3D CyberCOP: a Collaborative Platform for Cybersecurity Data Analysis and Training

Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand, Christophe Ponchel

3D CyberCOP: a Collaborative Platform for Cybersecurity Data Analysis and Training

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 Immersive Analytics solutions are now developed in order to ease data analysis, cyber security systems are still using classical graphical representations and are not harnessing yet the potential of virtual reality systems and collaborative virtual environments. 3D Collaborative Virtual Environments (3DCVE) can be used in order to merge learning and data analysis approaches, as they can allow users to have a better understanding of a cyber situation by mediating interactions towards them and also by providing different points of view of the same data, on different scales. So we propose a 3D Cyber Common Operational Picture (3D CyberCOP) that will allow operators to face together a situation by using immersive and non immersive visualizations and by collaborating through user-defined roles. After visiting French Security Operations Centers (SOCs), we have defined a collaborative interaction model and some use-cases, to assess of the effectiveness of our solution.

Keywords: Cybersecurity · Collaborative Interaction · Virtual Reality.

1 Introduction

Cybersecurity is a cross-domain activity that requires ground skills on several fields such as data analysis, scripting, compilation, risk assessment etc. This is why modern trend is to put the emphasis on users education and data analysis, as everything that occurs on a network is logged and data breaches are very often due to mistakes made by negligent employees. Far from pop culture stereotypes, cyber operators use classical Command Line Interfaces (CLI) and Graphical User Interfaces (GUI) to detect incidents and cyber threats whereas other domains look at Natural User Interfaces (NUI) to increase users situational awareness, which is one of the main objectives of data visualization solutions. Likewise, expert cyber training tools lack visual information, even though several serious games for cybersecurity are available. Although the actual trend is to regroup cyber operators into specific structures, few collaborative systems are used in cybersecurity.

We firstly show that 3D Collaborative Virtual Environments (3DCVE) can be used in cybersecurity as a mix between Immersive Analytics approaches and serious games for training to put users into cyber-physical environments where realistic scenarios and real-time data can be provided and we will propose a 3D Cyber Common Operational Picture (3D CyberCOP) to deal with these issues. Then we present the model we built after visiting French SOCs and analysing operators collaborative and visualization needs. Several roles and collaboration types, cyber-physical views and mutual awareness cues should be used in order to provide a relevant cyber COP both for experts and novice users.

Finally, we present a specific use case we are developing based on a ransomware attack scenario where analysts, coordinator and client roles will have to cooperate in order to determine Wannacry's Indicators Of Compromise (IOCs).

2 Collaborative virtual environments for cybersecurity

As more and more data are generated and collected on networks, analysts face a 'needle in a haystack' problem when they want to detect attacks. Thus, cybersecurity visualizations 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. 3D collaborative data visualizations and Immersive Analytics solutions can help solving these problems by either separate views towards different analysts but letting them having a common ground, or proposing aggregated 3D interactive data representations that can give more information [2, 5]. Even if 3D representations are useful in some cases highlighted by Cliquet et al. [3], we have not seen much 3D visualizations for cybersecurity, apart from the 2012 Daedalus-viz project developed by Inoue et al. [6]. Moreover, even if operator training is an important topic in cybersecurity, only few systems propose virtual environment for training, serious game-based scenarios and expert data analytics tools [1, 10].

This is why we are currently working on an immersive collaborative system for cybersecurity called 3D CyberCOP: we propose a 3DCVE that can be fitted for collaborative cybersecurity investigations and reporting practices [7] (Figure 1). Collaborative approaches can take advantage of metaphoric representations as each user can have her/his proper way of interacting and visualizing data according to her/his practices, and in order to analyze these practices and contexts of use, we have developed a collaborative activity model for cybersecurity.

3 Modeling cybersecurity collaborative activities

Actual national trend is to regroup cybersecurity employees into collaborative structures as Security Operations Centers (SOCs) or Computer Emergency Response Teams (CERTs). SOCs for example are well-defined structures[5] where

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

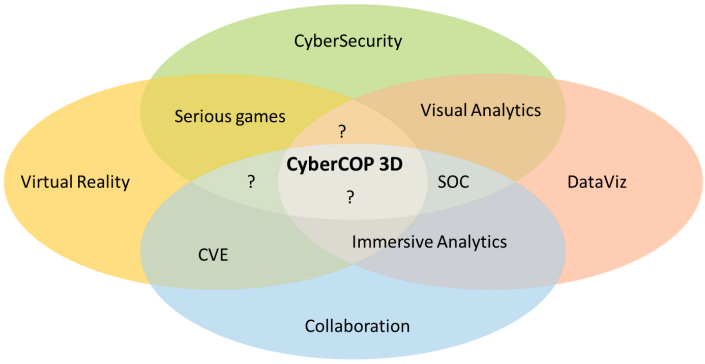

Fig. 1. Venn diagram of 3D CyberCOP, which is at the crossroads of CVE, DataViz and cyber security.

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. There exists studies about SOCs practices [11, 12] but as cybersecurity is by definition a confidential field it is still difficult to record data for making activity analysis.

3.1 SOC activity analysis

Thanks to our industrial partners from the CyberCNI chair[6], we have had the opportunity to visit some French SOCs to perform studies by asking questions and sending questionnaires inspired from [4]. Day to day SOC's operators work relies on getting aware of alerts from cybersecurity 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 kind of data, correlate them and raise alerts (with a quite high rate of false positives).

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 user-adapted visualization tools that will allow them to share information and even to interact simultaneously on datasets. We found out too that SOCs cannot act against malicious activities if decision-makers or clients does not give them proper authorizations.

These findings have allowed us to define a collaborative activity model that will complete our 3D CyberCOP proposal.

[6] https://www.chairecyber-cni.org/en/home/

3.2 3D CyberCOP collaborative activity model

As shown in Figure 2, 3D CyberCOP aims at proposing SOC operators adapted visualizations according to their individual (black arrows) and collaborative (red arrows) practices and interactions: with 3D CyberCOP, first we propose to enhance the individuals interactive systems to make them collaborative and/or more immersive, with collaborative interactions mediated by the systems (green arrows), and second we adapt the level of immersion (Virtual Reality, Windows, Icons, Menu and Pointers (WIMP), post-WIMP interfaces) to user's roles. After

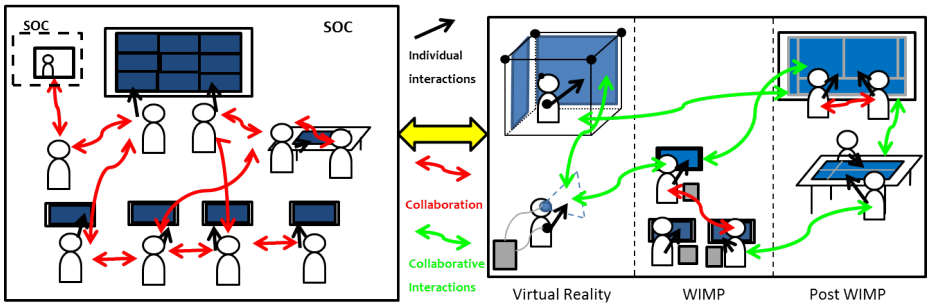

Fig. 2. Classical SOC activities (Left) and the role adaptation we want to do in 3D CyberCOP (Right).

taking into accounts SOC operators' information, we have decided to build our model regarding these points:

- Inspired from [9], user-defined roles as analyst (who dig into data), coordinator (who have a high-level view of the situation) and decision-maker (who can authorize remediation actions) will be proposed. These roles will be complementary as they give access to different kind of data.
- 2D, 3D and immersive views will be provided in order to give high and low level information. Egocentric and exocentric point of views and the abilities to filter data and to switch between views will facilitate data correlation. For example, network topology information could be displayed on a classical 2D dashboard or within a 3D cyber-physical environment where the physical position of its assets into company's offices will help operator to make direct links between IP Addresses, geographic positions and last known users.
- Horizontal (between user that have the same interaction and visualization capabilities) and vertical collaboration (between users that have not the same capabilities) will be supported with respect to hierarchical links and roles. Asymmetric interaction will be defined as well in order to provide mutual awareness by using annotations or orders, as in [8]. For example, analysts will be able to share their investigations traces with each other by letting visual cues on assets and Coordinator will be able to give them orders even if they are not sharing the same space by highlighting zones of interests.

– We will consider using aggregated SIEM-like data instead of raw information to build cyber incidents scenarios developed by experts in order to provide relevant situations, like in a serious-game approach.

In order to implement and evaluate our model, we have selected with our industrial partners a real-time attack analysis use-case.

4 3D cyber COP real-time analysis use case

We have decided to work on a real-time system's security state evaluation use case and we are currently developing a scenario based on a ransomware attack.

4.1 Real-time evaluation of a system's security state

To evaluate the security state of a system, users will have to understand the situation by gathering information from different sources (which can be other users) and by reasoning about these information. We can model cyber incidents behaviors by using relevant metrics as data flow and system's entropy and we can assess users interaction by monitoring these metrics (if a user is blocking ports on an asset, data flow measure will decrease for example).

For this use case, we have defined three users' roles:

– The analyst will be able to investigate data and report incidents or anomalous behaviors to coordinator. S/He will take advantage of immersive technologies in order to better apprehend the situation by switching between cyber and physical representations of the environment.
– The coordinator will dispose of an holistic view of system's security state. S/He will take analysts' reports and give them instructions according to what they are dealing with. He/She will give reports to client.
– The client will have access to specific visualizations (e.g. running applications and processes of his/her computers) and s/he will be able to ask for remediation actions from the analyst or a status report from the coordinator.

Each operator will have to deal with partial system's information. They will have to switch between exocentric or egocentric point of views or to collaborate in order to correlate information and to understand a situation. Figure 3 shows different operators' interfaces ((a) and (b) are coordinator views and (c) and (d) are analyst's ones)) : (a) contains a God's Eye View of the 3DCVE (red square) where red dot is an analyst and greed dot a selected asset and information about metrics and alerts (black square); (b) have a graph view of the network (red square) and information about assets and graph filters (black square); (c) and (d) are cyber-physical views of the environment that display different information.

As we want 3D CyberCOP to be used both for data analysis and training, we will rely on experts specifications to provide deterministic situations: data investigation will be simplified to allow novice and experts to perform system's

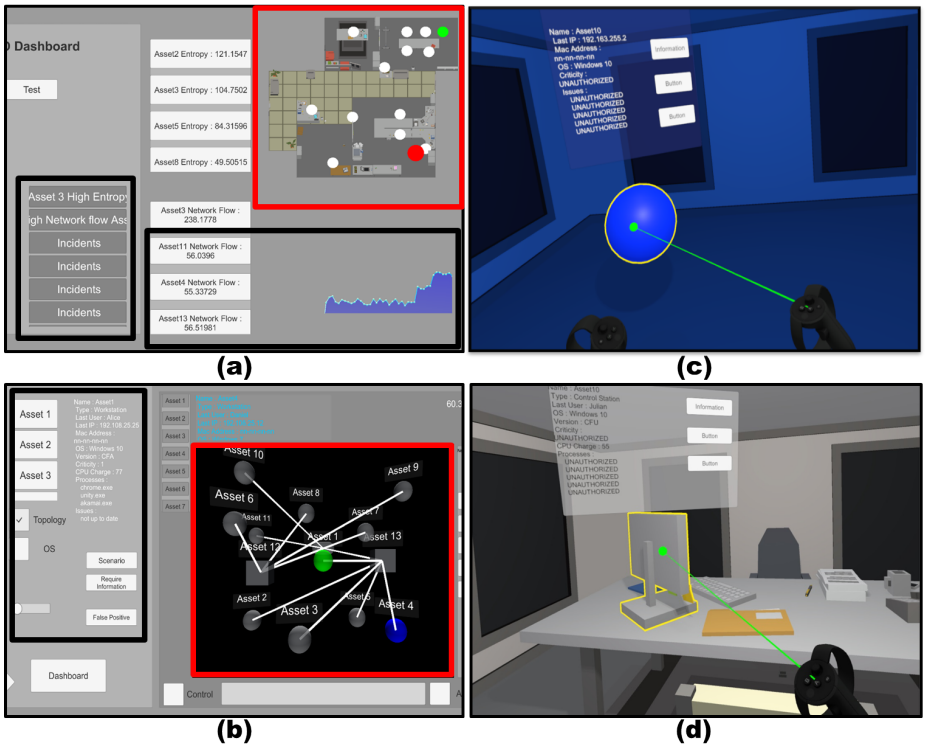

Fig. 3. Several views of our 3D CyberCOP Prototype.

security state evaluation. Novices will be able to deal with the situation by making simple actions (as an example getting network or operating system information from assets by selecting them and clicking an interface button), monitoring simple metrics (network data, as in Figure 3) (a)) and having visual or audio feedbacks of incidents (specific sound or particle effects) whereas experts will have the opportunity to dig into specific piece of evidence by creating data filters (by highlighting assets that shares common aspects) or exchanging precise information (by selecting a specific UI button while selecting an asset).

We are currently using an attack scenario based on Wannacry ransomware to develop a use case as an example of a possible use of our system.

4.2 3D cyberCOP Wannacry attack scenario

Wannacry is a ransomware that caused a lot of damages last year by encrypting computer's files and propagating itself through networks using operating systems exploits (DoublePulsar and EternalBlue). It only have attacked computers on Windows 7, not updated and without a direct link to internet. These behavior cues are called Wannacry Indicators Of Compromise (IOC). We have modeled

Wannacry by using only two metrics, the asset's entropy and data flow: if an asset is infected, its entropy rises and when the ransomware propagates to other assets the data flow increases. These metrics can represent simply Wannacry malicious activities but they can measure false positive activities too (for example if someone is doing a file backup on an extern server, both metrics will increase).

Scenario objective is to determine Wannacry IOCs by correlating partial information taken from cyber-physical representations and from classical data dashboards. Analysts will be able to use virtual reality interfaces to find evidences. Coordinator and client will have access to classical or tactile displays, with respect to SOC practices. Asymmetric interactions between operators will provide mutual awareness cues in order to help users to understand their respective actions such as providing a visualization of operators' actions history or assets highlighting. Data filtering and cyber-physical visualizations will be provided in order to ease correlation. Visual or audio cues will be available for novices in order to help them in the incidents detection. Collaboration will be co-localized and users will have roughly 15 minutes to find IOCs.

We are still working on 3D prototypes and scenarios (Figure 3) but soon we will be able to drive our first alpha experiments that will compare our solution to 2D classical ones, and will give us information on which parts of prototypes we need to improve and which parts work well. Cyber situational awareness evaluation methods will be employed too. Moreover, we will have the opportunity soon to use a real cyber-range tool provided by an industrial partner in order to use realistic cybersecurity data and scenarios rather than modeled ones.

5 Conclusion

Cybersecurity domain relies heavily on data analysis and people education in order to face a growing number of cyber attacks that exploit now employees mistakes more than security flaws to compromise systems. Struggling against cyber threats is a more and more demanding task but we have shown that practices are still underestimating the capabilities of 3D CVEs and virtual reality technologies. In order to tackle these issues, we propose a 3D CyberCOP platform that aims at coupling data visualization and serious gaming approaches. After visiting French SOCs where we have seen that the expected collaboration between users is not well mediated, we have proposed a collaborative activity model and we are developing a scenario based on a real-time cyber attack analysis in order to evaluate the platform. The objective of our 3D CyberCOP will be to merge immersive data visualizations with learning approaches by adapting existing cybersecurity collaborative practices in order to increase users cyber situational awareness.

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, EDF, Orange, La Poste, Nokia, Société Générale and the Regional Council of Brittany. It has been acknowledged by the Center of excellence in Cyber Security.

References

1. 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)
2. 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)
3. 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
4. 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)
5. 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
6. 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
7. 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)
8. 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)
9. 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)
10. 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
11. 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
12. 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)