Toward a Visualization-Supported Workflow for Cyber Alert Management Using Threat Models and Human-Centered Design

Cameron Noakes

February 2022

1 Sentence Overview

The proposed solution with regards to the conducted research is a report on their work with cyber analysts to understand the analytic process and how the MITRE ATT&CK framework matrix is used to structure analytic thinking and present their efforts to map specific data needed by analysts into this threat model. This is exclaimed to be able to inform the researchers visualization designs. and leverage this expert knowledge to identify gaps that might be filled with visual analytic tools.

The end proposition is a prototype visual analytic-supported alert management workflow to aid cyber analysts working with threat models.

2 Introduction

Most of this literature data and information was based off the two interviews they conducted with cyber analysts instead of more conventional ways to get data such as datasets.

The detailed acknowledgement of the tools at their disposal are often specific to a particular data type, resulting in an expanding number of tools between which an analyst has to switch during the investigative process instead of a handful the analysts could use for their work entirely. Another acknowledgement of how malicious activity itself is a moving dynamic, ever evolving target. Threats change over time as adversaries adopt new tactics and make use of newly-discovered resources to evade defenders.

The researchers mentioned a limitation in industry tooling as having few analytical tools directly being used for leveraging the ATT&CK framework. The researchers present an idea of a visual analytic tool for cyber defense that should engage a user centered design process that combines cyber models such as the ATT&CK framework.

They present a preliminary design space targeted at open gaps identified by cyber analysts and the researchers begin by describing the results of two knowledge elicitation interviews with expert cyber analysts. A description of the gaps within the two interviews helped discover and design spaces that the cyber analysts felt would help with their investigations.

3 Human-Centered Cyber Security

Various user-centered design techniques have been employed to help develop various tools for cyber security professionals as mentioned with regards to conducted interviews and field observations.

Descriptions from related work of how cognitive transformation as a hierarchy of data filters can produce intrusion data sets from raw network data. They also described a triage and escalation processes similar to what can be encountered in the conducted interviews with cyber analysts.

4 General Investigative Workflow Elicitation

Within the interviews, the cyber analysts were asked to elaborate on investigation workflows, which detailed how investigations are often to find the root cause of the alert and collecting relevant evidence on the related alert. They often check and use event logs as evidence as a way to invoke a 'sense making' process from often incomplete data. Event logs were repeatedly cited as the data type used across all parts of an investigation and all attack categories.

Key limitations were outlined in the literature from the use of interviews such as how the cyber analysts mentioned how most of their data is functionally useless but did not know what information was needed at the same time.

The researchers combine the mapping with the results from their first interview about daily and investigative workflows to establish a design space for tools supporting the investigative process.

5 Capability Gaps In Cyber Defender Support

The cyber analysts during the interviews mentioned some of the hard to detect stages that relate to the ATT&CK framework matrix of Tactics, techniques and procedures, they identified three stages of an attack as being particularly difficult to detect:

- Privilege Escalation
- Defense Evasion
- Lateral Movement.

The analysts noted a gap in the overall support for finding correlations between admin privileges and the presence of certain open source software. The researchers acknowledged that during their interview the cyber analysts said evasion techniques constantly evolve making it difficult to build or maintain rules to alert defenders.

6 Conclusion

a report was proposed on the researchers work with the use of various two interviews with different cyber analysts to understand the analytic process and how the MITRE ATT&CK framework matrix can be used to structure analytic thinking and present their efforts to map specific data needed by analysts into this threat model.

The end proposition is a prototype visual analytic-supported alert management workflow to aid cyber analysts working with threat models.

7 What problem does this solve?

The researchers proposed how there is a difficult challenge with structuring analytical thinking in reference to the relation between specific threat models such as the ATT&CK framework for cyber analyst work and alerts.

8 How do they solve it?

A report was developed by the researchers to better structure the analytical thinking process and the mapping of it to the MITRE ATT&CK framework matrix of TTPs.

9 How do they assess it?

The researchers identified for future work and evaluations that they want to consider design options to improve alert evaluation efficiency. Options include more sophisticated sorting functions, user-defined folder creation, and mixed-initiative recommendations of triage actions.