A Study of Algorithmic Threat Detection Against Investigator-Led Response Methodologies

Name: Byrch Baker

Date Started: 15 June, 2025

Last Updated: 15 June 2025

# 1. Abstract / Summary

This paper examines the comparative effectiveness of algorithmic endpoint detection and threat response (EDTR) systems versus analyst-led cybersecurity operations in identifying, assessing, and mitigating cyber threats. It focuses on key performance factors such as detection accuracy, response speed, operational scalability, and their overall impact on an organization's security posture.

# 2. Background / Motivation

The in this topic was sparked by the observation that a significant number of cyber threats are not detected or mitigated by automated endpoint detection systems, but rather by human analysts. Despite the sophistication of algorithmic tools, many rely heavily on user-generated feedback and data initially identified by human investigators. This raised questions about the true autonomy and effectiveness of such systems, and whether human-led approaches still play a more critical role than often acknowledged.

# 3. Research Questions / Objectives

This study aims to evaluate the effectiveness of algorithmic endpoint detection systems compared to human-led cybersecurity operations in detecting and responding to both known and novel threats. The primary objective is to determine whether human analysts outperform automated systems in identifying emerging threats and effectively mitigating them before significant damage occurs.

Key questions guiding this research include:

* Are human analysts faster or more accurate at detecting new, previously unknown threats compared to automated EDTR systems?
* How effective are endpoint solutions at identifying threats without prior signatures or behavioral data?
* In what types of scenarios do human-led responses outperform algorithmic detection?
* To what extent do automated systems rely on data or insights first uncovered by human investigation?

The goal is to assess the practical usefulness and limitations of endpoint detection technologies in real-world, evolving threat landscapes.