Solution Brief

Uncoder AI: Unleashing the Power of AI for Advanced Detection Engineering

Uncoder AI: Overview

Uncoder AI unleashes the power of AI and collective expertise to enable security teams to code, validate, and share detection ideas across any technology with an all-in-one tool for advanced detection engineering.

85% Faster cross-SIEM content translation & fine-tuning

33K+ Cyber defenders providing feedback on detection ideas

100x Better code with in-built validation & customization

10K+ Sigma rules for any TTP or attack behavior

27+ SIEM, EDR, and XDR solutions

FASTER

Engineer detections swiftly and smartly backed by Sigma and MITRE ATT&CK® as code assistants.

- **Streamline your coding**
  Code faster with a built-in autocomplete wizard aggregating detection logic from 10K+ Sigma rules
- **Eliminate manual routine**
  Structure your thoughts and reduce manual effort with Sigma rule templates tailored to your engineering needs
- **Autotag with MITRE ATT&CK**
  Automatically tag detections with MITRE ATT&CK acting as your autocomplete dictionary
- **Never miss a beat of your work**
  Proceed with your work anytime, having progress saved and the history of translations available at hand
- **Test detection logic in a split second**
  Run logic tests directly from your in-built browser add-on
- **Accelerate IOC matching**
  Auto-parse threat reports and IOC files into custom queries ready to run in your SIEM or EDR

BETTER

Develop flawless detection code in a matter of seconds with automagic quality enhancement powered by collective intelligence.

- **Validate detection code with in-built checks**
  Ensure your code quality with 100+ automated Sigma rule syntax & logic checks
- **Customize rule code to your security needs**
  Adjust detection rules to your SIEM data schema on the fly
- **Tune up detections to cover your environment needs**
  Choose from a broad collection of filters and exceptions always at hand
- **Accelerate detection engineering routine**
  Rely on commercial API support to automate mundane ad-hoc tasks

UNCODER

Make the most of AI to have high-quality detection rules and verified hunting queries always at hand tailored to any SIEM, EDR & XDR environment in use.

- **Rely on feedback from peers**
  Validate how rules perform in real-world environments with Global Action Loop backed by the global community of 33K+ cyber defenders.
- **Your code, your rules**
  Bring your own Sigmac and pySigma backends for streamlined detection engineering tailored to your needs
- **Simplify SIEM migration**
  Rely on reverse translation capabilities powered by AI, shaving hours off your SIEM & XDR logic migration
- **Delegate code translation to augmented intelligence tools**
  Choose from ChatGPT & Google Translate to adjust detection code to any environment or bring your own AI-assisted engine

Learn More

For more information about SOC Prime's AI-assisted solution, visit uncoder ai or get started with a public version of Uncoder at uncoder.io, available at no cost and without registration. Uncoder.IO is the result of the prolific teamwork of SOC Prime's engineering team located in Ukraine.

Explore SOC Prime to defend against attacks easier, faster, and more efficiently than ever before.

LEARN MORE