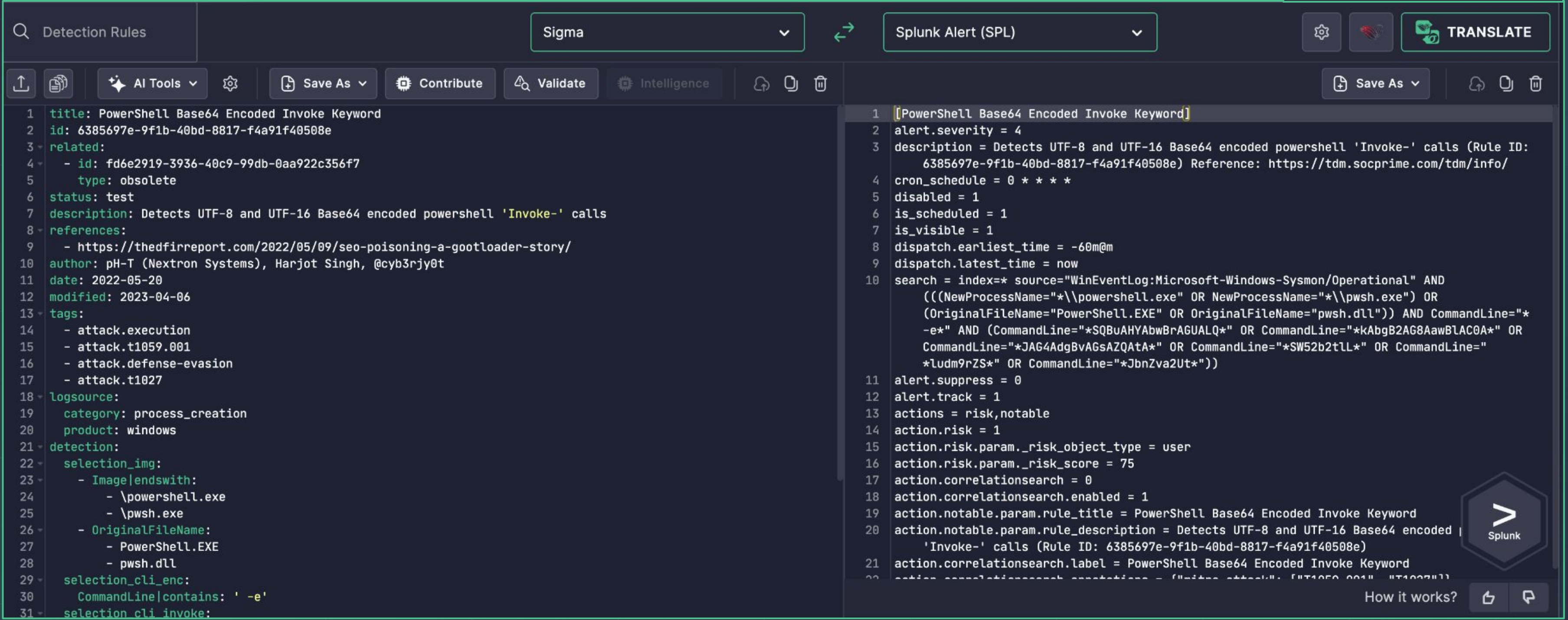
SOC PRIME

Translate from Sigma into 48 Languages

Uncoder AI

Translate from Sigma into 48 Languages

In production



```
title: PowerShell Base64 Encoded Invoke Keyword
id: 6385697e-9f1b-40bd-8817-f4a91f40508e
related:
  - id: fd6e2919-3936-40c9-99db-0aa922c356f7
    type: obsolete
status: test
description: Detects UTF-8 and UTF-16 Base64 encoded powershell 'Invoke-' calls
references:
  - https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
author: pH-T (Nextron Systems), Harjot Singh, @cyb3rjy0t
date: 2022-05-20
modified: 2023-04-06
tags:
  - attack.execution
  - attack.t1059.001
  - attack.defense-evasion
  - attack.t1027
logsource:
  category: process_creation
  product: windows
detection:
  selection_img:
    - Image|endswith:
        - \powershell.exe
        - \pwsh.exe
    - OriginalFileName:
        - PowerShell.EXE
        - pwsh.dll
  selection_cli_enc:
    CommandLine|contains: ' -e'
  selection_cli_invoke:
```

```
[PowerShell Base64 Encoded Invoke Keyword]
alert.severity = 4
description = Detects UTF-8 and UTF-16 Base64 encoded powershell 'Invoke-' calls (Rule ID:
    6385697e-9f1b-40bd-8817-f4a91f40508e) Reference: https://tdm.socprime.com/tdm/info/
cron_schedule = 0 * * * *
disabled = 1
is_scheduled = 1
is_visible = 1
dispatch.earliest_time = -60m@m
dispatch.latest_time = now
search = index=* source="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND
    (((NewProcessName="*\\powershell.exe" OR NewProcessName="*\\pwsh.exe") OR
    (OriginalFileName="PowerShell.EXE" OR OriginalFileName="pwsh.dll")) AND CommandLine="*
    -e*" AND (CommandLine="*SQBuAHYAbwBrAGUALQ*" OR CommandLine="*kAbgB2AG8AawBlAC0A*" OR
    CommandLine="*JAG4AdgBvAGsAZQAtA*" OR CommandLine="*SW52b2tlL*" OR CommandLine="
    *ludm9rZS*" OR CommandLine="*JbnZva2Ut*"))
alert.suppress = 0
alert.track = 1
actions = risk,notable
action.risk = 1
action.risk.param._risk_object_type = user
action.risk.param._risk_score = 75
action.correlationsearch = 0
action.correlationsearch.enabled = 1
action.notable.param.rule_title = PowerShell Base64 Encoded Invoke Keyword
action.notable.param.rule_description = Detects UTF-8 and UTF-16 Base64 encoded p
    'Invoke-' calls (Rule ID: 6385697e-9f1b-40bd-8817-f4a91f40508e)
action.correlationsearch.label = PowerShell Base64 Encoded Invoke Keyword
action.correlationsearch.annotations = {"mitre_attack": ["T1059.001", "T1027"]}
```

Translate from Sigma into 48 Languages

Don't get into a vendor lock-in with your security platform. Uncoder AI natively translates Sigma rues into multiple SIEM, EDR, XDR, and Data Lake languages.

- Detection portability & scalability across heterogeneous environments
- #1 translation engine for Sigma rules – by users, by languages, by features
- Security vendor agnosticism with Sigma as a single source of truth
- Removing translation overhead
- Leveraging large Sigma community for open-source detections
- Full use case life cycle support when combined with Threat Detection Marketplace

Translate from Sigma into 48 Languages

48 languages supported in production

ANOMALI	APACHE kafka	ArcSight	CORTEX XSIAM BY PALO ALTO NETWORKS	CORTEX XDR BY PALO ALTO NETWORKS	AWS Athena	OpenSearch	DEVO
CROWDSTRIKE	FORTINET	REGEX	graylog	DATADOG	DNIF	ElastAlert	Elastic Stack
HUNTERS	LOGPOINT	LogRhythm	Falco	CrowdStrike Falcon LogScale	FIREEYE	Google Security Operations	hawksearch
Radar	LACEWORK	LIMA CHARLIE	LOGIQ	Microsoft Defender for Endpoint	Microsoft Sentinel	nviso	PowerShell
Qualys	GREP	ROOTA	RSA NETWITNESS	securonix	SentinelOne	snowflake	splunk>
SQL	SQLite	STIX	StreamAlert	sumo logic	Sysmon	uberAgent	Carbon Black.