SAC

Al-Assisted Cross-Platform Translation

Uncoder Al

Confidential and Proprietary. Do not distribute without consent. © SOC Prime 2025. All rights reserved.

AI-Assisted Cross-Platform Translation

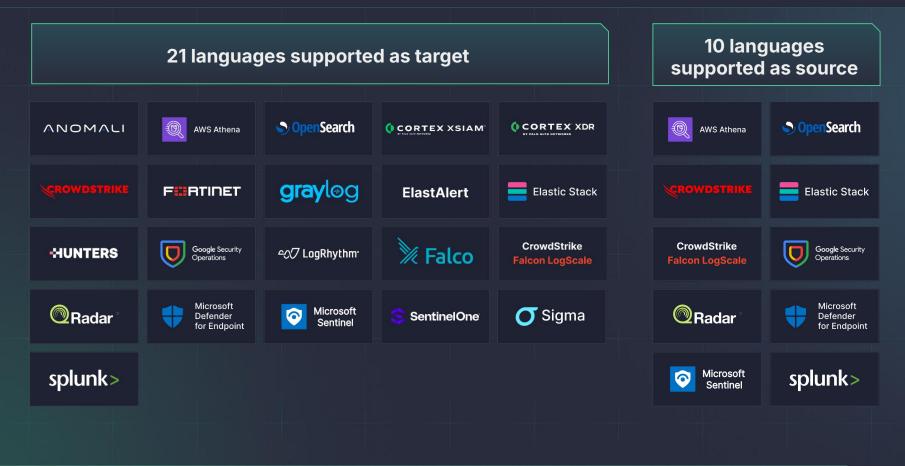
										In production
Q Detect	ion Rules		Ĵ Save As ∽	Contribute	Microsoft Sentinel		usto) 🗸	> S Sigma	plunk Query (SPL) 🗸	a ave As v A O
1 SAPBTF 2 when 3 exte 4 exte 5 CT 6 when 5 CT 6 when 6 pars 9 exte 10 Act 11 UF 12 proj	<pre>SAPBTPAuditLog_CL I where Message has "malware" I extend MessageData = parse_json(tostring(Message.data)) I extend ClusterID = tostring(MessageData.clusterID), WorkspaceID = tostring(MessageData.wsID), Message = tostring(MessageData.message) I parse Message with * 'user '.The following issues were detected: ' Malware ',' * I extend AccountName = tostring(split(User, '@')[0]), UPNSuffix = tostring(split(User, '@')[1]) I project</pre>						<pre>Sigins Splith Guesy(SFC) Solution Constraints of the state of the</pre>			
	ClusterID, WorkspaceID,									How it works? 🔥 🕻
16 Me 17 Us 18 Ma 19 Te 20 Sp 21 Ca 22 CT 23 Addition	ssage, ser, slware, snant, saceId, tegory, LoudApp = "SAP BT ccountName, PNSuffix	'₽",							ONSOLE (1) • 3] UNMAPPED FIELDS IN SOURCE	^

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



Confidential and Proprietary. Do not distribute without consent. © SOC Prime 2025. All rights reserved.