Detection through Visualization for the Multi-Agent System for APT Detection

Georgi Nikolov$^{1[0000-0002-9020-8408]}$, Thibault Debatty$^{1[0000-0003-2373-566X]}$, and Wim Mees$^{1[0000-0002-0696-8093]}$

Royal Military Academy, Avenue de la Renaissance 30, 1000 Brussels, Belgium
contact@cylab.be
https://cylab.be

Abstract. With the evolution of interconnectivity and the World Wide Web, we have become increasingly dependent on it, but also highly susceptible to attacks from malicious actors. Regarding the amount of traffic generated every day, it has become quite complicated to quickly find and identify possible breaches of security in the form of cyber threats and attacks. In recent years there has been a stronger push for better cyber situation awareness. This comes in many forms- threats and vulnerabilities need to be identified, processed and understood in real-time. The emergence of new sophisticated attacks, in the form of Advanced Persistent Threats (APTs) has made this almost impossible, as threats can stay hidden in the network for weeks, before being discovered.

To combat previously unknown attacks, we designed the Multi-Agent System for APT Detection (MASFAD), developed as a means of detecting abnormal and malicious activity inside a network, through the combined analysis of APT characteristics, evidence aggregation and visualization techniques. To augment the cyber operators' situation awareness, we have laid the groundwork through the development of strong detection algorithms, but more work needs to be done in the form of beyond the state-of-the-art visualization techniques.

In this paper we define how the MASFAD network can enhance cyber situation awareness and propose solution to augment it following the "Detection through Visualization" paradigm.

Keywords: cyber situation awareness · APT · detection through visualization · visual analytics

1 Introduction

The rapid expansion and integration of the Internet in every aspect of our lives has caused the cyber threats we encountered of old to evolve alongside it. With the substantial amount of traffic generated every day, it has become quite complicated to quickly find and identify possible security breaches in the form of cyber threats and attacks. New sophisticated attacks have become an ever-increasing fear for private, government and military information management environments. These attacks can flawlessly mimic normal network flows and human behaviour, ultimately causing enormous infrastructural damage. In this context, a high degree of cyber situation awareness is vital to combat these emergent threats by aiding the informed decision making when managing one's infrastructure [17, 31].

To combat advanced targeted threats, which might stay hidden for a long period before being discovered, the MASFAD framework [24, 26] was designed and developed, focusing on behavior and anomaly-based analysis, specifically targeting detection of APTs. This is aided through the detection and identification of APT characteristics, analysis of the abnormal behavior to get better understanding on how the attacks work and visualizations to get better insight in how they were detected and further protect against them. Testing the detection performance of the current MASFAD prototype has shown its usefulness, but one major problem persists: how do we visualize the large amount of data that is generated by the detection engine in such a way that a human analyst can process it in the most effective and efficient way possible. Therefore, we aim to propose a powerful, insight-driven visualization tool, named Multi-agent System Visualization (MASVIS), that facilitates the work of cyber analysts, who quickly need to distinguish true detections from false alarms.

In this paper we will present in short the MASFAD framework, followed by our proposal for a visualization module, which can be integrated within the framework to enhance the cyber situation awareness.

2 Cyber Situation Awareness

A lot of effort has been dedicated in the last years on defining specifically what cyber situation awareness is and how it can improve the efforts of cyber defense specialists to secure their networks. The unanimously accepted definition of situation awareness (SA) was defined by Endsley, in particular in dynamic environments [9]:

> "Situation awareness is the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."

The model established by Endsley is widely used in the psychology domain to define how humans can make sense of their surroundings and perceive complex situations. This is highly applicable to the cyber domain, as the never-ending flow of generated data and information creates a highly complex and stressful environment, where domain analysts must keep a constant eye on different sensors to be able to detect suspicious activity. The three essential components of SA, as shown in Fig. 1, are there to define how well a domain analyst can recognise an attack and react to it:

- **Perception -** this involves the capability of humans to monitor, detect cues and basic recognition. This is important in the domain of cyber defense, as domain analysts need to constantly be on guard, surveying the different network elements (events, people, systems, etc.) and their current states.

- **Comprehension -** after the initial stage of perception, it is vital to be able to interpret the perceived information, recognise possible patterns and evaluate it. This gives the domain analyst a better understanding of the meaning of the observed information, how the different elements are linked together and how it relates to the security of the network.
- **Projection -** as the data is gathered and better understood, a clear model of the evolution of the situation can be constructed to better understand its possible future impact.

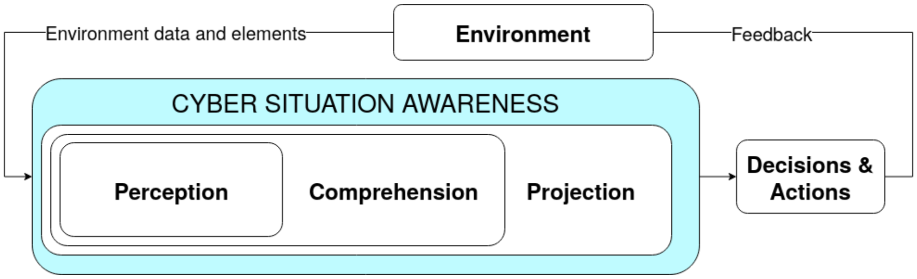


Fig. 1. Cyber situation awareness diagram

The theory behind SA is clear and straightforward, but in reality it is quite difficult to put it into practise. In regards to the cyber defense domain, analysts can quickly become overwhelmed by the significant amounts of alerts and events produced by detection assets in the network, as well as by the systems and applications producing logs and audit trails. For ages, humans have used visual aids to better understand complex situations and this is highly applicable for the cyber domain as well. Through the use of visual representation of the data, a domain analyst can perceive important information and suspicious events at a greater rate, interpret the significance of the findings through possible pattern recognition, and estimate the impact they might have on the system [19].

3 Visual Analytics and Detection Through Visualization

To better process the large quantities of data we can collect, a new way of analyzing it and displaying it in a clear and concise way is needed. There are clear challenges in how the data should be stored and presented for analysis [15, 3]. Through the use of Visual Analytics [30, 4] we can combine the strengths of a human analyst with the speed of the electronic data processing. This leads to the idea of "detection through visualization" [11], which has become a focal point of many new research. Until now, a major part of intrusion detection happens through the analysis of security logs, which are often in text form. Studies have been done [20, 34] on the applicability of currently used techniques for data

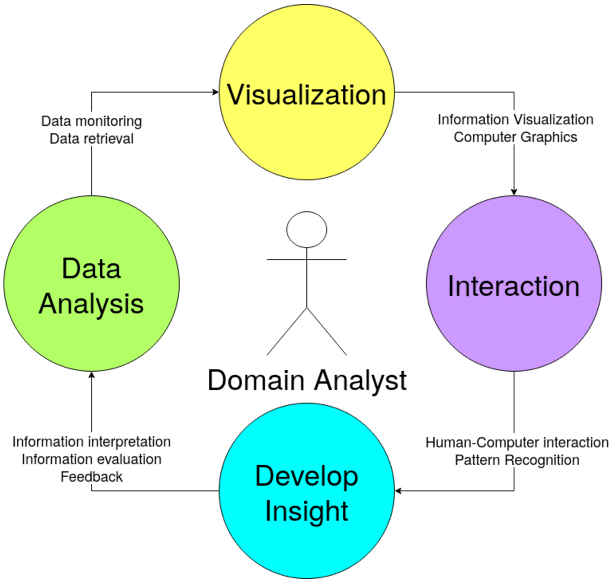


Fig. 2. Representation of the Visual Analytics loop

visualization. What has been concluded is that often the tools available will show only a time-slice of data or only a certain amount of logs, which leads to potentially vital information being overlooked. Tools such as SnortView [16] and ELVIS [14] are very powerful, but sometimes limited in what they can present to the analyst. It is also important to note that these tools are separate from the Intrusion Detection Systems (IDS) solution and bring extra overhead.

In general, the typical application of Visual Analytics follow closely Endsley's model described in Sect. 2. As shown in Fig. 2, the domain analyst needs to first use the available tools to analyse the data and retrieve that, which might be of importance. The retrieved data is then represented using information visualization techniques, typically done through the use of visual structures such as line charts, bar charts, graphs, geo-spatial representations etc. The visual analyst can gain valuable insight through the interaction with these representations, aiding in the detection and recognition of important patterns and evaluation of the data. Afterwards it is up to the analyst if a clear conclusion can be drawn from the analysis or more in-depth look is needed. This human-machine interaction, through the use of visualization, is the major cornerstone of the "Detection through Visualization".

4 The Multi-Agent System for APT Detection

Currently, domain analysts must evolve with the current threat landscape. With new emergent threats, in the form of Advanced Persistent Threats, private and government institutions are not safe against previously unknown attacks, the cyber situation awareness needs to evolve too. This key factor can be aided by the development of new detection tools, which greatly enhance the ability to recognise anomalous behaviour, recognise APT patterns and evaluate their impact on the network.

The nature of APTs is that they evolve constantly and through the use of zero-day vulnerabilities it is difficult to model a system that can defend against all possible known threats. Most research done in the domain of APT detection usually consists of analysis of case studies [32, 21, 25] of famous APTs, the description of their main features and offer best practices in combating them without considering a general framework for APT detection. In recent years, more importance has been put on designing more general frameworks that don't rely on the use of the knowledge-based detection approach, where the system uses a large amount of previously collected information to form opinions on the behavior of possibly malicious code in a system. A solution is to analyze the network traffic [28, 7], focusing on specific behavior or intrusion detection events. There are other techniques such as focusing on feature extraction and normalization [23] or event correlation [12]. The MASFAD framework [24, 26], built upon the Multi-agent Ranking Framework (MARk), already incorporates a big part of these proposed techniques. At the lowest level, we offer simple, but strong tools for detection of specific patterns. Through parameter refinement and easy extension of the detection capabilities, the framework can also serve as a tool for other types of detection, such as the detection of Insider threats and Botnet detection.

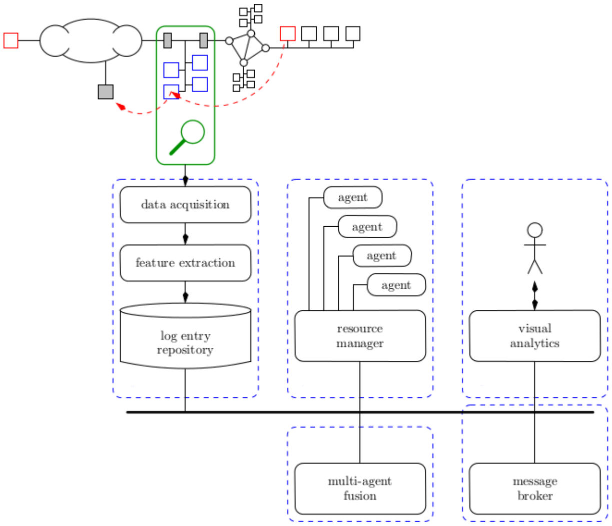


Fig. 3. The MARk Framework overview, representation of the flow of data through the framework

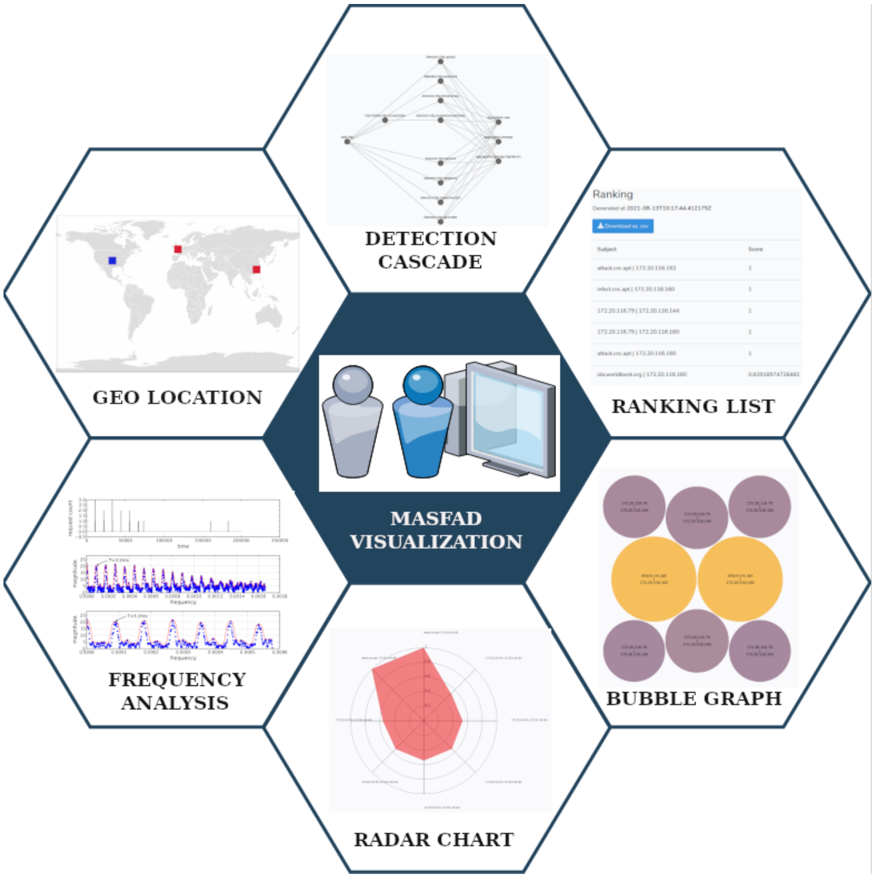
The framework consists of a wide variety of independent agents, each consisting of a specific analysis algorithm. The agents represent a black box, where the raw data serves as input and might generate evidence, depending on the analysis of the data. The evidence will consist of the result of the analysis and a ”suspiciousness” score, to indicate how likely it is that the analysis discovered an APT indicator. The structure of the MASFAD framework is shown in Fig. 3. It consists of multiple modules, which are responsible for the data collection, the detection agent activation and aggregation. The data generated from the various agents is combined and aggregated by the aggregation agents, which follow different methodologies to attribute weights to the evidences and agents, selecting which data and detection algorithm is of higher importance for the detection. The detector agents are linked together through the Activation Cascade, based on the concept of a ”detection cascade”, where the agents and aggregation serve as an initial filter of the data. Finally the aggregation output, in the form of a ranked list, is presented to the domain expert for analysis.

The APT detection is also hindered by the large quantity of data that is produced daily in operational networks. Every day Terabytes of data is collected from system logs, server logs, network IDS logs and other sources. Filtering through all this information is a costly process and the probability of intrusions being overlooked is quite high. A clear strategy is needed when considering the amount of data, how to process it and then visualize it. A good solution for that is presented by CERN [27], where a clear separation is established between the Data ingestion, Data processing, Storage and Visualization and Incident response. This idea is also central for the MASFAD framework, with the extra benefit that the framework is designed to be data agnostic and easily extendable. The framework does not have to know what type of data it is analyzing and new detection agents can be added on the fly to detect specific patterns of behavior.

4.1 Visual Analytics in the MASFAD framework

Most IDS present their findings using a Graphical User Interface for better visualization of the results. This is often accomplished by using powerful aggregation and visualization tools such as the Elasticsearch-Logstash-Kibana (ELK) stack [18, 13] or Grafana [1]. All Cyber Security Operations Centers (CSOC) have a wall of screens available, supervising and visualizing large amounts of different data and events. For this purpose, it is important that the MASFAD framework can also provide a clear and concise User Interface, facilitating the work of a network domain expert to analyze, validate and draw conclusions from the produced evidences. Currently, it is up to the cyber domain analysts to adapt the visualization tools to best serve their needs, using what is available ”out of the box”.

The MASFAD framework has the advantage of offering a complete package of an APT detection solution together with the necessary tools for visualizing the important data, be that logs, network traffic or context information, and the evidences produced by the system. Currently the visualization capabilities are still in development, offering the possibility to review the log data used and the



Ranking

Generated at 2021-08-13T10:17:44.412175Z

Subject	Score
attack.cnc.apt | 172.20.116.162	1
infect.cnc.apt | 172.20.116.160	1
172.20.116.79 | 172.20.116.144	1
172.20.116.79 | 172.20.116.160	1
attack.cnc.apt | 172.20.116.160	1
ida.worldbank.org | 172.20.116.160	0.83918974728482

Fig. 4. MASFAD visualization- examples of detection cascade, evidence ranking list, representations of evidences created, specific evidence analysis such as Frequency analysis and Geo Location

evidences produced. As per Fig. 4, we can see that the MASFAD framework offers multiple different views and specific visualizations, which the domain expert can use. The user is able to review the Activation Cascade- what data sources are feeding the detection agents, how the agents are triggered and linked together and what evidences they produce. Each agent produces a ranked list consisting of a pairing of client-server tuples and the score assigned to them after analysis. There are multiple different ways to visualize this ranked list, be that in text form or in a dynamically generated graphical representation. Alongside that, each agent will generate figures, specifically showing the results of the analysis- be that Frequency or Geographic location analysis.

This is beneficial when the interface wants to draw attention to very specific evidences produced, but there is one key question that needs to be answered- how can we design an interface to move away from showing individual "suspicious" occurrences and instead interconnect the different activity for better pattern and behavior recognition? Currently the aggregation agents are responsible for interpreting the evidences produced by different agents and finding a correlation between those to produce a possible "suspiciousness" score. But ultimately, humans are way more capable of detecting correlation and patterns, a trait which has helped humanity survive and thrive since the beginning of time. This brings us to the "Human Factors" as described by Dr. Varga in [31], designing a user interface is very tightly linked to the human interaction with its purpose. After spending time on gathering user requirements and reviewing design principles and constraints, we came to the following set of objectives the MASFAD framework needs to attain:

1. **Modular user interface -** the MASFAD framework needs to offer a certain level of customization, akin to what Kibana and Grafana offer. The goal is not to compete with those solutions, as the scope of the MASFAD framework is smaller and more focused on detecting specifically APT activity.
2. **Dynamic display generation -** the visualizations need to be dynamic, i.e. it needs to update in real-time, displaying the most relevant and up-to-date information at all times. When analysing complex behaviors, it is vital to have a good overview of changes and evolution inside the network.
3. **Tools aiding pattern recognition -** As stated before, it is of vital importance to aid the domain analyst to discover and recognise patterns of importance in the data. To aid this, new type of visualizations are needed, combining different inputs in a coherent whole and presenting a clear picture of the current situation in the network.
4. **Agent reporting -** The amount of data that is generated can be daunting to analyse and it is quite probable that vital information slips through the cracks. The interface must allow the analyst to quickly filter through the generated output, adapt the agents on-the-fly to suit the detection needs and validate the results. To this end, the agents need to generate a clear and concise report of their findings and the detection parameters used in the analysis.
5. **Input data validation -** There must be a reliable way in place to validate the data, which enters the system, to ensure its reliability and consistency.

Modular user interface As mentioned previously, the "Human Factors" is of vital importance when designing a user interface. Each user has different requirements and priorities about what needs to be displayed and how it should be represented. For example, a network analyst might be more interested in the netflow traffic and the times and number of connections established inside the network, while a forensic specialist will need a good oversight of the process trees, running on a machine, and which Dynamic Linking Libraries (DLLs) or Shared Objects (*.so) are being loaded by the processes. This is a major obstacle, when a unified user interface needs to be designed- it is not trivial to cram all this information in one screen. The solution to this problem is handing the users the power to customize their experience and deciding which tools are most apt for their intended task. Tools such as Kibana and Grafana offer the possibility to choose and match different visualizations, often presenting an interface with high customization options. This comes with its own problems, as a high degree of knowledge is often needed to correctly parameterize the different visualizations. The MASFAD framework visualization tool aims to provide the same capabilities, but reduce the overhead by limiting the scope, as the ultimate goal of the tool is to detect very specific activity inside the network, most notably the presence of a persistent APT in the network and its behavior. This will lead to a more curated list of possible visualizations available to the user, often based on the different APT characteristics analysed by the detection agents.

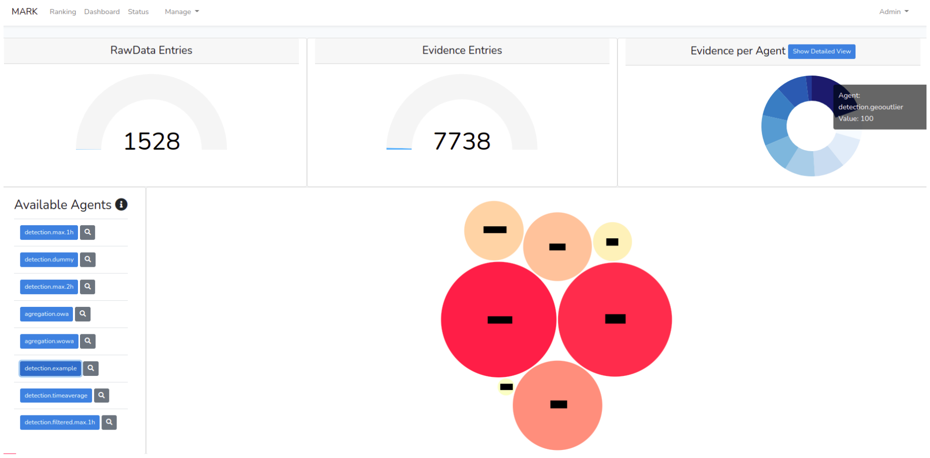
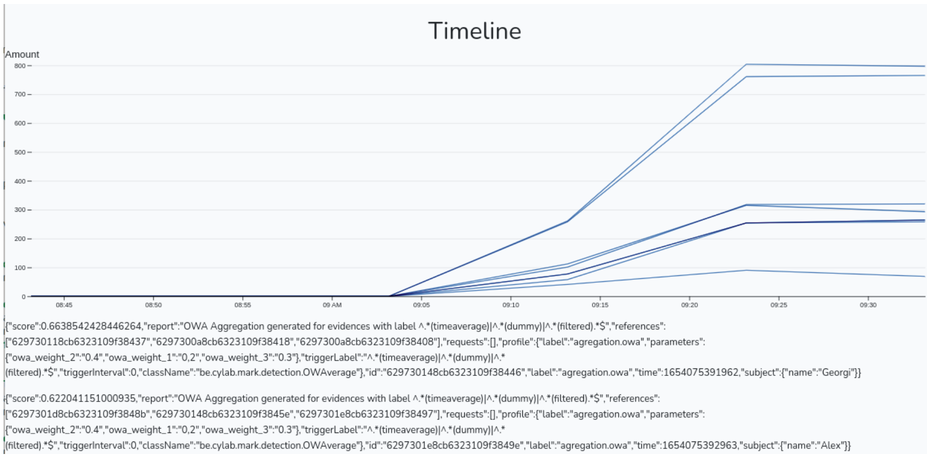


Fig. 5. The MASFAD dashboard prototype

An example of the proposed dashboard is shown in Fig. 5, showing some basic visualizations such as- the amount of entries (raw data/evidences), pie chart of amount of entries per agents and a graphical representation of the evidences produced per agent using a Bubble graph. Specifically with the Bubble graph, we see an application of a design choice tailored to how humans perceive information. The use of size, color and positioning, when displaying the evidences, results in a better understanding of what this information means and directly draws the eye of the analyst to what is important. This is the principle of exploiting the human visual perception and cognition, best explained by [33]. The Bubble graph directly shows that the circles, colored in red, by their size and position are more important to review than the other ones.

Dynamic display generation The amount of data generated each second is immense; it is simply not feasible to design a static system, as it will very rapidly be out-of-date and not represent the current state of the network. This leads to the need for certain mechanisms to dynamically keep the representations updated with the new data entering the system. As shown in Fig. 5, the views, which display the current amount of data and detection agent evidences, need to be updated at regular intervals, strengthening the ability to observe and evaluate the behavior of the network.



```
{"score":0.6638542428446264,"report":"OWA Aggregation generated for evidences with label ^.*(timeaverage)|^.*(dummy)|^.*(filtered).*$","references":
["629730118cb6323109f38437","6297300a8cb6323109f38418","6297300a8cb6323109f38408"],"requests":[],"profile":{"label":"agregation.owa","parameters":
{"owa_weight_2":"0.4","owa_weight_1":"0,2","owa_weight_3":"0.3"},"triggerLabel":"^.*(timeaverage)|^.*(dummy)|^.*
(filtered).*$","triggerInterval":0,"className":"be.cylab.mark.detection.OWAverage"},"id":"629730148cb6323109f38446","label":"agregation.owa","time":1654075391962,"subject":{"name":"Georgi"}}

{"score":0.622041151000935,"report":"OWA Aggregation generated for evidences with label ^.*(timeaverage)|^.*(dummy)|^.*(filtered).*$","references":
["6297301d8cb6323109f3848b","629730148cb6323109f3845e","6297301e8cb6323109f38497"],"requests":[],"profile":{"label":"agregation.owa","parameters":
{"owa_weight_2":"0.4","owa_weight_1":"0,2","owa_weight_3":"0.3"},"triggerLabel":"^.*(timeaverage)|^.*(dummy)|^.*
(filtered).*$","triggerInterval":0,"className":"be.cylab.mark.detection.OWAverage"},"id":"6297301e8cb6323109f3849e","label":"agregation.owa","time":1654075392963,"subject":{"name":"Alex"}}
```

Fig. 6. Detection agents' timeline example

Another example of dynamic visualization is shown in Fig. 6. The user can select a specific time-span of importance and generate a timeline of the amount of evidences produced by the different agents during that time window. This is vital, when we want to observe the behavior of the agents and infer from that possible suspicious activity inside the network. The eye will be directly drawn to possible spikes in activity, compared to periods of inactivity from the agents. The graph updates in real-time, offering the possibility to the user to select a specific agent, directly from the visualization, and review the evidences produced by it. Such visualizations are not new, but they show the importance of enhancing the capabilities of a domain analyst to quickly view, detect and analyse abnormal activity.

Tools aiding pattern recognition The most important aspect of the MAS-FAD framework is the behavior- and anomaly-detection through pattern recognition. This is a vital part of the analysis implementation, but machines are fallible and humans have evolved for centuries to sub-consciously be able to detect complex patterns to be able to survive. This leads to a need for visual capabilities to enhance the performance of the framework through the human-machine interface. This can be achieved through the combination of different outputs in new visualizations, which aid to determine if abnormal behavior is present within the system and pinpoint the origin of this abnormality. There is no clear cut way to resolve this problem- as with all things visual, it is highly dependent on human cognition and interpretation. Even though it is a daunting challenge, there are solutions present to tackle this problem, transforming complicated computer data into easily digestible information.

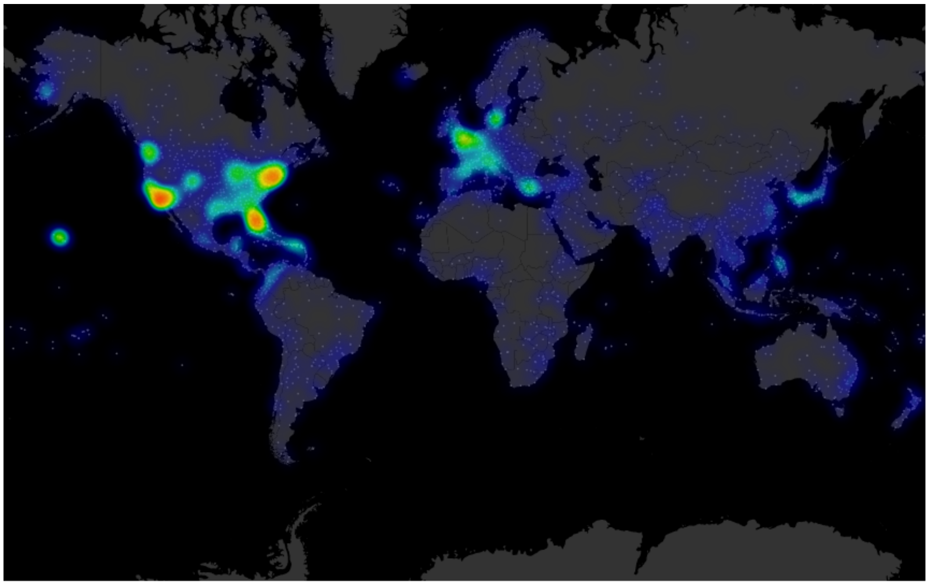
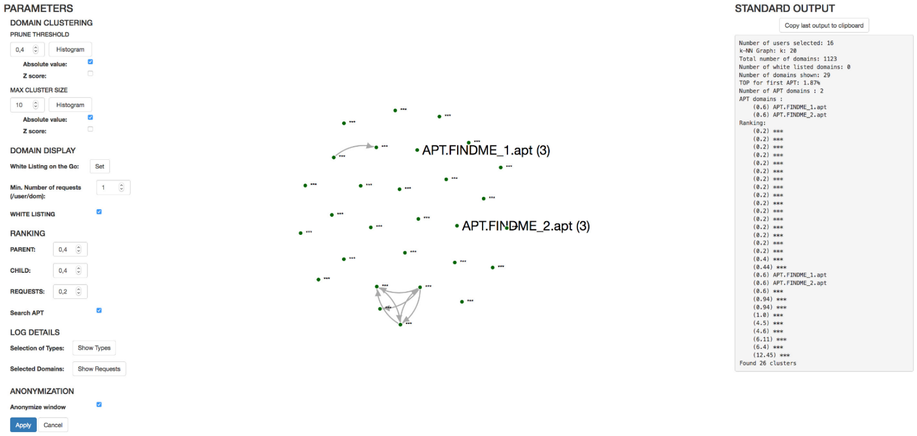


Fig. 7. Geo spatial heat map

Combining outputs from different detection agents and presenting them in a clear and understandable way is a step forward to helping the domain analyst to quickly discover possible patterns. An example of that is shown in Fig. 7. By combining the output of two agents, more specifically the Frequency and Geo Outlier agents, as previously shown in Fig. 4, we can create a visualization that shows possible suspicious server locations and the frequency with which clients inside the network connect to them. On one hand, the Geo Outlier agent will analyse all connections during a specific time window and create geographic clusters of servers to which clients connect to. Afterwards it will look for anomalies-clusters with a very low number of members and consider them as outliers, possible indicators of man-in-the-middle attacks or command & control servers. The Frequency agent will independently analyse the frequency of connections between a given client and server and determine if there is a specific periodicity present. The aggregation agent already combine the output of these agents when determining the overall "suspisiousness" score of a given connection, but there is a lack of specific graphical representation of the final results. By creating a heat map we can use a combination of spatial positioning and colours, intrinsically familiar to humans.



PARAMETERS

DOMAIN CLUSTERING

PRUNE THRESHOLD: 0,4 — Histogram

Absolute value: ☑

Z score: ☐

MAX CLUSTER SIZE: 10 — Histogram

Absolute value: ☑

Z score: ☐

DOMAIN DISPLAY

White Listing on the Go: Set

Min. Number of requests (/user/dom): 1

WHITE LISTING ☑

RANKING

PARENT: 0,4

CHILD: 0,4

REQUESTS: 0,2

Search APT ☑

LOG DETAILS

Selection of Types: Show Types

Selected Domains: Show Requests

ANONYMIZATION

Anonymize window ☑

Apply Cancel

STANDARD OUTPUT

```
Number of users selected: 16
k-NN Graph: k: 20
Total number of domains: 1123
Number of white listed domains: 0
Number of domains shown: 29
TOP for first APT: 1.87%
Number of APT domains : 2
APT domains :
    (0.6) APT.FINDME_1.apt
    (0.6) APT.FINDME_2.apt
Ranking:
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.2) ***
    (0.4) ***
    (0.44) ***
    (0.6) APT.FINDME_1.apt
    (0.6) APT.FINDME_2.apt
    (0.6) ***
    (0.94) ***
    (0.94) ***
    (1.0) ***
    (4.5) ***
    (4.6) ***
    (6.11) ***
    (6.4) ***
    (12.45) ***
Found 26 clusters
```

Fig. 8. Graph based APT detection visualization

Another example of a simple way to visualize complex data is shown in Fig. 8. The proposed graph-based detection is described in [6], through the use of k-nearest neighbours algorithm to construct a graph of HTTP traffic. As modern APTs have learned to hide their activity, obfuscated by regular user traffic, it is more difficult to discern which connections are normal and which are malicious. Through the use of graphs we can reconstruct HTTP traffic in the form of interconnected trees- each edge connected to the subsequent requests from a web page to load its appropriate resources (HTML, images, scripts, etc). The APTs hidden within them will stand out as they will have very weak connection to multiple different HTTP requests and this becomes blatantly obvious through the use of the graph visualization. The graph can be dynamically reconstructed each time the analyst would like to adapt the parameters or focus on specific parts of the logs, offering great customization and flexibility.

Agent reporting Producing a ”suspiciousness” score for the various connections established between clients and server is great, when a domain analyst is looking for a quick result to a query. But a more in-depth way of reporting and explaining the score produced is also required. Currently each detection agent produces an analysis report, available through the user interface, consisting of multiple items:

- The Client and the Server, between which the connection was established
- Score produced by the agent
- The timestamp associated with the generated report
- Short description and the various parameters used by the analysis
- Any figures generated by the agent
- The parameters used to trigger the agent
- The data queried by the agent for analysis

- A graphical representation of the history of the agent for this specific connection
- Any references to other detection agents

The reporting is detailed and can easily be accessed by, for example, selecting a specific connection in the Bubble graph in Fig. 5, or accessing the textual representation of the ranking generated by the different agents. We propose a further evolution of the generated report by organising it in easily digestible chunks and further enhancing it with outside information, such as the MITRE ATT&CK [2] framework. The MITRE ATT&CK framework is a large source of information on various APT attacks and their methodologies. This ties directly into the projection phase of the cyber situation awareness model- through the collection, interpretation and evaluation of information from inside the network, we can better construct threat models and design better protection. By cross-referencing the MASFAD framework findings with the MITRE ATT&CK framework and displaying a comprehensive overview of any relevant information, we can enhance the ability of the domain expert to correctly decide future courses of action.

Input data validation Last but not least, there must be a mechanism in place to ensure that the data retrieved from the network is valid and has not been tampered with. Advanced APTs may try to hide their activity by directly changing the data written to log files, network traffic packets or computer hard disks. Validating the data is a daunting task and doing this in a way in which we can present the findings of the validation through a graphical user interface is even more complex. At the moment this requirement remains an open question, as first the algorithmic side of the problem needs to be resolved, which is no small task. Once an appropriate solution is found to correctly validate the raw data, we can focus on visualizing the results of the validation and incorporating the knowledge and expertise of the cyber analyst. This can be quite beneficial, as mentioned above, erroneous data may signify tampering by malicious code, which is a certain indicator of abnormal behavior.

5 Evaluation of Cyber Situation Awareness

After the design and implementation phases, it is important to evaluate the usability of the visualization tool as a means to enhance the cyber situation awareness of a cyber analyst. There are different ways of achieving that, the two most widely used being the Situation Awareness Global Assessment Technique (SAGAT) [8] and the Situation Awareness Rating Technique (SART) [29]. Each of these approaches comes with their advantages and disadvantages, offering a completely different approach to evaluating the level of SA. The SAGAT method uses objective scoring by freezing the simulation and presenting the operator with a query, evaluating different aspects of the SA. This can lead to certain problems, such as reliance on memory and difficulties in implementing the evaluation as the freezes have to happen randomly and be tailored to the specific field of SA. Contrary to that, SART uses a subjective evaluation of the operator's SA, defining a general list of questions to be administered after or during the use of the visualization tool. SART is easier to implement, but a major disadvantage comes with its user centric evaluation, where the operator may have difficulty rating their own situation awareness and confounding how well they are doing and their actual level of SA. The two methodologies have been compared by Endlsey in [10]. The conclusion is that in general SAGAT performs overall better than SART, as the latter technique shows high correlation with the personal opinion of the user's performance.

In regards to evaluating the MASVIS tool, we opt for the SAGAT approach. It has been shown that this technique is highly appropriate for application in the cyber security domain [22]. The goal will be to prepare a predetermined dataset, mixing real world data with injected APTs and setting up a simulated environment, which closely mimics a real world infrastructure. This can be achieved through the use of our own cyber range [5]. The participants in this evaluation will be provided with a description of the evaluation environment, such as the topology of the network and the different data sources used for log collection. At random intervals the exercise can be interrupted and a questionnaire will be presented to the participants, asking them a wide variety of questions to establish their level of SA in regards to the three different levels- Perception, Comprehension and Projection. Each query will be in the form of a simple yes-no answer, evaluating the capabilities of the participants to correctly identify suspicious activity using the MASVIS tool, evaluate the comprehension and possible future impact of the discovered malicious activity on the network. After the exercise, the questionnaires will be evaluated and an individual score per participant will be attributed to the visualization tool. We expect that by using this technique we can achieve an objective evaluation of MASVIS, which can help us determine its usability and help us ameliorate it in future iterations.

6 Conclusion

Throughout this paper we discussed the difficulties inherent to designing a visual solution for the detection of APT attacks. Currently the MASFAD framework offers a high detection performance of such attacks, but lacks the visualization capabilities to enhance the human-machine interaction. We have determined that focusing on the human element and understanding the process by which an analyst can better explore, identify and detect possible abnormal activity needs to be a central point in designing a better user interface. Starting from there, we establish the needed requirements for a powerful Visual Analytics tool and how these requirements can be met.

By defining clearly the expectations and requirements of the user, we can design an interface which can aid in the process of enhancing cyber situation awareness by aiding the analyst to more efficiently traverse the different steps of the analysis loop. We propose different solution for each of the requirements, ranging from higher modularity and flexibility of what is displayed, the dynamic nature of the visualizations, complex representations to aid in pattern recognition to better reporting through the integration of an open-source knowledge base, such as the MITRE ATT&CK framework. Currently there is a lack of specific tools to detect previously undiscovered or highly complex advanced attacks, we are certain our solution will perform as well as currently available tools and take the detection one step further through the incorporation of Visual Analytics techniques.

References

1. [online] grafana, https://grafana.com/grafana, accessed: 2022-05-30
2. [online] mitre att&ck, https://attack.mitre.org/, accessed: 2022-05-30
3. Cardenas, A.A., Manadhata, P.K., Rajan, S.P.: Big data analytics for security. IEEE Security & Privacy **11**(6), 74–76 (2013)
4. Cui, W.: Visual analytics: A comprehensive overview. IEEE Access **7**, 81555–81573 (2019)
5. Debatty, T., Mees, W.: Building a cyber range for training cyberdefense situation awareness. In: 2019 International Conference on Military Communications and Information Systems (ICMCIS). pp. 1–6. IEEE (2019)
6. Debatty, T., Mees, W., Gilon, T.: Graph-based apt detection. In: 2018 International Conference on Military Communications and Information Systems (ICMCIS). pp. 1–8. IEEE (2018)
7. Do Xuan, C.: Detecting apt attacks based on network traffic using machine learning. Journal of Web Engineering pp. 171–190 (2021)
8. Endsley, M.R.: Design and evaluation for situation awareness enhancement. In: Proceedings of the Human Factors Society annual meeting. vol. 32, pp. 97–101. Sage Publications Sage CA: Los Angeles, CA (1988)
9. Endsley, M.R.: Toward a theory of situation awareness in dynamic systems. In: Situational awareness, pp. 9–42. Routledge (2017)
10. Endsley, M.R., Selcon, S.J., Hardiman, T.D., Croft, D.G.: 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, pp. 82–86. SAGE Publications Sage CA: Los Angeles, CA (1998)
11. Erbacher, R.F.: 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, pp. 2507–2513. IEEE (2003)
12. Friedberg, I., Skopik, F., Settanni, G., Fiedler, R.: Combating advanced persistent threats: From network event correlation to incident detection. Computers & Security **48**, 35–57 (2015)
13. Gormley, C., Tong, Z.: Elasticsearch: the definitive guide: a distributed real-time search and analytics engine. " O'Reilly Media, Inc." (2015)
14. Humphries, C., Prigent, N., Bidan, C., Majorczyk, F.: Elvis: Extensible log visualization. In: Proceedings of the Tenth Workshop on Visualization for Cyber Security. pp. 9–16 (2013)
15. Keim, D., Andrienko, G., Fekete, J.D., Görg, C., Kohlhammer, J., Melançon, G.: Visual analytics: Definition, process, and challenges. In: Information visualization, pp. 154–175. Springer (2008)

16. Koike, H., Ohno, K.: Snortview: visualization system of snort logs. In: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. pp. 143–147 (2004)
17. Kott, A., Wang, C., Erbacher, R.F.: Cyber defense and situational awareness, vol. 62. Springer (2015)
18. Lahmadi, A., Beck, F.: Powering monitoring analytics with elk stack. In: 9th international conference on autonomous infrastructure, management and security (aims 2015) (2015)
19. Lavigne, V., Gouin, D.: Visual analytics for cyber security and intelligence. The Journal of Defense Modeling and Simulation **11**(2), 175–199 (2014)
20. Lee, J., Jeon, J., Lee, C., Lee, J., Cho, J., Lee, K.: 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). pp. 1–6. IEEE (2016)
21. Lemay, A., Calvet, J., Menet, F., Fernandez, J.M.: Survey of publicly available reports on advanced persistent threat actors. Computers & Security **72**, 26–59 (2018)
22. Lif, P., Granåsen, M., Sommestad, T.: Development and validation of technique to measure cyber situation awareness. In: 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). pp. 1–8. IEEE (2017)
23. Marchetti, M., Pierazzi, F., Colajanni, M., Guido, A.: Analysis of high volumes of network traffic for advanced persistent threat detection. Computer Networks **109**, 127–141 (2016)
24. Mees, W., Debatty, T.: Multi-agent system for apt detection. In: 2014 IEEE International Symposium on Software Reliability Engineering Workshops. pp. 401–406. IEEE (2014)
25. Mwiki, H., Dargahi, T., Dehghantanha, A., Choo, K.K.R.: Analysis and triage of advanced hacking groups targeting western countries critical national infrastructure: Apt28, red october, and regin. In: Critical infrastructure security and resilience, pp. 221–244. Springer (2019)
26. Nikolov, G., Debatty, T., Mees, W.: Evaluation of a multi-agent anomaly-based advanced persistent threat detection framework
27. Panero, P., Valsan, L., Brillault, V., Schuszter, I.C.: Building a large scale intrusion detection system using big data technologies. In: International Symposium on Grids and Clouds 2018. p. 14 (2018)
28. Son, K., Lee, T., Won, D.: Design for zombie pcs and apt attack detection based on traffic analysis. Journal of The Korea Institute of Information Security & Cryptology **24**(3), 491–498 (2014)
29. Taylor, R.M.: Situational awareness rating technique (sart): The development of a tool for aircrew systems design. In: Situational awareness, pp. 111–128. Routledge (2017)
30. Thomas, J.J., Cook, K.A.: A visual analytics agenda. IEEE computer graphics and applications **26**(1), 10–13 (2006)
31. Varga, M., Winkelholz, C., Träber-Burdin, S.: Cyber situation awareness. Cyber Security Science and Engineering (STO-EN-IST-143) pp. 1–18 (2016)
32. Virvilis, N., Gritzalis, D.: The big four-what we did wrong in advanced persistent threat detection? In: 2013 international conference on availability, reliability and security. pp. 248–254. IEEE (2013)
33. Ware, C.: Information visualization: perception for design. Morgan Kaufmann (2019)

34. Zhang, T., Wang, X., Li, Z., Guo, F., Ma, Y., Chen, W.: A survey of network anomaly visualization. Science China Information Sciences **60**(12), 1–17 (2017)