Detection of previously unknown Advanced Persistent Threats through Visual Analytics with the MASFAD framework

1st Georgi Nikolov
Research Unit for Cyber Defense
Royal Military Academy
Brussels, Belgium
g.nikolov@cylab.be

2nd Wim Mees
Research Unit for Cyber Defense
Royal Military Academy
Brussels, Belgium
w.mees@cylab.be

***Abstract*—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 by Intrusion Detection Systems, Firewalls, Honeypots and other 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. In this paper, we discuss the principles inherent to Visual Analytics and propose a new technique for the detection of APT attacks through the use of anomaly and behavior-based analysis. Our ultimate goal is to define sophisticated cyber threats by their defining characteristics and combining those to construct a pattern of behavior, which can be presented in visual form to be explored and analyzed. This can be achieved through the use of our Multi-Agent System for Advanced Persistent Threat Detection (MASFAD) framework and the combination of highly-detailed and dynamic visualization techniques.**

This paper was originally presented at the NATO Science and Technology Organization Symposium (ICMCIS) organized by the Information Systems Technology (IST) Panel, IST-200 RSY – the ICMCIS, held in Skopje, North Macedonia, 16-17 May 2023.

***Index Terms*—advanced persistent threat, visual analytics, detection through visualization, cyber situation awareness**

I. Introduction

With the rapid growth of the Internet, network infrastructures need to keep pace and develop their cyber security awareness through the use of different Intrusion Detection (IDS) and Prevention Systems (IPS). These systems often are dependent on signature-based detection and the availability of signatures generated from previously detected attacks, but are lacking in their capability of detecting previously unknown threats. A major push has been made to develop new detection mechanisms to enhance cyber situation awareness, more precisely detection based on anomaly and behavior-based analysis.

One difficulty often encountered with the detection of anomalous behavior is the lack of support for highlighting what we can consider outlier behavior. It is in fact quite difficult to focus on specific data as the information an analyst has to sift through every day becomes larger and larger as network infrastructures grow. The vital task of network analysis gets bogged down by having to manually parse thousands, if not millions, of lines from log files, compare and fuse information from different sources and decide if a given activity is due to a network attack or network failure. There have been many proponents of the use of visualizations for anomaly detection [1] and its use for the enhancement of situation awareness [2]. Visual Analytics has great value for strengthening cyber security and gathering vital intelligence [3] and we intend to go deeper in possible applications of Visual Analytics for the modeling, visualizing and identifying new sophisticated attacks, which can flawlessly mimic normal network flows and human behavior. In this paper we will briefly go over what Visual Analytics is, the governing concepts and methodologies. Afterwards we will discuss how Visual Analytics can be used to enhance the human-machine interaction in the MASFAD framework and provide powerful APT detection capabilities.

II. Visual Analytics

There have been many attempts to give a proper definition to what Visual Analytics is, the one most precise is provided by researchers from the European Union Coordination Action, in their book [4] they define VA as"the medium of a semi-automated analytical process, where humans and machines cooperate using their respective, distinct capabilities for the most effective results". VA combines work in various fields of research as described in [5]. As shown in "Fig. 1", VA touches upon many different fields of research spanning from Visualization and interaction science to analytical reasoning. The goal of Visual Analytics is to tackle problems which size, complexity and the dependence of human-machine interaction makes them difficult to handle by normal means.

In recent years, one major issue has been prevalent in data analysis- the sheer data that is generated on a daily basis by

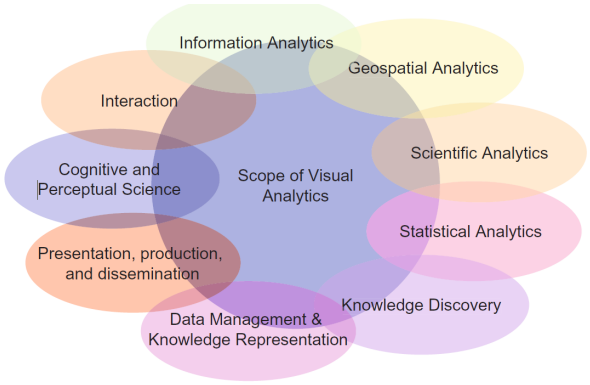

Fig. 1. Fields related to Visual Analytics

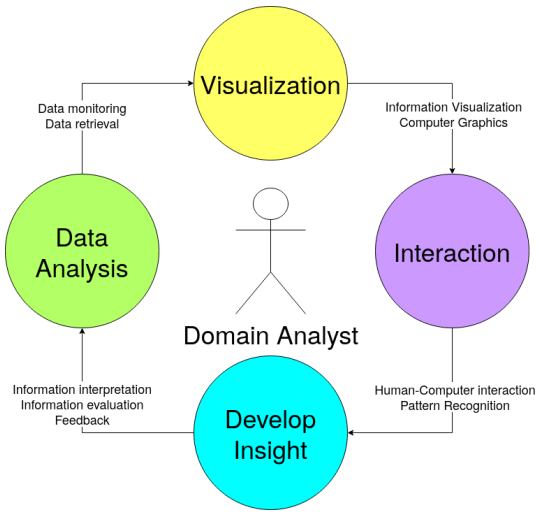

Fig. 2. Representation of the Visual Analytics loop

network systems. Domain analysts are often submerged by the generated alerts and that presents a clear challenge in how this information can be stored and presented to them [5], [6]. The high quantity of data demands new ways of parsing it and presenting it in a clear and understandable way. Regrettably, more often than not current available tools will focus on a time-slice of data or on a limited amount of logs, which can lead to any vital or pertinent information being overlooked. Much effort has been dedicated to defining a good framework for the representation of log files [1], [7], greatly helping analysts to identify possible problematic or abnormal behavior in the network.

More recently, tools such as Kibana [8] and Grafana [9] have been integrated into Security information and event management (SIEM) environments, offering variety of interfaces to the users. They offer great flexibility and cross-reference between different types of data. This shows that the use of Visual Analytics greatly enhances the Cyber Situation Awareness (CSA) of a domain analyst, offering a strong interaction loop, greatly aiding the three stages in Endsley's situation awareness model, namely: perception, comprehension and projection [10]. The Visual Analytics loop and how it relates to CSA is shown in "Fig. 2". Through the offered 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. 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.

A. Visualization

Since the early days of humanity we have conveyed information through the use of images. Since prehistoric times, pictograms and drawings have been used to enhance our cognitive abilities. Through the use of visual aids, humans have been able to identify, comprehend, analyze and operate in their surroundings. From maps to scientific figures, the most important aspect of data visualization is a crucial aspect of transforming complex information into a easily digestible format. This can be accomplished through correctly selecting the appropriate graphical representation for the task at hand. To represent the needed information, we have a choice between a vast collection of representations such as points, lines, shapes, colors, etc. Certain visualizations are better at conveying specific information than others and we have to rely on the study of human perception and cognition [11], [12].

In the context of Cyber Situation Awareness, the non-visual network data is a prime candidate to be transformed using visualizations, offering greater capabilities for navigation, interpretation, analysis and comprehension of large volumes of data [2]. Depending on the task at hand, the visualization can be static, for example displaying a specific attribute of the data, or dynamic, as is the case of temporal data. In most cases, our goal is to reinforce the rapid identification of targets of interest, reinforcing the "pre-attentive processing" as described by Healey [12]. The pre-attentive processing offers identification on large multi-element displays in less than 200 to 250 milliseconds. This aids 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 idea is shown in "Fig. 3", using basic techniques to quickly make a specific element stand out from its surrounding elements, or as Healey defines them, "distractor objects".

The examples shown in "Fig. 3" are only a subset of possible techniques, which aid the pre-attentive processing of visual information. Other examples would be the intensity,contrast or taking advantage of the nature of digital representations, such as exploring the characteristics of the elements in a 3D environment. The aforementioned techniques can be used

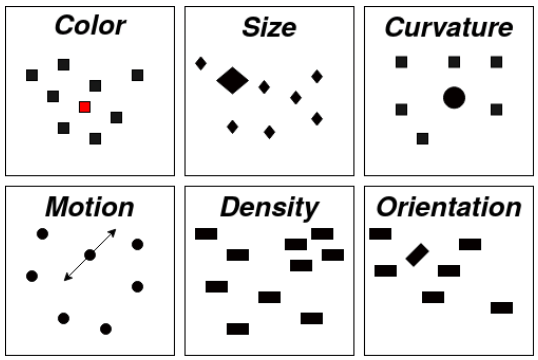

Fig. 3. Examples of pre-attentive visualizations

independently or in combinations to reinforce the perception and comprehension phases of the CSA. When discussing perception and comprehension, it is imperative to mention the capacity of humans to extract patterns from chaotic displays. This is largely explained by the Gestalt principles of perceptual organisation [13], [14], which govern how we interpret the complex inputs we receive. The six major elements of the Gestalt principles describe how we group a collection of small objects to form a larger one.

- Principle of Similarity states that similar objects are perceived as grouped together. This can be enhanced through the use of color, size, curvature or orientation.
- Principle of Simplicity defines how our brain tends to transform ambiguous or complex objects into something easier and simpler to comprehend.
- Principle Proximity states that objects, which are viewed as closer together, seem to have a greater relation than those which are far apart. This can be aided through the use of density techniques and playing with positioning in 3D space.
- Principle of Continuity explains how elements positioned in a straight or curved line seem to be more related to each other than those positioned randomly.
- Principle of Closure will group simple objects together to form a whole complex object, as our brains will fill in any missing information or gaps to create a meaningful image.
- Principle of Common Region states that elements, which have been positioned in the same enclosed area, are regarded as part of the same group, even if spatially they are far apart.

Through the use of pre-attentive techniques and adhering to the Gestalt principles, we can better understand human perception and design complex visualizations for the purpose of information extraction and pattern recognition. The principles of visualization described above are applied in our detection framework through the generation of figures by the detection agents. Each agent is responsible for identifying and analyzing a specific characteristics of cyber threats. By integrating the methodology of "pre-attentive processing" and the Gestalt principles, it enhances the perception of domain experts. How the methodologies are applied is explained in further detail in Section III-C.

B. Interaction

When we are talking about visualizations to aid Situation Awareness, and more precisely in the domain of Cyber Situation Awareness, it is imperative to mention one major issue that analysts encounter- the sheer volume of information generated on a daily basis. To be able to correctly explore and analyze available data, users need powerful and easy to use tools, which offer the possibility to navigate and explore the generated information with ease. This is a vital aspect of human-computer interaction and a basis of Visual Analytics- through the use of interactive visualizations offer the possibility to users to explore the data on multiple levels, form opinions about what they encounter, gain insight and expand their knowledge about the state of the environment. Heer and Schneiderman [15] offer a succinct explanation on what is expected of interactive visualizations: "To be most effective, visual analytics tools must support the fluent and flexible use of visualizations at rates resonant with the pace of human thought". Following this definition will enhance the capabilities of the users to explore and understand the data, while at the same time be able to form a hypothesis about what they are viewing. A taxonomy of interactive dynamics has been composed, shown in Table I showcasing the critical tasks that must be undertaken to enable an iterative visual analysis [15].

C. Interface Design Approaches

To facilitate the use of visualization tools through Visual Analytics, we need to determine how the human-machine interface will be implemented. As described in [2], there are different approaches to developing the interface, depending on the needs we want to address:

- user centered (task oriented) approaches
- system based approaches

The two approaches differ fundamentally in the way they provide CSA, as the user centered approach focuses on the user role and their needs, while the system based approach is centered around representing the complex relationships in a given system, aiming to display them in a clear and intuitive manner [2].

1) User Centered approach: Putting the user in the center of our visualization means we will opt for an interface that focuses on the needs and knowledge of the user. Depending on the specific task the user needs to accomplish, we will present a highly specialized visualization and the data that supports their needs. The Workforce Framework for Cybersecurity (NICE framework) [16] is a good example on how we can evaluate what is needed for a specific type of user role we are designing an interface for. The NICE framework is composed of two building blocks- the skills and knowledge the user has, and the tasks which the user need to accomplish in the scope of their work. As an example, at surface level the job of a Cyber Defense Analyst might seem similar to that of a

TABLE I
TAXONOMY OF INTERACTIVE DYNAMICS FOR VISUAL ANALYSIS

Data & view specification	**Visualize** data by choosing visual encodings
	Filter out data to focus on relevant items
	Sort items to expose patterns
	Derive values or models from source data
View Manipulation	**Select** items to highlight, filter, or manipulate them
	Navigate to examine high-level patterns and low-level details
	Coordinate views for linked, multidimensional exploration
	Organize multiple windows and workspaces
Process and Provenance	**Record** analysis histories for revisitation, review, and sharing
	Annotate patterns to document findings
	Share views and annotations to enable collaboration
	Guide users through analysis tasks or stories

Forensic Analyst, but their knowledge and tasks differ greatly. The Cyber Defense Analyst needs a global view of the environment, collecting information from a variety of sources (e.g., IDS alerts, proxy logs, SNORT network logs) and analyzing them to detect abnormal or possibly malicious activities. The Forensic Analyst on the other hand is focused on a specific subset of the data, be that end-point images or others, to specifically detect vulnerabilities and gain information in support of mitigating the aforementioned vulnerabilities. Thus, the two roles demand a different selection of data and have different tasks to accomplish, meaning different ways of visualizing the state of the environment or the needed data need to be designed.

2) System based approach: Contrary to the User Centered approach, the System based approach focuses on the best way to visualize and interpret the complex structure of systems and how they operate. By providing the users with the means to better understand how a complex system works, they have greater capabilities to address any incidents and identify their cause. By modeling the system structure, the users can gain in-depth knowledge on how it works in normal circumstances as well as unexpected ones.

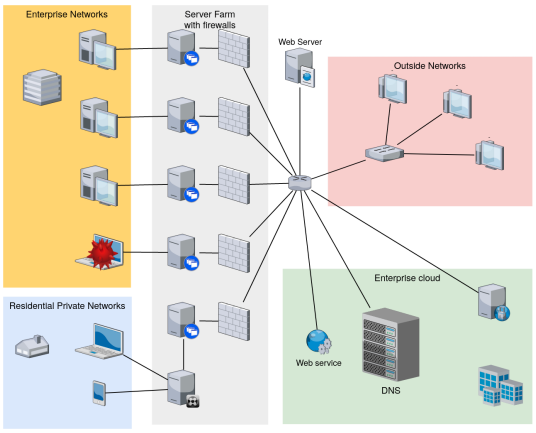

Fig. 4. System based Interface Design example

An example of a System based Interface is shown in "Fig. 4" showcasing the network topology of a fictional corporation. The user can review the relationships between the different end-points in the network and how they are interconnected. These types of visualizations give a good overview of the system and aid into the rapid response to possible issues or attacks when they arise. In the provided example, a client machine, covered in a red symbol, has been flagged as infected and the user can decide how to manage and mitigate the threat to stop its propagation through the network and minimize its impact. This type of interface provides great insight into how a complex system works, but lacks capabilities in providing information about the reason of the issue or what exactly is happening on the client's machine. To accomplish those specific tasks, a User Centered interface is needed.

III. DETECTION OF ADVANCED PERSISTENT THREATS

Currently the majority of the off-the-shelf detection tools offer a high performance signature-based detection. Such IDS or IPS tools rely on the generation of Indicators of Compromise (IoC), gathered from previously detected threats. In the current cyber warfare landscape, this offers some protection, but adversaries have become more proficient in hiding their activity through the use of advanced techniques to rapidly change the behavior of their malware. There have been advances in counteracting emerging threats through sharing of information in the form of Cyber Threat Intelligence (CTI) with tools such as MISP [17]. Malicious actors have an advantage in this regard, as the majority of detection systems are freely available to purchase, study and develop ways of circumventing them. Research in the field has shown that current signature-based detection has trouble detecting threats that use zero-day vulnerabilities or polymorphic techniques [18], [19]. The question then remains, how do we detect adversaries who use unique Tactics, Techniques and Procedures (TTPs)?

A. The MASFAD framework

The Multi-agent System for Advanced Persistent Threat Detection (MASFAD) [20], [21] offers a possible solution 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.

There has been much work in the field of malware detection on finding ways to detect threats based on their characteristics,

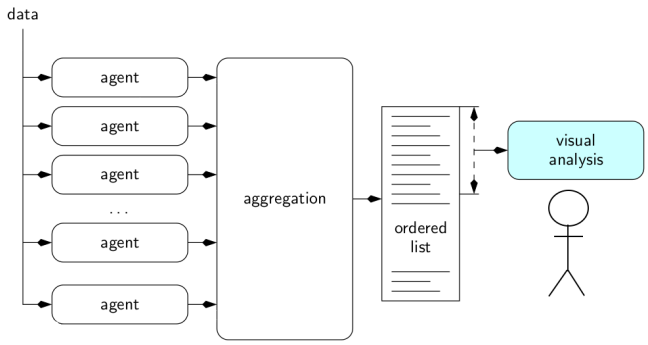

Fig. 5. MASFAD architecture

for example by analyzing malware characteristics extracted from network traffic [22]. The MASFAD framework follows the same approach, by identifying 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. These agents can work independently or be chained together. This is accomplished through the use of the Activation Cascade, based on the principle of the ”detection cascade”. The principal is shown in “Fig. 5”. 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.

The detection of APTs through specific algorithms that analyze malware characteristics is only one aspect of the MASFAD framework. As the analyst’s domain knowledge and expertise is of high importance for the correct identification and mitigation of attacks, the MASFAD framework needs to provide the needed tools for visual analysis, enforcing the ”detection through visualization” [23].

B. Pattern recognition through behaviour-based analysis

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. By applying signature-based detection, a system is sure to provide a low amount of false positives, but its reactive nature is not well suited for the detection of new attacks. Contrary to that, anomaly based detection offers high detection of previously unknown attacks, but the disadvantage is the generation of a high quantity of false alarms. The combination of the two helps drastically in managing the amount of false detections and still offer capabilities of detecting unknown APTs. 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. There is no clear-cut solution to achieving this goal, as discussed in previous chapters the usefulness of any visual representation is highly dependent on human cognition and interpretation.

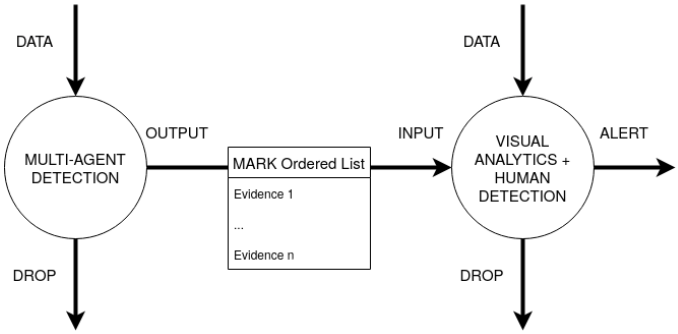

Fig. 6. MASFAD detection cascade

As mentioned previously, 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, the initial 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 in detail specific instances of potentially dangerous behavior inside the network, through a combination of the evidence produced by the system, the raw data logs and the visualizations provided to them. This is illustrated in “Fig. 6”. The analysis by the domain expert is purely based on anomaly- and behavior-based analysis, based on the domain knowledge of the operator.

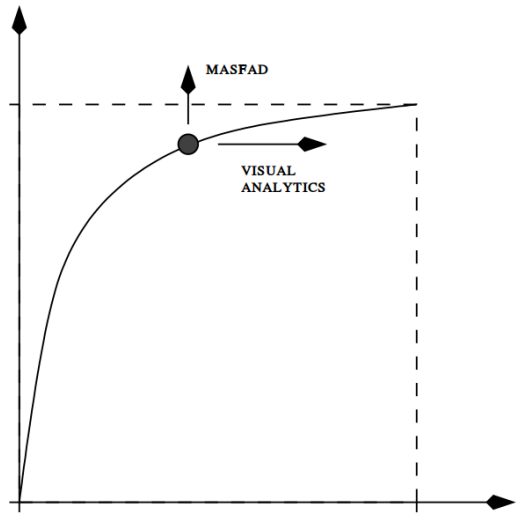

Fig. 7. MASFAD receiver operating characteristics curve

The detection capabilities of systems such as MASFAD, are often measured by the construction of a "Receiver operating characteristic" (ROC) curve, as shown in "Fig. 7". The y-axis represents the positive detection (Pd) observed in the system and the x-axis the false positive detection (Pfa). The ultimate goal is to have a curve which climbs fast and reaches as close as possible to 1 in Pd, while offering a manageable amount of Pfa. In "Fig. 7" 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. The multi-agent analysis and its result have been previously discussed and presented in [20], in the next sections we will address the Visual Analytics part of the framework.

Finally, we should also mention the possibility to include Cyber Threat Intelligence (CTI) to further the attack pattern detection. Each detection agent generates a report of its analysis, consisting of the parameters used for the detection and the relevant raw data. There are multitude of online sources, which can be used to compare the findings with and decide if they constitute a malicious attack or not. Frameworks such as MISP [17] offer a centralized tool for accessing multiple different feeds in an easy manner. Integrating CTI information into MASFAD will further our goal of displaying a comprehensive overview of the state of the environment, enhancing the comprehension stage of the Cyber Situation Awareness and enhancing the ability of the domain expert to correctly decide future courses of action.

C. Visual Analytics in the MASFAD framework

The MASFAD framework is a specialized tool, focusing predominantly on the detection of previously undetected or unknown threats. This is the case with the visualization offered by it too. We don't intend to compete with powerful visualization solutions such as Kibana [8] or Grafana [9], instead offering a specialized interface for the detection of APTs. As shown in II-C, this can be achieved through the use of User Centered approach, designing the interface around the requirements of the user and the tasks that need to be accomplished. Examples of related work in the field are the SIOON framework [24] and the Multi-step cyber Attack Detection (MAD) tool [25]. Both offer powerful visual representation of the network and specific information representations, combining system based and user based approaches to benefit the analysts with greater insight in what is currently happening in the environment. Compared to them, the MASFAD framework focuses more on the data collected by various sensors throughout the network and less on the network topology as is. We don't intend to replace existing tools for network topology mapping, instead placing the domain expert center stage and enhancing their domain knowledge with the proposed visualizations. Indeed, the analyst is the focal point of the MASFAD framework. Through the use of the different visualization principles described in II-A, high degree of interactivity as descibed in II-B and a strong user-centered approach, we aim to leverage

Fig. 8. MASFAD visualizations

the knowledge of domain experts by helping them quickly assimilate and understand the presented information, leading to correct assumptions about the activity in the network.

As shown in "Fig. 8", the MASFAD framework offers multiple different dedicated visualizations, each providing a different representation on a specific type of data.

- **Agent representation** - The Activation cascade shows what data is ingested by the framework, how the various detection agents are interconnected throughout the detection cascade and what evidence they produce.
- **Ranked List representation** - visualizing the evidence produced by the agents in a clear and understandable manner is very important. As described in II-A, we aim to use the pre-attentive processing of humans to single out information of importance.
- **Evidence representation** - alongside the reports generated by the various detection agents, figures specific for the agents are also produced. Be that geo-spacial information or frequency spectrum, 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.

A major requirement of visualization tools is to provide a unified overview of different types of information. This facilitates the correlation of information and enhances the perception of the user to the state of the environment. This is often done through the use of a dashboard- a visual interface, which combines different representations into a unified visualization. The MASFAD framework offers a dashboard as shown in "Fig. 9". As stated earlier, the goal of our interface is not to offer a large variety of visualizations, but instead

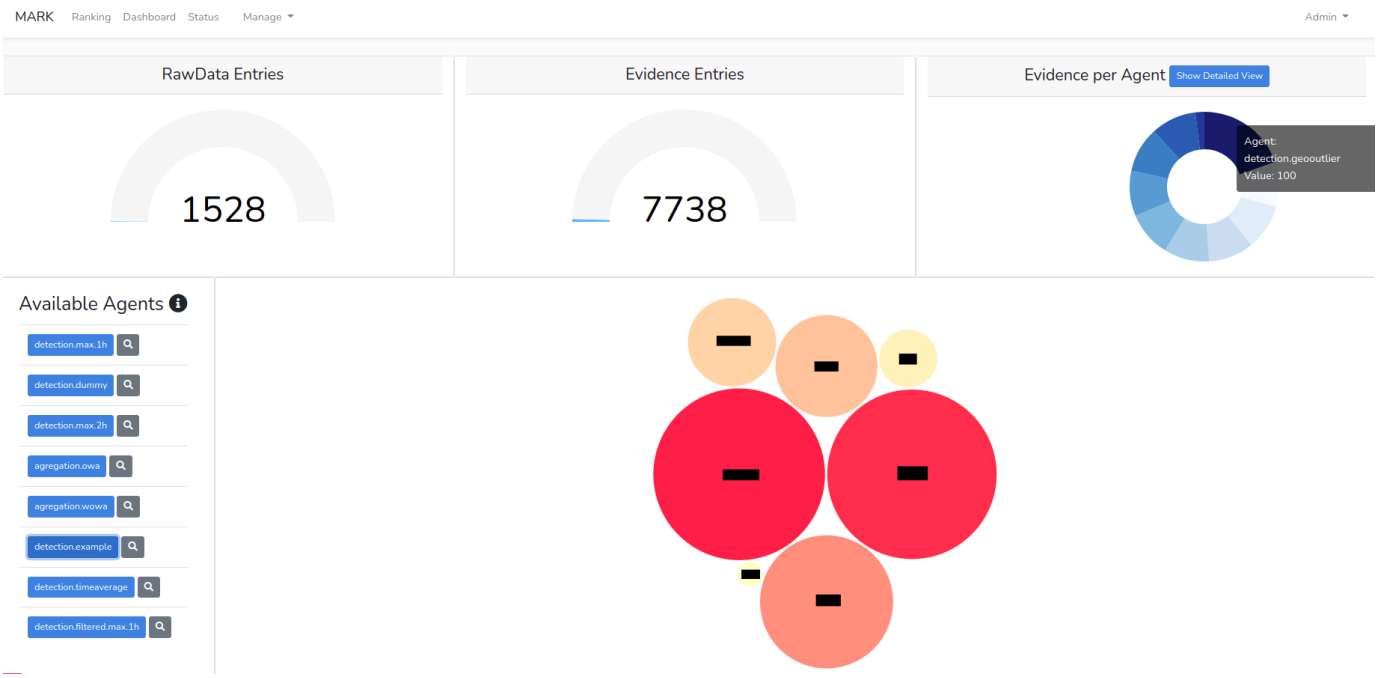

Fig. 9. MASFAD dashboard

have a reduced amount of specialized representations, each enhancing the ability of the domain expert to gain deeper insight in what has been detected. The MASFAD dashboard shows information in relation to the amount of data ingested by the framework, the amount of evidence produced and various representations on the state of the detection agents.

In the context of the evidence produced by detection agents, we are working with tabular data, data recorded as a series of events [1]. There are multiple ways to display such information, be that as single event based or group based visualization. When we want to show the single event based representation, one possibility is to use a heatmap, as shown in "Fig. 10". This type of visualization offers a good overview of the generated evidence and can be used for comparison. The vertical axis represents the different subjects of analysis, be that connections between internal and external machines or other, while the horizontal axis represents the different agents that were triggered. This greatly enhances the ability of an analyst to understand why was a specific score produced by the aggregation as by simply going over specific subject row, we can observe how the various detection agents analysed it and how that determines the aggregation score.

If we instead want to review the evidence in a grouped manner, the bubble graph shown in "Fig. 9" can be used. Each bubble represents one evidence generated by the aggregation and it can be enhanced further through the use of "circle packing", a technique for representing nested data [26]. This is why we can show not only the evidence produced, but also directly group together all evidence used during the aggregation. Multiple pre-attentive methods and representations based on the Gestalt principles are used, as explained in II-A, to help

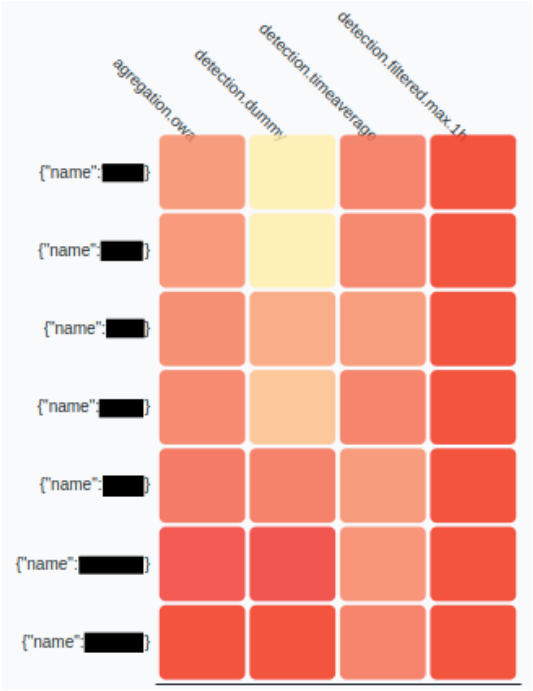

Fig. 10. Detection agent heatmap visualization

the domain analyst comprehend the information. Colors, sizes and positioning are used to draw the attention to what can be considered as the evidence of importance. Furthermore, by offering the possibility to the analyst to explore further each element of the bubble chart, we also adhere to the principles of Interaction, described in II-B.

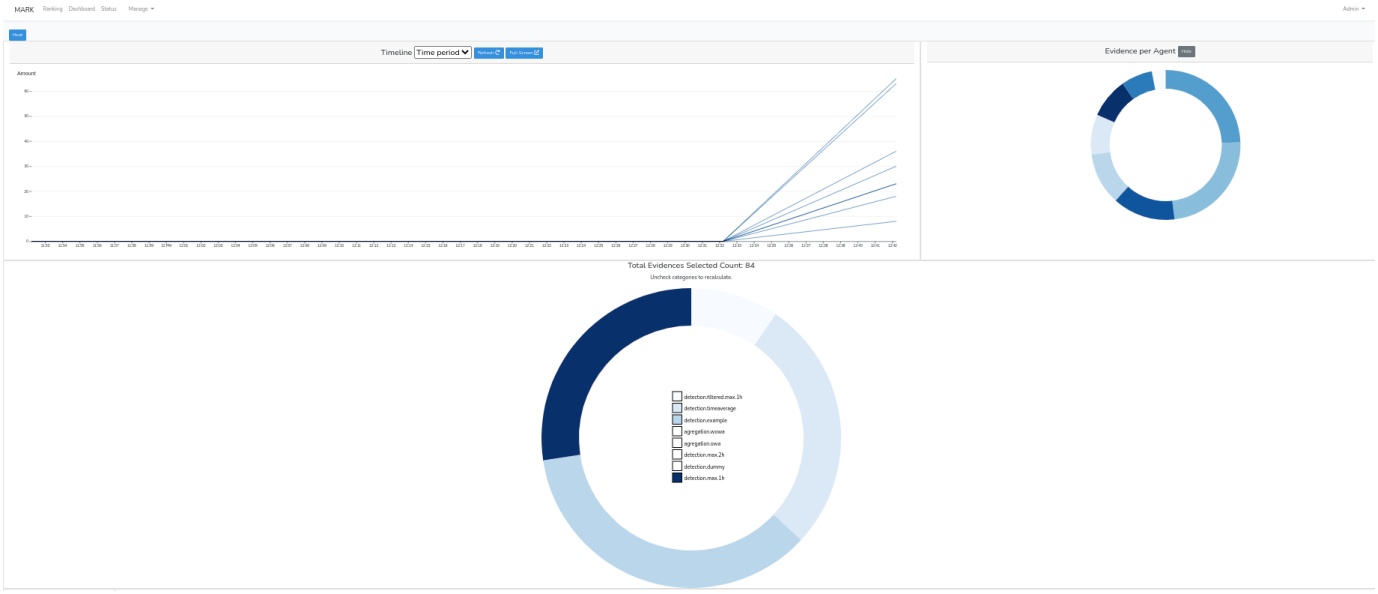

Fig. 11. Detection agent dynamic timeline and donut chart

Another aspect of importance of the data generated in any network is its temporal characteristic [1]. Information is generated constantly and there should be a way to visualize how the data and evidence produced evolve with time. As shown in "Fig. 11", we can visualize the activity of the various detection agents in a temporal fashion through the use of a dynamic timeline. The visualization can be adapted to show information for different time-spans and each line in the timeline can be queried to show how much evidence was generated for the specific agent. This representation will be useful when the user wants to infer abnormal spikes of activity from the agents, signifying the possible detection of suspicious activity. The eye will be directly drawn to these spikes of activity, compared to periods of inactivity from the agents. Alongside that, a detailed view of the evidence generated per agent is shown through the use of a donut chart. Both these representations are also interactive, as discussed in II-B, providing the user with ways to filter, compare and dig deeper in the information provided.

IV. Evaluation of the MASFAD visualization

Evaluating a visualization is no easy task, it is highly dependent on the methodology chosen by the evaluator and how the evaluation is structured. More often than not, we talk about the evaluation of the Situation Awareness, in regards to evaluating a specific interface. That means deciding how well the visualization helps the user during the perception, comprehension and projection phases of SA. There are two major methodologies in the evaluation of SA- the Situation Awareness Global Assessment Technique (SAGAT) [27] and the [28]. Both of these techniques have been previously compared and their benefits and drawbacks discussed by Endsley [29]. Originally both techniques were developed to test the interfaces designed for air crafts, but have been widely used for Cyber Situation Awareness, as the principles remain the same. In this chapter we will quickly explain the major differences between the two methods, which one suits the evaluation of the MASFAD visualization better and how we propose to perform the evaluation.

A. SAGAT

The SAGAT methodology is considered an objective technique for evaluating the SA of a user, in regards to their capabilities of perceiving, comprehending and analyzing information. An initial scenario is developed and used to create a simulation of a specific event. To correctly evaluate the CSA during this scenario, questionnaires are composed for specific moments in the scenario, pertaining to the state of the environment. The simulation is frozen at random instances and the operator is queried based on the questionnaires, evaluating their level of CSA. Each answer to a query is attributed a score, reflecting whether or not the user correctly assessed the current state of the environment. This means that SAGAT offers an objective and impartial assessment of the operator's SA through elements of all three levels. Disadvantages of the technique are that the user can't prepare for the queries and must rely on memory (as the displays are usually blanked during the freezes). However with experimentation, it has been proven that the users can correctly able to report their assessment if the freezes are in a manageable time, usually 5 to 6 minutes [29]. Another issue with SAGAT is the prepartion the scenarios and simulations can take a lot of effort and needs a sizable investment in time.

B. SART

Contrary to SAGAT, SART is a purely subjective technique for the evaluation of SA. The operators are asked to assess on a bipolar scale the demand on their abilities, supply of

resources provided to them and their understanding of the situation during a simulation. These three aspects are scored and then assembled to reflect their SA. As the queries are purely user oriented, this gives great flexibility to deploy SART in any given circumstance without much customization. However, the disadvantage of SART is non-negligible. The user centered approach leads to possible incorrect scoring by the participants as they may have difficulty assessing correctly their own situational awareness and confounding how well they are doing and their actual level of SA.

C. Evaluation Set-up

To evaluate the MASFAD visualization we opt for using SAGAT. The benefits of gathering an objective scoring of the SA gained from the interface outweigh the drawback of the laborious set-up. This technique has been proven highly appropriate for application in the cyber security domain [30]. We will prepare a scenario simulating typical network activity using the GHOSTS NPC framework [31] developed by researchers at Carnegie Mellon University. This framework is very powerful as it offers great customization of the different clients, each having their own behavior governed by a timeline configuration file. The cluster of clients will be regulated by the GHOSTS server, responsible for managing the clients and pushing updates to the timelines if needed. This will provide us with a good dataset of background traffic for the simulation. To mimic a sophisticated attack, we will use the Sly orchestration tool [32], developed by our research unit. This tool will be responsible for preparing the attack scenario and initiating the attack. Further, a suite of tools will be available for use by the operators, such as SNORT [33], Wireshark [34] and of course the MASFAD framework. Other tools will be integrated in the scenario during the preparation. An overview of the simulation set-up is shown in "Fig. 12". The simulation will be deployed in our Cyber Range, as it is a prime candidate for training and evaluating CSA [35].

The goals of this evaluation are two-fold:

- Evaluate the CSA gained from MASFAD
- Evaluate how the MASFAD framework works alongside established detection tools

The MASFAD framework is specialized in the detection of APTs, that means that deploying it as a stand-alone tool is possible but not optimal. To truly test the usefulness and the added value of the MASFAD visualization, it needs to be run in parallel with other tools. This way we can evaluate the performance of our framework when it is deployed in a Security Operations Center (SOC) environment. The questionnaires will be prepared to query specific stages of the APT life cycle such as, but not limited to, Initial Access, Reconnaissance/Beaconing, Establishing a Command & Control channel and Exfiltration.

V. Future Work

In this paper we have presented the currently accomplished work on the MASFAD framework and our intentions for the future. Currently the visualization aspect of the framework is

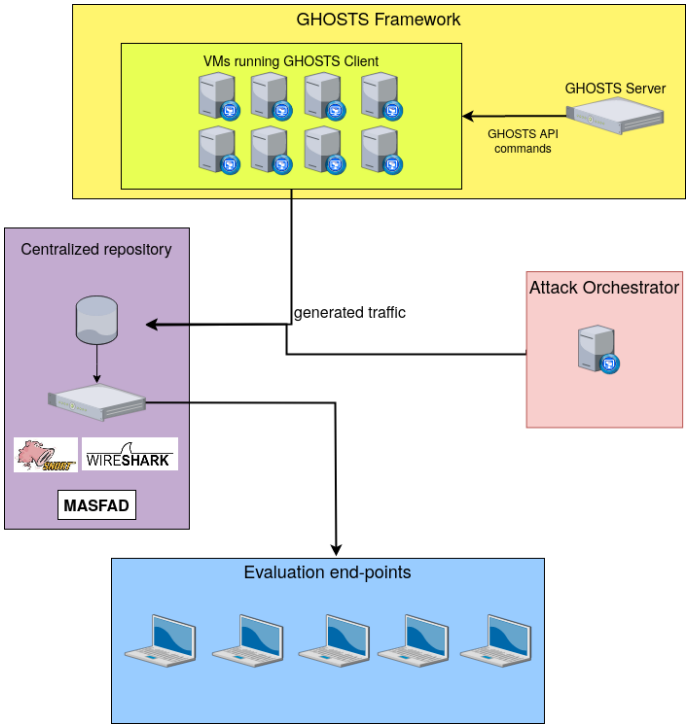

Fig. 12. Evaluation infrastructure

in its infancy, but we aim to develop it further by applying the principles of Visual Analytics discussed in II. The dashboard interface will be further developed and new visualizations will be integrated to facilitate the detection of APTs through behavior-based pattern recognition. Some examples of possible visualizations were already presented in this paper and new ones will be researched and developed to enhance its capabilities.

Multiple evaluation scenarios will be prepared, using variety of TTPs, through the use of the Sly orchestrator and the GHOSTS NPC framework. This will help to test the detection and visualization capacity of the framework. There has been work in creating APT datasets, but currently there is a certain lack of specific datasets to help the evaluation of cyber situation awareness [36]. We hope that by generating our own simulations, we will be able to propose new datasets, which can be used to correctly evaluate CSA during the detection and analysis of sophisticated APT attacks.

VI. Conclusion

The difficulties inherent to designing a visual solution for APT detection are not trivial. The field of Visual Analytics is ever expanding and new technologies have made it change radically in the last couple of years. As always, the human-computer interaction takes center stage and the paradigms governing the implementation of powerful visual interfaces are ever so important. In this paper we discussed the major aspects of Visual Analytics and what is needed to correctly design visualizations which enhance the cyber situation awareness of the user. We also presented our solution, the Multi-agent

System for Advanced Persistent Threat Detection, and how it can be used by domain analysts to enhance the different phases of CSA. The initial evaluation of the detection capabilities of the framework, found in [20], yielded great results, but there is still much work to be done to enhance the visualization side of APT detection. Multiple solutions have been discussed and an evaluation plan has been presented. Currently there is a lack of dedicated tools for the identification and detection of previously undiscovered and highly complex advanced threats and we are certain that the MASFAD framework can greatly aid in this aspect and further bolster detection capabilities through the incorporation of Visual Analytics techniques.

REFERENCES

[1] T. Zhang, X. Wang, Z. Li, F. Guo, Y. Ma, and W. Chen, "A survey of network anomaly visualization," *Science China Information Sciences*, vol. 60, pp. 1–17, 2017.

[2] M. Varga, C. Winkelholz, and S. Träber-Burdin, "Cyber situation awareness," *NATO/OTAN (STO-MP-IST-148)*, 2016.

[3] V. Lavigne and D. Gouin, "Visual analytics for cyber security and intelligence," *The Journal of Defense Modeling and Simulation*, vol. 11, no. 2, pp. 175–199, 2014.

[4] D. Keim, J. Kohlhammer, G. Ellis, and F. Mansmann, *Mastering the information age solving problems with visual analytics*. Eurographics Association, 2010.

[5] D. Keim, G. Andrienko, J.-D. Fekete, C. Gorg, J. Kohlhammer, and G. Melançon, "Visual analytics: Definition, process, and challenges," *Lecture notes in computer science*, vol. 4950, pp. 154–176, 2008.

[6] A. A. Cardenas, P. K. Manadhata, and S. P. Rajan, "Big data analytics for security," *IEEE Security & Privacy*, vol. 11, no. 6, pp. 74–76, 2013.

[7] J. Lee, J. Jeon, C. Lee, J. Lee, J. Cho, and K. Lee, "A study on efficient log visualization using d3 component against apt: How to visualize security logs efficiently?" in *2016 International Conference on Platform Technology and Service (PlatCon)*. IEEE, 2016, pp. 1–6.

[8] "Your window into the elastic stack," https://www.elastic.co/kibana/, accessed: 2023-02-05.

[9] "Grafana website," https://grafana.com/, accessed: 2023-02-05.

[10] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," in *Situational awareness*. Routledge, 2017, pp. 9–42.

[11] C. Ware, *Information visualization: perception for design*. Morgan Kaufmann, 2019.

[12] C. G. Healey *et al.*, "Perception in visualization," *Retrieved February*, vol. 10, p. 2008, 2007.

[13] K. Koffka, *Principles of Gestalt psychology*. Routledge, 2013.

[14] W. D. Ellis, *A source book of Gestalt psychology*. Routledge, 2013.

[15] J. Heer and B. Shneiderman, "Interactive dynamics for visual analysis," *Communications of the ACM*, vol. 55, no. 4, pp. 45–54, 2012.

[16] R. Petersen, D. Santos, K. Wetzel, M. Smith, and G. Witte, "Workforce framework for cybersecurity (nice framework)," 2020.

[17] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "Misp: The design and implementation of a collaborative threat intelligence sharing platform," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, 2016, pp. 49–56.

[18] A. Souri and R. Hosseini, "A state-of-the-art survey of malware detection approaches using data mining techniques," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, pp. 1–22, 2018.

[19] Ö. A. Aslan and R. Samet, "A comprehensive review on malware detection approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020.

[20] G. Nikolov, T. Debatty, and W. Mees, "Evaluation of a multi-agent anomaly-based advanced persistent threat detection framework," in *The Twelfth International Conference on Evolving Internet (INTERNET 2020)*, 2020. [Online]. Available: https://cylab.be/publications/22/2020-evaluation-of-a-multi-agent-anomaly-based-advanced-persistent-threat-detection-framework

[21] ——, "Evaluation through deployment of the multi-agent system for advanced persistent threat detection framework in a cyber range environment," in *Digital Transformation, Cybersecurity, And Resilience DIGILIENCE 2022*, 2022. [Online]. Available: https://cylab.be/publications/44/2022-evaluation-through-deployment-of-the-multi-agent-system-for-advanced-persistent-threat-detection-framework-in-a-cyber-range-environment

[22] K. Li, R. Chen, L. Gu, C. Liu, and J. Yin, "A method based on statistical characteristics for detection malware requests in network traffic," in *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*. IEEE, 2018, pp. 527–532.

[23] R. F. Erbacher, "Intrusion behavior detection through visualization," in *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme-System Security and Assurance (Cat. No. 03CH37483)*, vol. 3. IEEE, 2003, pp. 2507–2513.

[24] X. Fan, C. Li, X. Yuan, X. Dong, and J. Liang, "An interactive visual analytics approach for network anomaly detection through smart labeling," *Journal of Visualization*, vol. 22, pp. 955–971, 2019.

[25] M. Angelini, S. Bonomi, S. Lenti, G. Santucci, and S. Taggi, "Mad: A visual analytics solution for multi-step cyber attacks detection," *Journal of Computer Languages*, vol. 52, pp. 10–24, 2019.

[26] E. Meeks, *D3. js in Action*. Manning Shelter Island, NY, 2015.

[27] M. R. Endsley, "Situation awareness global assessment technique (sagat)," in *Proceedings of the IEEE 1988 national aerospace and electronics conference*. IEEE, 1988, pp. 789–795.

[28] R. M. Taylor, "Situational awareness rating technique (sart): The development of a tool for aircrew systems design," in *Situational awareness*. Routledge, 2017, pp. 111–128.

[29] M. R. Endsley, S. J. Selcon, T. D. Hardiman, and D. G. Croft, "A comparative analysis of sagat and sart for evaluations of situation awareness," in *Proceedings of the human factors and ergonomics society annual meeting*, vol. 42, no. 1. SAGE Publications Sage CA: Los Angeles, CA, 1998, pp. 82–86.

[30] P. Lif, M. Granåsen, and T. Sommestad, "Development and validation of technique to measure cyber situation awareness," in *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, 2017, pp. 1–8.

[31] "Ghosts npc framework," https://github.com/cmu-sei/GHOSTS, accessed: 2023-02-05.

[32] P. de La Vallee, G. Iosifidis, and W. Mees, "Cyber red teaming: overview of sly, an orchestration tool," in *Digital Transformation, Cybersecurity, And Resilience DIGILIENCE 2022*, 2022. [Online]. Available: https://cylab.be/publications/45/2022-cyber-red-teaming-overview-of-sly-an-orchestration-tool

[33] M. Roesch *et al.*, "Snort: Lightweight intrusion detection for networks." in *Lisa*, vol. 99, no. 1, 1999, pp. 229–238.

[34] A. Orebaugh, G. Ramirez, and J. Beale, *Wireshark & Ethereal network protocol analyzer toolkit*. Elsevier, 2006.

[35] T. Debatty and W. Mees, "Building a cyber range for training cyberdefense situation awareness," in *2019 International Conference on Military Communications and Information*, 2019. [Online]. Available: https://cylab.be/publications/2/2019-building-a-cyber-range-for-training-cyberdefense-situation-awareness

[36] B. Stojanović, K. Hofer-Schmitz, and U. Kleb, "Apt datasets and attack modeling for automated detection methods: A review," *Computers & Security*, vol. 92, p. 101734, 2020.