From Cyber Security Activities to Collaborative Virtual Environments Practices through the 3D CyberCOP Platform

Alexandre Kabil[1], Thierry Duval[1], Nora Cuppens[1], Gérard Le Comte[2], Yoran Halgand[3], and Christophe Ponchel[4]

[1] IMT Atlantique, UBL, Lab-STICC, UMR CNRS 6285
{surname.name}@imt-atlantique.fr
[2] Societe Generale {surname.name}@socgen.com
[3] EDF {surname.name}@edf.fr
[4] AIRBUS Defence and Space {surname.name}@airbus.com

Abstract. Although collaborative practices between cyber organizations are well documented, managing activities within these organizations is still challenging as cyber operators tasks are very demanding and usually done individually. As human factors studies in cyber environments are still difficult to perform, tools and collaborative practices are evolving slowly and training is always required to increase teamwork efficiency. Contrary to other research fields, cyber security is not harnessing yet the capabilities of Collaborative Virtual Environments (CVE) which can be used both for immersive and interactive data visualization and serious gaming for training. In order to tackle cyber security teamwork issues, we propose a 3D CVE called the 3D Cyber Common Operational Picture, which aims at taking advantage of CVE practices to enhance cyber collaborative activities.
Based on four Security Operations Centers (SOCs) visits we have made in different organizations, we have designed a cyber collaborative activity model which has been used as a reference to design our 3D CyberCOP platform features, such as asymetrical collaboration, mutual awareness and roles specialization. Our approach can be adapted to several use cases, and we are currently developing a cyber incident analysis scenario based on an event-driven architecture, as a proof of concept.

Keywords: Cybersecurity · Collaborative Interaction · Virtual Reality.

1 Introduction

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect organizations and users assets [36]. Because every organization, nation and company is subject to cyber threats, collaborative strategies and policies are required to manage effective cyber defence activities, but they are still difficult to develop [16]. Moreover, teamwork within organizations is still challenging,

as training sessions are time demanding and cyber security tools and softwares are often made for individual use. Far from pop culture stereotypes, cyber operators use classical Command Line Interfaces (CLI) and Graphical User Interfaces (GUI) to detect incidents and cyber threats such as the ELK stack[5], whereas other domains look at Natural User Interfaces (NUI) or even Immersive Analytics solutions to facilitate information sharing between users and even training practices [9].

In this paper we present a Collaborative Virtual Environment (CVE) called the 3D Cyber Common Operational Picture, which aims at enhancing cyber teamwork by applying design methods derived from CVE usages.

We will put the emphasis on how we have integrated cyber security collaborative practices into our CVE and how this general approach could work for several use cases including cyber incident analysis simulations.

In section 2 we will show that as collaboration between and within organizations is an important topic in cyber security, CVEs could tackle cyber teamwork effectiveness issues by providing shared environments and practices. Then in section 3 we will present the cyber collaborative activity model we have conceived by visiting Security Operations Centers (SOCs) and how we have managed to adapt its features to CVEs design practices through our 3D Cyber Common Operational Picture platform. Finally we will detail in section 4 the cyber incident analysis scenario we are still working on based on an event driven architecture, and we will conclude by perspectives of our approach.

2 Collaborative Practices in Cyber Security

As more and more data are generated and collected on networks and infrastructures, cyber security can not be effective without proper collaboration at different scales, from employees (experts and non-experts) to companies, organizations or even countries. As cyber world is not bounded by geographical limits, productivity and telepresence tools such as visioconference or virtual environments are effective when people need to share knowledge, data or experiences but these tools require specific learning methods and workflows.

2.1 Collaboration management in Cyber security organizations

Cyber collaboration is managed at different scales, from nation to private companies, with respect to threats gravity, strategic implications and trust policies, as shown by Petersen and Tjalve [26]. In order to coordinate cyber actions, specific structures such as Security Operations Centers (SOCs) or Computer Emergency Response Teams (CERTs) are well defined and standardized (such as the MITRE guide for example [6]). But even if collaborative strategies exist, communication is still difficult between organizations [39], and at employees level, practices and

[5] https://www.elastic.co/fr/elk-stack

[6] https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/ten-strategies-for-becoming-a-world-class

processes are often individual: analysts get tickets to observe, monitor and report incidents, and if they need to ask advice from others, they forward tickets or they communicate information in a tacit way [2]. Moreover, some structures such as SOCs are considered both organizations and teams, which changes the way of organizing processes and work practices [15].

As Rajivan and Cooke explain [28], teamwork effectiveness evaluation is a challenging task as it is more than the evaluation of each team member's Cyber Situational Awareness (CSA) capabilities. Working efficiently among a team requires specific collaborative tools and training sessions, which are not always available to cyber operators.

To fill this gap between collaborative expectations and cyber operators workflows, Computer Supported Cooperative Work (CSCW) systems such as Collaborative Virtual Environments (CVE) could be used in order to help users to share knowledge and develop understanding of each others' tasks [7].

2.2 Virtual Environments for Cyber security

Although there are some research papers about 3D metaphors for data representations in cyber security [12, 20] or about the usability of Virtual Environments for cyber teamwork [24, 27, 31], applying User Experience (UX) design for cyber security is quite recent [29], and the usefulness of 3D representations is just now accepted [8, 1] which explains maybe why we have not seen much 3D visualizations for cyber security in reviews of literature [34, 13], apart from the 2012 Daedalus-Viz project developed by Inoue et al. [17].

Moreover, experts cyber security tools face a paradox: they need to be simple enough in order to help analysts to understand what is going on on the network and they need to be precise enough to help them investigating incidents. CVEs and Immersive Analytics solutions can help solving these problems by either providing separate views towards different analysts but letting them having a common ground, or proposing aggregated 3D interactive data representations that can give more information [6, 14].

Another interesting aspect of CVEs is that they are considered useful for learning [10, 33], and they could be used to enhance existing cyber training tools which are still very technical or based on serious-gaming approaches[3, 30].

We think that CVEs for cyber security should blend educational or serious-gaming approaches and data analysis visualizations as these points are still difficult to manage in cyber organizations [18]. As shown in the Figure 1, ouar approach aims at providing both data visualization and training scenarios by immersing cyber operators into environments where they will be able to collaborate with respect to their organizational practices to perform specific activities.

3 Collaborative model and CVE design

In order to understand cyber security collaborative practices, we have had the opportunity to visit four SOCs of our industrial partners.

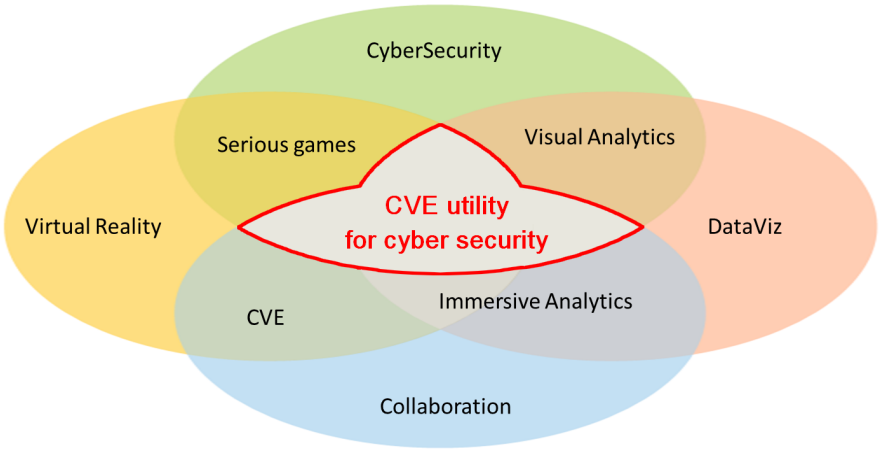


Fig. 1. Venn diagram of our approach combining collaboration, virtual reality and data visualization for cyber security.

We have seen that even if structures' organizations were different, we have been able to define a generic collaborative activity model that can be used to describe and model cyber security practices.

3.1 SOC Activity Analysis

SOCs are structures where networks are constantly monitored in real-time by analysts, who are separated in three technical levels and who investigate incidents either for client companies or for internal security. SOCs practices are studied either from the human factor or the organizational point of view [39, 38, 15], but as cyber security is by definition a confidential field it is still difficult to record data for making activity analysis. As a consequence, our visits were only one day long and we have not been able to record audio or video, but even with these limitations we were able to get some relevant findings on how SOC operators are working as a team. Day to day SOC's operators work relies on getting aware of alerts from cyber security sensors, suppressing false positive alerts, analyzing network meta-data and application logs, creating incident reports and exchanging information and requests with customer teams (network, security, decision). They need to work quickly, so if they consider that an incident is out of their technical scope, they forward it to an expert (escalation process).

We found out that operators work usually alone by taking tickets from the Security Information and Event Management (SIEM) tool, backbone of SOCs, which collects different kinds of data, analyses them and raises alerts (with a quite significant rate of false positives).

Moreover, collaboration is not so much mediated as operators exchange directly between them or during meetings with managers and decision-makers. As

a consequence, some of them have expressed the needs for better user-adapted visualization tools that will allow them to share information and even to interact simultaneously on datasets.

We could classify SOC employees roles by their decision-making and network analysis capabilities: analysts have to get information and report it to coordinators who can take decisions or ask for remediation actions [23].

All these findings helped us to define a cyber collaborative activity model which will be used to adapt current practices to 3D CVE usages (Figure 2):

Model features	SOC Activities
Roles	Tradeoff between decision and data analysis, hierarchical interactions
Tasks	Ticketing system, specific tasks
Visualizations	Several tools for monitoring, correlation and reporting
Data	Aggregated by SIEMs or from various sources (probes, logs…)
Explicit Collaboration	**Ticketing, processes, messages, reports**
Tacit Collaboration	**Communication, 'over the shoulder' interaction**

Fig. 2. Activity model designed for cyber security practices analysis.

- **Roles**: describes the hierarchical structure and the specific missions of operators.
- **Tasks**: describes how operators are working. Tasks are related to roles and data.
- **Visualizations**: concerns the fact that operators are using plenty of tools to monitor, observe and report cyber events. Objectives or tools are to correlate data in order to get a 'big picture', or Cyber Situational Awareness (CSA).
- **Data**: is available through SIEMs (aggregation of data) or logs from different sensors (raw data). When SIEM's information are insufficient, operators have to dig into specific chunks of data.
- **Explicit Collaboration**: concerns the actual processes of ticketing and reporting. Operators act only if they get a ticket and they coordinate their actions to close this ticket as quickly as possible.

– **Implicit Collaboration**: is effective as operators works in open-space environments and can discuss and ask for help in a informal way.

We have separated collaboration features into explicit and implicit categories as some collaborative activities were not part of operators' tasks but were more 'tacit' [2].

This model does not cover every aspect of tasks, data, roles and features needed for a visualization for cyber security as proposed by EEvi [32], but it will help us to determine our 3D Cyber Common Operational Picture features by taking inspiration from CSA taxonomies and models such as the ones from Evesti, Kanstren and Frantti [19, 11]

3.2 3D CyberCOP Platform

As shown in figure Figure 3, our activity model aims at proposing cyber operators adapted visualizations according to their individual (black arrows) and collaborative (red arrows) practices and interactions: individual interactive systems will be enhanced to make them collaborative and/or more immersive with collaborative interactions mediated by the systems (green arrows), and the level of immersion (Virtual Reality, Windows, Icons, Menu and Pointers (WIMP), post-WIMP interfaces) will be adapted to user's roles (for example an analyst and a coordinator will respectively use a Virtual Reality Headset and tactile wide screen).

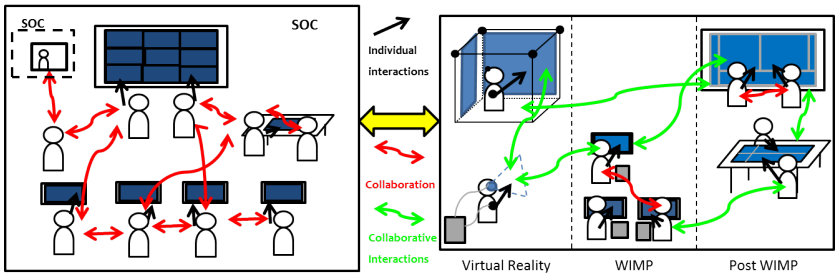


Fig. 3. SOC practices (Left) and their adaptation through the 3D CyberCOP platform (Right).

Roles will have specific visualizations and interaction capabilities according to their needs and tasks and one user can only have one role at a time (User 1 who plays role A can see only incident information and can only investigate network incidents whereas user 2 in role B has information about risk assessment or regulation policies). Roles will be bounded by hierarchical links, which could be strict (Role A should always wait orders from Role B) or loose (Role A and B should exchange freely information).

Tasks will be coordinated by a ticketing or alerting system: users will have to get tickets in order to execute actions related to their roles (for example an analyst will have to ask permissions for investigating specific assets and coordinator will have to confirm an escalation process). Actions could be defined by experts or more generally by cyber security tasks analysis as [39] or [32].

Visualizations will be 2D, 3D or Immersive, as shown in figure Figure 3. These visualizations will get filters with respects to roles and situations. Filters will for example display only network or kinetic related information (for example network topologies and IP addresses, employees' login lists, geographical position of workstations etc..), as in the solution proposed by Zhong *et al.* [41]. Existing visualization or data analysis tools could be used too if they have a proper communication API.

Data will be for the moment simulated or simplified: is it still cumbersome to represent whole network architectures in 3D or to manage Gigabytes of data so as for the visualizations we will let the opportunity to use existing tools to get realistic data to our platform.

Explicit collaboration will be done by displaying role-related avatars which will not necessarily be on the same scale: real-time analysts will be able to work together in a human-like scale by being immersed in offices whereas a Strategic analyst scale will be much bigger in order to get more high-level information. CVEs allows us to do Asymmetric Collaboration [21] where users could act at different scales from an environment and still get a notion of 'presence' of the others called the 'Mutual Awareness' [21]. Users will be able to share information with different visual feedback, for example analysts will see each other User Interfaces (UIs) and actions because they share the same visual scale whereas a coordinator will appear as a highlight of a whole floor or building, in order to make others understand that she have a global view of the situation.

Tacit collaboration will be available through oral communication and an historic logger of all users' actions: this will allow any user to know what is happening without needing to use the ticketing system (for example a coordinator will be able to follow analysts' actions through the historic). Users will also be able to hide some information, in order to select what they want to share, in a "What I See Is Not What You See" approach [42] (an analyst will be able to interact within the environment without raising historical logger).

Collaborative cues proposed in our 3D CyberCOP platform (shared context, awareness, communication, multiple viewpoints,) are also inspired from [35], from the Information Visualization community. The Figure 7 'CVE Design solutions' column sums up our design choices for the adaptation of our cyber security activity model into a CVE. We propose simple yet effective features for managing collaboration and we let the opportunity to use existing solutions for the Tasks, Visualization and Data parts as cyber tools are evolving quickly.

In order to instantiate our 3D CyberCOP model and to implement our features, we are developing a collaborative cyber incident analysis simulation based on a malware propagation modelling.

4 3D CyberCOP Use Case: Cyber Incident Analysis Scenario

By considering that incident analysis requires different points of view and specific datasets to evaluate a situation and after discussing with SOCs operators and our industrial partners, we have decided to choose a ransomware propagation analysis scenario as a simple use case to test our approach. We have built this scenario by using an event-driven architecture which have helped us to implement our activity model's features.

4.1 Ransomware Propagation Analysis Scenario

By taking inspiration from the Wannacry [7] attack that occurred in May 2017, we have decided to develop a ransomware propagation scenario by simulating malicious behaviors and investigations activities. Users' objective is to find the vulnerabilities that allow both the file encryption and the propagation through a small office network where workstations have different characteristics (different Operating Systems and known vulnerabilities, different levels of criticity etc..). Ransomware behavior is determined by two simulated metrics, namely the Entropy and the Network Anomaly:

- The **entropy metric** represents the file's system activity of an asset. It increases when files are being encrypted either in a legitimate or malicious way. When this metric reaches a limit, an alert is raised in the system and users will have to investigate to determine the causes of this alert.
- The **network anomaly metric** represents an unusual network activity of an asset which once again can be legitimate or due to a mistake (backup request or peer to peer download) or a malware propagation after a port scan attack (SMB exploit that scans port 445 for example).

With addition to these metrics, ransomware behavior is linked to specific simulated assets vulnerabilities[8]: the ransomware contaminates assets if and only if they have an old version of Windows (patched before march 2017), no direct access to internet and a SMB exploit available.

At the beginning of the simulation, an asset is infected by the ransomware. As a consequence, an entropy alert is raised while the concerned asset sees its entropy metrics reach a threshold. After a certain amount of time, a network alert is raised due to a high value of the network anomaly metric, as the ransomware propagates itself through exploits. If the ransomware successfully propagates, infected assets see their entropy metric increase, and again alerts are raised, and the infection continues until all assets are infected. To add false positive alerts, some assets will perform a daily encryption and backup which will raise entropy and network anomaly levels. Users will have to determine if the raised alerts are

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

[8] https://www.us-cert.gov/ncas/alerts/TA17-132A

from incidents or from false positives. With respect to their roles, they will have various information sources (cyber and kinetic views, alerts information) and collaboration will be necessary in order to characterize the incidents in an efficient way (by crossing information from different sources). To easily implement this scenario, we have used an event-driven architecture that helped us managing ransomware behaviors, users interactions, data visualization and simulation scenario progression.

4.2 Event-Driven Architecture

Event-driven architectures designates an asynchronous programming method where any action of the environment raises events which need to be caught to call functions. Events are not linked to a platform or a user, and the action of catching it (or to listen to it) determines the consequences. For example, clicking on a button could raise a 'Select' event, and according to the system's state, the selection function could be called or not. In our case, we have defined a parameterized event system, and we will give detail about users events (system events works the same).

Users interactions within the simulation (with objects or User Interfaces buttons) raises events like

$$UserEvent(objectId, env, action, userId, alertNumber) \tag{1}$$

where :

- *objectId* is the object on which the event should occur (e.g. Selection of the asset number three). When a user event is raised, every asset of the simulation gets it and launches actions if it is concerned by this event (for example deactivation of the previously selected asset).
- *env* gives the information on the type of objects this event is related to (for example network nodes and workstations are two different kinds of objects even if they are related to the same asset).
- *action* describes which action was triggered. These tasks (e.g. Selection, Information, Incident Declaration) and modify the scenario progression and the state of the simulation.
- *userId* transmits a reference to the user/role that has launched this event. This parameter allows us to manage the different feedback of actions and to display them with respect to different roles. This parameter can modify the scenario progression.
- *alertNumber* allows users to investigate several tickets at a time and to interact according to specific alerts. A user can get information of any asset for example, but if she is working on a specific ticket, her interaction will have different consequences (scenario update, feedback, and so on).

For example, if user 1 is selecting the cyber object of the asset 3 to investigate the network information required by the ticket 2, user event raised will be:

$$UserEvent(3, cyber, netinfo, 1, 2) \tag{2}$$

This event architecture gives us flexibility to manage our 3D CyberCOP features. For example, we can add extra visual feedback if needed or we can control the investigation procedure more strictly by waiting specific actions updating the cyber scenario. Events are not bounded to a specific device and we can trigger them from a 2D tactile display or from a Virtual Reality device. Based on this architecture, we have built the scenario and implemented our activity model features with respect to CVE design features presented before.

4.3 Activity Model Implementation

- We have decided to implement two roles in this simulation :
  - an **analyst** will have to investigate assets and to work on tickets given by a **coordinator**. She is immersed in Virtual Environment but can use a classical dashboard if needed.
  - a **coordinator** will have to transfer tickets to **analysts** and to decide if the alerts should be escalated. She will use a 2D dashboard to do so (but again she can use immersive visualization if needed).

  These roles will have to respect hierarchical interactions: an analyst cannot investigate an asset if she has not get a ticket and a coordinator could not validate an alert if she has not get the analyst's report. Users with same roles will have the same capabilities.
- Users will have to perform tasks in a precise order to progress through the scenario (Figure 4). First, the coordinator selects an alert and transmits it to an analyst. Then, an analyst who accepts the alert ticket investigates by selecting the concerned asset and the right information (kinetic or cyber) she needs, and then performs an analysis action through a UI. After that, she sends the analysis report to the coordinator via a reporting action on the UI. When the coordinator receives the report, she can validate it or ask for more information. Once she has all information, she escalates the alert to incident or she discards it if it is a false positive. When several assets are compromised (e.g. concerned by incidents), analysts and coordinators could filter assets information in order to find common points or differences between them. These information will be selected on a specific UI to determine if they have found the ransomware attack vectors.
- Users will be able to use 2D, 3D and immersive visualizations according to their roles or needs. Moreover, we will separate the simulation between two environments, the kinetic and the cyber one (Figure 6 top left and right views).
  - The kinetic environment represents a physical view of the network office, with workstations, office floors and rooms. When users navigate through this environment, they get information about assets entropy level, working processes, login of the last user etc...
  - The cyber environment represents the networked information. Users actions and visualizations will be about network topology, IP Addresses and so on.

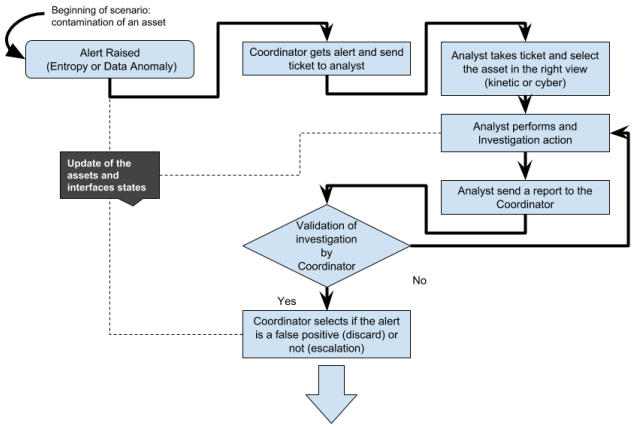


Fig. 4. Alert analysis management from the ticket to escalation.

Users will have to get information from these two environments in order to determine the nature of the alert and to have a global view of an asset state.

- Two metrics will be monitored: entropy and network anomalies. Users will get data from assets by selecting them and choosing an action through their graphical interfaces. Assets information are provided by a pre-defined scenario.
- To manage the ticketing feature, an alert list will be provided to the Coordinator who have to transfer them to Analysts. Tickets states allow users to know what others are doing. Coordinator will have a 2D map to follow analysts movements (Figure 5) and these analysts will have human-like avatars and visible pointers such as feedback and feedforward features. Feedback and feedforward are discrete and continuous interactions cues that allows mutual awareness. Feedback is the information of a consequence of an action (e.g. a visual highlight when a user is selecting an asset as is the right image of the Figure 5) and feedforward is the information of the action itself (e.g. the view of a users' pointer moving through the environment). These cues are various and with co-presence and the ticketing system they allow users to perform explicit collaboration. Moreover, all users will have information about the scenario's progression.
- Users will be co-located in the same physical area to perform the simulation. They will be allowed to communicate naturally and any role will have an event log where every users' actions will be displayed. Filtering this log will give insights on the actions performed by anyone.

  Users will have the opportunity to share or not their UI and their interactions: if a user wants to explain what she has done, she can show her UI to others or she can hide the fact that she is selecting an asset in order to get information.

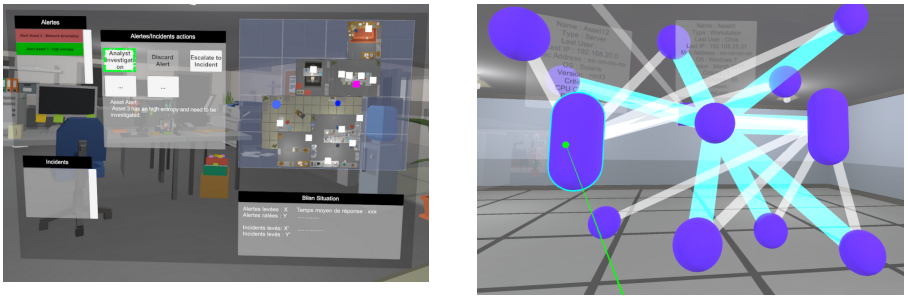


Fig. 5. 2D coordinator dashboard with a map of the environment and a list of current alerts (LEFT) and a selection of an asset from an immersive graph representation of the network (RIGHT).

On the left top of the Figure 6 a cyber representation of the environment is displayed from an analyst point of view. She has selected an asset which has malicious processes and so she is encouraged to declare the incident to the coordinator that has given her this alert. The right top image represents the same asset but seen from the kinetic environment: information are different and so actions. Both bottom images of the Figure 6 shows cyber and kinetic 2D views of the environment (respectively a graph representation of the network and a map of the environment). These views provide either topological and network information or IT-oriented data (last user, OS, running processes etc..)

The bottom view of Figure 6 is a 2D dashboard available for the coordinator: she can select assets from the top left list, she can follow analysts' movements on the map and she has specific actions regarding alerts she has selected.

This simulation is made by using the Unity Game Engine, and is still under development.

5 Conclusion

We have proposed in this paper a 3D CVE model called the 3D Cyber Common Operational Picture, which aims at taking advantage of best CVE practices to enhance cyber collaborative activities. From the cyber collaborative activity model we built, we have selected relevant CVE characteristics that can be used to implement our models features. We are still developing a proof of concept scenario which instantiate these features (last column of figure Figure 7). Evaluation of such platforms is complex as it tackles several issues such as cybersecurity skills learning [22], cyber security visualization [37], role adaptation from specifications [25], Computer Supported Collaborative Work (CSCW) [4, 5] or Team Cyber Situational Awareness [28] and User Experience [40]. We will evaluate differently our theoretical approach and our proposed simulation in order to get information of future refinements of the cyber or the CVE model.

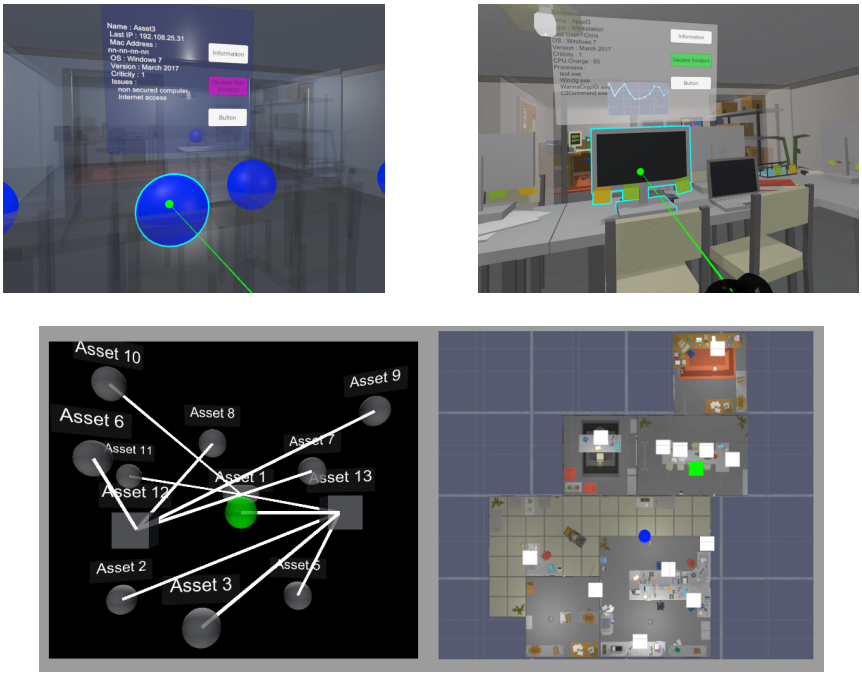


Fig. 6. Cyber (LEFT) and Kinetic (RIGHT) views of the environment, displayed using immersive (TOP) and non-immersive (BOTTOM) setups.

References

1. A., W.F.J., C.M.D.S., F., L., N.: Virtualdesk: A comfortable and efficient immersive information visualization approach. Computer Graphics Forum **37**(3), 415–426 (2018). https://doi.org/10.1111/cgf.13430, https://onlinelibrary.wiley.com/doi/abs/10.1111/cgf.13430
2. Ahrend, J.M., Jirotka, M., Jones, K.: On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge. In: 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA). pp. 1–10 (June 2016). https://doi.org/10.1109/CyberSA.2016.7503279
3. Alotaibi, F., Furnell, S., Stengel, I., Papadaki, M.: A review of using gaming technology for cyber-security awareness. International Journal for Information Security Research (IJISR) **6**(2), 660–666 (June 2016)
4. Antunes, P., Herskovic, V., Ochoa, S.F., Pino, J.A.: Structuring dimensions for collaborative systems evaluation. ACM Comput. Surv. **44**(2), 8:1–8:28 (Mar 2008). https://doi.org/10.1145/2089125.2089128, http://doi.acm.org/10.1145/2089125.2089128
5. Antunes, P., Herskovic, V., Ochoa, S.F., Pino, J.A.: Reviewing the quality of awareness support in collaborative applications. Journal of Systems and Software **89**, 146 – 169 (2014). https://doi.org/https://doi.org/10.1016/j.jss.2013.11.1078, http://www.sciencedirect.com/science/article/pii/S0164121213002756

	SOC	XXXXX Platform	Exemple Scenario
Roles	Tradeoff between decision and data analysis, hierarchical interactions	Users with specific visualizations and actions, Hierarchical interactions	Analyst immersed in VR, Coordinator with 2D Dashboard
Tasks	Ticketing system, specific tasks	Ticketing system, simulated interactions or experts scenarios	Simulated actions for collaborative incident analysis
Visualizations	Several tools for monitoring, correlation and reporting	2D, 3D or Immersive filtered views, integration of existing tools	2D and Immersive views, kinetic and cyber filters
Data	Aggregated by SIEMs or from various sources (probes, logs…)	Simulated data sets, simplified metrics or integration with cyber range tools	Simulated by two metrics, entropy and network anomalies
Explicit Collaboration	**Ticketing, processes, e-mails, reports**	**Ticketing, avatars, mutual awareness, Information sharing**	**Alerts list, Feedbacks and feedforward, copresence, deterministic scenario**
Tacit Collaboration	**Communication, 'over the shoulder' interaction**	**Communication, historic logger, information sharing**	**Co localisation, events logger, information distribution**
FEATURES	**Activity Model**	**CVE Design solutions**	**Instance of the model**

Fig. 7. Features adaptation from cyber security usages to CVE implementation.

6. Chandler, T., Cordeil, M., Czauderna, T., Dwyer, T., Glowacki, J., Goncu, C., Klapperstueck, M., Klein, K., Marriott, K., Schreiber, F., et al.: Immersive analytics. In: Big Data Visual Analytics (BDVA), 2015. pp. 1–8. IEEE (2015)
7. Churchill, E.F., Snowdon, D.: Collaborative virtual environments: An introductory review of issues and systems. Virtual Reality **3**(1), 3–15 (Mar 1998). https://doi.org/10.1007/BF01409793, https://doi.org/10.1007/BF01409793
8. Cliquet, G., Perreira, M., Picarougne, F., Prié, Y., Vigier, T.: Towards hmd-based immersive analytics. In: Immersive analytics Workshop, IEEE VIS 2017. Phoenix, United States (Oct 2017), https://hal.archives-ouvertes.fr/hal-01631306
9. Donalek, C., Djorgovski, S.G., Cioc, A., Wang, A., Zhang, J., Lawler, E., Yeh, S., Mahabal, A., Graham, M., Drake, A., Davidoff, S., Norris, J.S., Longo, G.: Immersive and collaborative data visualization using virtual reality platforms. In: 2014 IEEE International Conference on Big Data (Big Data). pp. 609–614 (Oct 2014). https://doi.org/10.1109/BigData.2014.7004282
10. Eller, C., Bittner, T., Dombois, M., Rüppel, U.: Collaborative immersive planning and training scenarios in vr. In: Smith, I.F.C., Domer, B. (eds.) Advanced Computing Strategies for Engineering. pp. 164–185. Springer International Publishing, Cham (2018)
11. Evesti, A., Kanstrn, 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
12. Gros, P., Abel, P., Dos Santos, R., Loisel, D., Trichaud, N., Paris, J.: Experimenting service-oriented 3d metaphors for managing networks using virtual reality. In: Laval Virtual–Virtual Reality International Conference (May 2000)
13. Guimaraes, V.T., Freitas, C.M.D.S., Sadre, R., Tarouco, L.M.R., Granville, L.Z.: A survey on information visualization for network and service management. IEEE Communications Surveys & Tutorials **18**(1), 285–323 (2016)

14. 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
15. 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)
16. Hui, P., Bruce, J., Fink, G., Gregory, M., Best, D., McGrath, L., Endert, A.: Towards efficient collaboration in cyber security. In: 2010 International Symposium on Collaborative Technologies and Systems. pp. 489–498 (May 2010). https://doi.org/10.1109/CTS.2010.5478473
17. Inoue, D., Eto, M., Suzuki, K., Suzuki, M., Nakao, K.: Daedalus-viz: Novel real-time 3d visualization for darknet monitoring-based alert system. In: Proceedings of the Ninth International Symposium on Visualization for Cyber Security. pp. 72–79. VizSec '12, ACM, New York, NY, USA (2012). https://doi.org/10.1145/2379690.2379700, http://doi.acm.org/10.1145/2379690.2379700
18. Kabil, A., Thierry, D., Nora, C., Gerard, L., Yoran, H., Christophe, P.: Why should we use 3d collaborative virtual environments (3dcve) for cyber security? In: 2018 IEEE Third VR International Workshop on Collaborative Virtual Environments (3DCVE) (March 2018)
19. Kanstrn, T., Evesti, A.: A study on the state of practice in security situational awareness. In: 2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). pp. 69–76 (Aug 2016). https://doi.org/10.1109/QRS-C.2016.14
20. Latvala, O.M., Kernen, T., Noponen, S., Lehto, N., Sailio, M., Valta, M., Olli, P.: Visualizing network events in a muggle friendly way. In: 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). pp. 1–4 (June 2017). https://doi.org/10.1109/CyberSA.2017.8073400
21. Le Chénéchal, M., Chalmé, S., Duval, T., Royan, J., Gouranton, V., Arnaldi, B.: Toward an enhanced mutual awareness in asymmetric cve. In: Proceedings of International Conference on Collaboration Technologies and Systems (CTS 2015) (2015)
22. Mäses, S., Randmann, L., Maennel, O., Lorenz, B.: Stenmap: Framework for evaluating cybersecurity-related skills based on computer simulations. In: Zaphiris, P., Ioannou, A. (eds.) Learning and Collaboration Technologies. Learning and Teaching. pp. 492–504. Springer International Publishing, Cham (2018)
23. 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)
24. Michel, M.C.K., Helmick, N.P., Mayron, L.M.: Cognitive cyber situational awareness using virtual worlds. In: 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). pp. 179–182 (Feb 2011). https://doi.org/10.1109/COGSIMA.2011.5753440
25. Newhouse, W., Keith, S., Scribner, B., Witte, G.: National initiative for cybersecurity education (nice) cybersecurity workforce framework. NIST Special Publication **800**, 181 (2017)
26. Petersen, K.L., Tjalve, V.S.: Intelligence expertise in the age of information sharing: publicprivate collection and its challenges to democratic control and accountability. Intelligence and National Security

33(1), 21–35 (2018). https://doi.org/10.1080/02684527.2017.1316956, https://doi.org/10.1080/02684527.2017.1316956
27. Pirker, J., Gütl, C.: Virtual worlds for 3d visualizations. In: 11th international conference on intelligent environments (Workshop). pp. 265–272 (2015)
28. Rajivan, P., Cooke, N.: Impact of Team Collaboration on Cybersecurity Situational Awareness, pp. 203–226. Springer International Publishing, Cham (2017)
29. Renaud, K., Flowerday, S.: Contemplating human-centred security & privacy research: Suggesting future directions. Journal of Information Security and Applications **34**, 76 – 81 (2017). https://doi.org/https://doi.org/10.1016/j.jisa.2017.05.006, http://www.sciencedirect.com/science/article/pii/S2214212617302387, human-Centred Cyber Security
30. Richards, D., Taylor, M.: A comparison of learning gains when using a 2d simulation tool versus a 3d virtual world. Comput. Educ. **86**(C), 157–171 (Aug 2015). https://doi.org/10.1016/j.compedu.2015.03.009, http://dx.doi.org/10.1016/j.compedu.2015.03.009
31. Robinson, M., Jones, K., Janicke, H., Maglaras, L.: Developing Cyber Peacekeeping: Observation, Monitoring and Reporting. ArXiv e-prints (Jun 2018)
32. 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
33. Shen, C.w., Ho, J.t., Ly, P.T.M., Kuo, T.c.: Behavioural intentions of using virtual reality in learning: perspectives of acceptance of information technology and learning style. Virtual Reality (May 2018). https://doi.org/10.1007/s10055-018-0348-1, https://doi.org/10.1007/s10055-018-0348-1
34. Shiravi, H., Shiravi, A., Ghorbani, A.A.: A survey of visualization systems for network security. IEEE Transactions on visualization and computer graphics **18**(8), 1313–1329 (2012)
35. Soares, A.G., dos Santos, C.G., de Paula Mendonca, S., Carneiro, N.J., Miranda, B.P., de Araujo, T.D., de Freitas, A.A., de Morais, J.M., Meiguins, B.S.: A review of ways and strategies on how to collaborate in information visualization applications. In: 2016 20th International Conference Information Visualisation (IV). vol. 00, pp. 81–87 (July 2016). https://doi.org/10.1109/IV.2016.69, doi.ieeecomputersociety.org/10.1109/IV.2016.69
36. von Solms, R., van Niekerk, J.: From information security to cyber security. Computers & Security **38**, 97 – 102 (2013), cybercrime in the Digital Economy
37. Staheli, D., Yu, T., Crouser, R.J., Damodaran, S., Nam, K., O'Gwynn, D., McKenna, S., Harrison, L.: Visualization evaluation for cyber security: Trends and future directions. In: Proceedings of the Eleventh Workshop on Visualization for Cyber Security. pp. 49–56. VizSec '14, ACM, New York, NY, USA (2014). https://doi.org/10.1145/2671491.2671492, http://doi.acm.org/10.1145/2671491.2671492
38. 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

39. 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)
40. TCHA-TOKEY, K., CHRISTMANN, O., Loup-Escande, E., Richir, S.: Proposition and Validation of a Questionnaire to Measure the User Experience in Immersive Virtual Environments. The International Journal of Virtual Reality **16**(1), 33–48 (2016), https://hal.archives-ouvertes.fr/hal-01404497
41. 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**, 910–919 (September 2018)
42. Zhu, H.: From wysiwis to wisinwis: role-based collaboration. In: 2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No.04CH37583). vol. 6, pp. 5441–5446 vol.6 (Oct 2004). https://doi.org/10.1109/ICSMC.2004.1401059