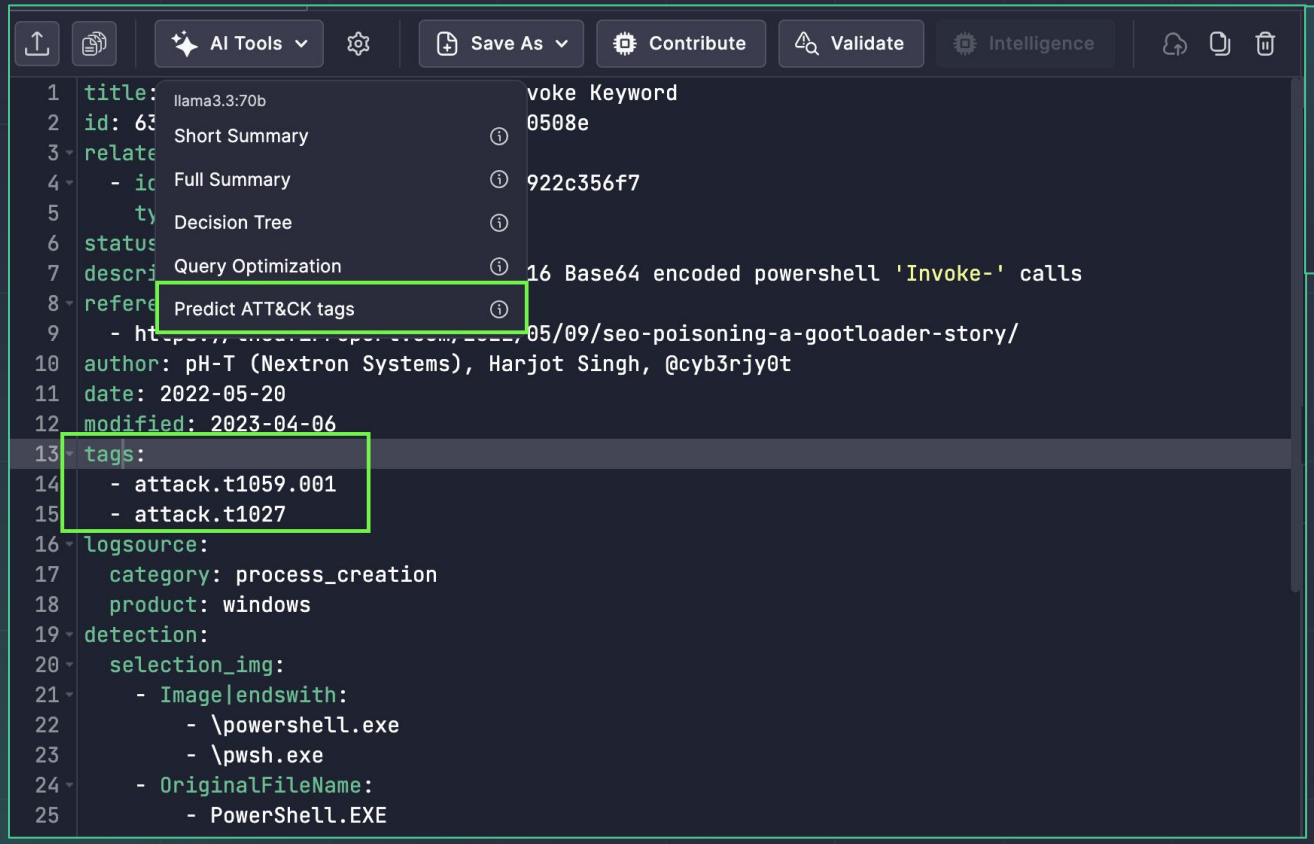
Predict ATT&CK Tags in Sigma Rules with ML

Uncoder AI

Predict ATT&CK Tags in Sigma Rules with ML



Released on April 16

Predict ATT&CK Tags in Sigma Rules with ML

MITRE ATT&CK is a widely used framework for detection content, yet mapping rules to it takes time and training. Uncoder AI uses a privately hosted ML model to map a provided Sigma rule to ATT&CK techniques and subtechniques.

- Data doesn't leave SOC Prime's infrastructure
- The model has been trained on over 20,000 Sigma rules, being the largest manually created dataset in existence
- SOC Prime has unique way of tagging Sigma rules as we have've invented this approach in 2018 and advocated it since then
- Reduces manual effort in mapping detections to ATT&CK
- Ensuring that detections are systematically aligned to ATT&CK:
  - Improves visibility into technique coverage and gaps
  - Facilitates better correlation with threat intel, red team findings, and adversary emulation plans
  - Helps in structured reporting