



# AI-Assisted Cross-Platform Translation

Uncoder AI

In production

Detection Rules

Microsoft Sentinel Query (Kusto)

Splunk Query (SPL)

TRANSLATE

AI Tools Save As Contribute

Sigma Splunk Query (SPL)

Save As

```
1 SAPBTPAuditLog_CL
2 | where Message has "malware"
3 | extend MessageData = parse_json(tostring(Message.data))
4 | extend
5 |   ClusterID = tostring(MessageData.clusterID),
6 |   WorkspaceID = tostring(MessageData.wsID),
7 |   Message = tostring(MessageData.message)
8 | parse Message with * 'user: ' User '.The following issues were detected: ' Malware ',' *
9 | extend
10 |   AccountName = tostring(split(User, '@')[0]),
11 |   UPNSuffix = tostring(split(User, '@')[1])
12 | project
13 |   UpdatedOn,
14 |   ClusterID,
15 |   WorkspaceID,
16 |   Message@,
17 |   User,
18 |   Malware,
19 |   Tenant,
20 |   SpaceId,
21 |   Category,
22 |   CloudApp = "SAP BTP",
23 |   AccountName,
24 |   UPNSuffix
```

```
1 source=WinEventLog:* AND Message="*malware*" | spath input=Message.data output=MessageData | eval
  ClusterID = coalesce(MessageData.clusterID, ""), WorkspaceID = coalesce(MessageData.wsID, ""),
  Message = coalesce(MessageData.message, "") | rex field=Message "user: (?<User>.*?)\." The following
  issues were detected: (?<Malware>.*?)" | eval AccountName = split(User, "@")[0], UPNSuffix = split
  (User, "@")[1] | table UpdatedOn, ClusterID, WorkspaceID, Message, User, Malware, Tenant, SpaceId,
  Category, CloudApp="SAP BTP", AccountName, UPNSuffix
2
3 *** uuid: aacd3c35-862d-40b0-8788-07718b85a247 ***
4 *** author: not defined in query/rule ***
5 *** licence: DRL 1.1 ***
```

How it works?

DEBUG CONSOLE (1)

[08:49:33] UNMAPPED FIELDS IN SOURCE

Message

Translating content across security platform languages can become a nightmare, especially as part of SIEM migration. Uncoder AI translates across platform-native languages:

- 10 source languages and 21 target languages supported
- Basic query logic translated natively by Uncoder. Advanced function translation generated by third-party AI (OpenAI's GPT-4o-mini model)
- Opt-in use of third-party AI, only advanced functions are sent as part of prompt (we're in the process of transitioning to a locally hosted Llama model to further improve on privacy and speed)
- Any unmapped fields and source parts that are not supported by target are listed for manual review
- Sigma rule generated for each translation to capture the basic logic

# AI-Assisted Cross-Platform Translation

21 languages supported as target

ANOMALI



AWS Athena

OpenSearch

CORTEX XSIAM

CORTEX XDR

CROWDSTRIKE

FORTINET

graylog

ElastAlert

Elastic Stack

HUNTERS



Google Security Operations

LogRhythm

Falco

CrowdStrike  
Falcon LogScale

Radar



Microsoft  
Defender  
for Endpoint



Microsoft  
Sentinel

SentinelOne

Sigma

splunk>

10 languages supported as source



AWS Athena

OpenSearch

CROWDSTRIKE

Elastic Stack

CrowdStrike  
Falcon LogScale



Google Security Operations

Radar



Microsoft  
Defender  
for Endpoint



Microsoft  
Sentinel

splunk>