Detection of APTs through the use of Visual Analytics with the MASFAD framework

Georgi Nikolov [1] Wim Mees [1]

[1]Royal Military Academy, Brussels, Belgium

With the rapid evolution of the Internet and the prevalence of sophisticated adversarial cyber threats, it has become apparent that an equally rapid development of new Situation Awareness techniques is needed. The vast amount of data produced everyday detection systems can quickly become insurmountable to analyze by the domain experts. To enhance the human - machine interaction, new Visual Analytics systems need to be implemented and tested, bridging the gap between the detection of possible malicious activity, identifying it and taking the necessary measures to stop its propagation. The detection of previously unknown, highly sophisticated Advanced Persistent Threats (APT) adds a higher degree of complexity to this task.

Detection of APTs

The Multi-agent System for Advanced Persistent Threat Detection (MASFAD) [1] offers a possible solution for the detection of APTs, by focusing on anomaly and behavior-based analysis. The goal of the framework is to work in parallel with existing detection tools, offering a bigger detection surface by detecting threats that might escape typical IDS and IPS technologies. The MASFAD framework identifies key characteristics present in the majority of APTs it aims to detect threats with a high percentage of true positives, while reducing the amount of false detection. This is accomplished by implementing a large number of stand-alone agents, each responsible for the analysis and identification of a specific characteristic. Contrary to the majority of tools on the market, MASFAD does not generate alerts, instead providing the analyst with a "suspiciousness score" based on the aggregation metrics.

A major aspect of the MASFAD framework is aiding pattern recognition through the use of behavior- and anomaly-based analysis. To achieve this goal, some type of signature analysis still needs to be present, detecting possible relations between the evidence generated by the different agents and correlating them with possible anomalous behavior. The fallibility of machines and the ingrained capacity of humans to detect complex patterns through centuries long evolution, positions the domain experts as a vital component of any analysis. This leads to a greater need to enhance the human-machine interaction, offering complex visualization capabilities, thus empowering the Cyber Situation Awareness (CSA) of the operator.

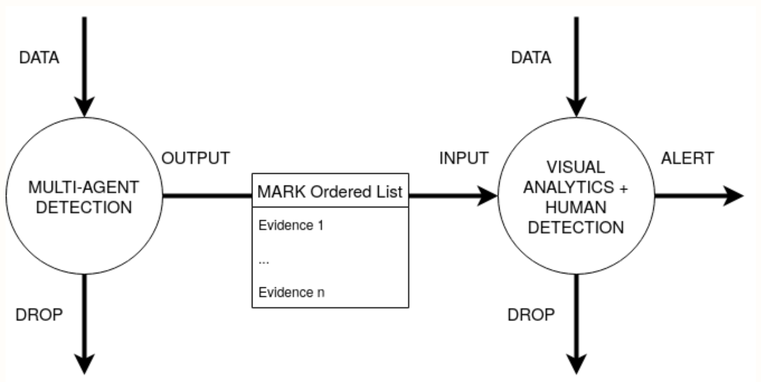

Figure 1: MASFAD pattern detection

The MASFAD framework is based on the principle of a “detection cascade”. Through the use of a mix of signature-based and anomaly-based algorithms, raw data is processed and information, deemed important, is retained to form the ordered list. Raw data, which does not show indicators of abnormal or malicious behavior is dropped. The ordered list is then used by the domain analyst to review instances of potentially dangerous behavior inside the network, through a combination of evidence produced by the system, raw data logs and visualizations.

Visual Analytics

Through the use of powerful visualizations the user can better focus on relevant information and go deeper, if needed, through the supplied interaction capabilities, greatly enhancing the perception phase of the CSA.

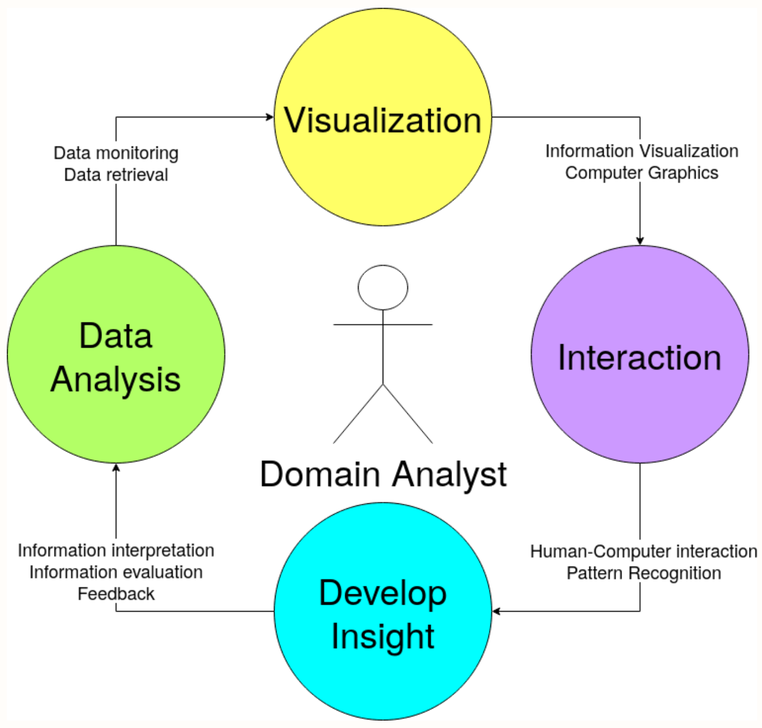

Figure 2: Visual Analytics Loop

By offering powerful visualizations and interactions, the analyst can develop greater insight into what has previously or is currently happening in the environment, aiding the comprehension. This is vital as interpreting the perceived information, recognising possible patterns and evaluating them gives better understanding of what has been observed and how to better counteract it. Finally a deeper analysis can be done on the data, using the gained insight, to construct a clear model of the situation and better understand its future impact on the environment.

Our goal is to reinforce the rapid identification of targets of interest, reinforcing the "pre-attentive processing". This helps greatly to quickly extract information as it demands little attention resources by the user, but is highly dependant on the type of displays used. The ultimate goal of any visualization is to use techniques to quickly make a specific element stand out from its surrounding elements, or better defined as "distractor objects".

Analysis and Visualization

The MASFAD framework offers multiple different dedicated visualizations:

- **Agent representation** - The Activation cascade shows what data is ingested, how the various detection agents are interconnected and what evidence they produce.
- **Ranked List representation** - Visualizing the evidence produced by the agents in a clear and understandable manner is very important. We aim to use the pre-attentive processing of humans to single out information of importance.
- **Evidence representation** - Figures specific to the agents are also produced. These representations aim to help the domain expert understand why the detection agent produced evidence for the specific data and explain the circumstances to the score generated by the agent.

Figure 3: Example of Bubble Graph Visualization

Anomaly based detection offers high detection of previously unknown attacks, but the disadvantage is the generation of a high quantity of false alarms. In “Fig. 4” we illustrate our intention for the MASFAD framework- through the use of the Multi-agent analysis, we aim to push the Pd as high as possible and through the combination with Visual Analytics expand the number of alerts which can be reviewed and the number of false alarms handled.

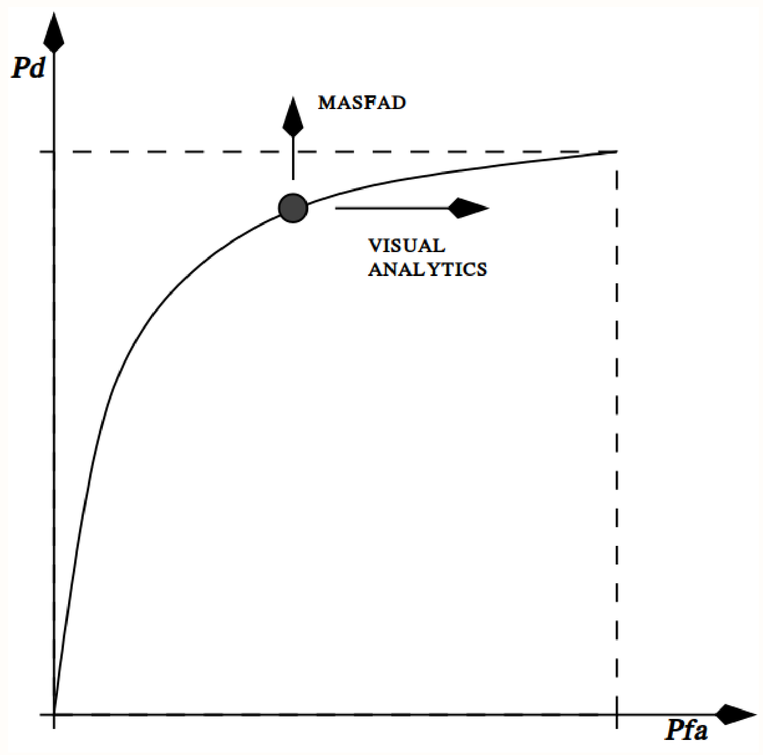

Figure 4: MASFAD receiver operating characteristics curve

Future Work

Currently the visualization aspect of the framework is in its infancy, but we aim to develop it further by applying the principles of Visual Analytics:

- Incorporate pre-attentive processing techniques
- Develop a robust dashboard visualization
- Evaluate the Situation Awareness of the users

References

[1] Nikolov, Georgi, and Wim Mees. "Detection of Previously Unknown Advanced Persistent Threats Through Visual Analytics with the MASFAD Framework." *2023 International Conference on Military Communications and Information Systems (ICMCIS). IEEE, 2023.*