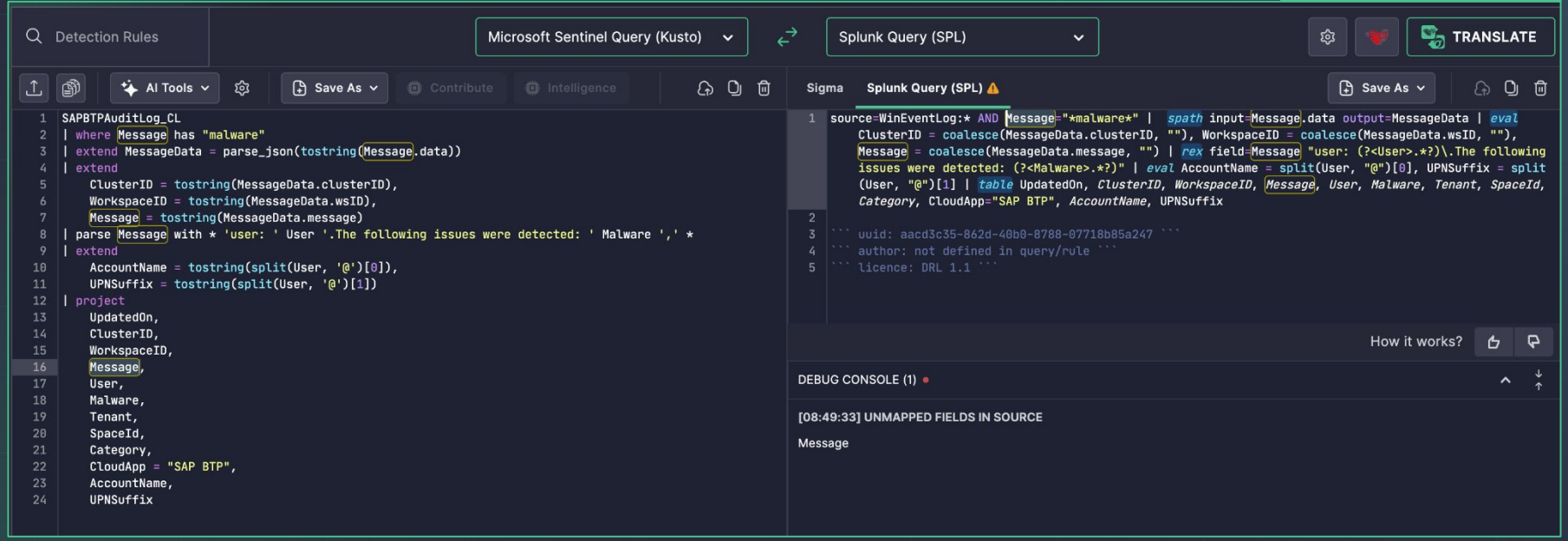
AI-Assisted Cross-Platform Translation

Uncoder AI

AI-Assisted Cross-Platform Translation

In production



AI-Assisted Cross-Platform Translation

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
- QRadar
- 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
- QRadar
- Microsoft Defender for Endpoint
- Microsoft Sentinel
- splunk>