

Ransomware Attack Detection

1. Brief / Purpose

This workflow detects and responds to ransomware attack detection. It receives alerts via a webhook, enriches the event, decides whether it's suspicious, and notifies the SOC team if necessary.

2. Components

- **Webhook Trigger:** Receives incoming alerts or events via HTTP POST.
- **Enrichment Node:** Calls an external API or threat intel to get reputation/context (e.g., VirusTotal, AbuseIPDB, PhishTank, GeoIP).
- **IF / Decision Node:** Examines enrichment results and decides whether to alert.
- **Slack Alert Node:** Posts a formatted message to #soc-alerts for SOC analysts.
- **Log Clean Event Node:** Records benign events for audit and reduces noise.

3. Workflow Flow

Webhook → Enrichment → IF Decision → [Slack Alert | Log Clean Event]

4. Configure Credentials

This workflow needs external integrations:

- **VirusTotal API**
 - **Node:** Check Hash in VirusTotal.
 - **Auth:** HTTP Header Auth.
 - **Add a header:**
 - **Key:** x-apikey
 - **Value:** your_virustotal_api_key.
 - [Get API key here.](#)
- **Slack API**



- Node: Send Slack Alert.
 - Configure with your Slack account.
 - Set the channel (e.g., #soc-alerts).
-

3. Webhook Security

- **Webhook Trigger** node listens on:
 - /webhook/ransomware-alert
 - It validates incoming requests using:

```
if ($headers["x-siem-token"] !== $env.SIEM_SECRET) {  
    throw new Error("Invalid Webhook Secret");  
}
```
 - **Setup:**
 - In your n8n environment variables, set:
 - SIEM_SECRET=your_shared_secret
 - Ensure your SIEM/security system sends:
 - hash (file hash to check)
 - endpoint (affected machine)
 - Header: x-siem-token: your_shared_secret.
-

4. Workflow Logic

1. **Webhook Trigger** → receives ransomware alert payload.
 2. **Validate Payload** → ensures request authenticity and required fields.
 3. **Check Hash in VirusTotal** → queries file hash.
 4. **Is Malicious?** → checks if VirusTotal reports >0 malicious detections.
 -  If malicious → **Send Slack Alert**.
 -  If clean → **Log Clean File**.
-

5. Testing

- Send a test POST request:

- `curl -X POST "https://your-n8n-url/webhook/ransomware-alert" \`
 - `-H "Content-Type: application/json" \`
 - `-H "x-siem-token: your_shared_secret" \`
 - `-d '{`
 - `"hash": "44d88612fea8a8f36de82e1278abb02f",`
 - `"endpoint": "host123"`
 - `}'`
 - Replace the hash with a known test hash.
-

6. Deployment Notes

- Keep your **SIEM_SECRET** safe — it prevents unauthorized alerts.
 - Consider logging malicious detections into a **ticketing system** (Jira, ServiceNow) in addition to Slack.
 - VirusTotal free API is rate-limited (4 requests/min). Use premium if needed.
-