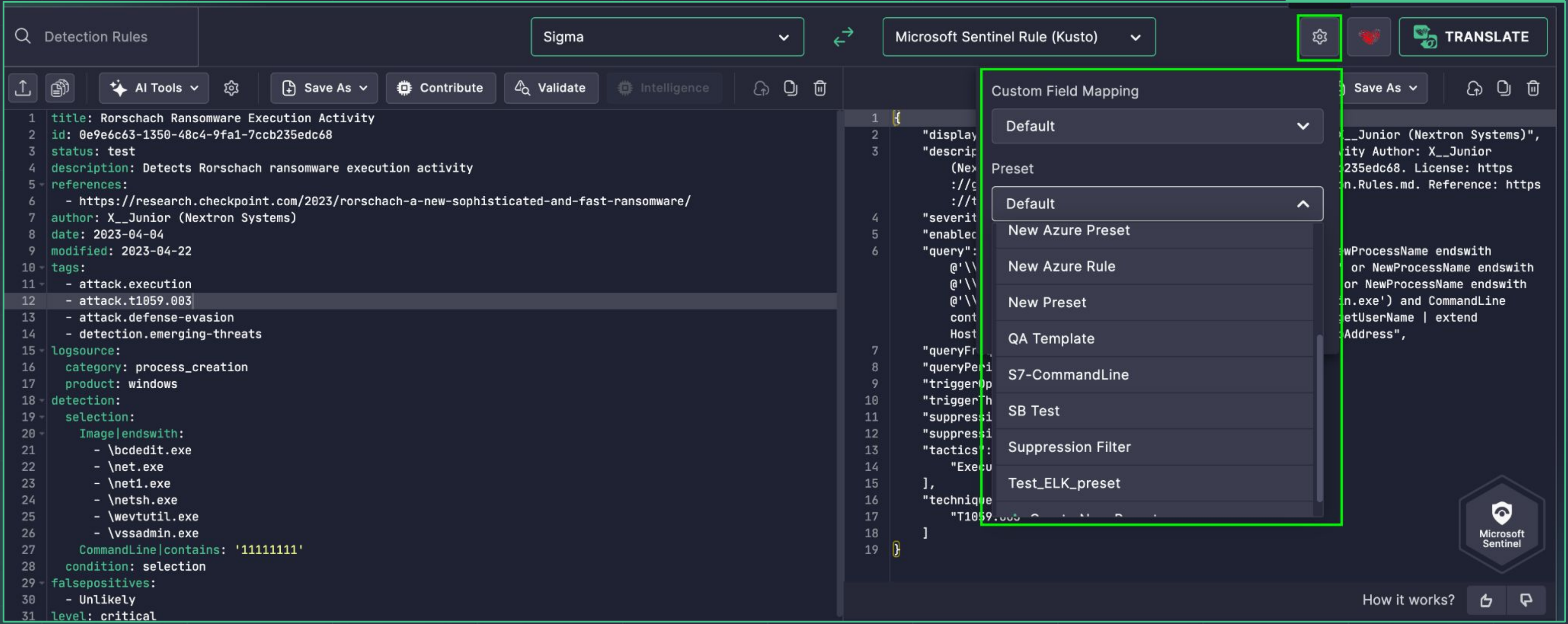
# Rule Customization On The Fly

Uncoder AI

# Rule Customization On The Fly

In production



```yaml
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
  - attack.defense-evasion
  - detection.emerging-threats
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|endswith:
      - \bcdedit.exe
      - \net.exe
      - \net1.exe
      - \netsh.exe
      - \wevtutil.exe
      - \vssadmin.exe
    CommandLine|contains: '11111111'
  condition: selection
falsepositives:
  - Unlikely
level: critical
```

Custom Field Mapping: Default

Preset: Default

```
{
    "display                                        __Junior (Nextron Systems)",
    "descrip                                        ity Author: X__Junior
        (Nex                                        235edc68. License: https
        ://g                                        n.Rules.md. Reference: https
        ://t
    "severit
    "enabled
    "query":                                        wProcessName endswith
        @'\\                                         or NewProcessName endswith
        @'\\                                        or NewProcessName endswith
        @'\\                                        n.exe') and CommandLine
        cont                                        etUserName | extend
        Host                                        Address",
    "queryFr
    "queryPeri
    "triggerOp
    "triggerTh
    "suppressi
    "suppressi
    "tactics":
        "Execu
    ],
    "technique
        "T1059.
    ]
}
```

# Rule Customization On The Fly

**Use customization profiles to modify your rules and queries on the fly:**

- Custom Field Mapping to tailor table/index and field names to your unique environment
    - Rapid deployment of detection content across heterogeneous environments
    - Compatibility across different log sources and normalization layers, enhancing detection fidelity
- Presets to modify rule/alert parameters
    - Supports rule modularity by externalizing variables like thresholds, severity, frequency, etc.
    - Enables SOCs to align alerts with internal risk models or escalation criteria without editing raw content
- Filters to add exceptions to the detection logic
    - Adds flexible suppression mechanisms for known-benign activity, asset-specific exceptions, or change windows
    - Minimizes alert fatigue and false positives while maintaining rule integrity

Customization profiles reduce the overhead of manual rule tuning, accelerate time-to-value in detection deployment, and support efficient lifecycle management across diverse environments without compromising detection integrity.