



Rule/Query Generation with a Custom AI Prompt

Uncoder AI

Released on April 16

Translate functions with Gpt-4o-Mini

Search Detection Rules

Custom Prompt

GENERATE

AI Tools

Contribute

Validate

Intelligence

1 Write 3 Splunk queries to detect activities associated with APT 29 in an environment where endpoint logging is limited to default Windows audit log

```
3 **Query 1: Detecting suspicious PowerShell activity**
4 ```spl
5 index=windows_security EventID=4688
6 | regex "powershell.exe"
7 | search (CommandLine="*Invoke-Command*" OR CommandLine="*Invoke-Expression*")
8 | stats count as num_events by ComputerName, UserName, CommandLine
9 | where num_events > 5
10 | sort -num_events
11 ```
12 This query looks for PowerShell execution events (Event ID 4688) that contain
   suspicious command lines, such as 'Invoke-Command' or 'Invoke-Expression', which
   are commonly used by APT 29. It then aggregates the results by computer name, user
   name, and command line, filtering out instances with fewer than 5 occurrences.
13
14 **Query 2: Identifying potential credential dumping**
15 ```spl
16 index=windows_security EventID=4663
17 | regex "lsass.exe"
18 | search (ObjectName="*SAM*" OR ObjectName="*LSA*")
19 | stats count as num_events by ComputerName, UserName, ObjectName
20 | where num_events > 2
21 | sort -num_events
```

How it works?

DEBUG CONSOLE (1)

Rule/Query Generation with a Custom AI Prompt

The context and requirements when writing detections may be unique. Uncoder AI analyzes the provided custom prompt and generates a rule/query to detect the described behavior taking into account user's instructions. For this purpose, Uncoder AI uses Llama 3.3 customized for detection engineering and threat intelligence processing, hosted at SOC Prime SOC 2 Type II private cloud for maximum security, privacy, and IP protection.

- All the capabilities of rule generation from threat report
- Custom instructions allow for generating detections tailored to a particular environment or context