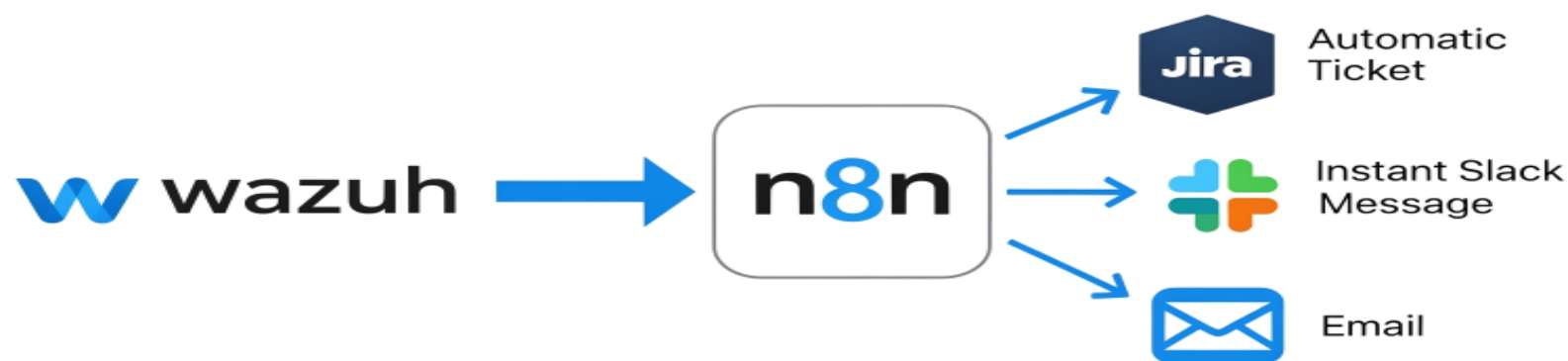




wazuh.



Step-by-Step Guide: Automating Wazuh Security Alerts using n8n + Jira + Slack + Gmail

Created By: Syed Jawad Ali Shah

🔗 Wazuh → n8n → Jira + Slack + Email Automation

🔗 Tools Used

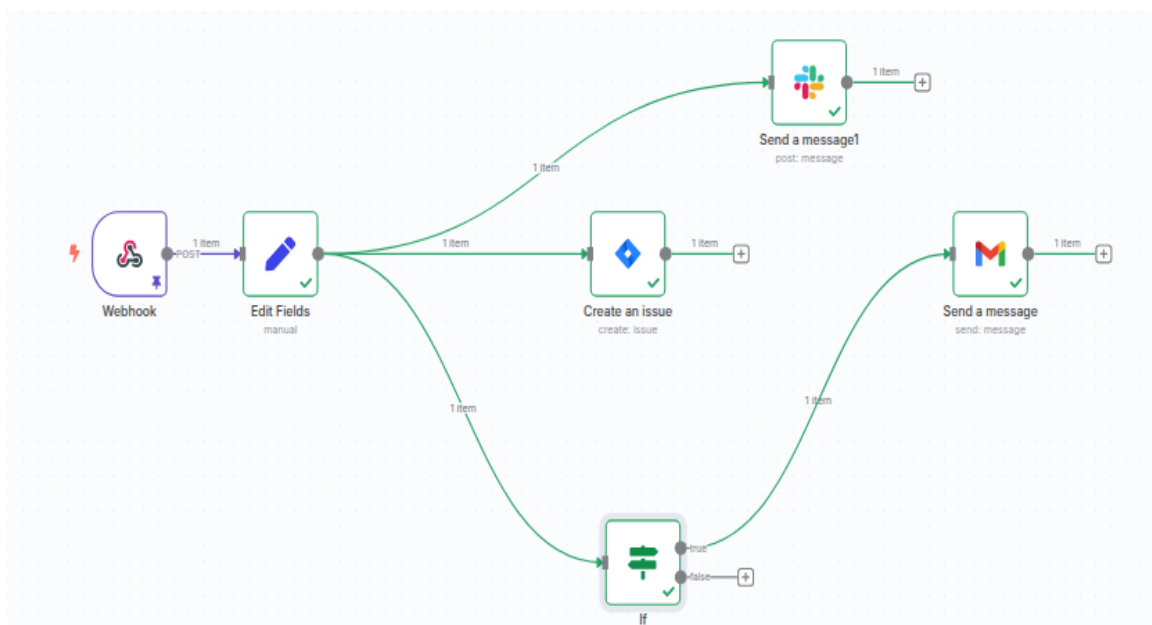
- **Wazuh** (SIEM - Security Information and Event Management)
- **n8n Cloud** (Automation Platform)
- **Jira Software** (Ticketing)
- **Slack** (Real-time notification)
- **Gmail** (Email alerting)

🌟 Objective

Automatically create Jira issues from Wazuh alerts and:

- Always send Slack notifications
- Additionally send email notifications to the team lead if the severity is 10 or higher

📋 Workflow Overview



1. **Webhook** – Receives incoming Wazuh alert
2. **Edit Fields (Set)** – Extracts key data from the nested JSON body
3. **Create an Issue (Jira)** – Creates a Jira ticket with extracted data
4. **Send a Message (Slack)** – Sends formatted alert to Slack
5. **IF** – Checks if `level >= 10`
6. **Send a Message (Gmail)** – If condition true, sends email to lead

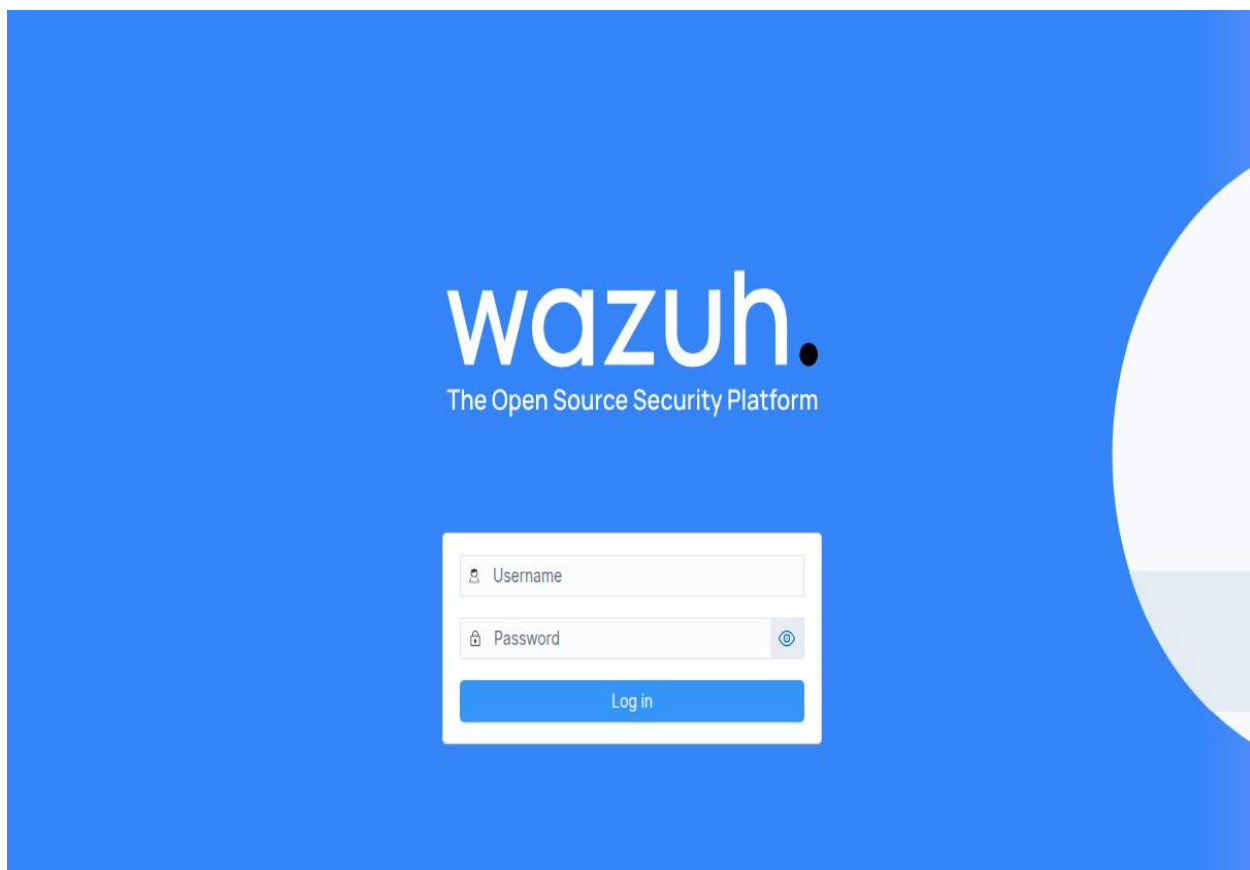
Step-by-Step Setup

Wazuh Setup & Integration

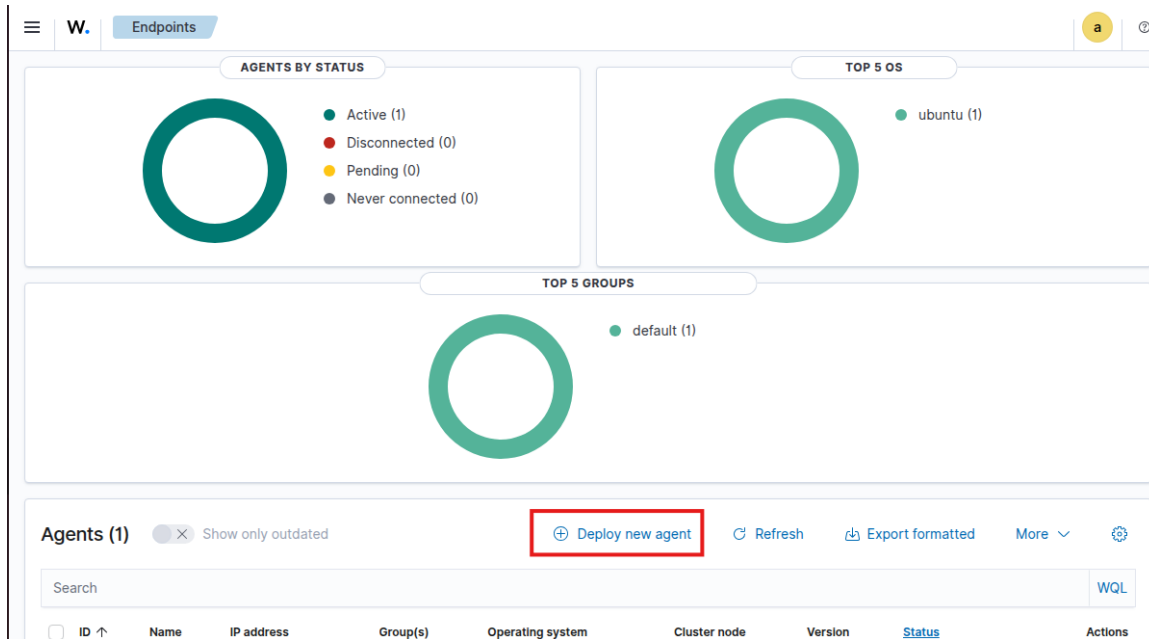
1. Install Wazuh Manager (Ubuntu Example)

```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo  
bash ./wazuh-install.sh -a
```

This installs the **Wazuh Manager**, **Dashboard**, and **Indexer** components.



2. Install Wazuh Agent (Ubuntu Example)



3. OSSEC Integration Configuration

Add the following integration block to the `ossec.conf` file on the **Wazuh Manager** under the `<integration>` section:

```
<integration>
  <name>custom-wazuh-integration</name>
  <hook_url>https://test767.app.n8n.cloud/webhook-test/Path:1a65bf7a.....<
/hook_url>
  <level>2</level>
  <alert_format>json</alert_format>
</integration>
```

4. Add Custom Python Script (Script is available in on my [GITHUB](#))


Place your script under:

```
/var/ossec/integrations/custom-n8n
```

Ensure it is executable:

```
chmod +x /var/ossec/integrations/custom-n8n
```

1. Webhook (Trigger)

 Webhook Listen for test event

Parameters Settings Docs

Webhook URLs

Test URL Production URL

POST https://test767.app.n8n.cloud/webhook-test/1a65bf7a-42b1-4ae7-8609-511cfeeed79f

HTTP Method

POST

Path

1a65bf7a-42b1-4ae7-8609-511cfeeed79f

Authentication

None

Respond

Immediately


Options

No properties

Add option

- **HTTP Method:** POST
- **Path:** /1a65bf7a.....
- **Response Mode:** Immediately


2. Set (Edit Fields)

 Edit Fields

Execute step

Parameters

Settings

Docs 

Jul 13 08:27:55 N8NW sudo[7032]: pam_unix(sudo:...

WazuhAlertID

A String

= `{{ $json["body"]["id"] }}`

1752395275.44352

Drag input fields here or Add Field

Include Other Input Fields

☒

Input Fields to Include

All

Options

No properties

Add option

Enable “Include other input fields” ☒ Extract nested fields using expressions:

Label	Expression
Agent	<code>{{ \$json["body"]["all_fields"]["agent"]["name"] }}</code>
RuleID	<code>{{ \$json["body"]["rule_id"] }}</code>
Title	<code>{{ \$json["body"]["title"] }}</code>
Log	<code>{{ \$json["body"]["body"] }}</code>
Severity	<code>{{ \$json["body"]["severity"] }}</code>
Timestamp	<code>{{ \$json["body"]["timestamp"] }}</code>
WazuhAlertID	<code>{{ \$json["body"]["id"] }}</code>
Level (For IF)	<code>{{ \$json["body"]["all_fields"]["rule"]["level"] }}</code>

3. Jira – Create Issue

Create an issue

Execute step

Parameters

Settings

Docs

Credential to connect with

Jira SW Cloud account 2

Resource

Issue

Operation

Create

Project

By ID

10001

Issue Type

By ID

10007

Summary

fx

{{ \$json.body?.title || 'Wazuh Alert' }}

PAM: Login session opened.

Additional Fields

Description

Agent: {{ \$json.body.all_fields.agent.name }}

Rule ID: {{ \$json.body.rule_id }}

Log: {{ \$json.body.text }}

Severity: {{ \$json.body.severity }}

Timestamp: {{ \$json.body.timestamp }}

- **Authentication:** API Token
- **Project ID:** 10001
- **Issue Type ID:** 10007 (Task)
- **Summary:** Wazuh Alert - Level {{ \$json["Severity"] }}
- **Description:**

Wazuh Alert

****Agent:**** {{ \$json.body.all_fields.agent.name }}


****Rule ID:**** {{ \$json.body.rule_id }}

****Log:**** {{ \$json.body.text }}

****Severity:**** {{ \$json.body.severity }}

****Timestamp:**** {{ \$json.body.timestamp }}

4. 🗨️ Slack – Send Message

 **Send a message1** Execute step

Parameters Settings Docs

Credential to connect with

Slack account

Resource

Message

Operation

Send

Send Message To

Channel

Channel

From list

wazuh-alerts

Message Type

Simple Text Message

Message Text

fx

🔔 *Wazuh Alert* created in Jira

Agent: {{\$json["body"]["all_fields"]["agent"]["name"]}}

Rule ID: {{\$json["body"]["all_fields"]["rule"]["id"]}}

Severity: {{\$json["body"]["severity"]}}

Timestamp: {{\$json["body"]["timestamp"]}}

Log: {{\$json["body"]["all_fields"]["full_log"]}}

Jira Ticket Created ✓

- **Mode:** Send to channel
- **Channel:** #wazuh-alerts
- **Text:**

🔔 ***Wazuh Alert* created in Jira**

Agent: {{\$json["body"]["all_fields"]["agent"]["name"]}}

Rule ID: {{\$json["body"]["all_fields"]["rule"]["id"]}}


Severity: {{\$json["body"]["severity"]}}

Timestamp: {{\$json["body"]["timestamp"]}}

Log: {{\$json["body"]["all_fields"]["full_log"]}}

Jira Ticket Created ✓

5. IF – Check Severity Level

 If Execute step

Parameters Settings Docs

Conditions

fx `{{ $json["Level"] > 2 }}`

☒ exists


Add condition

Convert types where required

- **Condition:** Value 1: `{{ $json["level"] > 10 }}`, Value 2: Exists

If TRUE, move to Gmail Node

6. Gmail – Send Email

 Send a message Execute step

Parameters Settings Docs

Credential to connect with

Gmail account

Resource

Message

Operation

Send

To

wazuh110@gmail.com

Subject


fx `High Severity Wazuh Alert - Level {{ $json["body"]["all_fields"]["rule"]["level"] }}`

High Severity Wazuh Alert - Level 3

Email Type

Text

Message

 *High Severity Alert from Wazuh*

- To: lead@company.com
- Subject: 🚨 High Severity Wazuh Alert - Level {{ \$json["body"]["all_fields"]["rule"]["level"] }}
- Body:

🚨 *High Severity Alert from Wazuh*

****Agent:**** {{ \$json["body"]["all_fields"]["agent"]["name"] }}

****Rule ID:**** {{ \$json["body"]["all_fields"]["rule"]["id"] }}

****Severity Level:**** {{ \$json["body"]["all_fields"]["rule"]["level"] }}

****Timestamp:**** {{ \$json["body"]["all_fields"]["timestamp"] }}

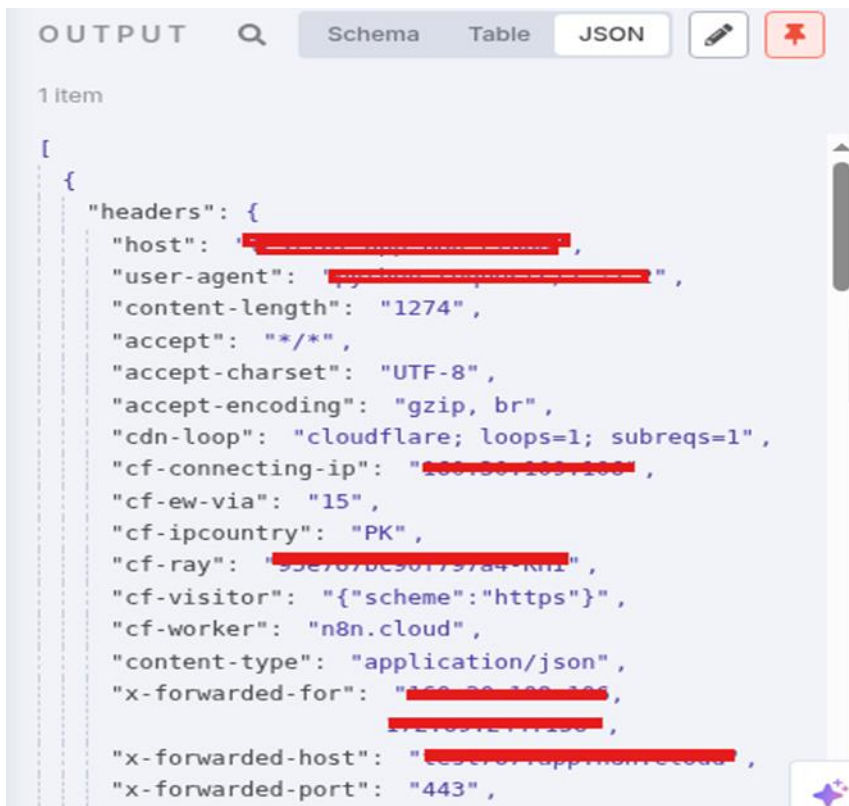
****Log:**** {{ \$json["body"]["all_fields"]["full_log"] }}

☐ A Jira ticket has already been created.

Please review and respond accordingly.

7.☐ Testing Tips

- Use custom Python script to POST alert JSON
- Confirm webhook receives and parses alert



The screenshot shows a JSON output viewer with tabs for 'Schema', 'Table', and 'JSON'. The 'JSON' tab is selected, displaying a single item. The JSON object contains a 'headers' field with various HTTP headers, including 'host', 'user-agent', 'content-length', 'accept', 'accept-charset', 'accept-encoding', 'cdn-loop', 'cf-connecting-ip', 'cf-ew-via', 'cf-ipcountry', 'cf-ray', 'cf-visitor', 'cf-worker', 'content-type', 'x-forwarded-for', 'x-forwarded-host', and 'x-forwarded-port'. Some values are redacted with black bars.



```
[
  {
    "headers": {
      "host": "100.100.100.100",
      "user-agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36",
      "content-length": "1274",
      "accept": "*/*",
      "accept-charset": "UTF-8",
      "accept-encoding": "gzip, br",
      "cdn-loop": "cloudflare; loops=1; subreqs=1",
      "cf-connecting-ip": "100.100.100.100",
      "cf-ew-via": "15",
      "cf-ipcountry": "PK",
      "cf-ray": "55e707bc907797a4-KM1",
      "cf-visitor": "{\"scheme\":\"https\"}",
      "cf-worker": "n8n.cloud",
      "content-type": "application/json",
      "x-forwarded-for": "100.100.100.100",
      "x-forwarded-host": "100.100.100.100",
      "x-forwarded-port": "443",
    }
  }
]
```



- Verify Jira ticket created with proper formatting

Projects

Security Incidents 1 ...


Summary Timeline **Board** Calendar List Forms Goals All work More 4 +

Q Search b...  


Group ▾   ...

TO DO 3 ...


PAM: Login session closed.

☒ SEC-1 

PAM: Login session closed.

☒ SEC-2 

PAM: Login session opened.

☒ SEC-3 



+ Create

IN PROGRESS

DONE ✓

- Confirm Slack receives all alerts

wazuh-alerts

1  Huddle ▾  ...


Messages Shared resources Team priorities Workflows +

Log: Jul 13 08:27:55 N8NW sudo[7032]: pam_unix(sudo:session): session opened for user root(uid=0) by N8N(uid=1000)

Jira Ticket Created ✓

Automated with this [n8n workflow](#)

Wazuh 9:19 AM

 Wazuh Alert created in Jira

Agent: N8NW

Rule ID: 5501






Severity: 1 low

Timestamp: 2025-07-13T08:27:55.451+0000

Log: Jul 13 08:27:55 N8NW sudo[7032]: pam_unix(sudo:session): session opened for user root(uid=0) by N8N(uid=1000)


Jira Ticket Created ✓


Automated with this [n8n workflow](#)

B I     

Message #wazuh-alerts


- Confirm email is triggered only for level ≥ 10 (For test I used level > 2)



High Severity Wazuh Alert - Level 

Inbox x

to me ▾

 *High Severity Alert from Wazuh*

Agent: N8NW


Rule ID: 5501

Severity Level: 3

Timestamp: 2025-07-13T08:27:55.451+0000

Log:

Jul 13 08:27:55 N8NW sudo[7032]: pam_unix(sudo:session): session opened for user root(uid=0) by N8N(uid=1000)

 A Jira ticket has already been created.

Please review and respond accordingly.

This email was sent automatically with n8n

<https://n8n.io>

Inspiration for Learners

- "Automation is good, so long as you know exactly where to put the machine."
– **Eliyahu Goldratt**
- "Learning is a treasure that will follow its owner everywhere." – **Chinese Proverb**
- "Start where you are. Use what you have. Do what you can." – **Arthur Ashe**