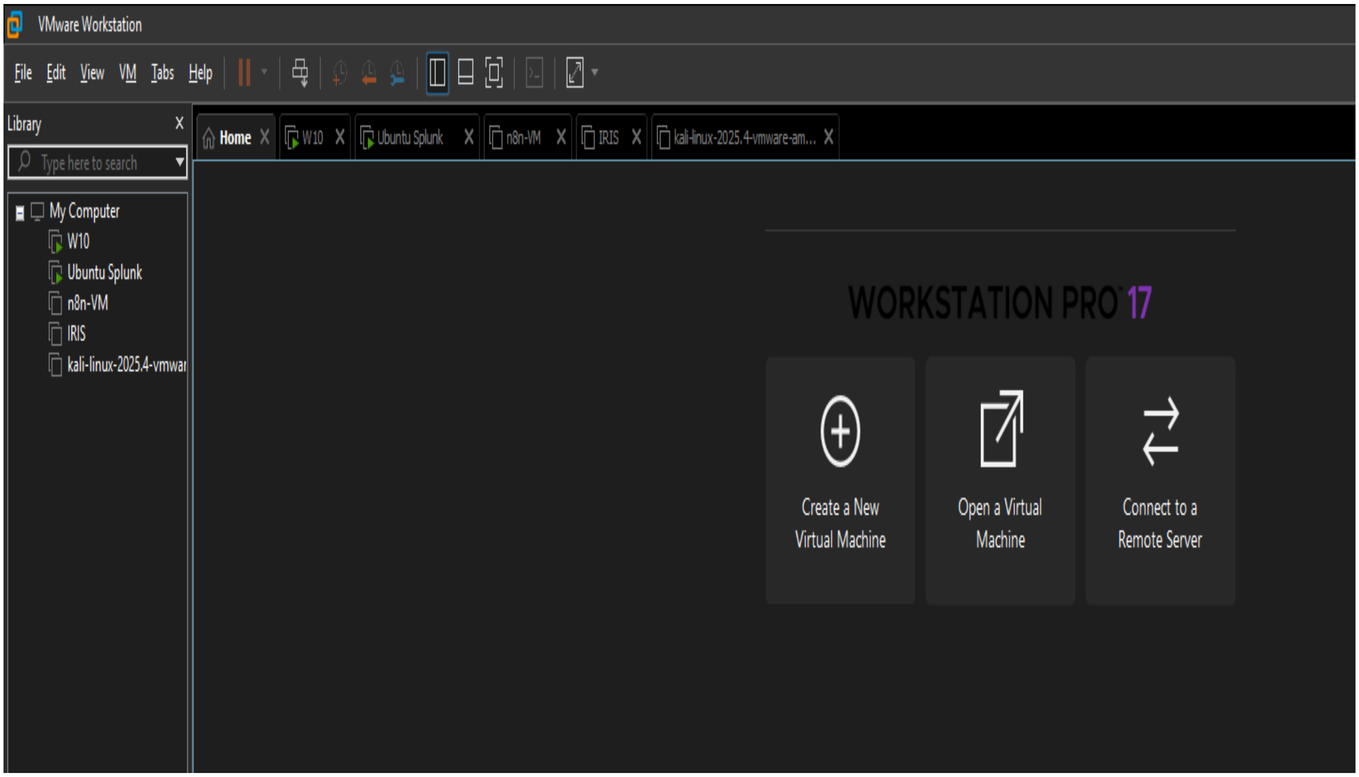
SOC Automation Project with AI

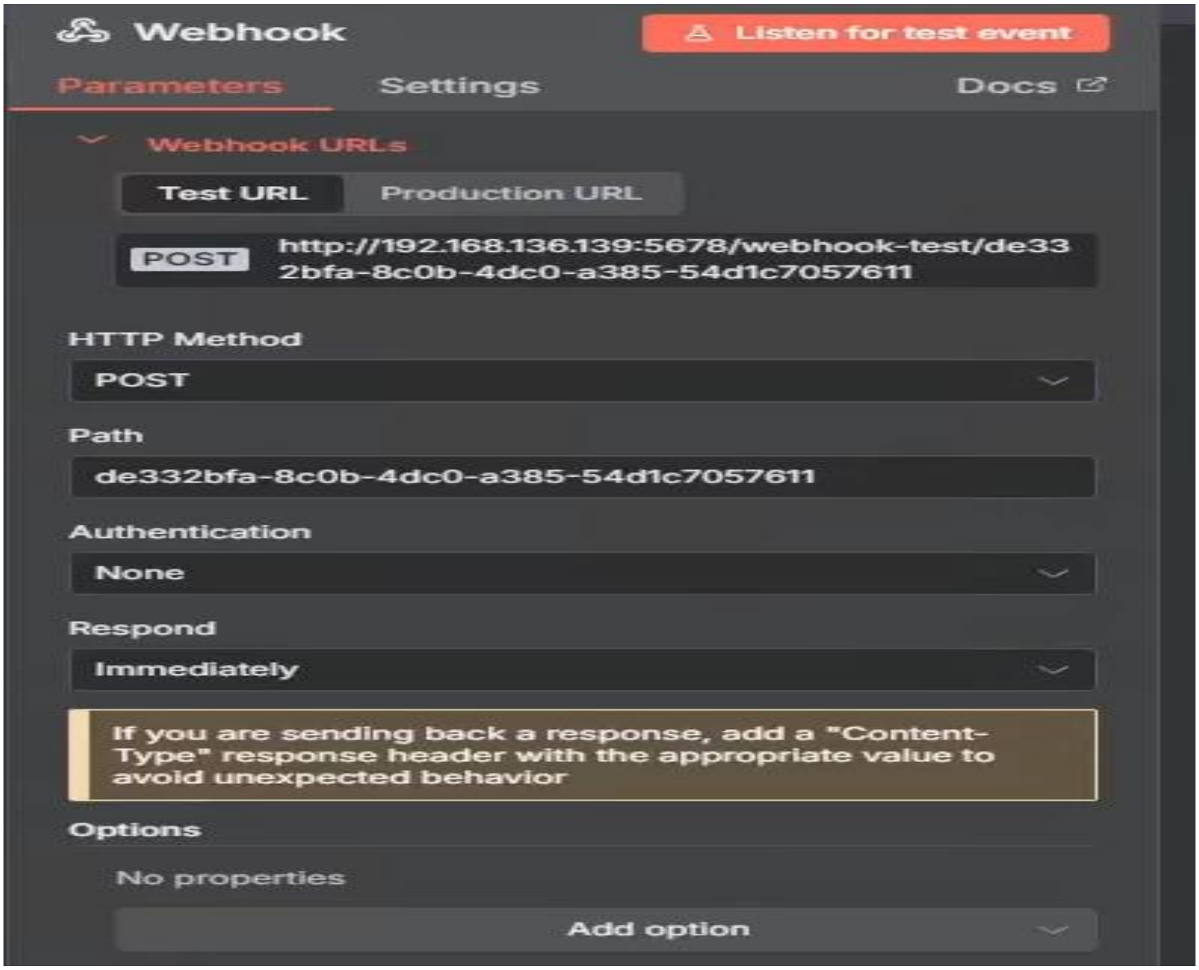
SOC Automation Project 2.0 is a hands-on cybersecurity initiative focused on designing and implementing an intelligent, automated SOC workflow. The project demonstrates how artificial intelligence can enhance detection, response, and investigation processes while reducing manual effort for security analysts.

Built within a multi-platform lab environment, the project integrates Windows 10 and Ubuntu endpoints to simulate real-world enterprise infrastructure, while Kali Linux is used to generate controlled attack scenarios for testing detection capabilities. Log data is centralized in Splunk, enabling deep visibility into system activity and security events. At the core of the project is an n8n virtual machine, which acts as the automation engine. Using n8n, security alerts are automatically ingested, enriched, prioritized, and routed through a structured workflow without requiring constant analyst intervention. IRIS serves as the incident response platform, where cases are created automatically, relevant artifacts are attached, and response actions can be triggered in seconds.



Full VM setup

To enable real-time automation, a webhook was configured between Splunk and n8n, allowing security alerts to be forwarded instantly into the automated workflow for processing and response.



Webhook URLs

POST http://192.168.136.139:5678/webhook-test/de332bfa-8c0b-4dc0-a385-54d1c7057611

HTTP Method: POST

Path: de332bfa-8c0b-4dc0-a385-54d1c7057611

Authentication: None

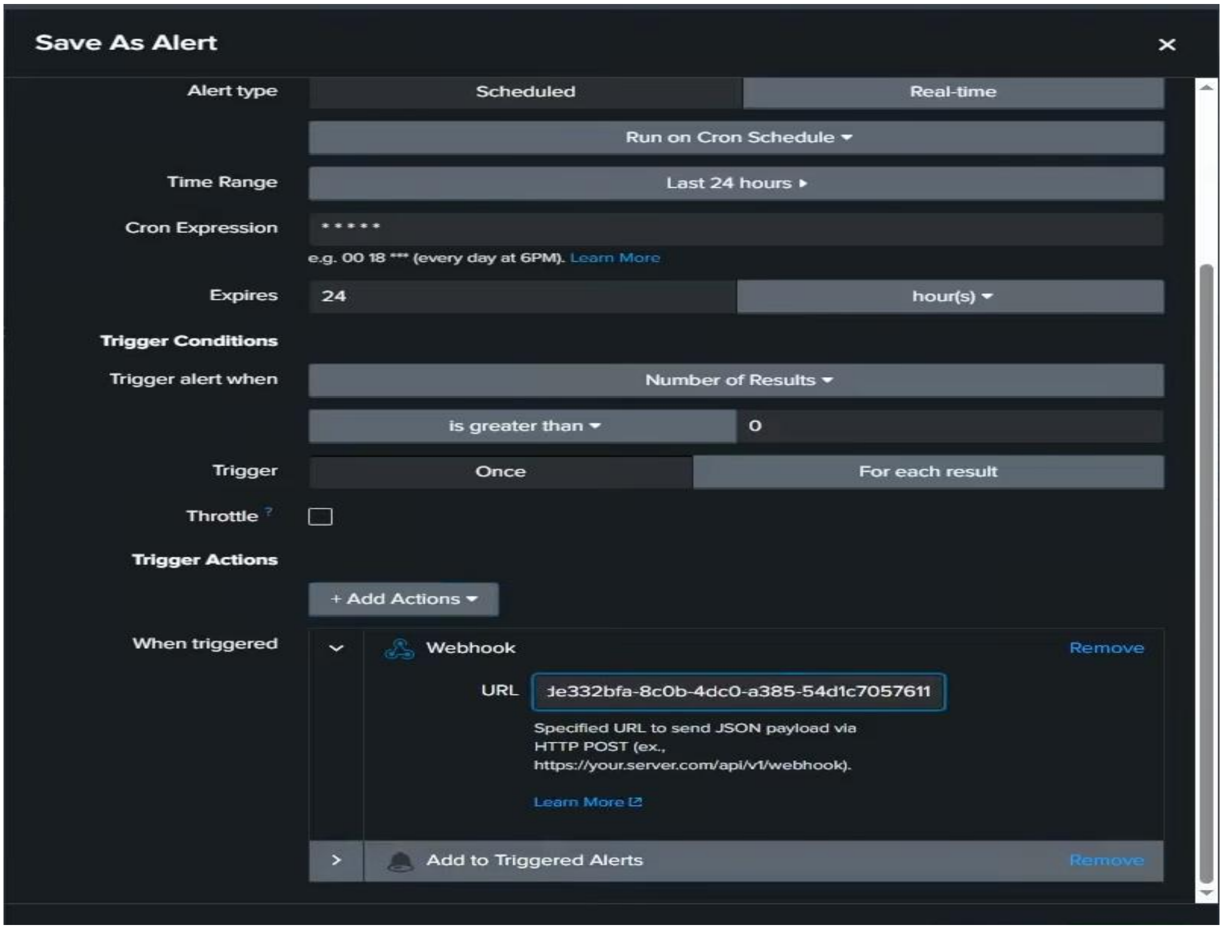
Respond: Immediately

If you are sending back a response, add a "Content-Type" response header with the appropriate value to avoid unexpected behavior

Options

No properties

n8n webhook setup


Save As Alert ×

Alert type: Scheduled | Real-time

Run on Cron Schedule ▾

Time Range: Last 24 hours ▸

Cron Expression: * * * * *

e.g. 00 18 *** (every day at 6PM). Learn More

Expires: 24 hour(s) ▾

Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than ▾ 0

Trigger: Once | For each result

Throttle ? □

Trigger Actions

+ Add Actions ▾

When triggered:

Webhook — Remove

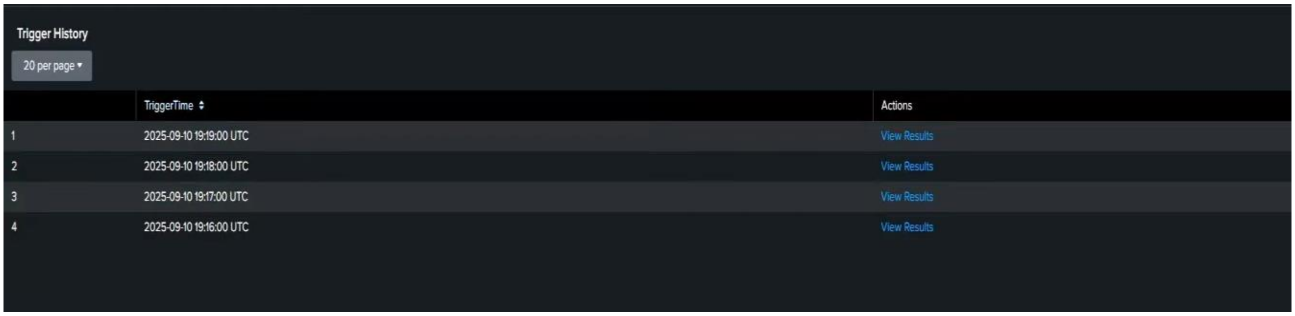
URL: ɟe332bfa-8c0b-4dc0-a385-54d1c7057611

Specified URL to send JSON payload via HTTP POST (ex., https://your.server.com/api/v1/webhook).

Learn More

Add to Triggered Alerts — Remove

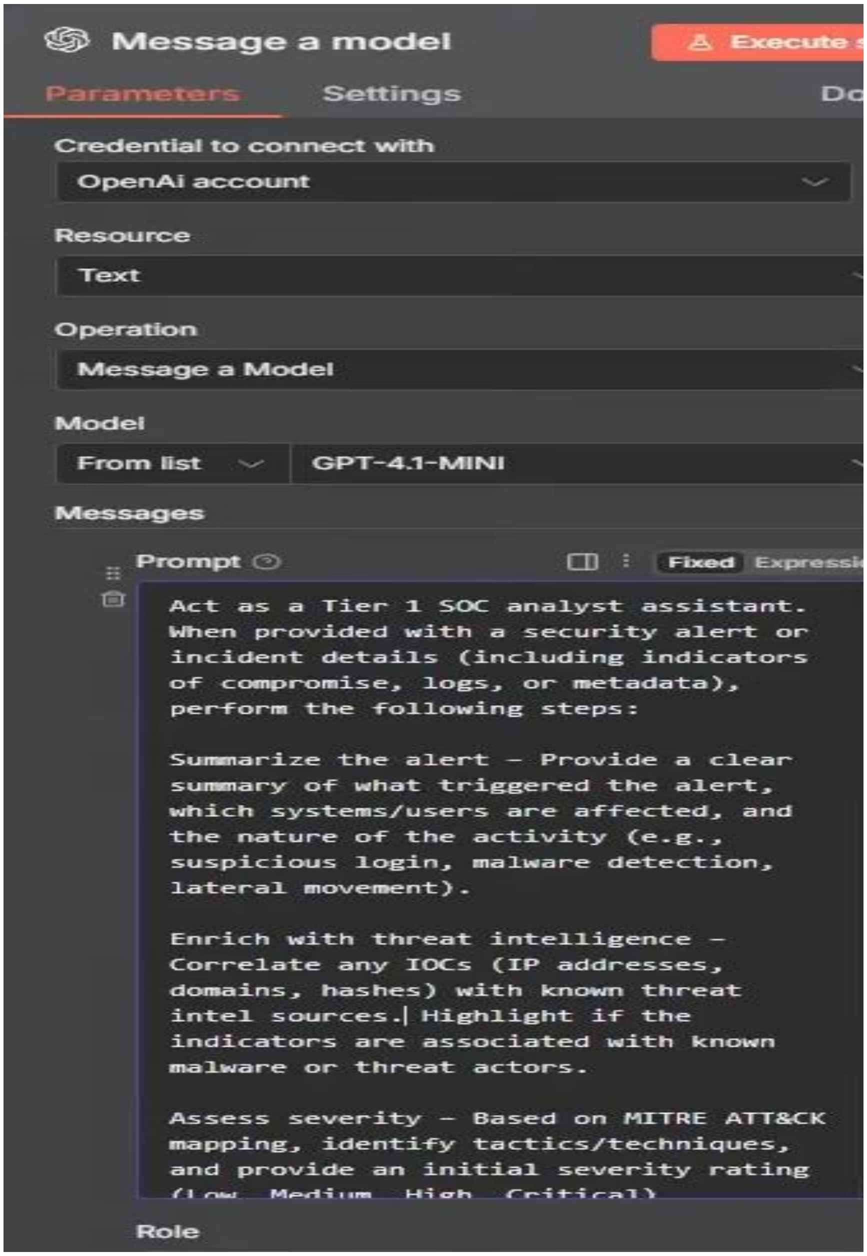
Splunk webhook setup


Trigger History

20 per page ▾

	TriggerTime	Actions
1	2025-09-10 19:19:00 UTC	View Results
2	2025-09-10 19:18:00 UTC	View Results
3	2025-09-10 19:17:00 UTC	View Results
4	2025-09-10 19:16:00 UTC	View Results

Webhook alerts



Credential to connect with
OpenAi account

Resource
Text

Operation
Message a Model

Model
From list
GPT-4.1-MINI

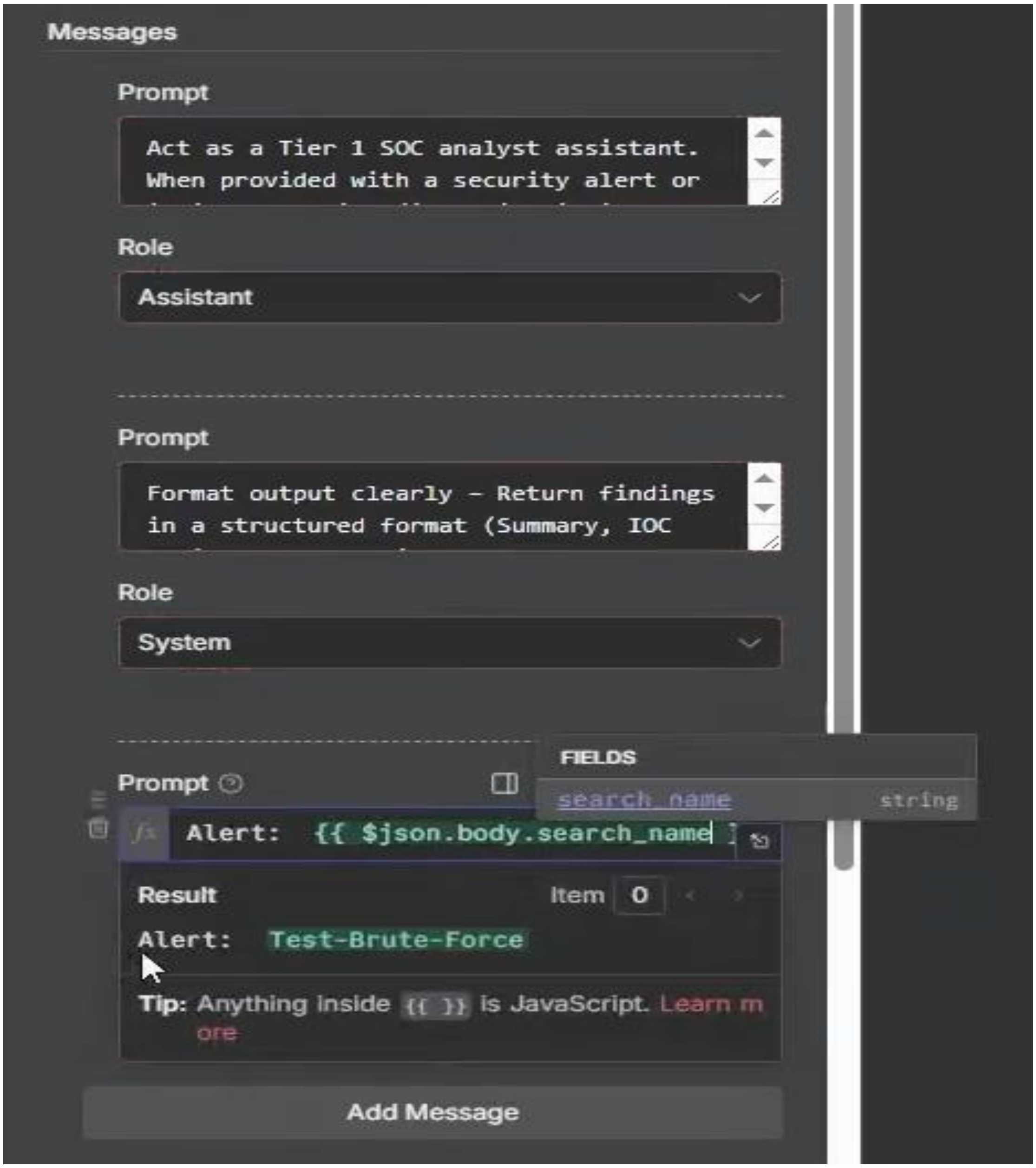
Messages

Prompt

```
Act as a Tier 1 SOC analyst assistant.
When provided with a security alert or
incident details (including indicators
of compromise, logs, or metadata),
perform the following steps:

Summarize the alert – Provide a clear
summary of what triggered the alert,
which systems/users are affected, and
the nature of the activity (e.g.,
suspicious login, malware detection,
lateral movement).

Enrich with threat intelligence –
Correlate any IOCs (IP addresses,
domains, hashes) with known threat
intel sources. Highlight if the
indicators are associated with known
malware or threat actors.

Assess severity – Based on MITRE ATT&CK
mapping, identify tactics/techniques,
and provide an initial severity rating
(Low, Medium, High, Critical).
```

Role

ChatGPT setup for automated alerts



Messages

Prompt

```
Act as a Tier 1 SOC analyst assistant.
When provided with a security alert or
```

Role

Assistant

Prompt

```
Format output clearly – Return findings
in a structured format (Summary, IOC
```

Role

System

Prompt

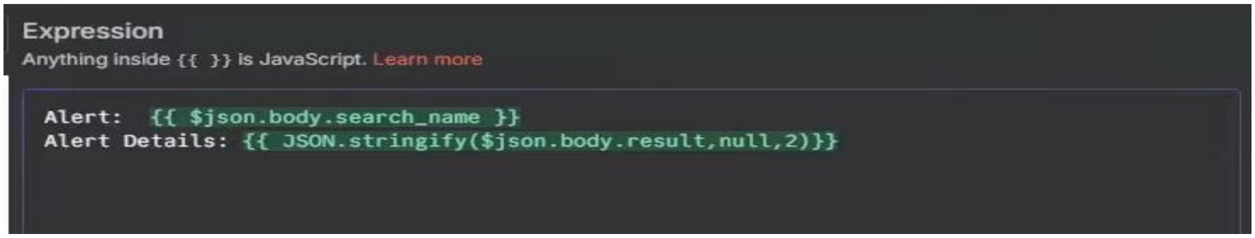
```
Alert:  {{ $json.body.search_name }}
```

Result Item 0

```
Alert:  Test-Brute-Force
```

Tip: Anything inside {{ }} is JavaScript. Learn more

Full prompt setup



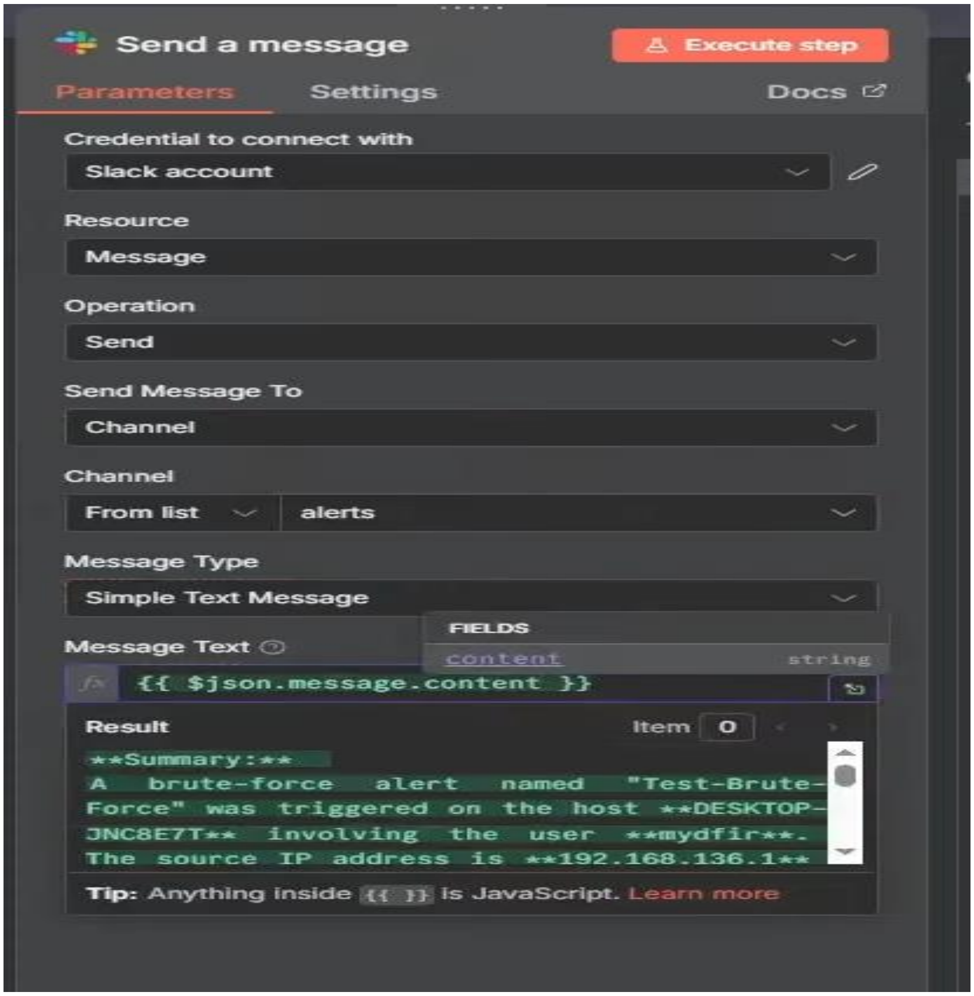
Expression

Anything inside {{ }} is JavaScript. Learn more

```
Alert:  {{ $json.body.search_name }}
Alert Details: {{ JSON.stringify($json.body.result,null,2)}}
```

Expression setup

Slack was integrated as the primary notification channel to deliver real-time security alerts. Automated messages ensure that analysts are immediately informed of potential threats, improving response times and team coordination.



Credential to connect with: Slack account

Resource: Message

Operation: Send

Send Message To: Channel

Channel: From list | alerts

Message Type: Simple Text Message

FIELDS: content string

Message Text

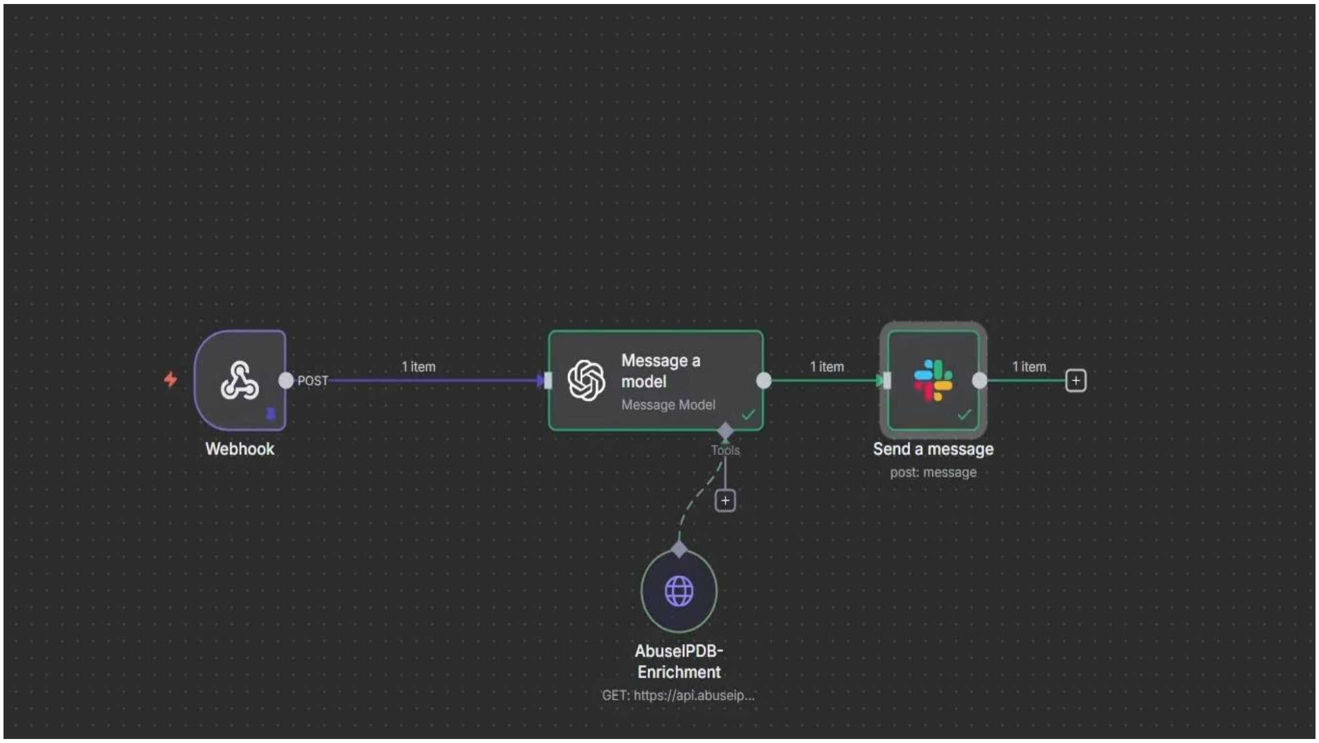
```
{{ $json.message.content }}
```

Result   Item 0

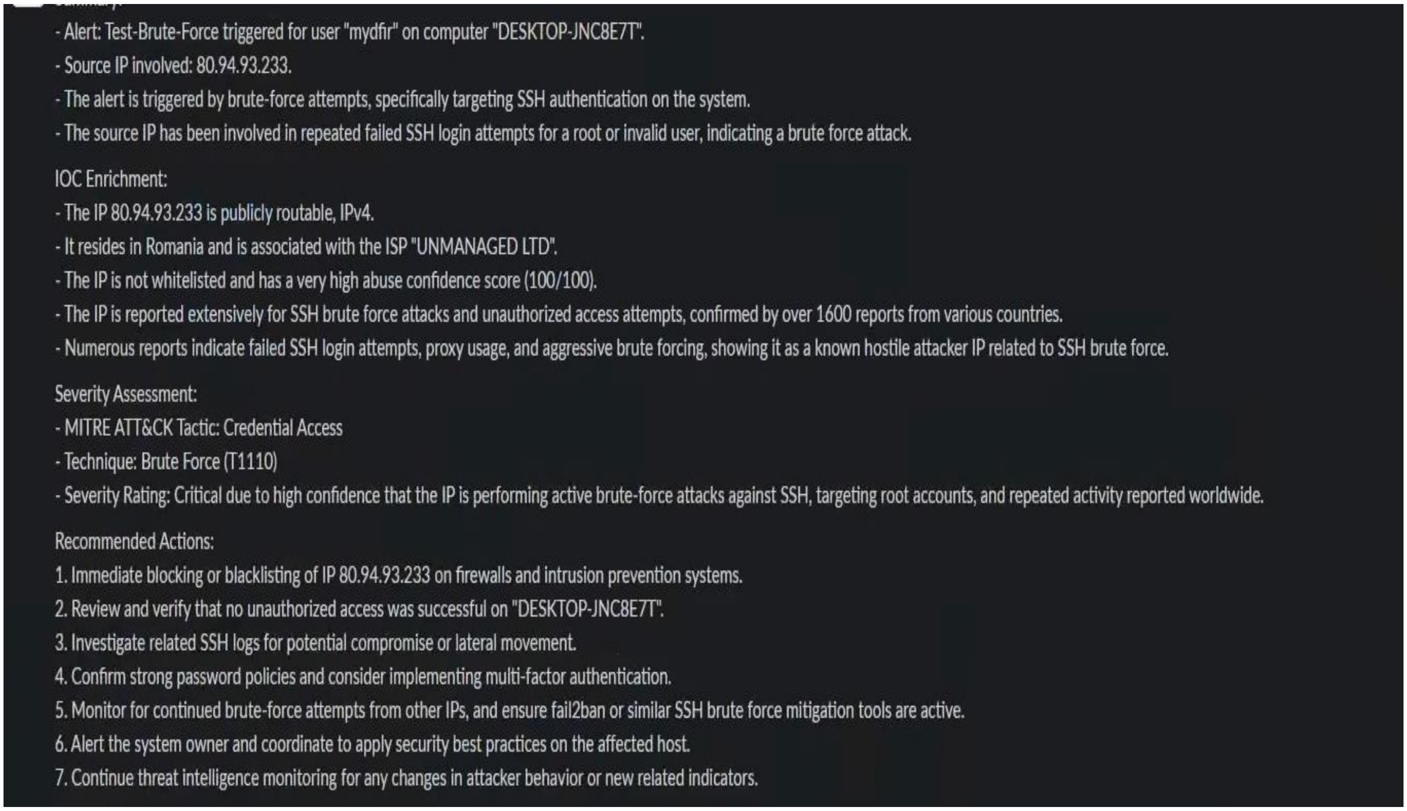
```
**Summary:**
A brute-force alert named "Test-Brute-
Force" was triggered on the host **DESKTOP-
JNC8E7T** involving the user **mydfir**.
The source IP address is **192.168.136.1**
```

Tip: Anything inside {{ }} is JavaScript. Learn more

Slack sending an alert



n8n workflow


Summary:

- Alert: Test-Brute-Force triggered for user "mydfir" on computer "DESKTOP-JNC8E7T".
- Source IP involved: 80.94.93.233.
- The alert is triggered by brute-force attempts, specifically targeting SSH authentication on the system.
- The source IP has been involved in repeated failed SSH login attempts for a root or invalid user, indicating a brute force attack.

IOC Enrichment:

- The IP 80.94.93.233 is publicly routable, IPv4.
- It resides in Romania and is associated with the ISP "UNMANAGED LTD".
- The IP is not whitelisted and has a very high abuse confidence score (100/100).
- The IP is reported extensively for SSH brute force attacks and unauthorized access attempts, confirmed by over 1600 reports from various countries.
- Numerous reports indicate failed SSH login attempts, proxy usage, and aggressive brute forcing, showing it as a known hostile attacker IP related to SSH brute force.

Severity Assessment:

- MITRE ATT&CK Tactic: Credential Access
- Technique: Brute Force (T1110)
- Severity Rating: Critical due to high confidence that the IP is performing active brute-force attacks against SSH, targeting root accounts, and repeated activity reported worldwide.

Recommended Actions:

1. Immediate blocking or blacklisting of IP 80.94.93.233 on firewalls and intrusion prevention systems.
2. Review and verify that no unauthorized access was successful on "DESKTOP-JNC8E7T".
3. Investigate related SSH logs for potential compromise or lateral movement.
4. Confirm strong password policies and consider implementing multi-factor authentication.
5. Monitor for continued brute-force attempts from other IPs, and ensure fail2ban or similar SSH brute force mitigation tools are active.
6. Alert the system owner and coordinate to apply security best practices on the affected host.
7. Continue threat intelligence monitoring for any changes in attacker behavior or new related indicators.

Alert message