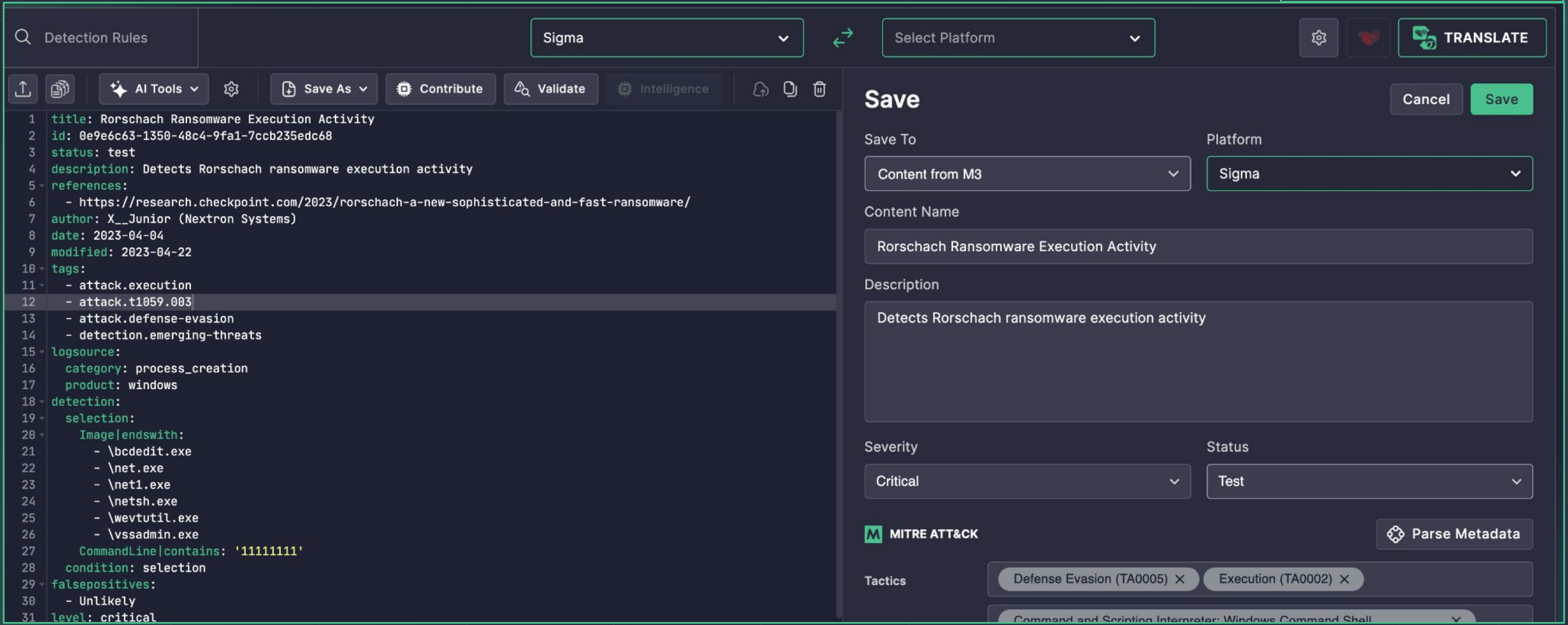
Saving Code and Intelligence to Custom Repositories

Uncoder AI

Saving Code and Intelligence to Custom Repositories

In production



```
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
```

Save

Save To: Content from M3

Platform: Sigma

Content Name: Rorschach Ransomware Execution Activity

Description: Detects Rorschach ransomware execution activity

Severity: Critical

Status: Test

Tactics: Defense Evasion (TA0005) ✕ Execution (TA0002) ✕

Command and Scripting Interpreter: Windows Command Shell ✕

Saving Code and Intelligence to Custom Repositories

Enable full detection content life cycle on the SOC Prime Platform. Save rules together with their intelligence and metadata in the standard Threat Detection Marketplace format. Use them just as stock content for manual or automated deployment, Attack Detective scans, etc.

- Storing in secure SOC Prime Platform's cloud infrastructure (with an encrypted rule body at rest)
- Enables centralized full detection content life cycle from development to deployment and documenting
- Native GitLab, GitHub, and Azure DevOps integrations supported
- Convenient access to and format consistency with Threat Detection Marketplace stock content