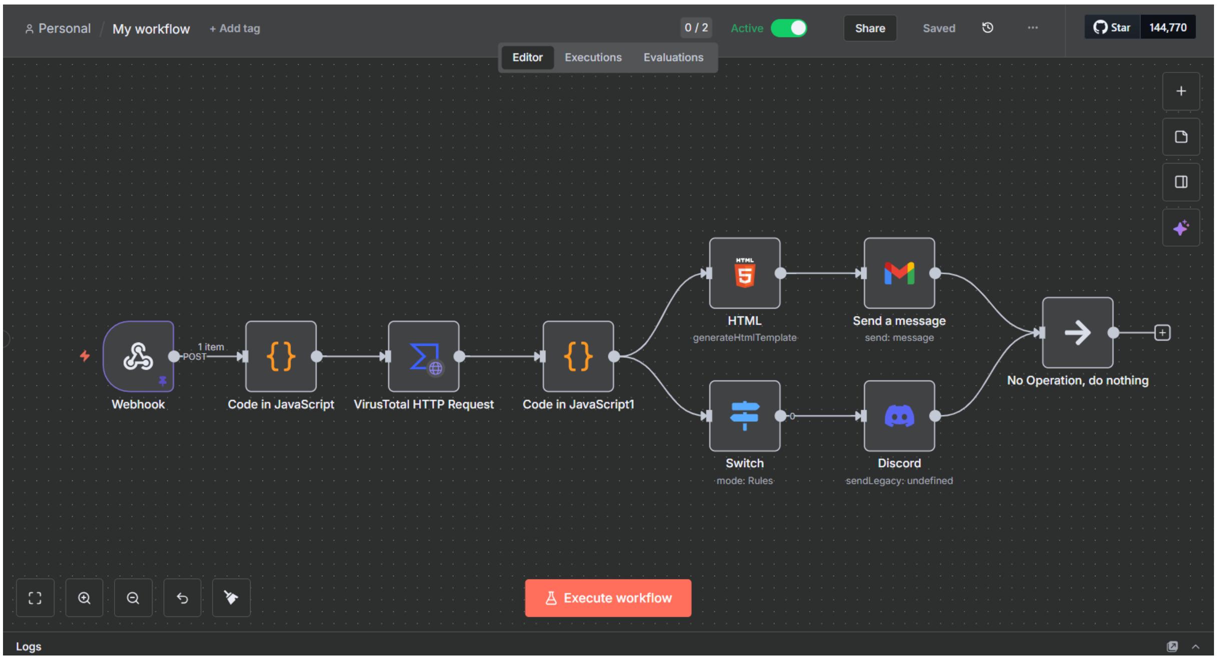
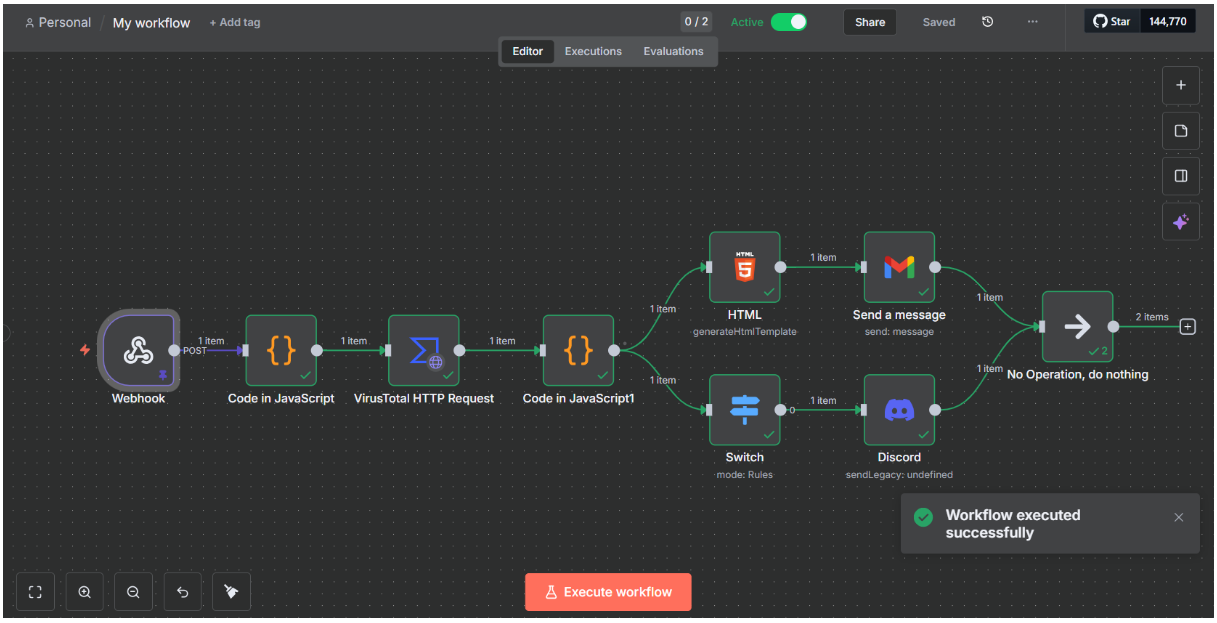
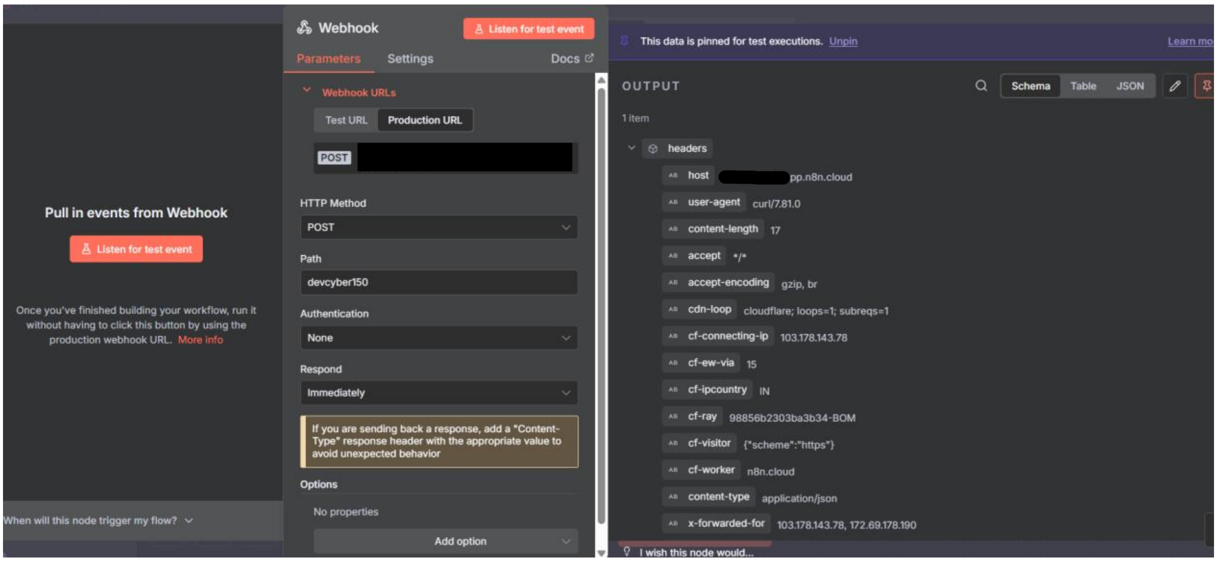




Workflow executed successfully



Once you've finished building your workflow, run it without having to click this button by using the production webhook URL. More info

POST [redacted]

HTTP Method: POST

Path: devcyber150

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

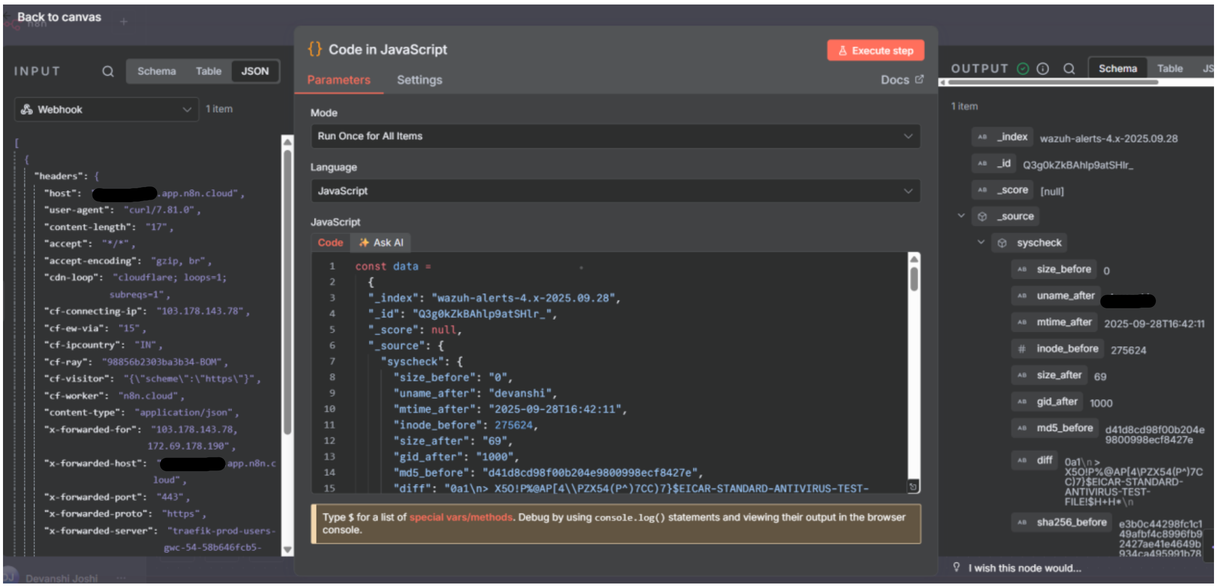
No properties

This data is pinned for test executions. Unpin

OUTPUT

1 item

```
headers
  host              [redacted]pp.n8n.cloud
  user-agent        curl/7.81.0
  content-length    17
  accept            */*
  accept-encoding   gzip, br
  cdn-loop          cloudflare; loops=1; subreqs=1
  cf-connecting-ip  103.178.143.78
  cf-ew-via         15
  cf-ipcountry      IN
  cf-ray            98856b2303ba3b34-BOM
  cf-visitor        {"scheme":"https"}
  cf-worker         n8n.cloud
  content-type      application/json
  x-forwarded-for   103.178.143.78, 172.69.178.190
```



```
[
  {
    "headers": {
      "host": "[redacted].app.n8n.cloud",
      "user-agent": "curl/7.81.0",
      "content-length": "17",
      "accept": "*/*",
      "accept-encoding": "gzip, br",
      "cdn-loop": "cloudflare; loops=1;
                  subreqs=1",
      "cf-connecting-ip": "103.178.143.78",
      "cf-ew-via": "15",
      "cf-ipcountry": "IN",
      "cf-ray": "98856b2303ba3b34-BOM",
      "cf-visitor": "{\"scheme\":\"https\"}",
      "cf-worker": "n8n.cloud",
      "content-type": "application/json",
      "x-forwarded-for": "103.178.143.78,
                          172.69.178.190",
      "x-forwarded-host": "[redacted]app.n8n.c
                          loud",
      "x-forwarded-port": "443",
      "x-forwarded-proto": "https",
      "x-forwarded-server": "traefik-prod-users-
                             gwc-54-58b646fcb5-
```

Mode: Run Once for All Items

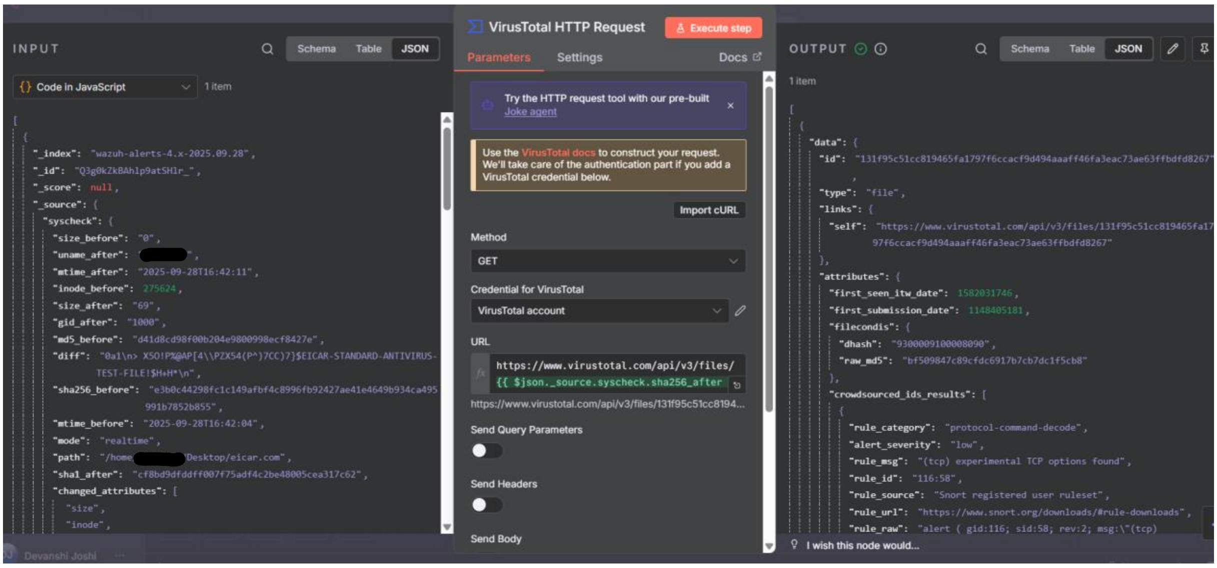
Language: JavaScript

JavaScript

```
const data =
  {
  "_index": "wazuh-alerts-4.x-2025.09.28",
  "_id": "Q3g0kZkBAhlp9atSHlr_",
  "_score": null,
  "_source": {
    "syscheck": {
      "size_before": "0",
      "uname_after": "devanshi",
      "mtime_after": "2025-09-28T16:42:11",
      "inode_before": 275624,
      "size_after": "69",
      "gid_after": "1000",
      "md5_before": "d41d8cd98f00b204e9800998ecf8427e",
      "diff": "0a1\n> X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
```

Type $ for a list of special vars/methods. Debug by using `console.log()` statements and viewing their output in the browser console.

```
_index          wazuh-alerts-4.x-2025.09.28
_id             Q3g0kZkBAhlp9atSHlr_
_score          [null]
_source
  syscheck
    size_before     0
    uname_after     [redacted]
    mtime_after     2025-09-28T16:42:11
    inode_before    275624
    size_after      69
    gid_after       1000
    md5_before      d41d8cd98f00b204e
                    9800998ecf8427e
    diff            0a1\n >
                    X5O!P%@AP[4\PZX54(P^)7C
                    C)7}$EICAR-STANDARD-
                    ANTIVIRUS-TEST-
                    FILE!$H+H*\n
    sha256_before   e3b0c44298fc1c1
                    49afbf4c8996fb9
                    2427ae41e4649b
                    934ca495991b78
```



```
[
  {
    "_index": "wazuh-alerts-4.x-2025.09.28",
    "_id": "Q3g0kZkBAhlp9atSHlr_",
    "_score": null,
    "_source": {
      "syscheck": {
        "size_before": "0",
        "uname_after": "[redacted]",
        "mtime_after": "2025-09-28T16:42:11",
        "inode_before": 275624,
        "size_after": "69",
        "gid_after": "1000",
        "md5_before": "d41d8cd98f00b204e9800998ecf8427e",
        "diff": "0a1\n> X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-
                TEST-FILE!$H+H*\n",
        "sha256_before": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495
                          991b7852b855",
        "mtime_before": "2025-09-28T16:42:04",
        "mode": "realtime",
        "path": "/home[redacted]Desktop/eicar.com",
        "sha1_after": "cf8bd9dfddff007f75adf4c2be48005cea317c62",
        "changed_attributes": [
          "size",
          "inode",
```

Try the HTTP request tool with our pre-built Joke agent ×

Use the VirusTotal docs to construct your request. We'll take care of the authentication part if you add a VirusTotal credential below.

Method: GET

Credential for VirusTotal: VirusTotal account

URL

```
https://www.virustotal.com/api/v3/files/
{{ $json._source.syscheck.sha256_after
```

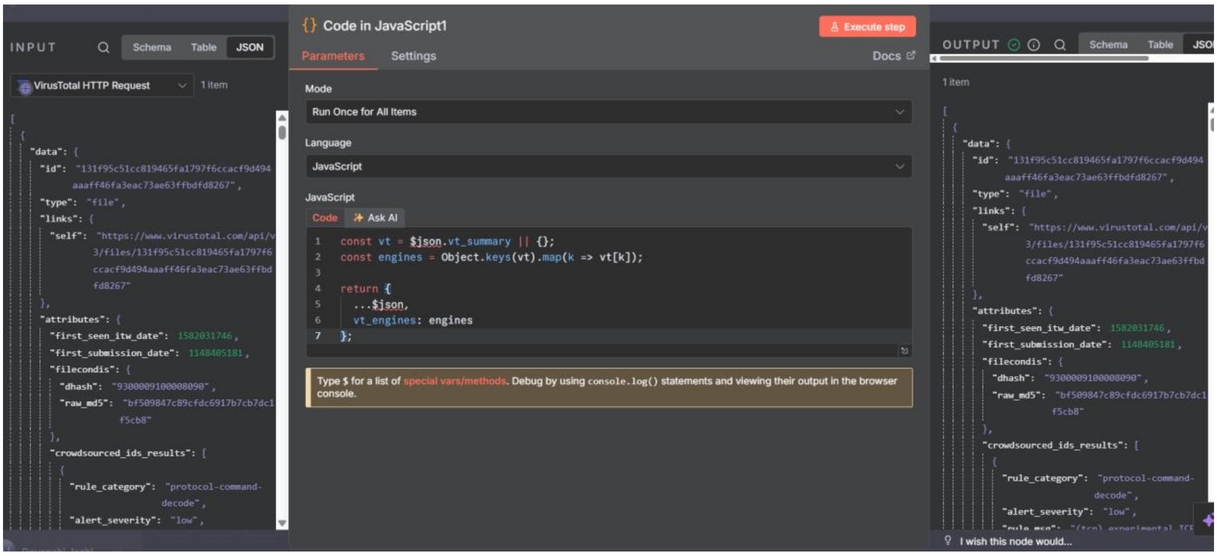
https://www.virustotal.com/api/v3/files/131f95c51cc8194...

Send Query Parameters

Send Headers

Send Body

```
[
  {
    "data": {
      "id": "131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267"
        ,
      "type": "file",
      "links": {
        "self": "https://www.virustotal.com/api/v3/files/131f95c51cc819465fa17
                97f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267"
      },
      "attributes": {
        "first_seen_itw_date": 1582031746,
        "first_submission_date": 1148405181,
        "filecondis": {
          "dhash": "9300009100008090",
          "raw_md5": "bf509847c89cfdc6917b7cb7dc1f5cb8"
        },
        "crowdsourced_ids_results": [
          {
            "rule_category": "protocol-command-decode",
            "alert_severity": "low",
            "rule_msg": "(tcp) experimental TCP options found",
            "rule_id": "116:58",
            "rule_source": "Snort registered user ruleset",
            "rule_url": "https://www.snort.org/downloads/#rule-downloads",
            "rule_raw": "alert ( gid:116; sid:58; rev:2; msg:\"(tcp)
```



```
[
  {
    "data": {
      "id": "131f95c51cc819465fa1797f6ccacf9d494
            aaaff46fa3eac73ae63ffbdfd8267",
      "type": "file",
      "links": {
        "self": "https://www.virustotal.com/api/v
                3/files/131f95c51cc819465fa1797f6
                ccacf9d494aaaff46fa3eac73ae63ffbd
                fd8267"
      },
      "attributes": {
        "first_seen_itw_date": 1582031746,
        "first_submission_date": 1148405181,
        "filecondis": {
          "dhash": "9300009100008090",
          "raw_md5": "bf509847c89cfdc6917b7cb7dc1
                      f5cb8"
        },
        "crowdsourced_ids_results": [
          {
            "rule_category": "protocol-command-
                              decode",
            "alert_severity": "low",
```

Mode: Run Once for All Items

Language: JavaScript

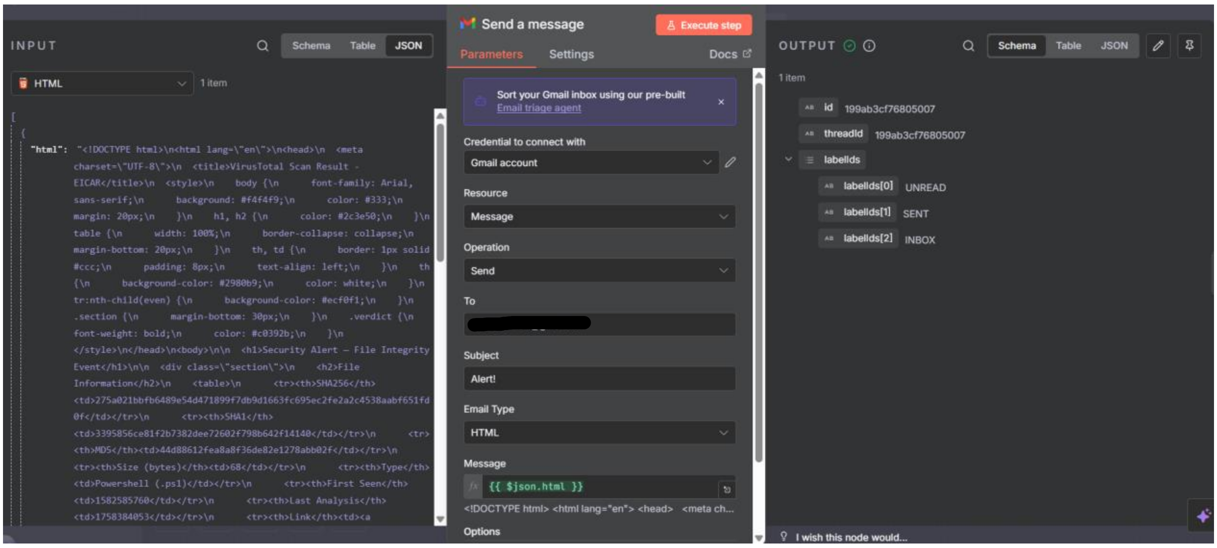
JavaScript

```
const vt = $json.vt_summary || {};
const engines = Object.keys(vt).map(k => vt[k]);

return {
  ...$json,
  vt_engines: engines
};
```

Type $ for a list of special vars/methods. Debug by using `console.log()` statements and viewing their output in the browser console.

```
[
  {
    "data": {
      "id": "131f95c51cc819465fa1797f6ccacf9d494
            aaaff46fa3eac73ae63ffbdfd8267",
      "type": "file",
      "links": {
        "self": "https://www.virustotal.com/api/v
                3/files/131f95c51cc819465fa1797f6
                ccacf9d494aaaff46fa3eac73ae63ffbd
                fd8267"
      },
      "attributes": {
        "first_seen_itw_date": 1582031746,
        "first_submission_date": 1148405181,
        "filecondis": {
          "dhash": "9300009100008090",
          "raw_md5": "bf509847c89cfdc6917b7cb7dc1
                      f5cb8"
        },
        "crowdsourced_ids_results": [
          {
            "rule_category": "protocol-command-
                              decode",
            "alert_severity": "low",
            "rule_msg": "(tcp) experimental TCP
```



INPUT — Schema | Table | **JSON**

HTML ▾ 1 item

```
[
  {
    "html": "<!DOCTYPE html>\n<html lang=\"en\">\n<head>\n  <meta
        charset=\"UTF-8\">\n  <title>VirusTotal Scan Result -
        EICAR</title>\n  <style>\n    body {\n      font-family: Arial,
        sans-serif;\n      background: #f4f4f9;\n      color: #333;\n
        margin: 20px;\n    }\n    h1, h2 {\n      color: #2c3e50;\n    }\n
        table {\n      width: 100%;\n      border-collapse: collapse;\n
        margin-bottom: 20px;\n    }\n    th, td {\n      border: 1px solid
        #ccc;\n      padding: 8px;\n      text-align: left;\n    }\n    th
        {\n      background-color: #2980b9;\n      color: white;\n    }\n
        tr:nth-child(even) {\n      background-color: #ecf0f1;\n    }\n
        .section {\n      margin-bottom: 30px;\n    }\n    .verdict {\n
        font-weight: bold;\n      color: #c0392b;\n    }\n
        </style>\n</head>\n<body>\n\n  <h1>Security Alert – File Integrity
        Event</h1>\n\n  <div class=\"section\">\n    <h2>File
        Information</h2>\n    <table>\n      <tr><th>SHA256</th>
        <td>275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd
        0f</td></tr>\n      <tr><th>SHA1</th>
        <td>3395856ce81f2b7382dee72602f798b642f14140</td></tr>\n      <tr>
        <th>MD5</th><td>44d88612fea8a8f36de82e1278abb02f</td></tr>\n
        <tr><th>Size (bytes)</th><td>68</td></tr>\n      <tr><th>Type</th>
        <td>Powershell (.ps1)</td></tr>\n      <tr><th>First Seen</th>
        <td>1582585760</td></tr>\n      <tr><th>Last Analysis</th>
        <td>1758384053</td></tr>\n      <tr><th>Link</th><td><a
```

Send a message — Execute step

Parameters | Settings | Docs

Sort your Gmail inbox using our pre-built Email triage agent ×

Credential to connect with: Gmail account

Resource: Message

Operation: Send

To: [redacted]

Subject: Alert!

Email Type: HTML

Message: `{{ $json.html }}`

<!DOCTYPE html> <html lang="en"> <head> <meta ch...

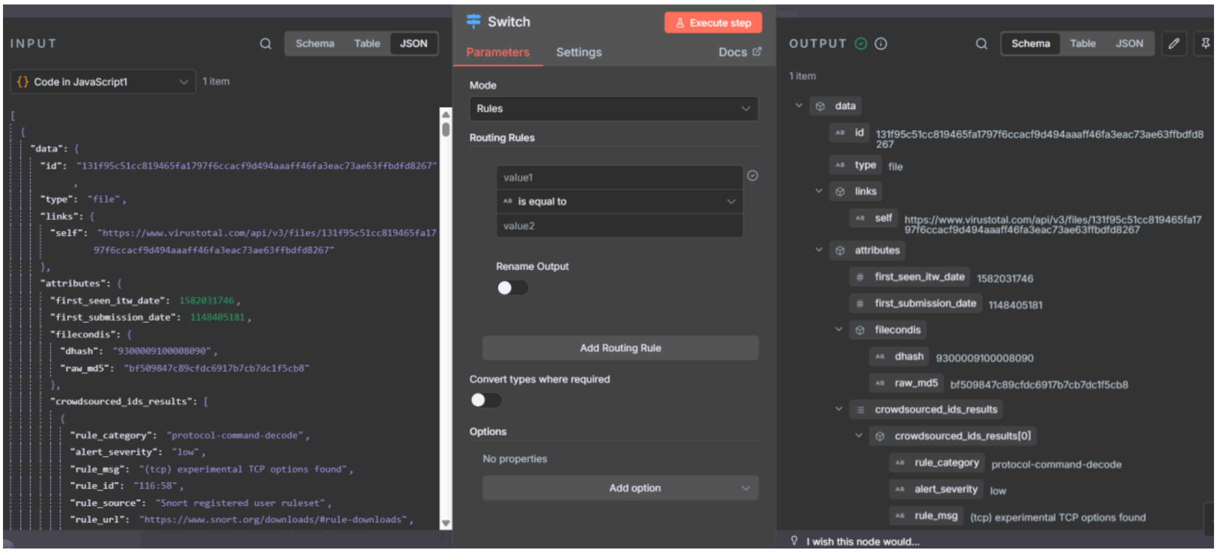
Options

OUTPUT — **Schema** | Table | JSON

1 item

```
id            199ab3cf76805007
threadId      199ab3cf76805007
labelIds
  labelIds[0] UNREAD
  labelIds[1] SENT
  labelIds[2] INBOX
```

I wish this node would...



INPUT — Schema | Table | **JSON**

Code in JavaScript1 ▾ 1 item

```
[
  {
    "data": {
      "id": "131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267"
        ,
      "type": "file",
      "links": {
        "self": "https://www.virustotal.com/api/v3/files/131f95c51cc819465fa17
            97f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267"
      },
      "attributes": {
        "first_seen_itw_date": 1582031746,
        "first_submission_date": 1148405181,
        "filecondis": {
          "dhash": "9300009100008090",
          "raw_md5": "bf509847c89cfdc6917b7cb7dc1f5cb8"
        },
        "crowdsourced_ids_results": [
          {
            "rule_category": "protocol-command-decode",
            "alert_severity": "low",
            "rule_msg": "(tcp) experimental TCP options found",
            "rule_id": "116:58",
            "rule_source": "Snort registered user ruleset",
            "rule_url": "https://www.snort.org/downloads/#rule-downloads",
```

Switch — Execute step

Parameters | Settings | Docs

Mode: Rules

Routing Rules

value1 — is equal to — value2

Rename Output: ○

Add Routing Rule

Convert types where required: ○

Options

No properties

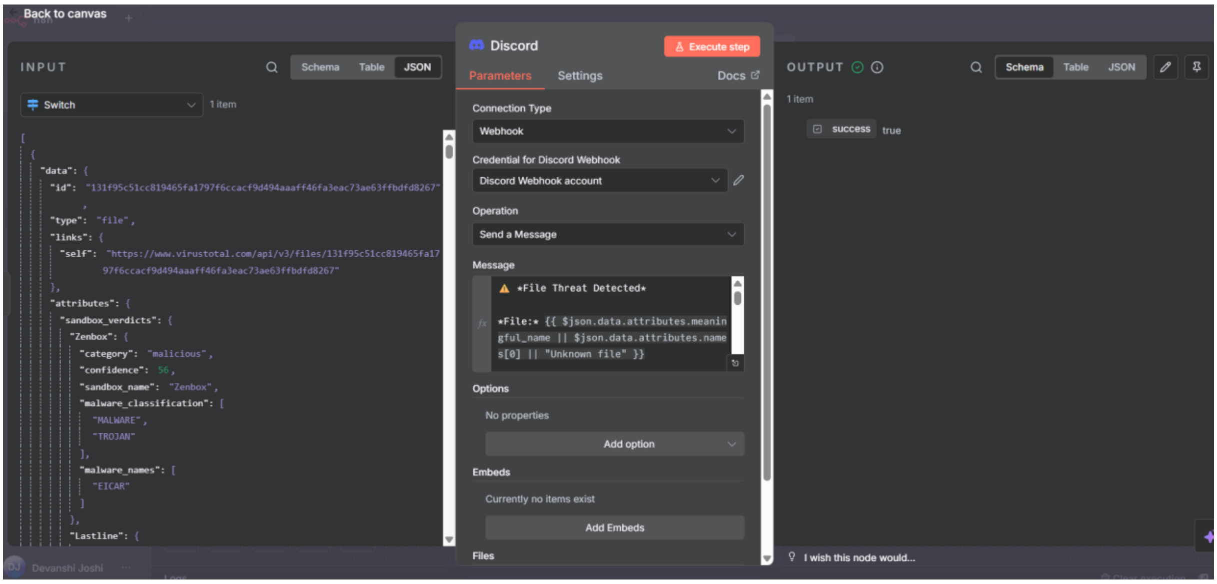
Add option

OUTPUT — **Schema** | Table | JSON

1 item

```
data
  id    131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8
        267
  type  file
  links
    self  https://www.virustotal.com/api/v3/files/131f95c51cc819465fa17
          97f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267
  attributes
    first_seen_itw_date     1582031746
    first_submission_date   1148405181
    filecondis
      dhash    9300009100008090
      raw_md5  bf509847c89cfdc6917b7cb7dc1f5cb8
    crowdsourced_ids_results
      crowdsourced_ids_results[0]
        rule_category   protocol-command-decode
        alert_severity  low
        rule_msg        (tcp) experimental TCP options found
```

I wish this node would...



Back to canvas

INPUT — Schema | Table | **JSON**

Switch ▾ 1 item

```
[
  {
    "data": {
      "id": "131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267"
        ,
      "type": "file",
      "links": {
        "self": "https://www.virustotal.com/api/v3/files/131f95c51cc819465fa17
            97f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267"
      },
      "attributes": {
        "sandbox_verdicts": {
          "Zenbox": {
            "category": "malicious",
            "confidence": 56,
            "sandbox_name": "Zenbox",
            "malware_classification": [
              "MALWARE",
              "TROJAN"
            ],
            "malware_names": [
              "EICAR"
            ]
          },
          "Lastline": {
```

Devanshi Joshi

Discord — Execute step

Parameters | Settings | Docs

Connection Type: Webhook

Credential for Discord Webhook: Discord Webhook account

Operation: Send a Message

Message:

```
⚠ *File Threat Detected*

*File:* {{ $json.data.attributes.meanin
gful_name || $json.data.attributes.name
s[0] || "Unknown file" }}
```

Options

No properties

Add option

Embeds

Currently no items exist

Add Embeds

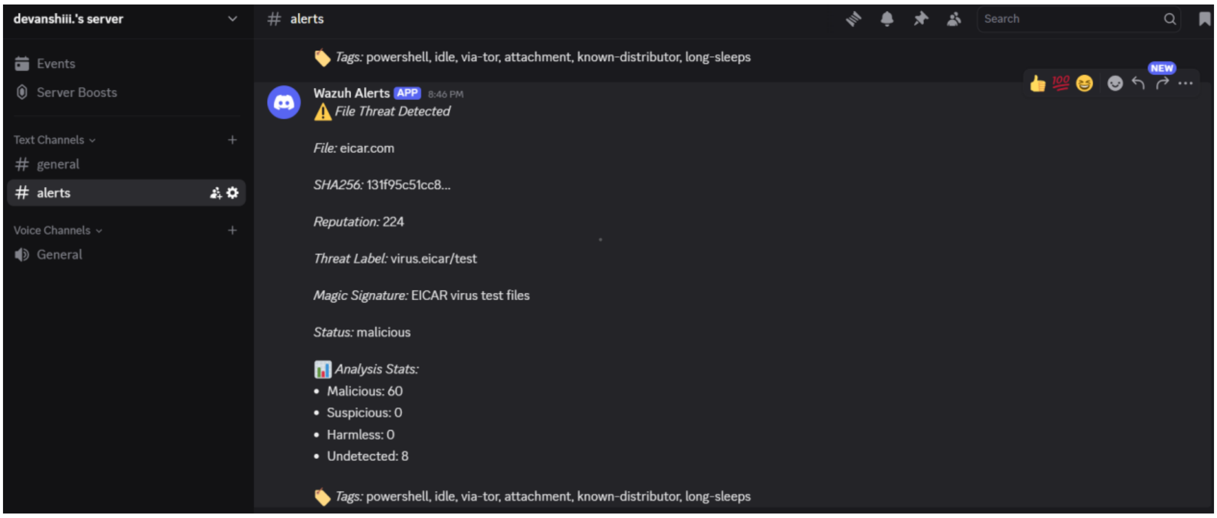
Files

OUTPUT — **Schema** | Table | JSON

1 item

```
success  true
```

I wish this node would...



🏷️ *Tags:* powershell, idle, via-tor, attachment, known-distributor, long-sleeps

Wazuh Alerts APP 8:46 PM

⚠️ *File Threat Detected*

File: eicar.com

SHA256: 131f95c51cc8...

Reputation: 224

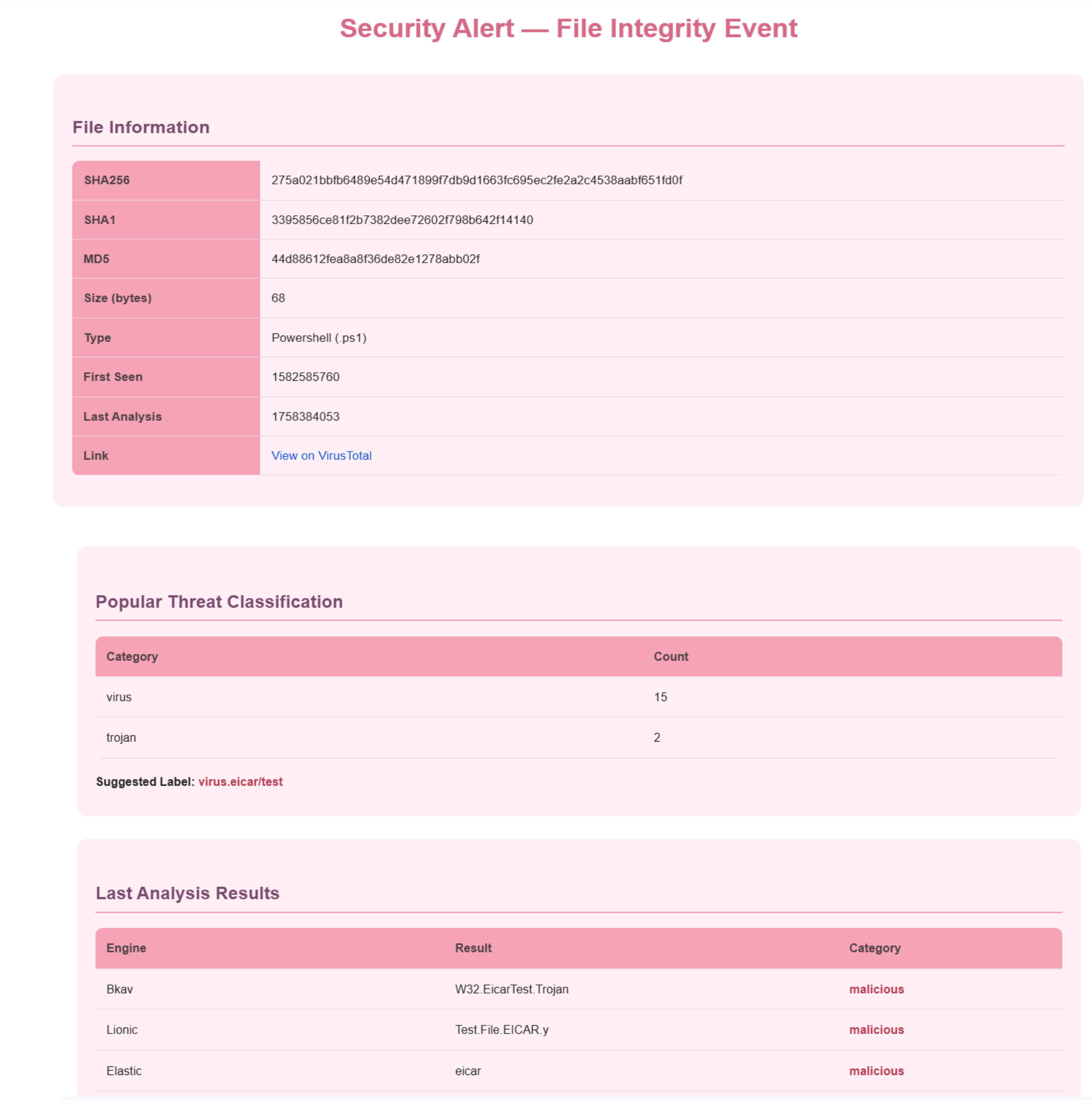
Threat Label: virus.eicar/test

Magic Signature: EICAR virus test files

Status: malicious

📊 *Analysis Stats:*
- Malicious: 60
- Suspicious: 0
- Harmless: 0
- Undetected: 8

🏷️ *Tags:* powershell, idle, via-tor, attachment, known-distributor, long-sleeps



Security Alert — File Integrity Event

File Information

SHA256	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
SHA1	3395856ce81f2b7382dee72602f798b642f14140
MD5	44d88612fea8a8f36de82e1278abb02f
Size (bytes)	68
Type	Powershell (.ps1)
First Seen	1582585760
Last Analysis	1758384053
Link	View on VirusTotal

Popular Threat Classification

Category	Count
virus	15
trojan	2

Suggested Label: **virus.eicar/test**

Last Analysis Results

Engine	Result	Category
Bkav	W32.EicarTest.Trojan	**malicious**
Lionic	Test.File.EICAR.y	**malicious**
Elastic	eicar	**malicious**

Votes & Reputation

Total Votes: **Harmless: 2207**, **Malicious: 397**

Reputation Score: **3687**

Crowdsourced AI Insight

EICAR is a test string used to detect and test antivirus software. It’s a “dummy virus” that triggers an antivirus engine to react, demonstrating its detection ability. It is **NOT a real virus**.