SOC Alert Triage & Brute Force Detection

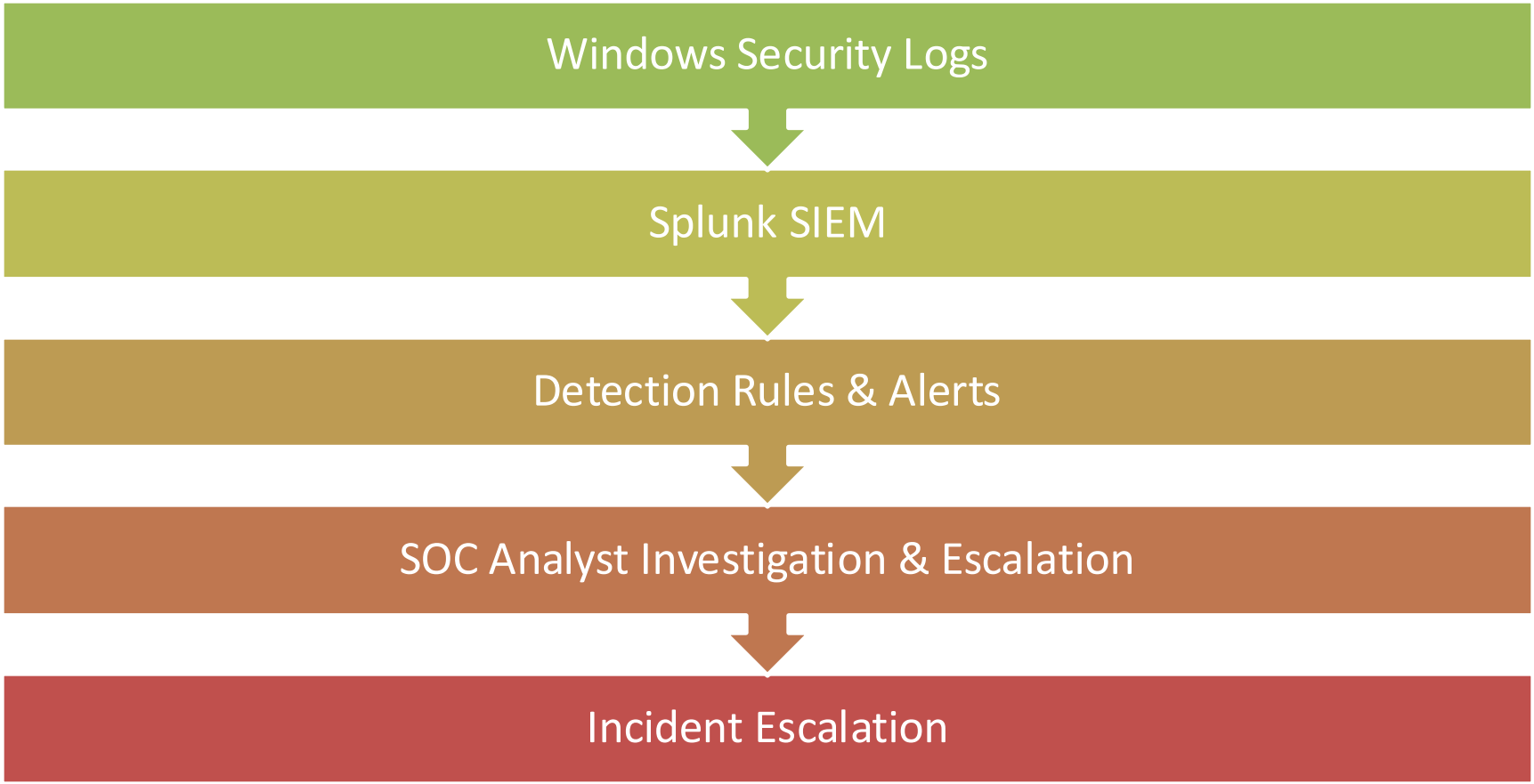
Hands-on SOC L2 Project using Splunk

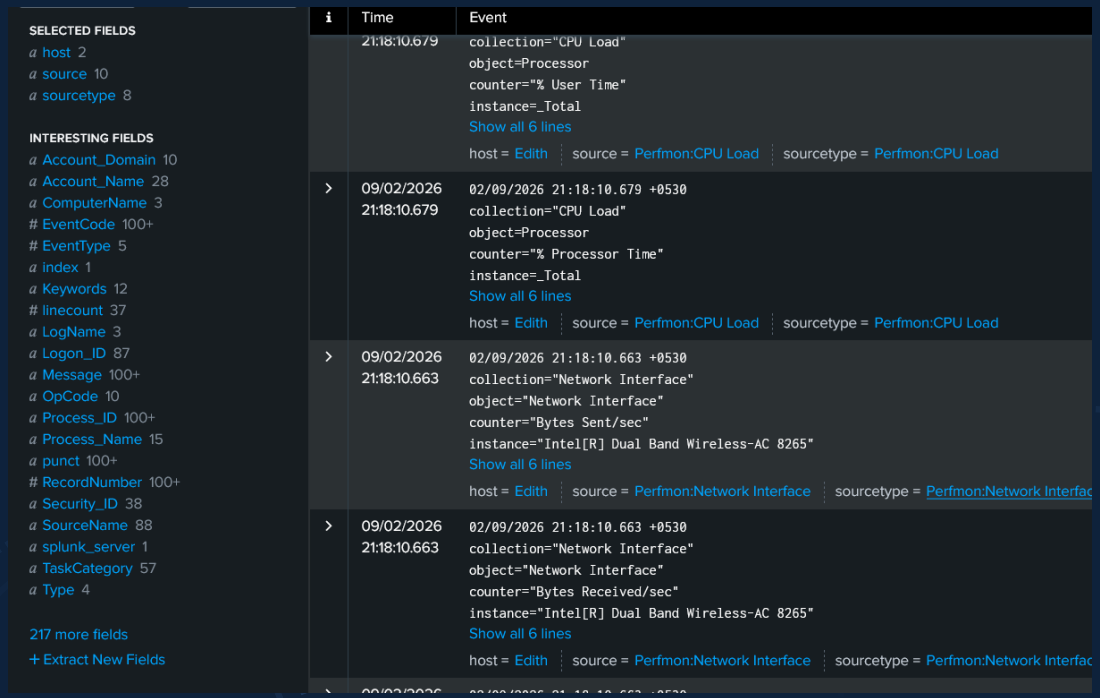
Sangram Rajput

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





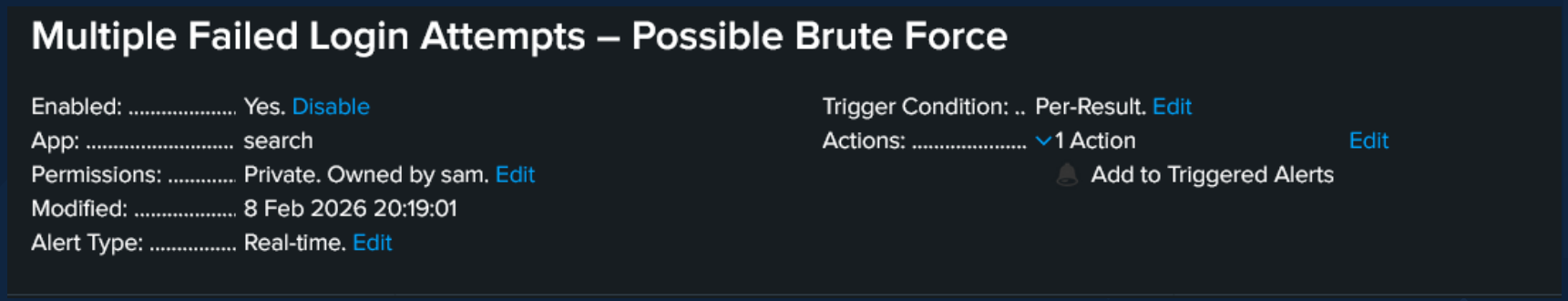
Log Ingestion

- 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



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

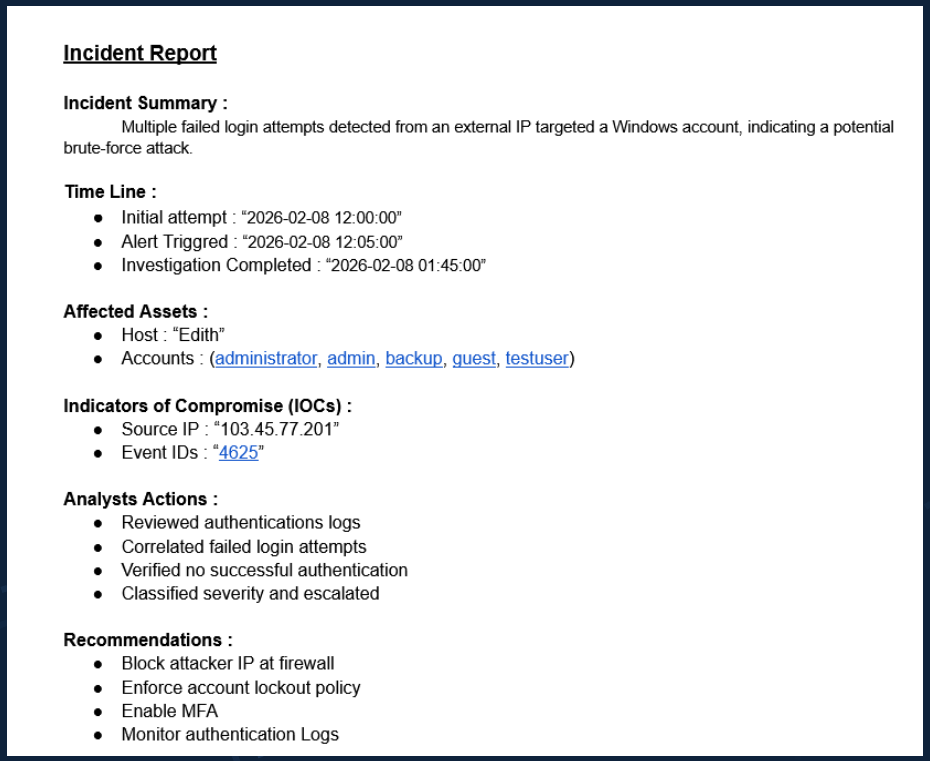
Condition	Observed	Severity
External IP	✔	⬆
Multiple failed Attempts	✔	⬆
Multiple users Targeted	✔	⬆
User Mistake	✘	⬆
Successful login	✘	⬇

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