

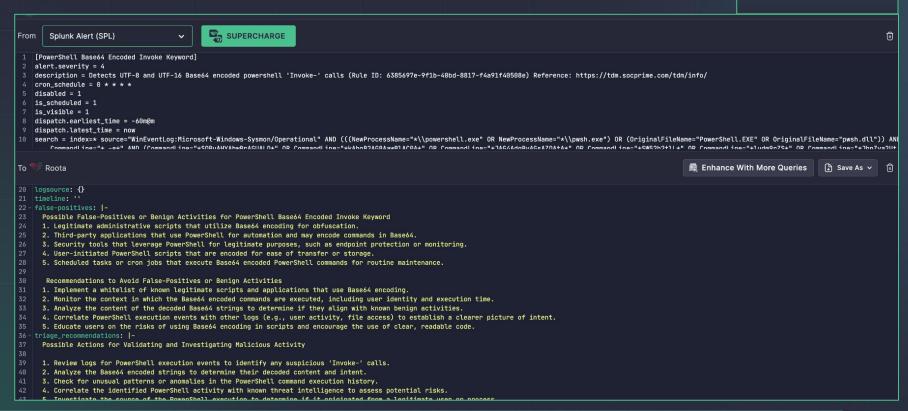
Supercharge into Roota

Uncoder Al



Supercharge into Roota

In production





Supercharge into Roota

Turn a platform-specific rule or query into a Roota rule and enrich it with metadata using SOC Prime's proprietary algorithms and Al.

- Al input on possible false positives and triage recommendations (only metadata is used for prompting)
- Adding possible log sources if they were not specified in the original content.
 Additionally, the audit section is filled that specifies what logging service should be enabled to have the logs required and how to enable it
- Prediction of relevant MITRE ATT&CK techniques and sub-techniques with a machine learning model