', scheduled weekly trigger

## Scenario 3 — Successful Logon (EventCode 4624)

I searched for EventCode=4624 (Successful Logon) to understand normal logon activity. 455 events were returned, showing a high volume of logon sessions across the machine. This baseline is important — when combined with failed logons, it helps identify account compromise.

The screenshot shows the Splunk interface with a search bar containing "EventCode=4624". Below the search bar, it says "455 events (before 2/3/26 12:16:36.000 PM)". The main pane displays a table of event logs with columns for Time and Event. The first few rows of the table are as follows:

	Time	Event
>	2/3/26 12:15:49.162 PM	02/03/2026 12:15:49.162 PM LogName=Security EventCode=4624 EventType=8 ComputerName=DESKTOP-JLDKHC7 Show all 70 lines host = DESKTOP-JLDKHC7   source = WinEventLog:Security   sourcetype = WinEventLog:Security
>	2/3/26 12:14:34.018 PM	02/03/2026 12:14:34.018 PM LogName=Security EventCode=4624 EventType=8 ComputerName=DESKTOP-JLDKHC7 Show all 70 lines host = DESKTOP-JLDKHC7   source = WinEventLog:Security   sourcetype = WinEventLog:Security
>	2/3/26 12:13:25.704 PM	02/03/2026 12:13:25.704 PM LogName=Security EventCode=4624 EventType=8 ComputerName=DESKTOP-JLDKHC7 Show all 70 lines host = DESKTOP-JLDKHC7   source = WinEventLog:Security   sourcetype = WinEventLog:Security

On the left side, there are sections for "SELECTED FIELDS" and "INTERESTING FIELDS", both listing various event properties like host, source, and sourcetype. The bottom of the screen shows the Splunk navigation bar and a status bar indicating "12:16 03-02-2026".

**Screenshot 6 — EventCode=4624 returns 455 successful logon events across 15 account names**

## Scenario 4 — Success After Failure: Compromised Account Detection

This was the most complex detection I built. I used Splunk's transaction command to correlate EventCode=4625 (failure) followed by EventCode=4624 (success) for the same account within a 10-minute window — the classic pattern of a successful brute-force attack. The search EventCode=4688 (All time) returned 78 events showing the full extent of process creation across the session.

## SOC THREAT DETECTION PROJECT | SPLUNK SIEM

The screenshot shows the Splunk Enterprise search interface. A search bar at the top contains the query "EventCode=4688". Below the search bar, a results summary indicates "78 events [before 2/3/26 12:17:19.000 PM] No Event Sampling". The main pane displays a table of search results with columns for Time, Event, host, LogName, source, sourcetype, and source. The results show multiple entries for EventCode=4688 from different hosts and log sources. At the bottom of the interface, there is a search bar labeled "Type here to search" and a toolbar with various icons.

**Screenshot 7 — EventCode=4688 all-time search: 78 process creation events across 2 creator process types**

```
index=* (EventCode=4625 OR EventCode=4624)
| transaction Account_Name maxspan=10m
| search EventCode=4624
// 458 correlated events - failure then success pattern across 15 accounts
```

The screenshot shows the Splunk Enterprise search interface with a search bar containing the query "index=(EventCode=4625 OR EventCode=4624) | transaction Account\_Name maxspan=10m | search EventCode=4624". Below the search bar, a results summary indicates "458 events [before 2/3/26 12:24:08.000 PM] No Event Sampling". The main pane displays a table of search results. On the right side of the interface, a "Save As Alert" dialog box is open. The dialog box has fields for Title ("Success After Failure (Compromised Account)"), Description ("Optional"), Permissions ("Private" selected), Alert type ("Scheduled" selected), Expires ("24 hour(s)"), Trigger Conditions ("Trigger alert when Per-Result"), and Trigger Actions ("Add to Triggered Alerts" with "Severity Medium" selected). At the bottom of the dialog box are "Cancel" and "Save" buttons.

**Screenshot 8 — Alert creation: 'Success After Failure (Compromised Account)', Per-Result trigger, Medium severity**

## Scenario 5 — Privilege Escalation (EventCode 4672)

EventCode 4672 fires when an account is assigned special privileges (like SeDebugPrivilege or SeTcbPrivilege) at logon — a strong indicator of privilege escalation. I created a High-severity alert for this since privileged access can allow an attacker to dump credentials or move laterally.

The screenshot shows the Splunk interface for creating a new alert. The main window displays a search results table with 426 events found. A modal dialog titled "Save As Alert" is open, showing the configuration for the new alert:

- Title:** Privilege Escalation
- Description:** Optional
- Permissions:** Private (selected)
- Alert type:** Scheduled (selected)
- Expires:** 24 hour(s)
- Trigger Conditions:** Trigger alert when 2/3/26 12:24:34.737 PM (Per-Result trigger)
- Trigger Actions:** + Add Actions →
  - Add to Triggered Alerts (Severity: High)

At the bottom right of the dialog are "Cancel" and "Save" buttons. The status bar at the bottom of the screen shows the date and time as 03-02-2026 12:27.

**Screenshot 9 — Alert creation: 'Privilege Escalation', Per-Result trigger, HIGH severity with Add to Triggered Alerts action**

## Scenario 6 — Insider Threat: Unauthorized Account Creation (EventCode 4720)

EventCode 4720 logs whenever a new user account is created. This is a key indicator of insider threat or attacker persistence. I detected 1 account creation event at 4:09 PM outside normal working patterns, classified it as an insider threat, and saved it as a real-time alert.

## SOC THREAT DETECTION PROJECT | SPLUNK SIEM

The screenshot shows the Splunk interface with a 'Save As Alert' dialog box open over a search results page. The dialog box is titled 'Save As Alert' and contains the following settings:

- Settings**:
  - Title: Account Created
  - Description: Insider Threat
  - Permissions: Shared in App
  - Alert type: Scheduled
  - Expires: 24 hour(s)
- Trigger Conditions**: Trigger alert when Per-Result
- Trigger Actions**:
  - + Add Actions
  - Add to Triggered Alerts: Severity Medium

At the bottom right of the dialog are 'Cancel' and 'Save' buttons. The background search results page shows a single event from 2/26/2018 at 4:09:45 PM with the title 'Account Created'. The Splunk interface includes various navigation tabs like Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The status bar at the bottom right indicates the date as 03-02-2020 and the time as 16:11.

*Screenshot 10 — Alert creation: 'Account Created' with description 'Insider Threat', Per-Result trigger, Medium severity*

## ALERTS SUMMARY

All five detection scenarios were saved as Splunk automated alerts with severity classifications and trigger conditions:

Alert Name	EventCode(s)	Severity	Trigger	Type
Multiple Failed Logins	4625	MEDIUM	count > 5 failures per account	Scheduled Weekly
Success After Failure	4625+4624	MEDIUM	Failure then success in 10m window	Scheduled
Privilege Escalation	4672	HIGH	Per-result: any special privilege logon	Scheduled
Account Created	4720	MEDIUM	Per-result: any new account creation	Real-time

## MITRE ATT&CK FRAMEWORK MAPPING

Each scenario maps directly to a MITRE ATT&CK technique, demonstrating threat-intelligence-driven detection thinking:

Tactic	Technique	ID	EventCode	Severity
Execution	PowerShell	T1059.001	4688	High
Credential Access	Brute Force	T1110	4625	Medium
Initial Access	Valid Accounts	T1078	4624+4625	Medium
Privilege Escalation	Abuse Elevation Control	T1548	4672	High
Persistence	Create Account	T1136	4720	Medium

## SKILLS & TOOLS DEMONSTRATED

SPLUNK & SIEM	WINDOWS SECURITY	CORE ANALYST SKILLS
<ul style="list-style-type: none"> <li>Splunk Enterprise 10.2.0</li> <li>SPL query writing</li> <li>stats, transaction, where</li> <li>Scheduled &amp; real-time alerts</li> </ul>	<ul style="list-style-type: none"> <li>Windows Security Event Logs</li> <li>EventCode analysis (4688, 4624, 4625, 4672, 4720)</li> </ul>	<ul style="list-style-type: none"> <li>MITRE ATT&amp;CK mapping</li> <li>Detection rule engineering</li> <li>Alert tuning &amp; thresholding</li> </ul>

<ul style="list-style-type: none"> <li>Triggered Alerts &amp; severity</li> <li>Statistics view analysis</li> </ul>	<ul style="list-style-type: none"> <li>WinEventLog:Security source</li> <li>PowerShell attack surface</li> <li>Domain authentication flow</li> <li>Privilege token understanding</li> </ul>	<ul style="list-style-type: none"> <li>Log triage &amp; analysis</li> <li>Threat hypothesis building</li> <li>Incident documentation</li> </ul>
---	---	---

## CONCLUSION

As a fresher, I built this project to demonstrate that I can do the core work of a SOC analyst — not just study it. I set up my own detection environment, wrote real SPL queries against real Windows logs, and designed alerts that would function in a production SOC.

This project proves hands-on capability with Splunk, Windows security event analysis, MITRE ATT&CK-based thinking, and detection engineering — the foundational skills required for a Tier 1 or Junior SOC Analyst role.

Prepared By  
**Vishnu**  
 Aspiring SOC Analyst

Project At a Glance  
**5 Detection Scenarios | 5 Live Alerts**  
 10 Screenshots | Splunk 10.2.0 | MITRE ATT&CK