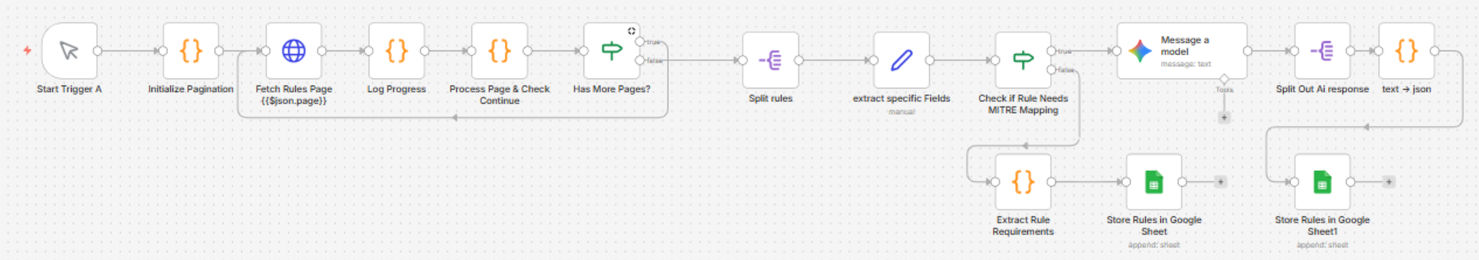
Automated SIEM Detection Coverage Lookup to MITRE ATT&CK

Trigger A

Implementation Details

Workflow Architecture



The n8n workflow consists of 14 interconnected nodes organized into a logical pipeline:

Phase 1: Initialization and Data Extraction

- Manual Trigger node to start the workflow on demand
- Pagination initialization to prepare for large-scale data retrieval
- API connection to Kibana detection engine

Phase 2: Rule Processing

- Iterative pagination handling to retrieve all rules
- Data parsing and field extraction
- Conditional routing based on MITRE mapping status

Phase 3: AI Enhancement and Storage

- AI-powered MITRE mapping for unmapped rules
- Data transformation and standardization
- Google Sheets storage for final inventory

Step-by-Step Implementation

Step 1: Workflow Initialization

##### Node: "Start Trigger A"**

- Type: Manual Trigger
- Purpose: Provides on-demand execution control for the workflow

##### Node: "Initialize Pagination"**

- Type: Code (JavaScript)
- Purpose: Sets up initial parameters for paginated API calls

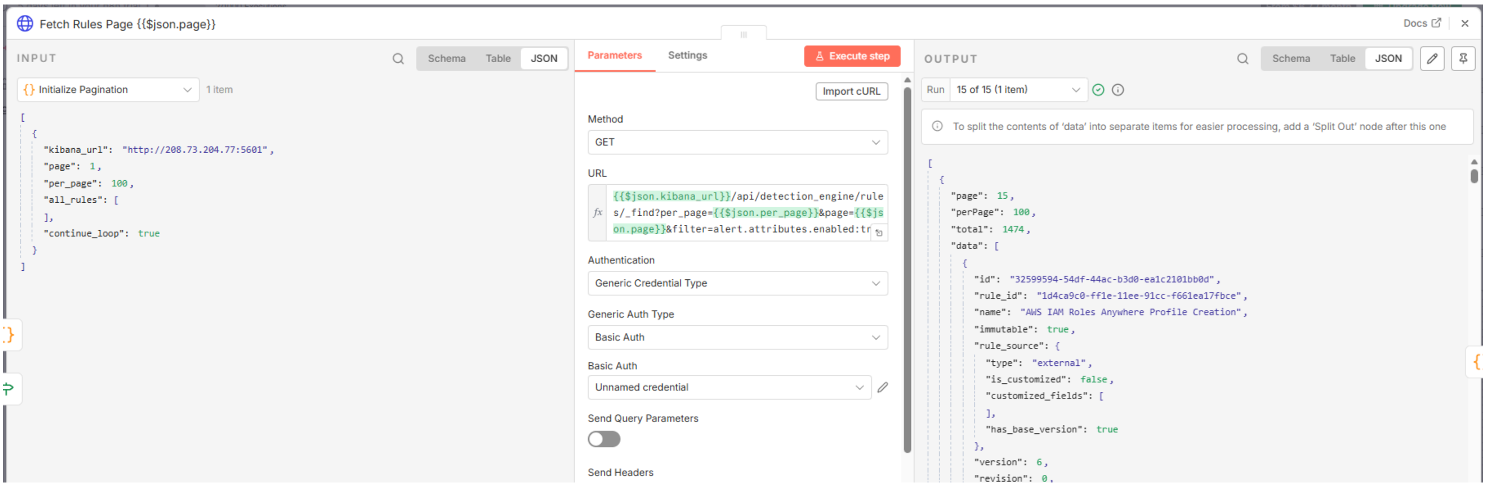
```
return {
  json: {
    kibana_url: 'http://208.73.204.77:5601',
    page: 1,
    per_page: 100,
    all_rules: [],
    continue_loop: true
  }
};
```

This initialization establishes:

- SIEM endpoint URL
- Starting page number
- Rules per page limit (100)
- Empty array to accumulate all rules
- Loop continuation flag

Step 2: Paginated Rule Extraction

##### Node: "Fetch Rules Page {{$json.page}}"**



Initialize Pagination 1 item

```
[
  {
    "kibana_url": "http://208.73.204.77:5601",
    "page": 1,
    "per_page": 100,
    "all_rules": [
    ],
    "continue_loop": true
  }
]
```

Method: GET

URL: {{$json.kibana_url}}/api/detection_engine/rules/_find?per_page={{$json.per_page}}&page={{$json.page}}&filter=alert.attributes.enabled:tr

Authentication: Generic Credential Type

Generic Auth Type: Basic Auth

Basic Auth: Unnamed credential

Send Query Parameters

Send Headers

Run 15 of 15 (1 item)

To split the contents of 'data' into separate items for easier processing, add a 'Split Out' node after this one

```
[
  {
    "page": 15,
    "perPage": 100,
    "total": 1474,
    "data": [
      {
        "id": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
        "rule_id": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
        "name": "AWS IAM Roles Anywhere Profile Creation",
        "immutable": true,
        "rule_source": {
          "type": "external",
          "is_customized": false,
          "customized_fields": [
          ],
          "has_base_version": true
        },
        "version": 6,
        "revision": 0,
```

- Type: HTTP Request
- Method: GET
- Authentication: HTTP Basic Auth
- Endpoint: `/api/detection_engine/rules/_find?per_page=100&page={{$json.page}}&filter=alert.attributes.enabled:true`

Key configuration:

- Custom headers: `kbn-xsrf: true` (required by Kibana API)
- Filter parameter: `alert.attributes.enabled:true` (only enabled rules)
- Dynamic page number from previous node

##### Node: "Log Progress"**

- Type: Code (JavaScript)
- Purpose: Provides visibility into extraction progress

```
const response = $input.first().json;
const page = response.page || 1;
const total = response.total || 0;
const dataLength = (response.data || []).length;

console.log(`📄 Fetched page ${page} - Got ${dataLength} rules out of ${total} total`);

return $input.all();
```

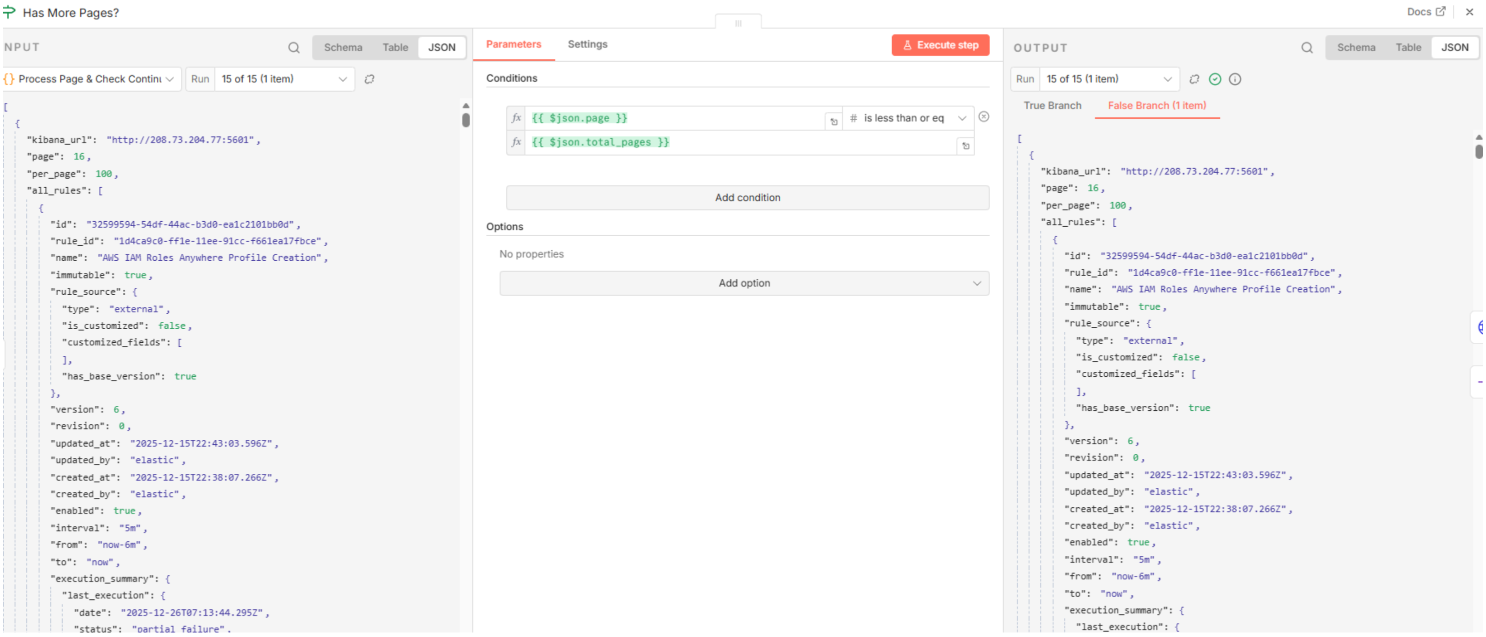
Step 3: Pagination Control

Node: "Process Page & Check Continue"**

- Type: Code (JavaScript)
- Purpose: Manages pagination state and determines when to stop

```
const currentState = $('Initialize Pagination').first().json;
const apiResponse = $input.first().json;

const rulesInPage = apiResponse.data || [];
const total = apiResponse.total || 0;
const currentPage = apiResponse.page || currentState.page;
const perPage = apiResponse.per_page || currentState.per_page;

const totalPages = Math.ceil(total / perPage);
const hasMorePages = currentPage < totalPages;

const allRules = [ ... currentState.all_rules,  ... rulesInPage];

return {
  json: {
    kibana_url: currentState.kibana_url,
    page: currentPage + 1,
    per_page: perPage,
    all_rules: allRules,
    continue_loop: hasMorePages,
    current_page: currentPage,
    total_pages: totalPages,
    total_rules: total,
    rules_fetched: allRules.length
  }
};
```

Node: "Has More Pages?"**



Process Page & Check Contin
Run 15 of 15 (1 item)

```
[
  {
    "kibana_url": "http://208.73.204.77:5601",
    "page": 16,
    "per_page": 100,
    "all_rules": [
      {
        "id": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
        "rule_id": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
        "name": "AWS IAM Roles Anywhere Profile Creation",
        "immutable": true,
        "rule_source": {
          "type": "external",
          "is_customized": false,
          "customized_fields": [
          ],
          "has_base_version": true
        },
        "version": 6,
        "revision": 0,
        "updated_at": "2025-12-15T22:43:03.596Z",
        "updated_by": "elastic",
        "created_at": "2025-12-15T22:38:07.266Z",
        "created_by": "elastic",
        "enabled": true,
        "interval": "5m",
        "from": "now-6m",
        "to": "now",
        "execution_summary": {
          "last_execution": {
            "date": "2025-12-26T07:13:44.295Z",
            "status": "partial failure",
```

Conditions

```
{{ $json.page }}   # is less than or eq
{{ $json.total_pages }}
```

Options

No properties

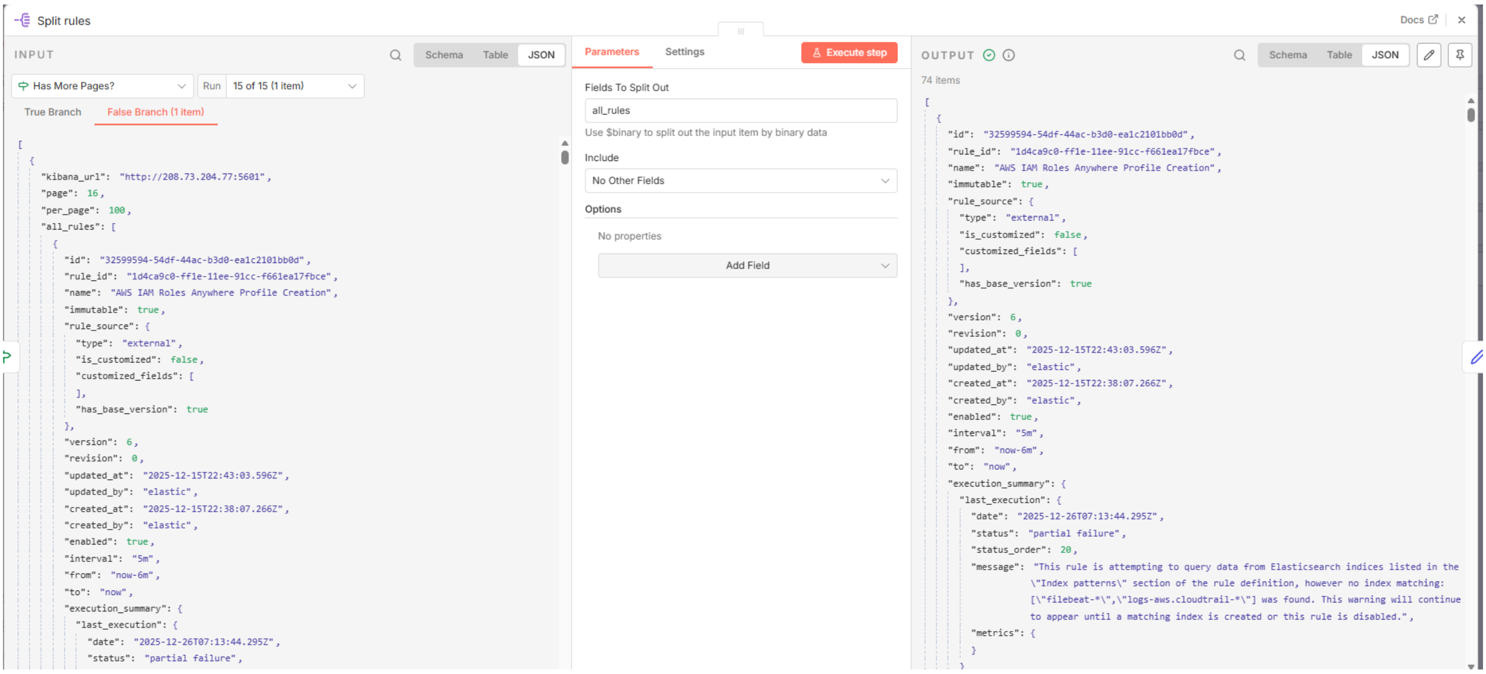
Run 15 of 15 (1 item)
True Branch
False Branch (1 item)

```
[
  {
    "kibana_url": "http://208.73.204.77:5601",
    "page": 16,
    "per_page": 100,
    "all_rules": [
      {
        "id": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
        "rule_id": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
        "name": "AWS IAM Roles Anywhere Profile Creation",
        "immutable": true,
        "rule_source": {
          "type": "external",
          "is_customized": false,
          "customized_fields": [
          ],
          "has_base_version": true
        },
        "version": 6,
        "revision": 0,
        "updated_at": "2025-12-15T22:43:03.596Z",
        "updated_by": "elastic",
        "created_at": "2025-12-15T22:38:07.266Z",
        "created_by": "elastic",
        "enabled": true,
        "interval": "5m",
        "from": "now-6m",
        "to": "now",
        "execution_summary": {
          "last_execution": {
```

- Type: IF Condition
- Logic: Compares current page against total pages
- True branch: Loops back to fetch next page
- False branch: Proceeds to rule processing

This creates a loop that continues until all pages are retrieved.

Step 4: Rule Data Splitting



Has More Pages?
Run 15 of 15 (1 item)
True Branch
False Branch (1 item)

```
[
  {
    "kibana_url": "http://208.73.204.77:5601",
    "page": 16,
    "per_page": 100,
    "all_rules": [
      {
        "id": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
        "rule_id": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
        "name": "AWS IAM Roles Anywhere Profile Creation",
        "immutable": true,
        "rule_source": {
          "type": "external",
          "is_customized": false,
          "customized_fields": [
          ],
          "has_base_version": true
        },
        "version": 6,
        "revision": 0,
        "updated_at": "2025-12-15T22:43:03.596Z",
        "updated_by": "elastic",
        "created_at": "2025-12-15T22:38:07.266Z",
        "created_by": "elastic",
        "enabled": true,
        "interval": "5m",
        "from": "now-6m",
        "to": "now",
        "execution_summary": {
          "last_execution": {
            "date": "2025-12-26T07:13:44.295Z",
            "status": "partial failure",
```

Fields To Split Out: all_rules

Use $binary to split out the input item by binary data

Include: No Other Fields

Options

No properties

74 items

```
[
  {
    "id": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
    "rule_id": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
    "name": "AWS IAM Roles Anywhere Profile Creation",
    "immutable": true,
    "rule_source": {
      "type": "external",
      "is_customized": false,
      "customized_fields": [
      ],
      "has_base_version": true
    },
    "version": 6,
    "revision": 0,
    "updated_at": "2025-12-15T22:43:03.596Z",
    "updated_by": "elastic",
    "created_at": "2025-12-15T22:38:07.266Z",
    "created_by": "elastic",
    "enabled": true,
    "interval": "5m",
    "from": "now-6m",
    "to": "now",
    "execution_summary": {
      "last_execution": {
        "date": "2025-12-26T07:13:44.295Z",
        "status": "partial failure",
        "status_order": 20,
        "message": "This rule is attempting to query data from Elasticsearch indices listed in the
                   \"Index patterns\" section of the rule definition, however no index matching:
                   [\"filebeat-*\",\"logs-aws.cloudtrail-*\"] was found. This warning will continue
                   to appear until a matching index is created or this rule is disabled.",
        "metrics": {
        }
      }
```

Node: "Split rules"**

- Type: Split Out
- Field: `all_rules`
- Purpose: Converts array of rules into individual items for processing

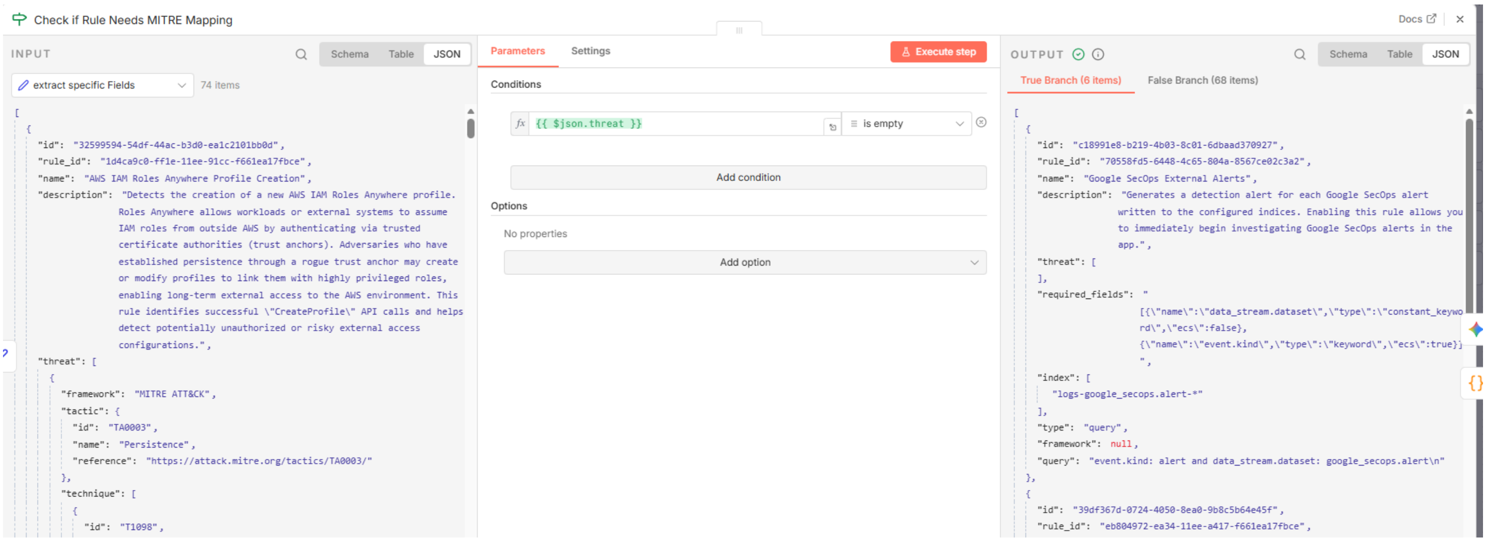
Node: "extract specific Fields"**

- Type: Set (Edit Fields)
- Purpose: Extracts essential fields from each rule for downstream processing

Fields extracted:

- `id`: Internal rule identifier
- `rule_id`: External rule identifier
- `name`: Rule name
- `description`: Rule description
- `threat`: MITRE ATT&CK mappings (array)
- `required_fields`: Fields needed for rule to execute
- `index`: Target log sources/indexes
- `type`: Rule type (query, eql, threshold, etc.)
- `framework`: Threat framework (MITRE ATT&CK)
- `query`: Detection query logic

Step 5: MITRE Mapping Decision



Check if Rule Needs MITRE Mapping

INPUT — Schema | Table | JSON

extract specific Fields — 74 items

```
[
  {
    "id": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
    "rule_id": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
    "name": "AWS IAM Roles Anywhere Profile Creation",
    "description": "Detects the creation of a new AWS IAM Roles Anywhere profile.
                   Roles Anywhere allows workloads or external systems to assume
                   IAM roles from outside AWS by authenticating via trusted
                   certificate authorities (trust anchors). Adversaries who have
                   established persistence through a rogue trust anchor may create
                   or modify profiles to link them with highly privileged roles,
                   enabling long-term external access to the AWS environment. This
                   rule identifies successful \"CreateProfile\" API calls and helps
                   detect potentially unauthorized or risky external access
                   configurations.",
    "threat": [
      {
        "framework": "MITRE ATT&CK",
        "tactic": {
          "id": "TA0003",
          "name": "Persistence",
          "reference": "https://attack.mitre.org/tactics/TA0003/"
        },
        "technique": [
          {
            "id": "T1098",
```

Parameters | Settings — Execute step

Conditions

{{ $json.threat }} — is empty

Add condition

Options

No properties

Add option

OUTPUT — Schema | Table | JSON — Docs

True Branch (6 items) | False Branch (68 items)

```
[
  {
    "id": "c18991e8-b219-4b03-8c01-6dbaad370927",
    "rule_id": "70558fd5-6448-4c65-804a-8567ce02c3a2",
    "name": "Google SecOps External Alerts",
    "description": "Generates a detection alert for each Google SecOps alert
                   written to the configured indices. Enabling this rule allows you
                   to immediately begin investigating Google SecOps alerts in the
                   app.",
    "threat": [
    ],
    "required_fields": "
                   [{\"name\":\"data_stream.dataset\",\"type\":\"constant_keywo
                   rd\",\"ecs\":false},
                   {\"name\":\"event.kind\",\"type\":\"keyword\",\"ecs\":true}]
                   ",
    "index": [
      "logs-google_secops.alert-*"
    ],
    "type": "query",
    "framework": null,
    "query": "event.kind: alert and data_stream.dataset: google_secops.alert\n"
  },
  {
    "id": "39df367d-0724-4050-8ea0-9b8c5b64e45f",
    "rule_id": "eb804972-ea34-11ee-a417-f661ea17fbce",
```

Node: "Check if Rule Needs MITRE Mapping"**

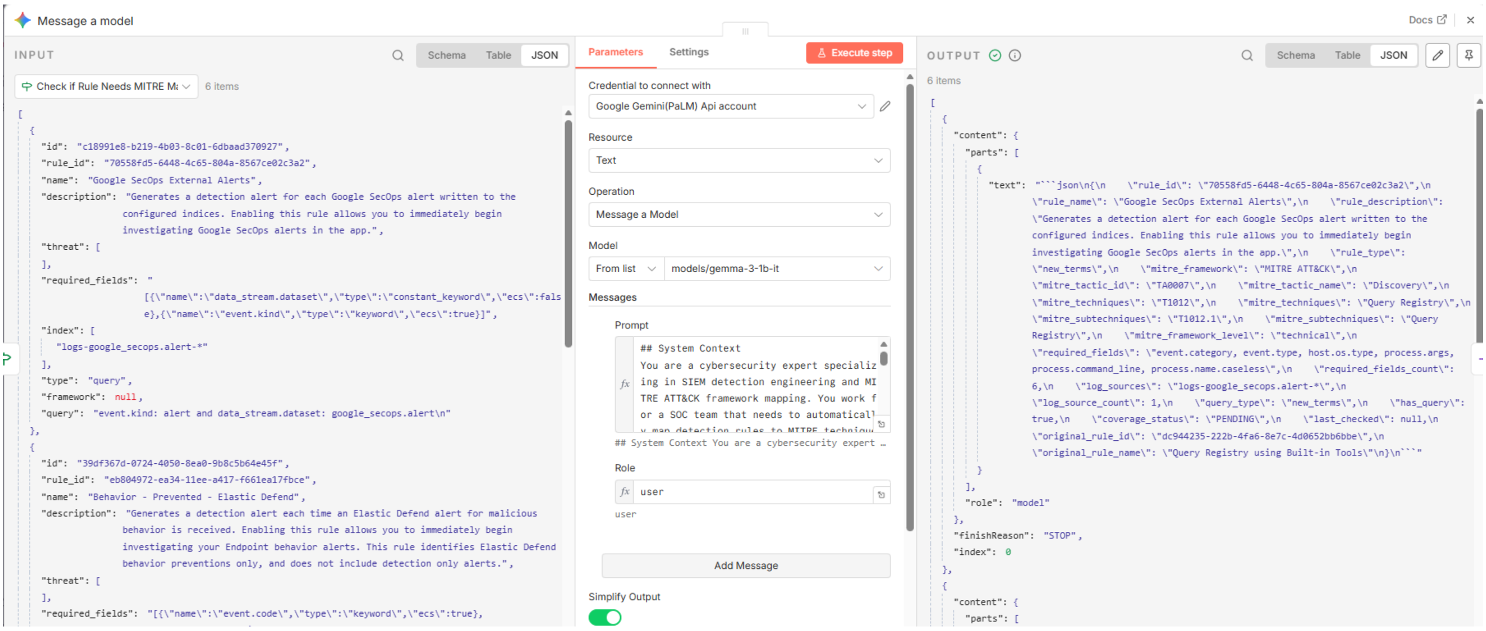
- Type: IF Condition
- Condition: `{{ $json.threat }}` is empty
- Purpose: Routes rules based on existing MITRE mappings

Logic:

- If `threat` array is empty → Route to AI mapping
- If `threat` array has data → Route to direct processing

This optimization prevents unnecessary AI API calls for rules that already have MITRE mappings.

Step 6: AI-Powered MITRE Mapping



Message a model

INPUT — Schema | Table | JSON

Check if Rule Needs MITRE Ma — 6 items

```
[
  {
    "id": "c18991e8-b219-4b03-8c01-6dbaad370927",
    "rule_id": "70558fd5-6448-4c65-804a-8567ce02c3a2",
    "name": "Google SecOps External Alerts",
    "description": "Generates a detection alert for each Google SecOps alert written to the
                   configured indices. Enabling this rule allows you to immediately begin
                   investigating Google SecOps alerts in the app.",
    "threat": [
    ],
    "required_fields": "
                   [{\"name\":\"data_stream.dataset\",\"type\":\"constant_keyword\",\"ecs\":fals
                   e},{\"name\":\"event.kind\",\"type\":\"keyword\",\"ecs\":true}]",
    "index": [
      "logs-google_secops.alert-*"
    ],
    "type": "query",
    "framework": null,
    "query": "event.kind: alert and data_stream.dataset: google_secops.alert\n"
  },
  {
    "id": "39df367d-0724-4050-8ea0-9b8c5b64e45f",
    "rule_id": "eb804972-ea34-11ee-a417-f661ea17fbce",
    "name": "Behavior - Prevented - Elastic Defend",
    "description": "Generates a detection alert each time an Elastic Defend alert for malicious
                   behavior is received. Enabling this rule allows you to immediately begin
                   investigating your Endpoint behavior alerts. This rule identifies Elastic Defend
                   behavior preventions only, and does not include detection only alerts.",
    "threat": [
    ],
    "required_fields": "[{\"name\":\"event.code\",\"type\":\"keyword\",\"ecs\":true},
```

Parameters | Settings — Execute step

Credential to connect with: Google Gemini(PaLM) Api account

Resource: Text

Operation: Message a Model

Model: From list — models/gemma-3-1b-it

Messages

Prompt

```
## System Context
You are a cybersecurity expert specializ
ing in SIEM detection engineering and MI
TRE ATT&CK framework mapping. You work f
or a SOC team that needs to automaticall
y map detection rules to MITRE techniqu
```

## System Context You are a cybersecurity expert …

Role: user

user

Add Message

Simplify Output

OUTPUT — 6 items — Schema | Table | JSON — Docs

```
[
  {
    "content": {
      "parts": [
        {
          "text": "```json\n{\n    \"rule_id\": \"70558fd5-6448-4c65-804a-8567ce02c3a2\",\n
                 \"rule_name\": \"Google SecOps External Alerts\",\n    \"rule_description\":
                 \"Generates a detection alert for each Google SecOps alert written to the
                 configured indices. Enabling this rule allows you to immediately begin
                 investigating Google SecOps alerts in the app.\",\n    \"rule_type\":
                 \"new_terms\",\n    \"mitre_framework\": \"MITRE ATT&CK\",\n
                 \"mitre_tactic_id\": \"TA0007\",\n    \"mitre_tactic_name\": \"Discovery\",\n
                 \"mitre_techniques\": \"T1012\",\n    \"mitre_techniques\": \"Query Registry\",\n
                 \"mitre_subtechniques\": \"T1012.1\",\n    \"mitre_subtechniques\": \"Query
                 Registry\",\n    \"mitre_framework_level\": \"technical\",\n
                 \"required_fields\": \"event.category, event.type, host.os.type, process.args,
                 process.command_line, process.name.caseless\",\n    \"required_fields_count\":
                 6,\n    \"log_sources\": \"logs-google_secops.alert-*\",\n
                 \"log_source_count\": 1,\n    \"query_type\": \"new_terms\",\n    \"has_query\":
                 true,\n    \"coverage_status\": \"PENDING\",\n    \"last_checked\": null,\n
                 \"original_rule_id\": \"dc944235-222b-4fa6-8e7c-4d0652bb6bbe\",\n
                 \"original_rule_name\": \"Query Registry using Built-in Tools\"\n}\n```"
        }
      ],
      "role": "model"
    },
    "finishReason": "STOP",
    "index": 0
  },
  {
    "content": {
      "parts": [
```

Node: "Message a model"**

- Type: Google Gemini AI
- Model: `models/gemma-3-1b-it`
- Purpose: Analyzes rule and returns MITRE ATT&CK mapping

AI Prompt Structure:

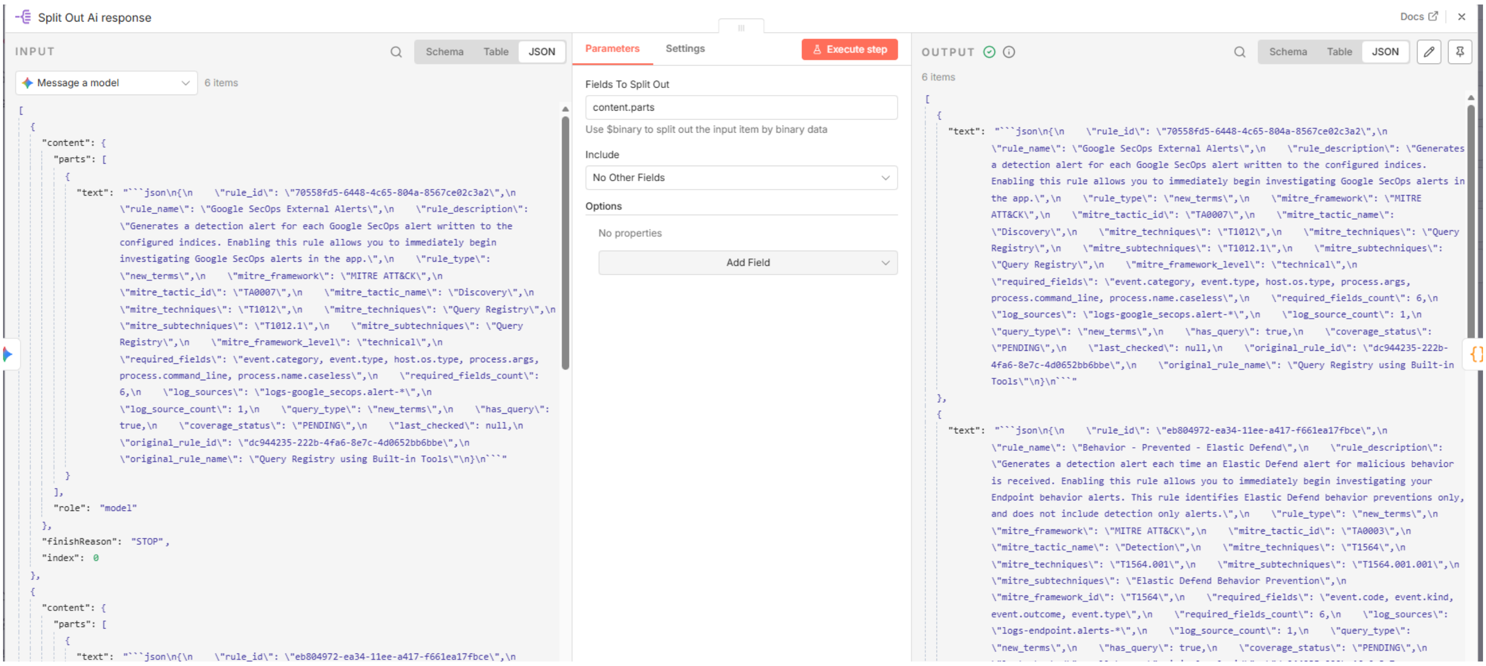
```
## System Context
You are a cybersecurity expert specializing in SIEM detection engineering and MITRE ATT&CK framework mapping. You work for a SOC team that needs to
automatically map detection rules to MITRE techniques.

## Task Description
Analyze the given SIEM detection rule and identify which MITRE ATT&CK technique(s) it detects. Consider the rule logic, query patterns, and context.

## Output Requirements
Return ONLY a JSON object with this exact structure:
{
    "rule_id": "ded09d02-0137-4ccc-8005-c45e617e8d4c",
    "rule_name": "Query Registry using Built-in Tools",
    "rule_description": "This rule identifies the execution of commands that can be used to query the Windows Registry. Adversaries may query the registry to
gain situational awareness about the host, like installed security software, programs and settings.",
```

```
    "rule_type": "new_terms",
    "mitre_framework": "MITRE ATT&CK",
    "mitre_tactic_id": "TA0007",
    "mitre_tactic_name": "Discovery",
    "mitre_techniques": "T1012",
    "mitre_technique_names": "Query Registry",
    "mitre_subtechniques": "",
    "required_fields": "event.category, event.type, host.os.type, process.args, process.command_line, process.name.caseless",
    "required_fields_count": 6,
    "log_sources": "logs-endpoint.events.process-*",
    "log_source_count": 1,
    "query_type": "new_terms",
    "has_query": true,
    "coverage_status": "PENDING",
    "last_checked": null,
    "original_rule_id": "dc944235-222b-4fa6-8e7c-4d0652bb6bbe",
    "original_rule_name": "Query Registry using Built-in Tools"
  },


## Critical Rules
1. **ONLY return valid JSON**, no additional text
2. **Use exact MITRE IDs** from official ATT&CK framework
3. **If uncertain**, use parent technique instead of sub-technique
4. **Never** return multiple techniques in one mapping
5. **Always** include all four fields in the JSON

## Ready for Analysis
Now analyze the following rule and provide MITRE mapping:
id:{{ $json.id }}
rule_id:{{ $json.rule_id }}
name:{{ $json.name }}
description:{{ $json.description }}
required_filed:{{ $json.required_fields }}
index :{{ $json.index }}
query: {{ $json.query }}
```

The prompt provides:

- Rule context and metadata
- Query logic for analysis
- Strict JSON output format requirements
- Guidelines for accurate MITRE mapping

Node: "Split Out Ai response"**



```
[
  {
    "content": {
      "parts": [
        {
          "text": "```json\n{\n    \"rule_id\": \"70558fd5-6448-4c65-804a-8567ce02c3a2\",\n
                \"rule_name\": \"Google SecOps External Alerts\",\n    \"rule_description\":
                \"Generates a detection alert for each Google SecOps alert written to the
                configured indices. Enabling this rule allows you to immediately begin
                investigating Google SecOps alerts in the app.\",\n    \"rule_type\":
                \"new_terms\",\n    \"mitre_framework\": \"MITRE ATT&CK\",\n
                \"mitre_tactic_id\": \"TA0007\",\n    \"mitre_tactic_name\": \"Discovery\",\n
                \"mitre_techniques\": \"T1012\",\n    \"mitre_techniques\": \"Query Registry\",\n
                \"mitre_subtechniques\": \"T1012.1\",\n    \"mitre_subtechniques\": \"Query
                Registry\",\n    \"mitre_framework_level\": \"technical\",\n
                \"required_fields\": \"event.category, event.type, host.os.type, process.args,
                process.command_line, process.name.caseless\",\n    \"required_fields_count\":
                6,\n    \"log_sources\": \"logs-google_secops.alert-*\",\n
                \"log_source_count\": 1,\n    \"query_type\": \"new_terms\",\n    \"has_query\":
                true,\n    \"coverage_status\": \"PENDING\",\n    \"last_checked\": null,\n
                \"original_rule_id\": \"dc944235-222b-4fa6-8e7c-4d0652bb6bbe\",\n
                \"original_rule_name\": \"Query Registry using Built-in Tools\"\n}\n```"
        }
      ],
      "role": "model"
    },
    "finishReason": "STOP",
    "index": 0
  },
  {
    "content": {
      "parts": [
        {
          "text": "```json\n{\n    \"rule_id\": \"eb804972-ea34-11ee-a417-f661ea17fbce\",\n
```

Fields To Split Out
content.parts
Use $binary to split out the input item by binary data

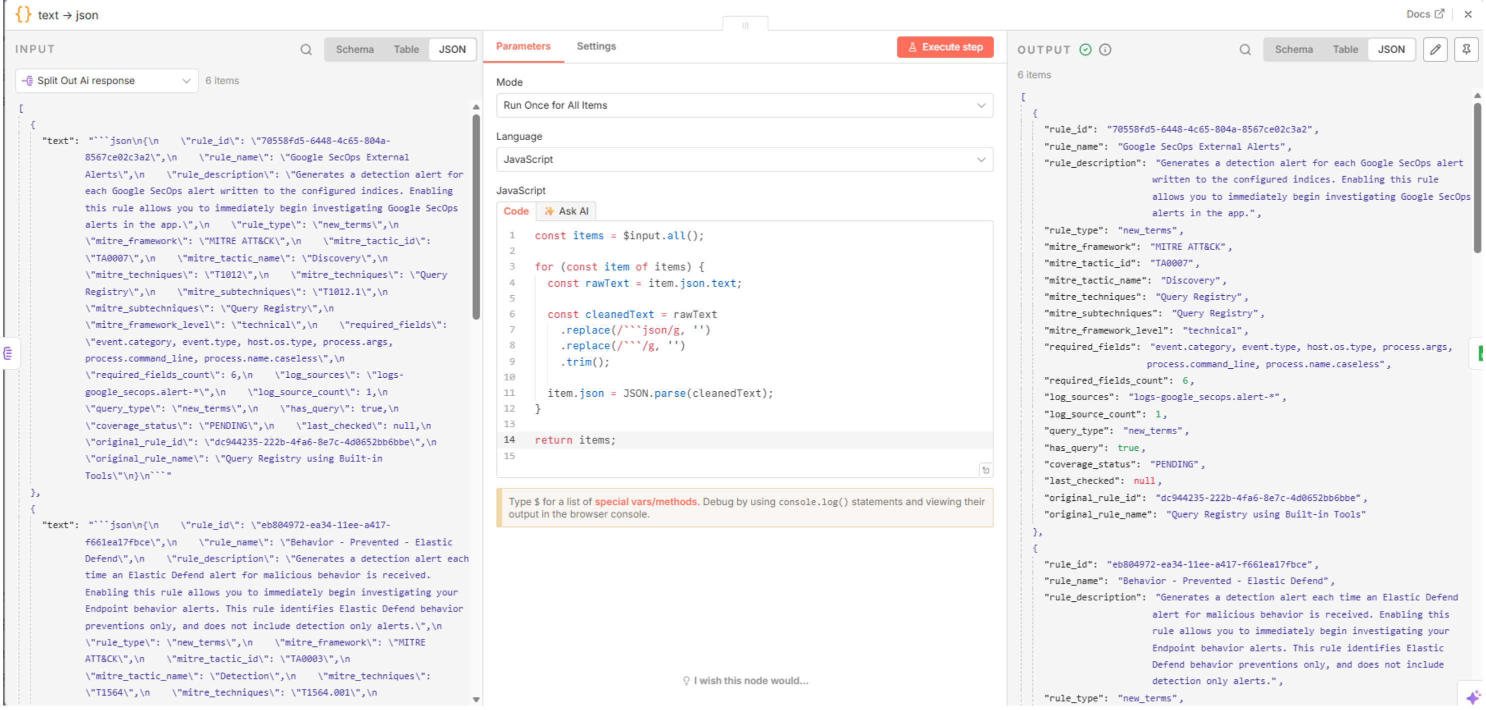
Include
No Other Fields

Options
No properties

```
[
  {
    "text": "```json\n{\n    \"rule_id\": \"70558fd5-6448-4c65-804a-8567ce02c3a2\",\n
          \"rule_name\": \"Google SecOps External Alerts\",\n    \"rule_description\": \"Generates
          a detection alert for each Google SecOps alert written to the configured indices.
          Enabling this rule allows you to immediately begin investigating Google SecOps alerts in
          the app.\",\n    \"rule_type\": \"new_terms\",\n    \"mitre_framework\": \"MITRE
          ATT&CK\",\n    \"mitre_tactic_id\": \"TA0007\",\n    \"mitre_tactic_name\":
          \"Discovery\",\n    \"mitre_techniques\": \"T1012\",\n    \"mitre_techniques\": \"Query
          Registry\",\n    \"mitre_subtechniques\": \"T1012.1\",\n    \"mitre_subtechniques\":
          \"Query Registry\",\n    \"mitre_framework_level\": \"technical\",\n
          \"required_fields\": \"event.category, event.type, host.os.type, process.args,
          process.command_line, process.name.caseless\",\n    \"required_fields_count\": 6,\n
          \"log_sources\": \"logs-google_secops.alert-*\",\n    \"log_source_count\": 1,\n
          \"query_type\": \"new_terms\",\n    \"has_query\": true,\n    \"coverage_status\":
          \"PENDING\",\n    \"last_checked\": null,\n    \"original_rule_id\": \"dc944235-222b-
          4fa6-8e7c-4d0652bb6bbe\",\n    \"original_rule_name\": \"Query Registry using Built-in
          Tools\"\n}\n```"
  },
  {
    "text": "```json\n{\n    \"rule_id\": \"eb804972-ea34-11ee-a417-f661ea17fbce\",\n
          \"rule_name\": \"Behavior - Prevented - Elastic Defend\",\n    \"rule_description\":
          \"Generates a detection alert each time an Elastic Defend alert for malicious behavior
          is received. Enabling this rule allows you to immediately begin investigating your
          Endpoint behavior alerts. This rule identifies Elastic Defend behavior preventions only,
          and does not include detection only alerts.\",\n    \"rule_type\": \"new_terms\",\n
          \"mitre_framework\": \"MITRE ATT&CK\",\n    \"mitre_tactic_id\": \"TA0003\",\n
          \"mitre_tactic_name\": \"Detection\",\n    \"mitre_techniques\": \"T1564\",\n
          \"mitre_techniques\": \"T1564.001\",\n    \"mitre_subtechniques\": \"T1564.001.001\",\n
          \"mitre_subtechniques\": \"Elastic Defend Behavior Prevention\",\n
          \"mitre_framework_id\": \"T1564\",\n    \"required_fields\": \"event.code, event.kind,
          event.outcome, event.type\",\n    \"required_fields_count\": 6,\n    \"log_sources\":
          \"logs-endpoint.alerts-*\",\n    \"log_source_count\": 1,\n    \"query_type\":
          \"new_terms\",\n    \"has_query\": true,\n    \"coverage_status\": \"PENDING\",\n
```

- Type: Split Out
- Field: `content.parts`
- Purpose: Extracts the AI response text from the API response structure

Node: "text -> json"**



```
[
  {
    "text": "```json\n{\n    \"rule_id\": \"70558fd5-6448-4c65-804a-
            8567ce02c3a2\",\n    \"rule_name\": \"Google SecOps External
            Alerts\",\n    \"rule_description\": \"Generates a detection alert for
            each Google SecOps alert written to the configured indices. Enabling
            this rule allows you to immediately begin investigating Google SecOps
            alerts in the app.\",\n    \"rule_type\": \"new_terms\",\n
            \"mitre_framework\": \"MITRE ATT&CK\",\n    \"mitre_tactic_id\":
            \"TA0007\",\n    \"mitre_tactic_name\": \"Discovery\",\n
            \"mitre_techniques\": \"T1012\",\n    \"mitre_techniques\": \"Query
            Registry\",\n    \"mitre_subtechniques\": \"T1012.1\",\n
            \"mitre_subtechniques\": \"Query Registry\",\n
            \"mitre_framework_level\": \"technical\",\n    \"required_fields\":
            \"event.category, event.type, host.os.type, process.args,
            process.command_line, process.name.caseless\",\n
            \"required_fields_count\": 6,\n    \"log_sources\": \"logs-
            google_secops.alert-*\",\n    \"log_source_count\": 1,\n
            \"query_type\": \"new_terms\",\n    \"has_query\": true,\n
            \"coverage_status\": \"PENDING\",\n    \"last_checked\": null,\n
            \"original_rule_id\": \"dc944235-222b-4fa6-8e7c-4d0652bb6bbe\",\n
            \"original_rule_name\": \"Query Registry using Built-in
            Tools\"\n}\n```"
  },
  {
    "text": "```json\n{\n    \"rule_id\": \"eb804972-ea34-11ee-a417-
            f661ea17fbce\",\n    \"rule_name\": \"Behavior - Prevented - Elastic
            Defend\",\n    \"rule_description\": \"Generates a detection alert each
            time an Elastic Defend alert for malicious behavior is received.
            Enabling this rule allows you to immediately begin investigating your
            Endpoint behavior alerts. This rule identifies Elastic Defend behavior
            preventions only, and does not include detection only alerts.\",\n
            \"rule_type\": \"new_terms\",\n    \"mitre_framework\": \"MITRE
            ATT&CK\",\n    \"mitre_tactic_id\": \"TA0003\",\n
            \"mitre_tactic_name\": \"Detection\",\n    \"mitre_techniques\":
            \"T1564\",\n    \"mitre_techniques\": \"T1564.001\",\n
```

Mode

Run Once for All Items

Language

JavaScript

JavaScript

```
const items = $input.all();

for (const item of items) {
  const rawText = item.json.text;

  const cleanedText = rawText
    .replace(/```json/g, '')
    .replace(/```/g, '')
    .trim();

  item.json = JSON.parse(cleanedText);
}

return items;
```

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

```
[
  {
    "rule_id": "70558fd5-6448-4c65-804a-8567ce02c3a2",
    "rule_name": "Google SecOps External Alerts",
    "rule_description": "Generates a detection alert for each Google SecOps alert
                         written to the configured indices. Enabling this rule
                         allows you to immediately begin investigating Google SecOps
                         alerts in the app.",
    "rule_type": "new_terms",
    "mitre_framework": "MITRE ATT&CK",
    "mitre_tactic_id": "TA0007",
    "mitre_tactic_name": "Discovery",
    "mitre_techniques": "Query Registry",
    "mitre_subtechniques": "Query Registry",
    "mitre_framework_level": "technical",
    "required_fields": "event.category, event.type, host.os.type, process.args,
                        process.command_line, process.name.caseless",
    "required_fields_count": 6,
    "log_sources": "logs-google_secops.alert-*",
    "log_source_count": 1,
    "query_type": "new_terms",
    "has_query": true,
    "coverage_status": "PENDING",
    "last_checked": null,
    "original_rule_id": "dc944235-222b-4fa6-8e7c-4d0652bb6bbe",
    "original_rule_name": "Query Registry using Built-in Tools"
  },
  {
    "rule_id": "eb804972-ea34-11ee-a417-f661ea17fbce",
    "rule_name": "Behavior - Prevented - Elastic Defend",
    "rule_description": "Generates a detection alert each time an Elastic Defend
                         alert for malicious behavior is received. Enabling this
                         rule allows you to immediately begin investigating your
                         Endpoint behavior alerts. This rule identifies Elastic
                         Defend behavior preventions only, and does not include
                         detection only alerts.",
    "rule_type": "new_terms",
```

- Type: Code (JavaScript)
- Purpose: Cleans and parses AI response into JSON

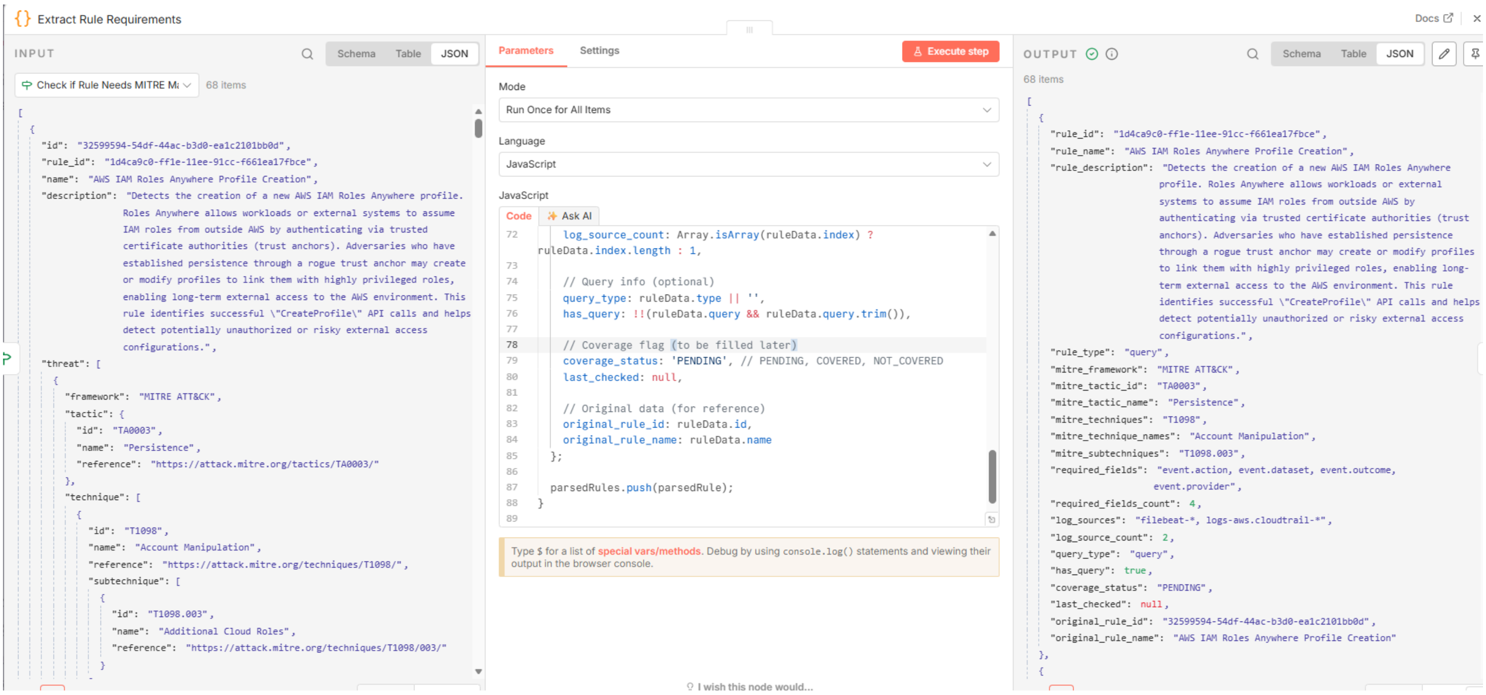
```
const items = $input.all();

for (const item of items) {
  const rawText = item.json.text;

  const cleanedText = rawText
    .replace(/```json/g, '')
    .replace(/```/g, '')
    .trim();

  item.json = JSON.parse(cleanedText);
}

return items;
```

This handles:

- Removal of markdown code blocks
- Trimming whitespace
- JSON parsing with error handling

Step 7: Rule Requirements Extraction

Node: "Extract Rule Requirements"**



```
[
  {
    "id": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
    "rule_id": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
    "name": "AWS IAM Roles Anywhere Profile Creation",
    "description": "Detects the creation of a new AWS IAM Roles Anywhere profile.
                   Roles Anywhere allows workloads or external systems to assume
                   IAM roles from outside AWS by authenticating via trusted
                   certificate authorities (trust anchors). Adversaries who have
                   established persistence through a rogue trust anchor may create
                   or modify profiles to link them with highly privileged roles,
                   enabling long-term external access to the AWS environment. This
                   rule identifies successful \"CreateProfile\" API calls and helps
                   detect potentially unauthorized or risky external access
                   configurations.",
    "threat": [
      {
        "framework": "MITRE ATT&CK",
        "tactic": {
          "id": "TA0003",
          "name": "Persistence",
          "reference": "https://attack.mitre.org/tactics/TA0003/"
        },
        "technique": [
          {
            "id": "T1098",
            "name": "Account Manipulation",
            "reference": "https://attack.mitre.org/techniques/T1098/",
            "subtechnique": [
              {
                "id": "T1098.003",
                "name": "Additional Cloud Roles",
                "reference": "https://attack.mitre.org/techniques/T1098/003/"
              }
```

Mode

Run Once for All Items

Language

JavaScript

JavaScript

```
      log_source_count: Array.isArray(ruleData.index) ? ruleData.index.length : 1,

      // Query info (optional)
      query_type: ruleData.type || '',
      has_query: !!(ruleData.query && ruleData.query.trim()),

      // Coverage flag (to be filled later)
      coverage_status: 'PENDING', // PENDING, COVERED, NOT_COVERED
      last_checked: null,

      // Original data (for reference)
      original_rule_id: ruleData.id,
      original_rule_name: ruleData.name
    };

    parsedRules.push(parsedRule);
  }

```

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

```
[
  {
    "rule_id": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
    "rule_name": "AWS IAM Roles Anywhere Profile Creation",
    "rule_description": "Detects the creation of a new AWS IAM Roles Anywhere
                         profile. Roles Anywhere allows workloads or external
                         systems to assume IAM roles from outside AWS by
                         authenticating via trusted certificate authorities (trust
                         anchors). Adversaries who have established persistence
                         through a rogue trust anchor may create or modify profiles
                         to link them with highly privileged roles, enabling long-
                         term external access to the AWS environment. This rule
                         identifies successful \"CreateProfile\" API calls and helps
                         detect potentially unauthorized or risky external access
                         configurations.",
    "rule_type": "query",
    "mitre_framework": "MITRE ATT&CK",
    "mitre_tactic_id": "TA0003",
    "mitre_tactic_name": "Persistence",
    "mitre_techniques": "T1098",
    "mitre_technique_names": "Account Manipulation",
    "mitre_subtechniques": "T1098.003",
    "required_fields": "event.action, event.dataset, event.outcome,
                        event.provider",
    "required_fields_count": 4,
    "log_sources": "filebeat-*, logs-aws.cloudtrail-*",
    "log_source_count": 2,
    "query_type": "query",
    "has_query": true,
    "coverage_status": "PENDING",
    "last_checked": null,
    "original_rule_id": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
    "original_rule_name": "AWS IAM Roles Anywhere Profile Creation"
  },
  {
```

- Type: Code (JavaScript)
- Purpose: Parses and structures rule metadata for rules with existing MITRE mappings

Key processing logic:

```
// Extract MITRE technique(s) - handle multiple techniques
let mitreTechniques = [];
if (ruleData.threat && Array.isArray(ruleData.threat)) {
  for (const threat of ruleData.threat) {
    if (threat.technique && Array.isArray(threat.technique)) {
      for (const tech of threat.technique) {
        const technique = {
          id: tech.id || '',
          name: tech.name || '',
          subtechnique: tech.subtechnique && Array.isArray(tech.subtechnique)
            ? tech.subtechnique.map(st => ({ id: st.id, name: st.name }))
            : []
        };
        mitreTechniques.push(technique);
      }
    }
  }
}

// Parse required_fields from JSON string
let requiredFields = [];
try {
  if (ruleData.required_fields && ruleData.required_fields !== '[]') {
    const fieldsJson = JSON.parse(ruleData.required_fields);
    if (Array.isArray(fieldsJson)) {
      requiredFields = fieldsJson.map(field => field.name || 'unknown');
    }
  }
} catch (error) {
  requiredFields = ['ERROR_PARSING_FIELDS'];
}
```

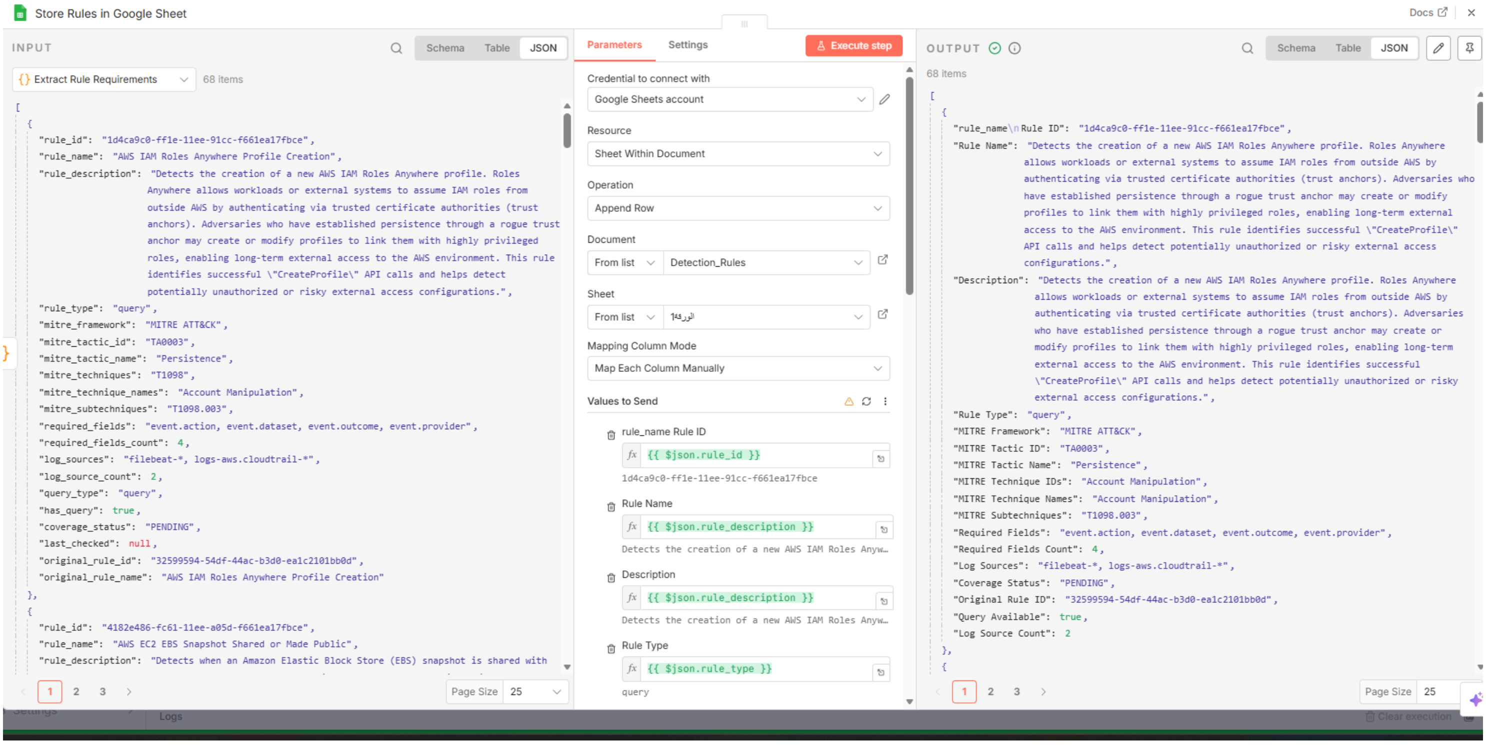
The code handles:

- Nested MITRE technique arrays
- Sub-technique extraction
- JSON string parsing for required fields
- Error handling for malformed data
- Array formatting for log sources

Output structure:

```
{
  rule_id: "...",
  rule_name: "...",
  rule_description: "...",
  rule_type: "...",
  mitre_framework: "MITRE ATT&CK",
  mitre_tactic_id: "...",
  mitre_tactic_name: "...",
  mitre_techniques: "T1012, T1082",
  mitre_technique_names: "Query Registry, System Information Discovery",
  mitre_subtechniques: "T1012.001",
  required_fields: "event.category, host.os.type, process.name",
  required_fields_count: 3,
  log_sources: "logs-endpoint.events.process-*",
  log_source_count: 1,
  query_type: "query",
  has_query: true,
  coverage_status: "PENDING",
  original_rule_id: "..."
}
```

Step 8: Data Storage



Extract Rule Requirements — 68 items

```
[
  {
    "rule_id": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
    "rule_name": "AWS IAM Roles Anywhere Profile Creation",
    "rule_description": "Detects the creation of a new AWS IAM Roles Anywhere profile. Roles
                        Anywhere allows workloads or external systems to assume IAM roles from
                        outside AWS by authenticating via trusted certificate authorities (trust
                        anchors). Adversaries who have established persistence through a rogue trust
                        anchor may create or modify profiles to link them with highly privileged
                        roles, enabling long-term external access to the AWS environment. This rule
                        identifies successful \"CreateProfile\" API calls and helps detect
                        potentially unauthorized or risky external access configurations.",
    "rule_type": "query",
    "mitre_framework": "MITRE ATT&CK",
    "mitre_tactic_id": "TA0003",
    "mitre_tactic_name": "Persistence",
    "mitre_techniques": "T1098",
    "mitre_technique_names": "Account Manipulation",
    "mitre_subtechniques": "T1098.003",
    "required_fields": "event.action, event.dataset, event.outcome, event.provider",
    "required_fields_count": 4,
    "log_sources": "filebeat-*, logs-aws.cloudtrail-*",
    "log_source_count": 2,
    "query_type": "query",
    "has_query": true,
    "coverage_status": "PENDING",
    "last_checked": null,
    "original_rule_id": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
    "original_rule_name": "AWS IAM Roles Anywhere Profile Creation"
  },
  {
    "rule_id": "4182e486-fc61-11ee-a05d-f661ea17fbce",
    "rule_name": "AWS EC2 EBS Snapshot Shared or Made Public",
    "rule_description": "Detects when an Amazon Elastic Block Store (EBS) snapshot is shared with
```

Credential to connect with: Google Sheets account
Resource: Sheet Within Document
Operation: Append Row
Document: From list — Detection_Rules
Sheet: From list — الورقة1
Mapping Column Mode: Map Each Column Manually
Values to Send
rule_name Rule ID: `{{ $json.rule_id }}` — 1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce
Rule Name: `{{ $json.rule_description }}` — Detects the creation of a new AWS IAM Roles Anyw…
Description: `{{ $json.rule_description }}` — Detects the creation of a new AWS IAM Roles Anyw…
Rule Type: `{{ $json.rule_type }}` — query

OUTPUT — 68 items

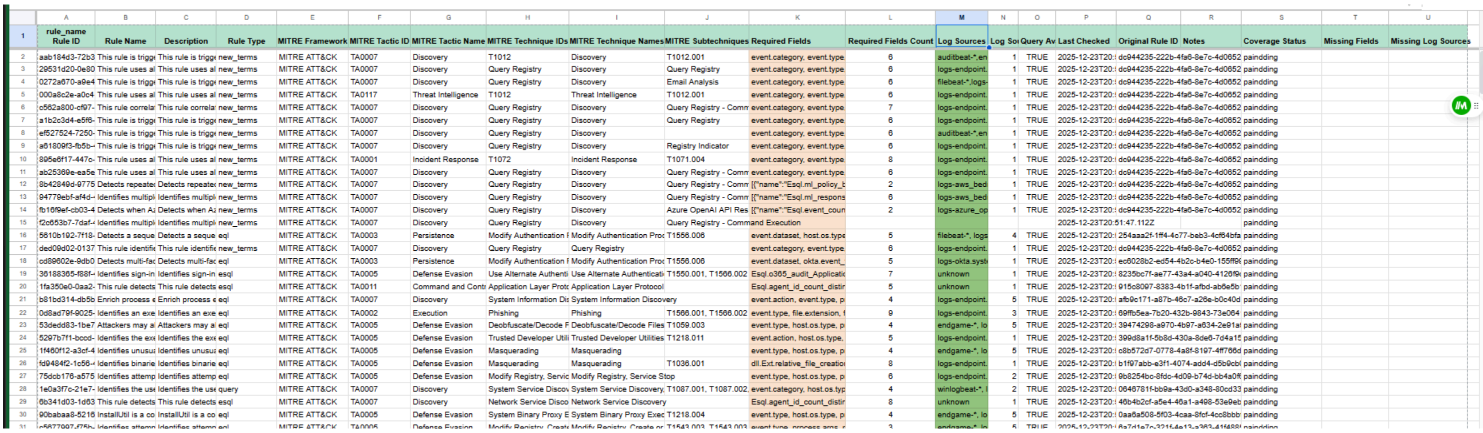
```
[
  {
    "rule_name\nRule ID": "1d4ca9c0-ff1e-11ee-91cc-f661ea17fbce",
    "Rule Name": "Detects the creation of a new AWS IAM Roles Anywhere profile. Roles Anywhere
                 allows workloads or external systems to assume IAM roles from outside AWS by
                 authenticating via trusted certificate authorities (trust anchors). Adversaries who
                 have established persistence through a rogue trust anchor may create or modify
                 profiles to link them with highly privileged roles, enabling long-term external
                 access to the AWS environment. This rule identifies successful \"CreateProfile\"
                 API calls and helps detect potentially unauthorized or risky external access
                 configurations.",
    "Description": "Detects the creation of a new AWS IAM Roles Anywhere profile. Roles Anywhere
                   allows workloads or external systems to assume IAM roles from outside AWS by
                   authenticating via trusted certificate authorities (trust anchors). Adversaries
                   who have established persistence through a rogue trust anchor may create or
                   modify profiles to link them with highly privileged roles, enabling long-term
                   external access to the AWS environment. This rule identifies successful
                   \"CreateProfile\" API calls and helps detect potentially unauthorized or risky
                   external access configurations.",
    "Rule Type": "query",
    "MITRE Framework": "MITRE ATT&CK",
    "MITRE Tactic ID": "TA0003",
    "MITRE Tactic Name": "Persistence",
    "MITRE Technique IDs": "Account Manipulation",
    "MITRE Technique Names": "Account Manipulation",
    "MITRE Subtechniques": "T1098.003",
    "Required Fields": "event.action, event.dataset, event.outcome, event.provider",
    "Required Fields Count": 4,
    "Log Sources": "filebeat-*, logs-aws.cloudtrail-*",
    "Coverage Status": "PENDING",
    "Original Rule ID": "32599594-54df-44ac-b3d0-ea1c2101bb0d",
    "Query Available": true,
    "Log Source Count": 2
  },
  {
```

Node: "Store Rules in Google Sheet" (for rules with existing MITRE mappings) ##### Node: "Store Rules in Google Sheet1" (for AI-mapped rules)

- Type: Google Sheets
- Operation: Append
- Document ID: `1VQQuZZRuMVy4yWgNLMdcDXDQuDzJLgjN-GEmYQHxrjM`
- Sheet: "الورقة1"

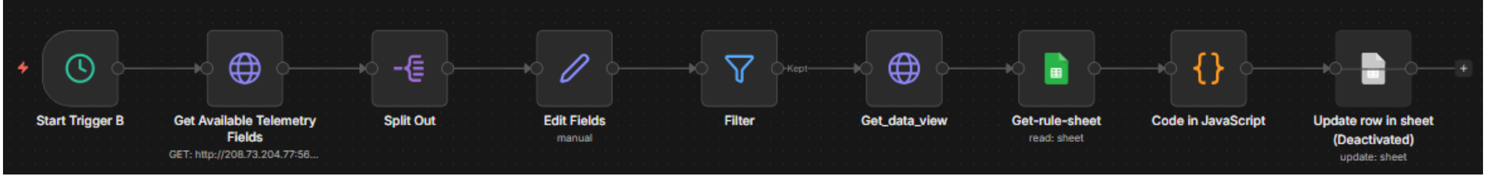
Column mappings:

```
Rule ID → rule_id
Rule Name → rule_description
Description → rule_description
Rule Type → rule_type
MITRE Framework → mitre_framework
MITRE Tactic ID → mitre_tactic_id
MITRE Tactic Name → mitre_tactic_name
MITRE Technique IDs → mitre_techniques
MITRE Technique Names → mitre_technique_names
MITRE Subtechniques → mitre_subtechniques
Required Fields → required_fields
Required Fields Count → required_fields_count
Log Sources → log_sources
Log Source Count → log_source_count
Query Available → has_query
Coverage Status → coverage_status
Last Checked → last_checked
Original Rule ID → original_rule_id
```



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	rule_name Rule ID	Rule Name	Description	Rule Type	MITRE Framework	MITRE Tactic ID	MITRE Tactic Name	MITRE Technique IDs	MITRE Technique Names	MITRE Subtechniques	Required Fields	Required Fields Count	Log Sources	Log Sou	Query Av	Last Checked	Original Rule ID	Notes	Coverage Status	Missing Fields	Missing Log Sources
2	aab184d3-72b3	This rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	T1012	Discovery	T1012.001	event.category, event.type,	6	auditbeat-*,en	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
3	29531d20-0e80	This rule uses al	This rule uses al	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Query Registry	event.category, event.type,	6	logs-endpoint.	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
4	0272a670-a9e4	This rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Email Analysis	event.category, event.type,	6	filebeat-*,logs-	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
5	000a8c2e-a0c4	This rule uses al	This rule uses al	new_terms	MITRE ATT&CK	TA0117	Threat Intelligence	T1012	Threat Intelligence	T1012.001	event.category, event.type,	6	logs-endpoint.	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
6	c562a800-cf97-	This rule correla	This rule correla	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Query Registry - Comm	event.category, event.type,	7	logs-endpoint.	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
7	a1b2c3d4-e5f6-	This rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Query Registry	event.category, event.type,	6	logs-endpoint.	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
8	ef527524-7250-	This rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery		event.category, event.type,	6	auditbeat-*,en	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
9	a61809f3-fb5b-	This rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Registry Indicator	event.category, event.type,	6	logs-endpoint.	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
10	895e6f17-447c-	This rule uses al	This rule uses al	new_terms	MITRE ATT&CK	TA0001	Incident Response	T1072	Incident Response	T1071.004	event.category, event.type,	8	logs-endpoint.	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
11	ab25369e-ea5e	This rule uses al	This rule uses al	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Query Registry - Comm	event.category, event.type,	6	logs-endpoint.	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
12	8b42849d-9775	Detects repeate	Detects repeate	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Query Registry - Comm	[{"name":"Esql.ml_policy_b	2	logs-aws_bed	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
13	94779ebf-af4d-	Identifies multipl	Identifies multipl	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Query Registry - Comm	[{"name":"Esql.ml_respons	6	logs-aws_bed	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
14	fb16f9ef-cb03-4	Detects when Az	Detects when Az	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Azure OpenAI API Res	[{"name":"Esql.event_coun	2	logs-azure_op	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
15	f2c653b7-7daf-	Identifies multipl	Identifies multipl	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Query Registry - Command Execution						2025-12-23T20:51:47.112Z			paindding		
16	5610b192-7f18-	Detects a seque	Detects a seque	eql	MITRE ATT&CK	TA0003	Persistence	Modify Authentication F	Modify Authentication Proc	T1556.006	event.dataset, host.os.type	5	filebeat-*, logs	4	TRUE	2025-12-23T20:	254aaa2f-1ff4-4c77-beb3-4cf64bfa		paindding		
17	ded09d02-0137	This rule identifie	This rule identifie	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Query Registry		event.category, event.type,	6	logs-endpoint.	1	TRUE	2025-12-23T20:	dc944235-222b-4fa6-8e7c-4d0652		paindding		
18	cd89602e-9db0	Detects multi-fac	Detects multi-fac	eql	MITRE ATT&CK	TA0003	Persistence	Modify Authentication F	Modify Authentication Proc	T1556.006	event.dataset, okta.event_	5	logs-okta.syst	1	TRUE	2025-12-23T20:	ec6028b2-ed54-4b2c-b4e0-155ff9		paindding		
19	36188365-f88f-	Identifies sign-in	Identifies sign-in	esql	MITRE ATT&CK	TA0005	Defense Evasion	Use Alternate Authenti	Use Alternate Authenticati	T1550.001, T1566.002	Esql.o365_audit_Applicatio	7	unknown	1	TRUE	2025-12-23T20:	8235bc7f-ae77-43a4-a040-4126f9		paindding		
20	1fa350e0-0aa2-	This rule detects	This rule detects	esql	MITRE ATT&CK	TA0011	Command and Contr	Application Layer Proto	Application Layer Protocol		Esql.agent_id_count_distir	5	unknown	1	TRUE	2025-12-23T20:	915c8097-8383-4b1f-afbd-ab6e5b		paindding		
21	b81bd314-db5b	Enrich process e	Enrich process e	eql	MITRE ATT&CK	TA0007	Discovery	System Information Dis	System Information Discovery		event.action, event.type, p	4	logs-endpoint.	5	TRUE	2025-12-23T20:	afb9c171-a87b-46c7-a26e-b0c40d		paindding		
22	0d8ad79f-9025-	Identifies an exe	Identifies an exe	eql	MITRE ATT&CK	TA0002	Execution	Phishing	Phishing	T1566.001, T1566.002	event.type, file.extension, f	9	logs-endpoint.	3	TRUE	2025-12-23T20:	69ffb5ea-7b20-432b-9843-73e064		paindding		
23	53dedd83-1be7	Attackers may al	Attackers may al	eql	MITRE ATT&CK	TA0005	Defense Evasion	Deobfuscate/Decode F	Deobfuscate/Decode Files	T1059.003	event.type, host.os.type, p	4	endgame-*, lo	5	TRUE	2025-12-23T20:	39474298-a970-4b97-a634-2e91a		paindding		
24	5297b7f1-bccd-	Identifies the exe	Identifies the exe	eql	MITRE ATT&CK	TA0005	Defense Evasion	Trusted Developer Utili	Trusted Developer Utilities	T1218.011	event.action, host.os.type,	5	logs-endpoint.	1	TRUE	2025-12-23T20:	399d8a1f-5b8d-430a-8de6-7d4a15		paindding		
25	1f460f12-a3cf-4	Identifies unusua	Identifies unusua	eql	MITRE ATT&CK	TA0005	Defense Evasion	Masquerading	Masquerading		event.type, host.os.type, p	4	endgame-*, lo	5	TRUE	2025-12-23T20:	c8b572d7-0778-4a8f-8197-4ff766d		paindding		
26	fd9484f2-1c56-	Identifies binarie	Identifies binarie	eql	MITRE ATT&CK	TA0005	Defense Evasion	Masquerading	Masquerading	T1036.001	dll.Ext.relative_file_creatio	8	logs-endpoint.	1	TRUE	2025-12-23T20:	b1f97abb-e3f1-4074-add4-d5b9cb		paindding		
27	75dcb176-a575	Identifies attemp	Identifies attemp	eql	MITRE ATT&CK	TA0005	Defense Evasion	Modify Registry, Servic	Modify Registry, Service Stop		event.type, host.os.type, p	6	logs-endpoint.	2	TRUE	2025-12-23T20:	9b8254bc-8fdc-4d09-b74d-bb4a0f		paindding		
28	1e0a3f7c-21e7-	Identifies the use	Identifies the use	query	MITRE ATT&CK	TA0007	Discovery	System Service Discov	System Service Discovery,	T1087.001, T1087.002,	event.category, host.os.typ	4	winlogbeat-*, l	2	TRUE	2025-12-23T20:	0646781f-bb9a-43d0-a348-80cd33		paindding		
29	6b341d03-1d63	This rule detects	This rule detects	esql	MITRE ATT&CK	TA0007	Discovery	Network Service Disco	Network Service Discovery		Esql.agent_id_count_distir	8	unknown	1	TRUE	2025-12-23T20:	46b4b2cf-a5e4-46a1-a498-53e9eb		paindding		
30	90babaa8-5216	InstallUtil is a co	InstallUtil is a co	eql	MITRE ATT&CK	TA0005	Defense Evasion	System Binary Proxy E	System Binary Proxy Exec	T1218.004	event.type, host.os.type, p	4	endgame-*, lo	5	TRUE	2025-12-23T20:	0aa6a508-5f03-4caa-8fcf-4cc8bbb		paindding		
31	c5877997-f75b-	Identifies attemp	Identifies attemp	eql	MITRE ATT&CK	TA0005	Defense Evasion	Modify Registry, Create	Modify Registry, Create or	T1543.003, T1543.003	event.type, process.args, r	3	endgame-*, lo	5	TRUE	2025-12-23T20:	6a7d1e7c-321f-4e13-a383-41f488		paindding		

Trigger B



Trigger B Implementation Report: Telemetry Inventory and Coverage

Trigger B is the second phase of the automated detection coverage system. Its primary responsibility is to build a comprehensive telemetry inventory from the SIEM and validate which detection rules can actually function based on available log sources and fields.

Workflow Architecture

The Trigger B workflow consists of 8 interconnected nodes that work sequentially to gather, process, and validate telemetry data against detection rules.

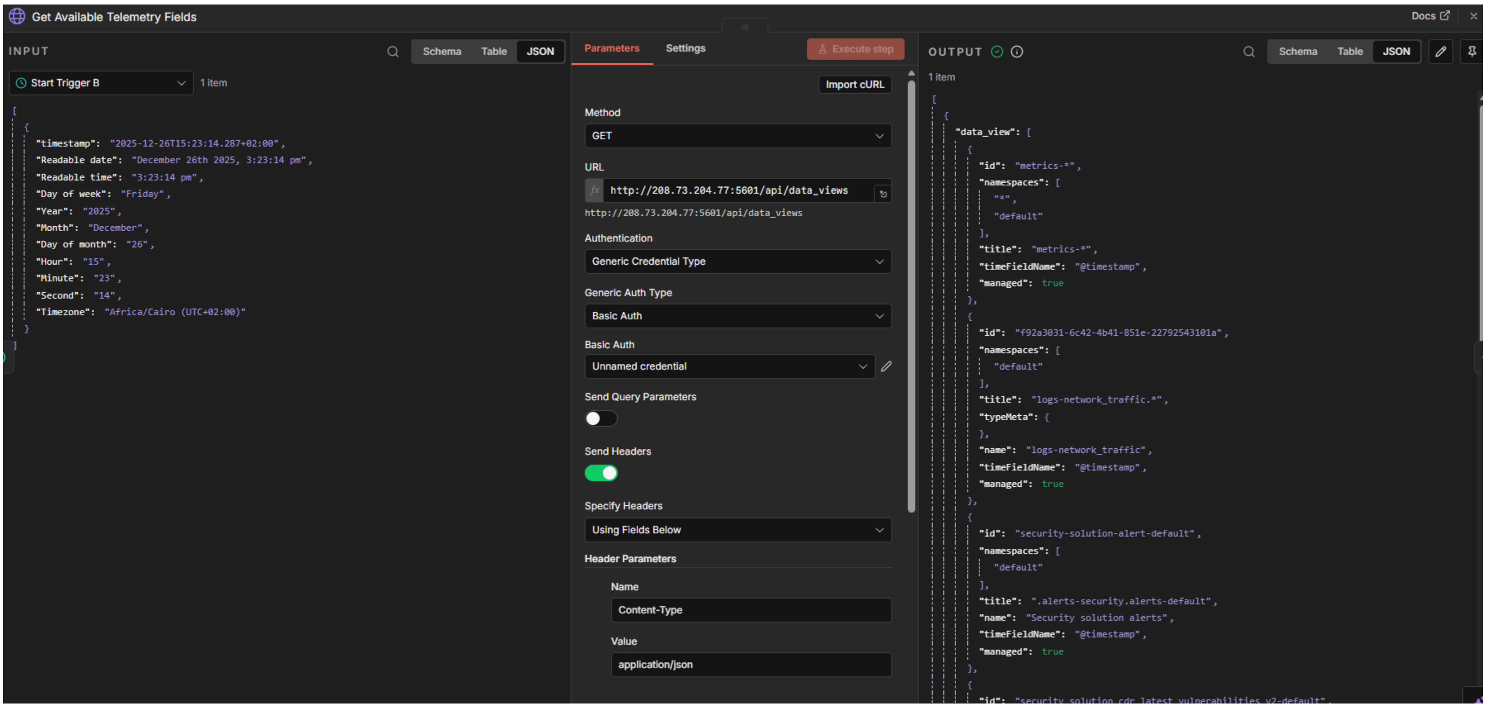
Node 1: Start Trigger B (Schedule Trigger)

This node initiates the entire Trigger B workflow on a scheduled basis. It runs at regular intervals to ensure the coverage status remains up-to-date as the SIEM environment changes.

Configuration:

- Type: Schedule Trigger
- Webhook ID: trigger-b
- Execution: Interval-based

Node 2: Get Available Telemetry Fields (HTTP Request)



```
[
  {
    "timestamp": "2025-12-26T15:23:14.287+02:00",
    "Readable date": "December 26th 2025, 3:23:14 pm",
    "Readable time": "3:23:14 pm",
    "Day of week": "Friday",
    "Year": "2025",
    "Month": "December",
    "Day of month": "26",
    "Hour": "15",
    "Minute": "23",
    "Second": "14",
    "Timezone": "Africa/Cairo (UTC+02:00)"
  }
]
```

Method: GET

URL: http://208.73.204.77:5601/api/data_views

http://208.73.204.77:5601/api/data_views

Authentication: Generic Credential Type

Generic Auth Type: Basic Auth

Basic Auth: Unnamed credential

Send Query Parameters: ○

Send Headers: ●

Specify Headers: Using Fields Below

Header Parameters

Name: Content-Type

Value: application/json

```
[
  {
    "data_view": [
      {
        "id": "metrics-*",
        "namespaces": [
          "*",
          "default"
        ],
        "title": "metrics-*",
        "timeFieldName": "@timestamp",
        "managed": true
      },
      {
        "id": "f92a3031-6c42-4b41-851e-22792543101a",
        "namespaces": [
          "default"
        ],
        "title": "logs-network_traffic.*",
        "typeMeta": {
        },
        "name": "logs-network_traffic",
        "timeFieldName": "@timestamp",
        "managed": true
      },
      {
        "id": "security-solution-alert-default",
        "namespaces": [
          "default"
        ],
        "title": ".alerts-security.alerts-default",
        "name": "Security solution alerts",
        "timeFieldName": "@timestamp",
        "managed": true
      },
      {
        "id": "security_solution_cdr_latest_vulnerabilities_v2-default",
```

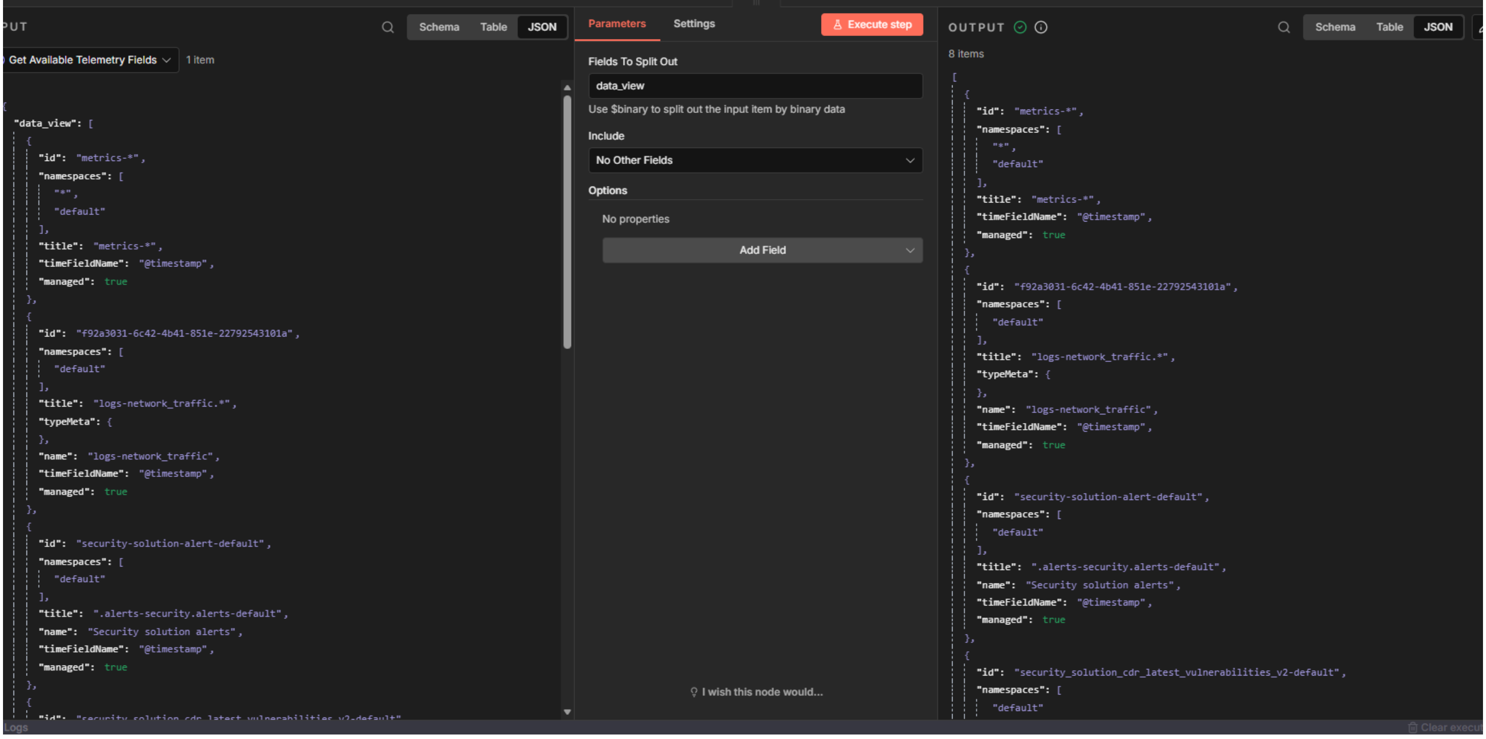
This node connects to the Kibana API to retrieve all available data views (index patterns) from the SIEM.

Configuration:

- URL: `http://208.73.204.77:5601/api/data_views`
- Authentication: HTTP Basic Auth
- Headers: Content-Type application/json
- Method: GET

Purpose: Fetches the complete list of data views that represent the log sources configured in the SIEM.

Node 3: Split Out



```
{
  "data_view": [
    {
      "id": "metrics-*",
      "namespaces": [
        "*",
        "default"
      ],
      "title": "metrics-*",
      "timeFieldName": "@timestamp",
      "managed": true
    },
    {
      "id": "f92a3031-6c42-4b41-851e-22792543101a",
      "namespaces": [
        "default"
      ],
      "title": "logs-network_traffic.*",
      "typeMeta": {
      },
      "name": "logs-network_traffic",
      "timeFieldName": "@timestamp",
      "managed": true
    },
    {
      "id": "security-solution-alert-default",
      "namespaces": [
        "default"
      ],
      "title": ".alerts-security.alerts-default",
      "name": "Security solution alerts",
      "timeFieldName": "@timestamp",
      "managed": true
    },
    {
      "id": "security_solution_cdr_latest_vulnerabilities_v2-default"
```

Fields To Split Out: data_view

Use $binary to split out the input item by binary data

Include: No Other Fields

Options

No properties

Add Field

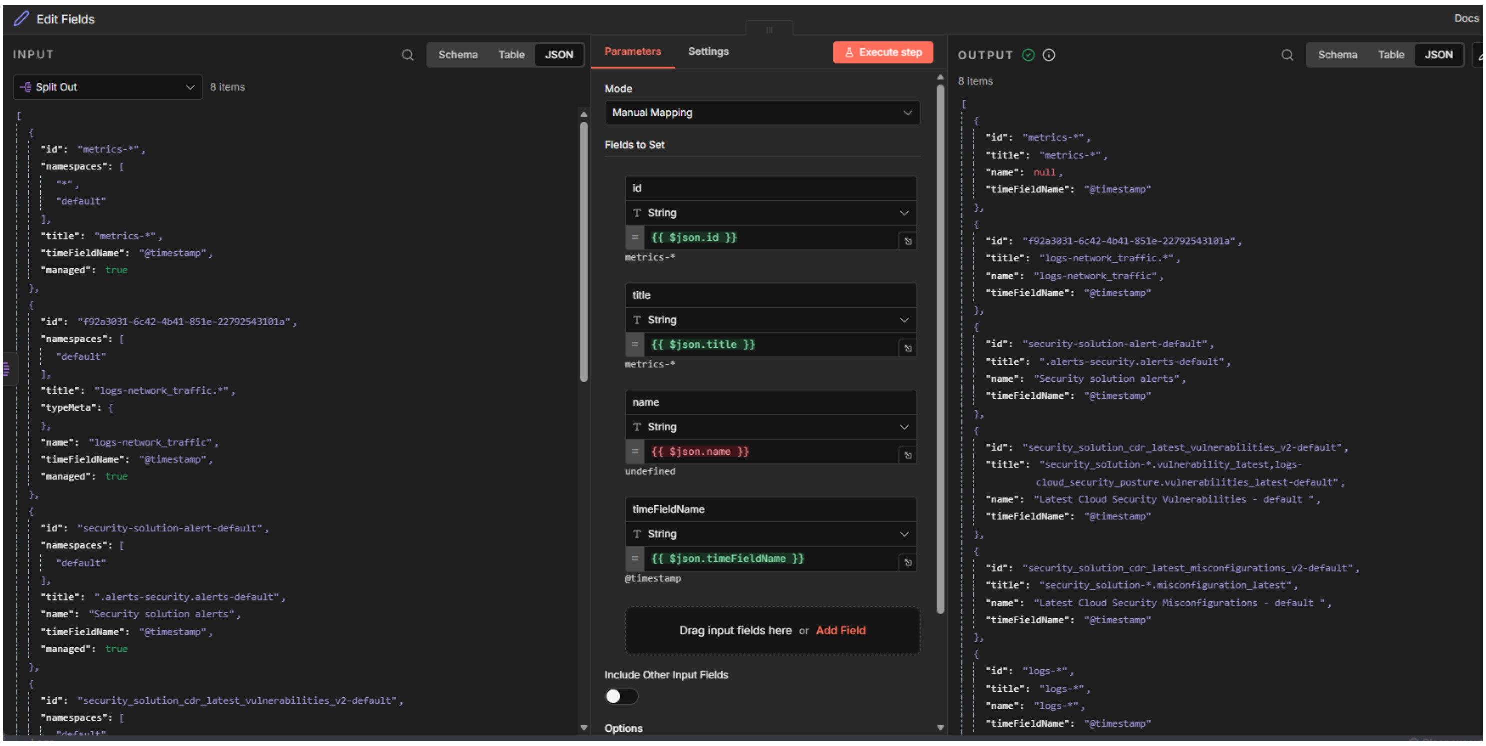
```
[
  {
    "id": "metrics-*",
    "namespaces": [
      "*",
      "default"
    ],
    "title": "metrics-*",
    "timeFieldName": "@timestamp",
    "managed": true
  },
  {
    "id": "f92a3031-6c42-4b41-851e-22792543101a",
    "namespaces": [
      "default"
    ],
    "title": "logs-network_traffic.*",
    "typeMeta": {
    },
    "name": "logs-network_traffic",
    "timeFieldName": "@timestamp",
    "managed": true
  },
  {
    "id": "security-solution-alert-default",
    "namespaces": [
      "default"
    ],
    "title": ".alerts-security.alerts-default",
    "name": "Security solution alerts",
    "timeFieldName": "@timestamp",
    "managed": true
  },
  {
    "id": "security_solution_cdr_latest_vulnerabilities_v2-default",
    "namespaces": [
      "default"
```

This node takes the array of data views returned from Kibana and splits them into individual items for processing.

Configuration:

- Field to split: data_view
- Purpose: Enables processing each data view separately in subsequent nodes

Node 4: Edit Fields



```
[
  {
    "id": "metrics-*",
    "namespaces": [
      "*",
      "default"
    ],
    "title": "metrics-*",
    "timeFieldName": "@timestamp",
    "managed": true
  },
  {
    "id": "f92a3031-6c42-4b41-851e-22792543101a",
    "namespaces": [
      "default"
    ],
    "title": "logs-network_traffic.*",
    "typeMeta": {
    },
    "name": "logs-network_traffic",
    "timeFieldName": "@timestamp",
    "managed": true
  },
  {
    "id": "security-solution-alert-default",
    "namespaces": [
      "default"
    ],
    "title": ".alerts-security.alerts-default",
    "name": "Security solution alerts",
    "timeFieldName": "@timestamp",
    "managed": true
  },
  {
    "id": "security_solution_cdr_latest_vulnerabilities_v2-default",
    "namespaces": [
      "default"
```

Mode: Manual Mapping

Fields to Set

id
String
{{ $json.id }}
metrics-*

title
String
{{ $json.title }}
metrics-*

name
String
{{ $json.name }}
undefined

timeFieldName
String
{{ $json.timeFieldName }}
@timestamp

Drag input fields here or Add Field

Include Other Input Fields ○

Options

```
[
  {
    "id": "metrics-*",
    "title": "metrics-*",
    "name": null,
    "timeFieldName": "@timestamp"
  },
  {
    "id": "f92a3031-6c42-4b41-851e-22792543101a",
    "title": "logs-network_traffic.*",
    "name": "logs-network_traffic",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security-solution-alert-default",
    "title": ".alerts-security.alerts-default",
    "name": "Security solution alerts",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security_solution_cdr_latest_vulnerabilities_v2-default",
    "title": "security_solution-*.vulnerability_latest,logs-
          cloud_security_posture.vulnerabilities_latest-default",
    "name": "Latest Cloud Security Vulnerabilities - default ",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security_solution_cdr_latest_misconfigurations_v2-default",
    "title": "security_solution-*.misconfiguration_latest",
    "name": "Latest Cloud Security Misconfigurations - default ",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "logs-*",
    "title": "logs-*",
    "name": "logs-*",
    "timeFieldName": "@timestamp"
```

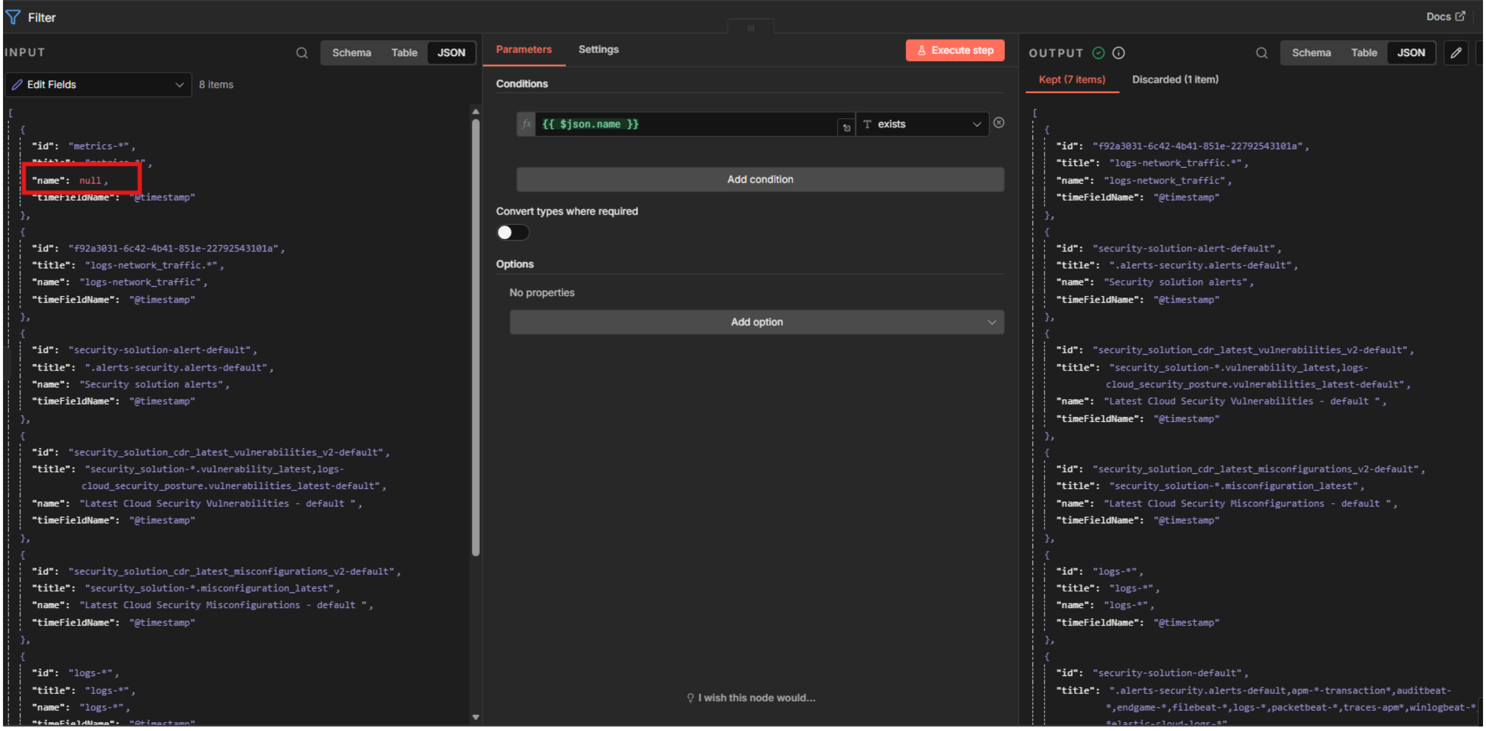
This node extracts and standardizes the key attributes from each data view.

Extracted Fields:

- id: Data view identifier
- title: Index pattern or data source name
- name: Human-readable name
- timeFieldName: Timestamp field used for time-based queries

Purpose: Normalizes the data structure for consistent processing downstream.

Node 5: Filter


Filter

INPUT — Edit Fields — 8 items

```
[
  {
    "id": "metrics-*",
    "title": "metrics-*",
    "name": null,
    "timeFieldName": "@timestamp"
  },
  {
    "id": "f92a3031-6c42-4b41-851e-22792543101a",
    "title": "logs-network_traffic.*",
    "name": "logs-network_traffic",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security-solution-alert-default",
    "title": ".alerts-security.alerts-default",
    "name": "Security solution alerts",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security_solution_cdr_latest_vulnerabilities_v2-default",
    "title": "security_solution-*.vulnerability_latest,logs-
          cloud_security_posture.vulnerabilities_latest-default",
    "name": "Latest Cloud Security Vulnerabilities - default ",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security_solution_cdr_latest_misconfigurations_v2-default",
    "title": "security_solution-*.misconfiguration_latest",
    "name": "Latest Cloud Security Misconfigurations - default ",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "logs-*",
    "title": "logs-*",
    "name": "logs-*",
    "timeFieldName": "@timestamp"
```

Parameters | Settings | Execute step

Conditions

`{{ $json.name }}` exists

Add condition

Convert types where required: off

Options

No properties

Add option

I wish this node would...

OUTPUT — Kept (7 items) | Discarded (1 item)

```
[
  {
    "id": "f92a3031-6c42-4b41-851e-22792543101a",
    "title": "logs-network_traffic.*",
    "name": "logs-network_traffic",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security-solution-alert-default",
    "title": ".alerts-security.alerts-default",
    "name": "Security solution alerts",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security_solution_cdr_latest_vulnerabilities_v2-default",
    "title": "security_solution-*.vulnerability_latest,logs-
          cloud_security_posture.vulnerabilities_latest-default",
    "name": "Latest Cloud Security Vulnerabilities - default ",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security_solution_cdr_latest_misconfigurations_v2-default",
    "title": "security_solution-*.misconfiguration_latest",
    "name": "Latest Cloud Security Misconfigurations - default ",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "logs-*",
    "title": "logs-*",
    "name": "logs-*",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security-solution-default",
    "title": ".alerts-security.alerts-default,apm-*-transaction*,auditbeat-
          *,endgame-*,filebeat-*,logs-*,packetbeat-*,traces-apm*,winlogbeat-*
          *elastic-cloud-logs-*"
```

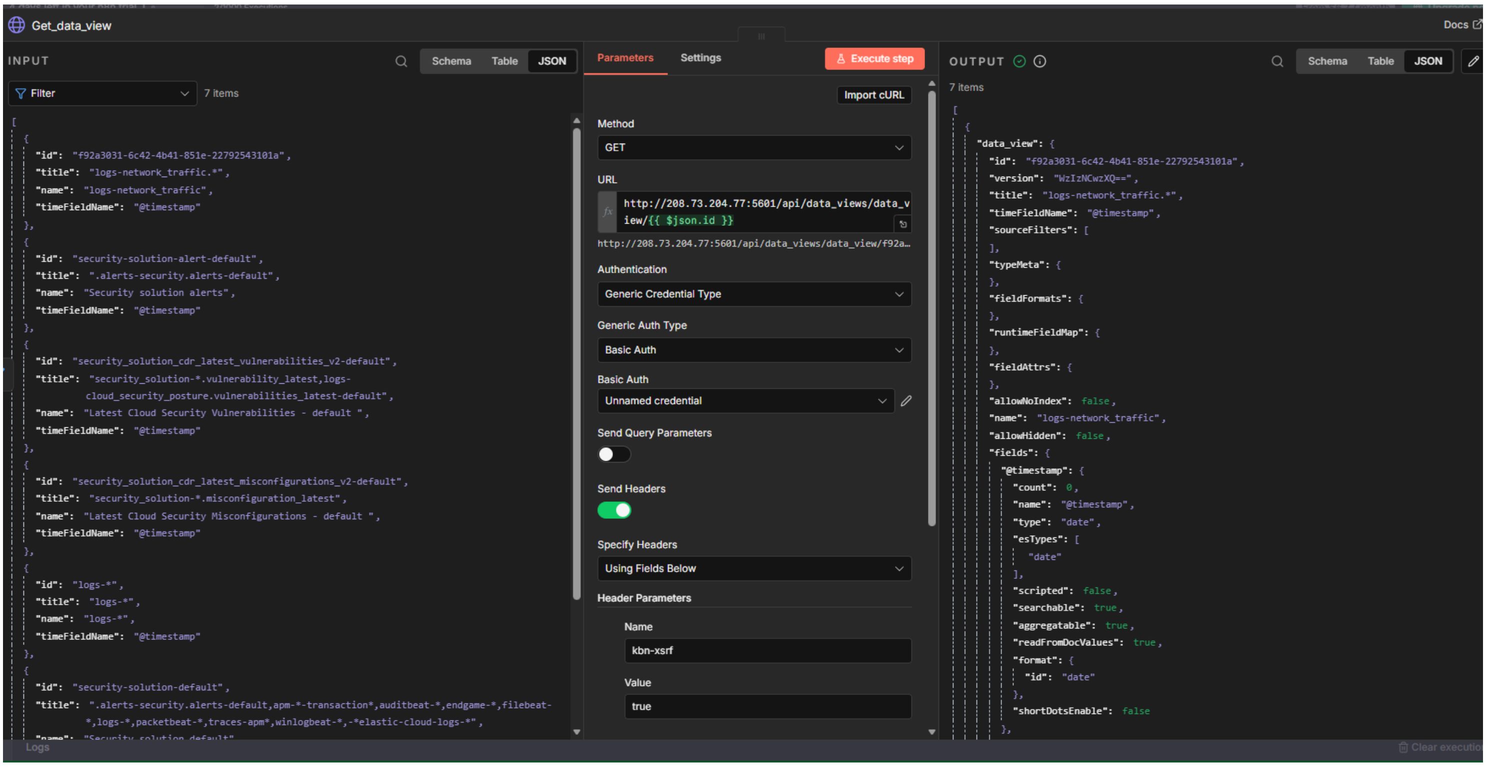
This node applies a validation check to ensure only valid data views proceed through the workflow.

Filter Condition:

- Checks if the "name" field exists
- Case sensitive validation
- Strict type checking enabled

Purpose: Removes any malformed or incomplete data view entries.

Node 6: Get_data_view (HTTP Request)


Get_data_view

INPUT — Filter — 7 items

```
[
  {
    "id": "f92a3031-6c42-4b41-851e-22792543101a",
    "title": "logs-network_traffic.*",
    "name": "logs-network_traffic",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security-solution-alert-default",
    "title": ".alerts-security.alerts-default",
    "name": "Security solution alerts",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security_solution_cdr_latest_vulnerabilities_v2-default",
    "title": "security_solution-*.vulnerability_latest,logs-
          cloud_security_posture.vulnerabilities_latest-default",
    "name": "Latest Cloud Security Vulnerabilities - default ",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security_solution_cdr_latest_misconfigurations_v2-default",
    "title": "security_solution-*.misconfiguration_latest",
    "name": "Latest Cloud Security Misconfigurations - default ",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "logs-*",
    "title": "logs-*",
    "name": "logs-*",
    "timeFieldName": "@timestamp"
  },
  {
    "id": "security-solution-default",
    "title": ".alerts-security.alerts-default,apm-*-transaction*,auditbeat-*,endgame-*,filebeat-
          *,logs-*,packetbeat-*,traces-apm*,winlogbeat-*,-*elastic-cloud-logs-*",
    "name": "Security solution default"
```

Parameters | Settings | Execute step

Import cURL

Method: GET

URL: `http://208.73.204.77:5601/api/data_views/data_view/{{ $json.id }}`

`http://208.73.204.77:5601/api/data_views/data_view/f92a...`

Authentication: Generic Credential Type

Generic Auth Type: Basic Auth

Basic Auth: Unnamed credential

Send Query Parameters: off

Send Headers: on

Specify Headers: Using Fields Below

Header Parameters

Name: kbn-xsrf

Value: true

OUTPUT — 7 items

```
[
  {
    "data_view": {
      "id": "f92a3031-6c42-4b41-851e-22792543101a",
      "version": "WzIzNCwzXQ==",
      "title": "logs-network_traffic.*",
      "timeFieldName": "@timestamp",
      "sourceFilters": [
      ],
      "typeMeta": {
      },
      "fieldFormats": {
      },
      "runtimeFieldMap": {
      },
      "fieldAttrs": {
      },
      "allowNoIndex": false,
      "name": "logs-network_traffic",
      "allowHidden": false,
      "fields": {
        "@timestamp": {
          "count": 0,
          "name": "@timestamp",
          "type": "date",
          "esTypes": [
            "date"
          ],
          "scripted": false,
          "searchable": true,
          "aggregatable": true,
          "readFromDocValues": true,
          "format": {
            "id": "date"
          },
          "shortDotsEnable": false
        },
```

Logs

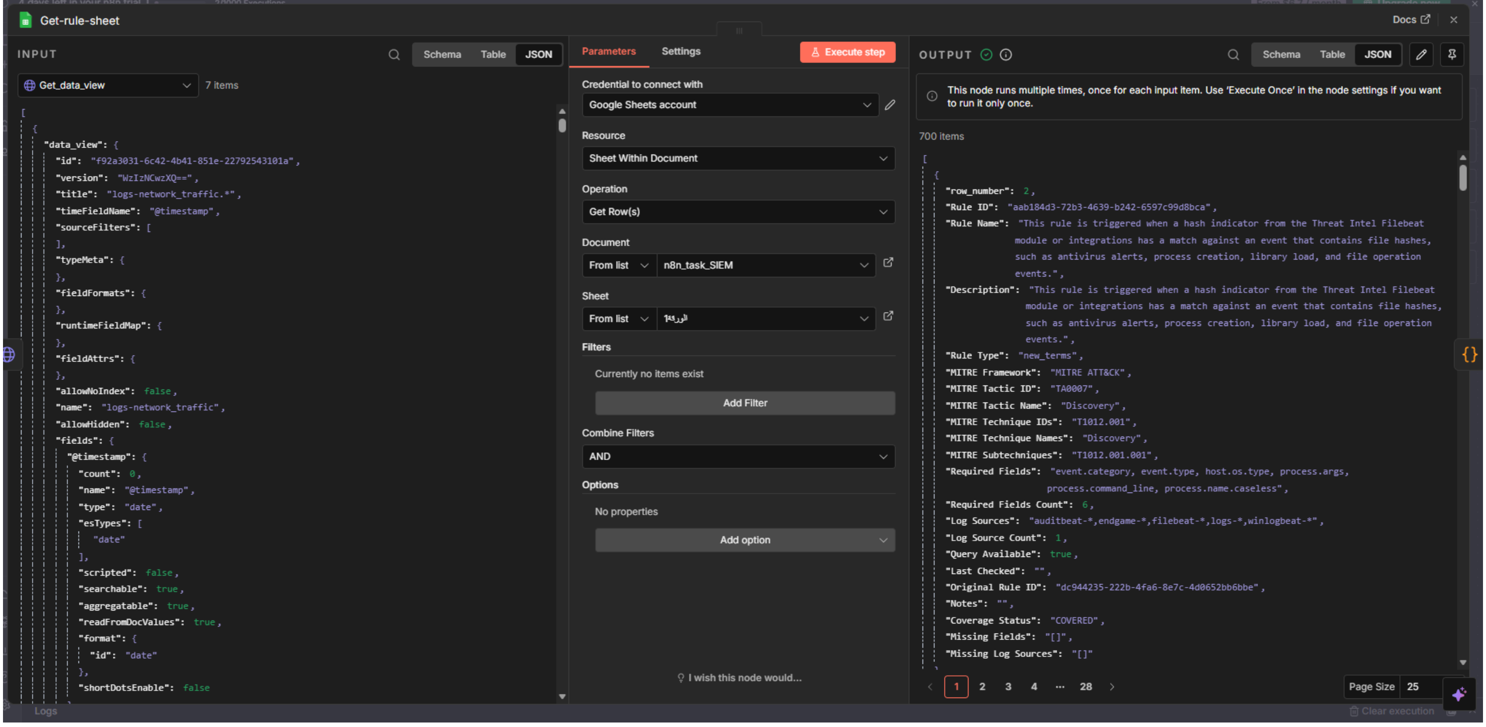
This node performs a detailed retrieval of each individual data view to access its complete field mapping.

Configuration:

- URL: `http://208.73.204.77:5601/api/data_views/data_view/{{ $json.id }}`
- Authentication: HTTP Basic Auth
- Headers: kbn-xsrf: true
- Dynamic URL construction using data view ID

Purpose: Fetches the complete field schema for each data source, including all available fields and their properties.

Node 7: Get-rule-sheet (Google Sheets)



Get-rule-sheet

INPUT

Get_data_view 7 items

```
[
  {
    "data_view": {
      "id": "f92a3031-6c42-4b41-851e-22792543101a",
      "version": "WzIzNCwzXQ==",
      "title": "logs-network_traffic.*",
      "timeFieldName": "@timestamp",
      "sourceFilters": [
      ],
      "typeMeta": {
      },
      "fieldFormats": {
      },
      "runtimeFieldMap": {
      },
      "fieldAttrs": {
      },
      "allowNoIndex": false,
      "name": "logs-network_traffic",
      "allowHidden": false,
      "fields": {
        "@timestamp": {
          "count": 0,
          "name": "@timestamp",
          "type": "date",
          "esTypes": [
            "date"
          ],
          "scripted": false,
          "searchable": true,
          "aggregatable": true,
          "readFromDocValues": true,
          "format": {
            "id": "date"
          },
          "shortDotsEnable": false
```

Parameters Settings Execute step

Credential to connect with: Google Sheets account

Resource: Sheet Within Document

Operation: Get Row(s)

Document: From list — n8n_task_SIEM

Sheet: From list — الورقة1

Filters: Currently no items exist

Add Filter

Combine Filters: AND

Options: No properties

Add option

I wish this node would...

OUTPUT

This node runs multiple times, once for each input item. Use 'Execute Once' in the node settings if you want to run it only once.

700 items

```
[
  {
    "row_number": 2,
    "Rule ID": "aab184d3-72b3-4639-b242-6597c99d8bca",
    "Rule Name": "This rule is triggered when a hash indicator from the Threat Intel Filebeat
                 module or integrations has a match against an event that contains file hashes,
                 such as antivirus alerts, process creation, library load, and file operation
                 events.",
    "Description": "This rule is triggered when a hash indicator from the Threat Intel Filebeat
                   module or integrations has a match against an event that contains file hashes,
                   such as antivirus alerts, process creation, library load, and file operation
                   events.",
    "Rule Type": "new_terms",
    "MITRE Framework": "MITRE ATT&CK",
    "MITRE Tactic ID": "TA0007",
    "MITRE Tactic Name": "Discovery",
    "MITRE Technique IDs": "T1012.001",
    "MITRE Technique Names": "Discovery",
    "MITRE Subtechniques": "T1012.001.001",
    "Required Fields": "event.category, event.type, host.os.type, process.args,
                       process.command_line, process.name.caseless",
    "Required Fields Count": 6,
    "Log Sources": "auditbeat-*,endgame-*,filebeat-*,logs-*,winlogbeat-*",
    "Log Source Count": 1,
    "Query Available": true,
    "Last Checked": "",
    "Original Rule ID": "dc944235-222b-4fa6-8e7c-4d0652bb6bbe",
    "Notes": "",
    "Coverage Status": "COVERED",
    "Missing Fields": "[]",
    "Missing Log Sources": "[]"
```

‹ 1 2 3 4 ··· 28 › Page Size 25

This node retrieves the detection rules from Google Sheets that were populated by Trigger A.

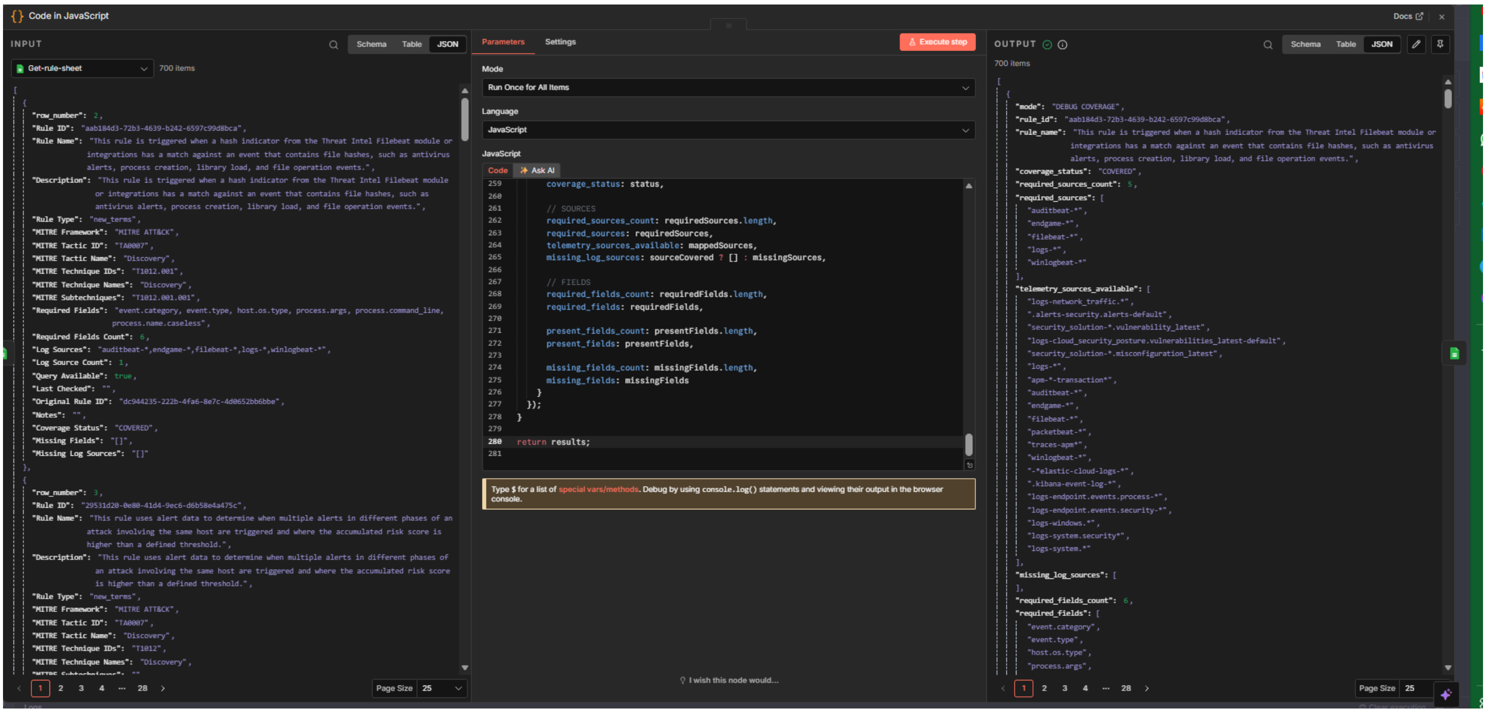
Configuration:

- Document ID: 1VQQuZZRuMVy4yWgNLMdcDXDQuDzJLgjN-GEmYQHxrjM
- Sheet Name: الورقة1 (Sheet 1)
- Operation: Read all rows

Retrieved Data:

- Rule ID
- Rule Name
- Required Fields
- Log Sources
- MITRE ATT&CK mappings
- All other rule metadata

Node 8: Code in JavaScript (Coverage Analysis Engine)



Code in JavaScript

INPUT

Get-rule-sheet 700 items

```
[
  {
    "row_number": 2,
    "Rule ID": "aab184d3-72b3-4639-b242-6597c99d8bca",
    "Rule Name": "This rule is triggered when a hash indicator from the Threat Intel Filebeat module or
                 integrations has a match against an event that contains file hashes, such as antivirus
                 alerts, process creation, library load, and file operation events.",
    "Description": "This rule is triggered when a hash indicator from the Threat Intel Filebeat module
                   or integrations has a match against an event that contains file hashes, such as
                   antivirus alerts, process creation, library load, and file operation events.",
    "Rule Type": "new_terms",
    "MITRE Framework": "MITRE ATT&CK",
    "MITRE Tactic ID": "TA0007",
    "MITRE Tactic Name": "Discovery",
    "MITRE Technique IDs": "T1012.001",
    "MITRE Technique Names": "Discovery",
    "MITRE Subtechniques": "T1012.001.001",
    "Required Fields": "event.category, event.type, host.os.type, process.args, process.command_line,
                       process.name.caseless",
    "Required Fields Count": 6,
    "Log Sources": "auditbeat-*,endgame-*,filebeat-*,logs-*,winlogbeat-*",
    "Log Source Count": 1,
    "Query Available": true,
    "Last Checked": "",
    "Original Rule ID": "dc944235-222b-4fa6-8e7c-4d0652bb6bbe",
    "Notes": "",
    "Coverage Status": "COVERED",
    "Missing Fields": "[]",
    "Missing Log Sources": "[]"
  },
  {
    "row_number": 3,
    "Rule ID": "29531d20-0e80-41d4-9ec6-d6b58e4a475c",
    "Rule Name": "This rule uses alert data to determine when multiple alerts in different phases of an
                 attack involving the same host are triggered and where the accumulated risk score is
                 higher than a defined threshold.",
    "Description": "This rule uses alert data to determine when multiple alerts in different phases of
                   an attack involving the same host are triggered and where the accumulated risk score
                   is higher than a defined threshold.",
    "Rule Type": "new_terms",
    "MITRE Framework": "MITRE ATT&CK",
    "MITRE Tactic ID": "TA0007",
    "MITRE Tactic Name": "Discovery",
    "MITRE Technique IDs": "T1012",
    "MITRE Technique Names": "Discovery",
    "MITRE Subtechniques": ""
```

‹ 1 2 3 4 ··· 28 › Page Size 25

Parameters Settings Execute step

Mode: Run Once for All Items

Language: JavaScript

JavaScript

Code Ask AI

```
      coverage_status: status,

      // SOURCES
      required_sources_count: requiredSources.length,
      required_sources: requiredSources,
      telemetry_sources_available: mappedSources,
      missing_log_sources: sourceCovered ? [] : missingSources,

      // FIELDS
      required_fields_count: requiredFields.length,
      required_fields: requiredFields,

      present_fields_count: presentFields.length,
      present_fields: presentFields,

      missing_fields_count: missingFields.length,
      missing_fields: missingFields
    }
  });
}

return results;

```

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

I wish this node would...

OUTPUT

700 items

```
[
  {
    "mode": "DEBUG COVERAGE",
    "rule_id": "aab184d3-72b3-4639-b242-6597c99d8bca",
    "rule_name": "This rule is triggered when a hash indicator from the Threat Intel Filebeat module or
                 integrations has a match against an event that contains file hashes, such as antivirus
                 alerts, process creation, library load, and file operation events.",
    "coverage_status": "COVERED",
    "required_sources_count": 5,
    "required_sources": [
      "auditbeat-*",
      "endgame-*",
      "filebeat-*",
      "logs-*",
      "winlogbeat-*"
    ],
    "telemetry_sources_available": [
      "logs-network_traffic.*",
      ".alerts-security.alerts-default",
      "security_solution-*.vulnerability_latest",
      "logs-cloud_security_posture.vulnerabilities_latest-default",
      "security_solution-*.misconfiguration_latest",
      "logs-*",
      "apm-*-transaction*",
      "auditbeat-*",
      "endgame-*",
      "filebeat-*",
      "packetbeat-*",
      "traces-apm*",
      "winlogbeat-*",
      "-*elastic-cloud-logs-*",
      ".kibana-event-log-*",
      "logs-endpoint.events.process-*",
      "logs-endpoint.events.security-*",
      "logs-windows.*",
      "logs-system.security*",
      "logs-system.*"
    ],
    "missing_log_sources": [
    ],
    "required_fields_count": 6,
    "required_fields": [
      "event.category",
      "event.type",
      "host.os.type",
      "process.args",
```

‹ 1 2 3 4 ··· 28 › Page Size 25

This is the core processing node that performs the intelligent matching between available telemetry and rule requirements.

Key Functions:

1. Build Telemetry Source Map

```
- Collects all available log sources from data views
- Extracts source titles and index patterns
- Builds a normalized set of available sources
```

2. Build Field Inventory

```
- Flattens nested field structures from Kibana
- Creates comprehensive field catalog
- Adds ECS field variations (lowercase, .keyword, .text)
- Handles complex object field paths
```

3. Mapping Layer

```
- Maps generic source patterns to specific implementations
- Handles common source naming conventions:
  * logs-* → logs-endpoint.events.process-*
  * winlogbeat-* → logs-windows.*
  * endgame-* → logs-endpoint.events.security-*
  * auditbeat-* → logs-system.*
  * filebeat-* → logs-*
```

4. Source Matcher Function

```
- Implements wildcard matching for source patterns
- Handles prefix-based matching (e.g., logs-*)
- Performs exact matching for specific sources
```

5. ECS-Aware Field Matcher Function

```
- Performs case-insensitive field matching
- Handles ECS field variations (.keyword, .text)
- Implements field equivalence mapping:
  * process.name.caseless ↔ process.name
  * event.type ↔ event.action
  * event.category ↔ event.kind
  * host.os.type ↔ host.os.name
- Handles flattened field name mismatches
```

6. Rule Coverage Evaluation Logic For each detection rule, the code:

a) Parses Rule Requirements:

- Splits comma-separated log sources
- Splits comma-separated required fields
- Trims and filters empty values

b) Evaluates Source Coverage:

- Checks if any required source exists in telemetry
- Tracks missing sources
- Sets sourceCovered flag

c) Evaluates Field Coverage:

- Checks each required field against field inventory
- Uses ECS-aware matching
- Categorizes fields as present or missing

d) Determines Coverage Status:

- COVERED: All sources and fields available
- PARTIALLY COVERED: Source available but some fields missing
- NOT COVERED: Required source not available

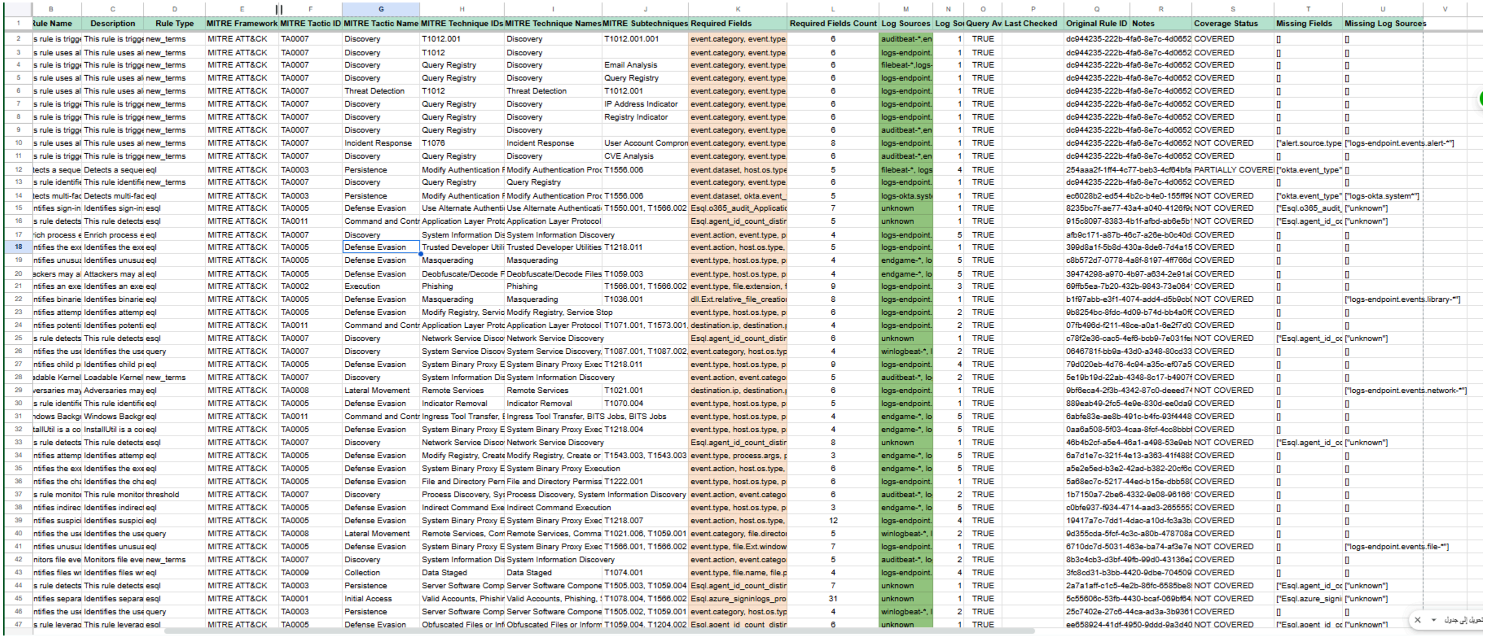
e) Generates Detailed Output:

```
{
  mode: "DEBUG COVERAGE",
  rule_id: string,
  rule_name: string,
  coverage_status: "COVERED" | "PARTIALLY COVERED" | "NOT COVERED",

  // Source Information
  required_sources_count: number,
  required_sources: array,
  telemetry_sources_available: array,
  missing_log_sources: array,

  // Field Information
  required_fields_count: number,
  required_fields: array,
  present_fields_count: number,
  present_fields: array,
  missing_fields_count: number,
  missing_fields: array
}
```

```
{
    "mode": "DEBUG COVERAGE",
    "rule_id": "aab184d3-72b3-4639-b242-6597c99d8bca",
    "rule_name": "This rule is triggered when a hash indicator from the Threat Intel Filebeat module or integrations has a match against an event that contains file hashes, such as antivirus alerts, process creation, library load, and file operation events.",
    "coverage_status": "COVERED",
    "required_sources_count": 5,
    "required_sources": [
      "auditbeat-*",
      "endgame-*",
      "filebeat-*",
      "logs-*",
      "winlogbeat-*"
    ],
    "telemetry_sources_available": [
      "logs-network_traffic.*",
      ".alerts-security.alerts-default",
      "security_solution-*.vulnerability_latest",
      "logs-cloud_security_posture.vulnerabilities_latest-default",
      "security_solution-*.misconfiguration_latest",
      "logs-*",
      "apm-*-transaction*",
      "auditbeat-*",
      "endgame-*",
      "filebeat-*",
      "packetbeat-*",
      "traces-apm*",
      "winlogbeat-*",
      "-*elastic-cloud-logs-*",
      ".kibana-event-log-*",
      "logs-endpoint.events.process-*",
      "logs-endpoint.events.security-*",
      "logs-windows.*",
      "logs-system.security*",
      "logs-system.*"
    ],
    "missing_log_sources": [],
    "required_fields_count": 6,
    "required_fields": [
      "event.category",
      "event.type",
      "host.os.type",
      "process.args",
      "process.command_line",
      "process.name.caseless"
    ],
    "present_fields_count": 6,
    "present_fields": [
      "event.category",
      "event.type",
      "host.os.type",
      "process.args",
      "process.command_line",
      "process.name.caseless"
    ],
    "missing_fields_count": 0,
    "missing_fields": []
  },
  {
    "mode": "DEBUG COVERAGE",
    "rule_id": "29531d20-0e80-41d4-9ec6-d6b58e4a475c",
    "rule_name": "This rule uses alert data to determine when multiple alerts in different phases of an attack involving the same host are triggered and where the accumulated risk score is higher than a defined threshold.",
    "coverage_status": "COVERED",
    "required_sources_count": 1,
    "required_sources": [
      "logs-endpoint.events.process-*"
    ],
    "telemetry_sources_available": [
      "logs-network_traffic.*",
      ".alerts-security.alerts-default",
      "security_solution-*.vulnerability_latest",
      "logs-cloud_security_posture.vulnerabilities_latest-default",
      "security_solution-*.misconfiguration_latest",
      "logs-*",
      "apm-*-transaction*",
      "auditbeat-*",
      "endgame-*",
      "filebeat-*",
      "packetbeat-*",
      "traces-apm*",
      "winlogbeat-*",
      "-*elastic-cloud-logs-*",
      ".kibana-event-log-*",
      "logs-endpoint.events.process-*",
      "logs-endpoint.events.security-*",
      "logs-windows.*",
      "logs-system.security*",
      "logs-system.*"
    ],
    "missing_log_sources": [],
    "required_fields_count": 6,
    "required_fields": [
        "event.category",
        "event.type",
        "host.os.type",
        "process.args",
        "process.command_line",
        "process.name.caseless"
      ],
      "present_fields_count": 6,
      "present_fields": [
        "event.category",
        "event.type",
        "host.os.type",
        "process.args",
        "process.command_line",
        "process.name.caseless"
      ],
      "missing_fields_count": 0,
      "missing_fields": []
    }
```

Node 9: Update row in sheet (Google Sheets)

This final node writes the coverage analysis results back to Google Sheets.



1	Rule Name	Description	Rule Type	MITRE Framework	MITRE Tactic ID	MITRE Tactic Name	MITRE Technique IDs	MITRE Technique Names	MITRE Subtechniques	Required Fields	Required Fields Count	Log Sources	Log Sou	Query Av	Last Checked	Original Rule ID	Notes	Coverage Status	Missing Fields	Missing Log Sources
2	s rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	T1012.001	Discovery	T1012.001.001	event.category, event.type	6	auditbeat-*,en	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
3	s rule uses al	This rule uses al	new_terms	MITRE ATT&CK	TA0007	Discovery	T1012	Discovery		event.category, event.type	6	logs-endpoint.	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
4	s rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Email Analysis	event.category, event.type	6	filebeat-*,logs-	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
5	s rule uses al	This rule uses al	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Query Registry	event.category, event.type	6	logs-endpoint.	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
6	s rule uses al	This rule uses al	new_terms	MITRE ATT&CK	TA0007	Threat Detection	T1012	Threat Detection	T1012.001	event.category, event.type	6	logs-endpoint.	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
7	s rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	IP Address Indicator	event.category, event.type	6	logs-endpoint.	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
8	s rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	Registry Indicator	event.category, event.type	6	logs-endpoint.	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
9	s rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery		event.category, event.type	6	auditbeat-*,en	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
10	s rule uses al	This rule uses al	new_terms	MITRE ATT&CK	TA0007	Incident Response	T1076	Incident Response	User Account Compron	event.category, event.type	8	logs-endpoint.	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		NOT COVERED	["alert.source.type	["logs-endpoint.events.alert-*"]
11	s rule is trigge	This rule is trigge	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Discovery	CVE Analysis	event.category, event.type	6	auditbeat-*,en	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
12	tects a seque	Detects a seque	eql	MITRE ATT&CK	TA0003	Persistence	Modify Authentication F	Modify Authentication Proc	T1556.006	event.dataset, host.os.type	5	filebeat-*, logs	4	TRUE		254aaa2f-1ff4-4c77-beb3-4cf64bfa		PARTIALLY COVERE	["okta.event_type"	[]
13	s rule identifie	This rule identifie	new_terms	MITRE ATT&CK	TA0007	Discovery	Query Registry	Query Registry		event.category, event.type	6	logs-endpoint.	1	TRUE		dc944235-222b-4fa6-8e7c-4d0652		COVERED	[]	[]
14	tects multi-fac	Detects multi-fac	eql	MITRE ATT&CK	TA0003	Persistence	Modify Authentication F	Modify Authentication Proc	T1556.006	event.dataset, okta.event_	5	logs-okta.syst	1	TRUE		ec6028b2-ed54-4b2c-b4e0-155ff9		NOT COVERED	["okta.event_type"	["logs-okta.system*"]
15	ntifies sign-in	Identifies sign-in	esql	MITRE ATT&CK	TA0005	Defense Evasion	Use Alternate Authenti	Use Alternate Authenticati	T1550.001, T1566.002	Esql.o365_audit_Applicatio	7	unknown	1	TRUE		8235bc7f-ae77-43a4-a040-4126f9		NOT COVERED	["Esql.o365_audit_	["unknown"]
16	s rule detects	This rule detects	esql	MITRE ATT&CK	TA0011	Command and Contr	Application Layer Protc	Application Layer Protocol		Esql.agent_id_count_distin	5	unknown	1	TRUE		915c8097-8383-4b1f-afbd-ab6e5b		NOT COVERED	["Esql.agent_id_cc	["unknown"]
17	rich process e	Enrich process e	eql	MITRE ATT&CK	TA0007	Discovery	System Information Dis	System Information Discovery		event.action, event.type, p	4	logs-endpoint.	5	TRUE		afb9c171-a87b-46c7-a26e-b0c40d		COVERED	[]	[]
18	ntifies the exe	Identifies the exe	eql	MITRE ATT&CK	TA0005	Defense Evasion	Trusted Developer Utili	Trusted Developer Utilities	T1218.011	event.action, host.os.type,	5	logs-endpoint.	1	TRUE		399d8a1f-5b8d-430a-8de6-7d4a15		COVERED	[]	[]
19	ntifies unusua	Identifies unusua	eql	MITRE ATT&CK	TA0005	Defense Evasion	Masquerading	Masquerading		event.type, host.os.type, p	4	endgame-*, lo	5	TRUE		c8b572d7-0778-4a8f-8197-4ff766d		COVERED	[]	[]
20	ackers may al	Attackers may al	eql	MITRE ATT&CK	TA0005	Defense Evasion	Deobfuscate/Decode F	Deobfuscate/Decode Files	T1059.003	event.type, host.os.type, p	4	endgame-*, lo	5	TRUE		39474298-a970-4b97-a634-2e91a		COVERED	[]	[]
21	ntifies an exe	Identifies an exe	eql	MITRE ATT&CK	TA0002	Execution	Phishing	Phishing	T1566.001, T1566.002	event.type, file.extension, f	9	logs-endpoint.	3	TRUE		69ffb5ea-7b20-432b-9843-73e064		COVERED	[]	[]
22	ntifies binarie	Identifies binarie	eql	MITRE ATT&CK	TA0005	Defense Evasion	Masquerading	Masquerading	T1036.001	dll.Ext.relative_file_creatio	8	logs-endpoint.	1	TRUE		b1f97abb-e3f1-4074-add4-d5b9cb		NOT COVERED	[]	["logs-endpoint.events.library-*"]
23	ntifies attemp	Identifies attemp	eql	MITRE ATT&CK	TA0005	Defense Evasion	Modify Registry, Servic	Modify Registry, Service Stop		event.type, host.os.type, p	6	logs-endpoint.	2	TRUE		9b8254bc-8fdc-4d09-b74d-bb4a0f		COVERED	[]	[]
24	ntifies potenti	Identifies potenti	eql	MITRE ATT&CK	TA0011	Command and Contr	Application Layer Protc	Application Layer Protocol	T1071.001, T1573.001,	destination.ip, destination.p	4	logs-endpoint.	2	TRUE		07fb496d-f211-48ce-a0a1-6e2f7d0		COVERED	[]	[]
25	s rule detects	This rule detects	esql	MITRE ATT&CK	TA0007	Discovery	Network Service Disco	Network Service Discovery		Esql.agent_id_count_distin	6	unknown	1	TRUE		c78f2e36-cac5-4ef6-bcb9-7e031fe		NOT COVERED	["Esql.agent_id_cc	["unknown"]
26	ntifies the use	Identifies the use	query	MITRE ATT&CK	TA0007	Discovery	System Service Discov	System Service Discovery,	T1087.001, T1087.002,	event.category, host.os.typ	4	winlogbeat-*, l	2	TRUE		0646781f-bb9a-43d0-a348-80cd33		COVERED	[]	[]
27	ntifies child p	Identifies child pr	eql	MITRE ATT&CK	TA0005	Defense Evasion	System Binary Proxy E	System Binary Proxy Exec	T1218.011	event.type, host.os.type, p	9	logs-endpoint.	4	TRUE		79d020eb-4d76-4c94-a35c-ef07a5		COVERED	[]	[]
28	adable Kernel	Loadable Kernel	new_terms	MITRE ATT&CK	TA0007	Discovery	System Information Dis	System Information Discovery		event.action, event.catego	5	auditbeat-*, lo	2	TRUE		5e19b19d-22ab-4348-8c17-b4907f		COVERED	[]	[]
29	versaries may	Adversaries may	eql	MITRE ATT&CK	TA0008	Lateral Movement	Remote Services	Remote Services	T1021.001	destination.ip, destination.p	6	logs-endpoint.	1	TRUE		9bf6eca4-2f3b-4342-87c0-deeed74		NOT COVERED	[]	["logs-endpoint.events.network-*"]
30	s rule identifie	This rule identifie	eql	MITRE ATT&CK	TA0005	Defense Evasion	Indicator Removal	Indicator Removal	T1070.004	event.type, host.os.type, p	5	logs-endpoint.	1	TRUE		889eab49-2fc5-4e9e-830d-ee0da9		COVERED	[]	[]
31	ndows Backgr	Windows Backgr	eql	MITRE ATT&CK	TA0011	Command and Contr	Ingress Tool Transfer, E	Ingress Tool Transfer, BITS Jobs, BITS Jobs		event.type, host.os.type, p	4	endgame-*, lo	5	TRUE		6abfe83e-ae8b-491c-b4fc-93f4448		COVERED	[]	[]
32	tallUtil is a co	InstallUtil is a co	eql	MITRE ATT&CK	TA0005	Defense Evasion	System Binary Proxy E	System Binary Proxy Exec	T1218.004	event.type, host.os.type, p	4	endgame-*, lo	5	TRUE		0aa6a508-5f03-4caa-8fcf-4cc8bbb		COVERED	[]	[]
33	s rule detects	This rule detects	esql	MITRE ATT&CK	TA0007	Discovery	Network Service Disco	Network Service Discovery		Esql.agent_id_count_distin	8	unknown	1	TRUE		46b4b2cf-a5e4-46a1-a498-53e9eb		NOT COVERED	["Esql.agent_id_cc	["unknown"]
34	ntifies attemp	Identifies attemp	eql	MITRE ATT&CK	TA0005	Defense Evasion	Modify Registry, Create	Modify Registry, Create or	T1543.003, T1543.003	event.type, process.args, p	3	endgame-*, lo	5	TRUE		6a7d1e7c-321f-4e13-a363-41f488		COVERED	[]	[]
35	ntifies the exe	Identifies the exe	eql	MITRE ATT&CK	TA0005	Defense Evasion	System Binary Proxy E	System Binary Proxy Execution		event.action, host.os.type,	6	endgame-*, lo	5	TRUE		a5e2e5ed-b3e2-42ad-b382-20cf6c		COVERED	[]	[]
36	ntifies the cha	Identifies the cha	eql	MITRE ATT&CK	TA0005	Defense Evasion	File and Directory Pern	File and Directory Permiss	T1222.001	event.type, host.os.type, p	6	logs-endpoint.	1	TRUE		5a68ec7c-5217-44ed-b15e-dbb580		COVERED	[]	[]
37	s rule monitor	This rule monitor	threshold	MITRE ATT&CK	TA0007	Discovery	Process Discovery, Sys	Process Discovery, System Information Discovery		event.action, event.catego	6	auditbeat-*, lo	2	TRUE		1b7150a7-2be6-4332-9e08-96166		COVERED	[]	[]
38	ntifies indirec	Identifies indirect	eql	MITRE ATT&CK	TA0005	Defense Evasion	Indirect Command Exe	Indirect Command Execution		event.type, host.os.type, p	3	endgame-*, lo	5	TRUE		c0bfe937-f934-4714-aad3-265555		COVERED	[]	[]
39	ntifies suspici	Identifies suspici	eql	MITRE ATT&CK	TA0005	Defense Evasion	System Binary Proxy E	System Binary Proxy Exec	T1218.007	event.action, host.os.type,	12	logs-endpoint.	4	TRUE		19417a7c-7dd1-4dac-a10d-fc3a3b		COVERED	[]	[]
40	ntifies the use	Identifies the use	query	MITRE ATT&CK	TA0008	Lateral Movement	Remote Services, Com	Remote Services, Comma	T1021.006, T1059.001	event.category, file.directo	5	winlogbeat-*, l	2	TRUE		9d355cda-5fcf-4c3c-a80b-478708a		COVERED	[]	[]
41	ntifies unusua	Identifies unusua	eql	MITRE ATT&CK	TA0005	Defense Evasion	System Binary Proxy E	System Binary Proxy Exec	T1566.001, T1566.002	event.type, file.Ext.window	7	logs-endpoint.	1	TRUE		6710dc7d-5031-463e-ba74-af3e7e		NOT COVERED	[]	["logs-endpoint.events.file-*"]
42	nitors file eve	Monitors file eve	new_terms	MITRE ATT&CK	TA0007	Discovery	System Information Dis	System Information Discovery		event.action, event.catego	5	auditbeat-*, lo	2	TRUE		8b3c4cb3-d3bf-49fb-99d0-43136e2		COVERED	[]	[]
43	ntifies files wr	Identifies files wr	eql	MITRE ATT&CK	TA0009	Collection	Data Staged	Data Staged	T1074.001	event.type, file.name, file.p	4	logs-endpoint.	4	TRUE		3fc8cd31-b3bb-4420-9dbe-704509		COVERED	[]	[]
44	s rule detects	This rule detects	esql	MITRE ATT&CK	TA0003	Persistence	Server Software Comp	Server Software Compone	T1505.003, T1059.004	Esql.agent_id_count_distin	7	unknown	1	TRUE		2a7a1aff-c1c5-4e2b-86fc-6585be8		NOT COVERED	["Esql.agent_id_cc	["unknown"]
45	ntifies separa	Identifies separa	esql	MITRE ATT&CK	TA0001	Initial Access	Valid Accounts, Phishir	Valid Accounts, Phishing, !	T1078.004, T1566.002	Esql.azure_signinlogs_pro	31	unknown	1	TRUE		5c55606c-53fb-4430-bcaf-069bf64		NOT COVERED	["Esql.azure_signi	["unknown"]
46	ntifies the use	Identifies the use	query	MITRE ATT&CK	TA0003	Persistence	Server Software Comp	Server Software Compone	T1505.002, T1059.001	event.category, host.os.typ	4	winlogbeat-*, l	2	TRUE		25c7402e-27c6-44ca-ad3a-3b9361		COVERED	[]	[]
47	s rule leverag	This rule leverag	esql	MITRE ATT&CK	TA0005	Defense Evasion	Obfuscated Files or Inf	Obfuscated Files or Inform	T1059.004, T1204.002	Esql.agent_id_count_distin	6	unknown	1	TRUE		ee658924-41df-4950-9ddd-9a3d40		NOT COVERED	["Esql.agent_id_cc	["unknown"]

Configuration:

- Operation: Update
- Matching Column: Rule ID
- Document: Detection_Rules spreadsheet

Updated Columns:

- Coverage Status: COVERED/PARTIALLY COVERED/NOT COVERED
- Missing Log Sources: Array of unavailable sources
- Missing Fields: Array of unavailable fields

Purpose: Persists the coverage analysis results for reporting and visibility.

Data Flow Summary

1. **Trigger initiation** → Scheduled execution begins
2. **API call to Kibana** → Retrieves all data views
3. **Split data views** → Separates into individual items
4. **Field extraction** → Normalizes data view attributes
5. **Validation filter** → Removes invalid entries
6. **Detailed field retrieval** → Gets complete field mappings per data view
7. **Rule retrieval** → Fetches detection rules from Google Sheets
8. **Coverage analysis** → Intelligent matching of requirements vs. availability
9. **Results persistence** → Updates Google Sheets with coverage status