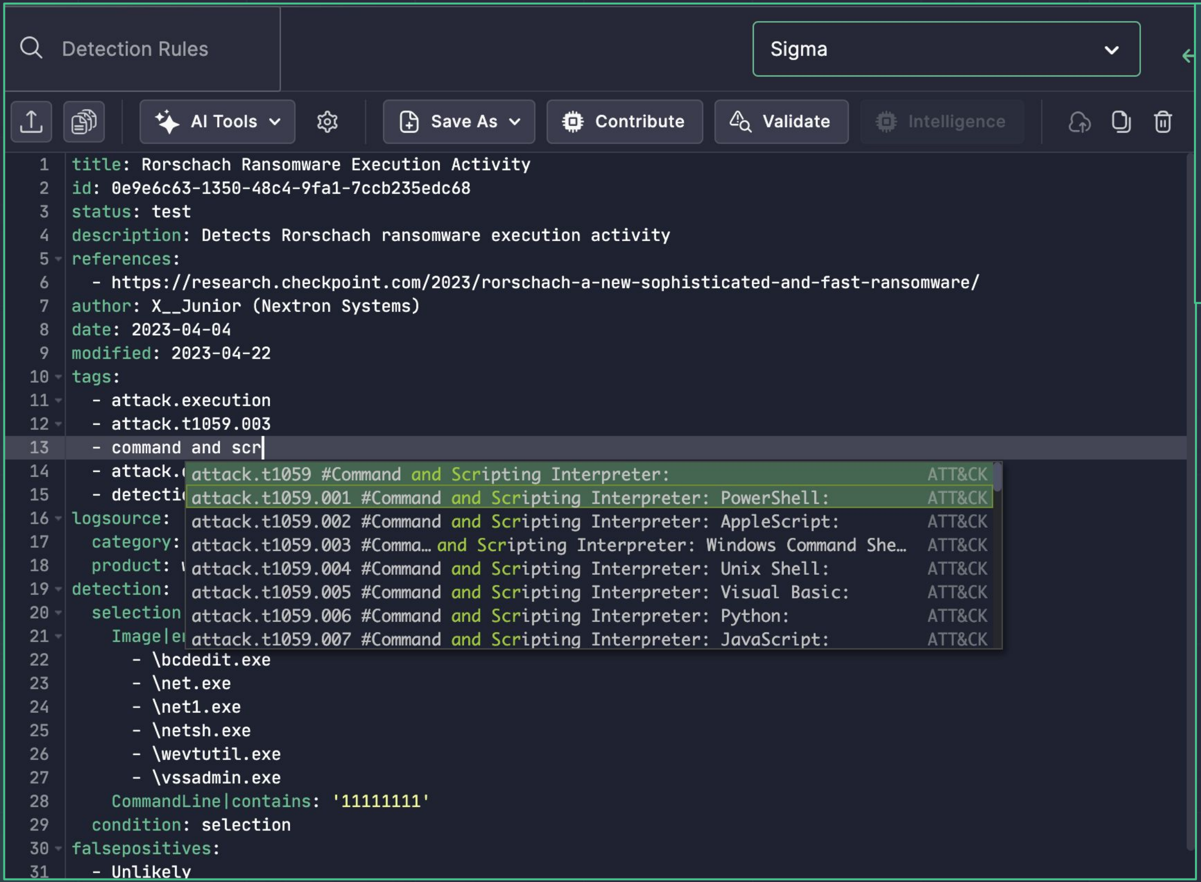
Convenient Detection Code Editor

Uncoder AI

Convenient Detection Code Editor



```
title: Rorschach Ransomware Execution Activity
id: 0e9e6c63-1350-48c4-9fa1-7ccb235edc68
status: test
description: Detects Rorschach ransomware execution activity
references:
  - https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/
author: X__Junior (Nextron Systems)
date: 2023-04-04
modified: 2023-04-22
tags:
  - attack.execution
  - attack.t1059.003
  - command and scr
  - attack.(
  - detecti
logsource:
  category:
  product: w
detection:
  selection
    Image|e
      - \bcdedit.exe
      - \net.exe
      - \net1.exe
      - \netsh.exe
      - \wevtutil.exe
      - \vssadmin.exe
    CommandLine|contains: '11111111'
  condition: selection
falsepositives:
  - Unlikely
```

```
attack.t1059 #Command and Scripting Interpreter:                                   ATT&CK
attack.t1059.001 #Command and Scripting Interpreter: PowerShell:                   ATT&CK
attack.t1059.002 #Command and Scripting Interpreter: AppleScript:                  ATT&CK
attack.t1059.003 #Comma… and Scripting Interpreter: Windows Command She…           ATT&CK
attack.t1059.004 #Command and Scripting Interpreter: Unix Shell:                   ATT&CK
attack.t1059.005 #Command and Scripting Interpreter: Visual Basic:                 ATT&CK
attack.t1059.006 #Command and Scripting Interpreter: Python:                       ATT&CK
attack.t1059.007 #Command and Scripting Interpreter: JavaScript:                   ATT&CK
```

In production

Convenient Detection Code Editor

Uncoder AI is an IDE for detection engineering. Any IDE starts with a convenient code editor.

- Language-specific syntax highlighting
- Automatic language detection
- Sigma and Roota templates
- Upload from file
- Code autocomplete including MITRE ATT&CK and log sources from all Sigma rules in Threat Detection Marketplace