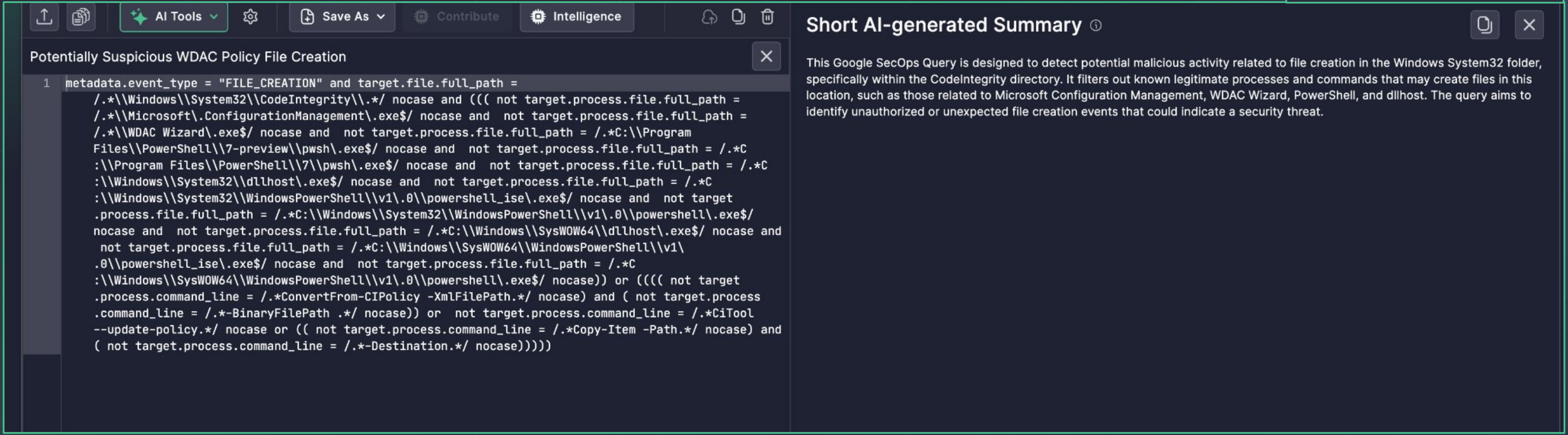
Rule/Query Short Summary with AI

Uncoder AI

Rule/Query Short Summary with AI

In production



Potentially Suspicious WDAC Policy File Creation

```
metadata.event_type = "FILE_CREATION" and target.file.full_path =
    /.*\\Windows\\System32\\CodeIntegrity\\.*/ nocase and ((( not target.process.file.full_path =
    /.*\\Microsoft\.ConfigurationManagement\.exe$/ nocase and  not target.process.file.full_path =
    /.*\\WDAC Wizard\.exe$/ nocase and  not target.process.file.full_path = /.*C:\\Program
    Files\\PowerShell\\7-preview\\pwsh\.exe$/ nocase and  not target.process.file.full_path = /.*C
    :\\Program Files\\PowerShell\\7\\pwsh\.exe$/ nocase and  not target.process.file.full_path = /.*C
    :\\Windows\\System32\\dllhost\.exe$/ nocase and  not target.process.file.full_path = /.*C
    :\\Windows\\System32\\WindowsPowerShell\\v1\.0\\powershell_ise\.exe$/ nocase and  not target
    .process.file.full_path = /.*C:\\Windows\\System32\\WindowsPowerShell\\v1\.0\\powershell\.exe$/
    nocase and  not target.process.file.full_path = /.*C:\\Windows\\SysWOW64\\dllhost\.exe$/ nocase and
     not target.process.file.full_path = /.*C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1\
    .0\\powershell_ise\.exe$/ nocase and  not target.process.file.full_path = /.*C
    :\\Windows\\SysWOW64\\WindowsPowerShell\\v1\.0\\powershell\.exe$/ nocase)) or (((( not target
    .process.command_line = /.*ConvertFrom-CIPolicy -XmlFilePath.*/ nocase) and ( not target.process
    .command_line = /.*-BinaryFilePath .*/ nocase)) or  not target.process.command_line = /.*CiTool
    --update-policy.*/ nocase or (( not target.process.command_line = /.*Copy-Item -Path.*/ nocase) and
    ( not target.process.command_line = /.*-Destination.*/ nocase)))))
```

Short AI-generated Summary ⓘ

This Google SecOps Query is designed to detect potential malicious activity related to file creation in the Windows System32 folder, specifically within the CodeIntegrity directory. It filters out known legitimate processes and commands that may create files in this location, such as those related to Microsoft Configuration Management, WDAC Wizard, PowerShell, and dllhost. The query aims to identify unauthorized or unexpected file creation events that could indicate a security threat.

Rule/Query Short Summary with AI

When working with third-party content, you often wish you could understand a query/rule at a glance. Uncoder AI transforms detection queries/rules into concise human-readable insights. For this purpose, Uncoder AI uses Llama 3.3 customized for detection engineering and threat intelligence processing, hosted at SOC Prime SOC 2 Type II private cloud for maximum security, privacy, and IP protection.

- "Executive level" summary of the detection logic
- Multiple languages supported
- Data doesn't leave SOC Prime's infrastructure

SOC PRIME

Rule/Query Short Summary with AI

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	C# 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.