Alert Characterization by Non-Expert Users in a Cybersecurity Virtual Environment: a Usability Study

Alexandre Kabil, Thierry Duval, Nora Cuppens

Alert Characterization by Non-Expert Users in a Cybersecurity Virtual Environment: a Usability Study

Alexandre Kabil[1], Thierry Duval[1], and Nora Cuppens[2]

[1] IMT Atlantique, Brest, France
Lab-STICC, UMR CNRS 6285
{alexandre.kabil,thierry.duval}@imt-atlantique.fr
[2] Polytechnique Montréal, Montréal, Canada
nora.boulahia-cuppens@polymtl.ca

Abstract. Although cybersecurity is a domain where data analysis and training are considered of the highest importance, few virtual environments for cybersecurity are specifically developed, while they are used efficiently in other domains to tackle these issues.
By taking into account cyber analysts' practices and tasks, we have proposed the 3D Cyber Common Operational Picture model (3D CyberCOP), that aims at mediating analysts' activities into a Collaborative Virtual Environment (CVE), in which users can perform alert analysis scenarios.
In this article, we present a usability study we have performed with non-expert users. We have proposed three virtual environments (a graph-based, an office-based, and the coupling of the two previous ones) in which users should perform a simplified alert analysis scenario based on the WannaCry ransomware. In these environments, users must switch between three views (alert, cyber and physical ones) which all contain different kinds of data sources. These data have to be used to perform the investigations and to determine if alerts are due to malicious activities or if they are caused by false positives.
We have had 30 users, with no prior knowledge in cybersecurity. They have performed very well at the cybersecurity task and they have managed to interact and navigate easily. SUS usability scores were above 70 for the three environments and users have shown a preference towards the coupled environment, which was considered more practical and useful.

Keywords: Virtual Reality · Cyber Security · Usability Study.

1 Introduction

More and more human activities are digitized and connected in cyberspace. The cyberspace could be defined as Gutzwiller does as a space that 'comprises communications between computing devices, the devices themselves, and the interconnections of machines and networks to the physical world as both sensors

and actuators' [5]. In this context cybersecurity grows in importance, as a small security breach in a network can have a huge impact on organizations or countries, as with the WannaCry Attack in 2017. Visual Analytics solutions are now provided to analysts to help them to understand cyber situations [20]. These solutions offer efficient 2D visualizations coupled with advanced data processing capabilities, but few 3D visualizations or Immersive Analytics solutions are developed for cybersecurity, even though they can leverage some issues in data analysis and are getting attention in other domains [6].

In the same way, training environments proposed for cybersecurity are still only developed for specific cases with expert tools or serious games for sensitization whereas Virtual Environments for Training have been used for years in the industry for different scenarios or practices [15].

In our opinion, Virtual Environments (VE) for cybersecurity should merge data visualization with contextual scenarios to be useful for both experts and non-experts [10]. Figure 1 shows in a Venn Diagram our position towards the usability of Virtual Reality (VR) for cybersecurity.

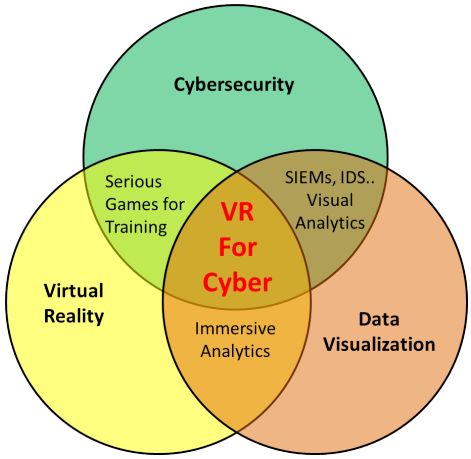

Fig. 1. Venn diagram of our position about the usability of Virtual Reality Applications for cybersecurity, which is at the intersection of three distinct domains, Virtual Reality, Data Visualization and Cybersecurity.

To develop such environments, the analysis of cyber activities, tasks and practices must be performed to model relevant use cases. To face this issue, we have developed a VE instantiation model, the 3D Cyber Common Operational Picture (3D CyberCOP) [8], based on activities and task analysis of Security Operations Centers (SOC) operators. We also have proposed an alert analysis scenario based on the WannaCry ransomware, as a use case of our model.

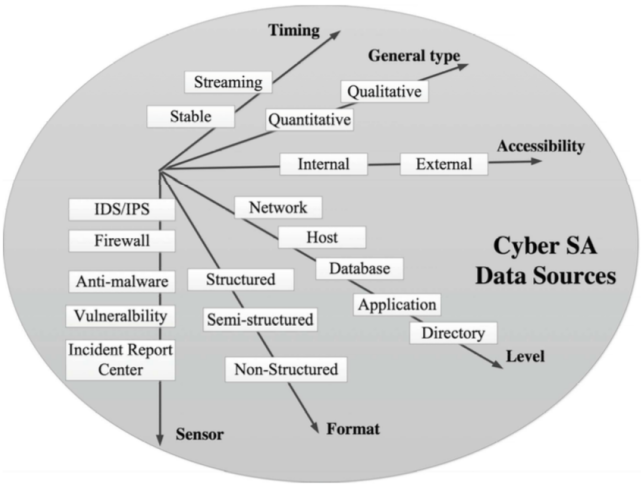

Fig. 2. Data sources treated by a cyber analyst to get Cyber SA, from [22].

To assess the effectiveness of a VE for both data visualization and training for cybersecurity, evaluations and exercises should be performed with various users.

In this article, we will present the usability study we have performed with non-expert users, based on an implementation of the 3D CyberCOP model. We will not emphasize new or innovative interaction techniques but rather more on the adaptation of cyber practices into a VE.

In section 2 we will present the 3D CyberCOP model and our use case based on the WannaCry ransomware. This model was based on a study of Security Operation Center (SOC) operators' activities, tasks and practices and aims at adapting these practices into a VE.

Then in section 3, we will present an instantiation of our model we have developed for a usability study with non-experts users. We will detail our usability study in section 4 and the results in section 5, and we will conclude by showing perspectives of our approach.

2 3D CyberCOP Model and analysis scenario

There is a growing interest in human factor field and cognitive science for cybersecurity, which aim at easing the burden of analysts, as they have to deal with a huge number of data sources to develop a mental model of the cyber situation, called the Cyber Situational Awareness (Cyber SA) (Figure 2).

Defining a cybersecurity operation activity model can facilitate the understanding of operators' activities within organizations and the collaboration between these organizations [19]. We have developed our 3D Cyber Common Operational Picture (3D CyberCOP) model with this in mind. In this section, we

will detail our model and the analysis of WannaCry ransomware we have made in order to create alert analysis scenarios.

2.1 Cyber Activity Modeling

Cyber activity studies take often place in Security Operations Centers (SOCs), which are well-defined structures where analysts are monitoring networks round-the-clock, and where they have to investigate alerts for client companies or internal security [7]. There exist anthropological studies in SOC in order to understand the roles and tasks of operators [18], and taxonomies were developed to characterize them [4]. Cognitive Tasks Analysis (CTA) were also performed to assess operator's sense-making capabilities [3] and to help to develop effective visualization tools via the EevI framework, for example [16].

We had had the opportunity to visit our industrial partners' SOCs and to perform the following activity analysis described hereafter [9]: after a preliminary visit to understand the context and to get authorizations, we had planned to interview SOC operators and to get information on their practices to develop adapted visualizations.

By using a SOC operator's roles model such as the one proposed by McKenna, Staheli and Meyer in [11] and features from a Computer Supported Cooperative Work (CSCW) model proposed by Casarin, Pacqueriaud, and Bechmann in [2] which are relevant in SOCs, we have defined an activity model which purpose is to adapt cybersecurity practices into a Collaborative VE. In this paper, we will focus only on single-user cyber activities and we are not taking into account collaborative ones. For each feature, we will describe how it is done in SOCs, how we could tailor it for Virtual Environments (VE), and an example of a possible instantiation in an alert analysis scenario, as summarized in Table 1.

Table 1. 3D CyberCOP model allowing the adaptation of SOC features into a Virtual Environment.

FEATURES	ACTIVITY MODEL	DESIGN SOLUTIONS	EXAMPLE SCENARIO
Roles	-Trade-off between decision and data analysis -Hierarchical interactions	-Users with specific actions -Hierarchical interactions	-Analyst immersed in VR -Coordinator with 2D Dashboard
Tasks	-Ticketing system -Specific tasks from defined roles	-Ticketing system -Simulated interactions or scenarios	-Simulated actions for incident analysis
Visualizations	-Tools for monitoring, correlation and reporting	-2D, 3D or immersive filtered visualizations -Integration of existing tools	-2D and immersive visualizations -Physical, Cyber and Alert views
Data	-Aggregated by SIEMs or IDS -From various sources	-Simulated data sets and metrics -Integration with existing tools	-High level events and alerts -Network & Entropy metrics

Roles Cyber activities are a trade-off between decisions and data analysis [17]. For example, an analyst has to execute the request of a coordinator by investigating alerts and sending reports, and the coordinator must take into account this analysis to make decisions.

To implement roles, we can define specific visualizations and interactions. For example, an analyst role could have a detailed view of an asset from an egocentric point of view whereas the coordinator role could have a global view of all assets of the network from an exocentric point of view (as in the Frame of Reference model from Salzman, Dede, and Loftin [14]). To respect the hierarchies between roles, we could implement hierarchical interactions: analysts are given orders and send reports whereas coordinators give orders and read reports.

Tasks Cyber analysts have different levels of expertise and they perform tasks with respect to it. To coordinate their actions, they use a ticketing system that tracks their activities and helps them following procedures. Analysts can perform a lot of actions but they can be regrouped into categories such as Asset Analysis, Log Cleaning or File Disassembling. The National Institute of Standards and Technology (NIST) gives global information about tasks in cybersecurity[3].

For our VE, we have modeled and simulated categories of actions such as **inspection** (getting information from a computer or an alert), **analysis** (performing anomaly analysis on a computer), or **reporting** (sending a report on alerts). The ticketing system has been implemented to keep the coordination between users' actions concerning existing procedures.

In an analysis scenario, we want users to perform simple yet relevant tasks by giving them contextual UIs. Tasks are represented by UI buttons and they are related to an incident analysis procedure.

Data As analysts have to face a lot of heterogeneous data from various sources and sensors [21], aggregation and correlation tools such as Security Information and Event Management systems (SIEMs) or Intrusion Detection Systems (IDS) give them high-level events or alerts that are much more interesting to investigate than raw data [13].

In our VE, we have simulated events or alerts from high-level data sources and we have provided contextual metrics that can give global information about the security state of the system.

In an analysis scenario, we could generate alerts triggered by some metrics provided by the simulated system such as the entropy of filesystems or the network traffic.

Visualizations Usually, 2D dashboards are used to give general information and status reports to everyone in the SOC. Analysts use a lot of dedicated tools to correlate or monitor data. These tools are tailored for specific cases and

[3] https://www.nist.gov/cyberframework

Visual Analytics solutions are used only if regular ones are not giving enough information [20].

In our VE, we have developed both 2D dashboards and immersive interfaces for different roles and needs. In an analysis scenario, analysts could be immersed while the coordinator will have a holistic point of view from a 2D dashboard (Figure 3).

Fig. 3. Examples of visualizations developed from our activity analysis: a 2D monitoring dashboard (TOP) and an immersive interface (BOTTOM).

To limit cognitive load while allowing data correlation [23], we have provided separate views that give complementary information about the monitored systems. For example, one physical view and one cyber view could be provided. These views respectively contain data about the 'physical' environment (device settings, last user logged on the device, geographical position of computers in a building, etc) and the network environment (network flow and topology, IP addresses).

To implement these features, we have designed an alert analysis scenario based on the WannaCry ransomware.

2.2 Ransomware modeling

We have chosen to model the Wannacry Ransomware[4], as it has caused major troubles in May 2017 and as its behavior could be described simply [12]. Figure 4 sums up our modeling of WannaCry ransomware.

When Wannacry infects a computer (by being downloaded and executed for example), it encrypts data on the computer and it propagates itself through the network by using Windows seven Operating System (OS) vulnerabilities. The user must pay a ransom to get her data back, as the encryption could not be broken. The entropy of filesystems and network traffic metrics are enough to describe Wannacry's high-level behavior: when it infects a computer, it raises the entropy metric (files are encrypted, resulting of high activity) and when it propagates, the network traffic increases as well. These metrics raise alerts when they reach thresholds and these alerts can be true or false positives (for example a data backup and encryption or a download activity from a computer will raise these metrics even if these activities are not caused by WannaCry). WannaCry can also raise only one metric, for example, if the computer is protected against data encryption but not patched (the ransomware can propagate), or if it is patched but not protected.

One specific analysis scenario will be presented in the following section.

3 Proposed environments and scenario for usability evaluation

To perform a usability evaluation, we have chosen specific features to implement into our environment. In this section, we will detail the VE and the alert analysis scenario we have designed for the evaluation.

3.1 Evaluated environment

As we want to assess the effectiveness of VE for cybersecurity, we have decided to implement the Analyst role of our 3D CyberCOP model. Users will be immersed in an environment containing a potentially infected network of computers and will have to gather information to characterize alerts.

In order to get information from the environment, we have provided three views, namely the alert, the cyber and the physical view (Figure 5). Users have to switch between them in order to get relevant information on the situation.

[4] http://cert-mu.govmu.org/English/Documents/White%20Papers/White%20Paper%20-%20The%20WannaCry%20Ransomware%20Attack.pdf

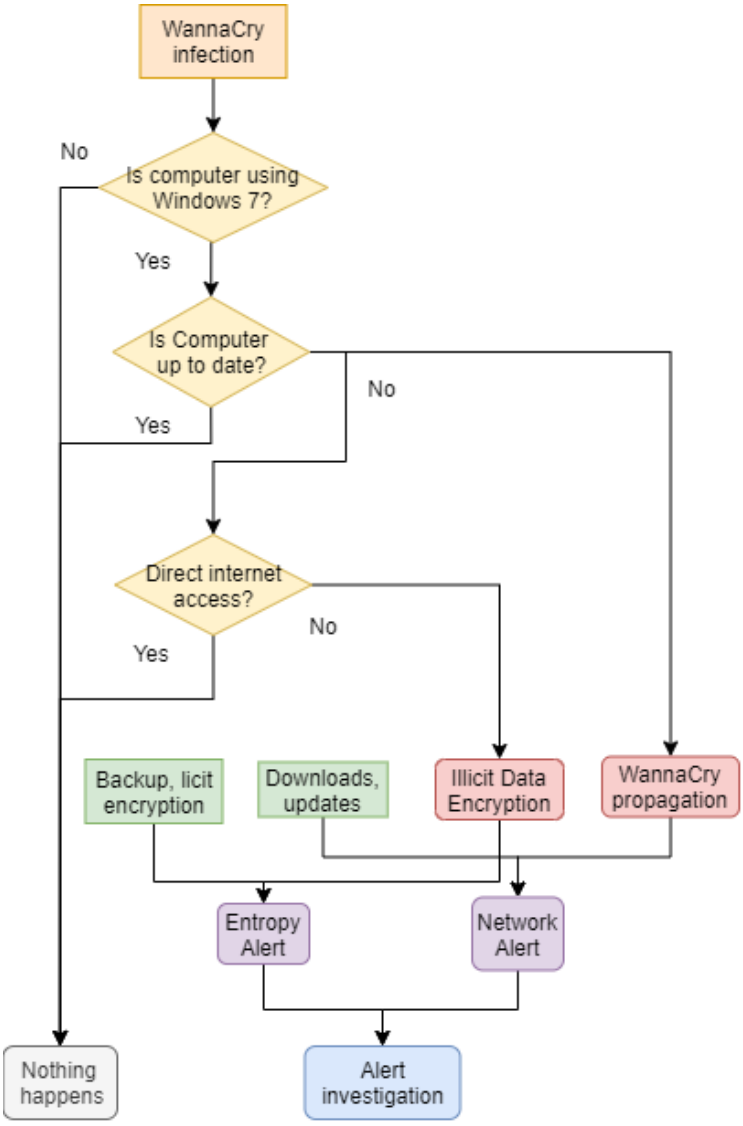

Fig. 4. WannaCry behavioral model used for alert analysis scenario creation.

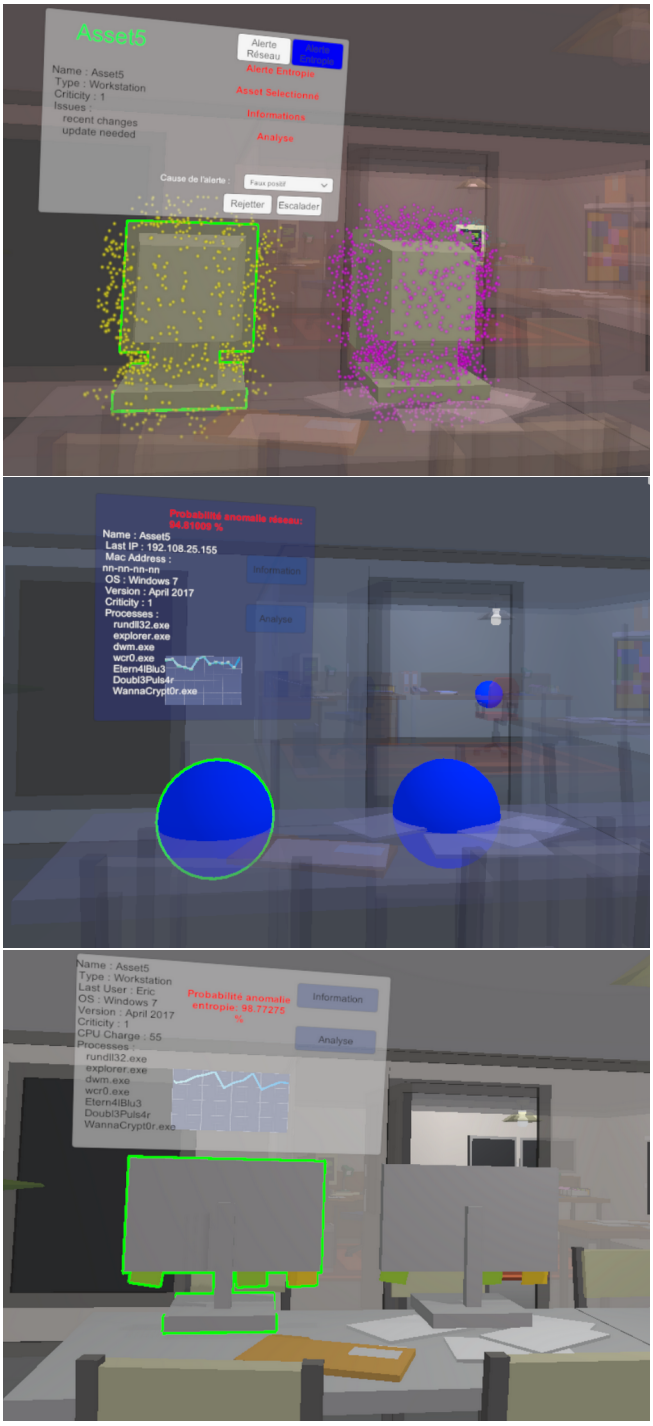

Fig. 5. From top to bottom, the alert view, the cyber view, and the physical view. Views are colocated in the VE, in order to facilitate the switching between them. Users select computer to access data relative to the current view.

- The alert view contains data regarding the alerts status. If a computer is concerned with an alert, it will be highlighted by a particle system for example.
- The cyber view allows users to get information from the network architecture or network processes.
- The physical view contains data related to the processes of computers, their operating system, and other information.

Navigation in the Virtual Environment is made by using the teleportation metaphor, but we also have let the possibility to the user to use a joypad to move.

Information is displayed through 2D interfaces that are accessible by selecting computers or relevant 3D objects. Selection is made by using the selecting ray metaphor.

3.2 Analysis scenario

The alert analysis task has been simplified to be achieved by users with no prior knowledge about cybersecurity: only a few data were available and the procedure was lightened. The analysis scenario was the following (Figure 6):

- Alerts appear on the alert view, and users have to follow an investigation procedure to resolve the case.
- The investigation is done by switching views to gather relevant information about the alert (an entropy alert should be investigated in the physical view and a network alert in the cyber one). Specific actions will be available for users, such as 'get information from this computer' or 'perform an anomaly analysis' (these actions are simulated according to procedures).
- Once the user thinks she has enough information, she has to characterize the alert by escalating or dismissing it. Once it is done, she has to select another alert and continue the investigation.

This scenario was successfully implemented into a VE, and we have proposed a usability study based on this implementation.

4 Usability evaluation protocol

As we wanted to evaluate the usability of a VE for an alert analysis task, we have designed three different environments and an evaluation protocol.

4.1 Virtual Environments for alert analysis

Abstract environments, as 3D graph visualization are more and more used for data analysis whereas concrete environments are usually used for training sessions.

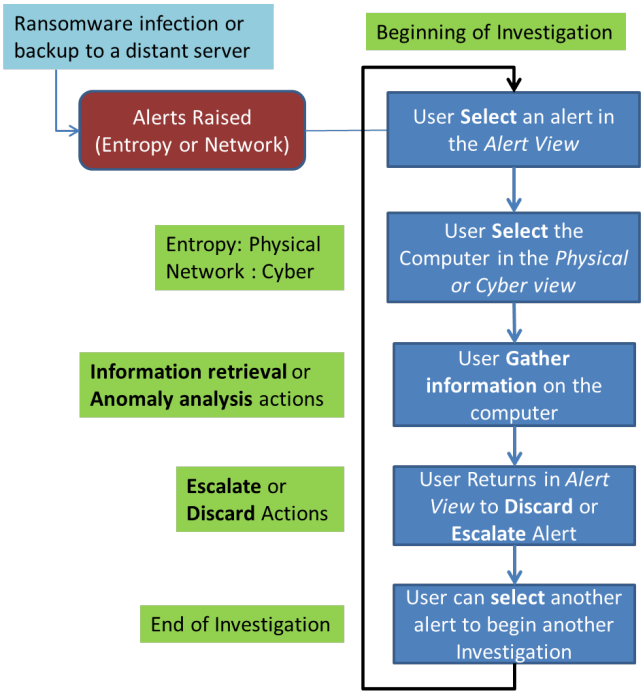

Fig. 6. Alerts investigation simplified scenario.

We have wanted to see if users would perform better in a classical 3D Graph visualization representing the network topology or in an office-based one where computers, desktops and so on are represented.

To go beyond this comparison, we have also proposed an environment containing both the network topology and the office assets. These environments are represented in the Figure 7.

Order of the three proposed environment was defined by two conditions: even users begin with the graph-based environment (Abstract-Concrete-Mixed condition) whereas odd users begin with the office-based one (Concrete-Abstract-Mixed condition). The third environment was always the mixed one.

4.2 Protocol

We thought that users would find the concrete environment more entertaining but that they would also be more efficient in the abstract environment while the mixed one would be considered too complex. We have defined three scenarios presenting similarities so that the tasks were different in each environment to avoid a learning effect. These scenarios contained the same infected assets but positioned differently into the environments.

We had performed the evaluation with an Oculus Rift CV1. VE was developed with the Unity Game Engine and the VRTK toolkit for interaction

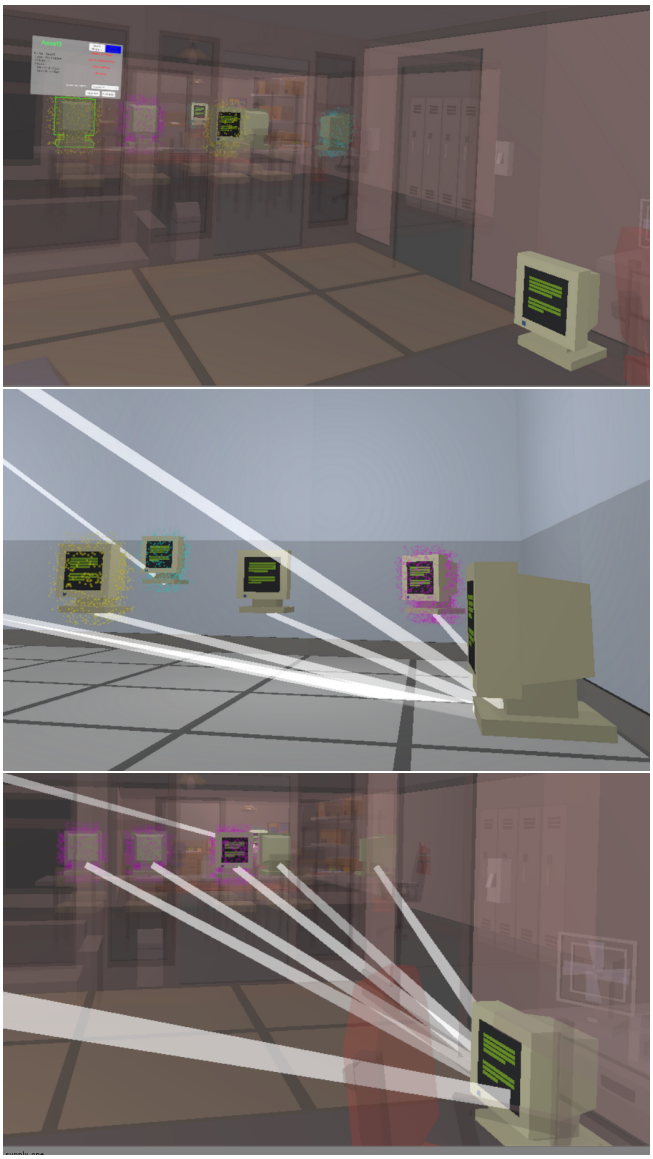

Fig. 7. From top to bottom: concrete office environment, abstract graph-based environment, and mixed environment. In these environments, users had to analyze cybersecurity alerts by following specific analysis scenarios.

metaphors. An event-based architecture was used to implement the scenario and to facilitate action logging [9].

Users had to fill a consent form where we explained the purpose of the experiment. Then, they had to perform a tutorial task in order to get familiar with the immersive devices and the VE. Alert analysis tasks lasted fifteen minutes; there were eleven alerts to investigate, and two false positives among them.

In between immersive tasks, we asked users to fill a SUS usability questionnaire [1] and to answer some questions about the task itself.

At the end of the third immersive task, after filling the SUS and task questionnaires, we asked users which interface they had preferred and why. We asked also some questions about the physiological effects of immersive experiments and technology adoption.

The experimentation protocol is summed up in the Table 2.

Table 2. Usability experiment protocol

Experimentation Step	**Duration**
Greeting and consent form	15 min
Tutorial and familiarization task	10 min
Three VE experiments in two different orders	10 x 3 min
Usability and task analysis survey	5 x 3 min
User Experience and preferences survey	10 min

5 Results and Findings

We carried out our experiment for a month and collected the results of thirty users, mostly computer science students. Most users were unfamiliar with immersive technologies and cybersecurity but familiar with video games. The total average duration of a user's evaluation was one hour and thirty minutes, and all users passed the analysis scenarios. In the Figures that we are going to present, the margin of error comes from the standard deviation. The p-values given come from ANOVA-type variance analyzes at 95%.

5.1 Results

The abstract, concrete and mixed environments respectively obtained SUS usability scores of 76.41, 72.42 and 77.33 out of 100 (Figure 8), which means that they are considered usable (the usability threshold of an interface is set to 70/100 for the SUS test). There were no significant differences in the environmental usability scores between the users who started experimenting with the abstract environment (ACM condition) and users who started with the concrete environment (CAM condition) (Figure 9).

The results of ANOVA-type variance analysis at 95% between the two conditions and for the abstract, concrete and mixed environments give p = 0.81, p = 0.71 and p = 0.69 respectively.

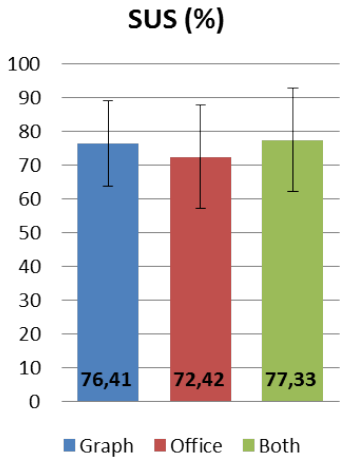

Fig. 8. Mean values (with standard deviation error) of SUS usability score for each environment. All environments gets a score higher than 70, which means that they are usable (from the SUS test perspective).

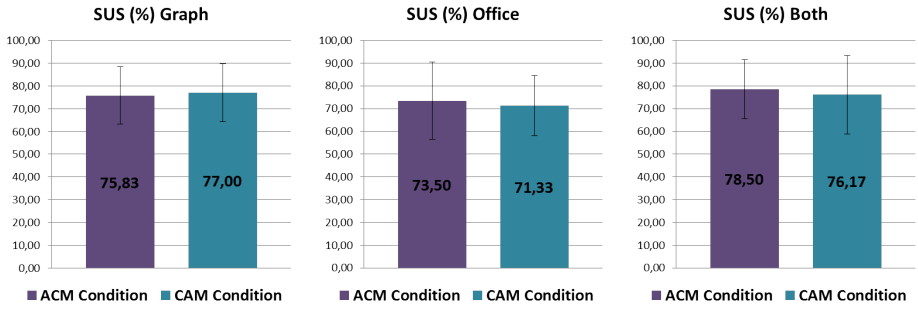

Fig. 9. Mean values of SUS usability score for each environment and for both experimentations' conditions. No significant differences between experimentations' conditions.

Users have preferred the mixed environment combining abstract and concrete data representation. The ACM and CAM conditions for passing the experiment

(i.e. starting with the abstract or concrete environment) had no effect on user preferences (Figure 10). Contrary to what we thought, the complexity of this environment was not a limiting factor for most users, but the fact that it was always explored in the third session may have influenced their choice.

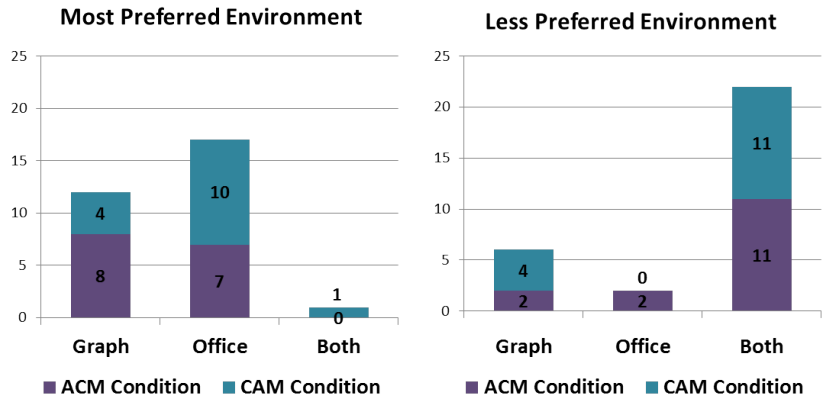

Fig. 10. Users' preferences for proposed environments. No significant differences between experimentations' conditions.

The average score for the questions concerning physiological disorders was 3.08/10, which means that users did not experience any discomfort during the experiments (Figure 11), although we have found that six users (three out of five users older than thirty-five years old, two users under the age of twenty-five and one user between twenty-five and thirty-five years old) felt more dizziness than the others.

Users have considered that they could easily acquire the skills required to use this VE (average score of 8/10), with a significant effect of age (average score of 5.8 / 10 for those older than thirty-five years old).

Immersive devices were considered pleasant and potentially usable at work. Environments and immersive technology were generally found to be relevant, with scores on questions about technology adoption and user experience above 6 out of 10.

An analysis score was assigned to users based on the accuracy of their alert characterization. A score of eight out of eleven means, for example, that they correctly characterized eight alerts (including false positives) out of the eleven present in the scenarios. On average, users have performed well during the experiments (average score greater than 8.5/11) (Figure 12 on the left). We found out that alert analysis time was significantly higher in the concrete environment than in the abstract and mixed environments ($p = 4 \times 10^{-4}$). Users have analyzed alerts more quickly in the mixed environment, although there were no signifi-

Cybersickness questions	Mean Score
1. I felt tired during my interaction within the Virtual Environment	3,43/10
2. I felt headache during my interaction within the Virtual Environment	3,1/10
3. I felt visual fatigue during my interaction within the Virtual Environment	4,03/10
4. I had nausea within the Virtual Environment	2,8/10
5. I had headaches while interacting within the Virtual Environment	2,66/10
6. I felt dizzy during my interaction within the Virtual Environment	2,5/10

Fig. 11. Cybersickness questionnaire answers. Users have not felt particularly dizzy while performing the experimentation.

cant differences in analysis times between abstract and mixed environments (p = 0.1).

As the mixed environment was always explored last, adaptation to the experiment as well as familiarity with the task can explain this result (Figure 12 on the middle). On the other hand, we did not find any differences concerning the distance traveled in different environments (p = 0.59) (Figure 12 on the right).

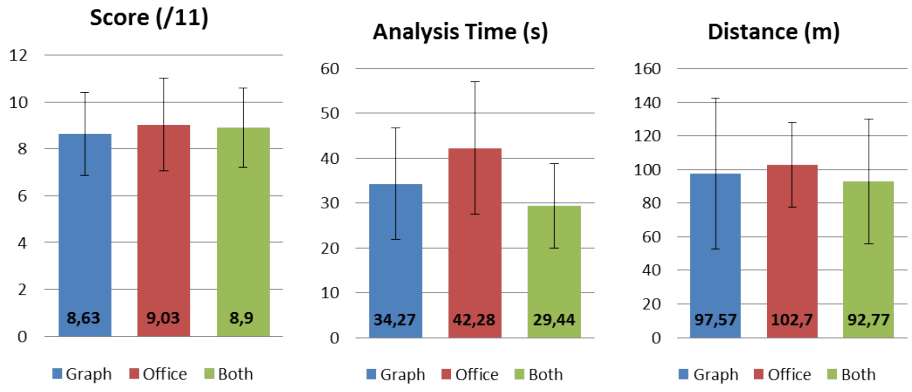

Fig. 12. Mean values of scenario scores, analysis time per alert and distance traveled for each environment.

There was barely any effect of age or familiarity on results, but our sample of users was too small to interpret significant differences between familiarities (for example we had only five users that were more than thirty-five years old).

Some data were available to users to help them to characterize alerts (as the Operating System version or the IP address), and between each experiment, we asked users which data sources were useful. We have noticed that users tended to use more and more data sources to analyze alerts while they were gaining experience during the experiment (Figure 13).

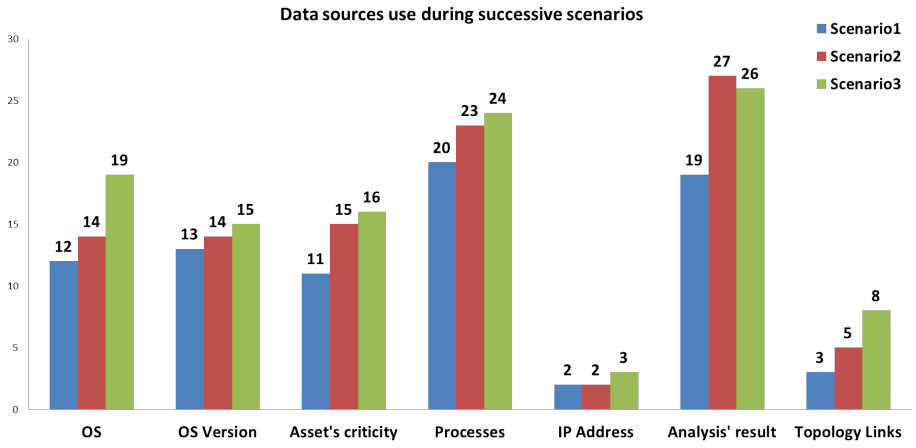

Fig. 13. Data usages for characterizing alerts. We can see a progression of data usages from scenario 1 to scenario 3 (scenarios were always made in the same order).

5.2 Findings

This experiment showed us that a VE for non-experts in cybersecurity is usable, even if results can be discussed.

Users' performance (e.g. score) was not better from the first try to the last one. Maybe the task was too simple so that most of the users had been performing well but have not progressed through experiments. Because we gave users barely any indication (except in the inter-experiment questionnaires in which was mentioned which data source could be used to conduct the analysis), they had sometimes no idea about their performances: they knew that they were correctly characterizing alerts, but sometimes they were having some doubts.

Globally, users did not face cybersickness, even if our five subjects who have more than thirty-five years old and were familiar neither with video games nor with immersive interfaces felt more dizzy according to the questionnaire answers.

The three views were well used by users, but some users pointed out that data were not so different between them, and that alert view was not useful. Maybe a

2D User Interface (UI) could be provided to users to get alerts information and to reduce views switching.

Some users have regretted that any help was available during the experiment. This could be provided easily by adding a 2D UI attached to any user's hand and showing pieces of advice.

Instead of investigating alerts one after the other, users have tended to cross-analyze alerts to see if there were some redundancies in data or if computers close to each other in the network topology have the same processes and alerts.

The fact that users preferred the graph-office mixed environment is maybe due to that it was the last environment they explored, and that they were more familiar with the system. The fact that they have not preferred the office-based environment regardless of condition is an interesting result that we need to investigate.

Overall, users have considered that these VEs for cybersecurity were usable and they were ready to use them, but as they were not cybersecurity experts, we need to perform other studies to analyze this point. Immersive technologies were appreciated by users and they were interested in using them for their work or activities.

6 Conclusion

By studying Security Operations Centers (SOCs) operators' practices, we have designed an activity model, the 3D CyberCOP, which aims at translating cybersecurity activities into a Collaborative Virtual Environment (CVE). This model have allowed us to design a Virtual Environment (VE) in which users could perform cybersecurity alert analysis scenarios based on the WannaCry ransomware. In order to assess the effectiveness of merging both data visualization and training approaches for cybersecurity operators, we have conducted a usability study with non-expert users.

This study has shown that they have succeeded in interacting and navigating through the environments. They have managed to gather data and to understand the cyber situation only after few sessions with great scores, even if the task seemed difficult on the first try. Users have shown a preference to the environment that contained both graph and office visualizations and have found these environments useful for analyzing cyber threats, with a usability score superior to 70.

Further studies should be made to assess the effectiveness of such environments for cybersecurity experts.

In the future we will develop a 2D version of the experimentation, to compare the results between immersive and non-immersive interfaces. The usefulness of view switching will be evaluated maybe in a collaborative experiment. Linking our VE with an existing cyber data analysis tools will bring us more capabilities and more realistic cases, and we will evaluate the reliability of this approach by comparing training with a cyber training tool and with our VE.

Acknowledgments

This work was supported by the Cyber CNI Chair of Institute Mines Télécom, which is held by IMT Atlantique and supported by Airbus Defence and Space, Amossys, BNP Paribas, EDF, Nokia and the Regional Council of Brittany. It has been acknowledged by the Center of excellence in Cyber Security.

References

1. Brooke, J., et al.: Sus-a quick and dirty usability scale. Usability evaluation in industry **189**(194), 4–7 (1996)
2. Casarin, J., Pacqueriaud, N., Bechmann, D.: Umi3d: A unity3d toolbox to support cscw systems properties in generic 3d user interfaces. Proc. ACM Hum.-Comput. Interact. **2**(CSCW), 29:1–29:20 (Nov 2018). https://doi.org/10.1145/3274298, http://doi.acm.org/10.1145/3274298
3. DAmico, A., Buchanan, L., Kirkpatrick, D., Walczak, P.: Cyber operator perspectives on security visualization. In: Advances in Human Factors in Cybersecurity, pp. 69–81. Springer (2016)
4. Evesti, A., Kanstrén, T., Frantti, T.: Cybersecurity situational awareness taxonomy. In: 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). pp. 1–8 (June 2017). https://doi.org/10.1109/CyberSA.2017.8073386
5. Gutzwiller, R.: Situation awareness in defensive cyberspace operations: An annotated bibliographic assessment through 2015. Tech. rep., NIWC Pacific San Diego United States (2019)
6. Hackathorn, R., Margolis, T.: Immersive analytics: Building virtual data worlds for collaborative decision support. In: 2016 Workshop on Immersive Analytics (IA). pp. 44–47 (March 2016). https://doi.org/10.1109/IMMERSIVE.2016.7932382
7. HÁMORNIK, B.P., KRASZNAY, C.: Prerequisites of virtual teamwork in security operations centers: Knowledge, skills, abilities and other characteristics. Academic and Applied Research in Military and Public Management Science p. 73 (2017)
8. Kabil, A., Duval, T., Cuppens, N., Le Comte, G., Halgand, Y., Ponchel, C.: 3D CyberCOP: a Collaborative Platform for Cybersecurity Data Analysis and Training. In: Luo, Y. (ed.) 15th International Conference on Cooperative Design, Visualization and Engineering. pp. 176–183. Cooperative Design, Visualization, and Engineering, Springer, Hangzou, China (Oct 2018), https://hal.archives-ouvertes.fr/hal-01831965, in proceedings of CDVE 2018 (15th International Conference on Cooperative Design, Visualization and Engineering), Springer, p. 176-183, Hangzhou, China, October 21-24, 2018
9. Kabil, A., Duval, T., Cuppens, N., Le Comte, G., Halgand, Y., Ponchel, C.: From Cyber Security Activities to Collaborative Virtual Environments Practices through the 3D CyberCOP Platform. In: International Conference on Information Systems Security. pp. 272–287. proceedings of ICISS 2018, 14th International Conference on Information Systems Security, Bengaluru, India (Dec 2018), https://hal.archives-ouvertes.fr/hal-01892161
10. Kabil, A., Duval, T., Cuppens, N., Le Comte, G., Halgand, Y., Ponchel, C.: Why should we use 3D Collaborative Virtual Environments for Cyber Security? In: IEEE Fourth VR International Workshop on Collaborative Virtual Environments (IEEEVR 2018). Reutlingen, Germany (Mar 2018), https://hal.archives-ouvertes.fr/hal-01770064

11. McKenna, S., Staheli, D., Meyer, M.: Unlocking user-centered design methods for building cyber security visualizations. In: Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on. pp. 1–8. IEEE (2015)
12. Mohurle, S., Patil, M.: A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science **8**(5) (2017)
13. Pahi, T., Leitner, M., Skopik, F.: Data exploitation at large: your way to adequate cyber common operating pictures. In: Proceedings of the 16th European Conference on Cyber Warfare and Security. pp. 307–315 (2017)
14. Salzman, M.C., Dede, C., Loftin, R.B.: Vr's frames of reference: A visualization technique for mastering abstract multidimensional information. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 489–495. CHI '99, ACM, New York, NY, USA (1999). https://doi.org/10.1145/302979.303141, http://doi.acm.org/10.1145/302979.303141
15. Sebok, A., Nystad, E., Droivoldsmo, A.: Improving safety and human performance in maintenance and outage planning through virtual reality-based training systems. In: Proceedings of the IEEE 7th Conference on Human Factors and Power Plants. pp. 8–8 (Sep 2002). https://doi.org/10.1109/HFPP.2002.1042867
16. Sethi, A., Wills, G.: Expert-interviews led analysis of eevi - a model for effective visualization in cyber-security. In: 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). pp. 1–8 (Oct 2017). https://doi.org/10.1109/VIZSEC.2017.8062195
17. Staheli, D., Mancuso, V., Harnasch, R., Fulcher, C., Chmielinski, M., Kearns, A., Kelly, S., Vuksani, E.: Collaborative data analysis and discovery for cyber security. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association, Denver, CO (2016), https://www.usenix.org/conference/soups2016/workshop-program/wsiw16/presentation/staheli
18. Sundaramurthy, S.C., McHugh, J., Ou, X., Wesch, M., Bardas, A.G., Rajagopalan, S.R.: Turning contradictions into innovations or: How we learned to stop whining and improve security operations. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). pp. 237–251. USENIX Association, Denver, CO (2016), https://www.usenix.org/conference/soups2016/technical-sessions/presentation/sundaramurthy
19. Takahashi, T., Kadobayashi, Y., Nakao, K.: Toward global cybersecurity collaboration: Cybersecurity operation activity model. In: Proceedings of ITU Kaleidoscope 2011: The Fully Networked Human? - Innovations for Future Networks and Services (K-2011). pp. 1–8 (Dec 2011)
20. Varga, M., Winkelholz, C., Träber-Burdin, S.: The application of visual analytics to cyber security (2017)
21. Zhang, S., Shi, R., Zhao, J.: A visualization system for multiple heterogeneous network security data and fusion analysis. KSII Transactions on Internet & Information Systems **10**(6) (2016)
22. Zhong, C., Yen, J., Liu, P., Erbacher, R.F., Garneau, C., Chen, B.: Studying Analysts' Data Triage Operations in Cyber Defense Situational Analysis, chap. 2, pp. 128–169. Springer International Publishing, Cham (2017)
23. Zhong, Z., Zhao, Y., Shi, R., Sheng, Y., Liu, J., Meng, H., Lin, D.: A user-centered multi-space collaborative visual analysis for cyber security. Chinese Journal of Electronics **27**(5), 910–919 (2018). https://doi.org/10.1049/cje.2017.09.021