



Predict ATT&CK Tags in Sigma Rules with ML

Uncoder AI

Predict ATT&CK Tags in Sigma Rules with ML

```
1 title: llama3.3:70b invoke Keyword
2 id: 63 0508e
3 relate Short Summary ⓘ
4 - id Full Summary ⓘ 922c356f7
5 ty Decision Tree ⓘ
6 status
7 descri Query Optimization ⓘ 16 Base64 encoded powershell 'Invoke-' calls
8 refer Predict ATT&CK tags ⓘ
9 - ht-.../05/09/se0-poisoning-a-gootloader-story/
10 author: pH-T (Nextron Systems), Harjot Singh, @cyb3rjy0t
11 date: 2022-05-20
12 modified: 2023-04-06
13 tags:
14 - attack.t1059.001
15 - attack.t1027
16 logsource:
17 category: process_creation
18 product: windows
19 detection:
20 selection_img:
21 - Image|endswith:
22 - \powershell.exe
23 - \pwsh.exe
24 - OriginalFileName:
25 - PowerShell.EXE
```

Released on April 16

Predict ATT&CK Tags in Sigma Rules with ML

MITRE ATT&CK is a widely used framework for detection content, yet mapping rules to it takes time and training. Uncoder AI uses a privately hosted ML model to map a provided Sigma rule to ATT&CK techniques and subtechniques.

- Data doesn't leave SOC Prime's infrastructure
- The model has been trained on over 20,000 Sigma rules, being the largest manually created dataset in existence
- SOC Prime has unique way of tagging Sigma rules as we have've invented this approach in 2018 and advocated it since then
- Reduces manual effort in mapping detections to ATT&CK
- Ensuring that detections are systematically aligned to ATT&CK:
 - Improves visibility into technique coverage and gaps
 - Facilitates better correlation with threat intel, red team findings, and adversary emulation plans
 - Helps in structured reporting