Automated SOC Alerting Workflow

Splunk • n8n • Chat GPT • AbuseIPDB • Slack

Author: A. Brito

Date: October 2025

1. Executive Summary

This lab demonstrates the automation of security alert triage using **Splunk**, **n8n**, **OpenAI** (**ChatGPT**), **AbuseIPDB**, and **Slack**. When suspicious activity is detected on a Windows 10 endpoint, Splunk generates an alert, which is then sent to n8n through a webhook. ChatGPT analyzes the log data for Indicators of Compromise (IOCs), AbuseIPDB enriches the data with IP reputation scores, and a structured alert is automatically delivered to Slack. This workflow closely simulates a real-world SOC (Security Operations Center) environment, enhancing speed, accuracy, and context in alert triage.

2. Architecture Overview

• **Windows 10 Endpoint:** Generates Windows Security Events (logon attempts)

• **Splunk Enterprise:** Collects and indexes logs from the endpoint.

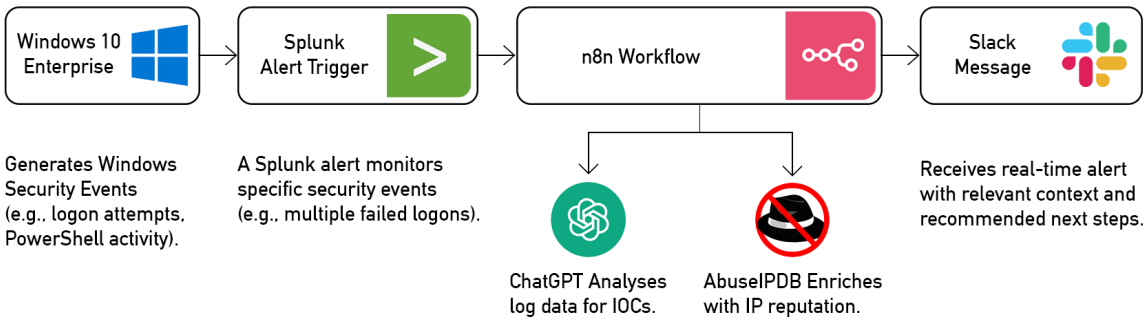
• **Alert Trigger:** A Splunk alert monitors specific security events (e.g., multiple failed logons).

• **n8n Workflow:** Receives Splunk alert payload via webhook → sends log data to ChatGPT for analysis → enriches IP reputation with AbuseIPDB → sends structured alert to Slack.

• **AbuseIPDB:** Provides reputation intelligence for public IPs, helping identify high-risk sources quickly.

• **Slack:** Receives real-time alert with relevant context, IOC enrichment, and recommended next steps.

Lab Diagram



3. Splunk Configuration

• **Data Source:** Windows Security Event Logs (WinEventLog).

• **Search Query:**

```
index="n8n-project" EventCode=4625
| stats count by _time, ComputerName, user, src_ip
```

• **Alert Description:** Triggers on Windows Event ID 4625 (failed logon attempts) to detect brute force or unauthorized access attempts.

• **Alert Condition:** Trigger when event count ≥ 1 in 2 minutes.

• **Action:** Webhook to n8n, sending src_ip, ComputerName, user, and _time.

4. n8n Workflow

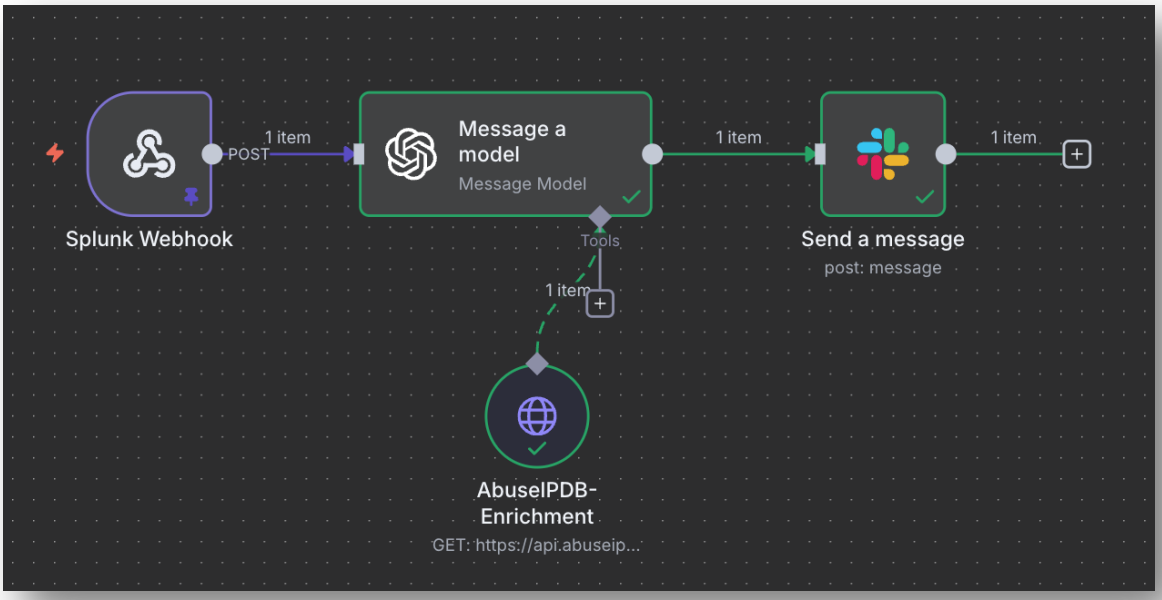
• **Trigger Node:** Webhook receives Splunk alert payload.

• **OpenAI (ChatGPT) Node:** Analyzes event log for Indicators of Compromise (IOCs) and severity level.

• **AbuseIPDB Node:** Enriches public IP addresses with threat scores and reputation details.

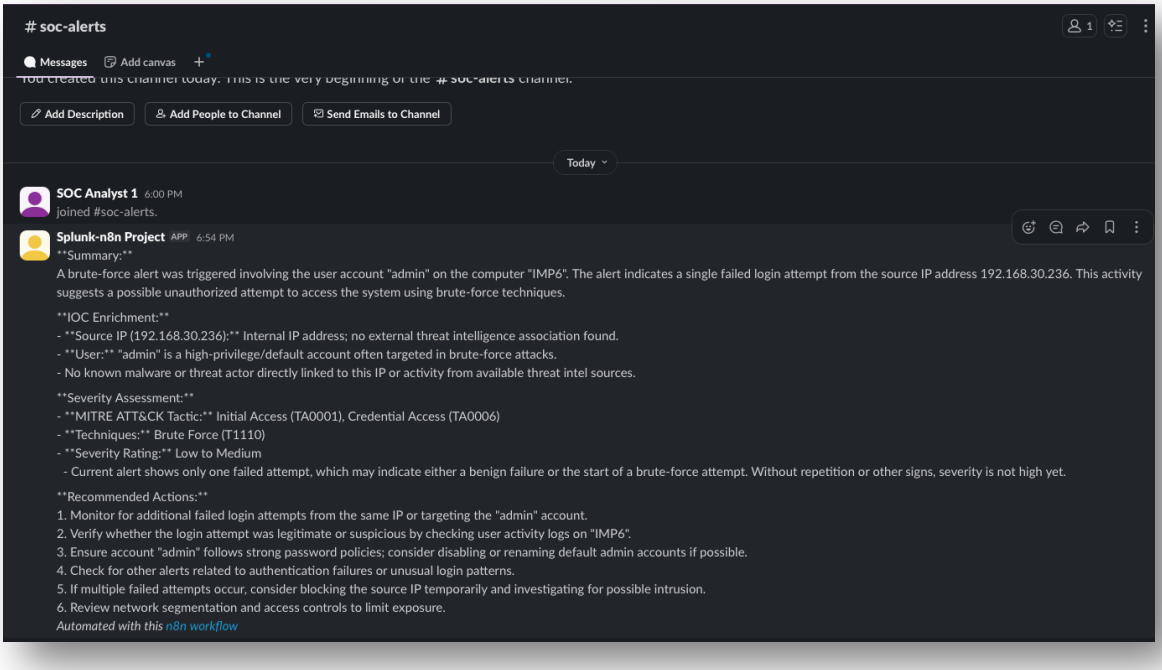
• **Slack Node:** Sends a formatted SOC alert message including event type, IOC classification, MITRE ATT&CK mapping (if applicable), threat score, and recommended action.

N8n Workflow



5. Sample Alert Output (Slack)

[High] Suspicious Logon Activity Detected
- **Host:** WIN10-LAB
- **User:** Administrator
- **Source IP:** 185.199.110.153
- **Event ID:** 4625 (Failed Logon)
- **IOC Analysis:** Multiple failed attempts → Potential brute force
- **Threat Intel:** AbuseIPDB score 98 (High risk)
- **Recommended Action:** Block IP, investigate source, check AD logs



6. Benefits of the Automation

- Real-time alerting and triage.
- Reduces manual log review and speeds up decision-making.
- Provides contextual analysis (IOC + recommended action).
- Integrates threat intelligence (AbuseIPDB) for higher fidelity alerts.
- Scalable to other event types and endpoints.

7. Next Steps & Enhancements

- Add dynamic IOC correlation with MITRE ATT&CK techniques.
- Implement alert prioritization based on IOC severity.
- Expand to additional log sources (e.g., Sysmon, firewall logs).
- Integrate additional threat intel feeds (e.g., VirusTotal, OTX).
- Implement automated response actions or ticket creation for faster containment.

Disclaimer

This lab is entirely fictional and intended for educational purposes. It simulates SOC workflows and is not connected to any production environment. All IP addresses and events used in this report are fictional or sourced from benign test environments.