Multilingual AI to SIEM threat detection logic creation

Oisin Hickey - C00247185

At a glance

This research aims to use experimental research to evaluate the ability of AI to act as a human to SIEM abstraction layer in the creation of threat detection logic; specifically when prompted in various languages such as Russian, Chinese, french, Spanish and Irish.

Key metrics

Some readers might prefer details like a breakdown of your funding while others, like your trustees, will be more interested in the challenges you encountered and the lessons you learned from them.

11
Total languages tested

6
Atomic red Team Tests

3
Total levels of complexity

198
Total unique tests

RESEARCH GAP

Although research exists relating to LLM's creating detection's or recognizing malicious logs, not much research has been performed into the ability of AI to operate in multiple languages when prompted to create detection's. Also, little research exists into prompting in complexities in multiple languages with a cybersecurity goal.

TECHNOLOGIES USED

Several technologies have been used in the experimental approach in this research. A dataset has been translated by volunteers with n8n used to send those prompts to Gemini, outputting a detection in SPL. This detection is then tested against atomic red team tests fired from caldera and ingested into Splunk.

CALDERA

RESEARCH QUESTIONS

1

Question One

Can out of the box models create effective threat detection logic?

2

Question Two

Can out of the box AI models create detection logic when prompted in different languages and complexities?

3

Question Three

Can AI create threat detection logic for various attacks that holds up against the scrutiny of a defined framework against industry standards?