

SOC Alert Triage & Brute Force Detection

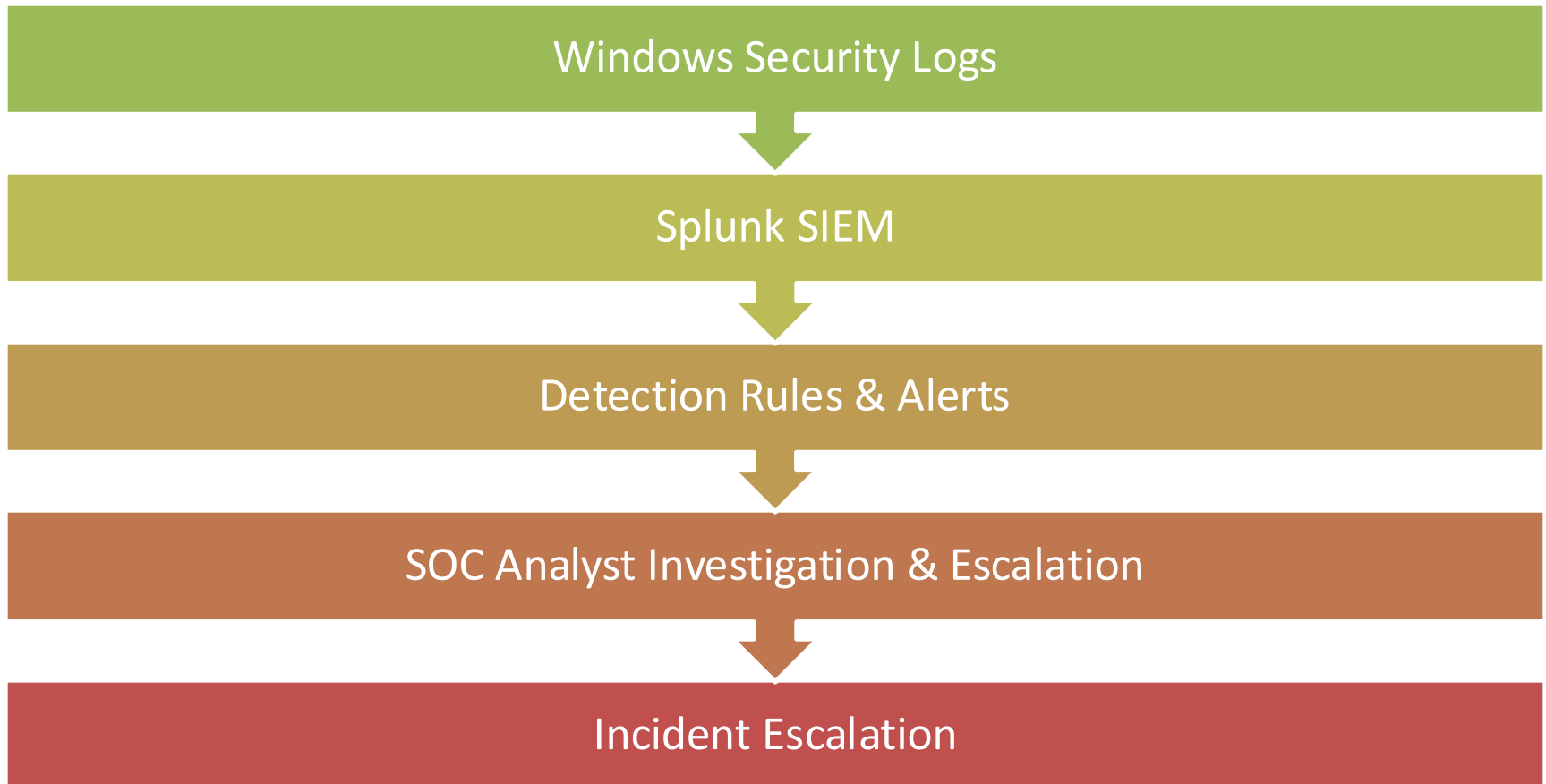
Hands-on SOC L2 Project using Splunk

Sangram Rajput

Project Objectives

- Detect brute-force authentication attacks using Splunk
- Perform alert triage and in-depth investigation
- Classify incident severity and determine escalation
- Simulate real-world SOC L2 workflow

Lab Architecture



SELECTED FIELDS	
<i>a</i> host	2
<i>a</i> source	10
<i>a</i> sourcetype	8
INTERESTING FIELDS	
<i>a</i> Account_Domain	10
<i>a</i> Account_Name	28
<i>a</i> ComputerName	3
# EventCode	100+
# EventType	5
<i>a</i> index	1
# Keywords	12
# linecount	37
<i>a</i> LogName	3
<i>a</i> Logon_ID	87
<i>a</i> Message	100+
<i>a</i> OpCode	10
<i>a</i> Process_ID	100+
<i>a</i> Process_Name	15
<i>a</i> punct	100+
# RecordNumber	100+
<i>a</i> Security_ID	38
<i>a</i> SourceName	88
<i>a</i> splunk_server	1
<i>a</i> TaskCategory	57
<i>a</i> Type	4
217 more fields	
+ Extract New Fields	

i	Time	Event
	21:18:10.679	collection="CPU Load" object=Processor counter="% User Time" instance=_Total Show all 6 lines host = Edith source = Perfmon:CPU Load sourcetype = Perfmon:CPU Load
>	09/02/2026 21:18:10.679	02/09/2026 21:18:10.679 +0530 collection="CPU Load" object=Processor counter="% Processor Time" instance=_Total Show all 6 lines host = Edith source = Perfmon:CPU Load sourcetype = Perfmon:CPU Load
>	09/02/2026 21:18:10.663	02/09/2026 21:18:10.663 +0530 collection="Network Interface" object="Network Interface" counter="Bytes Sent/sec" instance="Intel[R] Dual Band Wireless-AC 8265" Show all 6 lines host = Edith source = Perfmon:Network Interface sourcetype = Perfmon:Network Interface
>	09/02/2026 21:18:10.663	02/09/2026 21:18:10.663 +0530 collection="Network Interface" object="Network Interface" counter="Bytes Received/sec" instance="Intel[R] Dual Band Wireless-AC 8265" Show all 6 lines host = Edith source = Perfmon:Network Interface sourcetype = Perfmon:Network Interface

Log Ingestion

- Installed Splunk Enterprise
- Ingested Windows Security logs
- Validated authentication events (Event ID 4625)

.....
.....
.....
.....

.....
.....
.....
.....

src_ip ↕	Account_Name ↕	_time ↕
103.45.77.201	admin	2026-02-08 12:00
103.45.77.201	administrator	2026-02-08 12:00
103.45.77.201	backup	2026-02-08 12:00
103.45.77.201	guest	2026-02-08 12:00
103.45.77.201	sqlsvc	2026-02-08 12:00
103.45.77.201	testuser	2026-02-08 12:00

Brute Force Detection

- Analyzed failed login attempts
- Detected brute-force and password spray patterns
- Used time-based threshold logic

Multiple Failed Login Attempts – Possible Brute Force

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by sam. [Edit](#)

Modified: 8 Feb 2026 20:19:01

Alert Type: Real-time. [Edit](#)

Trigger Condition: .. Per-Result. [Edit](#)

Actions: [▼](#) 1 Action [Edit](#)

 Add to Triggered Alerts

Alert Creation

- Scheduled Splunk alert
- Triggered on multiple failed logins
- Severity set to Medium

Incident Case

Incident id : SOC-Brute-001

Incident type : Brute Force Authentication Attempt

Source IP : "103.45.77.201"

Targeted Accounts : ([administrator](#), [admin](#), [guest](#))

Time Windows : "12:00-12:02"

Detected By : Splunk SIEM Alert

Status : under Investigation

Incident Case Selection

- Incident ID: SOC-BRUTE-001
- Incident Type: Brute Force Authentication Attempt
- Source IP, Target Account, Time Window

_time ↕	EventCode ↕ ↗	Account_Name ↕ ↗	src_ip ↕ ↗	host ↕ ↗
2026-02-08 12:00:00	4625	administrator	103.45.77.201	Edith
2026-02-08 12:00:15	4625	admin	103.45.77.201	Edith
2026-02-08 12:00:30	4625	guest	103.45.77.201	Edith
2026-02-08 12:00:45	4625	testuser	103.45.77.201	Edith
2026-02-08 12:01:00	4625	backup	103.45.77.201	Edith
2026-02-08 12:01:15	4625	sqlsvc	103.45.77.201	Edith

Investigation & Evidence

- Investigated attacker IP activity
- Correlated failed login events
- Checked for successful authentication

Security Classification Table

<u>Condition</u>	<u>Observed</u>	<u>Severity</u>
External IP	✓	↑
Multiple failed Attempts	✓	↑
Multiple users Targeted	✓	↑
User Mistake	✗	↑
Successful login	✗	↓

Final Security : Medium

Severity & Escalation

- External IP with repeated attempts
- No successful login observed
- Final Severity: MEDIUM
- Escalated to SOC L2 / IR Team

Risk Impact: Account compromise risk if attack succeeds

Incident Report

Incident Summary :

Multiple failed login attempts detected from an external IP targeted a Windows account, indicating a potential brute-force attack.

Time Line :

- Initial attempt : "2026-02-08 12:00:00"
- Alert Triggred : "2026-02-08 12:05:00"
- Investigation Completed : "2026-02-08 01:45:00"

Affected Assets :

- Host : "Edith"
- Accounts : ([administrator](#), [admin](#), [backup](#), [guest](#), [testuser](#))

Indicators of Compromise (IOCs) :

- Source IP : "103.45.77.201"
- Event IDs : "[4625](#)"

Analysts Actions :

- Reviewed authentications logs
- Correlated failed login attempts
- Verified no successful authentication
- Classified severity and escalated

Recommendations :


- Block attacker IP at firewall
- Enforce account lockout policy
- Enable MFA
- Monitor authentication Logs

Incident Report & Recommendations

- Documented investigation and findings
- Blocked malicious IP
- Recommended MFA and lockout policy



Skills Demonstrated

- Splunk SIEM
 - Windows Security Log Analysis
 - Brute-Force & Password Spray Detection
 - Alert Triage & Incident Escalation
 - SOC Documentation & Reporting
- 



Thank You !

For queries or walk-through, feel free to ask



Prepared by: Sangram Rajput