CyberCOP 3D : visualisation 3D interactive et collaborative de l'état de sécurité d'un système informatique

Alexandre Kabil

DOCTORAT BRETAGNE LOIRE MATHSTIC

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

THÈSE DE DOCTORAT DE

L'ÉCOLE NATIONALE SUPERIEURE MINES-TELECOM ATLANTIQUE
BRETAGNE PAYS DE LA LOIRE – IMT ATLANTIQUE

ÉCOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Informatique*

Par
Alexandre KABIL

CyberCOP 3D: visualisation 3D interactive et collaborative de l'état de sécurité d'un système informatique

Thèse présentée et soutenue à Rennes, le 16 Décembre 2019
Unité de recherche : Lab-STICC Équipe IHSEV — UMR CNRS 6285
Thèse N° : 2019IMTA0166

Rapporteurs avant soutenance :

Guillaume BONFANTE, Maître de Conférences (HDR), École des Mines de Nancy-Université de Lorraine
Jean-Pierre JESSEL, Professeur, IRIT-Université Paul Sabatier

Composition du Jury :

Présidente :	Pascale ZARATÉ, Professeure, Université Toulouse 1 Capitole
Examinateur :	Bruno ARNALDI, Professeur, INSA de Rennes-IRISA
Rapporteurs :	Guillaume BONFANTE, Maître de Conférences (HDR), Mines de Nancy-Université de Lorraine
	Jean-Pierre JESSEL, Professeur, IRIT-Université Paul Sabatier
Dir. de thèse :	Thierry DUVAL, Professeur, IMT Atlantique
Co-dir. de thèse :	Nora CUPPENS, Directrice de Recherche, IMT Atlantique

Invité(s) :

Youssef LAAROUCHI, Ingénieur partenaire Chaire Cyber CNI, EDF
Christophe PONCHEL, Ingénieur partenaire Chaire Cyber CNI, Airbus Defence and Space

Remerciements

Une thèse n'est jamais le travail d'une seule personne. Son accomplissement résulte d'échanges complexes et remercier tous ses contributeurs est un exercice compliqué.

Je n'aurai jamais pu proposer ce manuscrit sans les efforts de mes deux directeurs, Nora CUPPENS et Thierry DUVAL, qui m'ont à la fois guidé et accompagné dans mes réflexions et travaux, mais qui ont su me laisser libre de mes actions et pensées. J'ai pu me former à la recherche par la recherche de la manière dont je le souhaitais, et pour cela je les remercie grandement.

Je tiens à remercier tout particulièrement Thierry pour m'avoir aidé à canaliser ma 'créativité scientifique', pour ses nombreux conseils et d'encouragements et pour m'avoir laissé faire (quasi) ce que je voulais !

Je remercie Jean-Pierre JESSEL et Guillaume BONFANTE pour avoir accepté de relire ce manuscrit et pour leurs conseils quant à son amélioration.

Je remercie également Pascale ZARATÉ et Bruno ARNALDI pour leur présence au sein de mon jury de thèse, respectivement comme présidente et examinateur, et pour leurs remarques et questions qui ont fait évoluer ma recherche.

Je tiens à remercier Youssef LAAROUCHI ainsi que Christophe PONCHEL, qui ont fait en sorte que je puisse proposer des travaux liés fortement à des thématiques actuelles d'acteurs industriels majeurs.

Je tiens à adresser mes remerciements à l'ensemble du département LUSSI de l'IMT Atlantique, dont les personnels ont tous contribué de près ou de loin au bon déroulement de cette thèse, autant au niveau administratif qu'aux niveaux scientifiques, festifs et humains.

Souvent oubliés, les personnels administratifs s'occupant des doctorants, qui font en sorte que tout fonctionne bien et que toutes les cases soient cochées m'ont vraiment aidé et je les en remercie.

Je pense que je peux aussi remercier la ville de Brest dans son ensemble pour son soutien moral et affectif. Bien qu'il peut être perçu comme malpoli de ma part de ne pas citer individuellement toutes les personnes qui m'ont accompagné durant mes trois ans de thèse, ces dernières se reconnaîtront ;)

Par sa relecture assidue et simplement par sa présence à mes côtés, je remercie Eva, ma muse.

Enfin je remercie mes parents pour leur soutien indéfectible.

SOMMAIRE

INTRODUCTION

La cybersécurité (ou sécurité informatique) devient, à mesure que les services se numérisent de plus en plus, une problématique dont l'importance grandit exponentiellement et que l'on ne peut plus ignorer. Elle concerne à la fois nos données personnelles et celles gérées par des entreprises voire des États, le domaine cyber étant même considéré comme le 5ème théâtre d'opérations militaires (les quatre autres étant la mer, la terre, l'air et l'espace).

Analyser l'état de sécurité d'un système nécessite la collecte et l'analyse d'énormément de données de différentes natures. L'analyse de l'état de sécurité des systèmes informatiques s'appelle la *Cyber Situational Awareness* (CSA). Elle s'effectue à plusieurs niveaux (outils, humains et organisationnels) et nécessite un couplage fort entre outils utilisés et modèles mentaux des cyber analystes. Mais ces outils ont actuellement des limites, notamment du point de vue de la collaboration, de la visualisation de données ainsi que de la formation. Ces limites sont actuellement étudiées et sont des problématiques fortes en cybersécurité.

Nous avons pu constater par exemple que dans les *Security Operations Centers* (SOCs), centres où des analystes surveillent en permanence l'état de sécurité des systèmes, la collaboration n'était pas ou peu médiatisée, qu'il n'y avait pas encore d'outils de visualisation immersifs, et que la formation des personnels était faite soit sur des outils experts soit dans un cadre éloigné des contraintes opérationnelles.

L'objectif de cette thèse est de montrer que les Environnements Virtuels Collaboratifs (EVC) peuvent apporter des réponses à ces problématiques. En effet, ils sont utilisés depuis longtemps pour la formation et l'apprentissage humain, et de plus en plus pour la visualisation de données. Ils permettent aussi à plusieurs utilisateurs d'avoir une vue différente d'une situation en fonction de leur degré d'expertise ou de leur rôle dans la simulation.

Ces travaux s'inscrivent dans le cadre de la Chaire Cyber CNI de l'Institut Mines-Télécom, portée par IMT Atlantique. Cette chaire fait de la recherche et de la formation dans le domaine de la cybersécurité des infrastructures critiques (réseaux d'énergie, processus industriels, usines de production d'eau, systèmes financiers, etc.) sa spécialité. Elle collabore étroitement avec Télécom ParisTech, Télécom SudParis et les entreprises Airbus Defence and Space, AMOSSYS, BNP Paribas, EDF et Nokia Bell Labs. La chaire est financée par le Conseil Régional de Bretagne, complété de fonds européens FEDER et par ses partenaires industriels.

Pour bâtir un EVC qui puisse être utilisé pour l'analyse de l'état de sécurité d'un

système informatique (et donc être un outil pour l'acquisition de la CSA), nous avons étudié l'activité collaborative au sein des SOCs de nos partenaires industriels de la chaire Cyber CNI et proposé un modèle de l'activité collaborative, le CyberCOP 3D (Common Operational Picture). Ce modèle a pour objectif de médiatiser l'activité collaborative d'un SOC et de la transposer dans un EVC où les utilisateurs pourraient effectuer des tâches relatives à leurs rôles et besoins.

Notre étude des SOCs s'est déroulée durant la vague de diffusion du rançongiciel WannaCry [1] et nous avons choisi ce dernier comme cas d'utilisation pour l'implémentation du CyberCOP 3D. Nous avons modélisé son comportement et proposé un scénario d'analyse en EVC validé par nos partenaires industriels.

Les contributions de la thèse sont les suivantes (Figure 1) :

— Étude des modèles et outils de CSA et mise en évidence de problèmes liés à la collaboration, l'immersion et l'adaptation à l'utilisateur.
— Proposition des Environnements Virtuels Collaboratifs comme outils pour la Cybersécurité et pour la CSA en particulier.
— Présentation d'un modèle de l'activité collaborative dans les SOCs.
— Proposition d'un modèle comportemental du rançongiciel WannaCry.
— Développement d'un démonstrateur multi-utilisateur, multi-vue 2D et 3D Immersif permettant à des utilisateurs d'effectuer un scénario collaboratif d'analyse d'alertes liées à WannaCry.
— Évaluation de l'utilisabilité d'un Environnement Virtuel pour l'analyse d'alertes par des novices en cybersécurité.

1. `https://www.lexpress.fr/actualite/monde/vague-internationale-de-cyberattaques_1907798.html`

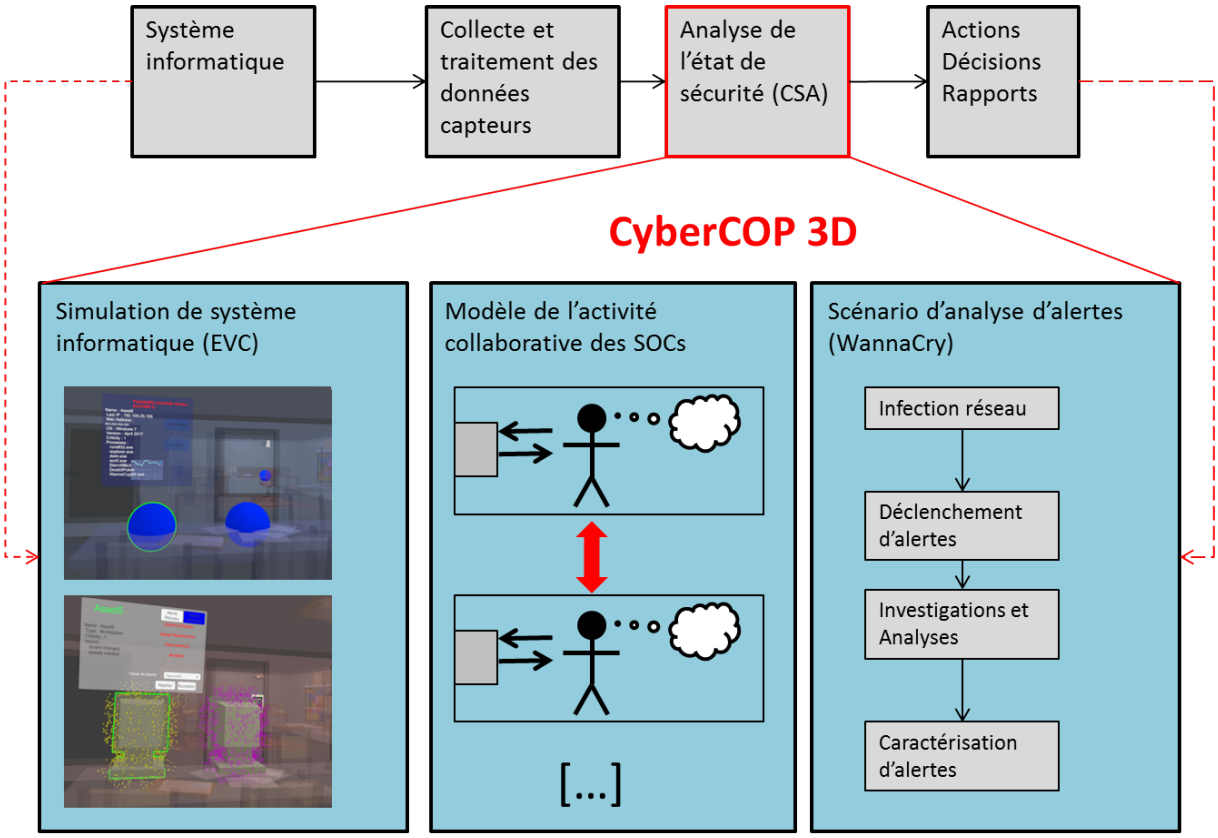


FIGURE 1 – Contributions de la thèse, qui s'inscrivent dans le cadre de l'analyse de l'état de sécurité des systèmes informatiques.

Dans un premier temps, nous montrerons que l'analyse de l'état de sécurité d'un système, à savoir la CSA, s'appuie à la fois sur des outils de traitement de données et sur les modèles mentaux des analystes. Nous décrirons les modèles de CSA existants ainsi que les outils permettant d'analyser une situation soit lors d'une tâche de monitoring soit en entraînement.

Nous présenterons dans un deuxième chapitre la Réalité Virtuelle et les Environnements Virtuels Collaboratifs ainsi que les applications de ces derniers dans les domaines de la visualisation de données et de la formation.

Nous détaillerons dans un troisième chapitre notre étude de l'activité collaborative que nous avons menée dans les SOCs de nos partenaires industriels et le modèle CyberCOP 3D issu de cette étude, qui a pour objectif de transposer les pratiques collaboratives en cybersécurité dans un EVC. Nous présenterons le scénario d'analyse basé sur la modélisation du rançongiciel WannaCry que nous avons choisi comme cas d'utilisation pour l'implémentation du modèle CyberCOP 3D.

Le quatrième chapitre présentera l'architecture de l'EVC que nous avons développé afin d'implémenter les différentes capacités notre modèle CyberCOP 3D, ainsi que les interfaces et interactions que nous avons proposées.

Le cinquième chapitre sera dédié à la présentation de l'instanciation de notre modèle CyberCOP 3D dans un EVC et à la présentation de l'étude de l'utilisabilité d'un Environnement Virtuel pour l'analyse d'alertes que nous avons effectuée.

Enfin, nous concluerons quant à l'utilisation d'Environnements Virtuels Collaboratifs (EVC) pour l'analyse de l'état de sécurité d'un système informatique et nous présenterons des perspectives à nos travaux de thèse.

Chapitre 1

Analyse de l'état de sécurité d'un système

Définir l'état de sécurité d'un système est une problématique en soi car celui-ci dépend de bon nombre de facteurs et de sa nature même. Des recommandations fournies par des organismes nationaux comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ou la National Institute of Standards and Technology (NIST) américaine, et des normes comme les ISO 27000 de l'Association Française de NORmalisation (AFNOR) peuvent faciliter l'appréhension de l'état de sécurité d'un système, mais son analyse requiert une capacité à prendre conscience de cet état de sécurité. Cette prise de conscience s'appelle la *Cyber Situational Awareness* (CSA).

La CSA est une adaptation au domaine 'Cyber' de la Situational Awareness (SA), définie dans un premier temps dans un contexte militaire ; elle décrivait l'ensemble des informations et des réflexions qui permettaient une prise de décision, comme dans le modèle de prise de décision *Observe Orient Decide Act* (OODA) proposé par Boyd en 1997 [10] (Figure 1.1).

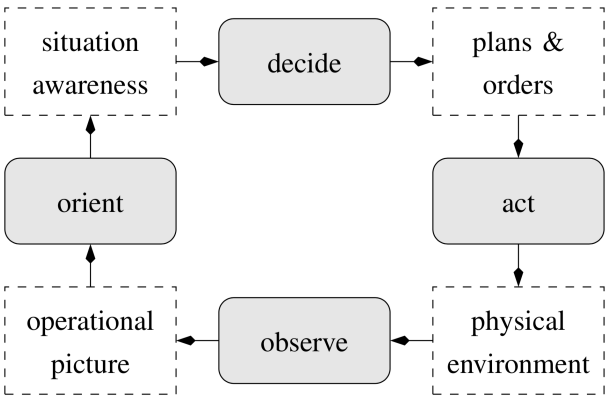


Figure 1.1 – Modèle de prise de décision OODA de Boyd, extrait de [92] (© 2015, IEEE). La situation awareness facilite l'aide à la décision et s'obtient grâce à une *operational picture*, représentation de l'état de l'environnement.

La définition la plus souvent utilisée de la SA est fournie par Endsley, à savoir *the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future* [39].

L'adaptation de la SA au domaine cyber nécessite de définir ce dernier. Il est vu dans un contexte militaire comme le 5e théâtre d'opération, transverse aux autres, comme une dimension parallèle au spectre élecromagnétique de la réalité, tel que l'a présenté Conti *et al.* [24] (Figure 1.2). Constitué de plusieurs couches aussi bien techniques que cognitives ou même sociales [103], son analyse nécessite des outils spécifiques, de par sa nature non-physique et la rapidité des actions qui s'y déroulent (Figure 1.2).

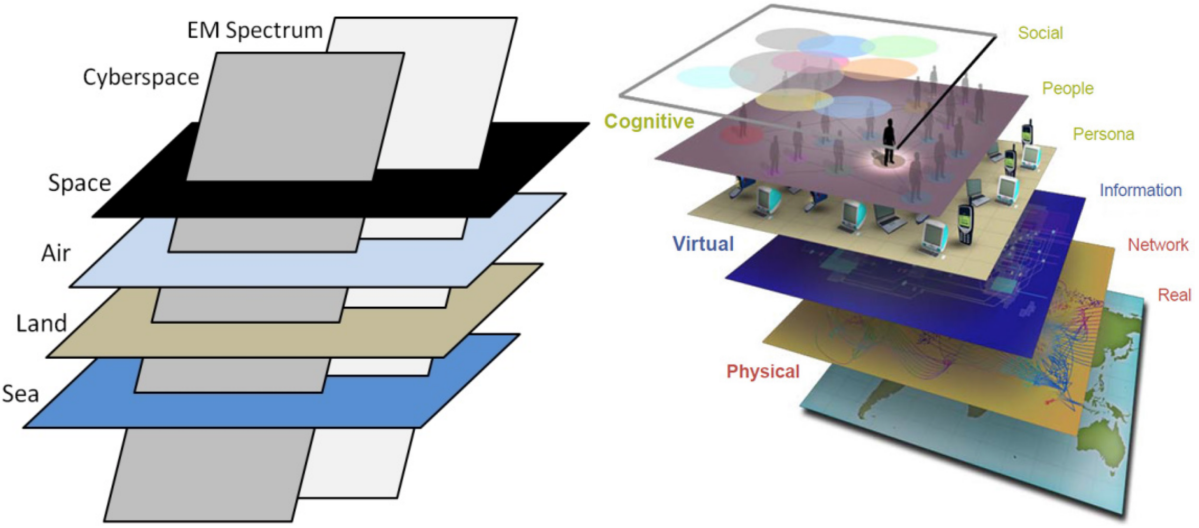


FIGURE 1.2 – Représentations du domaine cyber, transverse aux autres environnements et constitué de plusieurs couches d'informations, extrait de [24] (© 2013, IEEE) et de [103] (licence CC BY 4.0).

La CSA concerne à la fois les outils de fusion de données facilitant la compréhension d'une situation et les processus cognitifs des cyber analystes. De nombreux modèles centrés sur la technologie ou sur l'homme ont été proposés et tous s'accordent sur le fait que l'analyse de l'état de sécurité d'un système résulte d'un couplage entre des outils plus ou moins perfectionnés et les capacités cognitives d'analyse des cyber opérateurs.

Afin d'acquérir une CSA, les outils de visualisation de données, appelés aussi outils de *Visual Analytics* (VA), sont de plus en plus utilisés. Ces derniers se basent sur des représentations 2D des données et sont principalement mono-utilisateurs alors que l'activité de cybersécurité nécessite une coordination entre différents acteurs.

La CSA étant une capacité cognitive, l'entraînement des personnels permet son amélioration. Les exercices de défense et d'attaque de réseaux appelés 'Capture The Flag' (CTF) sont beaucoup utilisés. Ils se basent sur une modélisation et une virtualisation des infrastructures réseau. Une autre catégorie d'outils d'entraînement est celle des simulateurs et des jeux sérieux de sensibilisation aux attaques informatiques.

L'objectif de ce chapitre est de présenter les modèles de CSA, ainsi que les outils d'analyse visuelle et les outils d'entraînement qui permettent de l'acquérir.

1.1 Modèles de Cyber Situational Awareness

Les modèles de CSA présentés dans la littérature peuvent être séparés en plusieurs catégories comme le font Pahi *et al.* [102], à savoir les modèles axés sur l'évolution des technologies de fusion d'informations et de corrélation de données, et les modèles cognitifs (Figure 1.3). Ces différents modèles décrivent les processus d'acquisition et de traitement de données à des fin d'analyse, que ce soit par un outil ou un humain.

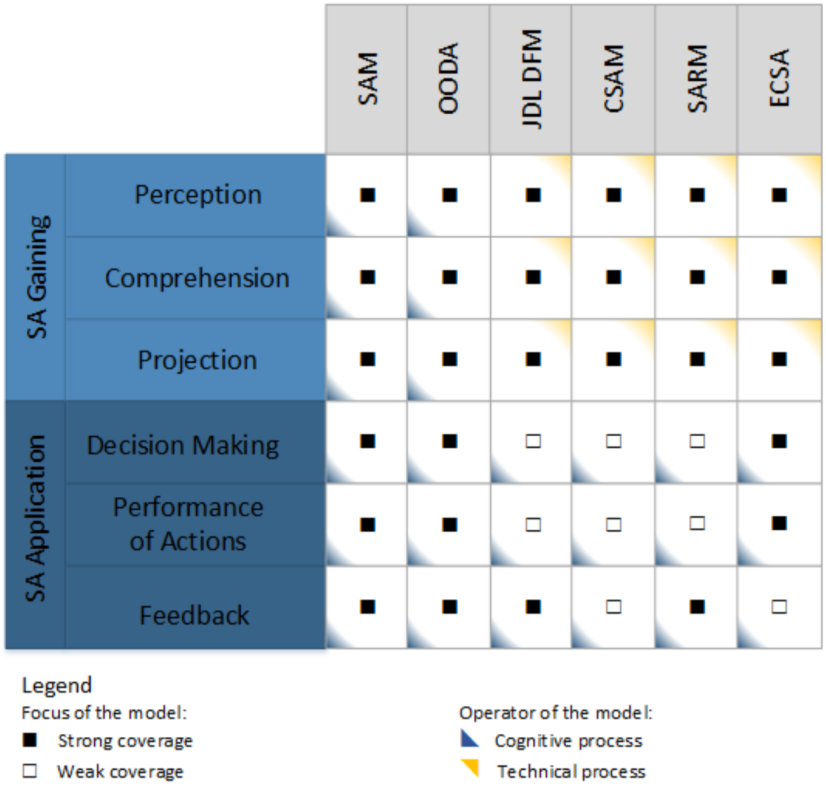


FIGURE 1.3 – Classification par Pahi *et al.* des modèles de CSA (ligne grise), par rapport à leurs caractéristiques (en bleu clair et bleu foncé) et à leur couverture, forte ou faible, des aspects algorithmiques ou cognitifs [102] (licence CC BY-NC-ND 4.0).

Dans cette section nous présenterons dans un premier temps les modèles de fusion de données puis les modèles cognitifs de la CSA.

1.1.1 Modèles de fusion de données pour la CSA

Les modèles de fusion et de corrélation pour la CSA sont centrés sur le traitement des données, comme présenté dans la partie gauche du schéma de traitement de l'information en cybersécurité (Figure 1.4). Tim Bass fut le premier à parler de *Cyberspace Situational*

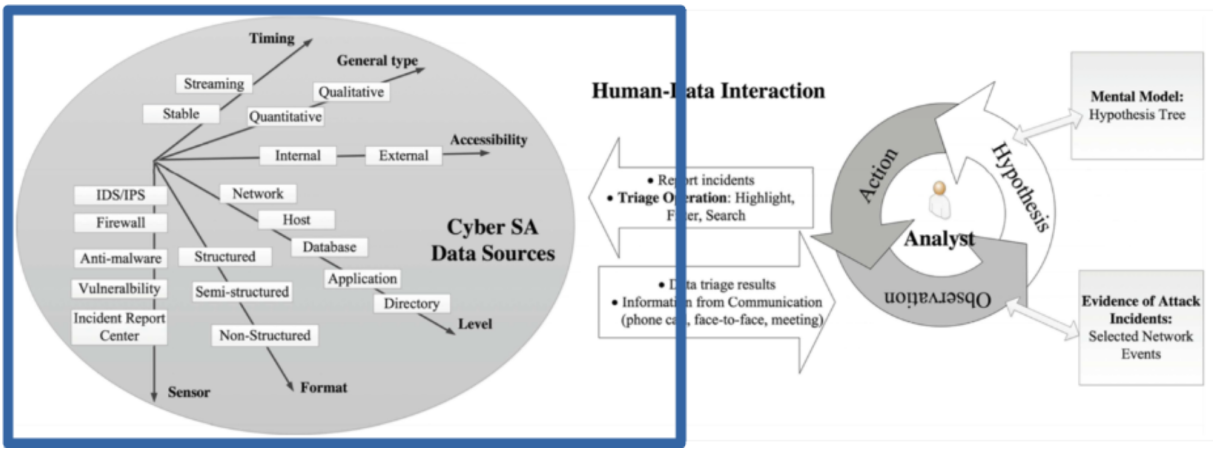


FIGURE 1.4 – Traitement techno-centré (partie encadrée, à gauche) des données en cybersécurité, extrait de [134] (© 2017, Springer). Les modèles de fusion et de corrélation de données pour la CSA ne concernent que l'aspect technique du traitement de l'information.

Awareness [6] en décrivant les mécanismes de fusion de données des *Intrusion Detection System* (IDS), outils indispensables fournissant à un utilisateur des alertes d'intrusion en agrégeant des données de bas niveau issues de sondes et capteurs réseau [34].

Le mécanisme de fusion de données contribue à la CSA car il fournit une pré-analyse de la situation aux utilisateurs. De plus, le domaine cyber étant par définition non-physique, des outils sont nécessaires pour son observation. Face au nombre toujours plus grand de sources de données utilisées pour caractériser une situation, la fusion et la corrélation d'informations sont indispensables pour ne pas submerger l'analyste (Figure 1.5). Les outils de fusion traitent les données brutes afin de les analyser et de les regrouper dans une base de connaissances que l'utilisateur peut consulter.

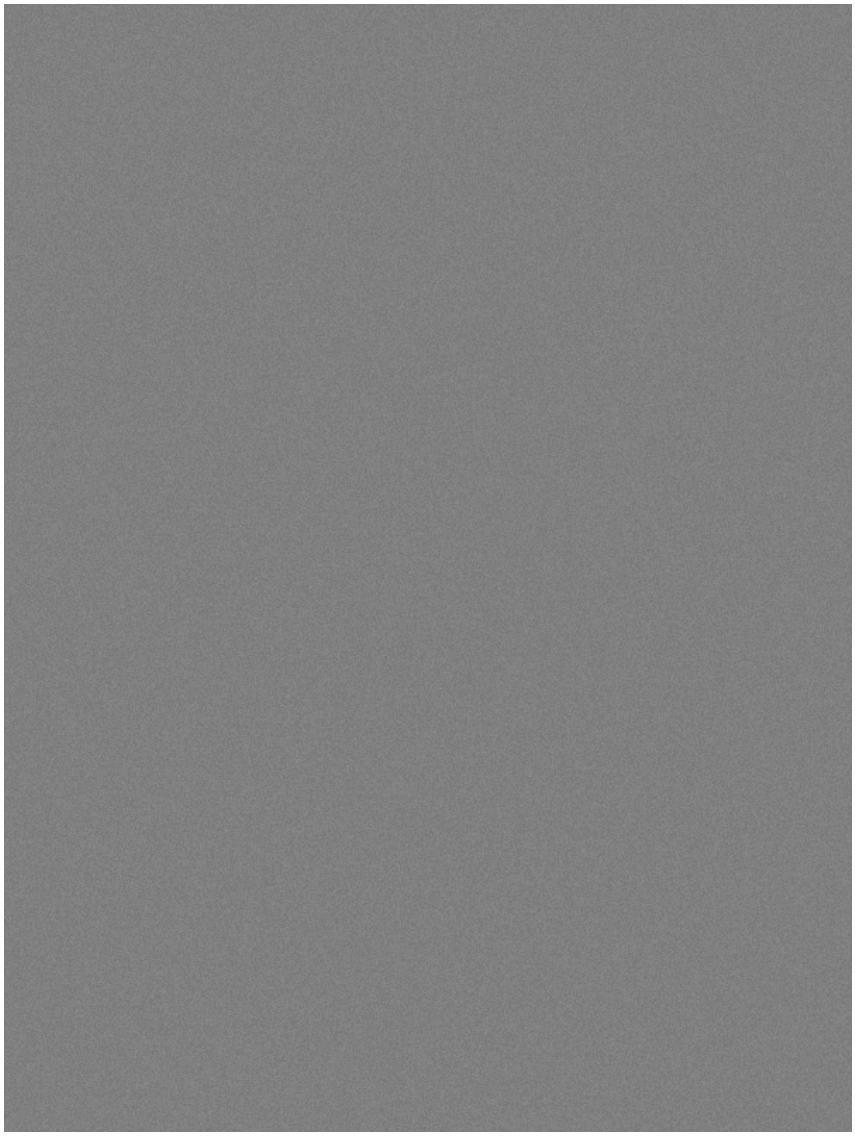


FIGURE 1.5 – Modele de Cyberspace Situational Awareness de Tim Bass [6]. Différentes étapes successives de traitement des données brutes (de bas en haut) permettent d'obtenir une connaissance de l'état de sécurité du système.

Un autre modèle de fusion de données proposé dans la littérature est le *Joint Director of Laboratories* (JDL). Son adaptation et révision au domaine de la cybersécurité a été présentée par Giacobe en 2010 [49]. Ce modèle permet de représenter la succession d'analyses et de fusions de données nécessaires à l'établissement d'un diagnostic sur l'état de sécurité des systèmes. Les différents niveaux hiérarchiques concernent différents types de données, des plus proches des capteurs aux plus fusionnées et agrégées (Figure 1.6).

La différence entre le modèle JDL et celui de Bass est l'ajout d'une étape d'agrégation des informations traitées sous une forme visuelle adaptée aux humains (étape 5 de la Figure 1.6). Cette étape fournit à l'analyste une *Operational Picture* (OP), qui est un support à la CSA comme présenté dans la Figure 1.1 vue précédemment.

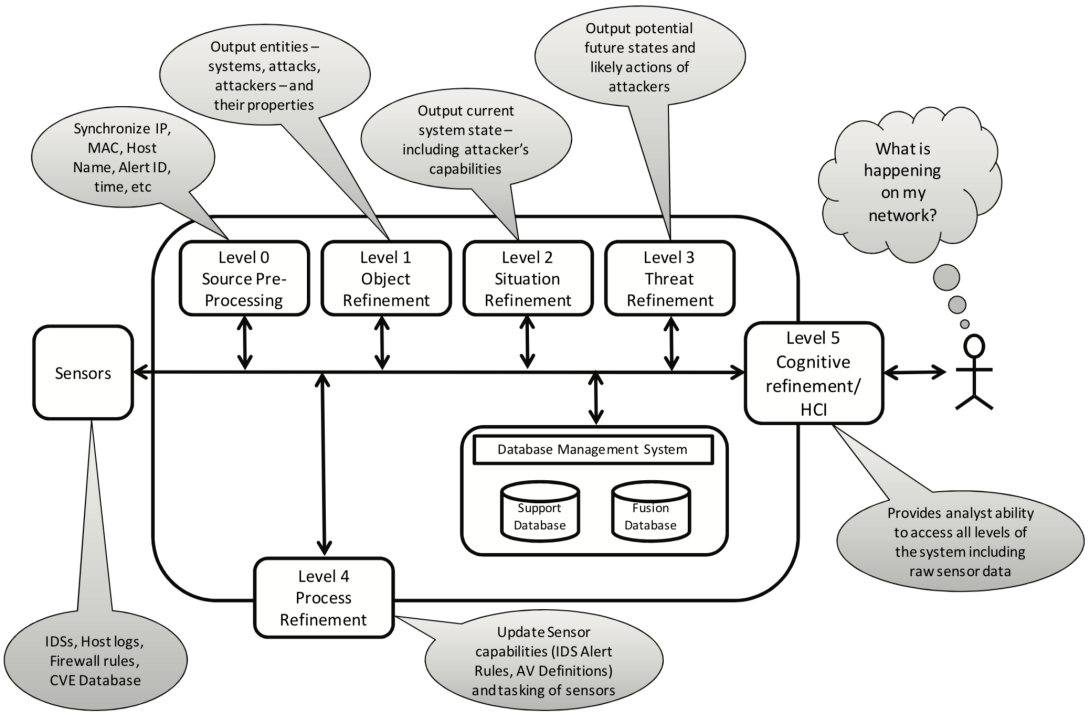


FIGURE 1.6 – Modèle *Joint Director of Laboratories* (JDL) adapté à la cybersécurité, proposé par Giacobe [49] (© 2010, SPIE). Dans ce modèle, les données sont fusionnées dans une vue agrégée de la situation.

Le modèle JDL appliqué à la cybersécurité a été utilisé pour développer des outils facilitant le traitement des informations par un opérateur humain, comme le framework *Situational Awareness of Critical Infrastructure and Networks* (SACIN) présenté par Lääperi et Vankka [75] ou le *Cyber Situational Awareness System* de Kokkonen [69].

Toutefois, ce modèle et les autres modèles de fusion de données ne décrivent qu'une partie du processus d'analyse de l'état de sécurité d'un système. En effet, bien que la fusion et la corrélation d'informations facilitent la compréhension d'une situation en fournissant à un humain une vision globale et agrégée, elles ne sont pas suffisantes. C'est seulement l'étude des processus cognitifs qui permet de mieux comprendre sa manière de traiter l'information et donc d'interpréter ce que lui transmettent les outils.

1.1.2 Modèles cognitifs de la CSA

Ces modèles sont issus des modèles de SA, adaptés au domaine cyber. Ils concernent la partie cognitive de l'analyse des données, comme présenté sur la partie droite du schéma de traitement de l'information en cybersécurité (Figure 1.7).

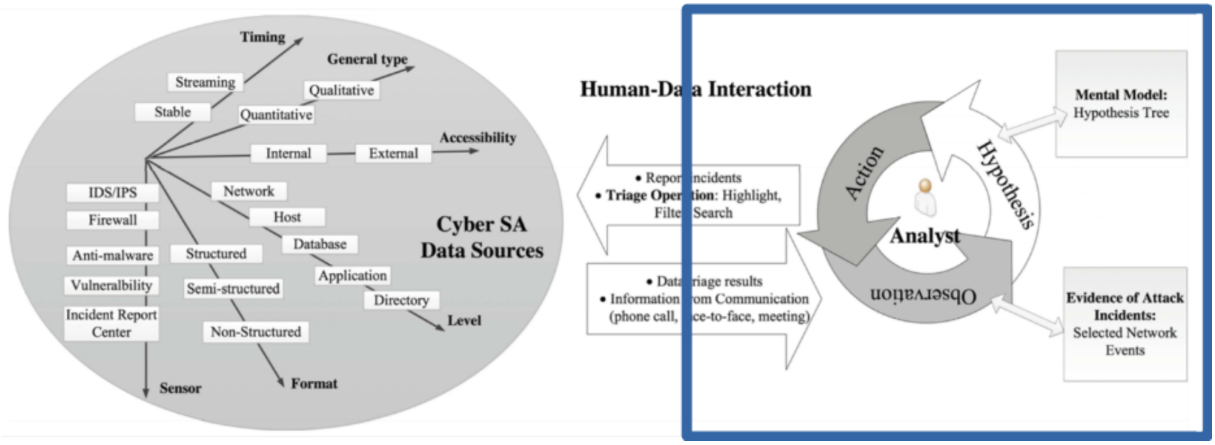


FIGURE 1.7 – Traitement humano-centré (partie encadrée, à droite) des données en cybersécurité, extrait de [134] (© 2017, Springer). Les modèles cognitifs de la CSA concernent la prise d'informations par un opérateur humain.

Le modèle le plus courant de Cyber-SA est celui d'Endsley, basé sur sa définition de la SA vue précédemment et adaptée au traitement de l'information en cybersécurité (Figure 1.8). Ce modèle se décompose en trois étapes cognitives successives, à savoir que l'étape deux ne peut s'effectuer que si l'étape une est validée et ainsi de suite :

— phase d'observation, celle qui prend le plus de temps, qui concerne l'acquisition des données issues d'outils ou de capteurs.
— phase de compréhension après analyse des données de la situation. Cette phase concerne principalement l'état du système à un instant donné.
— phase de projection sur l'évolution de l'état de la situation dans laquelle est le système.

Le modèle d'Endsley décrit les étapes d'analyse et de corrélation des informations effectuées par un humain : à partir d'un état d'une situation, un analyste se crée un modèle mental, une *Operational Picture* (OP) mentale, en utilisant différentes sources d'informations provenant d'outils plus ou moins complexes comme des sondes et capteurs analysant le flux réseau, ou des outils de fusion de données (Figure 1.9).

Une version à quatre étapes du modèle d'Endsley fut présentée par McGuiness et Foy [90], et fut adaptée à la cybersécurité par Onwubiko [101]. La quatrième étape de traitement, la résolution des situations, va au-delà de la projection et permet de modéliser les réponses apportées par un analyste (Figure 1.10).

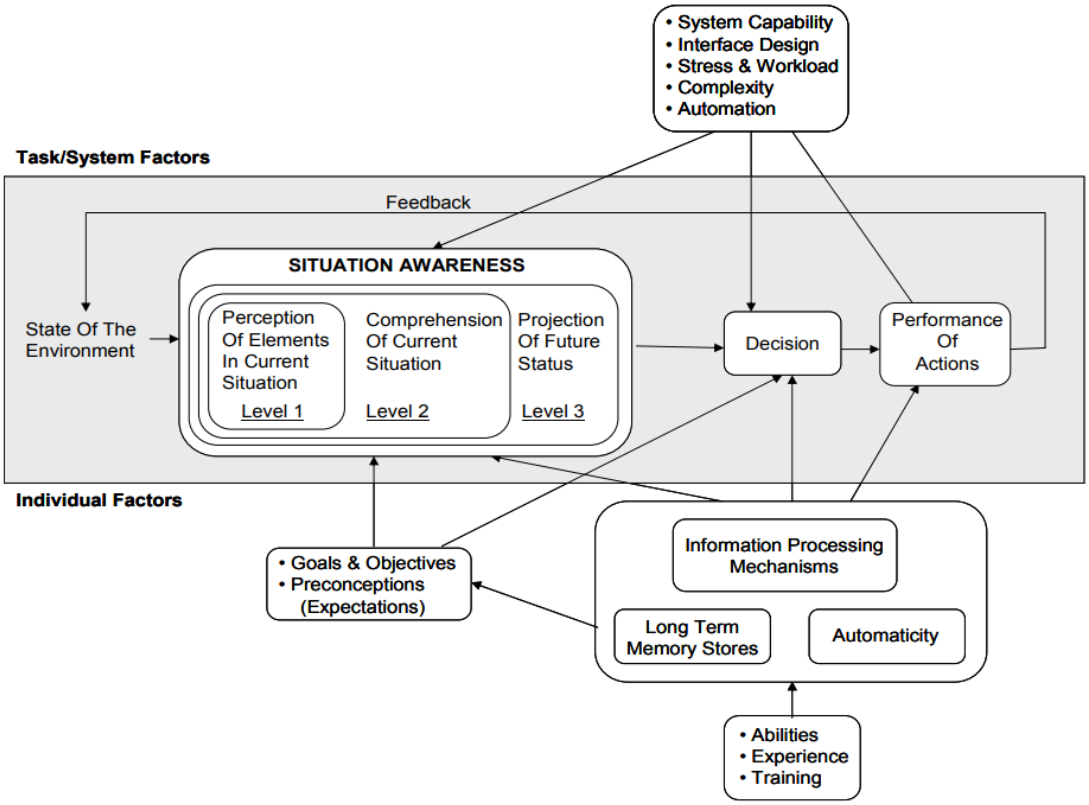


FIGURE 1.8 – Modèle de Situational Awareness d'Endsley [39] (© 1995, SAGE). Ce modèle cognitif de traitement de l'information se décompose en trois niveaux d'analyse de l'état de l'environnement, à savoir la perception, la compréhension et la projection.

FIGURE 1.9 – Sources d'informations relatives aux trois niveaux d'analyse du modèle de CSA d'Endsley (perception, compréhension, projection), extrait de [40] (© 2014, Springer). Les données utiles à la perception sont issues de capteurs de bas niveaux (timestamp, adresses IP, trafic réseau), celles utiles à la compréhension proviennent d'outils croisant les informations des capteurs et permettant d'établir des diagnostics, tandis que celles permettant de se projeter dans l'évolution d'une situation sont plus complexes et issues d'outils d'analyse (prédictions de vulnérabilités et de risques d'attaques).

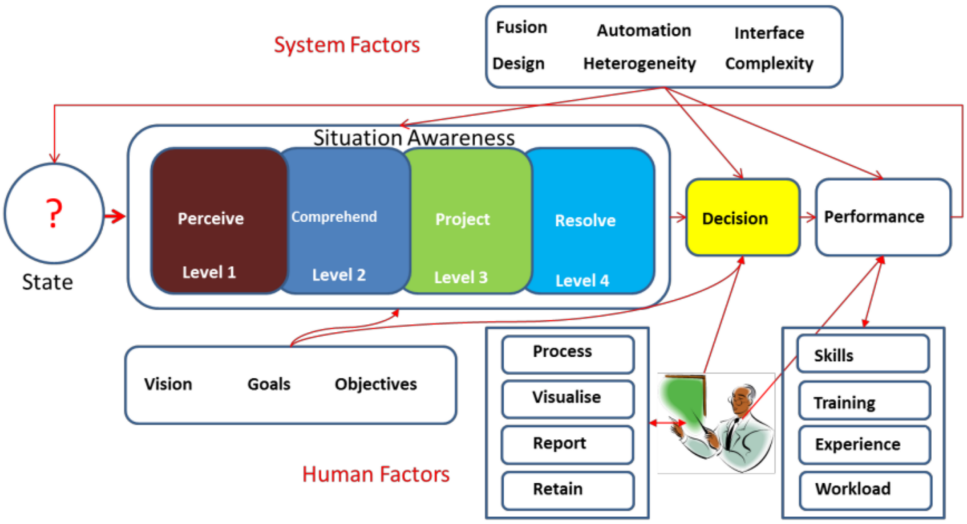


FIGURE 1.10 – Modèle de CSA d'Onwubiko à 4 niveaux cognitifs (ajout d'un niveau de résolution des situations), extrait de [101] (licence CC BY 4.0). Ce dernier niveau permet de prendre en compte les conséquences prévues des actions de l'analyste.

Les modèles cognitifs de CSA ne décrivent eux aussi qu'une partie du processus d'acquisition de la CSA et ne prennent pas en compte le traitement des données par les outils de fusion et de corrélation (qui ne sont vus que comme des sources d'informations). L'analyse de l'état de sécurité d'un système nécessite de prendre en compte le traitement des données à la fois par des outils informatiques et par des opérateurs humains.

1.1.3 Couplage humain-agent pour l'analyse de l'état de sécurité des systèmes

Nous avons vu dans les sections précédentes que nous pouvions décrire la CSA en se centrant soit sur les outils de fusion de données soit sur les capacités cognitives des opérateurs. L'analyse humaine et l'analyse automatique des situations sont toutes deux indispensables car un humain ne peut pas traiter tous les flots de données circulant sur un réseau, et une machine n'a pas la finesse d'analyse d'un humain [51]. La CSA est donc distribuée entre différents acteurs, humains ou logiciels, comme présenté par Tyworth *et al.* [125] ou Bradshaw *et al.* [11]. Elle résulte d'un couplage entre un ou des humains et un ou des agents informatiques, coopérant afin de développer une compréhension de la situation (Figure 1.11).

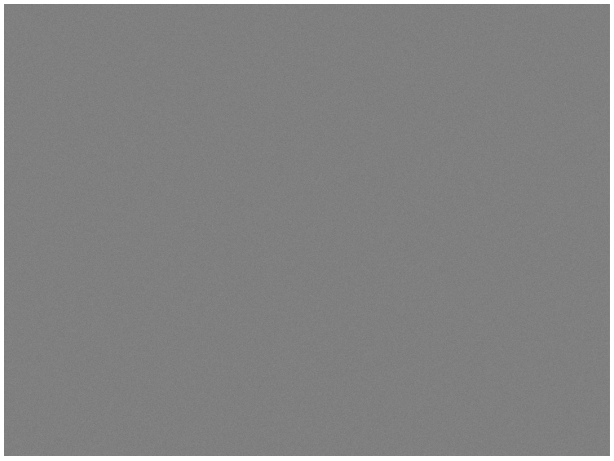


FIGURE 1.11 – Couplage humain-agent favorisant le développement de la compréhension d'une situation, extrait de [11] (© 2012, ICST). Un analyste humain se base sur les informations fournies par un outil et cet outil utilise les recherches de l'analyste afin de traiter les données.

On peut d'ailleurs observer un lien entre les différentes étapes d'analyses cognitives proposées par Endsley et les étapes de traitement de données fournies dans le modèle JDL. Ces deux approches ont été couplées dans le modèle de Tadda et Salerno [119], qui a pour objectif d'offrir une approche globale de la CSA (Figure 1.12). Ce modèle reste toutefois de haut niveau et ne décrit pas les relations existantes entre les différentes tâches des analystes et les outils utilisés afin de récupérer des informations sur l'état de sécurité du système. Cela peut s'expliquer par le fait que la CSA est un processus holistique, à savoir qu'elle concerne l'analyse de l'état de sécurité d'un système dans son ensemble ; elle ne dépend donc pas forcément d'une tâche ou d'un outil en particulier.

De plus, bien que les pratiques actuelles en cybersécurité se basent sur des processus coopératifs entre différents acteurs, il n'existe pas à ce jour de modèle collaboratif de la CSA. Cette dernière est souvent analysée individuellement, et la CSA d'une équipe est vue comme l'agrégation de la CSA de chaque membre, comme présenté par Huang *et al.* [132]. Ce problème est toutefois propre à la SA, qui est difficile à évaluer au sein d'un groupe [54].

L'acquisition de la CSA est effective lorsque la représentation de l'état de sécurité d'un système, à savoir l'*Operational Picture* (OP), correspond au modèle mental de la situation de l'opérateur humain. Les outils de visualisation de données sont utilisés pour développer cette OP, et les outils d'entraînement permettent de favoriser la construction de modèles mentaux pertinents.

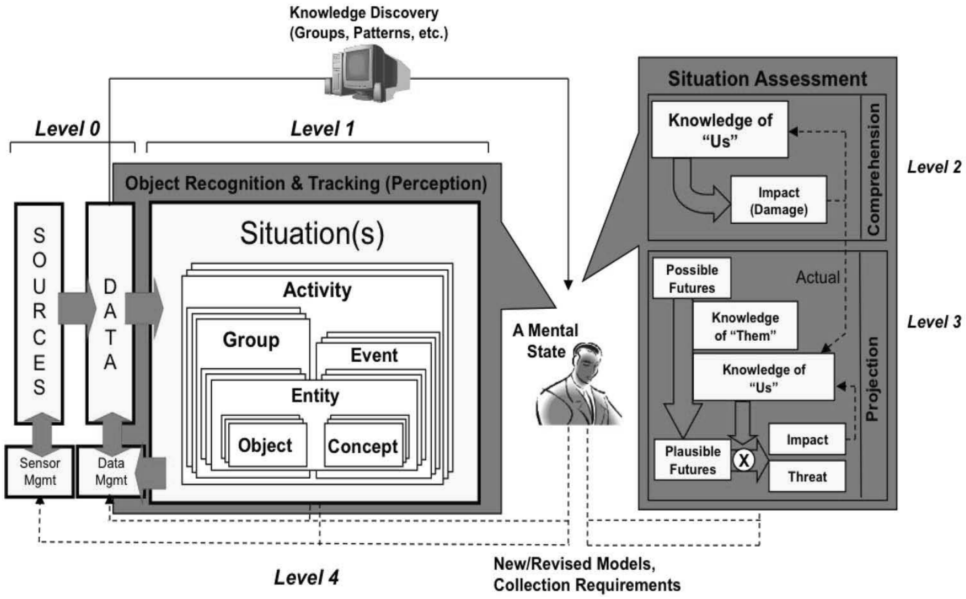


FIGURE 1.12 – Modèle de Tadda et Salerno regroupant à la fois les étapes du modèle de fusion de données JDL de Giacobe et les étapes cognitives du modèle d'Endsley, extrait de [119] (© 2010, Springer). Les différents niveaux de traitement concernent à la fois la fusion d'informations par des outils et le modèle mental d'un analyste.

Modèles de l'analyse de l'état de sécurité

La CSA représente le processus d'analyse de l'état de sécurité d'un système informatique. Ce processus peut être décrit d'un point de vue techno-centré, via les modèles et outils de fusion de données, ou d'un point de vue humano-centré, via les modèles cognitifs. Il résulte du couplage entre un analyste et ses outils de traitement de données, collaborant afin de caractériser une situation de cybersécurité. Les modèles de CSA sont utilisés pour faciliter le développement d'outils de fusion d'informations ou pour mieux analyser les capacités de traitement d'un cyber analyste et donc optimiser ses performances d'analyse. Il n'existe pas à ce jour de modèle collaboratif de la CSA permettant de caractériser l'activité d'une équipe d'analystes.

1.2 Outils d'acquisition de la CSA

Les outils de *Visual Analytics* (VA) agrégeant des données et présentant une vue compréhensible d'une situation sont de plus en plus utilisés afin de fournir une *Operational Picture* (OP), nécessaire à l'acquisition de la CSA [127]. Ces outils sont développés sur la base des besoins et les tâches des utilisateurs, afin de leur fournir des représentations de données adaptées à leurs pratiques.

La CSA étant une capacité cognitive, des outils d'entraînement sont aussi utilisés afin de favoriser son acquisition. Ces outils utilisent soit des réseaux virtuels permettant la reproduction réaliste de situations d'attaque ou de défense d'infrastructures, soit des simulateurs mettant l'utilisateur en situation d'apprentissage non technique ou de sensibilisation.

Dans cette section nous allons présenter l'utilisation d'outils de visualisation de données ainsi que d'outils d'entraînement pour l'acquisition de la CSA.

1.2.1 Visualisation de données pour la CSA

Développement d'outils de visualisation pour la CSA

Selon Varga *et al.* [126], les outils de VA peuvent être utilisés afin d'effectuer des tâches permettant d'acquérir une CSA car ils offrent une vue complète sur l'état d'une situation. La Figure 1.13 présente les relations entre les tâches que les analystes doivent effectuer, qui sont issues des travaux de D'Amico et Whitley [29], les phases de la CSA du modèle d'Endsley vu précédemment et les usages offerts par les outils de VA. Par exemple, les outils de VA peuvent être utilisés pour faciliter l'acquisition d'une phase de la CSA (en orientant l'attention de l'utilisateur sur des données précises par exemple, ce qui participe à la phase de perception) ou pour permettre de comprendre une situation dans son ensemble (en facilitant l'explicabilité d'une situation ou en offrant un compte-rendu détaillé).

En se basant sur la même description des tâches de D'Amico et Whitley [29], Sethi *et al.* ont proposé un framework de développement d'applications de visualisation pour la cybersécurité, EEVi [109]. Ce framework décrit les relations entre les rôles des utilisateurs, les tâches à effectuer, les données à analyser et les caractéristiques de visualisation de l'outil à développer (Figure 1.14).

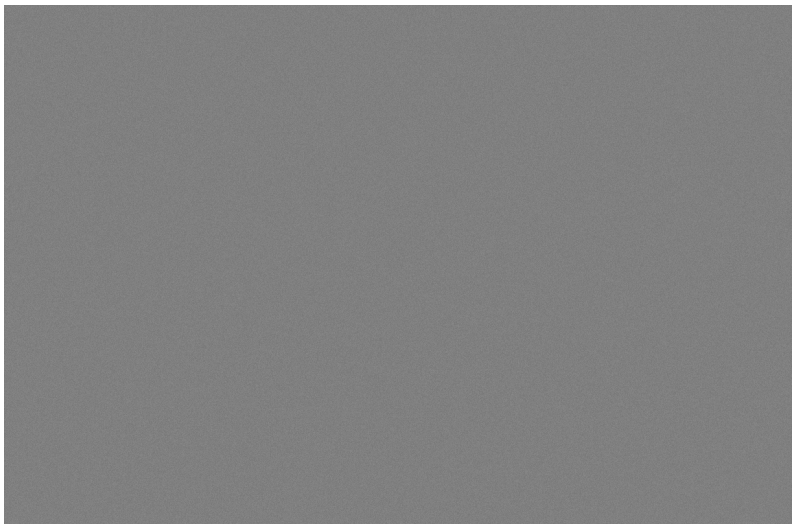


FIGURE 1.13 – Relations entre les phases de la CSA (perception, compréhension, projection) du modèle d'Endsley, les huit tâches que doivent effectuer les cyber analystes (en gris) et les usages des outils de VA (en blanc), extrait de [126]. Les outils de VA peuvent être utilisés à différents stades de l'acquisition de la CSA.

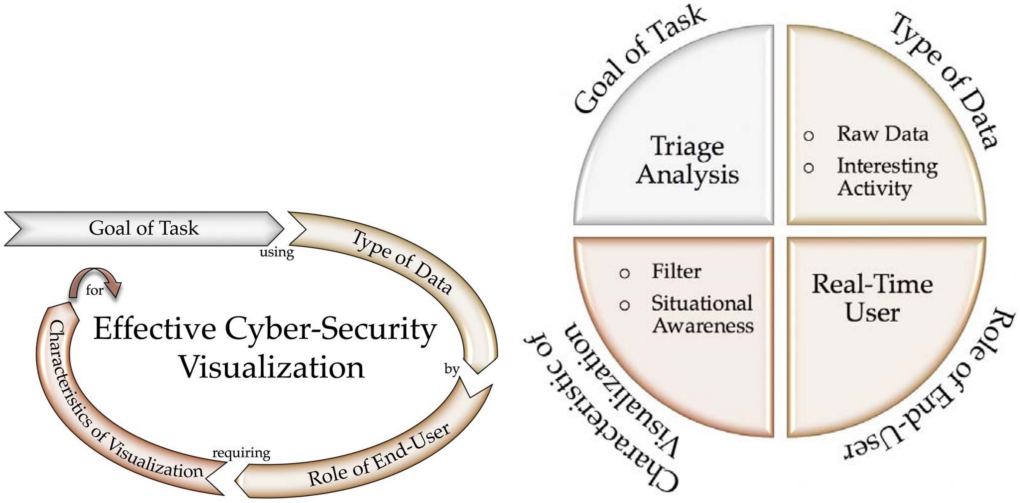


FIGURE 1.14 – Framework EEVi pour le développement de visualisations adaptées aux utilisateurs, extrait de [108] (© 2017, IEEE). L'image de gauche décrit le processus de développement d'un outil de visualisation tandis que l'image de droite présente un exemple de relations entre une tâche de triage de données, les données à utiliser, les rôles dédiés à cette tâche ainsi que les caractéristiques de l'outil.

L'objectif du framework EEVi est d'offrir un cadre de développement et d'évaluation de solutions de visualisation pour la cybersécurité [108]. La Figure 1.15 présente les différents aspects que doit avoir une visualisation permettant l'acquisition de la CSA selon ce framework.

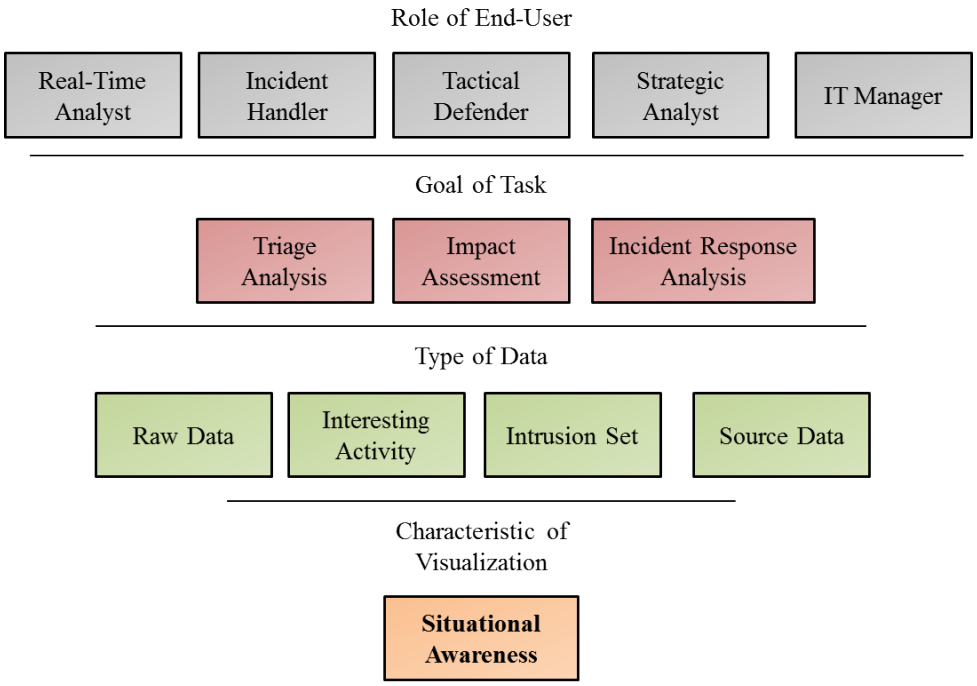


FIGURE 1.15 – Représentation dans le framework EEVi des liens entre visualisation de données pour la CSA, rôles et tâches des analystes et les sources de données requises, adapté de [108]. On peut remarquer que la CSA concerne beaucoup de rôles différents d'utilisateurs ainsi que des sources de données hétérogènes.

Le framework EEVi, comme le modèle relationnel de Varga *et al.* présenté précédemment ne donne pas de consignes spécifiques quant à la représentation des données au sein d'un outil de visualisation pour la CSA.

Cette représentation peut être basée sur la nature des données que l'on souhaite analyser, comme proposé par Raffael Marty dans son livre *"Applied Security Visualization"* [88]. Marty propose un arbre décisionnel permettant de choisir une représentation de données 2D en fonction de l'analyse que l'on souhaite effectuer (Figure 1.16). Par exemple, si l'on souhaite comprendre les relations entre des sources de données du même type, une représentation sous forme de coordonnées parallèles est préconisée si le nombre de dimensions à analyser est supérieur à trois. Sinon, un simple graphe peut suffire.

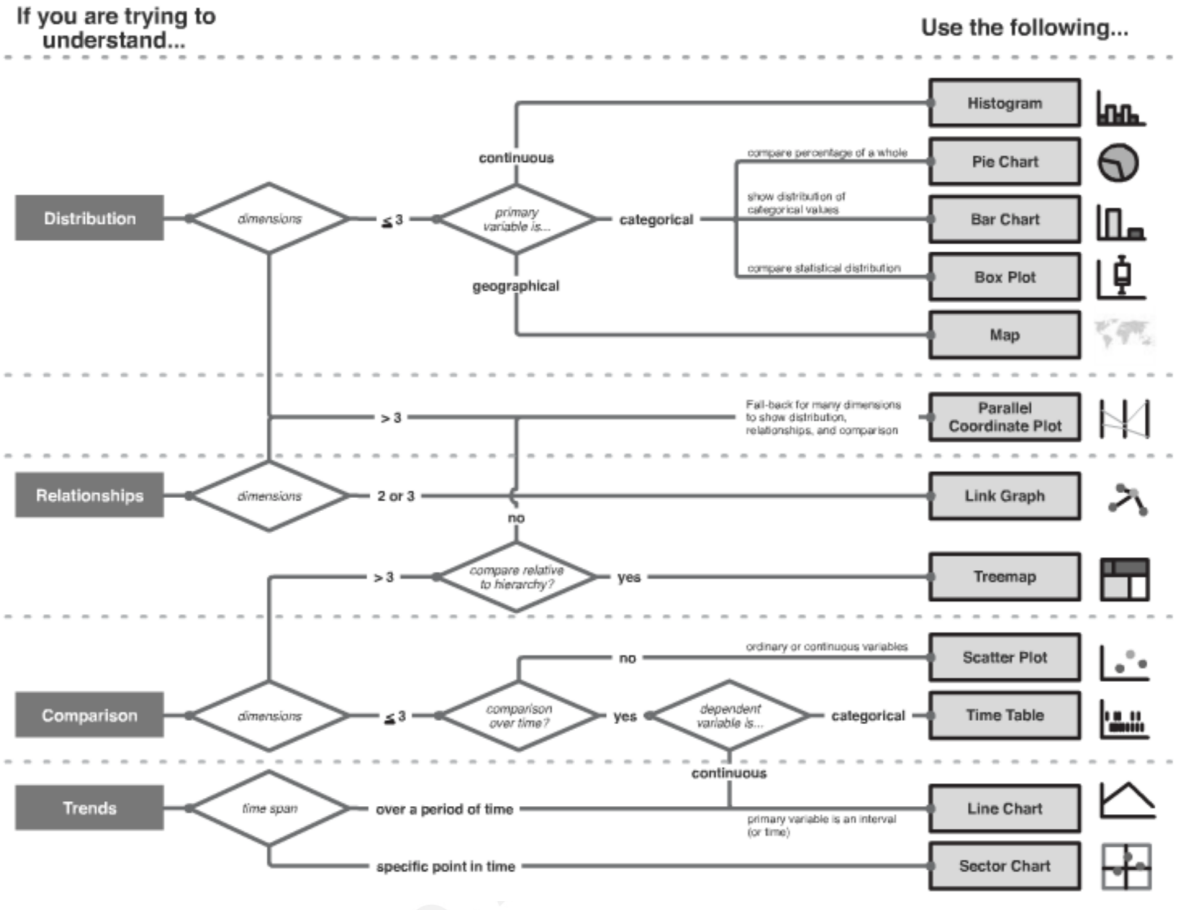


FIGURE 1.16 – Arbre de décision des représentations 2D de données utilisables en cybersécurité, en fonction du type de questions que l'on se pose sur les données, extrait de [88] (© 2009, Raffael Marty). Les représentations proposées sont uniquement en 2D.

Cet arbre décisionnel reste toutefois très général car il pourrait s'appliquer à d'autres domaines que la cybersécurité et il ne permet pas d'adapter la visualisation à la tâche à effectuer. Etoty et Erbacher [42] ont proposé un tableau de correspondance entre les tâches à effectuer par un analyste et les techniques de visualisation nécessaires à la réalisation de ces tâches (Figure 1.17).

Les tâches décrites dans la Figure 1.17 sont indépendantes des rôles des utilisateurs et ne sont donc pas liées à des pratiques spécifiques. Elles restent assez générales mais peuvent permettre de prototyper un outil pour la CSA.

Afin d'adapter les techniques de visualisation aux utilisateurs et non pas aux tâches, des méthodes de design centré utilisateur sont utilisées. Ces dernières nécessitent d'analyser les pratiques des utilisateurs afin de leur proposer des outils qui correspondent à leurs besoins.

Parmi ces méthodes d'analyse des pratiques des utilisateurs, l'analyse cognitive des tâches, (*Cognitive Task Analysis* ou CTA) est couramment utilisée car elle permet de faire correspondre les tâches effectuées aux modèles cognitifs comme celui d'Endsley [107]. La Figure 1.18 présente un processus de développement d'application pour la cybersécurité :

— Les pratiques des utilisateurs sont analysées via des observations, des interviews ou des sondages.
— Ces analyses permettent de proposer à la fois des modèles théoriques de l'activité cognitive des utilisateurs mais aussi des prototypes d'applications.
— Ces prototypes sont alors testés par les utilisateurs et leurs pratiques sont mesurées.
— Ces mesures sont alors comparées aux modèles théoriques et permettent de corriger les prototypes de manière itérative.

Les méthodes de design centré utilisateur permettent de développer des outils de visualisation pour la CSA dans un cadre opérationnel et pas seulement théorique. Toutefois, comme le souligne Gutzwiller [54], ces méthodes sont complexes à mettre en place car elles nécessitent d'être en contact direct avec des utilisateurs et de pouvoir effectuer des études qui peuvent prendre plusieurs heures par utilisateur. Mais elles permettent de prendre en compte à la fois les aspects relatifs aux données, aux tâches à effectuer ainsi qu'aux rôles des utilisateurs.

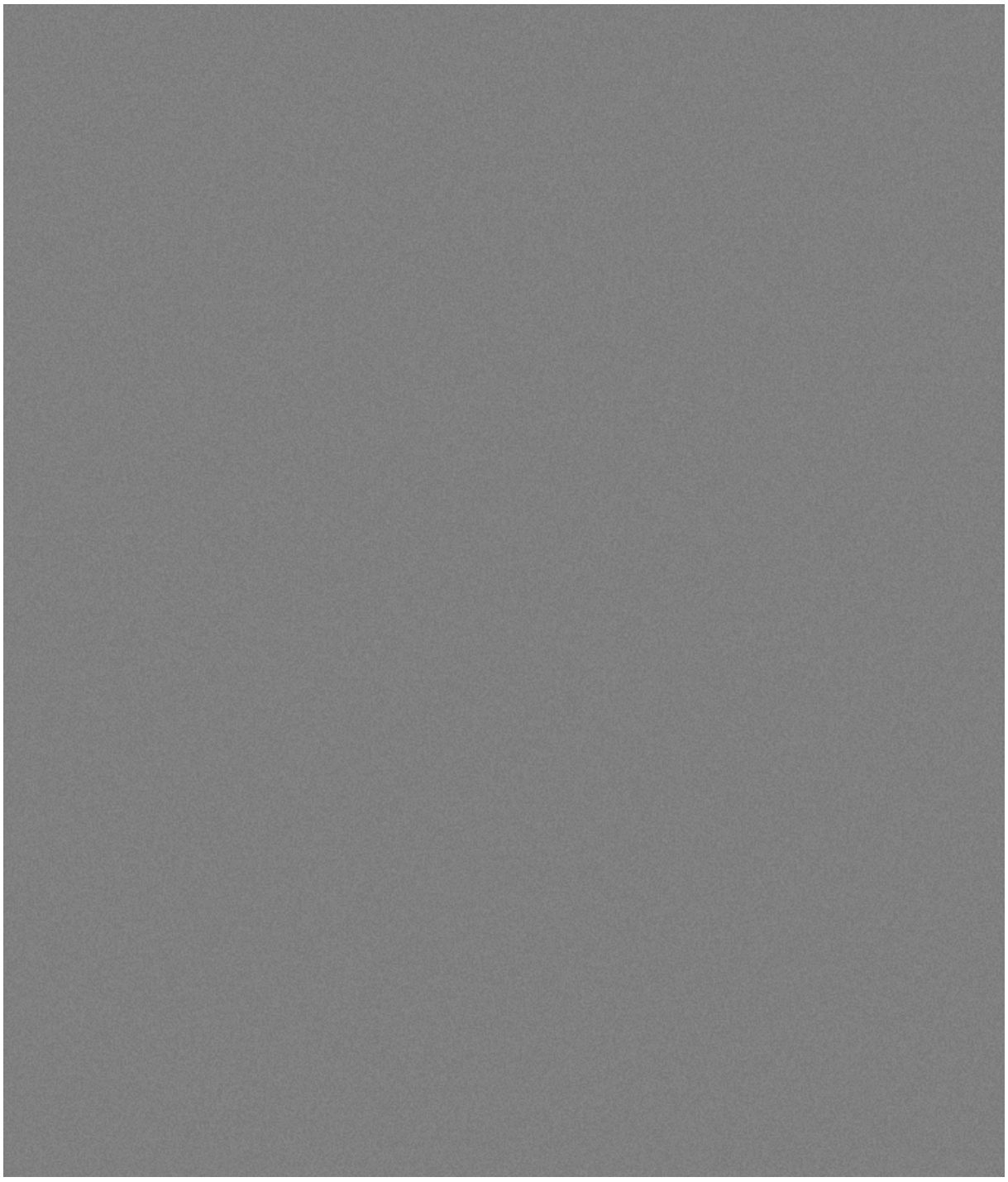


FIGURE 1.17 – Classification des techniques de visualisation à implémenter en fonction des tâches devant être effectuées par des cyber analystes, extrait de [42]. Les techniques de visualisation proposées restent de haut niveau et assez générales.

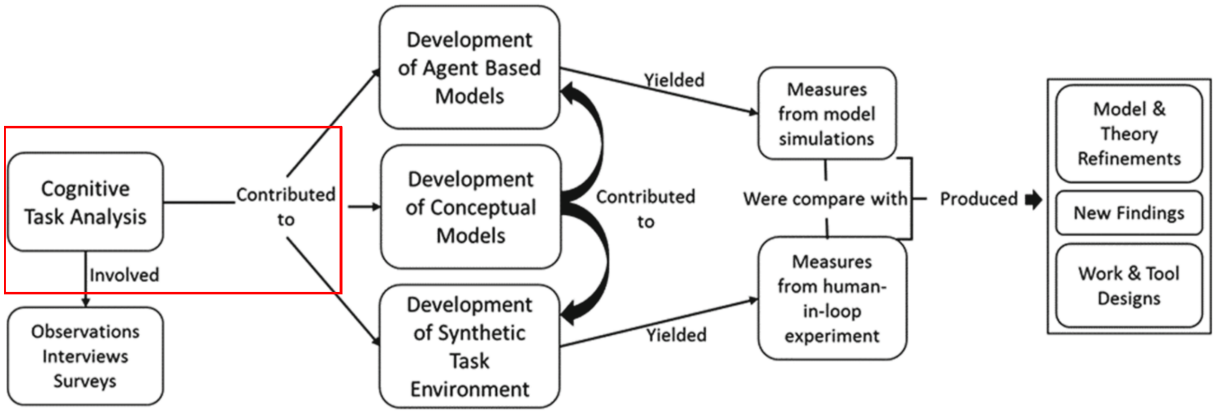


FIGURE 1.18 – Utilisation de la *Cognitive Task Analysis* (CTA) dans le processus de développement d'applications pour la cybersécurité, par Rajivan et Cooke [107] (© 2017, Springer). Cette analyse se base sur des interviews et une observation des pratiques des utilisateurs, et permet de développer des modèles d'applications qui sont testés. La pratique humaine est mesurée et comparée aux modèles cognitifs théoriques.

Visualisation de données pour la CSA

La plupart des outils de visualisation de données pour la cybersécurité utilisent des représentations 2D, comme présenté par Shiravi *et al.* dans leur revue de littérature [111]. Ces outils se basent sur la métaphore du tableau de bord, à savoir la représentation sur un seul écran de différentes sources d'informations, comme par exemple la solution EntVis de Zhou *et al.* [136], qui permet de détecter les anomalies du trafic réseau de manière visuelle (Figure 1.19, en haut), ou l'outil CyberPetri, proposé par Arendt *et al.* [2], qui permet d'analyser l'état de progression d'une compétition en cybersécurité d'un seul coup d'oeil (bas de la Figure 1.19).

Ces tableaux de bord sont adaptés à différents types d'utilisateurs, mais sont peu adaptables et peu interactifs. En l'occurrence, EnVis est dédié à une utilisation par des experts en détection d'anomalies tandis que CyberPetri a été développé afin de permettre à des spectateurs de suivre l'état d'un challenge de cybersécurité.

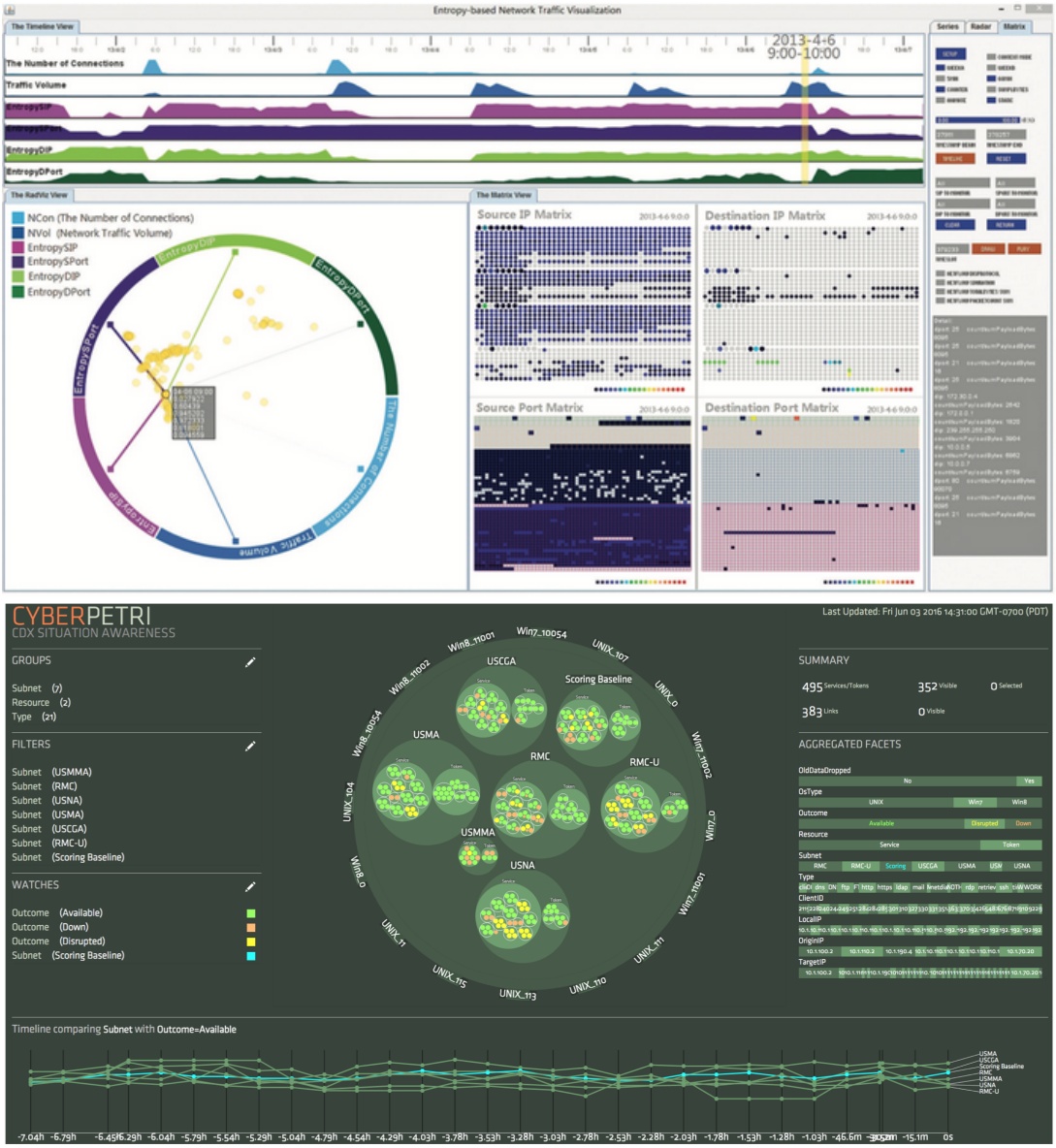


FIGURE 1.19 – En haut, EntVis, Outil de *Visual Analytics* pour les détections d'anomalies du trafic réseau, extrait de [136] (© 2015, IEEE). En bas, Outil CyberPetri, pour l'étude de l'évolution de l'état d'un challenge de cybersécurité, extrait de [2] (© 2016, IEEE).

Bien que les analyses de données en cybersécurité s'effectuent de plus en plus de manière collaborative, en échangeant des informations entre les différentes structures (SOC, CERT, CSIRT) ou au sein de ces structures, les outils d'analyse restent individuels et adaptés aux besoins des différents personnels (analystes, coordinateurs, décisionnaires). Cela peut s'expliquer par la difficulté à fournir des représentations de données qui soient adaptées à plusieurs rôles ou activités.

Nous pouvons toutefois regrouper les outils collaboratifs d'analyse de l'état de sécurité des systèmes en deux catégories :

— Les outils de partage d'information permettant de suivre les activités des autres utilisateurs, via un historique d'actions ou des traces d'interactions. Ces outils permettent une collaboration distante mais le partage d'information augmente le risque de fuite de données. Les outils OCEANS et AOH-Map, proposés respectivement par Chen *et al.* [19] et Zhong *et al.* [133], rentrent dans cette catégorie car ils offrent des interfaces permettant d'échanger des informations sur des alertes et de suivre les raisonnements des autres utilisateurs (Figure 1.20).

— Les outils dits de *Common Operational Picture*, ou COP, qui ont pour objectif de permettre à différents acteurs de se coordonner et d'étudier une situation sous différents angles en se basant sur une représentation graphique commune. Ces outils s'inspirent des représentations tactiques des différents domaines du champ de bataille (air, terre, mer, espace) d'après Gregory Conti [24]. L'outil CyCOP proposé par Esteve *et al.* [41] ainsi que l'outil proposé par Zhong *et al.* [135] rentrent dans cette catégorie car ils proposent d'analyser l'état de sécurité via un tableau de bord qui agrège plusieurs représentations de données adaptées aux différents rôles et besoins des utilisateurs (Figure 1.21). Cette agrégation est d'ailleurs le point faible de ce type d'outils : en effet, plus nous souhaitons présenter de sources de données adaptées à différents utilisateurs sur un tableau de bord de taille finie, plus ces représentations de données seront petites, ce qui peut limiter l'interaction et la visualisation.

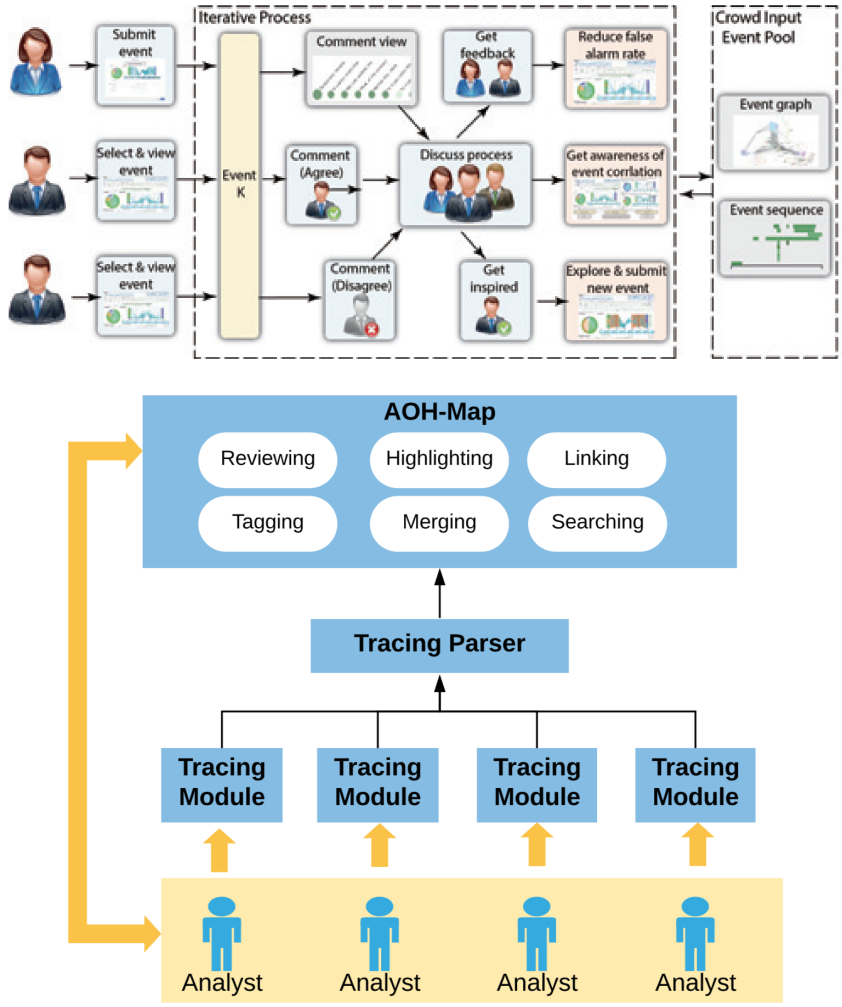


FIGURE 1.20 – Architecture collaborative des outils d'analyse d'événements OCEANS (extrait de [19], en haut) et AOH-Map (extrait de [133],en bas) (© 2019, IEEE). Ces outils permettent à plusieurs utilisateurs d'échanger des informations et de visualiser leurs traces d'interaction et leurs raisonnements. L'échange d'information est un vecteur de risque de fuite de données.

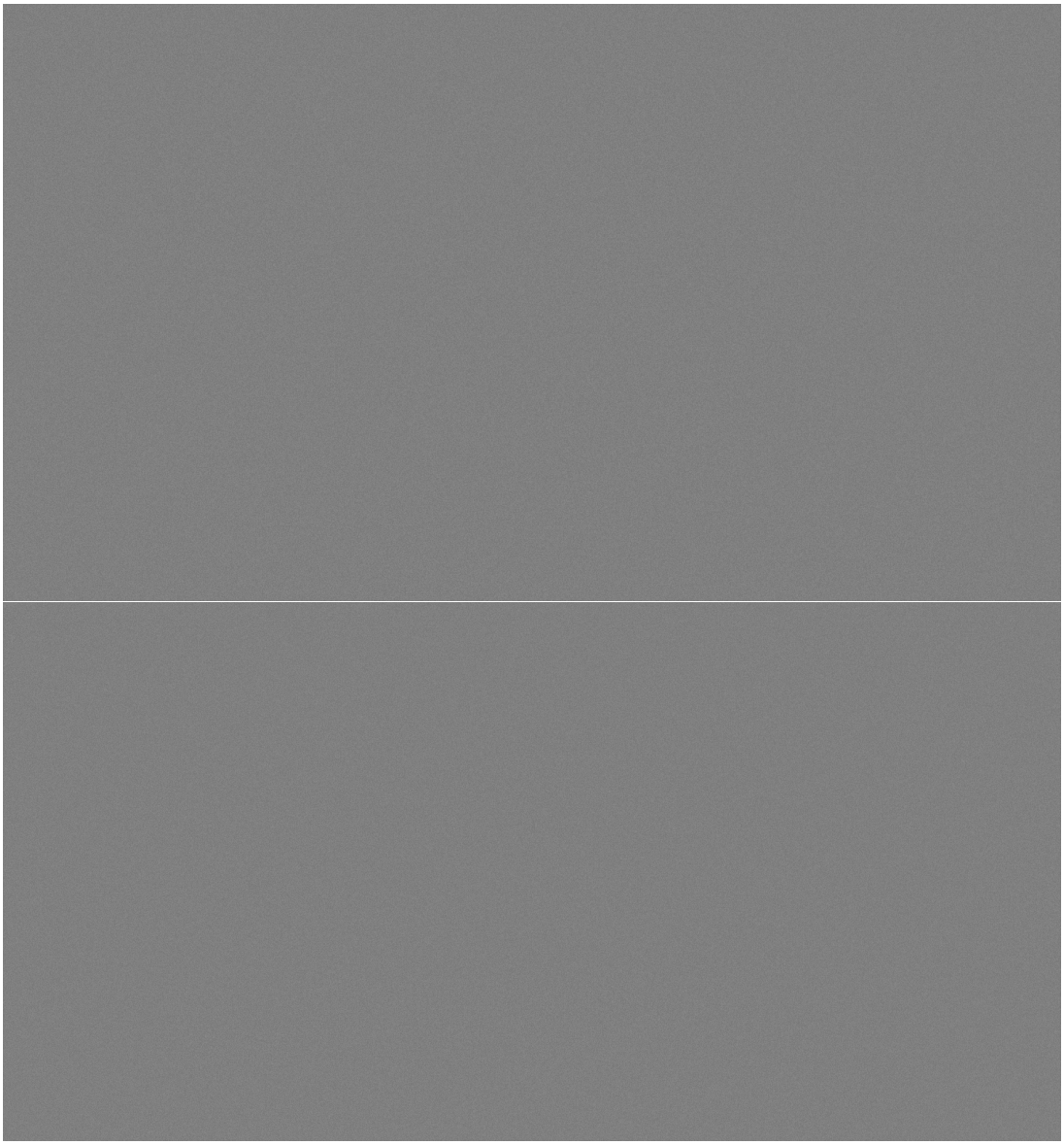


FIGURE 1.21 – Outil CyCOP d'analyse de situations tactiques (extrait de [41], en haut) et l'outil d'analyse comparée des localisations topologiques et géographiques d'adresses IP proposé par Zhong *et al.* (en bas, extrait de [135]) (© 2019, IET). Ces outils se basent sur l'utilisation d'un tableau de bord (une COP) séparé en différentes représentations de données adaptées aux rôles des utilisateurs. Cette séparation limite l'interaction et la visibilité des données.

Nous avons pu constater de plus que durant les deux dernières décennies, plusieurs propositions ont été faites dans la communauté scientifique d'Environnements Virtuels (EV) pour la représentation de données pour la cybersécurité, mais que ces propositions sont restées pour ainsi dire lettres mortes.

Par exemple, Harrop et Armitage [59] (Figure 1.22), Michel *et al.* [93] ou Hall *et al.* [56] (Figure 1.23) ont respectivement proposé des EV pour la détection d'intrusions, l'analyse de trafic réseau ou l'analyse collaborative de données, mais ces travaux n'ont pas été poursuivis.

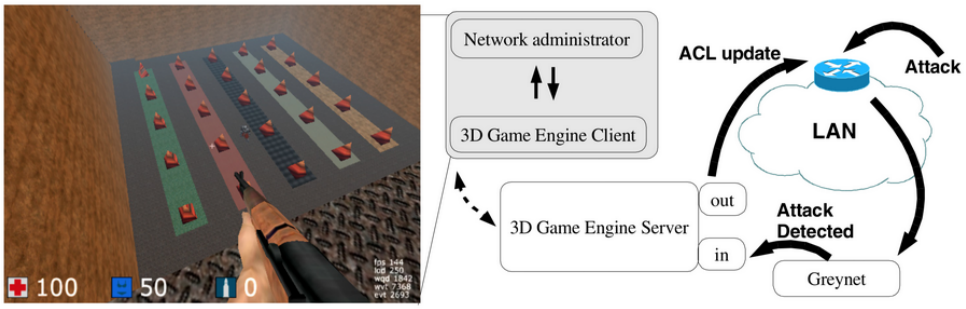


FIGURE 1.22 – Exemple d'application immersive pour la détection d'intrusions basée sur la métaphore du jeu de tir à la première personne, extrait de [59] (© 2006, ACM). L'utilisateur peut 'tirer' sur les données d'intrusion afin de les filtrer et de les signaler.

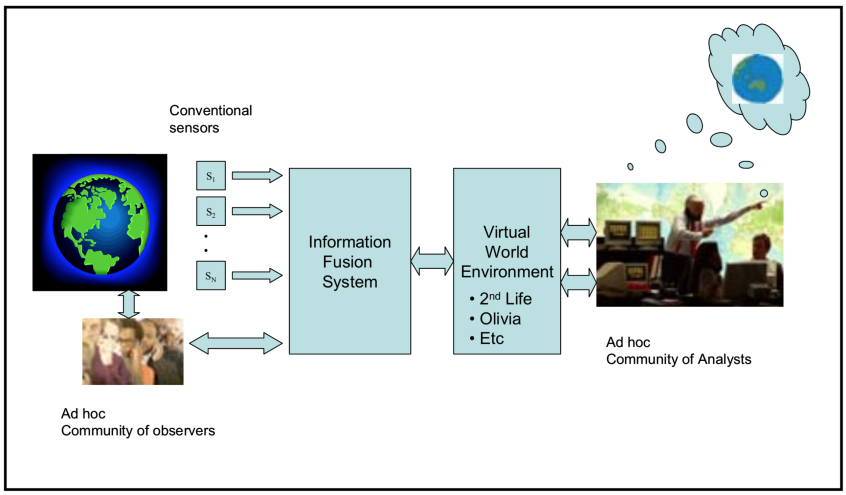


FIGURE 1.23 – Architecture de solution pour l'analyse collaborative immersive de données pour la cybersécurité, extrait de [56] (© 2008, IEEE). L'EV reçoit des données fusionnées et transmet des commandes de filtrage à la base de données.

De la même manière, le projet CyberNet [53, 1], qui proposait une visualisation de données pour l'analyse des réseaux, basée sur la métaphore de la ville, a aussi été abandonné, alors que récemment une entreprise innovante, ProtectWise, a proposé une visualisation du même type pour son outil de surveillance des réseaux (Figure 1.24).

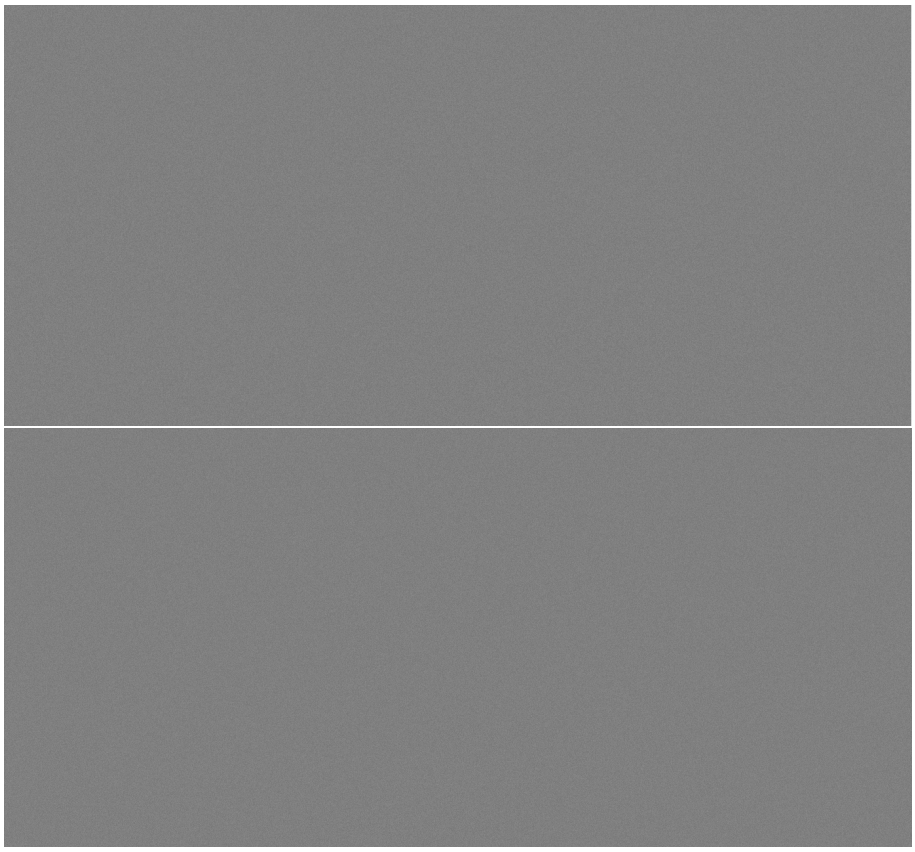


FIGURE 1.24 – Métaphore de visualisation de données de la ville virtuelle, proposée lors du projet Cybernet (en haut, extraite de [53]), et représentation artistique de l'*Immersive Grid* de l'entreprise ProtectWise (en bas, extraite de `https://www.behance.net/gallery/62606863/ProtectWise-The-Immersive-Grid`). On peut remarquer qu'au-delà des différences graphiques, les données sont représentées de la même manière, à savoir des groupes d'immeubles plus ou moins hauts en fonction du volume de données et possédant différentes caractéristiques (fenêtres, portes) en fonction de la sémantique des données, alors que dix-sept ans séparent les projets.

Les limitations techniques des années 1990 ou 2000 peuvent expliquer l'abandon rapide des solutions immersives pour la cybersécurité. En effet, les outils de CSA nécessitent le traitement et l'affichage temps-réel d'un nombre important d'informations, ce qui était difficile et coûteux à proposer en 3D ne serait-ce qu'il y a une vingtaine d'années. Comme nous le montrons dans la section 2.1.2, un dispositif immersif haut de gamme coûtait 250000 dollars dans les années 1990 tandis qu'un dispositif actuel dont les performances sont bien meilleures coûte moins de 5000 dollars. L'évolution des unités de calcul graphique et le développement des technologies immersives permettent de remettre au goût du jour des projets du type CyberNet, comme le propose ProtectWise.

Des propositions de visualisations immersives pour la cybersécurité voient le jour, comme les travaux d'Inoue *et al.* [61] (Figure 1.25) concernant le monitoring 3D d'alertes du dark web, les travaux de Latvala *et al.* [77] (Figure 1.26) proposant une métaphore d'aquarium 3D pour la visualisation d'événements réseau, ou ceux de Kullman *et al.* [72] proposant une visualisation 3D des données d'un challenge de cybersécurité.

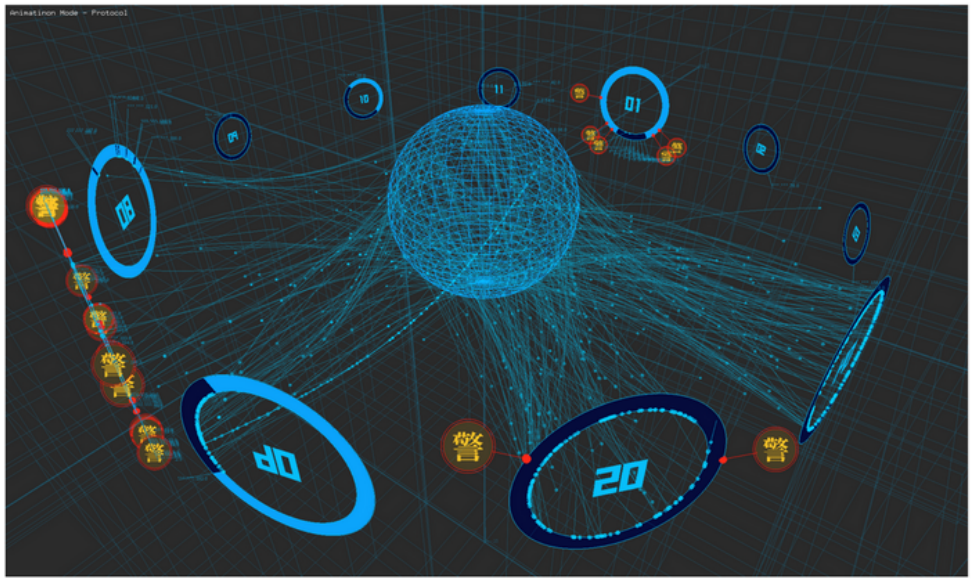


FIGURE 1.25 – Outil DAEDALUS permettant de monitorer des adresses IP du darknet en temps-réel et de manière interactive, extrait de [61] (© 2012, ACM).

Il existe de plus une certaine méfiance vis-à-vis des représentations de données en 3D, qui n'est pas cantonnée au domaine cyber. Nous présentons dans la partie 2.2.1 les avantages des visualisations 3D par rapport aux représentations 2D. Kullman *et al.* [73] présentent les avantages des visualisations immersives pour la cybersécurité par rapport aux représentations 2D sous forme de tableau de bord. La stéréoscopie ainsi que le changement de perspective sur les données lié aux mouvements de la tête (le *motion parallax*) permettent selon eux de mieux interpréter de grandes quantités de données.

FIGURE 1.26 – Visualisation d'événements réseau utilisant la métaphore de l'aquarium, extrait de [77] (© 2017, IEEE). Cette métaphore permet à des utilisateurs non experts en cybersécurité d'appréhender la situation du réseau et d'analyser les événements qui s'y déroulent.

Les outils de visualisation de données pour l'acquisition de la CSA, bien qu'adaptés aux pratiques et besoins des utilisateurs, n'utilisent que des représentations 2D des données, souvent présentées sous la forme de tableaux de bord. Ces tableaux de bords limitent l'interaction lorsque le nombre d'utilisateurs est trop élevé du fait de la limite de la taille d'affichage et ne tirent pas parti des possibilités qu'offrent les technologies immersives, qui pourraient faciliter l'interaction collaborative avec de grands volumes de données.

La CSA étant aussi une capacité qui doit s'acquérir, nous allons à présent nous pencher sur les outils d'entraînement pour la CSA et déterminer quelles sont leurs caractéristiques et limites.

1.2.2 Outils d'entraînement pour la CSA

La CSA dépend à la fois des outils de fusion de données et des capacités cognitives d'un opérateur humain. Ce dernier doit disposer de modèles mentaux pertinents quant à l'analyse de situations, modèles mentaux qui s'acquièrent via un apprentissage. Cet apprentissage en cybersécurité s'effectue sous deux formes, à savoir des exercices réalistes d'attaque et de défense de réseaux basés sur une architecture virtuelle appelée un Cyber Range et des mises en situation via des simulateurs. Subasu *et al.* ont représenté ces deux types d'entraînements sous la forme d'un continuum [116], avec d'un côté les exercices sur des réseaux créés de toutes pièces et d'un autre côté les exercices simulés de mise en situation (Figure 1.27).

Outils de Cyber Range

Les exercices de cybersécurité s'effectuent pour la plupart sur des réseaux isolés, afin de contrôler les sessions et d'éviter les effets de bords ou la propagation de *malwares* sur

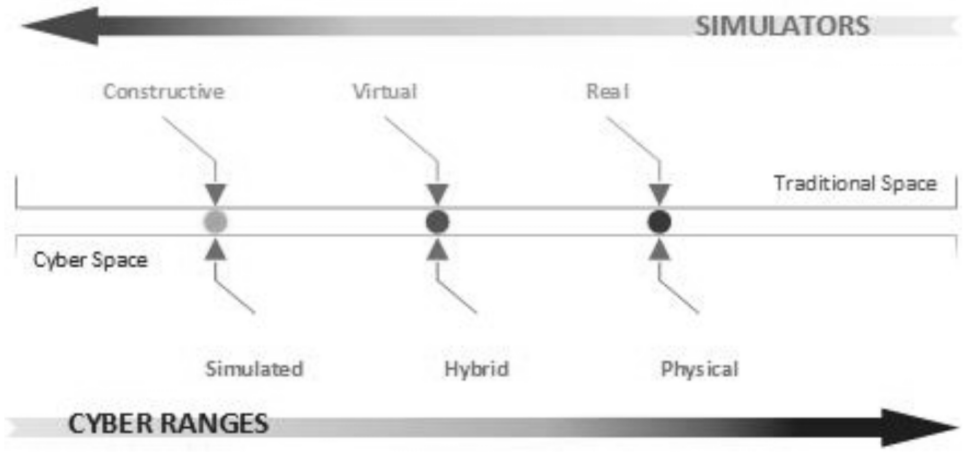


FIGURE 1.27 – Continuum des techniques d'entraînement utilisées en cybersécurité, extrait de [116] (© 2017, IEEE). Les outils de Cyber Range concernent des situations plus réalistes et un environnement d'entraînement physique (un réseau d'entraînement est alors crée) tandis que les simulateurs permettent des mises en situation simulées (simulateur de procédures d'alertes par exemple).

un réseau opérationnel. Des outils permettant de créer des réseaux virtuels et simulant un trafic de données, appelés Cyber Ranges, facilitent la mise au point d'exercices de formation. Les Cyber Ranges sont constitués de machines virtuelles générées par des outils permettant de les contrôler et de les mettre en réseau [97].

Les Cyber Ranges permettent de proposer des exercices réalistes à plusieurs utilisateurs, et sont donc utilisés comme plateformes collaboratives d'entraînement [95, 80].

Les exercices les plus souvent proposés sur les Cyber Ranges sont les *Capture The Flag* (CTF). Lors de ces exercices, les participants sont séparés en plusieurs équipes chargées de missions différentes, à savoir l'attaque d'un réseau, la défense de ce réseau et l'analyse et la gestion du déroulement de l'exercice. La Figure 1.28 présente l'organisation d'un exercice de CTF, le *Locked Shields* 2012 (LS12) : l'équipe rouge a pour objectif d'attaquer plusieurs infrastructures défendues par les équipes bleues, l'équipe blanche est là pour simuler la présence d'organismes externes pouvant aider les équipes bleues, et les équipes jaunes et vertes sont en support logistique et analysent le déroulement.

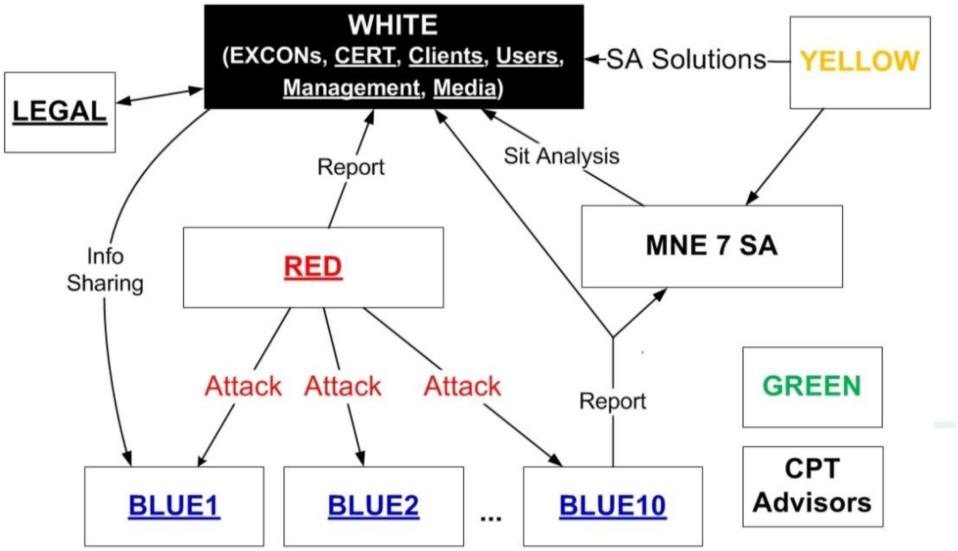


FIGURE 1.28 – Organisation de l'exercice de cyber défense Locked Shields 2012, dont l'objectif était d'entraîner les équipes bleues à défendre une infrastructure contre les attaques de l'équipe rouge.

Les CTF sont des exercices collaboratifs où les utilisateurs doivent utiliser des outils experts d'analyse comme ceux qu'ils utiliseraient lors de leurs activités professionnelles afin d'accomplir des objectifs prédéfinis (intrusion dans un système ou détection de l'intrusion).

Une comparaison des différents outils permettant de proposer des CTF a été présentée par Taylor *et al.* en 2017 [120] (Figure 1.29). Cette comparaison montre que la plupart des outils ont une architecture statique et ne sont pas ouverts aux modifications, ce qui limite leur déploiement et leur réutilisabilité.

La performance des utilisateurs lors d'un CTF est mesurée soit en comptabilisant les objectifs réalisés, soit en appliquant les méthodes d'analyse cognitive comme la *Cognitive Task Analysis* (CTA) présentée précédemment, qui permet d'évaluer la pratique des utilisateurs en fonction de modèles cognitifs [52]. La mise en place de scénarios 'gamifiés' est actuellement envisagée, afin de proposer d'autres métriques d'évaluation tout en ajoutant un aspect ludique aux exercices, comme présenté par Mäses *et al.* [89].

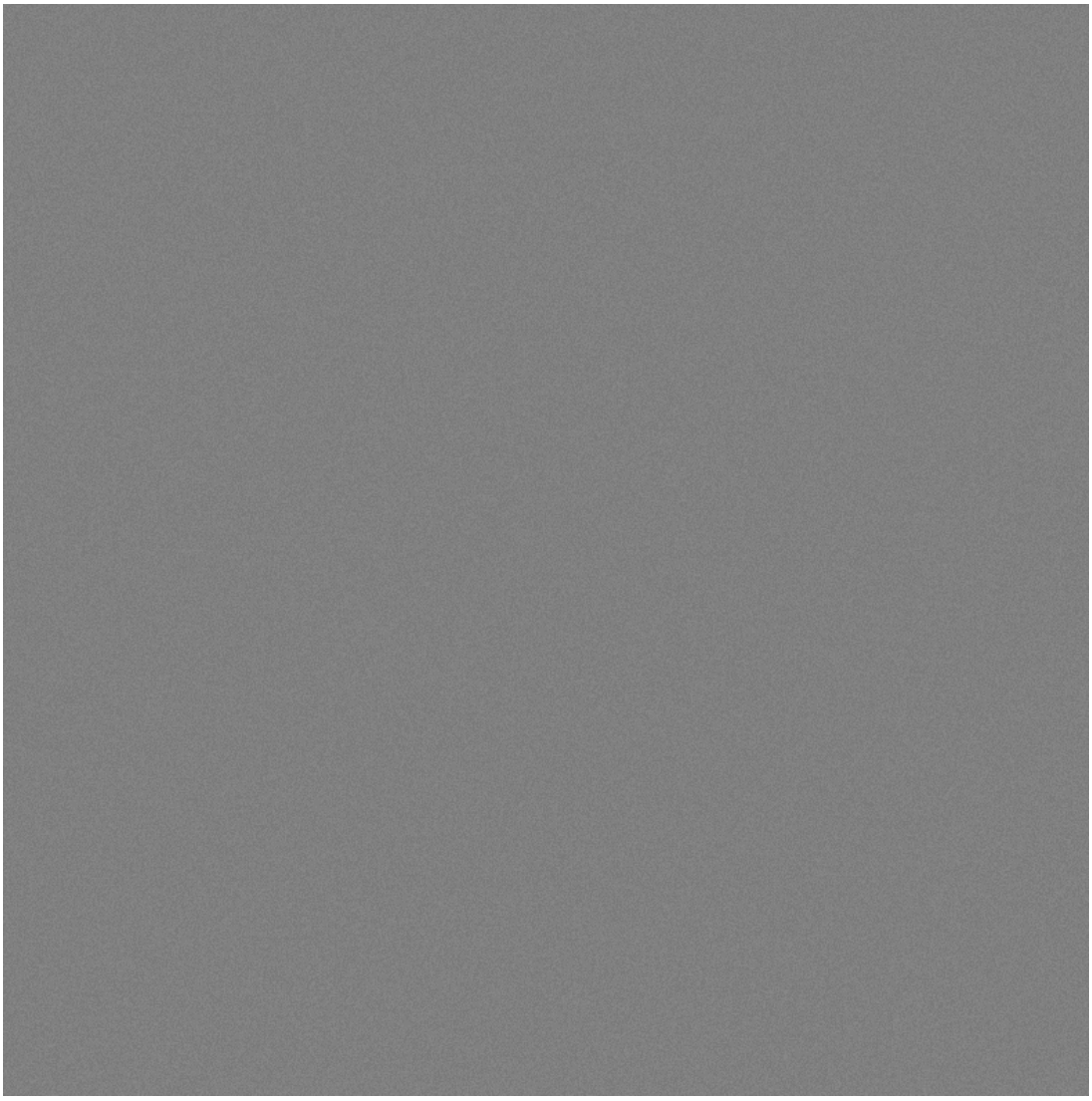


FIGURE 1.29 – Classification des outils de CTF, extraite de [120]. La plupart des outils présentés ont une architecture statique et ne sont pas open source.

Les outils de CTF sont très intéressants pour le maintien en condition opérationnelle des professionnels et pour la formation d'analystes ayant déjà des connaissances dans les outils et les activités cyber. Toutefois, ces outils ne sont pas adaptés à la formation des non-experts même s'il existe quelques propositions allant dans ce sens comme celle de Ford *et al.* [44]. Ils ne permettent actuellement pas d'obtenir une représentation immersive du réseau virtuel, ce qui pourrait aider à la compréhension de la situation, contrairement aux simulateurs de sensibilisation à la cybersécurité et de mise en situation.

Outils de simulation pour la cybersécurité

Il existe de nombreux jeux sérieux (*serious games*) pour la cybersécurité, ayant principalement pour objectif de sensibiliser de manière ludique des utilisateurs, étudiants ou professionnels, aux problématiques de la sécurité informatique. D'ailleurs, ces simulateurs

concernent la 'Security Awareness' et non pas la 'Situation Awareness' : la Security Awareness concerne une compréhension des enjeux et problématiques relatives à différents aspects de la sécurité informatique (aspects stratégiques, économiques, opérationnels, humains) tandis que la Situation Awareness concerne la capacité à comprendre une situation dans le domaine de la cybersécurité dans son ensemble. Les frontières entre ces deux CSA sont poreuses et c'est pour cela que des simulateurs permettant l'entraînement à la *Security Awareness* fonctionnent pour l'amélioration de la *Situational Awareness*.

Les jeux sérieux pour la CSA sont pour la plupart dédiés à la compréhension d'une situation de manière générale, sans entrer dans les détails de cette situation. Ils permettent de comprendre les risques et les conséquences d'attaques informatiques mais n'offrent pas la possibilité d'analyser la situation via des outils de visualisation par exemple, contrairement aux outils de CTF. De fait, ils sont plus adaptés à la formation des non-experts, à leur sensibilisation.

Toutefois, Nagarajan *et al.* [96] ont proposé CyberNex, un jeu sérieux basé sur des théories de game design et les recommandations du *NICE Security Workforce Framework*, issu des travaux du *National Institute of Standards and Technology* (NIST) américain. Ce *framework* a pour objectif de classifier les compétences à développer pour réaliser des tâches en cyber sécurité et permet donc de définir des scénarios adaptés aussi bien aux experts qu'aux novices en cybersécurité. L'outil CyberNex permet donc à des utilisateurs de différents degrés de compétence d'effectuer des scénarios encadrés et normalisés.

Les jeux sérieux pour la CSA se basent sur un moteur de jeu, et l'architecture du simulateur *CyberCIEGE*, proposé par Cone *et al.* [23] (Figure 1.30), est un bon exemple de la structure de ces outils d'entraînement. Ils sont composés d'un moteur de scénarios permettant d'implémenter des scénarios adaptés aux utilisateurs dans le simulateur. Ce simulateur est souvent composé d'une partie logique gérant les interactions et le déroulement de l'exercice, et d'une partie graphique proposant des interfaces immersives aux utilisateurs. Les traces d'exécution sont ensuite utilisées par l'instructeur et l'utilisateur afin de mesurer leur apprentissage.

Ces simulateurs ne sont toutefois pas collaboratifs et ne permettent pas une analyse détaillée de l'architecture d'un réseau simulé comme le permet un outil de Cyber Range. Mis à part la proposition de Subasu *et al.* [116] d'une architecture modulaire pour la formation en cybersécurité, il n'existe actuellement pas d'outils permettant à la fois d'immerger des utilisateurs dans un EV où ils doivent effectuer un scénario tout en leur laissant la possibilité d'analyser de manière précise des données simulées.

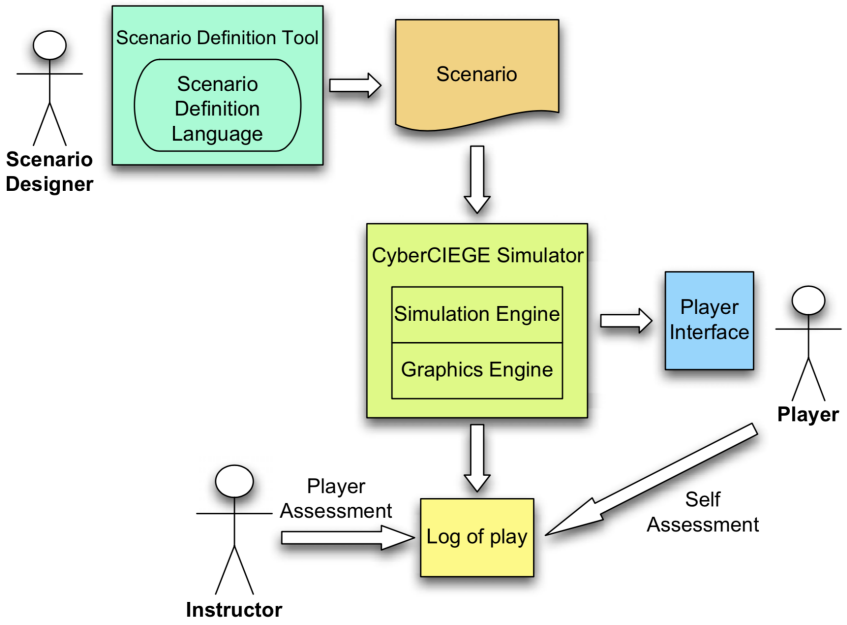


FIGURE 1.30 – Architecture du *serious game* CyberCIEGE [23] (© 2007, Elsevier), composée d'un moteur de scénarios qui permet de définir et d'implémenter des scénarios dans le simulateur, du simulateur à proprement parler qui gère la progression de l'utilisateur dans le scénario et qui lui propose une interface immersive adaptée, ainsi que d'un outil de visualisation des traces utilisateurs permettant à un instructeur d'évaluer la pratique de l'utilisateur.

Outils pour l'acquisition de la CSA

L'analyse de l'état de sécurité d'un système informatique se fait principalement via des outils de *Visual Analytics* (VA), qui proposent des vues agrégées des données et métriques d'un réseau. Ces outils se présentent la plupart du temps sous la forme de tableaux de bord 2D, développés à partir d'études des pratiques des analystes, et il n'existe actuellement que peu d'outils de visualisation 3D collaboratifs d'analyse permettant de faciliter l'acquisition d'une CSA. Cette dernière étant une capacité aussi bien technique que cognitive, les outils d'entraînement utilisés en cybersécurité participent aussi à son acquisition. Ces derniers se présentent principalement sous deux formes, des exercices dits de *Capture The Flag* (CTF) au cours desquels des équipes d'utilisateurs doivent défendre ou attaquer un réseau simulé, ou des simulations permettant de plonger un utilisateur dans une situation où il doit analyser les causes et conséquences d'attaques informatiques. Ces outils d'entraînement s'adressent soit à un public d'experts dans le cas des CTF, soit à un public de novices dans le cas des simulateurs. Il n'existe actuellement pas d'outils collaboratifs immersifs permettant à la fois d'interagir avec un réseau simulé et d'analyser une situation d'attaque informatique le tout de manière immersive.

1.3 Conclusion sur l'analyse de l'état de sécurité d'un système informatique

Le processus d'analyse de l'état de sécurité d'un système, aussi appelé la *Cyber Situational Awareness* ou CSA, résulte d'un couplage entre le traitement de données fournis par des outils de fusion d'informations et les processus cognitifs des cyber analystes. La CSA est obtenue par l'adéquation entre l'image d'une situation fournie par des outils d'analyse de données et l'image mentale que se forge un analyste utilisant ces outils. Les outils d'analyse de données pour la CSA actuels se basent principalement sur la métaphore du tableau de bord, qui est peu adaptée aux analyses collaboratives de grands volumes de données. Les outils d'entraînement à l'analyse de l'état de sécurité des systèmes informatiques sont soit dédiés aux experts, comme les outils d'attaque et de défense de réseaux, soit aux novices auxquels ils offrent des simulations de sensibilisation aux attaques informatiques. Il n'existe pas actuellement de solutions permettant à la fois d'analyser de manière immersive un réseau simulé tout en respectant les étapes d'un scénario de sensibilisation.

Nous pensons que les Environnements Virtuels Collaboratifs (EVC) pourraient favoriser l'acquisition de la CSA, à la fois en offrant des capacités de visualisation de données permettant de faciliter le monitoring temps-réel de systèmes, et en étant des outils de formation adaptés aux pratiques expertes ou non expertes. Nous allons présenter dans le chapitre suivant notre positionnement quant à l'utilisation d'EVC pour la CSA.

Chapitre 2

Réalité Virtuelle et Cybersécurité

Les casques immersifs comme l'Oculus Rift ou le HTC Vive ont relancé l'intérêt du grand public pour la Réalité Virtuelle (RV), mais cette dernière, bien qu'étudiée depuis des décennies, n'est pas toujours bien présentée ou exploitée, tout comme l'Intelligence Artificielle ou même la cybersécurité. On la limite trop souvent à l'utilisation ludique de casques immersifs, et une redéfinition nous semble nécessaire.

L'un des intérêts des Environnements Virtuels Collaboratifs (EVC) est qu'ils peuvent permettre à plusieurs utilisateurs d'interagir simultanément et de partager une expérience commune. Le développement de tels environnements nécessite toutefois la prise en charge de cette collaboration, que ce soit au niveau de la mise en réseau des applications, de la gestion multi-supports et de la représentation des utilisateurs, et de leurs actions dans l'environnement.

Les EVC peuvent être utilisés dans le cadre de la visualisation de données et sont utilisés aussi depuis des années pour proposer des situations immersives d'entraînement.

Dans ce chapitre nous allons dans un premier temps expliquer que la Réalité Virtuelle concerne l'étude et le développement de simulations dans lesquelles un ou plusieurs utilisateurs interagissent en temps réel. Nous allons détailler les contraintes techniques et ergonomiques que requiert le développement de telles simulations. Puis, nous montrerons que les EVC sont des outils pouvant favoriser le travail collaboratif et qu'ils peuvent être utilisés pour des tâches de visualisation de données ou de formation humaine.

2.1 Réalité Virtuelle Collaborative

Contrairement à ce que l'on peut constater en effectuant une recherche d'image sur internet (recherche "réalité virtuelle" ou "virtual reality") ou en lisant certaines définitions proposées par des sites de divertissement, la Réalité Virtuelle (RV) ne concerne pas seulement l'utilisation ludique de visiocasques.

Différentes définitions de la RV ont été proposées à la fin des années 90, lorsque l'essor de l'informatique et des technologies de la communication ont poussé des réflexions sur le virtuel et les cyberespaces créés par la mise en réseau d'ordinateurs [104]. La RV est souvent mal comprise car le sens des termes Réel, Virtuel ou Réalité sont interprétés hors du cadre de l'informatique ; dans ce cadre-ci, elle concerne des simulations temps réel interactives et adaptées à des besoins et des objectifs.

Le développement d'Environnements Virtuels (EV) nécessite donc de prendre en compte d'une part des contraintes techniques et d'autre part les capacités des utilisateurs à interagir entre eux ou avec l'environnement de manière naturelle. Ces contraintes doivent être respectées afin de ne pas briser l'immersion des utilisateurs et de faciliter la médiatisation de la collaboration.

Nous allons présenter dans cette section les définitions de la Réalité Virtuelle et décrire les contraintes existantes lors du développement d'environnements virtuels collaboratifs.

2.1.1 Définition(s) de la Réalité virtuelle

Les différences d'interprétation et de compréhension de la Réalité Virtuelle proviennent de plusieurs facteurs, dont la langue. En effet, le terme *Virtual Reality*, souvent attribué à Jaron Lanier, ingénieur en informatique, a le sens en anglais d'une quasi-réalité, une réalité incomplète, alors qu'en français le terme virtuel a le sens usuel de ce qui n'existe pas directement, qui n'est pas (encore) réel (virtuel provenant de *Virtus* en latin, la force ou le potentiel) [79]. Antonin Artaud est souvent cité comme le premier utilisateur de l'expression "réalité virtuelle", dans son oeuvre *Le Théâtre et son double* (1938). Pour Pierre Lévy, il existe différentes définitions du mot virtuel, philosophiques, usuelles et informatiques, présentées dans la Figure 2.1.

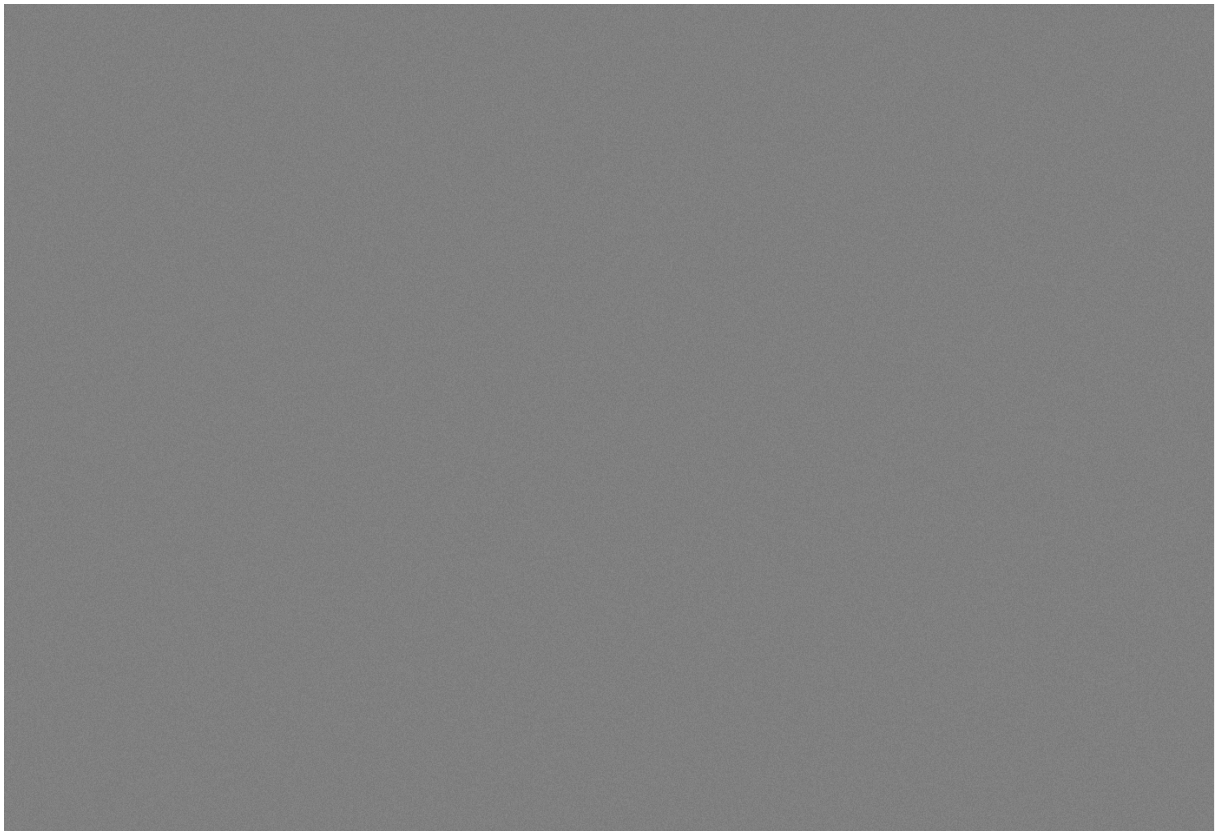


FIGURE 2.1 – Définitions du mot virtuel, en philosophie, dans le langage courant et en informatique, extrait de [104] (© 1997, Odile Jacob).

En fonction de la définition utilisée, Réalité Virtuelle devient donc un oxymoron, une figure de style décrivant le couplage de deux termes sémantiquement opposés (un clair-obscur, mort-vivant voire pour certains intelligence artificielle), ou un pléonasme, figure de style de renforcement (monter en haut, voir de ses yeux). Ce paradoxe, présenté aussi par Tisseau [122], est à la source de confusions et de fantasmes sur la Réalité Virtuelle et sur son rapport au Réel. Nannipieri et Fuchs [98] ont présenté ces liens entre Réalité Virtuelle et la Réalité, en précisant que l'on peut considérer que ces environnements (environnements virtuels et réels) coexistent dans un même espace physique, et que la Réalité Virtuelle ne va pas remplacer la Réalité.

Pour limiter ces confusions, une définition technique de la Réalité Virtuelle a été proposée par Bruno Arnaldi, Philippe Fuchs et Jacques Tisseau dans le premier chapitre du premier tome de l'édition de 2003 du *Traité de la Réalité Virtuelle* (TRV) [45], ouvrage rédigé par un consortium de chercheurs en informatique, sciences cognitives et psychologie :

> "La réalité virtuelle est un domaine scientifique et technologique exploitant l'informatique et les interfaces comportementales en vue de simuler dans un monde virtuel le comportement d'entités 3D, qui sont en interaction en temps-réel et avec un ou des utilisateurs en immersion pseudo-naturelle par l'intermédiaire de canaux sensori-moteurs."

Cette définition a pour avantage de mettre en évidence les caractéristiques techniques et humaines de la Réalité Virtuelle, à savoir qu'elle concerne à la fois les technologies immersives mais aussi la compréhension des interactions des utilisateurs.

En complément de cette définition, le modèle 3I2 (pour Immersion et Interaction) a été présenté par Fuchs, toujours dans le TRV [45] (Figure 2.2).

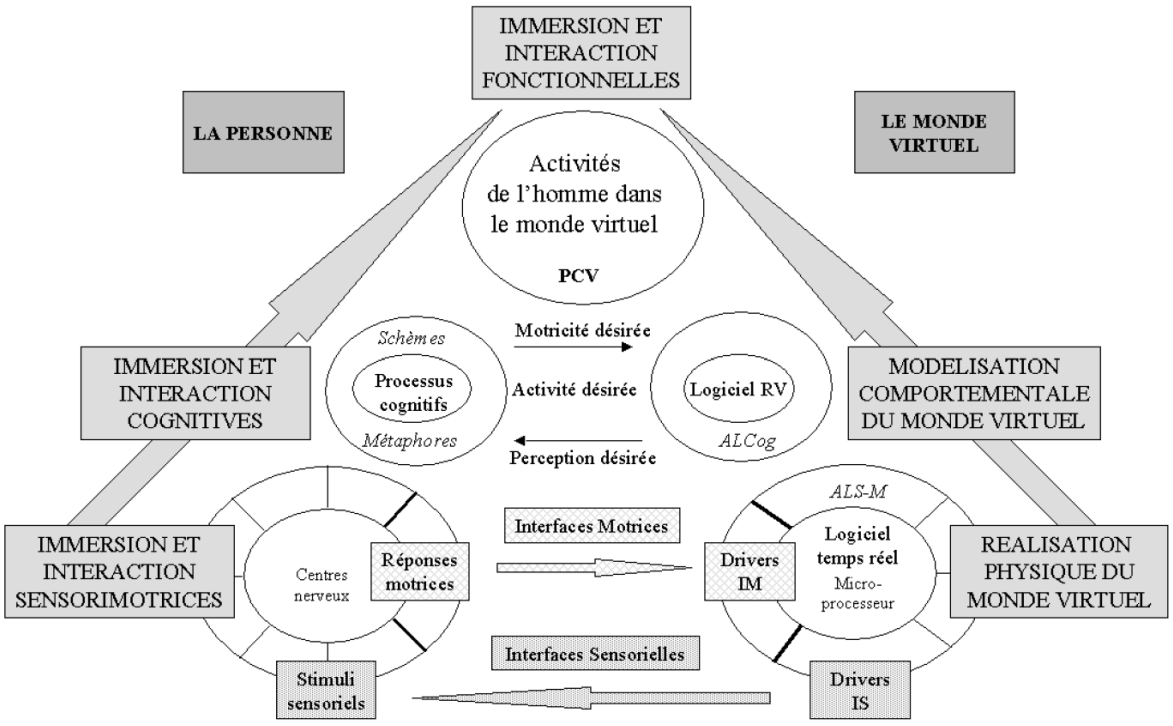


FIGURE 2.2 – Schéma technocentrique de référence en RV, extrait de [45].

Ce modèle décrit (de bas en haut) les différents processus humains et informatiques d'interaction et d'immersion sensori-motrices (l'utilisateur utilise des interfaces pour agir sur l'environnement), et d'interaction et d'immersion cognitives (l'environnement présenté est conforme aux schèmes mentaux de l'utilisateur), permettant une activité au sein d'un environnement virtuel. L'on parle aussi de boucles sensori-motrices et sémiotico-cognitives, comme le dirait Denis Berthier [33], permettant à un utilisateur d'agir et de comprendre l'environnement dans lequel il est immergé.

Immerger un utilisateur dans un EV nécessite donc de prendre en compte ces différents aspects afin qu'il se sente présent dans cet environnement, à savoir que ses actions et réactions soient semblables à celles qu'il aurait dans une situation réelle [114].

Dans la définition technique de la RV ainsi que dans le modèle 3I2, l'Immersion et l'Interaction sont considérées comme les bases des EV, mais une troisième dimension est parfois rajoutée, l'Autonomie.

En effet, l'autonomie de l'environnement et des agents qui le peuplent ajoute une certaine crédibilité à l'interaction, et le cube AIP (pour Autonomy, Interaction et Presence) proposé par Zeltzer [131] et revu par Tisseau [123] présente la RV comme un élément de coordonnée (1,1,1) dans la base (immersion,interaction,autonomie) (Figure 2.3).

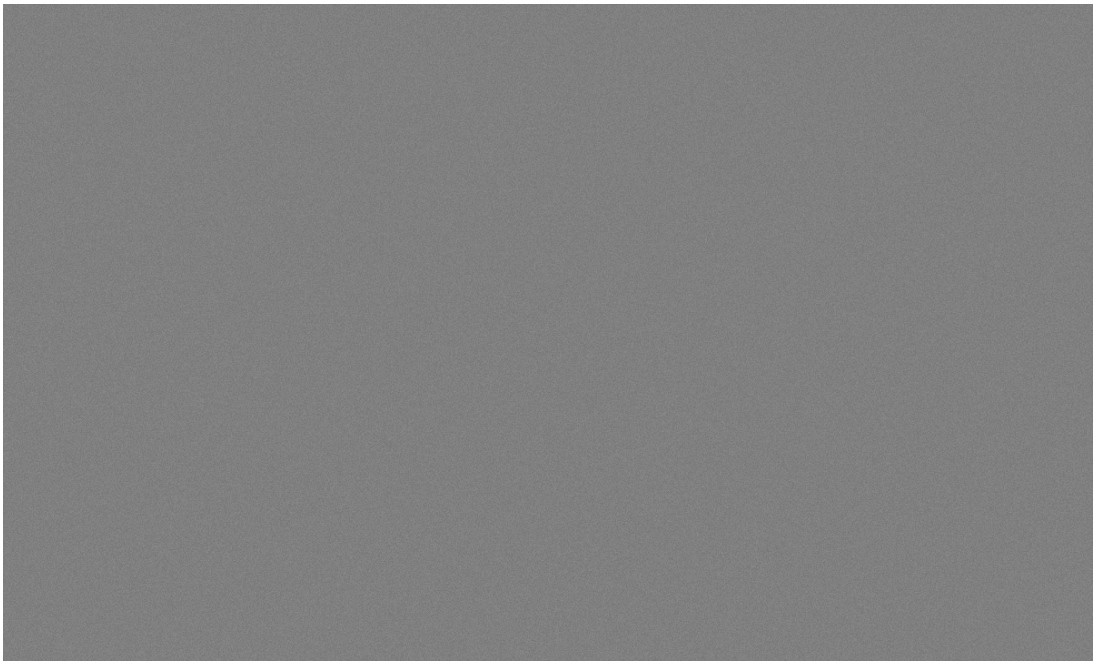


FIGURE 2.3 – cube AIP représentant trois dimensions (Autonomie, Interaction et Présence) des Environnements Virtuels, extrait de [123].

Cette définition permet de séparer les jeux vidéo, les simulateurs et le cinéma 3D des applications de la réalité virtuelle, et est résumée par cette formule de Tisseau :

> La réalité virtuelle permet de vivre une expérience cognitive et sensori-motrice dans un univers peuplé d'entités autonomes et d'avatars d'utilisateurs. En d'autres termes, elle permet de **vivre une expérience de pensée**.

Une autre dimension est parfois rajoutée aux définitions de la Réalité Virtuelle, celle de la Narration Interactive, ou Interactive Storytelling (IS). En effet, même si le schéma précédent la montre comme un point de la base (immersion, interaction, autonomie), Nannipieri et Fuchs nous rappellent que les EV sont toujours développés en fonction d'objectifs que doivent réaliser les utilisateurs [98]. Les conséquences de leurs actions sont prédéfinies et modifient l'environnement de manière à leur permettre de se rapprocher ou non des objectifs. La narration permet de décrire la causalité entre les actions et est donc implicitement présente dans les EV, comme présenté par Aylett et Louchart [4] (Figure 2.4).

	Cinema	**Theatre**	**Literature**	**VR**
Contingency on time and space	Low	Medium	Low	Strong
Narrative Representation	Visual	Visual	Mental	Visual
Presence	Not physical	Physical	Not physical	Not physical but immersive
Interactivity	No	No / Yes in the case of interactive theatre	No	Yes

FIGURE 2.4 – la Réalité Virtuelle décrite comme forme narrative, extrait de [4] (© 2003, Springer). La RV est une forme narrative disposant d'une forte unité de temps et d'espace, immergeant les utilisateurs dans un environnement immersif et interactif par des interfaces visuelles.

Nous avons vu dans cette partie que la Réalité Virtuelle concerne en informatique le développement d'environnements graphiques en 3D temps réel et interactifs, dans lesquels des utilisateurs interagissent afin de réaliser un objectif. Le développement de tels environnements nécessite de prendre en compte des contraintes techniques et ergonomiques que nous allons présenter dans la partie suivante.

2.1.2 Développement des Environnements Virtuels Collaboratifs

Il y a deux décennies, Philippe Coiffet considérait que les limitations techniques des ordinateurs rendaient impossible le développement d'EV suffisament immersifs pour que des utilisateurs 'croient' à leur présence dans un monde virtuel [22]. Comme montré sur la Figure 2.5, les traitements successifs des informations utilisateurs, entre l'interaction et l'affichage, entraînent des délais ou retards qui peuvent, s'ils sont trop importants, compromettre l'immersion des utilisateurs [62] voire les rendre malades.

Comme précisé par Raaen et Kjellmo [106], l'évaluation des valeurs limites de ces délais est complexe car elle dépend des utilisateurs. John Carmack, alors directeur technique d'Oculus, a toutefois précisé qu'une latence comprise entre vingt et cinquante millisecondes était recommandée pour l'utilisation de casques immersifs [1].

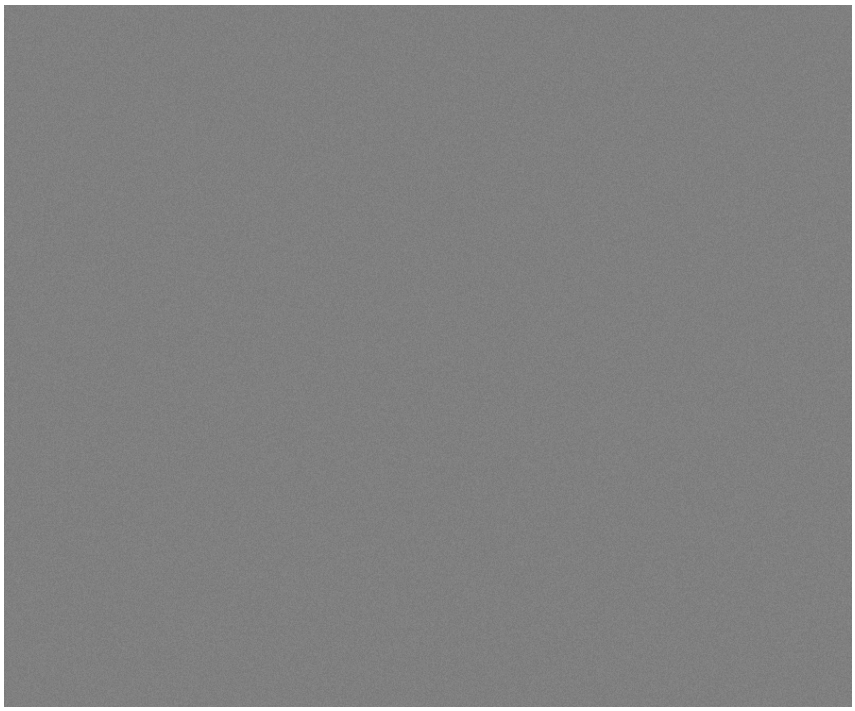


FIGURE 2.5 – Retard cumulé des différentes couches de traitement de l'information en réalité virtuelle impactant l'immersion et la présence, extrait de [62].

1. https://danluu.com/latency-mitigation/

Or, l'informatique a fait des progrès quasi exponentiels dans tous les domaines (puissance de calcul graphique ou logique, stockage, connexions réseau...) depuis l'apparition des premiers dispositifs immersifs, ce qui a favorisé le développement d'EVC utilisables et suffisamment immersifs pour que des expérimentations ou des sessions de jeu puissent être effectuées sans indisposer les utilisateurs.

À titre d'exemple, dans les années 1990, le casque immersif EyePhone HRX proposé par la société VPL Research de Jaron Lanier coûtait quarante-neuf-mille dollars et disposait d'un *tracking* de tête et d'une résolution d'affichage de 720x480 pixels [2]. Ce casque nécessitait une station graphique pour fonctionner, et le coût total du système était évalué à deux cent-cinquante mille dollars, pour un taux de rafraîchissement n'atteignant pas les trente images par seconde [3]. Le casque HTC Vive pro sorti en avril 2018 dispose d'une résolution de 2880x1600 pixels, d'accéléromètres, de gyroscopes ainsi que d'un système de positionnement infrarouge pour le *tracking* de la tête et des mains de l'utilisateur, pour un prix de huit cent dollars [4]. Pour le faire fonctionner à un taux de rafraîchissement de quatre-vingt-dix images par secondes, un ordinateur à deux mille euros suffisait en 2018. Il est donc actuellement possible de développer des EVC dans lesquels des utilisateurs peuvent jouer, apprendre, expérimenter, bref vivre des Expériences Utilisateurs.

Bien que le développement de tels environnements soit régi par des contraintes liées aux systèmes distribués, aux applications graphiques et interactives [139], ce dernier a été facilité par l'utilisation d'outils complets comme les moteurs de jeu, qui sont composés de briques technologiques gérant différents aspects des EV ou de simulations 3D (Figure 2.6), et qui nous permettent dorénavant de nous focaliser sur les contraintes ergonomiques liées à l'interaction et à la médiatisation de la collaboration entre les utilisateurs et non plus sur les problématiques techniques de réalisation des environnements.

2. `https://apps.dtic.mil/dtic/tr/fulltext/u2/a263498.pdf`
3. `https://delta2020.com/blog/221-here-s-what-you-didn-t-know-about-the-history-of-virtual-reality`
4. `https://www.digitaltrends.com/virtual-reality/oculus-rift-vs-vive-pro/`

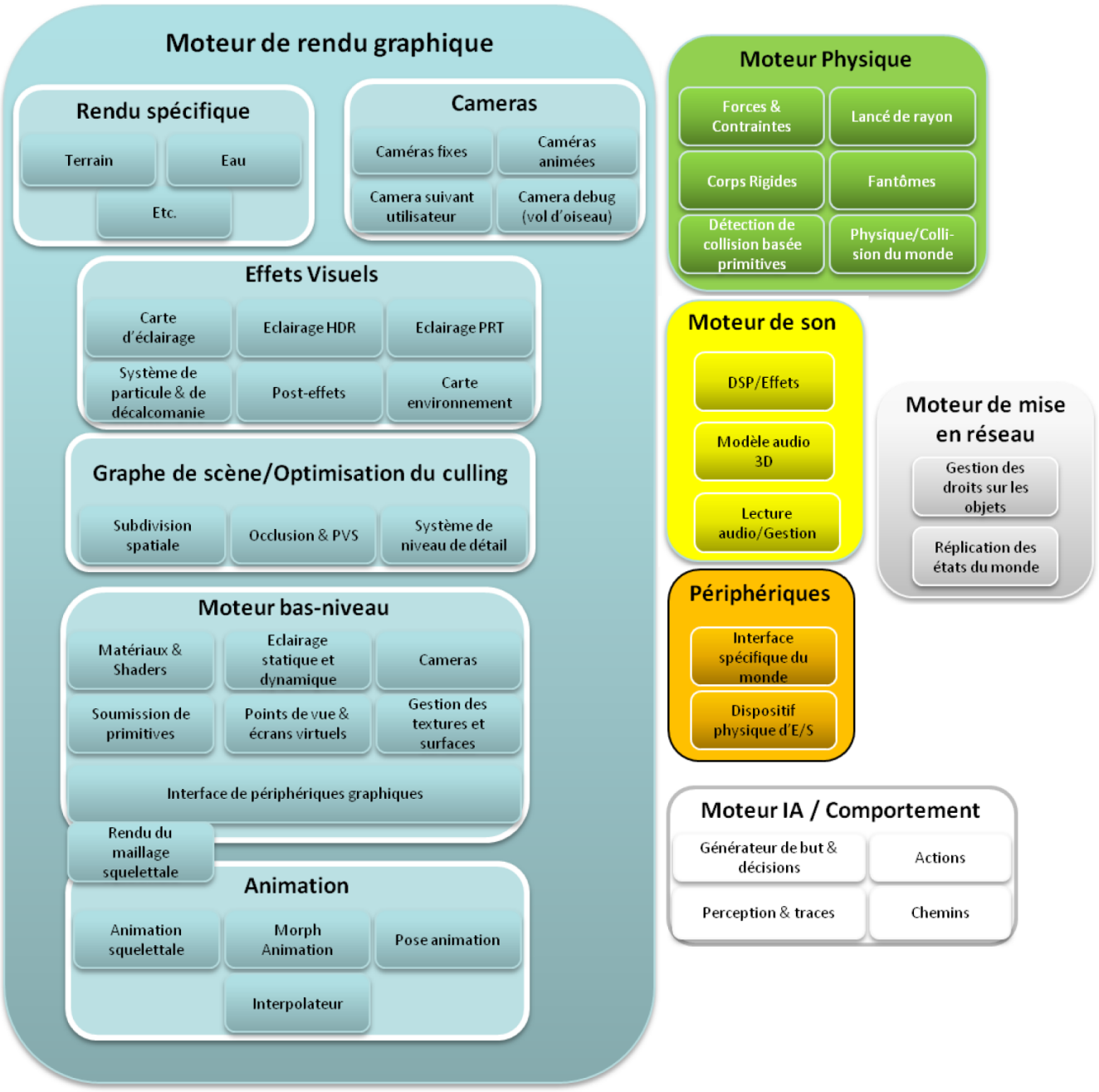


FIGURE 2.6 – Briques technologiques d'un moteur de jeu, extraites de [9]. Ces dernières peuvent être utilisées sans difficultés techniques (dans la plupart des cas), ce qui fait que le développeur d'applications immersives peut se concentrer actuellement sur les contraintes ergonomiques de l'utilisation des EV.

Les EVC sont constitués de cinq caractéristiques, selon Zyda et Singhal [139], qui doivent être prises en compte afin d'offrir aux utilisateurs une sensation de présence :

1 Le partage de l'espace (*Shared sense of space*), en mettant les utilisateurs dans le même environnement.

2 Le partage de la présence (*Shared sense of presence*), en utilisant des avatars ou autres métaphores représentatives des actions des utilisateurs.

3 Le partage du temps (*Shared sense of time*), permettant aux utilisateurs d'interagir et de collaborer en temps réel entre eux et avec l'environnement.

4 La communication entre utilisateurs (*Way to communicate*), de manière verbale ou non verbale.

5 La capacité d'échanger de l'information ou des informations (*Way to share*), permettant aux utilisateurs de coopérer pour effectuer des tâches spécifiques par exemple.

La Figure 2.7 présente un EVC pour la revue de projet, proposé par la société WorldViz.

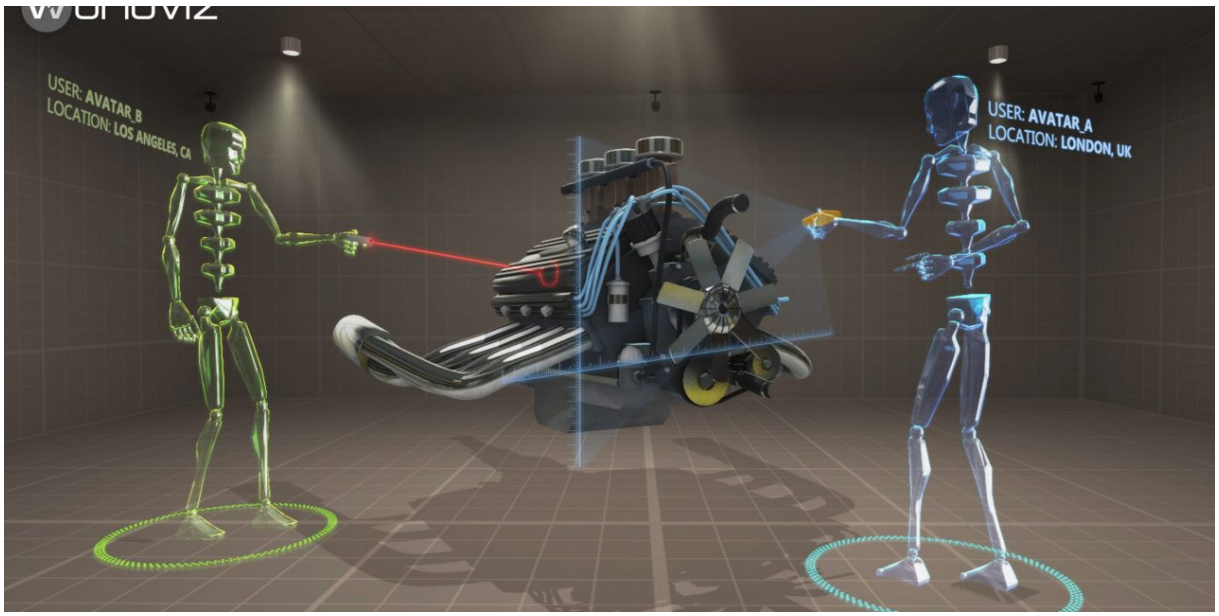


FIGURE 2.7 – EVC de l'entreprise WorldViz. Les caractéristiques des EVC décrites précédemment sont représentées par l'environnement lui-même ainsi que par les avatars et les méthodes d'interaction. Image extraite de `https://designandmotion.net/news/worldviz-announces-new-virtual-reality-communication-platform/`.

Les caractéristiques de temps et d'espace (**1** et **3**) sont représentées par l'environnement dans lequel évoluent les avatars des utilisateurs tandis que les capacités collaboratives (**2**, **4** et **5**) sont représentées par les avatars et leurs méthodes d'interaction.

Les EVC sont aussi considérés par bien des aspects comme des outils de *Computer Supported Cooperative Work* (CSCW), outils médiatisant la collaboration entre utilisateurs par l'utilisation de l'informatique. Dès 1998, Elizabeth Churchill [20] proposait des

caractéristiques des outils de CSCW devant être prises en compte dans les EVC, comme la transition entre des activités individuelles ou partagées, la perception des autres utilisateurs et la mise à disposition de plusieurs points de vue. En 2018, soit vingt ans après, Julien Casarin [17] présentait les caractéristiques des outils de CSCW nécessaires à la gestion de tâches collaboratives, comme l'implémentation de rôles utilisateurs, l'incarnation dans des avatars et la malléabilité (flexibilité) des interfaces proposées.

Dans la Table 2.1 nous exposons ces caractéristiques ainsi que les liens qu'elles présentent avec les caractéristiques des EVC proposées par Zyda et Singhal [139]. Ces dernières n'ont que peu évolué en vingt ans, et regroupent à la fois des composantes graphiques de l'environnement (par exemple les *feedbacks* d'interaction) et des composantes conceptuelles (la proposition de plusieurs points de vue et les transitions entre activités).

TABLE 2.1 – Caractéristiques des CSCW devant être implémentés dans les EVC, et lien avec les cinq caractéristiques des EVC proposées par Zynda et Singhal [139].

Selon Churchill [20]	**Selon Casarin [17]**
Transitions between shared and individual activities **(2,3,5)**	Individual feedbacks **(2,5)**
Flexible and multiple viewpoints **(2,5)**	User roles **(2,4,5)**
Sharing context **(1,3,5)**	Shared content and feedbacks **(1,2,3,4,5)**
Awareness of others **(1,2,3)**	Embodiments **(1,2,4,5)**
Negotiation and Communication **(3,4,5)**	Communication **(4,5)**
	Coordination mechanisms **(1,2,3,4,5)**
	Malleability **(4,5)**

Les propriétés décrites par Churchill et Casarin concernent à chaque fois plusieurs caractéristiques des EVC proposées par Zynda et Singhal. Par exemple, la propriété *Awareness of others* proposée par Churchill concerne les caractéristiques de partage de l'espace, de la présence et du temps (**1**, **2** et **3**) entre les utilisateurs d'un EVC. La propriété *User roles* présentée par Casarin concerne seulement les caractéristiques de partage de présence, de communication et d'échange d'informations entre utilisateurs (**2**, **4** et **5**), car le partage de l'espace et du temps ne sont pas nécessaires aux utilisateurs disposant de différents rôles au sein d'un EVC. En revanche, les propriétés de partage de contenu et de *feedbacks*, et les mécanismes de coordination (*Shared content and feedbacks* et *Coordination mechanisms*) concernent toutes les caractéristiques des EVC selon Casarin, car les utilisateurs doivent pouvoir agir dans un même espace-temps et doivent se percevoir afin de se coordonner et partager du contenu.

Dans cette partie nous voulions montrer que les EVC sont des environnements complexes à développer, et que bien que les technologies aient facilité leur conception, la prise en compte des facteurs ergonomiques ainsi que des facteurs issus des outils de CSCW est nécessaire afin de proposer aux utilisateurs une interaction adaptée à leurs besoins et une médiatisation efficace de la collaboration.

Réalité virtuelle collaborative

La Réalité Virtuelle connaît un regain d'intérêt suite à l'arrivée de visiocasques grands publics et d'ordinateurs performants. Toutefois, elle est parfois mal définie et mal interprétée. La Réalité Virtuelle concerne en informatique le développement de simulateurs en temps réel permettant à des utilisateurs d'interagir dans un environnement afin de réaliser un objectif. Le développement de ces environnements a été facilité par l'émergence de moteurs de jeux et par l'évolution des technologies de communication et d'interaction. Les aspects ergonomiques de ces environnements, peu dépendants des technologies, doivent cependant être pris en compte afin d'offrir une capacité d'immersion suffisante aux utilisateurs. La gestion de la collaboration au sein des Environnements Virtuels nécessite de prendre en compte des caractéristiques spécifiques comme la gestion de la représentation des utilisateurs et de leurs interactions, ainsi que l'utilisation de moyens de communication ou d'échange d'informations. Ces caractéristiques font que les EVC peuvent être considérés comme des outils de *Computer Supported Cooperative Work* (CSCW).

2.2 Réalité Virtuelle et Cybersécurité

La Réalité Virtuelle et le Cyberespace ont été présentés comme connexes dans les oeuvres des années 90 traitant des nouvelles technologies, comme le livre *Cyberculture* de Pierre Lévy [79]. De même, dans la science fiction, le Cyberespace est vu comme un Environnement Virtuel où des utilisateurs peuvent visualiser les données d'un réseau et interagir avec ces dernières de manière 'naturelle', comme si les éléments le composant étaient physiques, comme dans *Neuromancien* de Gibson [50].

Toutefois, bien que le Cyberespace soit décrit comme un environnement parallèle à l'environnement physique et qu'il soit même cartographié (comme par exemple avec *l'atlas du Cybersespace* de Dodge et Kitchin [35]), les pratiques en cybersécurité, à savoir l'analyse et la mise en place d'outils de contrôle de cet espace, sont très éloignées des problématiques des EV. Pour reprendre l'adage de Korzybsky, "La carte n'est pas le territoire" [70] : les représentations de l'environnement cyber ne reflètent pas les pratiques actuelles des cyber opérateurs, qui opèrent à un niveau bien plus pragmatique.

Néanmoins, nous défendons dans cette thèse l'utilité des EVC pour la cybersécurité à travers deux domaines dans lesquels ils sont utilisés de manière efficace, à savoir la visualisation de données et l'entraînement humain. Comme montré dans le chapitre précédent, ces domaines sont utilisés afin d'aider à la *Cyber Situational Awareness* (CSA), la compréhension de l'état de sécurité d'un système. Nous avons présenté notre positionnement dans un résumé étendu [66] du workshop 3D Collaborative Virtual Environments (3DCVE), affilié à la conférence IEEE VR.

2.2.1 Visualisation 3D immersive de données

Il existe depuis des années un débat dans les communautés de la visualisation de données, qui concerne l'utilisation des représentations 3D par rapport aux représentations 2D [37]. Ces dernières sont souvent préférées par leur facilité de développement et l'intuitivité de leurs interprétations [68], mais Mariott et al. ont montré que l'écart de performance entre représentations 2D et 3D était assez faible concernant la visualisation de données multivariées [86]. Bien que l'utilité des visualisations 3D ait été montrée dans certains domaines, comme les visualisations de données volumétriques [76] ou l'analyse de clusters [129], ces dernières ne sont pas souvent exploitées [46].

Pourtant, l'utilisation de visiocasques possédant des capteurs de position, ou l'utilisation de salles ou murs immersifs couplés à des lunettes stéréoscopiques permettent aux utilisateurs de visualiser les données sous différents angles et de mieux apprécier les distances, ce qui favorise la compréhension de ces données. Mariott et al. montrent que les bénéfices des représentations immersives concernent l'utilisation de la profondeur comme dimension abstraite, la visualisation sur surfaces non-planes, la représentation spatiale de données abstraites, l'utilisation de plusieurs vues à la fois dans l'environnement ainsi que

l'engagement accru des utilisateurs [86] (Figure 2.8).

	Linear Perspective	Aerial Perspective	Occlusion	Motion Perspective	Accommodation	Convergence	Binoc. Disparity and Stereopsis	User-controlled PoV	Subjective Motion	Interactive Content Manipulation	Examples
Regular photography or print	Y	Y	Y	N	N	N	N	N	N	N	
Desktop Computer Virtual Reality	Y	P	Y	Y	N	D	D	Y	N	D	[87]
Fishtank Virtual Reality	Y	P	Y	Y	N	D	D	P	Y	D	[104]
Non-disparity monocular/binocular viewing	Y	P	P	P	N	N	N	P	P	D	[99]
Head-mounted Binocular Displays	Y	P	Y	Y	N	Y	Y	P	Y	D	[90]
Multi-display Environments, Large Displays	Y	P	Y	Y	N	N	N	P	P	D	[43, 72, 73]
Binocular CAVEs	Y	P	Y	Y	N	Y	Y	P	Y	D	[22]
Gazer (Simulation of Accommodation)	Y	P	P	P	D	P	P	P	P	D	[66, 67]
Accommodation Optics VR Headset	Y	P	P	P	Y	Y	Y	P	Y	D	[81]
Multiview Autostereoscopic	Y	P	Y	Y	D	Y	Y	P	Y	D	[25, 49]
Volumetric 3D Displays	Y	N	N	Y	Y	Y	Y	P	Y	D	[36]
Optical Holographic 3D Displays	Y	N	N	Y	Y	Y	Y	P	Y	D	[55]
Augmented Reality (AR)	Y	P	D	Y	D	D	Y	N	Y	D	[5]
AR Hybrids	Y	P	Y	Y	D	D	Y	D	P	D	[56]
Physical Visualisations (reality)	Y	P	Y	Y	Y	Y	Y	N	Y	Y	[52]

FIGURE 2.8 – Gestion des indices de profondeur en fonction des technologies immersives, tiré de [86] (© 2018, Springer). La couleur verte foncée (lettre Y) indique que l'indice de profondeur est géré par le dispositif. La couleur verte claire (P) indique une possibilité de gestion, la couleur jaune (D) indique que des adaptations du dispositif sont nécessaires pour la gestion de l'indice, et la couleur rouge (N) indique une impossibilité de gestion à l'heure actuelle.

L'un des avantages des visualisations de données 2D est qu'elles sont plus faciles à développer et à implémenter que les visualisations 3D. En effet, il existe de nombreux outils de prototypage de visualisations 2D (Figure 2.9) et de guides de visualisation permettant de représenter des données sous des formes prédéfinies, comme la classification périodique des méthodes de visualisation proposée par Lengler et Eppler [78] (Figure 2.10).

Tool	Description	URL
D3.js	JavaScript library	http://d3js.org
Flare	ActionScript library	http://flare.prefuse.org
Google Public Data Explorer	Online data analysis and visualization program	www.google.com/publicdata
InfoVis Toolkit	Java library	http://ivtk.sourceforge.net
Mathematica	Commercial computation and visualization system	www.wolfram.com/mathematica
Matlab	Commercial numerical-computing environment	www.mathworks.com/products/matlab
Many Eyes[1]	IBM research project	www-958.ibm.com/software/data/cognos/manyeyes
NodeXL	Excel template	http://nodexl.codeplex.com
OpenGL[2]	C library for computer graphics programming	www.opengl.org
Piccolo2D[3]	Java and .NET library	www.piccolo2d.org
Prefuse[4]	Java library	http://prefuse.org
Processing[5]	Programming language	http://processing.org
Protovis	JavaScript library	http://mbostock.github.com/protovis
R	Statistical-computing software	www.r-project.org
Spotfire	Commercial tool for business data analysis	http://spotfire.tibco.com
Tableau[6]	Commercial tool for business data analysis	www.tableausoftware.com
XmdvTool[7]	Tool for multivariate data visualization	http://davis.wpi.edu/xmdv

FIGURE 2.9 – Liste d'outils de développement de visualisations de données, extrait de [137] (© 2012, IEEE). Ces outils sont utilisés dans les cours de visualisation de données par exemple.

Il n'existe à ce jour que peu d'outils de développement de visualisations de données immersives comme l'adaptation du *Visualization ToolKit* (VTK) aux EV par O'Leary *et al.* [100] ou l'outil DXR par Sicat *et al.* [112] (Figure 2.11). Büschel *et al.* [14] rappellent qu'une interface de visualisation doit respecter certains critères comme fournir des feedbacks d'interaction immédiats et l'utilisation de transitions douces entre les vues, tout en précisant que les interfaces immersives nécessitent à la fois plus de temps de développement et plus de puissance de calcul, ce qui peut expliquer le faible nombre d'outils immersifs de visualisation de données.

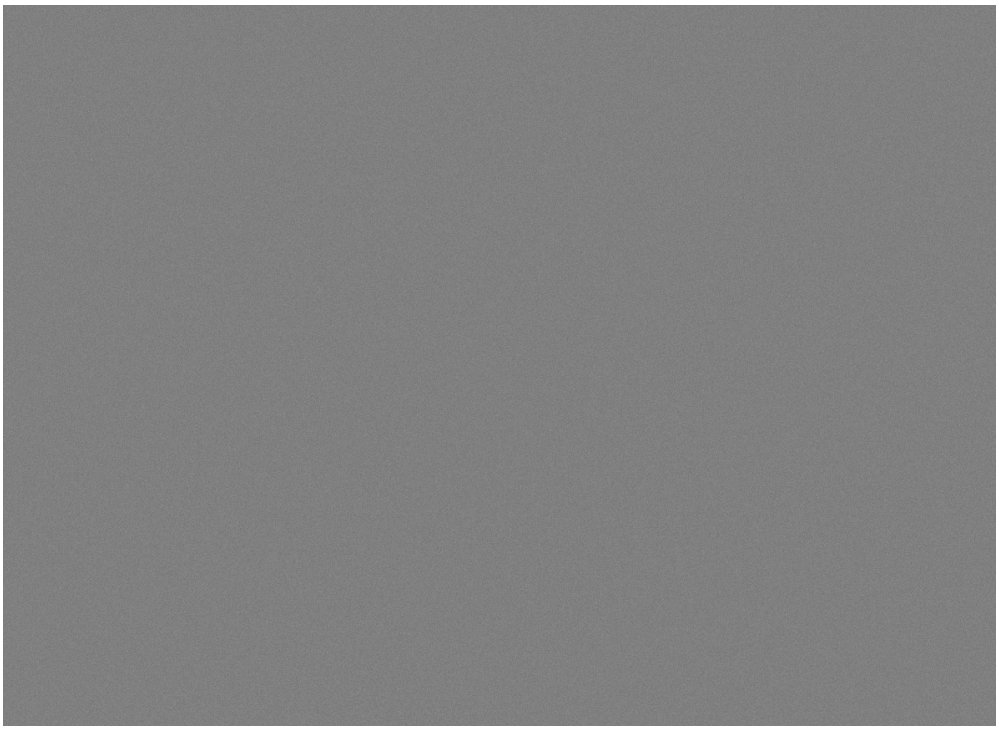


FIGURE 2.10 – Classification périodique des méthodes de visualisation, tiré de [78]. Cette table permet de choisir la représentation de données appropriée en fonction des besoins et de la nature des informations à afficher.

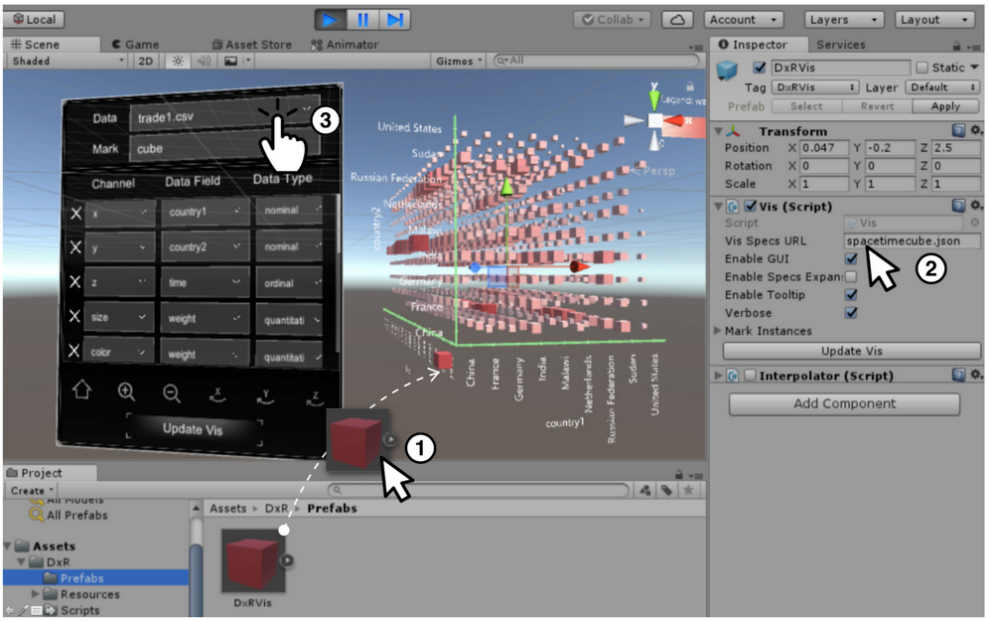


FIGURE 2.11 – Outil DXR de développement de visualisations de données immersives, extrait de [112] (© 2019, IEEE).

Les visualisations immersives nécessitent des algorithmes de représentation spécifiques [67] et des métaphores d'interaction adaptées [71, 128], afin de faciliter la prise en main et de tirer parti des caractéristiques des EV. Citons par exemple *ImAxes* [25] de Cordeil *et al.*, qui permet de croiser des graphes 2D au sein de l'environnement 3D afin de détecter des corrélations ou des relations entre les données (Figure 2.12).

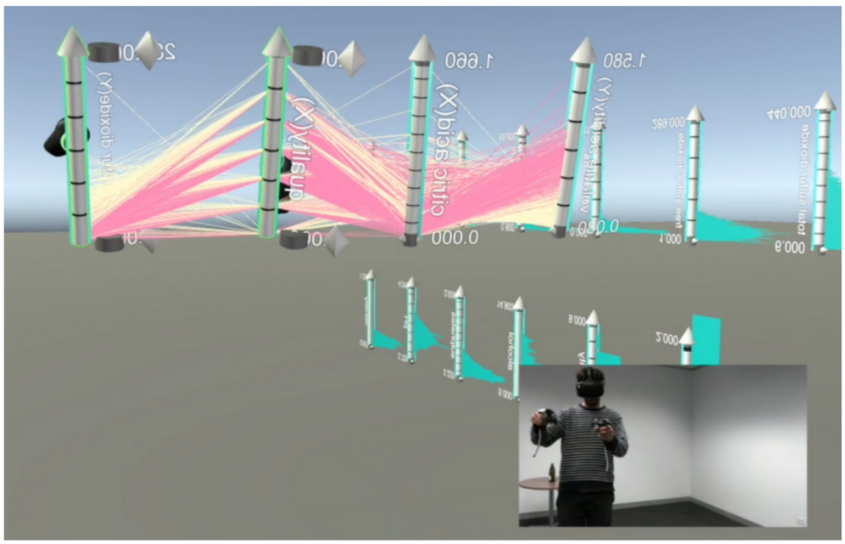


FIGURE 2.12 – ImAxes, extrait de [25] (© 2017, ACM). Cette métaphore d'interaction permet de croiser des graphes 2D afin de voir directement les corrélations entre les données.

Des EVC et frameworks collaboratifs pour la visualisation de données ont été proposés par Duval *et al.* [38], Donalek *et al.* [36] et Nguyen *et al.* [99], et le domaine des *Collaborative Immersive Analytics* est en plein développement quoique relativement récent. Le terme *Immersive Analytics* a été en effet présenté par Chandler et Hackathorn en 2015 [18, 55], et un premier livre sur le domaine a été publié en 2018 [87]. Butscher *et al.* [15] ont proposé par exemple en 2018 un environnement de réalité mixte collaboratif permettant d'analyser des données multidimensionnelles grâce à des coordonnées 3D parallèles et une table tactile (Figure 2.13).

L'analyse de données étant nécessaire quant à l'acquisition d'une CSA, la visualisation de données peut être utilisée pour réaliser cet objectif, et l'on peut considérer que les objectifs des visualisations immersives collaboratives correspondent à l'acquisition d'une CSA, comme représenté par notre adaptation du schéma proposé par Billinghurst *et al.* [7] (Figure 2.14).

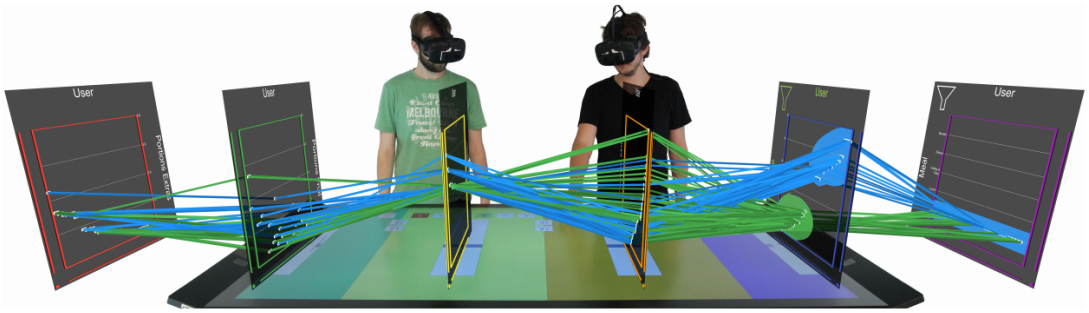


FIGURE 2.13 – Exemple d'un environnement de *Collaborative Immersif Analytics* permettant l'analyse collaborative de données multidimensionnelles, extrait de [15] (© 2018, ACM). Les utilisateurs munis de casques de Réalité Virtuelle interagissent sur des données via des gestes et via l'utilisation d'une table tactile.

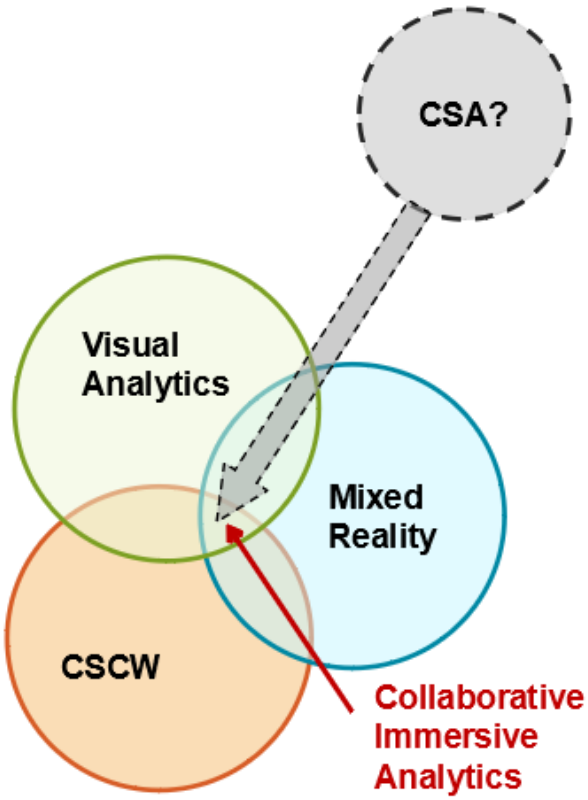


FIGURE 2.14 – Adaptation du schéma décrivant le domaine de la *Collaborative Immersive Analytics*, extrait de [7]. Nous avons rajouté la CSA, qui peut être acquise via des outils de CSCW immersifs et dédiés à l'analyse de données.

La plupart des données cyber étant représentées sous forme de graphe, l'utilisation de graphes immersifs semble prometteuse, comme présenté par Kwon *et al.* [74], mais d'autres métaphores peuvent aussi être envisagées.

Les EVC semblent donc utilisables pour fournir des représentations de données immersives aux cyber analystes. Nous allons maintenant montrer que leurs capacités de formation humaine peuvent aussi être utilisées pour favoriser l'analyse de l'état de sécurité d'un système.

2.2.2 Environnements Virtuels pour l'Apprentissage Humain

L'utilisation de la RV pour l'entraînement et l'apprentissage a été étudiée très tôt. Par exemple, William Winn présentait en 1993 le potentiel de la RV pour l'éducation [130] et Domitile Lourdeaux soutenait sa thèse de doctorat [82] relative à la conception d'environnements virtuels pédagogiques en 2001. La même année, Erica De Vries présentait une classification des logiciels d'apprentissage par rapport à leurs fonctions pédagogiques [32] (Figure 2.15).

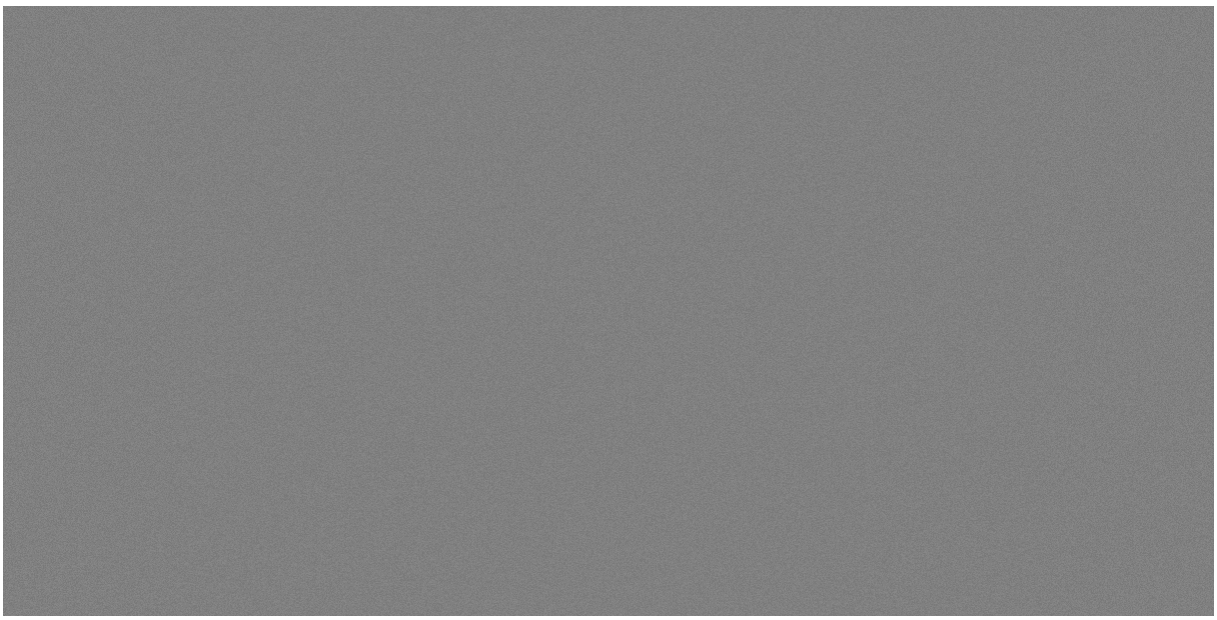


FIGURE 2.15 – Classification des logiciels d'apprentissage par rapport à la fonction pédagogique, extraite de [32] (© 2001, JSTOR). Les environnements virtuels rentrent dans les catégories des logiciels de simulation, de micromonde et de jeu éducatif.

Des Environnements Virtuels pour l'Apprentissage Humain (EVAH), ou *Virtual Environment for Training (VET)* ont été développés dans le cadre d'entraînements à la lutte contre les incendies comme SécuRéVI [105], ou pour faciliter l'apprentissage de procédures avec GVT [48].

Dans un EVAH, l'utilisateur (ou apprenant) doit suivre un scénario pédagogique de manière plus ou moins guidée, afin de construire ses connaissances et de pouvoir ensuite les restituer en environnement réel. L'avantage des EVAH est qu'ils permettent une adaptation des scénarios pédagogiques en fonction du niveau de l'apprenant et du degré de guidage [5, 60]. De plus, les procédures ou gestes appris en environnement virtuel sont utilisables en situation réelle : on parle alors d'un transfert d'apprentissage [8].

La conception d'un EVAH nécessite de déployer un modèle pédagogique [30] et/ou d'analyser l'activité des apprenants [26, 16] en plus des contraintes énoncées précédemment dans la partie 2.1.2. La Figure 2.16 décrit le processus de développement d'un EVAH, entre modélisation de l'activité, création des scénarios pédagogiques et développement de l'environnement virtuel.

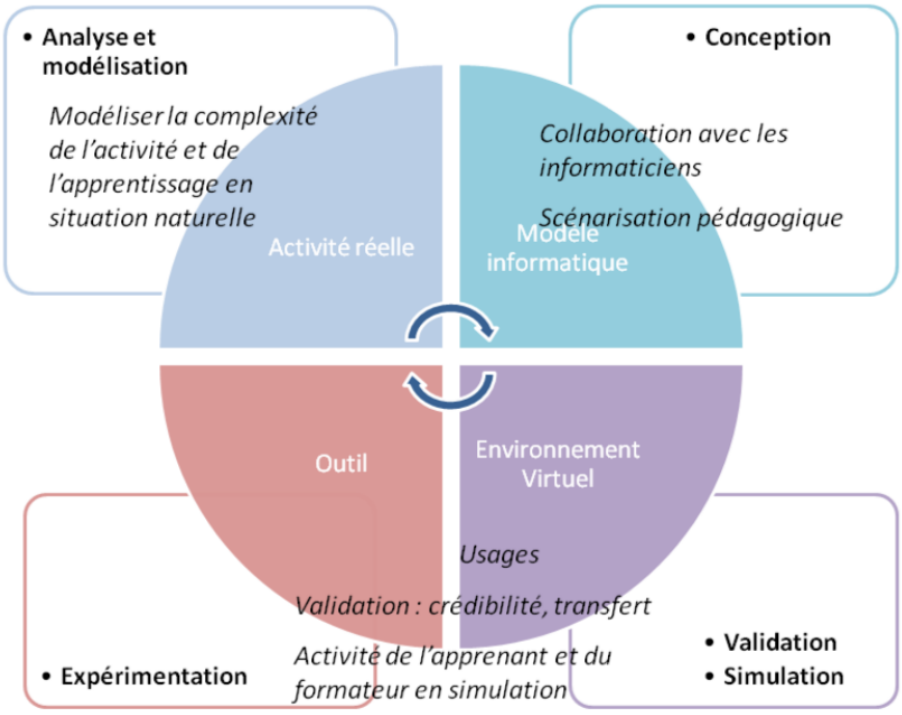


FIGURE 2.16 – Démarche de développement d'un EVAH, extraite de [16]. Une analyse de l'activité des apprenants est nécessaire afin de développer et d'implémenter un modèle informatique de cette activité dans un EVAH, qui permettra d'évaluer l'apprentissage.

Pour faciliter le développement d'EVAH, des architectures d'EV ont été proposées, comme MASCARET [13], métamodèle d'environnement virtuel pouvant intégrer des scénarios pédagogiques. Notons que les jeux sérieux (*serious games*) sont une catégorie d'EVAH dans lesquelles une composante ludique a été ajoutée afin d'améliorer l'engagement des utilisateurs [27, 57].

Les EVC sont aussi parfois utilisés afin de former plusieurs personnels en fonction de leurs rôles [21] ou de modéliser une relation d'apprentissage entre humains ou agents virtuels, qu'ils soient des agents 'tuteurs' guidant l'apprenant [63, 83] ou des apprenants simulés [47, 81] (Figure 2.17). Les EVC permettent une réduction des coûts mais aussi la mutualisation de scénarios d'apprentissages différents au sein du même environnement.

La cybersécurité étant un domaine où la formation individuelle ou collaborative de personnels à différentes tâches et situations est un enjeu majeur, l'utilisation de CVE pour l'apprentissage en cyber sécurité peut donc être envisagée, la gamification de l'environnement facilitant l'apprentissage des non experts tandis que la modélisation des activités expertes offre des scénarios pédagogiques réalistes.

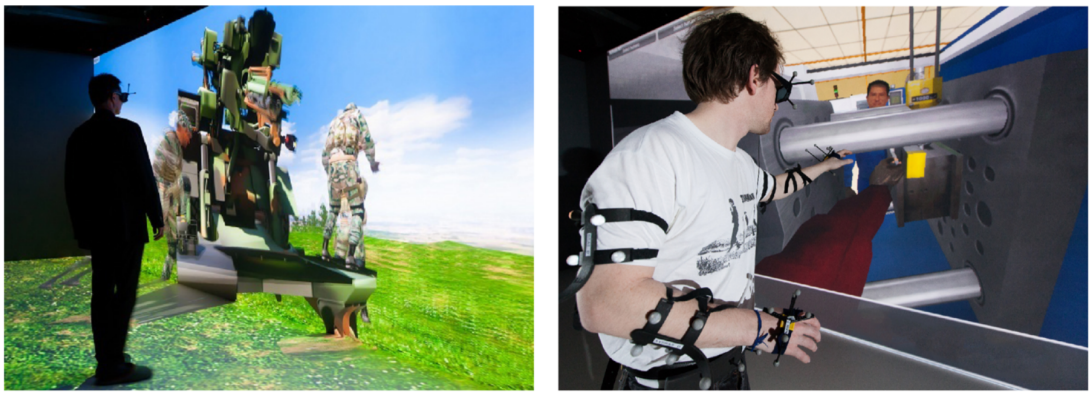


FIGURE 2.17 – Exemples d'utilisation de EVC pour l'apprentissage pour la formation militaire ou industrielle, extraits de [81]. L'apprentissage se fait en présence d'agents virtuels.

Environnements Virtuels Collaboratifs pour la cybersécurité

Malgré la mauvaise presse des visualisations de données 3D, les EV commencent à être utilisés pour analyser et visualiser des données, car ils offrent aux utilisateurs la possibilité de se mouvoir autour des représentations de données et donc de disposer d'une pluralité de points de vue. Ils sont de plus utilisés depuis des années pour la formation et l'apprentissage humain de procédures, gestes ou situations. Comme les problématiques de visualisations de données et de formation sont actuelles et importantes en cybersécurité, nous pensons que la Réalité Virtuelle est pertinente pour résoudre ces problématiques, à travers l'utilisation d'EVC pour l'analyse de données ou la formation. Ils pourraient pallier les manques des outils actuels et offrir de nouveaux outils pour l'analyse de l'état de sécurité des systèmes informatiques.

2.3 Conclusion sur l'utilisation de la Réalité virtuelle pour la visualisation de données et l'apprentissage humain

La Réalité Virtuelle (RV) connait un regain d'intérêt actuellement, grâce à l'émergence de visiocasques performants et à coûts relativement faibles. Toutefois, elle est souvent mal comprise et les capacités des Environnements Virtuels Collaboratifs (EVC), qui permettent à un ou plusieurs utilisateurs d'interagir au sein d'une simulation temps-réel afin d'accomplir des tâches prédéfinies, ne sont pas forcément bien exploitées. Le développement d'un EVC nécessite la prise en compte de contraintes techniques et ergonomiques afin de permettre aux utilisateurs d'interagir entre eux et avec l'environnement de manière naturelle.

Les EV peuvent être utilisés afin de visualiser des données complexes de manière immersive et interactive, et bien que les représentations 3D des données soient peu présentes actuellement, le domaine des *Collaborative Immersive Analytics* tend à les promouvoir ; en effet, le fait d'être immergé dans des données, de pouvoir se mouvoir autour et d'échanger avec d'autres utilisateurs peut apporter beaucoup quant à la compréhension et l'échange d'informations. Or, la visualisation et l'analyse de données sont nécessaires quant à l'acquisition d'une bonne CSA, la capacité à comprendre l'état de sécurité d'un système informatique, par les cyber analystes. Nous pensons que les EVC peuvent être utilisés dans ce cadre.

De la même manière, les Environnements Virtuels pour l'Apprentissage Humain (EVAH) sont utilisés depuis des années afin de favoriser l'apprentissage de procédures ou de gestes. Ils permettent à plusieurs utilisateurs de se former à des tâches diverses de manière efficace et nous pensons donc qu'un EVC basé sur une analyse de l'activité de personnels des SOCs pourrait être utilisé afin d'améliorer leur CSA.

La Figure 2.18 présente notre positionnement quant à l'utilisation d'EVC pour la cybersécurité : ils peuvent à la fois servir à médiatiser la collaboration, donc comme outil de CSCW, mais aussi comme support à l'analyse collaborative de données ou à la formation humaine.

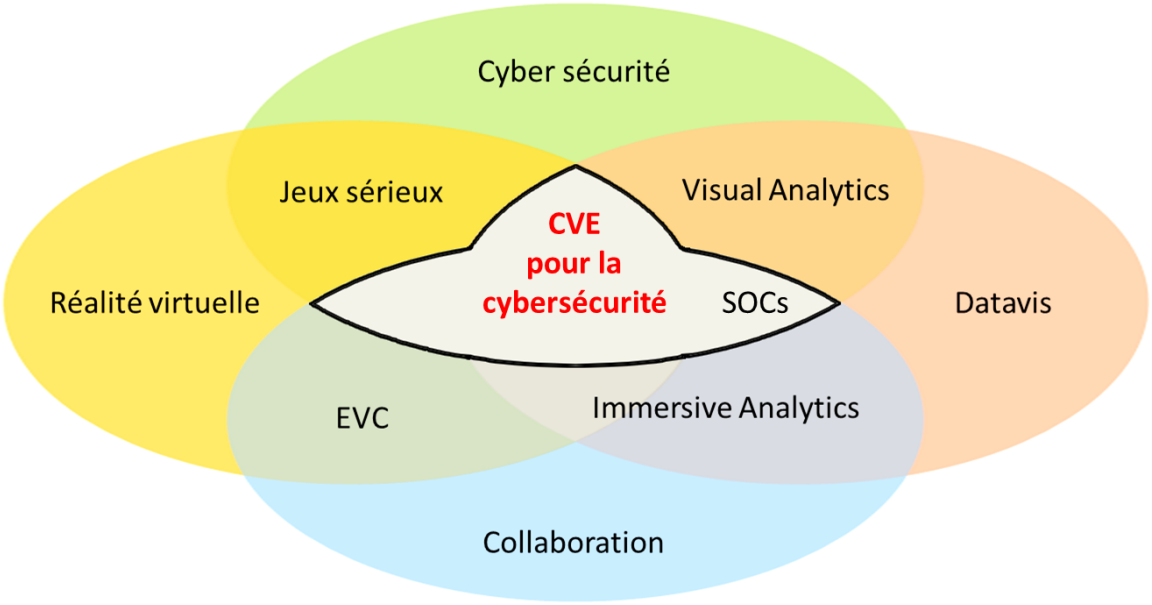


FIGURE 2.18 – Diagramme de Venn présentant l'utilisation des EVC pour la cybersécurité. Les EVC peuvent être utilisés pour répondre aux problématiques de visualisation de données et de formation humaine.

Dans le chapitre suivant, nous allons présenter l'étude que nous avons menée afin d'établir un modèle de l'activité collaborative au sein d'une structure opérationnelle de cybersécurité nous permettant de proposer un EVC adapté aux besoins des cyber analystes.

Chapitre 3

Modèle de l'activité CyberCOP 3D et scénario collaboratif d'analyse d'incidents

Pour développer un Environnement Virtuel Collaboratif (EVC) qui faciliterait l'acquisition de la CSA par des utilisateurs, nous devons comprendre les besoins et les activités de ces utilisateurs. La modélisation du périmètre de leurs actions est nécessaire afin de délimiter les objectifs de l'EVC. La cybersécurité étant un domaine vaste, il nous faut de plus définir des scénarios inspirés de cas d'utilisation réels à partir d'une étude des pratiques collaboratives des cyber analystes.

3.1 Modélisation de l'activité collaborative en cybersécurité

Pour faire face au nombre grandissant des menaces informatiques et pour améliorer la réactivité et la coordination des personnels de cybersécurité, ces derniers se regroupent au sein de structures, qui coopèrent et échangent des informations afin de faciliter la surveillance des systèmes informatiques. La Figure 3.1 représente les rôles et caractéristiques des principales structures de cybersécurité, à savoir les *Security Operations Centers* (SOCs) chargés de la surveillance (monitoring) des réseaux, les *Computer Emergency Response Team* (CERT) et les *Computer Security Incident Response Team* (CSIRT), qui ont des fonctions simulaires et sont dédiés au traitement des incidents et à la coordination entre structures (Figure 3.1).

Les SOCs sont les centres les plus étudiés et sont en constante évolution. Nous avons eu la possibilité d'étudier les SOCs de quatre de nos partenaires industriels de la chaire Cyber CNI, à savoir la Société Générale, EDF, Airbus et Orange, afin de proposer un modèle de l'activité collaborative qui soit instanciable dans un EVC et qui corresponde à leurs attentes.

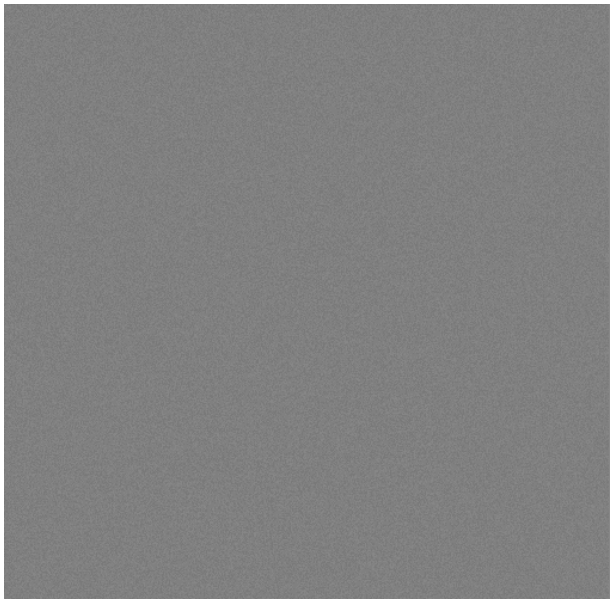


FIGURE 3.1 – Diagramme de Venn décrivant les rôles et caractéristiques des SOCs (centres d'analyse des réseaux), CERT et CSIRT (centres d'analyse d'incidents et de coordination), extrait de `https://www.exabeam.com/incident-response/csirt/`.

3.1.1 Security Operations Centers

Les SOCs (aussi parfois appelés Cyber SOC) sont des structures où des opérateurs surveillent en permanence l'état de sécurité d'un réseau informatique. Un standard des SOCs a été proposé par la MITRE [138], qui est une organisation américaine proposant des *frameworks* et outils pour l'ingénierie système, la sécurité informatique ou la sécurité civile par exemple. Ce standard décompose les rôles et actions des personnels au sein des structures, ainsi que les communications entre ces différentes structures. Un SOC est composé d'analystes de différents degrés d'expertise, d'un responsable (SOC Manager) et de spécialistes en développement informatique, en collecte d'informations ou en administration des systèmes qui travaillent dans une même salle (Figure 3.2).

Les rôles de ces différents personnels ont été présentés par Alissa Torres dans son rapport "Building a World-Class Security Operations Center : A Roadmap" [124] (Figure 3.3).

FIGURE 3.2 – Exemple de disposition des personnels au sein d'un SOC, extrait de [58]. Les analystes de niveau 1 sont proches d'un écran géant utilisé afin d'offrir une vue globale de la situation, tandis que les analystes de niveaux 2 et 3 ainsi que le SOC Manager sont en retrait.

Les analystes de niveau 1 sont les personnels qui traitent en permanence des alertes issues d'outils de monitoring et de corrélation. Lorsqu'ils sont confrontés à des cas complexes, ils 'escaladent' l'alerte et la confient à des analystes de niveau 2 ou 3. Ces derniers disposent alors de plus de temps pour analyser les alertes et fournir des rapports d'incidents. Le SOC Manager reçoit ces rapports et les transmet aux autres instances. Il coordonne les actions des différents analystes si besoin est.

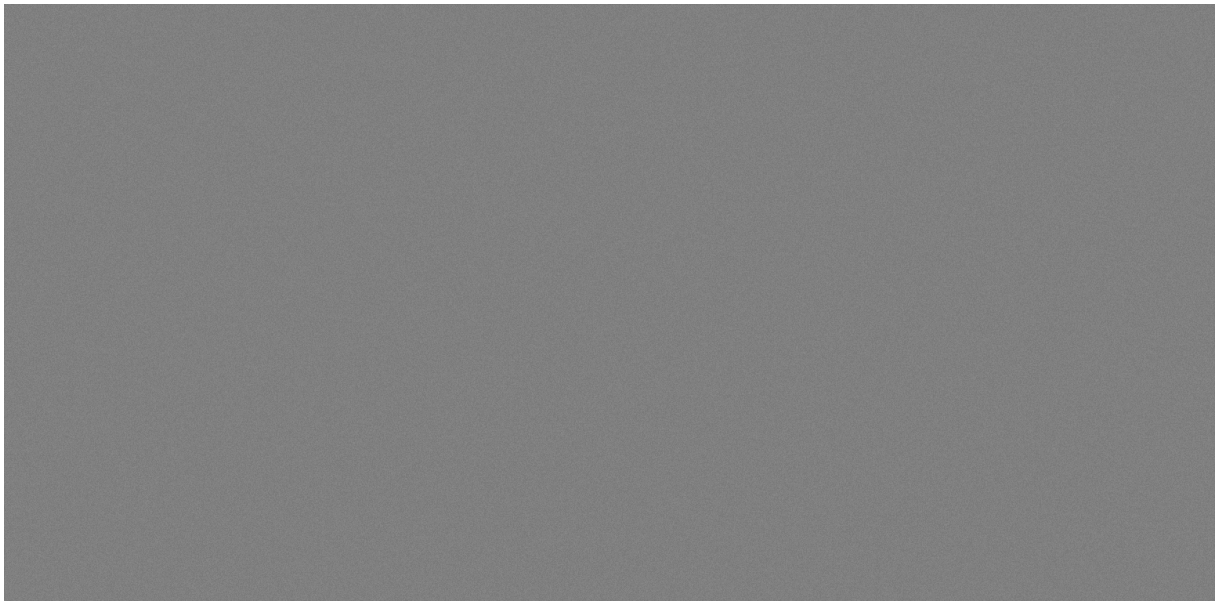


FIGURE 3.3 – Description des métiers d'un SOC, extrait de [124] (© 2015, SANS). Les analystes de niveau 1 vérifient et trient les alertes, tandis que les analystes de niveau 2 et 3 effectuent des analyses en profondeur.

La pierre angulaire des SOCs est le *Security Information Event Management tool*, ou SIEM. Il s'agit d'un outil qui agrège les données des capteurs implémentés dans le réseau informatique et qui corrèle des alertes afin de fournir une information enrichie aux analystes. Le SIEM permet de regrouper les incidents et de suivre l'activité du réseau informatique (Figure 3.4).

Les SIEMs ont de nombreuses fonctionnalités allant du monitoring temps-réel d'événements à la gestion du partage des tâches entre analystes, voire à la production de rapports destinés aux décisionnaires. Toutes ces fonctionnalités participent à l'acquisition de la CSA par les personnels utilisant le SIEM, car elles permettent d'obtenir une vue complète de l'état de sécurité du système informatique (Figure 3.5).

Les procédures d'analyse d'incidents se basent sur les alertes relevées par le SIEM. La Figure 3.6 décrit un protocole de traitement d'alertes. Les alertes sont listées et transmises aux analystes qui peuvent ensuite les traiter. Si l'alerte est considérée comme pertinente, elle est signalée, et à l'issue d'une seconde vérification un rapport est envoyé. Des outils de gestion d'historiques et d'alertes sont utilisés afin de mesurer la performance des analystes lors du traitement des tickets, et de fournir un rapport d'incident.

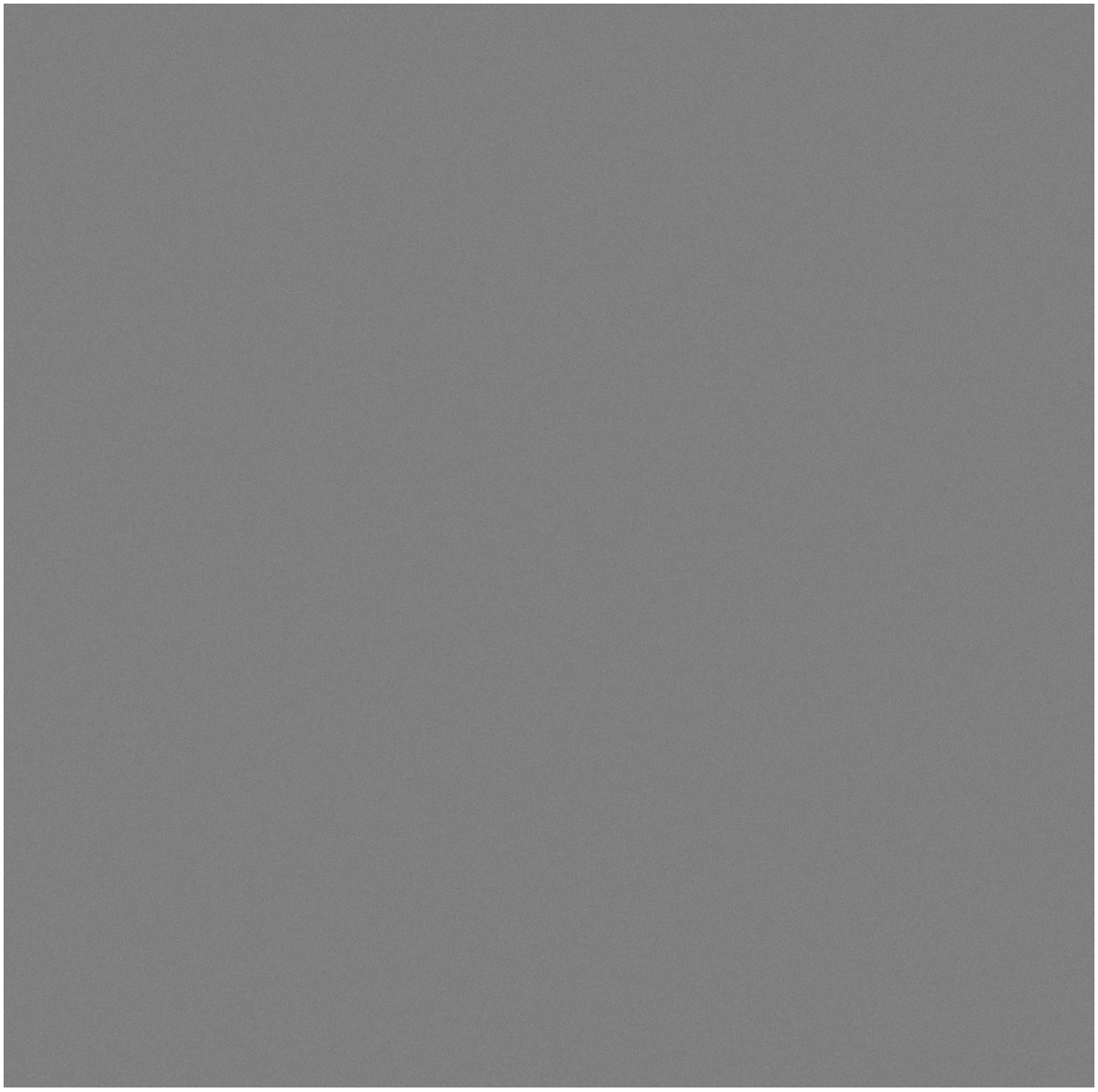


FIGURE 3.4 – Utilisation d'un SIEM au sein d'un SOC, extrait de [138] (© 2014, MITRE). Ses fonctionnalités lui permettent d'être utilisé par tous les acteurs des SOCs.

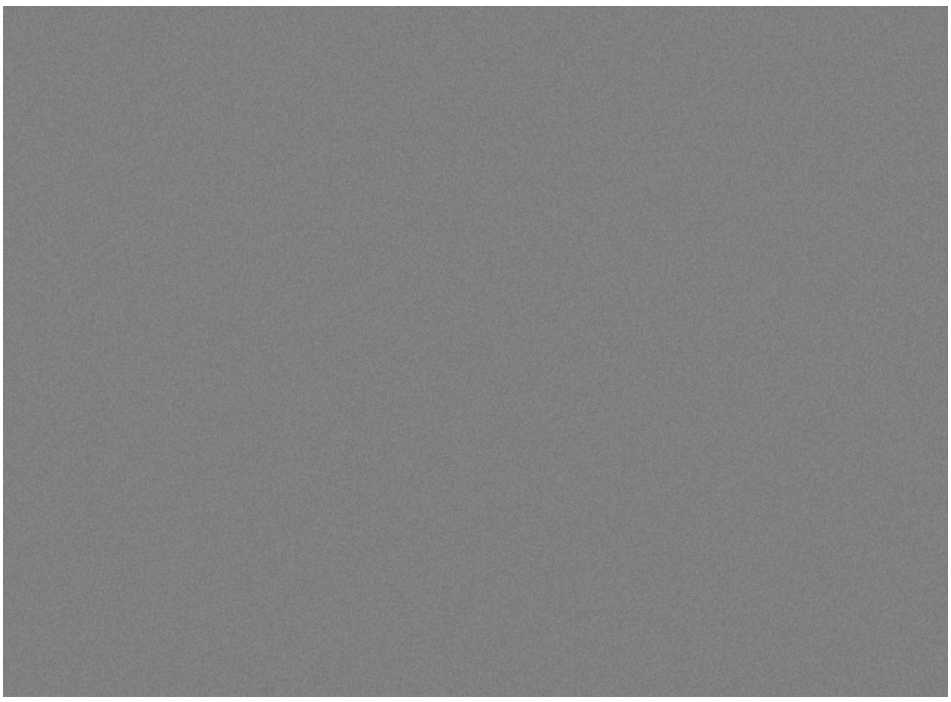


FIGURE 3.5 – Fonctionnalités offertes par un SIEM favorisant l'acquisition de la CSA par les personnels, extrait de [138].

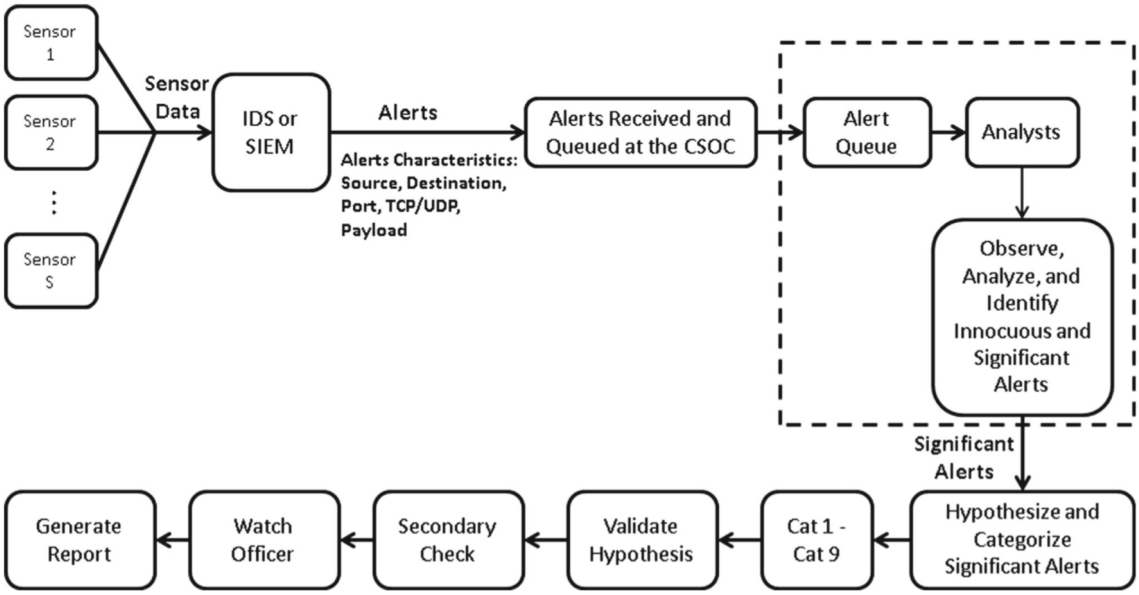


FIGURE 3.6 – Procédure d'analyse de traitement d'alertes, extrait de [110] (© 2018, Springer). Ces dernières sont centralisées par le SIEM et transmises aux analystes qui les traitent individuellement. Si une alerte est jugée pertinente, elle est alors vérifiée une seconde fois et à l'issue de la vérification un rapport est produit.

La collaboration au sein des SOCs est définie à haut niveau par des processus métiers, mais il n'existe pas de règles précises quant à l'échange d'informations entre analystes ou avec le SOC Manager. De plus, la collaboration n'est que peu médiatisée, car outre l'envoi de messages électroniques ou les systèmes de gestion d'incidents, peu d'outils permettent à plusieurs personnels de travailler ensemble. Les SIEMs par exemple ne font que coordonner les activités des personnels mais n'offrent pas d'interface collaborative permettant aux analystes d'agir à plusieurs sur une alerte.

Afin de comprendre comment les personnels travaillent dans les SOCs et acquièrent leur CSA et afin de développer un modèle de l'activité collaborative adapté à leurs besoins, nous avons défini, avec le concours de nos partenaires industriels, un protocole de visite et d'étude de leurs SOCs.

3.1.2 Protocole d'analyse de l'activité des SOCs

L'objectif de la modélisation de l'activité collaborative des SOCs est de proposer une médiatisation des interactions entre les différents acteurs au travers un Environnement Virtuel Collaboratif (EVC) (Figure 3.7). En proposant aux analystes et aux responsables des SOC des interfaces immersives adaptées aux besoins des différents personnels, et en leur fournissant un outil collaboratif d'analyse d'alertes, nous pensons pouvoir les aider à résoudre les alertes nécessitant l'action simultanée de plusieurs personnes à la fois.

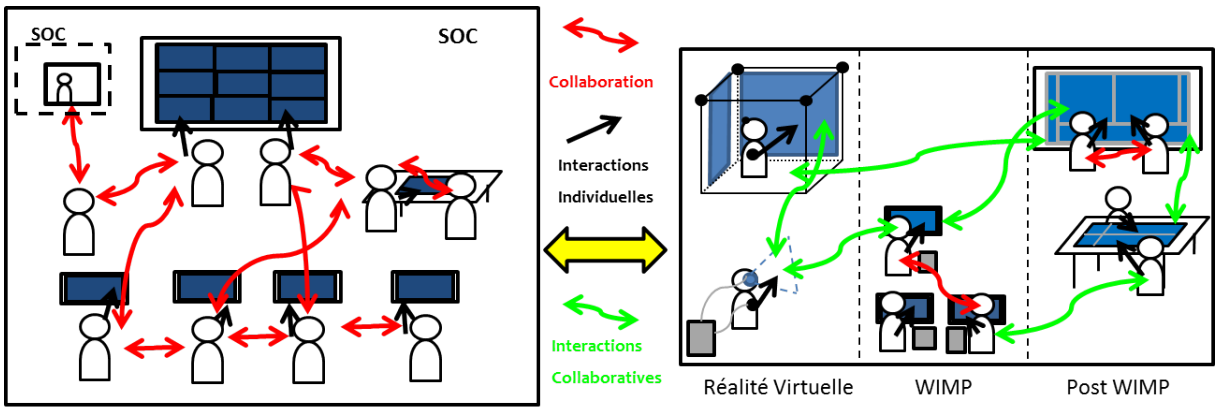


FIGURE 3.7 – Proposition de médiatisation de la collaboration au sein des SOCs via un EVC. Les échanges entre les personnels des SOCs pourra s'effectuer via un EVC et les personnels disposeront d'interfaces adaptées à leurs besoins.

Afin de développer notre modèle, que nous avons appelé le CyberCOP 3D (*Common Operational Picture*), nous avons défini un protocole de visite des SOCs de nos partenaires industriels.

Pour bâtir ce protocole, nous nous sommes inspirés d'études anthropologiques des SOCs comme celles de Sundaramurthy *et al.* [117, 118] qui décrivent les activités quotidiennes des usagers d'un SOC. Nous nous sommes aussi inspirés de l'étude d'Hamornik et Krasznay [58], qui ont interviewé des experts des SOCs afin de caractériser leurs compétences, leurs connaissances ainsi que les tâches qu'ils doivent effectuer.

Nous nous sommes aussi penchés sur les méthodes d'analyse de l'activité collaborative adaptées au développement de CVE comme celle proposée par Yohann Cardin [16], que nous avons présentée dans le chapitre précédent (Figure 2.16).

Afin de développer des interfaces adaptées aux rôles des personnels des SOCs, nous avons étudié les méthodes de design centré utilisateur proposées par McKenna *et al.* [91] qui décrivent le développement de solutions en fonction des rôles des utilisateurs ainsi que des relations entre ces rôles. Nous avons aussi étudié le framework EEVi proposé par Sethi *et al.* [109] que nous avons présenté également dans la section 1.2.1 (Figure 1.14). Notre protocole d'analyse de l'activité collaborative se décompose en trois étapes et a été validé par l'ensemble de nos partenaires industriels impliqués dans l'étude des SOCs (Figure 3.8). Nous allons maintenant décrire les différentes étapes de ce protocole.

Visites préliminaires

Afin de mieux cerner le périmètre d'analyse et de prendre contact avec les différents acteurs et responsables des SOCs, des visites préliminaires de 'découverte de terrain' ont été proposées comme premières étapes. Ces visites avaient aussi pour but d'établir un planning de visites ultérieures, de demander les autorisations nécessaires quant à la capture audio ou vidéo d'interviews de personnels, et de présenter aux analystes intéressés l'objectif de l'étude et de nos travaux de thèse.

Ces visites ne devaient durer qu'une demi-journée et devaient aboutir à des autorisations de capture d'informations et à un planning de visites.

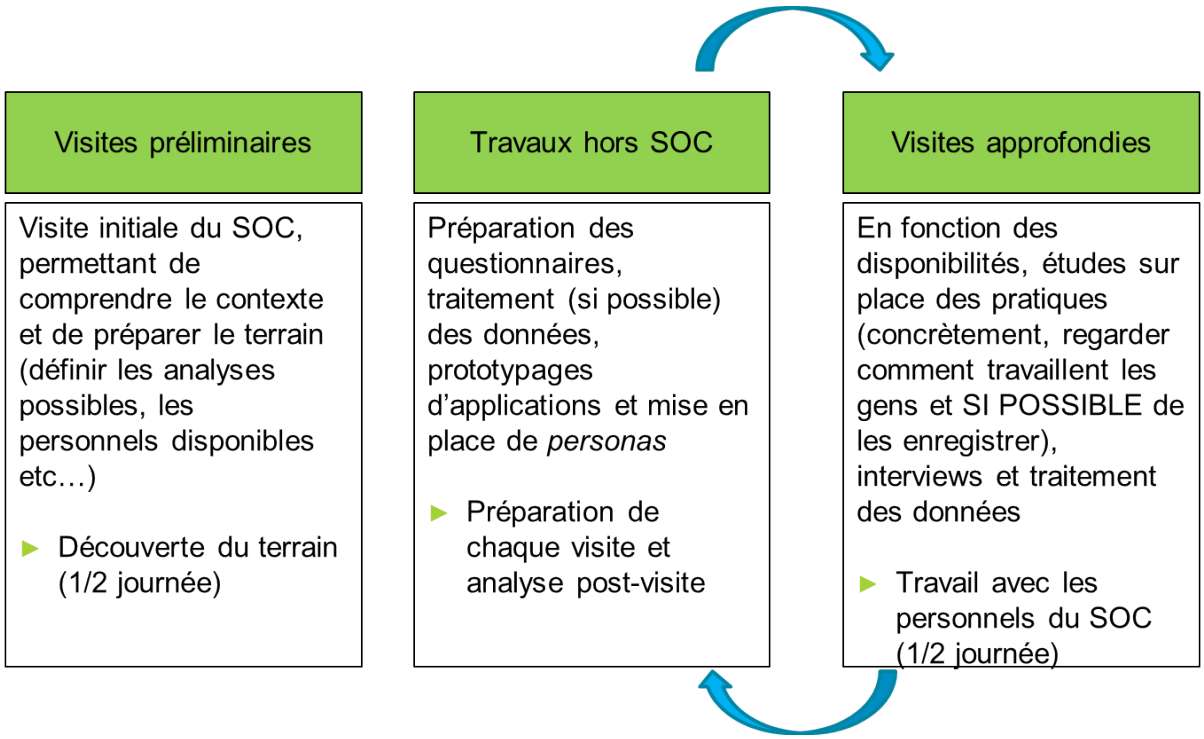


FIGURE 3.8 – Protocole d'analyse de l'activité au sein des SOCs en trois phases, une phase de visites préliminaires, une phase de visites approfondies et une phase entre les deux de travaux hors du SOC.

Travaux hors SOCs

Durant la période hors visites des SOCs, le temps devait être consacré à l'élaboration de prototypes d'interfaces, au traitement des données recueillies auprès des personnels et aux tests d'applications collaboratives immersives. Les prototypes d'interfaces devaient s'appuyer sur les informations récoltées durant les visites, via les interviews ou les retours d'expériences sur l'utilisation de ces prototypes (procédure en cycle court issue du design centré utilisateur).

Le planning des visites des SOC a été établi durant ces périodes.

Visites approfondies

Les visites des SOCS devaient permettre de recueillir des données via des interviews de personnels, des questionnaires relatifs à l'utilisation d'outils pour la CSA et des prises de notes manuscrites.

Nous avions préparé et soumis aux responsables des SOCs un questionnaire sur la visualisation de données pour la cybersécurité adapté de celui de D'Amico *et al.* [31], permettant d'obtenir des informations sur l'utilisation d'outils d'analyse visuelle de données au sein des SOCs.

Les visites permettaient aussi de valider certains prototypes ou design d'interfaces, en recueillant les propositions des personnels et en leur faisant tester des prototypes d'applications immersives. Les visites ne devaient pas être trop intrusives, et le recueil des données devait s'effectuer en accord avec la politique de sécurisation des données de nos partenaires industriels.

En parallèle de cette étude, nous avons défini un cas d'utilisation collaboratif permettant de proposer un scénario basé sur notre modèle de l'activité.

Modèle de l'activité collaborative en cybersécurité

Les cyber analystes travaillent de plus en plus au sein de structures standardisées, afin d'améliorer le traitement d'incidents et le partage d'informations stratégiques. Les *Security Operations Centers* ou SOCs sont les centres de d'analyse de l'état de sécurité des systèmes d'information. Nous avons proposé et fait valider par nos partenaires industriels de la chaire Cyber CNI un protocole de l'analyse de l'activité collaborative au sein de leurs SOCs respectifs, afin de mieux cerner leurs besoins. Cette analyse avait comme objectif la création d'un modèle, le CyberCOP 3D, qui vise à améliorer la médiatisation de la collaboration entre personnels des SOCs via l'utilisation d'un EVC.

3.2 Cas d'utilisation pour l'implémentation du CyberCOP 3D

Afin de proposer un cas d'utilisation qui puisse être implémenté dans un EVC basé sur notre modèle CyberCOP 3D, nous nous sommes penchés sur la modélisation d'attaques informatiques et sur les actions à effectuer pour y remédier.

Les attaques complexes de type Advanced Persistent Threat (APT) représentent un cas d'étude pertinent, de par leur importance stratégique et la complexité de leur mode opératoire. Ce type d'attaques vise à voler des données à une entreprise en infectant un réseau de la manière la plus furtive possible [3, 84]. Une attaque APT met généralement plusieurs mois à être détectée, souvent au moment de la fuite des données. Ces attaques posent actuellement un problème de détection plus que d'analyse [85, 113], et la prévention contre ces attaques nécessite des moyens qui sont hors du périmètre de la thèse (corrélation de données provenant de différentes sources sur plusieurs mois, accès à des services internes et à des outils dédiés).

Notre étude des SOCs ayant eu lieu durant l'apparition du rançongiciel Wannacry, nous nous sommes finalement penchés sur sa modélisation et avons basé notre cas d'utilisation sur sa détection.

3.2.1 Attaque WannaCry

WannaCry est un rançongiciel, un type de *malware* chiffrant les données d'un utilisateur puis demandant une rançon afin de lui rendre l'accès à ses données. Il a pour particularité de se propager à la manière d'un ver informatique, contrairement aux précédents rançongiciels [1]. WannaCry a eu un impact gigantesque à la fois sur l'esprit des personnes et sur les systèmes informatiques [2] car il a mis en évidence les failles de sécurité de bon nombre d'entreprises et de services [94].

Lorsque WannaCry s'exécute sur un ordinateur sous Windows 7 (par l'action d'un utilisateur ou d'un script), il commence par chiffrer les données du poste de travail et à scanner les ports utilisés par le protocole de service *Server Message Block (SMB)* de Microsoft. Ce dernier permet au rançongiciel de se propager via les failles de sécurité *EternalBlue* et *DoublePulsar*, révélées par le groupe d'hacktivistes *The Shadow Brokers* quelques mois auparavant. Le chiffrement des fichiers est irréversible et une connexion à un serveur distant via TOR, un réseau informatique permettant des connexions anonymes, est nécessaire pour envoyer la rançon si nécessaire.

Bien qu'il fut considéré comme l'attaque informatique la plus virulente de ces dernières années, des solutions ont été trouvées rapidement, notamment un *killswitch* permettant

1. `https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf`
2. `https://www.sciencedirect.com/science/article/pii/S1361372318301027`

d'annuler les effets de WannaCry si l'ordinateur infecté pouvait se connecter à un site internet spécifique. De nombreux travaux concernant la protection au chiffrement des rançongiciels ont été relancés suite à cette attaque.

L'exécution de WannaCry est détaillée dans la Figure 3.9.

WannaCry a ouvert la voie à d'autres *malwares* comme *NotPetya*, qui ont profité de l'inertie des corrections à apporter et de la fragilité de la sécurité des entreprises pour faire des dégâts. L'analyse de ces malwares permet de décrire leurs comportements à différentes échelles et de trouver des moyens de s'en prémunir, ou alors de développer des solutions pour les analyser.

3.2.2 Modélisation comportementale de WannaCry

Les différentes actions de WannaCry sur un système peuvent être modélisées par des fonctions de haut niveau comme le chiffrement ou la propagation. Ces fonctions permettent alors de définir des métriques et événements qui décrivent le déroulement de l'infection virale.

Métriques de détection de l'activité de WannaCry

Dans le cadre de cette thèse, nous avons choisi de modéliser l'activité de WannaCry par l'utilisation de deux métriques, l'entropie des systèmes de fichiers et le débit réseau qui concernent respectivement le chiffrement et la propagation du rançongiciel. Ces métriques permettent de caractériser l'activité de WannaCry mais sont aussi sujettes aux faux positifs, ce qui nous permet de modéliser ces deux cas de figures.

La métrique d'entropie des systèmes de fichiers mesure l'activité de ces derniers. Elle augmente lors de certaines activités licites ou illicites, comme une sauvegarde automatique ou un chiffrement malveillant.

De la même manière, la métrique de débit réseau mesure le transfert de données et peut augmenter lors d'un téléchargement de fichier, d'une connexion à un serveur de sauvegarde ou d'une attaque et d'une propagation virale. Nous pouvons dans le cadre de nos travaux nous contenter d'une analyse du débit réseau concernant les connexions utilisant les failles *EternalBlue* et *DoublePulsar*, afin de simuler leur utilisation.

Préconditions aux événements d'infection ou de propagation

Des préconditions sont nécessaires à l'exécution des événements du rançongiciel. Par exemple, pour s'exécuter, WannaCry nécessitait d'être sur un poste sous Windows 7 non patché contre les failles *EternalBlue* et *DoublePulsar*. Si le poste disposait d'un accès direct à internet, le chiffrement ne s'exécutait pas, car WannaCry pouvait se connecter au site de *killSwitch*, ce qui le désactivait.

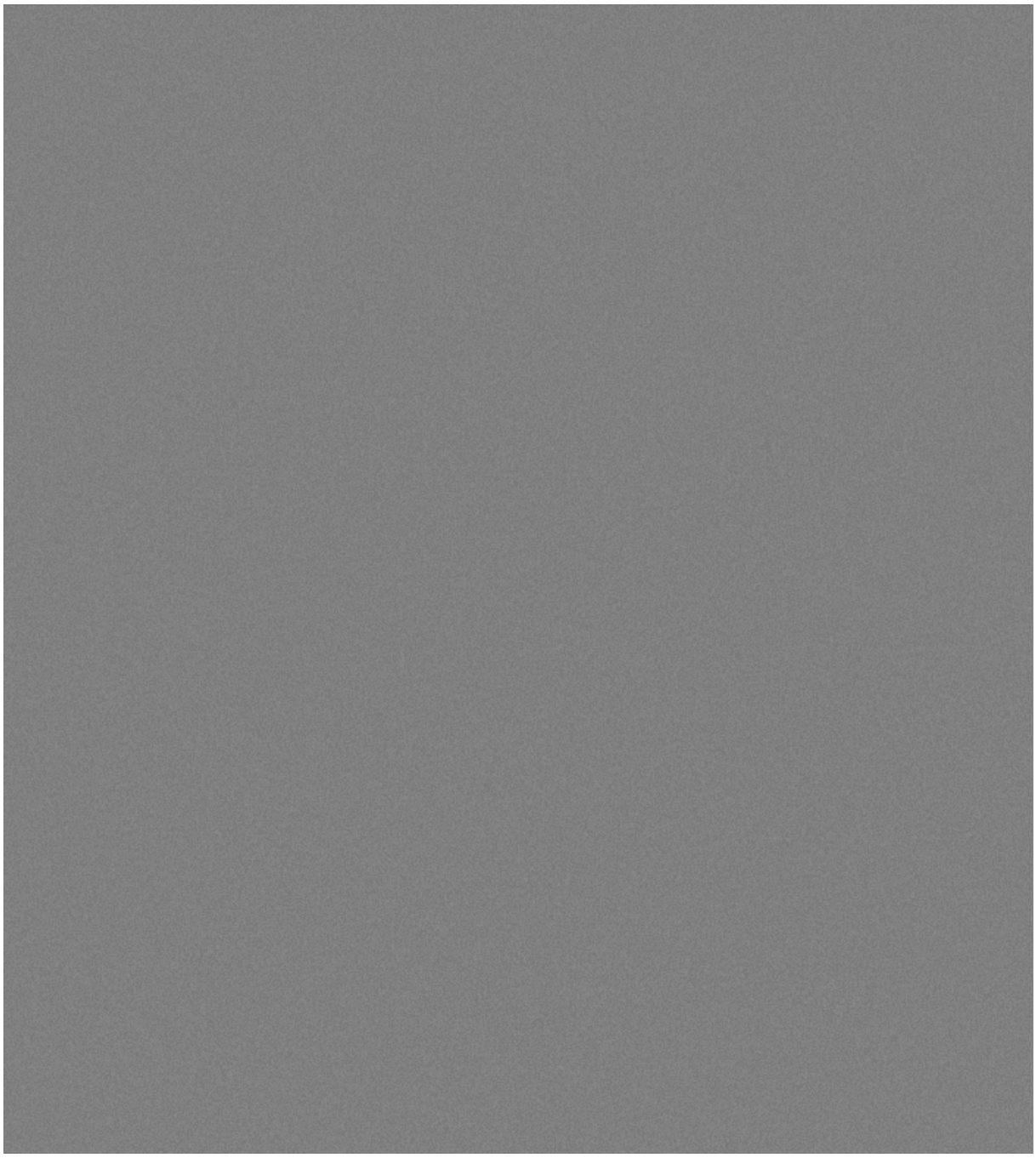


FIGURE 3.9 – Exécution du rançongiciel WannaCry. Après un test de connexion au site de killswitch (annulant l'action de chiffrement si la connexion était réalisée), WannaCry exécute différentes tâches dont le chiffrement des fichiers du poste infecté et sa propagation sur les ordinateurs du réseau. Image extraite du site `https://www.antiy.net/p/in-depth-analysis-report-on-wannacry-ransomware/`.

La modélisation des préconditions permet de modifier le comportement dynamique du rançongiciel. Par exemple, un poste **patché** sous **Windows 7** ne peut pas être infecté. Des préconditions pour des événements licites peuvent aussi être modélisées (par exemple une sauvegarde automatique des fichiers ou un téléchargement de mises à jour) afin de lever des alertes sur les métriques d'entropie et de débit réseau.

Actions utilisateurs et système

Les actions des analystes investiguant sur WannaCry dépendent de leurs rôles et pratiques au sein des SOCs. Pour simplifier les interactions, les utilisateurs pourront analyser de la même manière les postes infectés et non infectés, ce qui normalement est impossible (car WannaCry bloquait l'accès aux ordinateurs infectés).

Un chiffrement sur un poste par WannaCry se traduira aussi par l'apparition dans la liste des processus de l'ordinateur d'un exécutable **"WannaCrypt0r.exe"**, très clairement identifiable. De la même manière, la propagation aura comme autre effet l'ajout d'un thread particulier à la liste des connexions du poste. Ces données seront disponibles pour que les utilisateurs puissent caractériser l'action du rançongiciel.

Nous allons proposer des actions d'analyse collaborative comme par exemple un partage des tâches d'investigations entre utilisateurs ayant le même rôle ou une validation collective des tickets d'incidents relatifs à l'action de WannaCry.

Modèle de WannaCry proposé

La Figure 3.10 décrit la modélisation comportementale que nous avons proposée. Lorsque WannaCry infecte un poste, si ce dernier n'est pas sur Windows 7, s'il est patché ou s'il a accès à internet, rien ne se passe. Sinon, les données du poste sont chiffrées et WannaCry se propage.

Ces deux actions ont pour conséquence de lever des alertes relatives aux métriques d'entropie du système de fichiers et du débit réseau. Ces alertes sont alors transmises aux analystes qui devront les traiter. La sauvegarde des données du poste ainsi que des téléchargements ou mises à jour lèveront aussi des alertes d'entropie et de débit réseau. Ces alertes devront être caractérisées comme des faux positifs par les analystes.

L'implémentation de ce modèle dépendra des tâches, rôles et actions définis par notre étude de l'activité collaborative des SOCs.

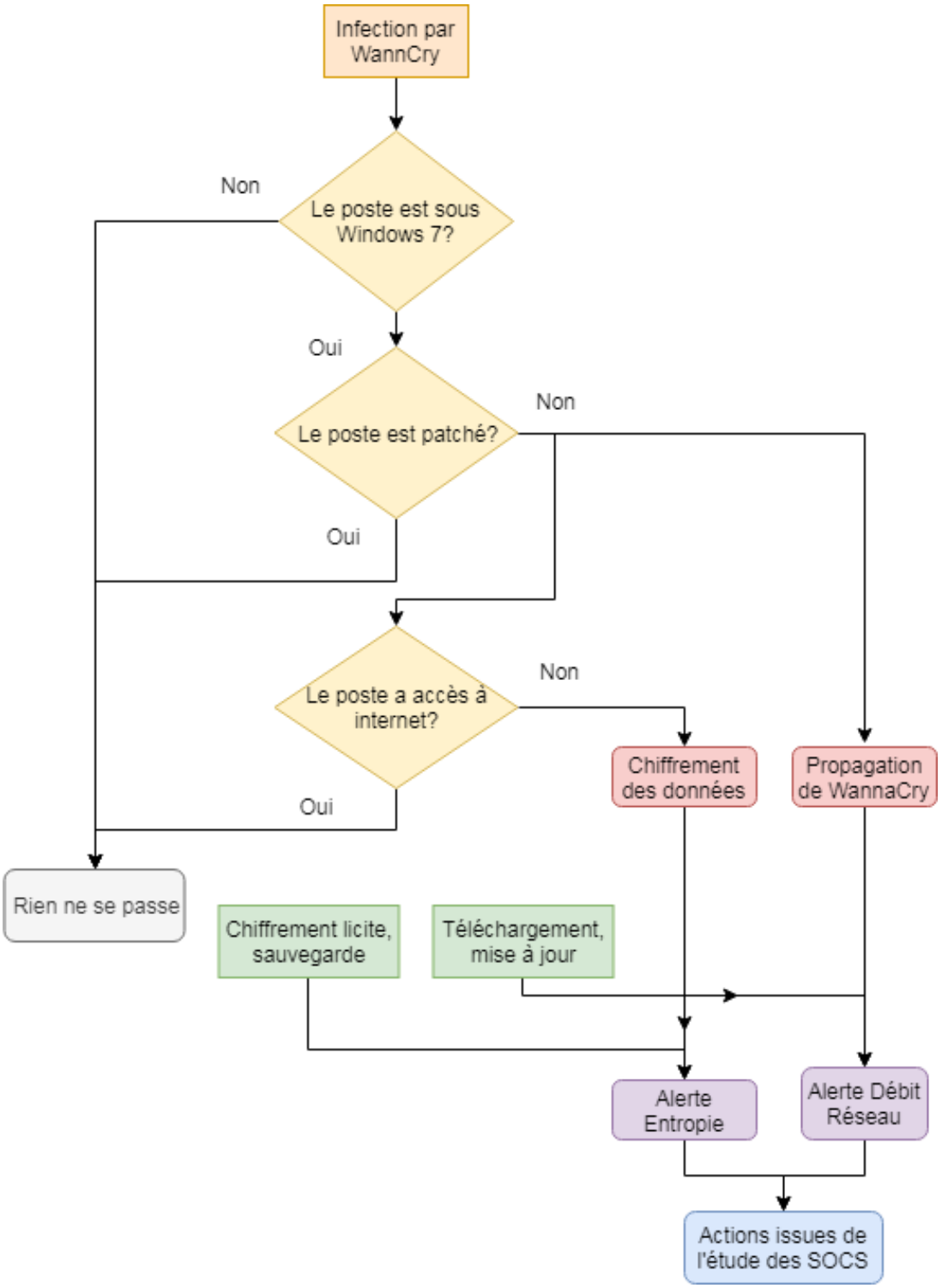


FIGURE 3.10 – Proposition de modélisation du rançongiciel WannaCry. L'infection d'un poste lève des alertes relatives à l'entropie ou au débit réseau. Ces alertes devront être traitées par les analystes, qui auront aussi affaire à des alertes déclenchées par des actions licites (faux positifs).

Cas d'utilisation d'analyse du rançongiciel WannaCry

Nous avons modélisé les actions du rançongiciel WannaCry en nous basant sur son comportement, afin de proposer un cas d'utilisation pouvant être implémenté dans un EVC pour la cybersécurité. Les actions de chiffrement et de propagation de WannaCry sont représentées par une hausse de deux métriques, l'entropie des systèmes de fichiers et le débit réseau. Ces métriques peuvent caractériser aussi l'activité licite sur le poste de travail, comme une sauvegarde ou un téléchargement. La hausse de ces métriques déclenche des alertes qui devront alors être analysées par les utilisateurs de l'EVC.

3.3 Résultats de l'étude et modèle CyberCOP 3D

Dans cette partie nous allons présenter les résultats de notre étude des SOCs qui nous ont permis d'élaborer le modèle CyberCOP 3D, modèle permettant l'adaptation dans un EVC des pratiques collaboratives des SOCs. Nous allons aussi détailler le scénario collaboratif d'analyse développé à partir du cas d'utilisation de l'analyse de WannaCry.

3.3.1 Résultat de l'analyse de l'activité

Nos visites des SOCs de nos partenaires industriels ont eu lieu entre mars et juillet 2017. Cette période a coïncidé avec l'infection du rançongiciel WannaCry, ce qui a limité nos interactions avec les SOCs. Malgré les autorisations et validations, aucune visite n'a été effectuée comme nous le souhaitions, du fait de la surcharge d'activité qu'a générée le rançongiciel. Néanmoins, nous avons quand même pu caractériser l'activité au sein des SOCs selon certaines capacités ou critères, en nous basant sur les travaux de Sundaramurthy *et al.* [118] d'analyse anthropologique des SOCs, et sur la taxonomie de la CSA d'Evesti *et al.* [43] qui décrit les liens entre données, tâches, outils et représentations visuelles utilisées dans les SOCs.

Visites préliminaires

Les visites 'découverte de terrain' des SOCs se sont déroulées de manière optimale. Nous avons pu présenter nos travaux, demander des autorisations de récupération de données et prévoir les visites ultérieures. Durant ces visites préalables, nous avons pu constater que tous les SOCs avaient des fonctionnements différents, bien que les standards présentés dans la section précédente étaient respectés (trois niveaux d'analystes, grand écran affichant les données du SIEM, échanges d'informations, etc...).

Nous avons pu observer certaines procédures de gestion d'alertes par des analystes. Ces derniers utilisent un système de *ticketing*, qui leur permet de traiter une alerte après l'autre. Ce système est à la base de la coordination et la communication entre les personnels du SOC. Nous n'avions pas reçu l'autorisation de filmer ou d'enregistrer les personnels en situation, nous avons donc dû nous contenter de poser des questions et de prendre des notes manuscrites.

Les analystes de niveau 1 n'avaient que peu de temps pour résoudre les tickets et utilisaient les nombreux outils à leur disposition. Ils ne semblaient pas vraiment intéressés par un outil immersif, car ils ne souhaitaient pas qu'on leur rajoute une charge supplémentaire. Pour certains cas cependant, comme celui de l'affichage croisé de données normalement disponibles dans des bases de données séparées (le croisement entre position d'une adresse IP dans la topologie du réseau, géolocalisation de cette adresse IP et informations concernant l'utilisateur lié à cette adresse par exemple), les CVE leur semblaient être adéquats.

L'utilisation de la Réalité Virtuelle pour le rejeu de situation a aussi été évoquée et a éveillé l'intérêt de plusieurs analystes.

Les rôles décrits dans la littérature, à savoir les **analystes** et le SOC Manager (ou **coordinateur**) étaient représentés dans les SOCs. Nous avons donc pu constater qu'il existait une hiérarchisation de la collaboration et des interactions entre ces rôles ; les analystes pouvaient s'échanger des informations et rendaient compte au coordinateur tandis que ce dernier pouvait distribuer des tickets et valider les rapports d'incidents. Analystes et coordinateur utilisaient des outils différents afin d'effectuer leurs tâches.

La collaboration entre personnels n'était pas vraiment médiatisée. Les analystes discutaient directement entre eux ou échangeaient par téléphone, et les seuls outils collaboratifs que nous avons remarqués sont l'outil de *ticketing* et les messages électroniques. Notre proposition de mettre en place un système permettant à plusieurs personnes d'interagir ensemble sur certains cas a intéressé les personnels.

Ces premières visites nous ont permis de cadrer nos travaux et de cibler le développement de nos prototypes. De plus, à la suite de ces visites, nous avons transmis des questionnaires sur la visualisation pour la cybersécurité aux responsables des SOCs, afin de récupérer des avis de différentes catégories de personnels sur cet aspect.

Travaux hors SOCs

À l'issue des visites préliminaires, nous avons pu commencer le développement d'un EVC pour la cybersécurité. En nous basant sur une première définition des rôles et tâches des personnels des SOCs et en nous inspirant de travaux du domaine du *Computer Supported Cooperative Work* (CSCW) comme ceux de Casarin [17] présentés dans le chapitre précédent, nous avons élaboré un modèle de l'activité collaborative en cybersécurité pouvant être transposé dans un EVC.

Toutefois, nous n'avons pas reçu beaucoup de réponses aux questionnaires sur la visualisation pour la cybersécurité. Ce manque de réponses (seulement 8 réponses individuelles pour 5 SOCs contactés alors que nous en attendions environ 40) nous a pénalisés quant à une comparaison des besoins des personnels par rapport aux recherches académiques dans le domaine, et ne nous a pas facilité la tâche quant à la spécification des interfaces utilisateurs. Nous nous sommes néanmoins tournés vers deux types d'interfaces, une **interface 2D** permettant à un utilisateur d'avoir une vue globale de la situation, et une **interface 3D immersive** permettant d'analyser des données de manière plus détaillée. Ces interfaces étaient faites pour être utilisables par deux types de rôles : les **Analystes**, qui devaient résoudre des tickets et transmettre des comptes-rendus, et les **Coordinateurs** qui devaient distribuer les tickets d'alertes et valider les comptes-rendus.

En nous basant sur notre cas d'utilisation d'analyse d'alertes liées à l'infection du rançongiciel WannaCry, nous avons proposé un environnement virtuel représentant une salle contenant 13 postes de travail qui peuvent potentiellement être la cible de WannaCry.

Des données descriptives (type de système d'exploitation, nom de l'utilisateur, liste des processus...) ont été implémentées afin de permettre une investigation des postes de travail via plusieurs actions d'analyse.

Visites approfondies

Lors des visites approfondies des SOCs faisant suite à la visite préliminaire, nous aurions dû corriger nos prototypes, faire valider ou non les différents aspects de notre modèle, et proposer aux personnels des SOCs de tester les différents types d'interfaces, afin d'avoir des retours utilisateurs.

Malheureusement, l'attaque WannaCry a totalement perturbé notre planning, et nous n'avons pu effectuer aucune visite de SOCs. Néanmoins, nous avons pu présenter nos travaux durant des événements organisés par nos partenaires industriels (et donc à un public plus large que celui des SOCs), et durant des forums professionnels (par exemple au Forum International de la Cybersécurité à Lille, en Janvier 2018). Ces présentations nous ont permis d'avoir des retours d'experts en cybersécurité de différents milieux, et nos travaux ont été très bien accueillis par ces experts et par nos partenaires. Nous avons pu justifier notre positionnement, notre choix d'utiliser la Réalité Virtuelle pour la cybersécurité, et nous avons pu affiner notre cas d'utilisation et nos modèles.

De plus, nous avions des réunion bi-mensuelles d'avancement de thèse. Ces réunions nous ont permis d'avoir des réponses à des questions concernant les SOCs et de faire valider notre approche durant différentes étapes de développement. Nous avons pu faire tester notre prototype d'EVC, pas suffisamment certes pour effectuer des évaluations, mais assez pour avoir des retours utilisateurs quant à l'acceptabilité de telles solutions.

Même si l'étude de l'activité ne s'est pas déroulée comme prévu, du fait de l'attaque WannaCry, du non retour des questionnaires, ou de la difficulté à récupérer des données issues d'une structure de cybersécurité, nous avons pu développer notre modèle de l'activité collaborative, le CyberCOP 3D.

3.3.2 Modèle CyberCOP 3D

Le modèle CyberCOP 3D a pour objectif de caractériser les pratiques collaboratives étudiées au sein des SOCs et de les transposer dans un EVC. L'objectif est de proposer une collaboration médiatisée à des personnels de la cybersécurité, afin d'évaluer si cette collaboration facilite le traitement de cas d'utilisations spécifiques.

Il se décompose en capacités qui nous ont permis de classifier l'activité au sein des SOCs. Ces capacités peuvent être définies pour les EVC de manière générale, et nous présentons ici nos choix quant à l'instanciation du modèle et l'implémentation du cas d'utilisation d'analyse d'alertes (Figure 3.11).

	SOC	**CyberCOP 3D**	**Scénario d'utilisation**
Rôles	Compromis entre prise de décision et analyses de données. Interactions hiérarchiques.	Utilisateurs avec des interfaces et des actions spécifiques. Interactions hiérarchisées.	Analyste immergé en EV. Coordinateur disposant d'un dashboard 2D
Tâches	Système de ticketing. Tâches spécifiques	Système de ticketing. Simulation des interactions. Scénarios experts.	Simulation d'un système d'analyse collaborative d'incidents liés à WannaCry.
Visualisations	Outils de monitoring, d'analyse et de comptes-rendus.	Vues 2D, 3D ou immersives. Filtres sémantiques sur les vues. Intégration d'outils existants.	Vues 2D et immersives. Fltres de données physiques (IT) et réseau (Cyber).
Données	Agrégées par les SIEMS et autres outils. Provenant de diverses sondes et capteurs.	Données simulées. Métriques simplifiées Intégration avec un outil de type Cyber Range.	Simulation de deux métriques, l'entropie des systèmes de fichiers et le débit réseau. Données statiques des postes de travail (assets).
Collaboration Explicite	**Système de ticketing. gestion des processus. Courriers électroniques. Comptes-rendus**	**Système de ticketing. Utilisation d'avatars. Mutual awareness et partage d'informations**	**Listes des alertes. Feedbacks et feedforwards. Coprésence. Scénario déterministe.**
Collaboration Tacite	**Communication verbale directe. Collaboration non médiatisée.**	**Outils de communication. Historique des actions. Partage d'informations**	**Co-localisation. Historique d'évènements. Partage d'informations contextuelles**
	Modèle de l'activité	**Implémentation EVC**	**Instance du modèle**

FIGURE 3.11 – Modèle CyberCOP 3D de l'activité collaborative en cybersécurité. La colonne de gauche décrit les compétences (ou capacités) que nous avons observées dans les SOCs. La colonne du milieu décrit les implémentations possibles dans un EVC et la colonne de droite présente l'instanciation que nous avons effectuée en nous basant sur un scénario d'analyse d'alertes.

Rôles

Nous avons pu constater que les rôles des personnels au sein des SOCs pouvaient se définir comme un compromis entre la prise de décision et l'analyse de données, comme présenté par McKenna *et al.* [91] (Figure 3.12). L'analyste doit rendre compte de ses investigations, et le SOC Manager (ou coordinateur) doit prendre une décision en fonction des rapports d'investigation. Les interactions entre rôles sont hiérarchisées : le coordinateur envoie des ordres aux analystes qui lui remontent des rapports. Les interactions sont donc horizontales entre personnels ayant des rôles similaires et verticales entre différents rôles.

Ces rôles peuvent s'implémenter dans un EVC en proposant des interactions et des interfaces spécifiques aux utilisateurs. La hiérarchisation de l'interaction peut s'intégrer dans un système de gestion des actions, avec des actions d'ordres et des actions de comptes-rendus par exemple. Une séparation des *feedbacks* entre interactions horizontales et verticales peut aussi être proposée.

Pour l'instanciation du CyberCOP 3D, nous avons proposé une vue immersive au rôle d'analyste, qui doit investiguer dans un environnement virtuel, et une vue 2D de type tableau de bord au rôle de coordinateur, qui doit suivre les actions des analystes. Ces interfaces seront présentées en détail dans la section 4.2.

Tâches

La tâche principale des analystes des SOCs est de traiter les tickets d'incidents fournis par le SIEM. Il s'agit d'une tâche fastidieuse mais qui permet de trier les alertes en fonction de leur complexité. Si une alerte est jugée comme sérieuse par un analyste de niveau 1, il l'escalade, à savoir il la transmet à un analyste plus expert (de niveau 2 ou 3). Au-delà de la gestion des tickets, les analystes doivent utiliser de nombreux outils permettant d'investiguer sur les alertes, que ce soient des bases de données de *logs* ou de trames réseau, des désassembleurs de fichiers executables ou autres outils. Les tâches les plus simples des analystes sont décrites par des procédures. L'objectif est alors d'effectuer la procédure le plus rapidement possible, et de fournir un rapport détaillé.

Le système de *ticketing* peut s'implémenter dans un EVC, ou du moins se simuler relativement facilement. Les actions utilisateurs peuvent être simulées et modélisées en s'appuyant sur des taxonomies existantes ou sur des procédures standardisées, comme celle proposée par Hamornik et Krasznay [58] (Figure 3.13).

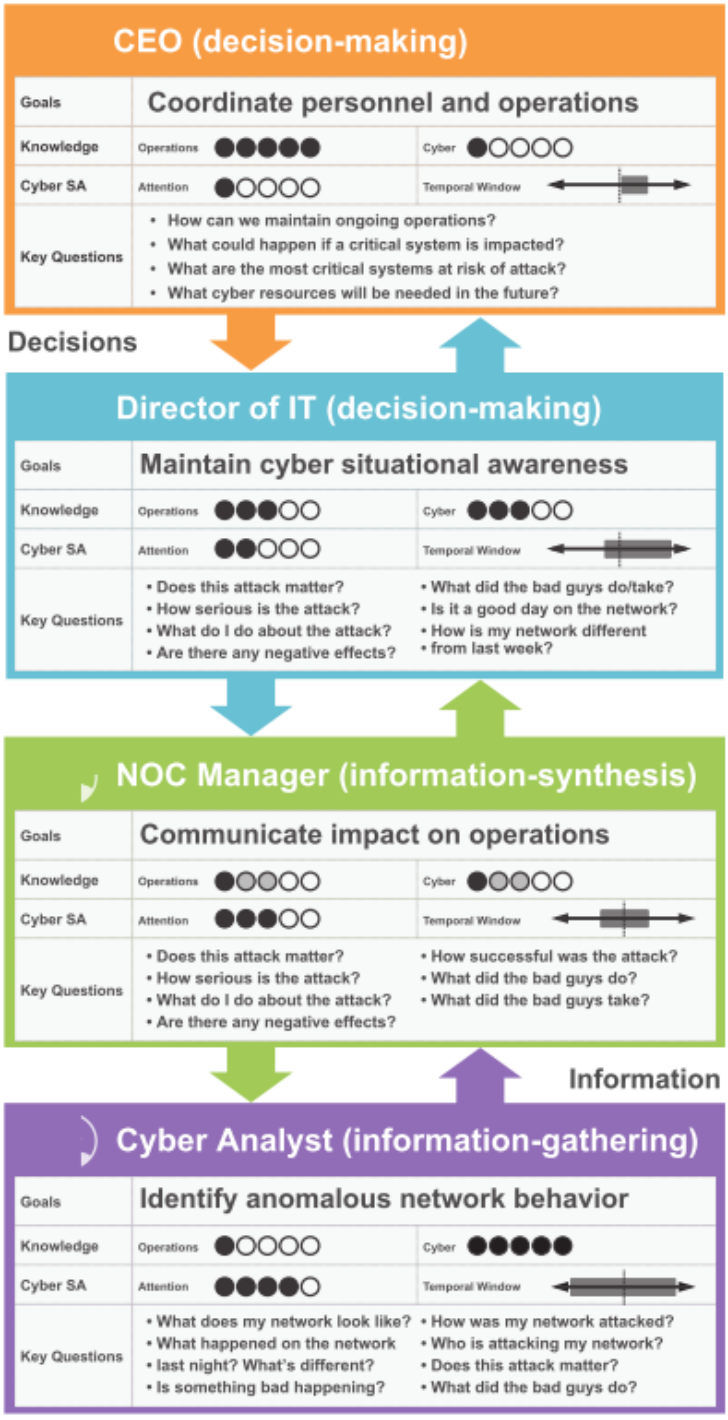


FIGURE 3.12 – Description des rôles spécifiques dans une structure de cybersécurité, extraite de [91] (© 2015, IEEE). Les analystes sont au plus proche des données et les décideurs reçoivent des rapports qui leur permettent de prendre des décisions.

FIGURE 3.13 – Procédure de traitement de ticket, extraite de [58]. Le SIEM transmet une alerte aux analystes de niveau un, qui la traitent ou qui décident de la transmettre à un analyste de niveau trois. La clôture d'un ticket d'alerte s'effectue en produisant un rapport contenant toutes les informations relatives à la caractérisation de l'alerte.

Nous avons décidé de simuler un système de *ticketing* ainsi que des tâches de haut niveau dans notre scénario d'analyse de WannaCry. Par exemple, un analyste devra **sélectionner des tickets** relatifs à des alertes afin d'aller **récupérer des données** et **effectuer des analyses** (simulées) sur les postes concernés. Les tâches à effectuer seront basées sur les rôles des différents utilisateurs.

Visualisations

La visualisation de données est utilisée dans les SOCs à la fois pour l'analyse temps réel des alertes (via le SIEM), pour l'analyse a posteriori de cas complexes (analyse post-mortem ou forensique) et pour la création de comptes-rendus. Les outils de *Visual Analytics* (VA) ne sont utilisés que dans certaines procédures.

Nous pouvons développer des interfaces 2D, 3D desktop ou 3D immersives pour un EVC, permettant d'afficher différents points de vue sur une situation. Un système de filtres sémantiques peut aussi être appliqué par l'utilisateur, afin qu'il sélectionne lui-même les données qu'il souhaite analyser, et qu'il puisse faire des croisements entre ces dernières. Par exemple, un filtre géographique permettrait à un analyste d'avoir une visualisation 3D de la disposition du réseau informatique tandis qu'un filtre réseau afficherait les classes d'adresses IP ordonnées, comme proposé par Zhong *et al.* [135]. L'intégration d'outils existants est aussi possible, via des interfaces et protocoles d'échanges d'information.

Nous proposons dans notre EVC des vues 2D et 3D immersives complémentaires et adaptées aux différents rôles des utilisateurs. Ces vues sont dotées de filtres réseau et

physique qui permettent d'observer l'état de sécurité sous différents angles. Le filtre physique (ou **filtre IT** pour *Information Technology*) permet d'accéder aux données des utilisateurs, à l'emplacement géographique des postes de travail ainsi qu'aux informations relatives à l'entropie des systèmes de fichiers, tandis que le filtre réseau (ou **filtre Cyber**) affiche les données concernant la topologie réseau et les adresses IP.

Données

Les analystes des SOCs doivent traiter de grandes quantités de données hétérogènes en s'aidant des SIEMs ou d'outils dédiés. Ces données doivent être croisées afin d'en extraire une connaissance nécessaire quant au traitement d'alertes et de tickets.

Simuler les sources de données et autres capteurs disponibles sur les réseaux est possible dans un EVC, mais cela requiert de connaître les typologies de données et de déterminer avec précision leur utilité. Il est plus aisé de simuler des données agrégées et des métriques simplifiées comme celles fournies par les SIEMs. L'intégration d'outils d'analyse existants ou d'outils d'entraînements comme les Cyber Ranges, qui simulent l'activité d'un réseau, peut aussi être envisagée.

Pour notre scénario d'analyse d'alertes relatives à une infection par WannaCry, nous avons décidé de simuler deux métriques : **l'entropie des systèmes de fichiers** et **le débit réseau**. Ces métriques permettent de caractériser l'activité du rançongiciel tout en laissant la possibilité de simuler des fausses alertes dues à des sauvegardes ou téléchargements. Nous avons de plus implémenté les données simplifiées de plusieurs postes de travail. Les utilisateurs peuvent inspecter **la liste des processus, le type de système d'exploitation** et d'autres données statiques afin de déterminer si les postes sont victimes d'attaques ou non. Le couplage avec un outil de Cyber Range fournissant des données précises et complètes a aussi été envisagé et constitue une perspective aux travaux de la thèse.

Collaborations

Nous avons pu constater deux types de collaborations au sein des SOCs : une explicite et une implicite. La collaboration explicite, qui concerne l'utilisation d'outils et de procédés collaboratifs s'effectue via un système de *ticketing* et l'envoi de messages électroniques ou de comptes-rendus. Cette collaboration s'inscrit dans des procédures et est médiatisée et cadrée. Par exemple, un suivi de ticket par un coordinateur et un analyste leur permet de collaborer et d'échanger des informations. La collaboration implicite, elle, n'est pas médiatisée et concerne les échanges informels entre personnels des SOCs. Nous avons remarqué par exemple que certains analystes s'entraidaient et que cet échange d'information n'apparaissait pas sur l'historique d'actions des tickets alors que ces derniers sont parfois utilisés rétroactivement pour améliorer les procédures.

Dans un EVC, les collaborations explicites et implicites sont médiatisées et leurs représentations peuvent être adaptées aux besoins. Par exemple, dans le cas de la collaboration explicite, **la représentation d'avatars et de traces d'interactions** (*feedbacks* et *feedforwards*) permet aux utilisateurs de comprendre leurs actions respectives, d'acquérir une *mutual awareness*. Des outils de partage d'informations et un système de *ticketing* peuvent aussi être intégrés afin de respecter certaines pratiques collaboratives des SOCs. La collaboration implicite peut s'appuyer sur **un historique d'actions** partagé entre utilisateurs et sur l'utilisation de microphones, permettant à plusieurs utilisateurs d'échanger à distance et de partager des informations à plusieurs.

Pour l'implémentation de notre scénario, nous avons décidé de simuler le système de **ticketing** utilisé dans les SOCs. Un système de gestion des actions utilisateurs leur permettant de comprendre leurs actions respectives (via des *feedbacks* et un historique d'actions) sera présent. Le scénario étant basé sur une procédure d'analyse collaborative, les différents utilisateurs pourront savoir quelles sont les actions à effectuer par les différents rôles et pourront même modifier les scénarios afin de les enrichir.

Notre modèle CyberCOP 3D devra pouvoir permettre de bâtir des EVC pour l'analyse de l'état de sécurité des systèmes (ou CSA). Les capacités proposées sont génériques et peuvent être réutilisées dans d'autres scénarios d'utilisation. L'implémentation des capacités de l'EVC seront présentées dans le chapitre 4.

Dans la partie suivante, nous décrirons le scénario collaboratif que nous avons proposé pour l'implémentation dans un EVC du modèle CyberCOP 3D.

3.3.3 Scénario Collaboratif d'analyse d'incidents

En parallèle de l'élaboration du modèle CyberCOP 3D, nous avons proposé un scénario collaboratif d'analyse immersive d'alertes basé sur notre modélisation du rançongiciel WannaCry et sur les capacités des utilisateurs décrits dans le CyberCOP 3D.

Le scénario commence par l'infection de postes de travail (aussi appelés *assets*) par WannaCry. L'action de ce dernier sur les assets dépend de leurs systèmes d'exploitation et des préconditions définies précédemment.

Cette infection déclenche des alertes qui sont visibles par le coordinateur. Ce dernier doit alors les sélectionner et créer des tickets pour permettre à un ou plusieurs analystes d'investiguer. Dans notre scénario, nous nous sommes basés dans un premier temps sur la collaboration d'un coordinateur et de plusieurs analystes.

Un analyste choisit le ticket et le traite en sélectionnant l'asset concerné dans une des deux vues à sa disposition (physique ou réseau) : un ticket concernant une alerte entropie doit être examiné dans la vue physique (ou IT) tandis qu'une alerte réseau doit s'analyser dans la vue réseau (ou Cyber). Un analyste ne peut traiter qu'un ticket à la fois et un ticket ne peut être choisi que par un seul analyste.

Une fois l'asset sélectionné, l'analyste doit effectuer des actions d'investigations et envoyer un rapport d'analyse au coordinateur. Si le coordinateur considère que l'analyse est insuffisante, l'analyste doit alors fournir d'autres informations. Sinon, le coordinateur doit caractériser l'alerte, à savoir la considérer comme une vraie menace ou comme un faux positif.

Une fois l'alerte caractérisée par le coordinateur, l'analyste peut clôturer le ticket et en sélectionner un autre.

Ce scénario est résumé sur la Figure 3.14.

Nous avons proposé une suite à ce scénario, à savoir une phase de corrélation d'incidents, qui sera présentée dans la section 5.1, mais cette suite n'a pas pu être implémentée et testée faute de temps et de retours utilisateurs sur la première phase.

Etude des SOCs et Modèle CyberCOP 3D

Notre étude des SOCs, bien qu'impactée par la propagation du rançongiciel WannaCry, nous a permis de proposer un modèle de l'activité collaborative en cybersécurité pouvant être instancié dans un EVC, le CyberCOP 3D. Ce modèle permet de transposer des pratiques existantes en cybersécurité dans un environnement virtuel où les utilisateurs peuvent échanger de l'information et collaborer. Nous avons de plus proposé un scénario d'analyse collaborative d'incidents basé sur une modélisation du rançongiciel WannaCry.

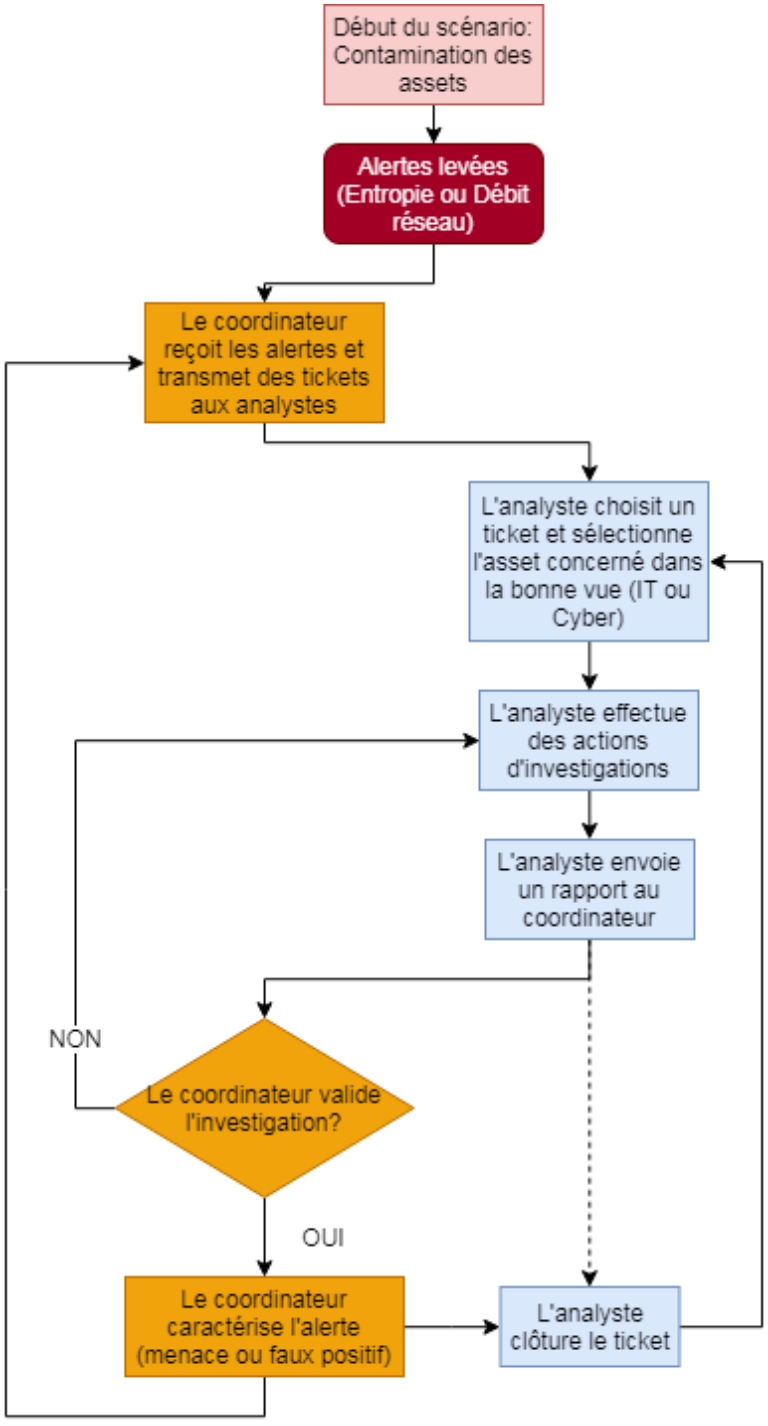


FIGURE 3.14 – Scénario collaboratif d'analyse de WannaCry proposé pour une instanciation du modèle CyberCOP 3D dans un EVC. Le coordinateur reçoit les alertes et transmet des tickets aux analystes. Ces derniers sélectionnent l'asset concerné dans la vue requise par l'analyse (Cyber ou IT), puis effectuent des actions d'investigation. Enfin, ils transmettent un rapport au coordinateur qui caractérise l'alerte, ce qui permet aux analystes de clôturer le ticket.

3.4 Conclusion sur l'analyse de l'activité collaborative des SOCs et sur le modèle CyberCOP 3D

La collaboration en cybersécurité se développe de plus en plus afin de lutter contre des attaques informatiques toujours plus complexes. Cependant, peu d'outils collaboratifs sont mis en place au sein des structures de sécurité comme les *Security Operations Centers* (SOCs). En collaboration avec quatre partenaires industriels de la chaire Cyber CNI, à savoir la Société Générale, EDF, Airbus et Orange, nous avons pu visiter leurs SOCs et proposer un protocole de l'analyse de l'activité. Ce protocole nous a permis d'élaborer un modèle, le CyberCOP 3D, qui a pour objectif de transposer les pratiques de cybersécurité dans un EVC et de médiatiser la collaboration.

Afin d'élaborer un scénario permettant à des utilisateurs d'acquérir une *Cyber Situational Awareness* (CSA), nous avons proposé un cas d'utilisation d'analyse d'incidents liés à la propagation sur un réseau du rançongiciel WannaCry. Ces modèles et scénarios ont été présentés dans les conférences internationales **International Conference on Information Systems Security** (ICISS) [65] et **International Conference on Cooperative Design, Visualization and Engineering** (CDVE) [64].

Dans le chapitre suivant, nous allons présenter plus en détail l'implémentation de ce scénario dans un Environnement Virtuel Collaboratif (EVC).

Chapitre 4

Architecture du CyberCOP 3D : événements, interfaces et interactions

Dans ce chapitre, nous allons présenter l'architecture de l'EVC que nous avons développé afin d'implémenter les différentes capacités notre modèle CyberCOP 3D présenté dans la section 3.3 (Figure 3.11), ainsi que les interfaces et interactions que nous avons proposées.

4.1 Architecture de la solution

Nous avons basé notre solution sur une architecture événementielle, pour gérer les actions utilisateurs et les modifications d'état des *assets* de la simulation. Cette architecture a facilité le développement multi-utilisateurs du simulateur et la gestion des modifications successives dues aux retours d'utilisateurs experts en cybersécurité, en accord avec les règles du design centré utilisateur.

4.1.1 Système événementiel

Nous avons décidé de décrire les actions utilisateurs, les changements d'états des objets et les alertes informatiques par des événements. Ces derniers nous ont permis de proposer une implémentation pour différentes plateformes tout en s'assurant que le comportement du système reste le même. De plus, ce choix nous a permis de tester de manière indépendante les composants d'émission et de réception d'événements. Nous avons donc pu modifier bon nombre de composants, de visualisations et de parties du scénario tout en gardant des fonctionnalités minimales pour présenter des prototypes fonctionnels.

Comme les personnels des SOCs n'étaient pas familiers des possibilités offertes par les technologies immersives, nous avions décidé de leur présenter rapidement des prototypes afin que les prises en compte de l'expression de leurs besoins s'effectuent en cycle court. Ce choix a nécessité de simplifier l'architecture de nos prototypes, tout en gardant en tête une certaine généricité, afin de ne pas avoir à tout refaire lors d'un changement de procédure, d'un ajout de rôles ou autre modifications. Cette simplification est un frein

potentiel à un possible 'passage à l'échelle' de notre architecture, et a nécessité une gestion manuelle de la séquentialité des actions du scénario et de la propagation des événements.

Les événements ont été implémentés grâce à des composants spécifiques au moteur de jeu Unity, les *Scriptable Objects*[1]. Ces derniers sont modifiables via l'interface utilisateur de Unity et ne nécessitent pas d'exécution pour être testés ou modifiés. Ils sont référencés dans les scripts d'exécution via l'éditeur graphique (référence à une variable publique), et existent donc toujours quelque soit la scène exécutée ou le composant activé. Un script de réception d'événement est utilisé pour traiter ces derniers et déclencher des fonctions précises en fonction des paramètres.

La Figure 4.1 décrit le découplage que permettent les *Scriptable Objects* entre émission des événements et réception : lorsque le *Scriptable Object* **PlayerHP** contenant la valeur des points de vie d'un joueur est modifié, l'interface graphique **HP UI** et le système sonore du jeu **Audio System** se modifient aussi, indépendamment du fait que la modification provienne d'un objet **Player** ou non.

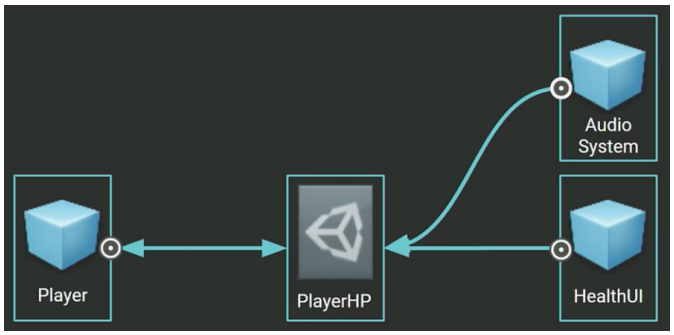


FIGURE 4.1 – Exemple de découplage entre émission et réception d'événements proposé par l'utilisation des Scriptable Objects, extrait de `https://blogs.unity3d.com/2017/11/20/making-cool-stuff-with-scriptableobjects/`.

1. `https://unity3d.com/fr/how-to/architect-with-scriptable-objects`

Dans notre achitecture, nous les avons utilisés de la manière suivante (Figure 4.2) :

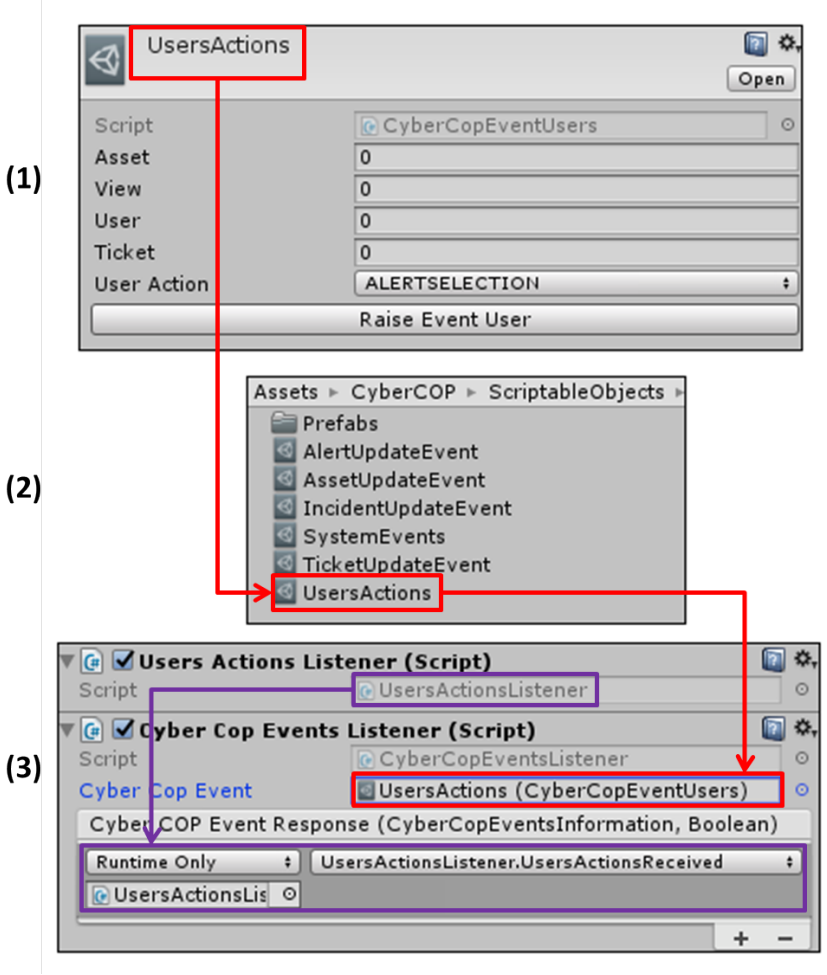


FIGURE 4.2 – Scriptable Object **UsersActions** d'événements. (1) Modification des attributs via un éditeur fourni par Unity. (2) **UsersActions** s'instancie directement via un menu de l'explorateur de fichiers. (3) Il s'utilise en le glissant-déposant dans un script d'objet de Unity et en y faisant référence dans le script.

— le *Scriptable Object* **UsersActions** est créé directement dans l'éditeur de Unity (2) via un menu contextuel, de la même manière qu'un script ou un objet 3D. Il est modifiable via une interface dédiée (1). Cette interface permet de modifier ses attributs via les champs *Asset*, *View*, *User*, *Ticket* et *User Action*, et permet de déclencher l'événement sans avoir à exécuter la simulation via le bouton *Raise Event User*.

— Il est ensuite référencé dans un script MonoBehavior attaché à un objet de la scène, **CyberCopEventsListener** (3). Lorsque l'événement associé au *Scriptable Object* est déclenché durant la simulation, une méthode du script **UsersActionsListener** est appelée. Cet appel se fait via une interface utilisateur, dans le champ **Cyber COP Event Response** (3).

Une fois les *Scriptable Objects* créés et référencés dans des scripts attachés à une scène, ils peuvent être utilisés par ces derniers pour déclencher les événements ou les recevoir.

Les événements que nous utilisons dans notre architecture sont sous la forme :

$$\mathit{CyberCopEvent}(\mathbf{AssetId}, \mathbf{AssetView}, \mathbf{EventAction}, \mathbf{UserId}, \mathbf{TicketID})$$

Les différents paramètres des événements nous permettent de modifier l'état de l'environnement ou de propager des informations.

Le paramètre **AssetID** est une référence à l'asset de l'environnement auquel se réfère l'événement. Si l'événement n'est pas directement lié à un asset (un événement de basculement de vues par exemple), ce paramètre peut servir à transférer d'autres informations ou alors est laissé nul. Sinon, il permet au script de réception d'événements de choisir à quel asset transmettre un appel de fonction.

AssetView est une référence à la vue dans laquelle a été déclenché l'événement. Nous avons implémenté deux vues, une vue physique et une vue réseau, qui concernent deux aspects différents des assets. Les interactions sur l'environnement ont toujours lieu dans une vue, et ces dernières sont indépendantes d'un point de vue événementiel.

EventAction décrit l'action propagée par l'événement. Ce paramètre est issu d'une énumération et filtré par le listener via une structure de contrôle conditionnelle *Switch..Case*. Ce filtrage nous a facilité le déclenchement d'actions appropriées et la liaison entre événements, mais nous oblige à décrire de manière manuelle les liens entre les différents événements.

Lorsqu'un événement utilisateur est reçu (CyberCopEventsInformation e), la composante **EventAction** est filtrée par la structure conditionnelle, et un autre événement est envoyé via une fonction déléguée (AssetUpdateDelegate(assetEvent)) (Figure 4.3).

```
public void UsersActionsReceived(CyberCopEventsInformation e, bool b)
{
    switch(e.EventAction)
    {
        case (int)RequiredActions.ASSETSELECTION:
            [...]
            CyberCopEventsInformation assetEvent = new CyberCopEventsInformation
            ....(e.Asset,e.View,(int)AssetUpdateActions.ASSETSELECTION,
            ........user.id,user.CurrentTicketID);
            AssetUpdateDelegate(assetEvent);
        break;
    }
}
```

FIGURE 4.3 – Exemple d'utilisation du paramètre EventAction pour le filtrage des actions utilisateurs via une structure de contrôle conditionnelle, et envoi d'un autre événement via une fonction déléguée AssetUpdateDelegate.

La liste des actions utilisateurs et relatives à la modification d'état des assets proviennent respectivement de deux énumérations, RequiredActions et AssetUpdateActions. Ces énumérations permettent de rendre humainement lisible l'intitulé des événements (Figure 4.4).

```
public enum RequiredActions
{
    ALERTDETECTION,
    ALERTSELECTION,
    ALERTUNSELECTION,
    ASSETSELECTION,
    ASSETSELECTION_COORD,
    ASSETSELECTION_ANALYST,
    ASSETUNSELECTION,
    ASSETUNSELECTION_COORD,
    ASSETUNSELECTION_ANALYST,
    ALERTSELECTION_COORD,
    ALERTSELECTION_ANALYST,
    [...]
}
[...]
public enum AssetUpdateActions
{
    ADDMALICIOUSPROCESSES,
    ADDLEGITPROCESSES,
    METRICRAISE,
    ALERT,
    ASSETSELECTION,
    [...]
    REPORTASSET,
    NONE,
}
```

FIGURE 4.4 – Énumérations décrivant les actions utilisateurs (RequiredActions) et les actions liées aux assets (AssetUpdateActions).

Le paramètre **UserID** définit l'utilisateur qui a déclenché l'événement. Le système est considéré comme un utilisateur à part entière (pour l'envoi d'actions concernant le scénario par exemple). Ce paramètre nous permet de filtrer si les actions effectuées sont celles de l'utilisateur local ou d'un utilisateur distant, et permet aussi de vérifier l'accomplissement du scénario.

TicketID est le paramètre explicitant le ticket d'alerte auquel se rattache l'action liée à l'événement. Il permet de guider l'utilisateur et de mettre à jour les interfaces en fonction de la progression.

La Figure 4.5 résume le déroulement de la propagation d'un événement utilisateur :

— Lorsqu'un utilisateur est en interaction, il déclenche des appels de fonctions déléguées auxquelles sont abonnées des fonctions d'émission d'événements utilisateurs.

— Ces fonctions déclenchent l'émission des événements, qui sont alors réceptionnés, filtrés, et qui déclenchent à leur tour un appel de fonctions dont des fonctions déléguées qui concernent la mise à jour de l'état des assets.

— Ces fonctions déclenchent à leur tour une émission d'événements assets, qui sont eux aussi filtrés et qui finalement modifient l'état des assets.

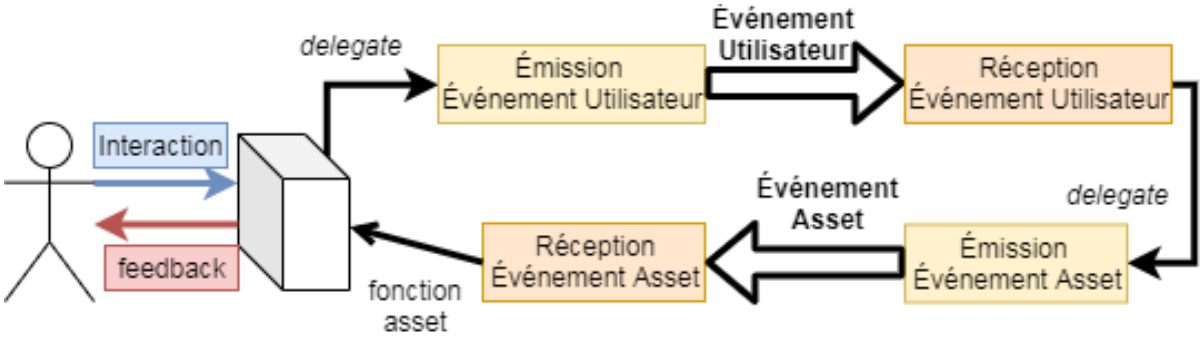


FIGURE 4.5 – Propagation d'événements, de l'interaction utilisateur à l'appel de fonction sur l'asset concerné. L'interaction déclenche un appel de fonction déléguée qui appelle une fonction d'émission d'événement utilisateur, qui est réceptionné, filtré, et transmis aux assets.

Dans les pages suivantes nous allons décrire en détail la propagation d'informations lors de la sélection d'un asset.

Lorsque l'utilisateur sélectionne un asset par un moyen quelconque (pointage dans l'environnement immersif via un rayon d'interaction, clic sur un bouton sur le tableau de bord), une fonction déléguée est appelée afin de permettre au composant gérant l'émission d'événements utilisateurs de transmettre l'information (Figure 4.6).

```
//Fonction déclenchée lors de la sélection d'un asset
public void SetButtonAction()
{
    //déclaration de l'évènement via utilisation de la classe CyberCopEventsInformation
    CyberCopEventsInformation assetaction = new CyberCopEventsInformation(GetAssetInfoID(), view,
    ....RequiredActions.ASSETSELECTION, Scenario.Currentuser.id, Scenario.Currentuser.CurrentTicketID);
    //envoi du paramètre via une fonction détaillée
    Asset3DDelegate(assetaction);
}
[...]

//déclaration de la fonction déléguée dans le même script que la fonction précédente
public delegate void ON3DAssetClickDelegate(CyberCopEventsInformation e);
    public static event ON3DAssetClickDelegate Asset3DDelegate;
-----------------------------------
//abonnement à la fonction déléguée dans le script d'envoi d'évènements utilisateurs
CyberCOP3DInteractiveObject.Asset3DDelegate += Asset3DSelection;
[...]
//liaison dans l'éditeur à l'évenement, sous forme de ScriptableObject
public CyberCopEventUsers UserEvent;
[...]
//Déclenchement de l'évènement (le booléen est un paramètre interne de test)
public void Asset3DSelection(CyberCopEventsInformation e)
{
    UserEvent.Raise(e, true);
    //possibilité de déclencher d'autres actions liées au scénario
}
```

FIGURE 4.6 – Appel de la fonction déléguée Asset3DDelegate au script gérant l'envoi d'événements utilisateurs, et envoi d'un événement via la méthode Asset3DSelection abonnée à la fonction déléguée.

Une fois l'événement émis, il est réceptionné par un composant dédié et filtré, puis retransmis sous une autre forme (en l'ocurrence comme événement d'asset) via une fonction déléguée (Figure 4.7).

```
//réception de l'évènement et filtrage
public void UsersActionsReceived(CyberCopEventsInformation e, bool b)
{
    [...]
    //filtrage en fonction de l'utilisateur, distant ou non
    if (e.UserId == Scenario.Currentuser.id)
    {
        //filtrage en fonction de l'action
        switch(e.EventAction)
        {
            //action de sélection d'asset
            case (int)RequiredActions.ASSETSELECTION:
                //mise à jour de la liste des actions effectuées sur un asset
                Scenario.Assets[e.Asset - 1].State.ActionsDoneOnAsset.Add(e);
                GetComponent<AudioSource>().Play();
                //mise à jour des actions utilisateur
                SelectedAsset(user, e);
                //envoi d'un évènement via une fonction déleguée
                AssetUpdateDelegate(new CyberCopEventsInformation
                ....(e.Asset, e.View, (int)AssetUpdateActions.ASSETSELECTION,
                ........user.id, user.CurrentTicketID));
            break;
            [...]
        }
        [...]
    }
    //mise à jour de la progression du scénario
    ProgressTicket(user, e);
}
```

FIGURE 4.7 – Réception de l'événement utilisateur, filtrage en fonction de l'utilisateur (Scenario.Currentuser.id) et de l'événement (RequiredActions.ASSETSELECTION) et appel d'une fonction déléguée AssetUpdateDelegate au script d'envoi d'événements assets (l'envoi de l'événement en lui même est similaire à celui décrit dans la Figure 4.6).

Une fois l'événement d'asset reçu, il est filtré et envoyé à l'asset concerné via une requête LINQ. Les mises à jour du scénario et des différentes interfaces se font en parallèle de la réception d'événement (permettant de mettre en surbrillance des boutons d'actions ou de progresser dans la procédure) (Figure 4.8).

```
//réception de l'évènement relatif aux assets
public void AssetUpdateState(CyberCopEventsInformation e, bool b)
{
    //filtrage en fonction de l'action
    switch(e.EventAction)
    {
        //action de sélection
        case (int)AssetUpdateActions.ASSETSELECTION:
            //déclenchement de l'action de sélection
            AssetSelectionType(e, true);
            //mise en évidence de l'asset
            HighlightAssetAfterTicketValidation(e, false);
            //mise à jour de l'interface utilisateur
            AssetUIModification(e);
        break;
        [...]
    }
    [...]
}
[...]
public void AssetSelectionType(CyberCopEventsInformation e, bool b)
{
    //si l'utilisateur qui a déclenché l'évènement est l'utilisateur courant
    if(e.UserId==Scenario.currentUser)
    {
        //si l'action a été effectuée dans l'environnement virtuel
        if(Scenario.currentUser.isImmersive)
        {
            //requête LINQ pour sélectionner le bon asset (id & vue)
            var asset = (from item in _assets where item.GetAssetInfoID() == e.AssetId
            ....&& item.view== e.AssetView select item).FirstOrDefault();
            //appel d'une fonction de sélection sur l'asset en question
            asset.SetUserInteraction(e,b);
        }
        [...]

    }
    [...]
}
```

FIGURE 4.8 – Réception de l'événement de l'asset dans la méthode AssetUpdateState. Filtrage de l'action sur l'asset, et appel de la méthode AssetSelectionType pour envoyer l'action requise à l'asset concerné (qui est sélectionné par une requête LINQ) via la méthode SetUserInteraction.

Si un utilisateur distant avait déclenché les événements, le déroulé aurait été sensiblement similaire, mais des notifications et *feedbacks* auraient été fournis à l'utilisateur local en plus de ceux transmis à l'utilisateur distant.

Ce système événementiel nous a facilité la gestion de la collaboration entre utilisateurs ainsi que la création de scénarios.

4.1.2 Gestion de la collaboration

L'utilisation d'événements pour déclencher des actions et changer l'état du système facilite le déploiement multi-utilisateurs de l'application car nous pouvons tester les différents *feedbacks* et actions en simulant la présence d'utilisateurs distants. Toutefois, cela nécessite de s'assurer du caractère déterministe de notre système, à savoir que les mêmes événements doivent toujours avoir les mêmes conséquences.

Si cette condition est vérifiée, nous pouvons alors transmettre simplement des événements entre les applications pour qu'elles soient dans un même état. Cela d'une part limite le trafic réseau entre les systèmes et d'autre part nous permet de 'brancher' soit des utilisateurs humains, soit des *bots* jouant des rôles spécifiques. Un rejeu de situation est également possible, en rejouant de manière contrôlée le déclenchement des événements ayant eu lieu dans une simulation.

Les applications étant indépendantes, leur synchronisation peut s'effectuer en comparant la liste des événements reçus par chaque application. Si un utilisateur se déconnecte par inadvertance, à sa reconnexion il suffit que les utilisateurs toujours connectés lui envoient la liste des événements ayant eu lieu jusqu'à sa reconnexion afin que sa simulation se resynchronise. De plus, cette liste d'événements peut aussi être utilisée pour fournir un historique d'actions, facilitant la *mutual awareness* entre utilisateurs.

Des *feedbacks* d'interaction relatifs aux interfaces ont également été implémentés. Les utilisateurs peuvent visualiser les changements d'états des objets de l'environnement et déterminer l'origine de ces changements. Par exemple, la sélection d'un asset par un autre utilisateur produit un effet visuel qui dépend de l'interface utilisée. Cette action fera apparaître soit un cercle sous l'objet, si l'utilisateur distant l'a sélectionné via un tableau de bord 2D, soit mettra en surbrillance l'asset s'il a été sélectionné via une interface immersive.

Les choix des mises en évidence (la surbrillance et le cercle) sont arbitraires et illustrent davantage la prise en compte de l'asymétrie des *feedbacks* entre utilisateurs distants et locaux, et entre les interfaces 2D et 3D immersives. Des études ergonomiques des interfaces seront nécessaires afin de sélectionner les *feedbacks* les plus pertinents.

Les positions des différents avatars et des outils d'interaction (en l'occurrence des rayons partant de l'avatar des utilisateurs) ne peuvent se décrire par des événements, et sont donc transmises à une fréquence fixée. Afin de pallier les problèmes liés à la

latence, nous avons décidé d'effectuer nos expérimentations via un réseau local et une co-localisation des utilisateurs : ces derniers peuvent alors communiquer verbalement afin de coordonner leurs actions, si les *feedbacks* visuels fournis ne sont pas suffisants.

Même si notre architecture événementielle et nos envois minimaux de données entre applications nous permettent de n'utiliser que des connexions de type TCP ou UDP, nous avons décidé d'utiliser *Photon Unity Network* (PUN), un outil de gestion d'applications multi-utilisateurs pour Unity. Ce dernier offre de nombreux services (gratuits ou payants) permettant de s'assurer une Qualité de Service de l'expérience multi-utilisateurs en offrant des stratégies de compensation de latence, de synchronisation d'objets ou de scripts distribués et d'autorisation d'actions.

Nous n'avons utilisé que les services d'identification, de gestion de connexion et de Remote Procedure Call (RPC) fournis par PUN. Nous avons pu installer un serveur en local, afin de pouvoir effectuer nos expérimentations sans avoir besoin d'une connexion internet aux serveurs Photon.

L'avantage d'utiliser Photon et un système événementiel est que nous pouvons fournir aux utilisateurs différentes interfaces et environnements sans avoir à dupliquer totalement les environnements 3D : il est par exemple possible de connecter un tableau de bord web ou une interface mobile (pour Android par exemple) qui reçoivent et envoient des événements à notre EVC via les commandes RPC.

La connexion entre utilisateurs se fait via un *lobby*, fourni par Photon. Lors de la connexion d'un premier utilisateur, un *lobby* est créé permettant aux utilisateurs suivants de se connecter et de se synchroniser directement avec ce *lobby* (Figure 4.9). Lorsqu'un autre utilisateur se connecte, il reçoit la liste des événements qui ont eu lieu avant sa connexion, afin de mettre à jour l'état de sa simulation. La déconnexion d'un utilisateur envoie un signal aux autres et au serveur Photon, afin d'effectuer automatiquement une migration du *lobby* (en cas de déconnexion du premier utilisateur).

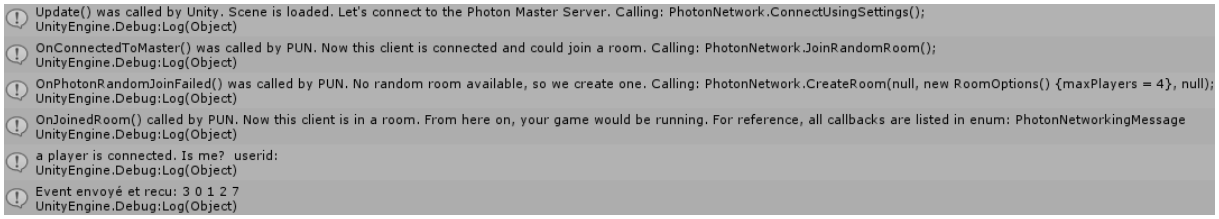


FIGURE 4.9 – Log transmis lors d'une création de lobby par Photon et connexion d'un joueur. Le troisième message indique la création du *lobby* par le premier utilisateur et le message suivant indique la connexion d'un autre utilisateur.

Maintenant que nous avons présenté le système d'événements et la gestion de la collaboration, nous allons décrire la gestion des données de la simulation et du scénario d'analyse d'alertes.

4.1.3 Gestion des données

Les données décrivant l'état des assets et du scénario sont représentées en utilisant les *Scriptable Objects* de Unity, tout comme les événements. Ceci nous permet de modifier les valeurs des données dans l'éditeur, voire d'offrir la possibilité à un expert en cybersécurité non familiarisé avec les moteurs de jeux de disposer d'une interface lui permettant de les modifier aussi.

Les données des assets sont représentées par des *Scriptable Objects*, qui sont créés et modifiés dans l'éditeur de Unity. Ces *Scriptable Objects* contiennent des données statiques (nom de l'utilisateur, adresse IP, système d'exploitation) et des données dynamiques (valeurs des métriques d'entropie et de débit réseau) (Figure 4.10). Les champs de données doivent actuellement être remplies à la main et doivent être vérifiées par le créateur des scénarios d'analyse.

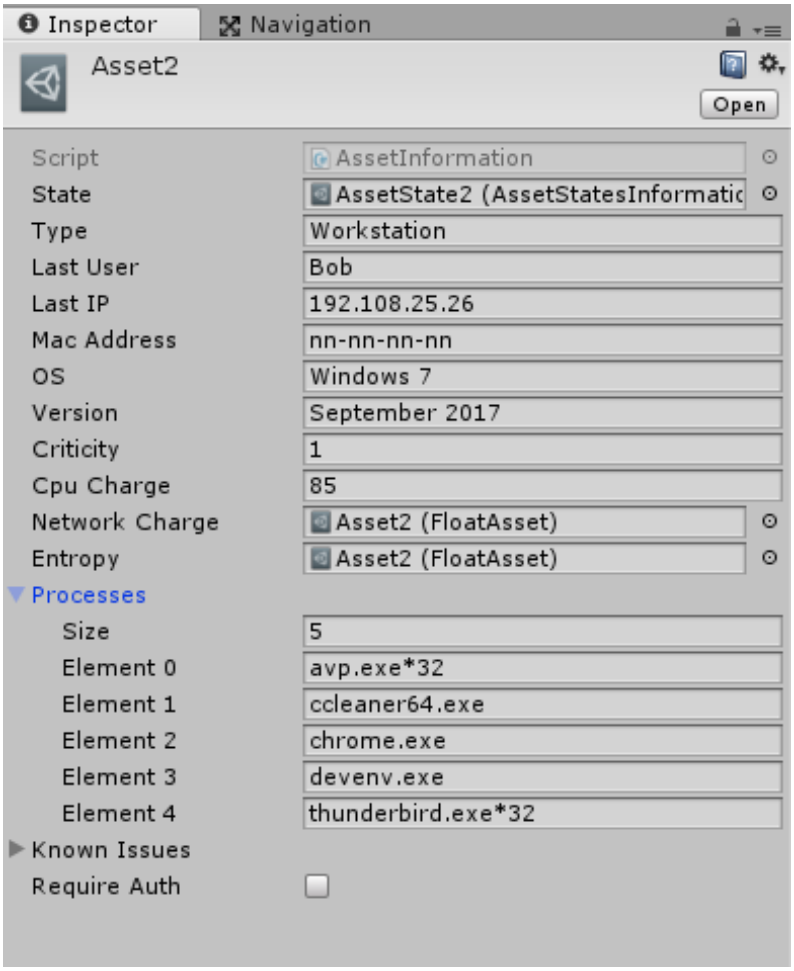


FIGURE 4.10 – Vue éditeur du *Scriptable Object* Asset2 contenant les informations d'un asset de la simulation. Ces informations sont modifiables directement dans l'éditeur de Unity et seront ensuite utilisées dans le *Scriptable Object* de scénario présenté précédemment.

Les *Scriptable Objects* d'attaques informatiques contiennent les informations relatives à la résolution des alertes. Ils sont eux aussi créés et modifiés directement dans l'éditeur de Unity. Ils sont de type CyberCOPAttack et contiennent les informations relatives à la vue concernée par l'alerte (Cyber ou IT), le numéro de l'asset concerné, le type d'alerte (attaque réelle ou faux positif) et la liste des actions utilisateurs attendues pour la résolution d'un ticket. Cette description permet de proposer des scénarios différents sur les mêmes assets (Figure 4.11).

L'inconvénient de notre approche est que le créateur de scénario doit lui-même s'assurer de sa cohérence : si jamais il définit mal une attaque, en se trompant dans l'asset ou la vue concernée, l'éditeur ne lui remontera pas d'erreur.

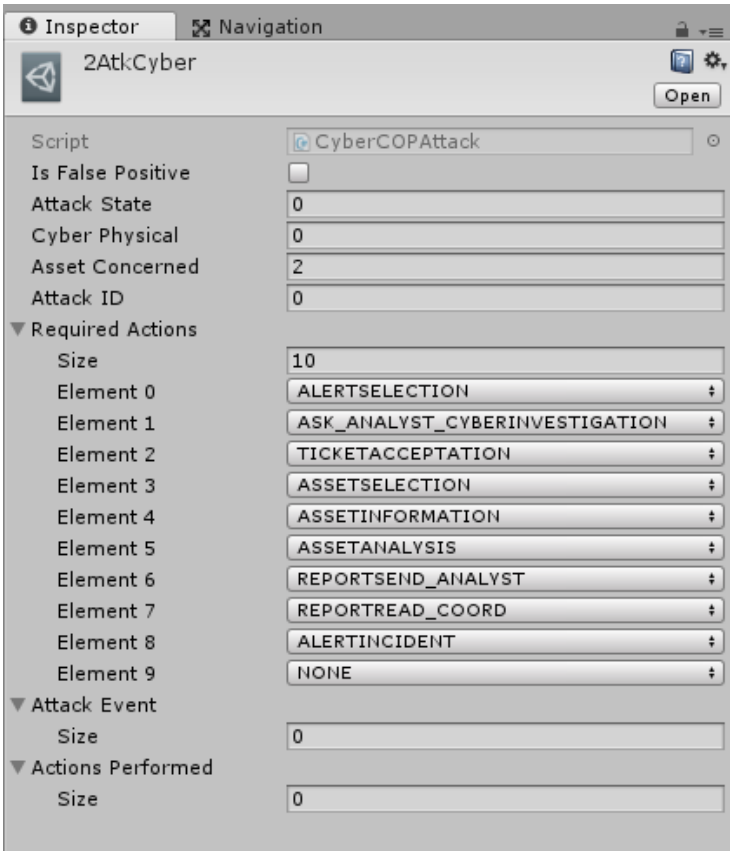


FIGURE 4.11 – Vue éditeur du *Scriptable Object* de l'attaque 2AtkCyber. C'est dans cette vue que le créateur du scénario peut modifier les propriétés d'une attaque sur un asset, en paramètrant le numéro de l'asset concerné, la vue concernée (IT ou Cyber), la nature de l'attaque (véritable attaque ou faux positif) et la procédure des actions à effectuer pour réussir l'analyse de l'alerte liée à cette attaque.

Les données des utilisateurs sont elles aussi représentées par des *Scriptable Objects* modifiables dans l'éditeur de Unity. Ces derniers contiennent les informations de rôle (analyste ou coordinateur), les actions que l'utilisateur peut effectuer, le numéro de ticket courant ainsi que le degré d'immersion de l'utilisateur (Figure 4.12).

Les actions possibles et le numéro de ticket courant permettent de filtrer les actions utilisateurs : si l'utilisateur effectue une action sur un asset concerné par une alerte dont l'identifiant est le numéro du ticket courant de l'utilisateur, ce dernier progresse dans son analyse de l'alerte. Le booléen concernant le degré d'immersion permet d'adapter les interacteurs et les représentations de l'environnement à l'interface déployée.

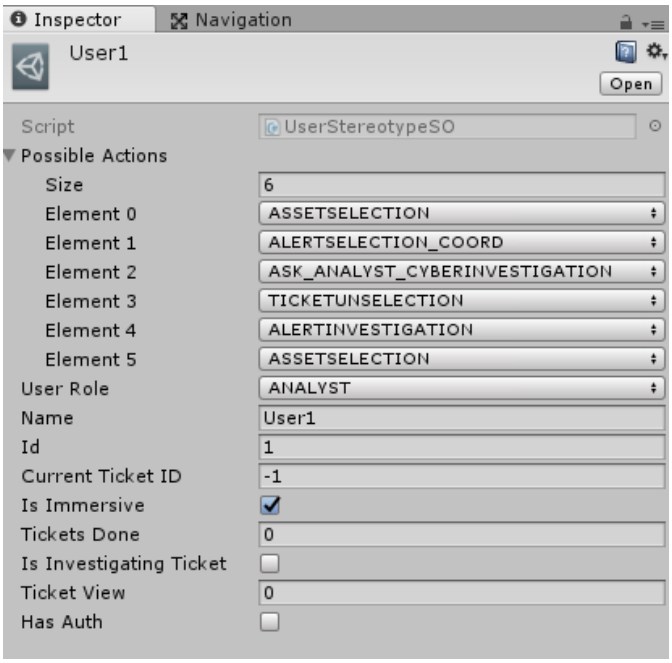


FIGURE 4.12 – Vue éditeur du *Scriptable Object* User1 contenant les informations d'un utilisateur. Ces informations sont modifiables directement dans l'éditeur de Unity et seront ensuite utilisées dans le *Scriptable Object* de scénario présenté précédemment.

La création d'un scénario d'analyse d'alertes nécessite de créer des *Scriptable Objects* pour tous les assets, toutes les alertes et tous les utilisateurs et de les référencer dans le *Scriptable Object* du scénario. Ce dernier doit ensuite être lié aux différents scripts gérant la mise à jour de l'environnement ou le déroulement de la simulation.

Le *Scriptable Objects* **Scenario1** contient les informations relatives au scénario d'analyse, à savoir la liste des assets, des attaques et des utilisateurs (Figure 4.13). C'est dans le scénario que nous définissons l'utilisateur local (ici User1 qui est un *Scriptable Object* de type UserStereotypeSO), la liste des assets du scénario (liste Assets) et la liste des attaques déclenchées dans ce scénario (liste Attacks contenant des *Scriptable Objects* d'événements d'attaque CyberCOPAttack).

Les scénarios se créent à la main directement dans l'éditeur de Unity. L'utilisateur doit ensuite glisser-déposer dans la liste Assets les *Scriptable Objects* qui contiennent des attributs relatifs aux assets comme les valeurs des métriques d'entropie et de débit réseau. De la même manière, il dépose dans la liste Attacks les *Scriptable Objects* CyberCOPAttack relatifs aux attaques que l'on souhaite déclencher dans le scénario. Enfin, il choisit son utilisateur courant.

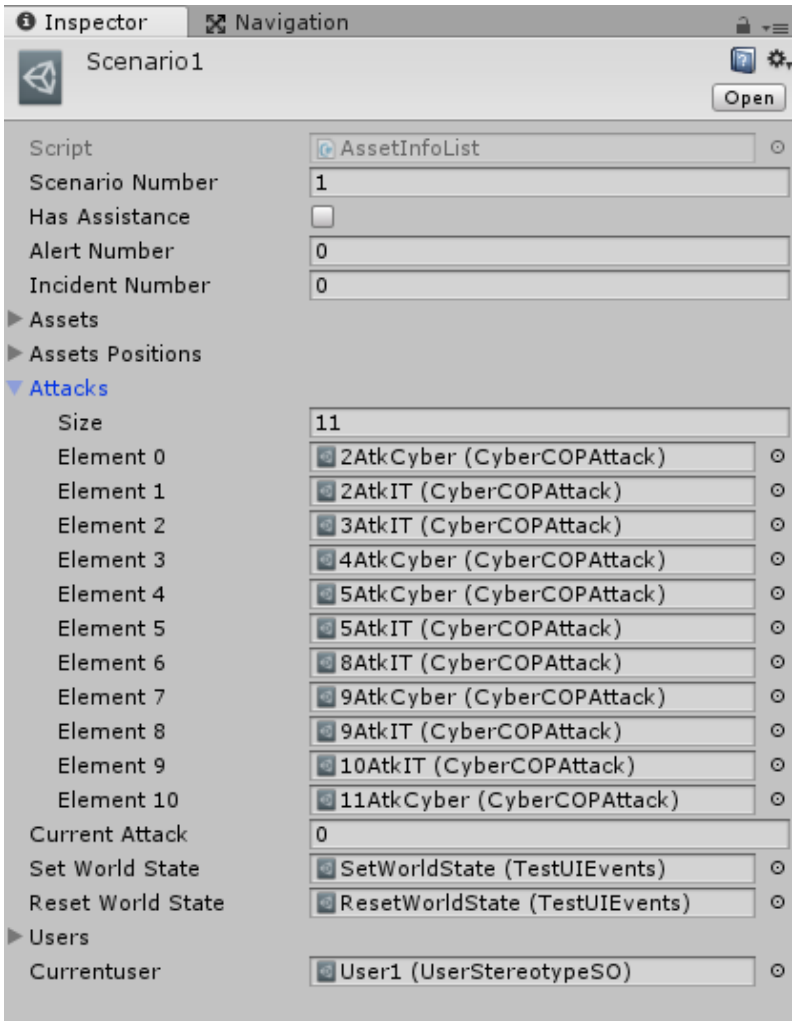


FIGURE 4.13 – Vue éditeur d'un scénario avec les informations des assets, des attaques et des utilisateurs. Ce scénario se prépare à la main en glissant-déposant les Scriptable Objects relatifs aux attaques, assets et utilisateurs. La référence à ce *Scriptable Object* est utilisée pour accéder aux informations durant l'exécution.

Cette mise en place est fastidieuse et n'est pas robuste aux erreurs humaines mais elle a l'avantage d'être généralisable et modulaire : un utilisateur expert en cybersécurité peut créer ses propres scénarios d'analyse en définissant les attaques informatiques (ainsi que leur procédure d'analyse), les assets concernés par ces attaques et les rôles des utilisateurs devant analyser ces attaques.

Dans la section suivante nous décrirons les interfaces et les techniques d'interaction que nous avons développées afin d'utiliser notre architecture d'EVC.

Architecture événementielle et gestion des données

Nous avons choisi de développer une architecture simple basée sur un système événementiel et des structures de données modifiables dans l'éditeur du moteur de jeu Unity. Cette solution nous a facilité la gestion du multi-utilisateur le déploiement multi-supports. La gestion des données et des événements via des *Scriptable Objects* nous a permis de prototyper rapidement différentes versions de notre EVC, et elle nous a permis de créer des scénarios simples d'analyse d'alertes. Bien que cette architecture ne soit pas faite pour un passage à l'échelle des scénarios et interactions, elle est suffisament extensible pour servir de socle à des implémentations plus complexes.

4.2 Interfaces et interactions

Afin de répondre aux besoins des différents rôles définis dans notre modèle CyberCOP 3D, nous avons développé des interfaces 2D et 3D immersives, et nous avons proposé un système de changement de vues ainsi qu'une gestion de la propagation des événements en fonction de l'état de l'environnement.

4.2.1 Interfaces immersives et non immersives

Une interface 2D disponible sur tablette ou ordinateur a été développée pour le rôle de coordinateur. Elle permet à ce dernier de recevoir les alertes et d'agir en conséquence, et de disposer d'une vue de haut de l'environnement virtuel (Figure 4.14).

FIGURE 4.14 – Interface 2D du coordinateur, avec la liste des alertes reçues ainsi que les actions possibles. La minicarte permet de suivre l'évolution des analyses (les alertes IT et Cyber sur les assets sont représentées respectivement par des carrés jaunes et roses) et de localiser les utilisateurs (l'utilisateur local est représenté ici par un rond bleu et l'utilisateur distant par un rond blanc).

L'environnement virtuel immersif a été développé à l'aide du moteur de jeu Unity et en utilisant le toolkit d'interaction VRTK, qui propose entre autres des métaphores d'interaction et de locomotion utilisables sur différents supports (casques immersifs, applications desktop etc...). En complément à VRTK, nous avons utilisé plusieurs *Assets* disponibles dans Unity afin de modéliser l'environnement 3D. Cet environnement a été modifié pour correspondre aux besoins de notre scénario d'analyse d'alertes (Figure 4.15).

Il est composé d'un étage d'immeuble et représente les locaux d'une entreprise fictive. Des postes de travail sont positionnés dans différentes salles et bureaux.

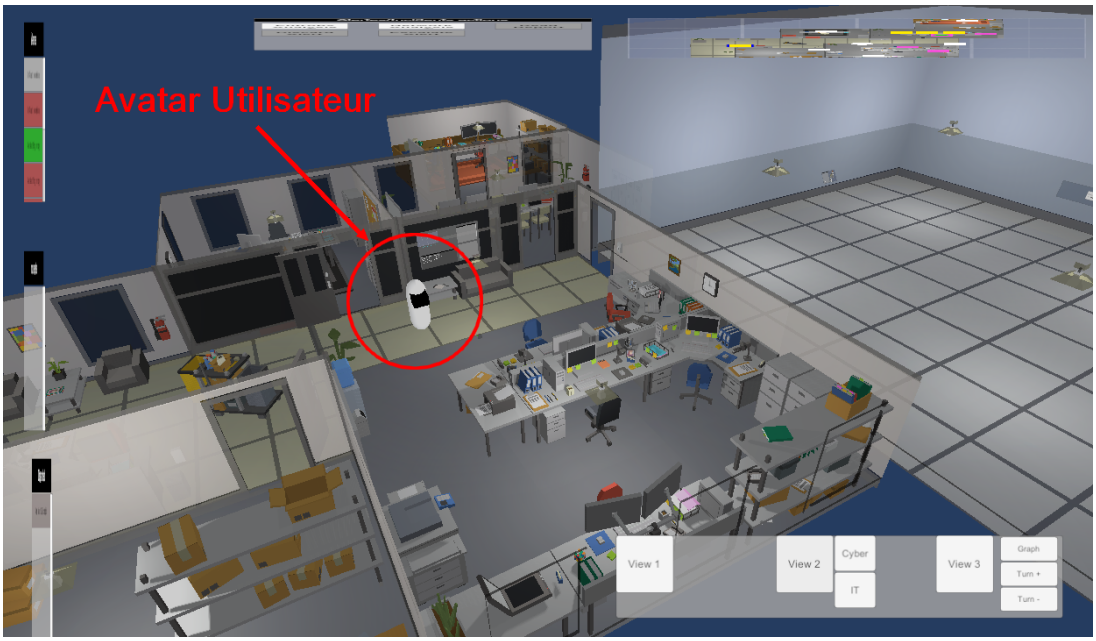


FIGURE 4.15 – Vue de haut de l'environnement virtuel dans lequel évoluent les analystes. Les utilisateurs sont représentés par des capsules dotées de visiocasques. L'environnement est composé d'un étage d'immeuble dans lequel des postes de travail sont positionnés dans différentes salles.

De plus, nous avons proposé un graphe 3D interactif. Ce graphe permet de visualiser les liens physiques entre les assets (topologie réseau) mais aussi des liens sémantiques avec l'asset sélectionné (par exemple les assets du réseau ayant le même système d'exploitation). La disposition des noeuds du graphe est définie par la topologie du réseau : les assets du même sous-réseau sont en dessous de l'asset tandis que les autres éléments sont répartis au dessus (Figure 4.16).

Le graphe 3D est situé dans une salle spéciale à côté des bureaux de notre environnement (à droite sur la Figure 4.15).

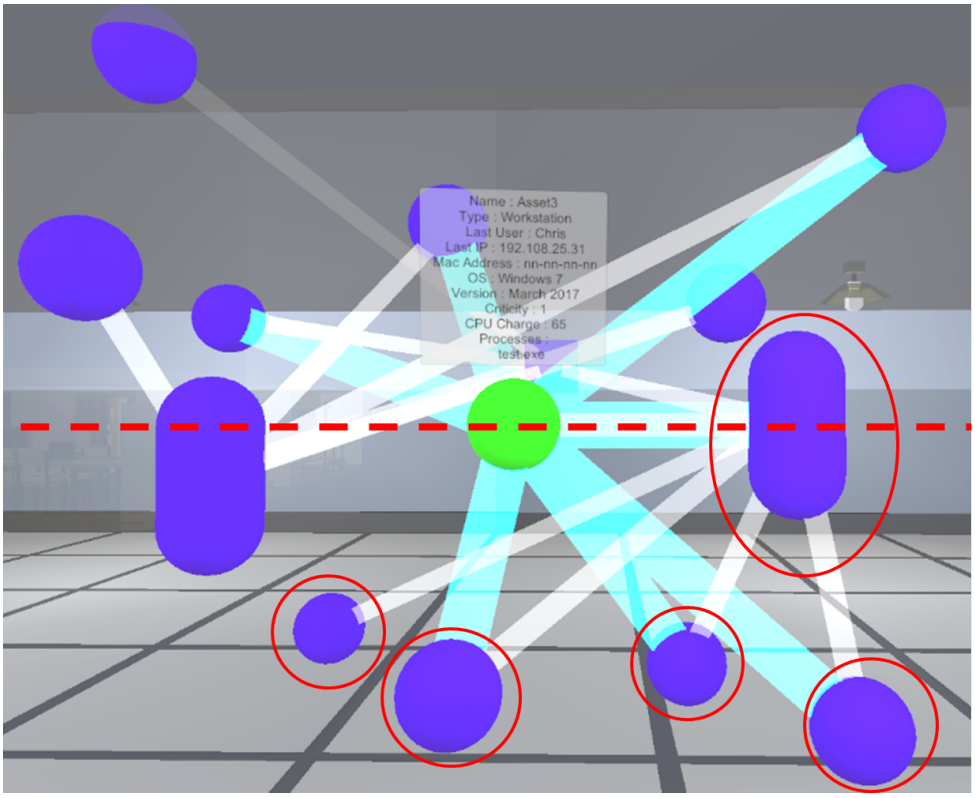


FIGURE 4.16 – Graphe 3D interactif représentant les relations entre un asset sélectionné et le reste du réseau. Les liens bleus permettent de visualiser les assets ayant une propriété similaire (en l'occurrence le système d'exploitation) et les liens blancs indiquent la topologie réseau. Les assets du même sous-réseau que l'asset sélectionné sont situés en dessous de lui (en rouge).

Nous avons implémenté nos interfaces sur tablettes Android et Windows, sur ordinateur de bureau (pour utilisation immersive avec un casque de RV ou non), et dans un CAVE (Figure 4.17), en ne modifiant que les *feedbacks* d'interaction et d'événements.

FIGURE 4.17 – Déploiement du CyberCOP 3D dans un CAVE.

Un système de changement de vues a été implémenté dans l'environnement afin de limiter la surcharge de données présentes à l'écran.

4.2.2 Changements de vues

Comme présenté dans la section 3.3, nous avons proposé différentes vues dans l'EVC permettant d'afficher différents aspects des données et situations. La vue réseau (Cyber) contient les informations concernant la topologie et les connexions réseau tandis que la vue physique (IT) contient les informations sur les utilisateurs et sur l'utililisation des ordinateurs.

Ces vues ont été implémentées en dupliquant les objets de l'environnement, en leur appliquant des *Materials* différents et en les affichant sur une couche d'affichage différente de la caméra virtuelle (Figure 4.18).

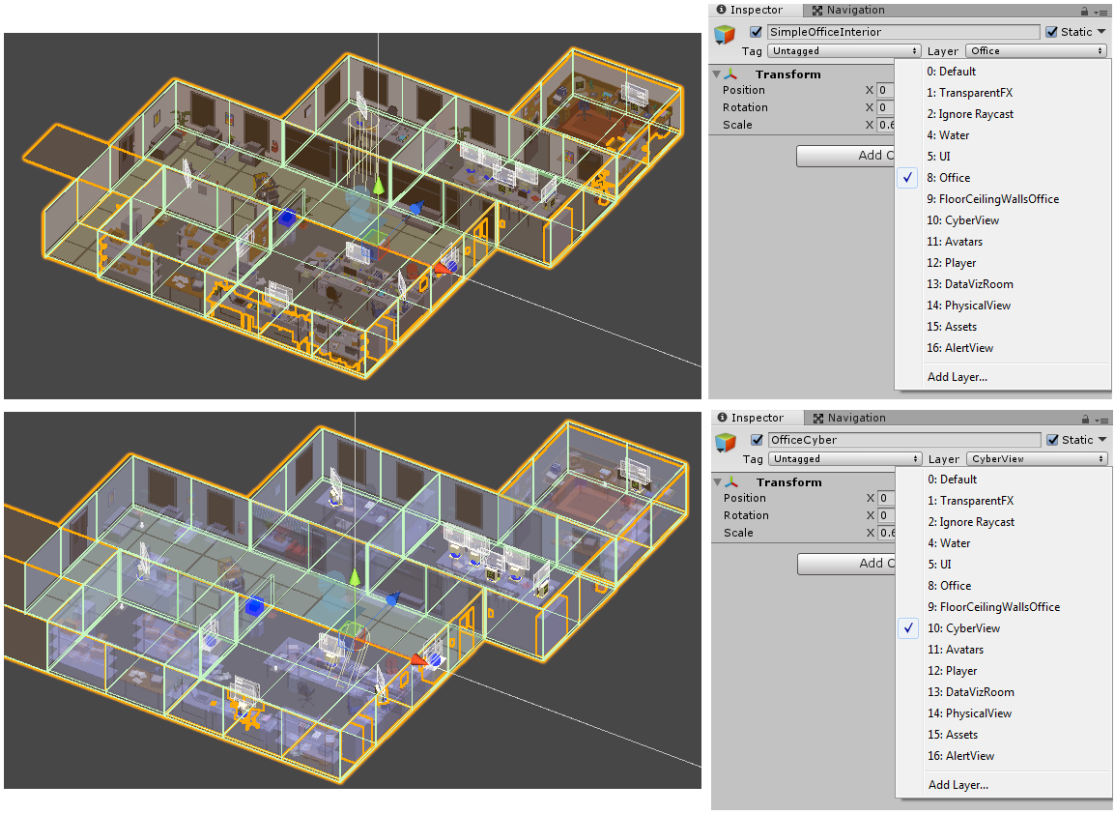


FIGURE 4.18 – Duplication des objets 3D et séparation en plusieurs couches de rendu (Office et Cyberview) qui correspondent aux vues IT et Cyber.

Ainsi, lorsqu'un événement de changement de vue est reçu, le *culling mask* de la caméra virtuelle et le script de gestion des interactions sont modifiés, et les objets de la vue non affichés sont désactivés (Figure 4.19).

Les différentes représentations du même asset dans les différentes vues sont co-localisées, ce qui permet de garder en tête le contexte d'interaction lors d'un changement de vues, qui est instantané (Figure 4.20).

Les changements de vue se font par événements et peuvent donc être pris en compte dans la réalisation du scénario.

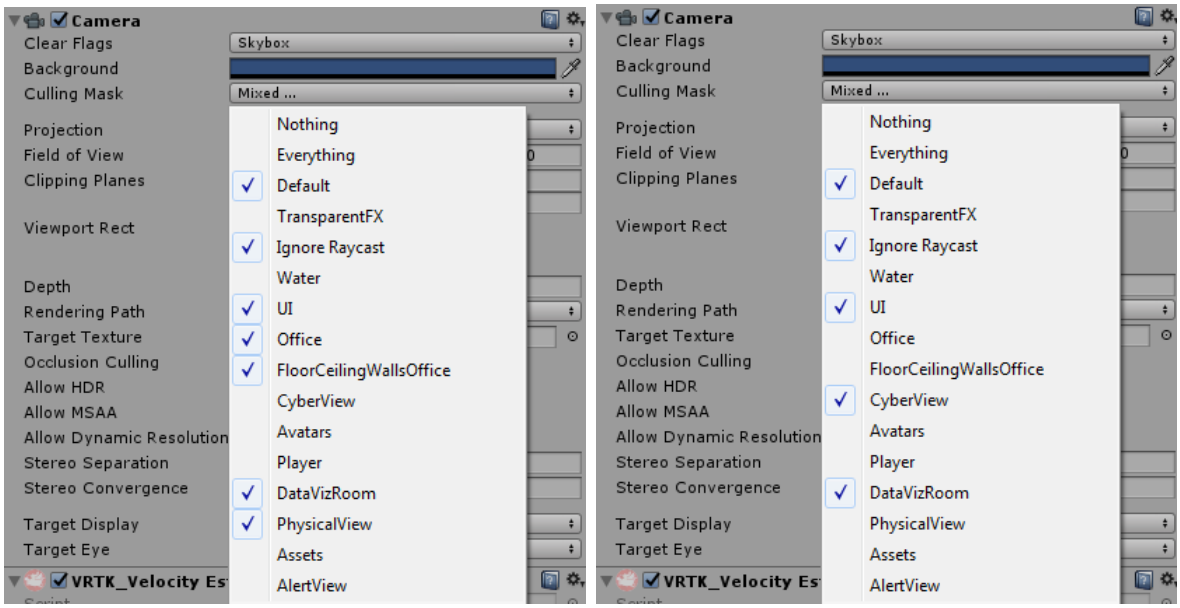


FIGURE 4.19 – Couches d'affichage des caméras en vue IT et Cyber. On peut remarquer que les couches de rendu Office et Cyberview vues dans la Figure 4.18 sont activées ou désactivées en fonction de la vue.

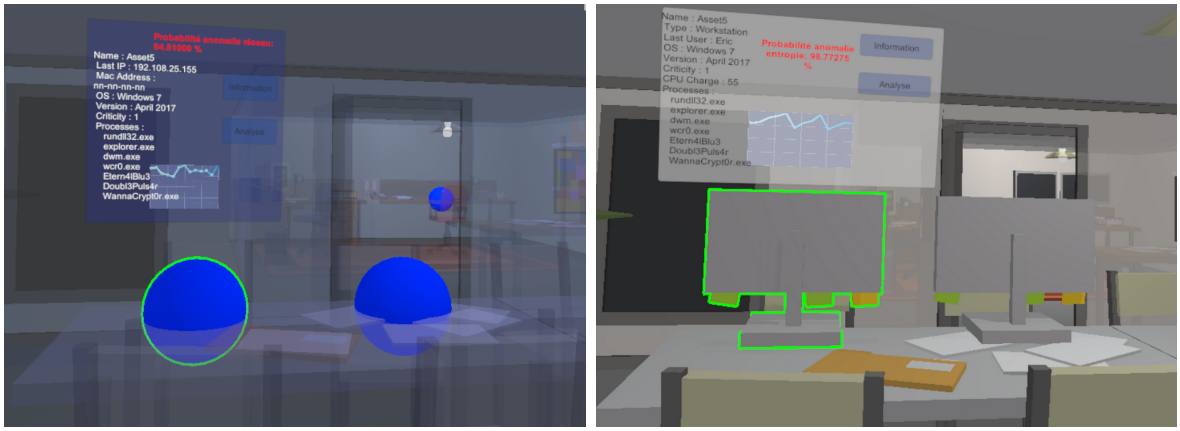


FIGURE 4.20 – De gauche à droite, vues Cyber et IT des assets. La vue Cyber contient les informations relatives au réseau (adresse IP, mesures du débit réseau) tandis que la vue IT contient celles relatives à l'utilisation de l'asset (dernier utilisateur, mesures d'entropie).

4.2.3 Interaction contextualisée et déroulement du scénario

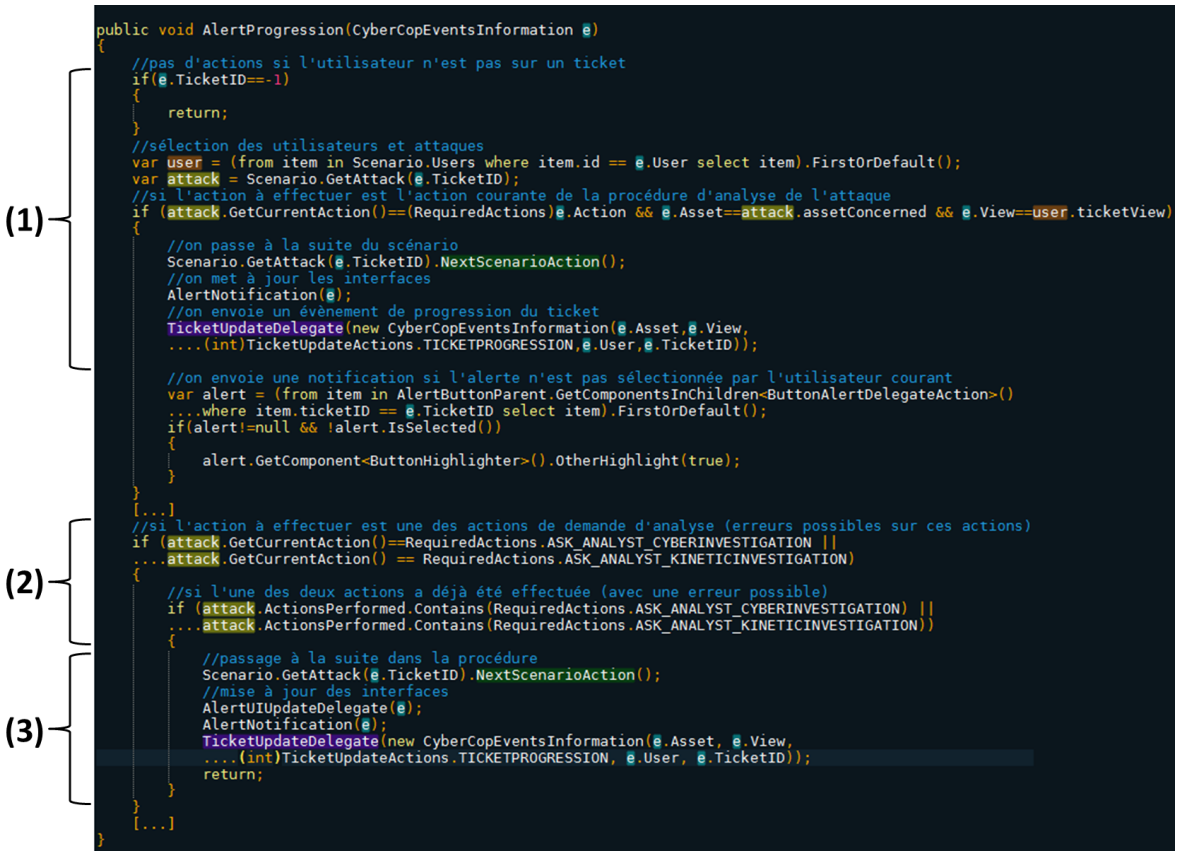
Comme montré précédemment, les interactions et changements d'états se font via notre architecture événementielle. C'est lors de la réception des événements que nous effectuons les filtrages contextuels en fonction des rôles, interfaces, voire des actions des utilisateurs.

L'affichage des interfaces utilisateurs nécessite aussi un filtrage afin de prendre en considération l'avancée des utilisateurs dans le scénario. Cette avancée dépend des événements effectués et peut donc être définie à différentes granularités : soit nous validons tous les événements effectués, soit nous validons seulement des événements majeurs, afin d'autoriser une certaine souplesse dans l'application des procédures.

Par exemple, si un événement est attendu et que l'utilisateur en effectue un autre que nous considérons comme proche (une demande d'analyse de l'entropie au lieu d'une demande d'analyse du débit réseau), nous pouvons soit considérer que l'utilisateur s'est trompé mais faire avancer quand même la procédure (l'utilisateur a demandé une analyse), soit considérer que les actions sont trop différentes et ne pas faire avancer cette dernière (l'utilisateur doit effectuer une demande d'analyse précise) (Figure 4.21).

Nous avons implémenté un système simplifié de gestion d'erreurs de cette manière : le coordinateur peut se tromper sur la demande du type d'analyse à effectuer (analyse de l'entropie ou du débit réseau) et sur la caractérisation de l'alerte (escalade ou faux positif) tandis que l'analyste peut se tromper sur les informations à remonter (rapport incomplet).

Toutefois, si le coordinateur s'est trompé dans sa demande d'analyse (entropie au lieu de débit réseau par exemple) et que l'analyste effectue une analyse de l'entropie, nous considérons que seul le coordinateur a fait une erreur, car l'analyste a respecté la demande.

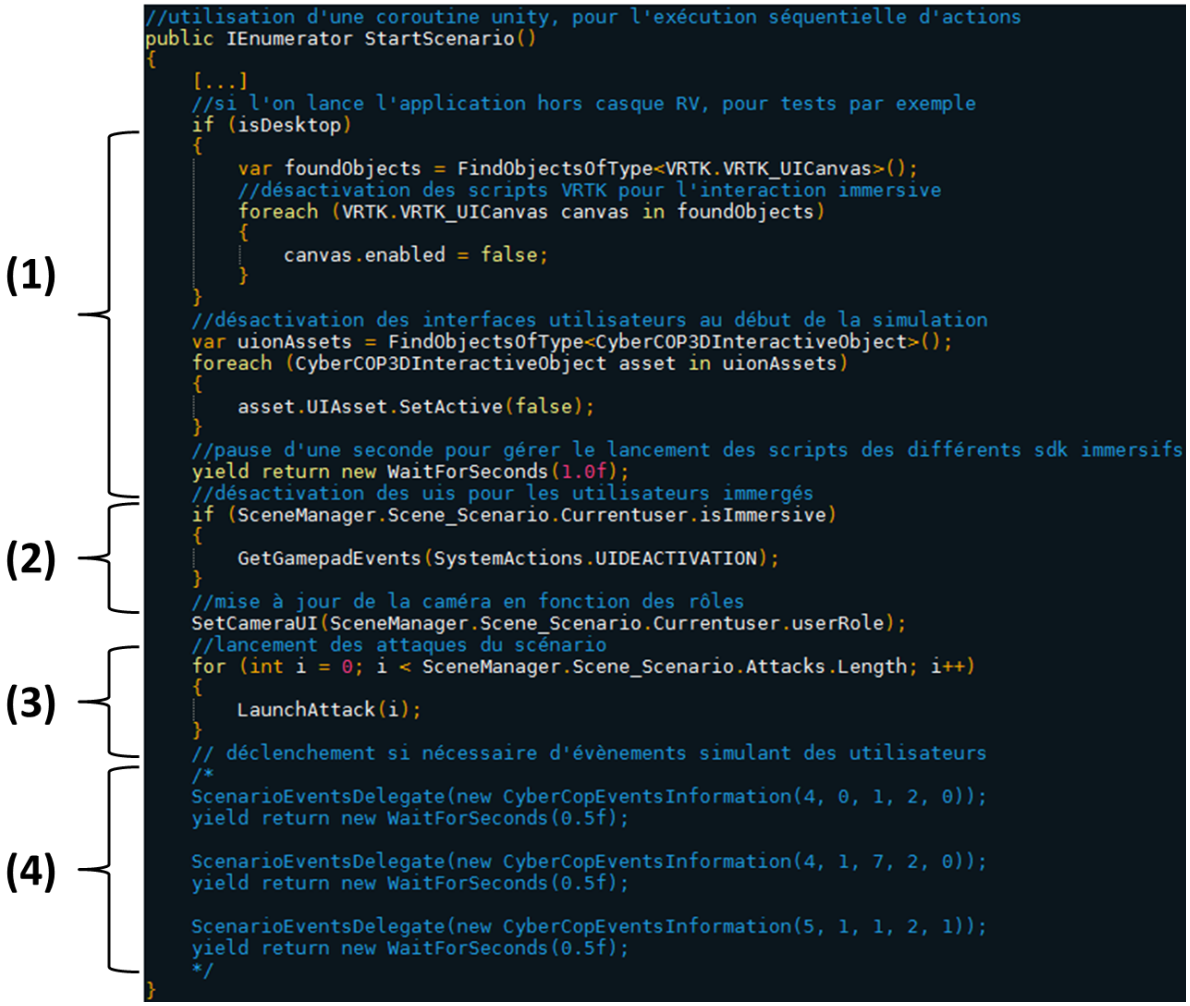



```
public void AlertProgression(CyberCopEventsInformation e)
{
    //pas d'actions si l'utilisateur n'est pas sur un ticket
    if(e.TicketID==-1)
    {
        return;
    }
    //sélection des utilisateurs et attaques
    var user = (from item in Scenario.Users where item.id == e.User select item).FirstOrDefault();
    var attack = Scenario.GetAttack(e.TicketID);
    //si l'action à effectuer est l'action courante de la procédure d'analyse de l'attaque
    if (attack.GetCurrentAction()==(RequiredActions)e.Action && e.Asset==attack.assetConcerned && e.View==user.ticketView)
    {
        //on passe à la suite du scénario
        Scenario.GetAttack(e.TicketID).NextScenarioAction();
        //on met à jour les interfaces
        AlertNotification(e);
        //on envoie un évènement de progression du ticket
        TicketUpdateDelegate(new CyberCopEventsInformation(e.Asset,e.View,
        ....(int)TicketUpdateActions.TICKETPROGRESSION,e.User,e.TicketID));

        //on envoie une notification si l'alerte n'est pas sélectionnée par l'utilisateur courant
        var alert = (from item in AlertButtonParent.GetComponentsInChildren<ButtonAlertDelegateAction>()
        ....where item.ticketID == e.TicketID select item).FirstOrDefault();
        if(alert!=null && !alert.IsSelected())
        {
            alert.GetComponent<ButtonHighlighter>().OtherHighlight(true);
        }
    }
    [...]
    //si l'action à effectuer est une des actions de demande d'analyse (erreurs possibles sur ces actions)
    if (attack.GetCurrentAction()==RequiredActions.ASK_ANALYST_CYBERINVESTIGATION ||
    ....attack.GetCurrentAction() == RequiredActions.ASK_ANALYST_KINETICINVESTIGATION)
    {
        //si l'une des deux actions a déjà été effectuée (avec une erreur possible)
        if (attack.ActionsPerformed.Contains(RequiredActions.ASK_ANALYST_CYBERINVESTIGATION) ||
        ....attack.ActionsPerformed.Contains(RequiredActions.ASK_ANALYST_KINETICINVESTIGATION))
        {
            //passage à la suite dans la procédure
            Scenario.GetAttack(e.TicketID).NextScenarioAction();
            //mise à jour des interfaces
            AlertUIUpdateDelegate(e);
            AlertNotification(e);
            TicketUpdateDelegate(new CyberCopEventsInformation(e.Asset, e.View,
            ....(int)TicketUpdateActions.TICKETPROGRESSION, e.User, e.TicketID));
            return;
        }
    }
    [...]
}
```

FIGURE 4.21 – (1) Progression du scénario en fonction des informations de l'événement reçu et de l'action courante. Si l'événement courant est une action attendue, appel de la fonction NextScenarioAction(). (2) Gestion des erreurs potentielles de demande d'analyse. (3) Si l'action courante du scénario est une demande d'analyse mais qu'une autre demande a déjà été effectuée, le scénario progresse.

Nous avons défini des conditions initiales à notre scénario en fonction des interfaces et du scénario : en utilisant le système de *coroutines* fourni par Unity, nous pouvons déclencher de manière séquentielle des événements et activer ou non certains objets. Nous pouvons de plus simuler le comportement d'un utilisateur afin de tester la collaboration et l'affichage des *feedbacks* d'interaction (Figure 4.22).




```
//utilisation d'une coroutine unity, pour l'exécution séquentielle d'actions
public IEnumerator StartScenario()
{
    [...]
    //si l'on lance l'application hors casque RV, pour tests par exemple
    if (isDesktop)
    {
        var foundObjects = FindObjectsOfType<VRTK.VRTK_UICanvas>();
        //désactivation des scripts VRTK pour l'interaction immersive
        foreach (VRTK.VRTK_UICanvas canvas in foundObjects)
        {
            canvas.enabled = false;
        }
    }
    //désactivation des interfaces utilisateurs au début de la simulation
    var uionAssets = FindObjectsOfType<CyberCOP3DInteractiveObject>();
    foreach (CyberCOP3DInteractiveObject asset in uionAssets)
    {
        asset.UIAsset.SetActive(false);
    }
    //pause d'une seconde pour gérer le lancement des scripts des différents sdk immersifs
    yield return new WaitForSeconds(1.0f);
    //désactivation des uis pour les utilisateurs immergés
    if (SceneManager.Scene_Scenario.Currentuser.isImmersive)
    {
        GetGamepadEvents(SystemActions.UIDEACTIVATION);
    }
    //mise à jour de la caméra en fonction des rôles
    SetCameraUI(SceneManager.Scene_Scenario.Currentuser.userRole);
    //lancement des attaques du scénario
    for (int i = 0; i < SceneManager.Scene_Scenario.Attacks.Length; i++)
    {
        LaunchAttack(i);
    }
    // déclenchement si nécessaire d'évènements simulant des utilisateurs
    /*
    ScenarioEventsDelegate(new CyberCopEventsInformation(4, 0, 1, 2, 0));
    yield return new WaitForSeconds(0.5f);

    ScenarioEventsDelegate(new CyberCopEventsInformation(4, 1, 7, 2, 0));
    yield return new WaitForSeconds(0.5f);

    ScenarioEventsDelegate(new CyberCopEventsInformation(5, 1, 1, 2, 1));
    yield return new WaitForSeconds(0.5f);
    */
}
```

FIGURE 4.22 – Coroutine d'initialisation séquentielle. (1) Désactivation des objets d'interface non immersifs et pause d'une seconde, puis (2) désactivation des objets d'interface et (3) déclenchement des événements d'alertes. (4) En commentaire, événements pouvant simuler un comportement utilisateur.

Comme présenté dans la partie 3.3.3, dans notre scénario les analystes ne peuvent choisir qu'un ticket à la fois et un ticket ne peut être traité que par un seul analyste. Ceci nous a permis d'éviter les problèmes de concurrence d'action. Les tickets se résolvant de manière successive, si un utilisateur effectue une action sur un ticket qui n'est pas celui de l'utilisateur courant, ce dernier sera notifié de cette action, ce qui lui permet de suivre l'évolution du scénario.

À ce jour nous n'avons pas implémenté de score utilisateur en fonction des actions effectuées, mais cela peut se faire en comparant la liste d'actions effectuées avec la procédure optimale, et en implémentant un système de pondération dépendant du temps de réalisation des tâches. De même, l'ajout de procédure de demande de privilèges, ou *credential* nous a été suggéré, mais cette procédure n'a pas encore été implémentée.

Ces différents aspects sont implémentables mais devront être testés durant des réalisations de scénarios. Comme nous avons développé nous-mêmes le moteur de scénarisation, nous pouvons soit modifier nous même les procédures, soit montrer aux experts des SOCs comment le faire via l'éditeur de Unity.

Interaction et interfaces

Nous avons implémenté notre modèle CyberCOP 3D dans un EVC contenant à la fois une représentation sous forme de locaux d'entreprise et une représentation des données sous forme de graphe 3D. Nous avons développé des interfaces 2D ou 3D immersives, qui nous ont permis d'offrir des vues adaptées aux différents rôles de notre scénario d'analyse et nous ont aussi permis de développer les différentes capacités de notre modèle, comme le changement de vues. La contextualisation des interactions au sein de l'EVC est gérée par notre système événementiel, ce qui nous permet d'adapter les scénarios en fonction des utilisateurs.

4.3 Conclusion sur l'architecture proposée

Afin d'implémenter notre modèle CyberCOP 3D dans un Environnement Virtuel Collaboratif (EVC), nous avons développé une architecture basée sur un système événementiel et sur des structures de données modifiables directement dans l'éditeur du moteur de jeu Unity. Cette architecture permet à des utilisateurs non familiarisés avec les moteurs de jeu de proposer des scénarios collaboratifs d'analyse d'alertes. La création des scénarios se fait manuellement et nécessite de définir les assets, les attaques informatiques, les procédures d'analyse ainsi que les rôles des utilisateurs dans l'éditeur de Unity, sans avoir à modifier le code informatique.

Nous avons proposé une architecture simple qui nous a permis de proposer différents prototypes d'interfaces 2D ou 3D immersives, adaptés aux rôles définis dans notre modèle CyberCOP 3D, basé sur l'étude des SOCs. Ces interfaces permettent aux utilisateurs de collaborer afin d'effectuer des procédures d'analyses.

Un des défauts de notre architecture est que les scénarios doivent être créés à la main dans l'éditeur de Unity. Toutefois, étant basée sur un filtrage simple des événements et actions utilisateurs, elle pourra être améliorée en fonction des cas d'utilisations, voire être couplée avec des outils de scénarisation existants.

Dans le chapitre suivant, nous allons présenter l'implémentation du scénario d'analyse collaborative de WannaCry que nous avons développé, ainsi que l'évaluation de l'utilisabilité d'un EV pour l'analyse d'alertes que nous avons effectuée.

Chapitre 5

Instanciation et évaluation du CyberCOP 3D

Dans ce chapitre, nous allons décrire dans un premier temps l'instanciation de notre modèle CyberCOP 3D dans un EVC, basée à la fois sur notre architecture présentée dans le chapitre précédent et sur le scénario collaboratif d'analyse du rançongiciel présenté dans la section 3.3.3, et dans un second temps l'étude de l'utilisabilité d'un Environnement Virtuel pour l'analyse d'alertes que nous avons effectuée.

5.1 Instanciation du modèle et du scénario d'analyses d'alertes

Dans cette partie, nous allons présenter le déroulé de notre scénario. Ce déroulé est découpé en deux phases, une phase d'analyse et une phase de corrélation d'alertes. La phase d'analyse correspond au scénario présenté dans le chapitre 3.3.3, tandis que la phase de corrélation a été proposée durant le développement du prototype de l'EVC, après des retours d'experts. Ce déroulé décrira à la fois les étapes du scénario et les interactions permettant l'accomplissement de ces étapes. Pour plus de simplicité, le scénario est décrit avec deux participants, un coordinateur et un analyste, mais il peut bien évidemment s'adapter à davantage d'utilisateurs.

5.1.1 Phase d'analyse d'alertes

La première phase de notre scénario est la phase d'analyse d'alertes, qui a été présentée dans la section 3.3.3. Le déroulement du scénario est disponible sur la Figure 3.14, et nous allons décrire ici son instanciation. Sur chaque figure, l'étape correspondante du scénario sera précisée (à gauche de la capture d'écran).

Cette première phase démarre sur une infection de plusieurs postes par WannaCry. Durant la simulation, certains postes effectueront des actions programmées comme des téléchargements ou des sauvegardes ; ces actions devront être analysées par les utilisateurs et classées comme fausses alertes tandis que les infections liées à l'action de WannaCry devront être détectées et signalées. L'infection des assets ainsi que les téléchargements et

sauvegardes déclenchent des alertes concernant l'entropie des systèmes de fichiers et de débit réseau. Ces alertes apparaissent sur l'interface 2D du coordinateur (Figure 5.1).

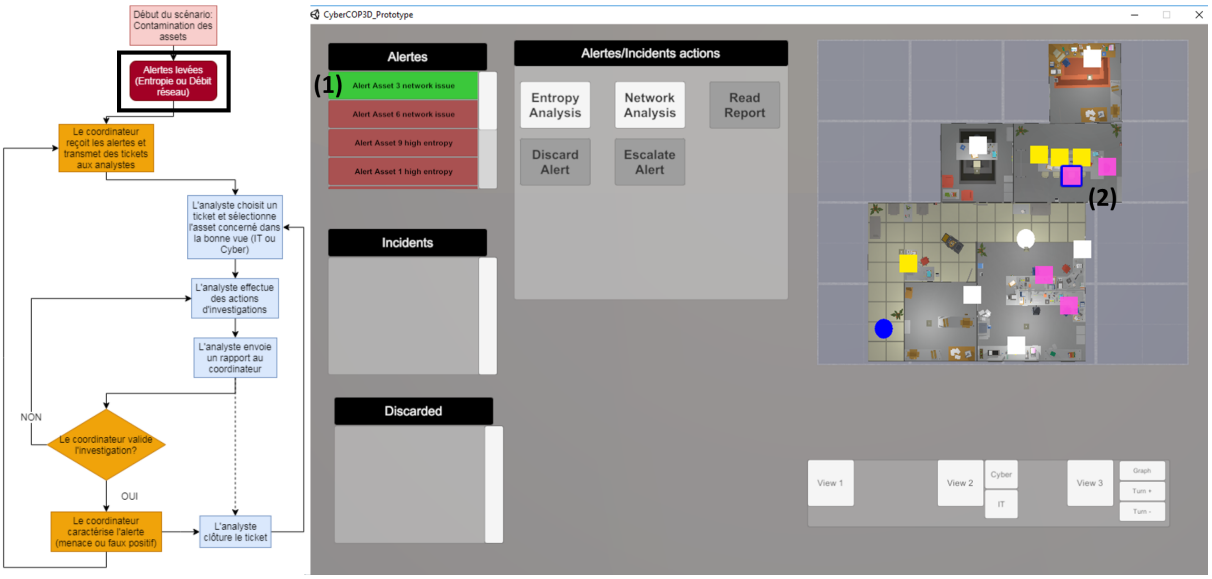


FIGURE 5.1 – (1) Sélection d'une alerte sur la vue coordinateur. Sur la minicarte, l'asset concerné par l'alerte est encadré de bleu (2) et les couleurs rose et jaune représentent respectivement les alertes Cyber et IT.

Le coordinateur peut alors les sélectionner et demander une analyse de l'entropie ou du débit réseau, en fonction du type d'alerte (Figure 5.2, en haut). Le coordinateur peut se tromper ici dans sa demande d'analyse, à savoir qu'il peut demander une analyse sur le niveau d'entropie d'un asset alors que l'alerte a été levée par rapport au débit réseau.

Cette action déclenche la création d'un ticket, que l'analyste doit sélectionner sur un tableau de bord dans l'environnement virtuel (Figure 5.2, en bas).

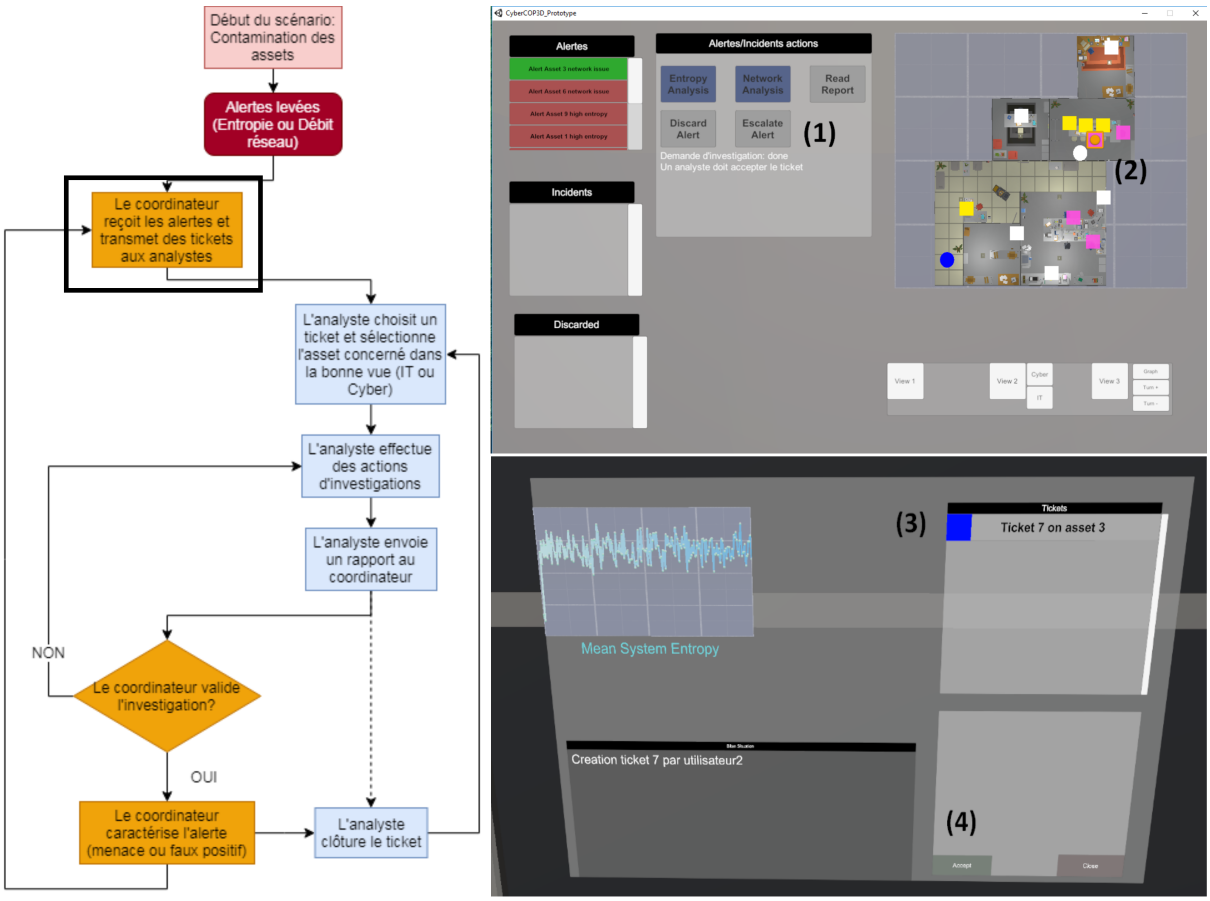


FIGURE 5.2 – Demande d'analyse par le coordinateur. Les boutons d'actions d'analyse changent de couleur (1) pour préciser que l'action de demande a été effectuée. Sur la minicarte, l'asset concerné par la demande d'analyse change de couleur (2). (3) Apparition d'une notification d'analyse sur le tableau de bord disponible dans l'environnement 3D. Un analyste doit alors le sélectionner et accepter le ticket, via un bouton en bas de l'interface (4).

Une fois les tickets créés, l'analyste en sélectionne un et accepte de le traiter. Il ne peut traiter qu'un ticket à la fois. Une notification est envoyée au coordinateur afin qu'il suive le déroulement de l'analyse (Figure 5.3).

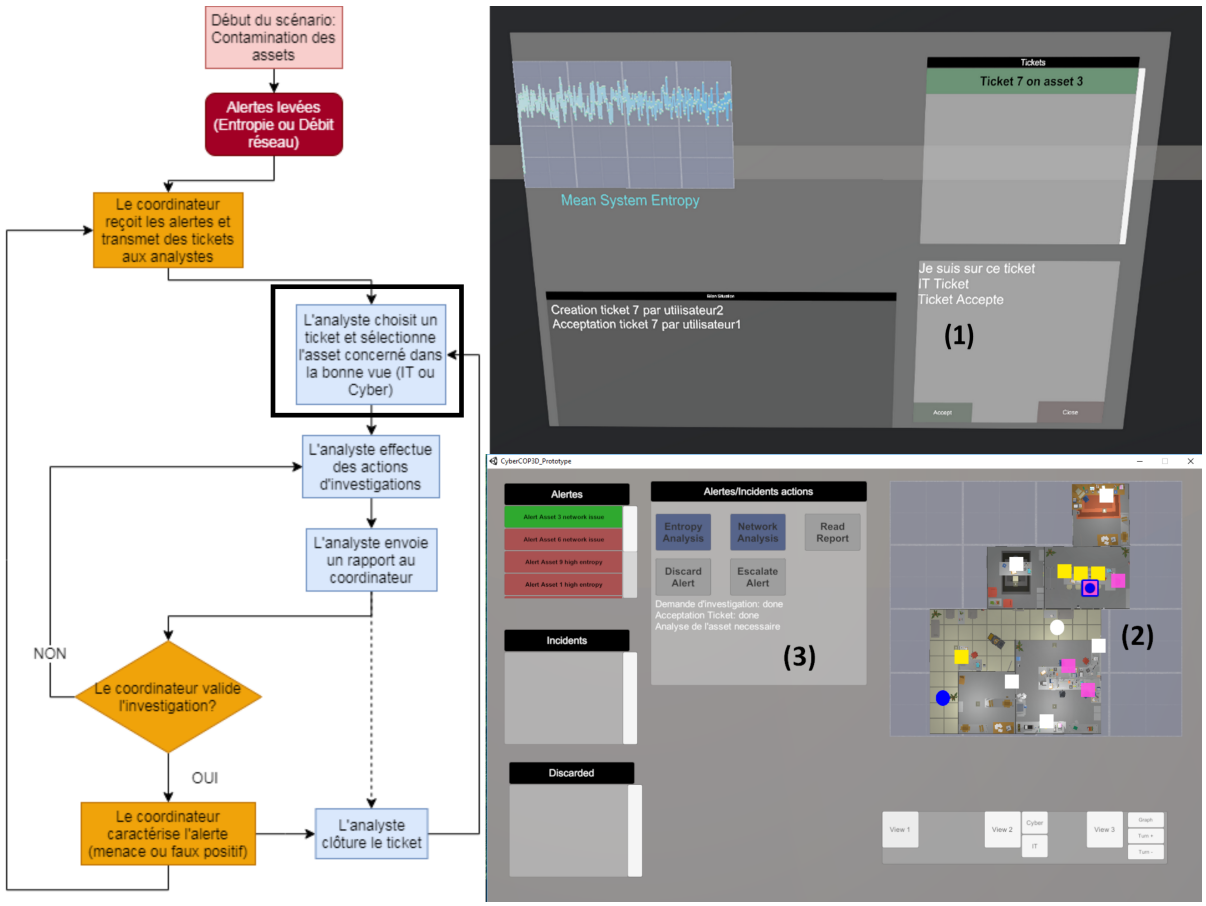


FIGURE 5.3 – (1) Acceptation du ticket par l'analyste et mise à jour de l'interface du coordinateur ((2) changement de couleur de l'asset concerné et (3) mise à jour des informations sur l'alerte).

L'asset concerné par le ticket est alors mis en évidence dans la vue correspondante (IT ou Cyber). L'analyste doit donc changer de vue afin de démarrer son investigation de l'asset (Figure 5.4). Nous avons choisi une mise en évidence via un système de particules, mais d'autres moyens visuels ou sonores peuvent s'appliquer.

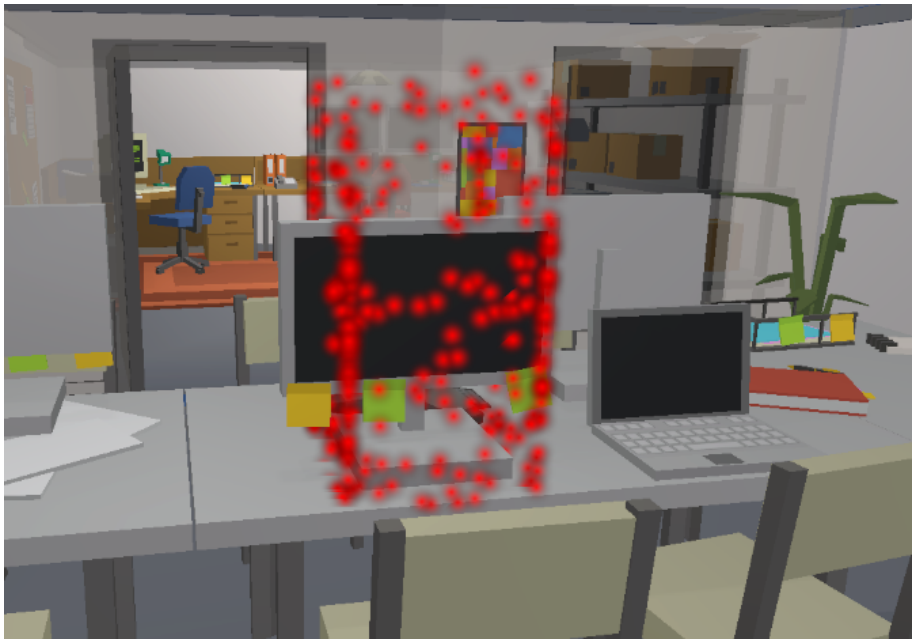


FIGURE 5.4 – Mise en évidence (par un système de particules) de l'asset concerné par le ticket de l'analyste.

L'investigation est effectuée en sélectionnant l'asset et en déclenchant des actions de récolte d'informations et d'analyse via un menu contextuel lié à l'asset. Seul l'asset concerné par le ticket peut être analysé, les boutons d'actions des autres assets étant désactivés (Figure 5.5). Nous avons fait ce choix pour faciliter l'interaction des analystes et guider l'exécution de la procédure.

La sélection de ces actions déclenche une notification sur l'interface du coordinateur, ce qui peut lui permettre de suivre les actions de l'analyste, indiquer à ce dernier l'asset concerné (grâce à la minicarte), voire lui demander de changer de vue (Figure 5.6).

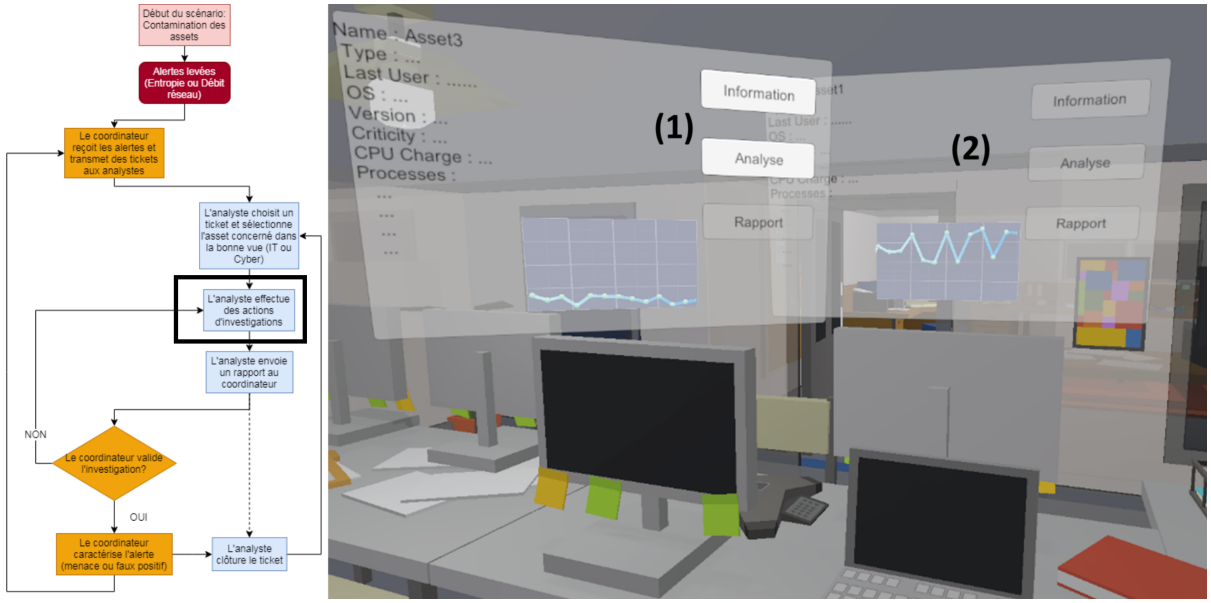


FIGURE 5.5 – (1) Menu contextuel de récupération d'informations sur l'asset concerné. (2) Les autres assets ne peuvent pas être analysés.

FIGURE 5.6 – (1) Notification sur l'alerte, représentée par un carré bleu. L'analyste, représenté par (2) le point blanc sur la minicarte est bien à côté de l'asset concerné par l'alerte.

Une fois l'analyse effectuée (analyse automatique donnant un score probable d'anomalie), l'analyste doit sélectionner le bouton 'Rapport' afin de transmettre son rapport d'analyse au coordinateur (Figure 5.7).

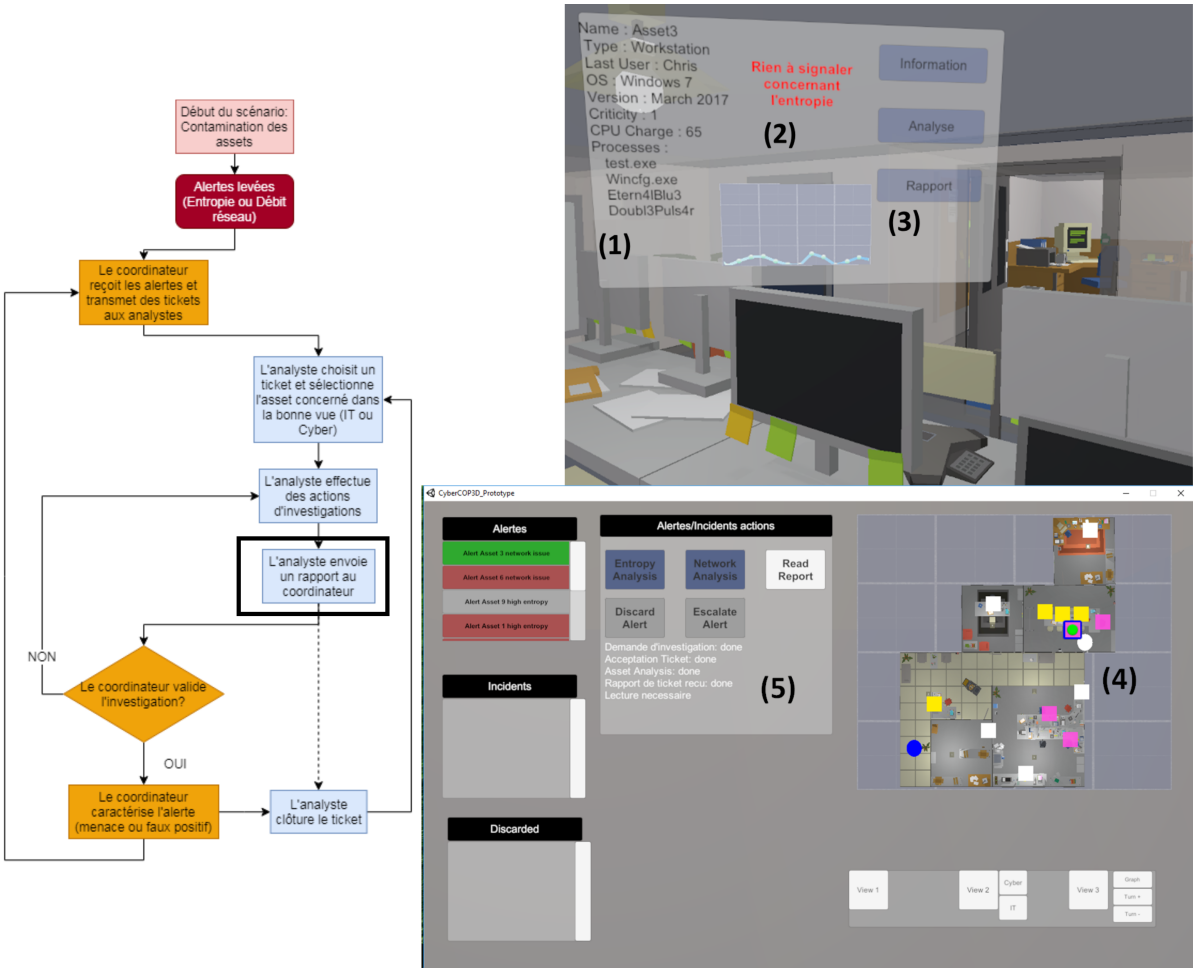


FIGURE 5.7 – (1) Récupération des informations, du (2) résultat d'analyse et (3) envoi du rapport par l'analyste. Réception du rapport par le coordinateur : (4) mise à jour de la minicarte (l'asset concerné change de couleur) et (5) des actions utilisateur (action de lecture de rapport activée.

Une fois que le coordinateur reçoit et lit le rapport de l'analyste, les actions de caractérisation d'alertes deviennent disponibles dans son interface. Il peut alors soit escalader l'alerte en incident (et donc considérer que l'alerte concerne un vrai problème), soit mettre de côté l'alerte (s'il considère qu'il s'agit d'une fausse alerte). Cette caractérisation a pour effet de créer un incident ou une fausse alerte dans sa vue (Figure 5.8).

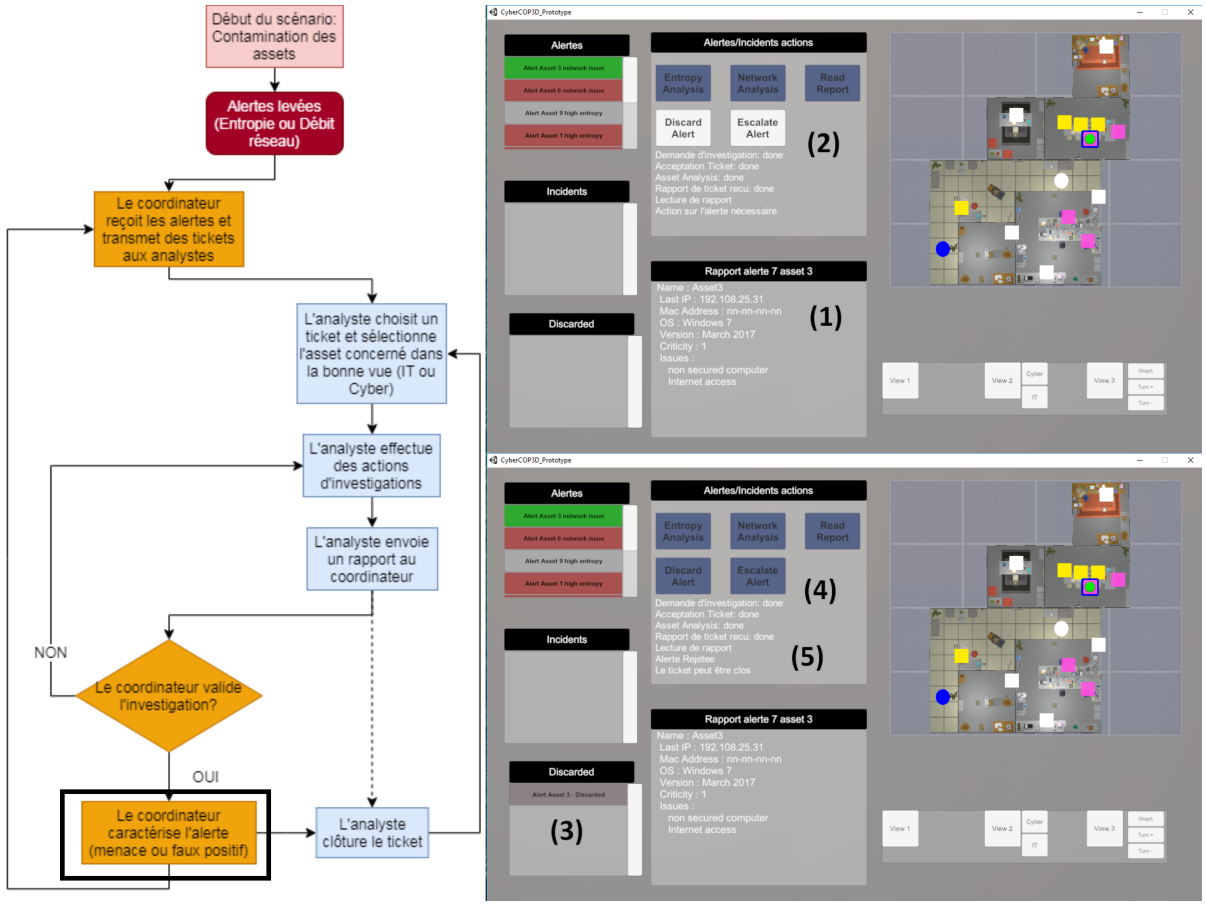


FIGURE 5.8 – (1) Lecture du rapport par le coordinateur (qui contient dans cet exemple les données de l'asset), ce qui active (2) les actions de caractérisation. Une fois l'alerte caractérisée, elle apparaît dans la liste des incidents ou des (3) faux positifs. (4) Les boutons d'actions de l'interface sont ensuite desactivés et (5) l'historique d'actions concernant le ticket est mis à jour.

Une fois la caractérisation effectuée par le coordinateur, l'analyste peut clôturer le ticket actuel et en sélectionner un autre (Figure 5.9).

Lorsque toutes les alertes ont été analysées et caractérisées, et que tous les tickets sont clos, la phase une du scénario prend fin.

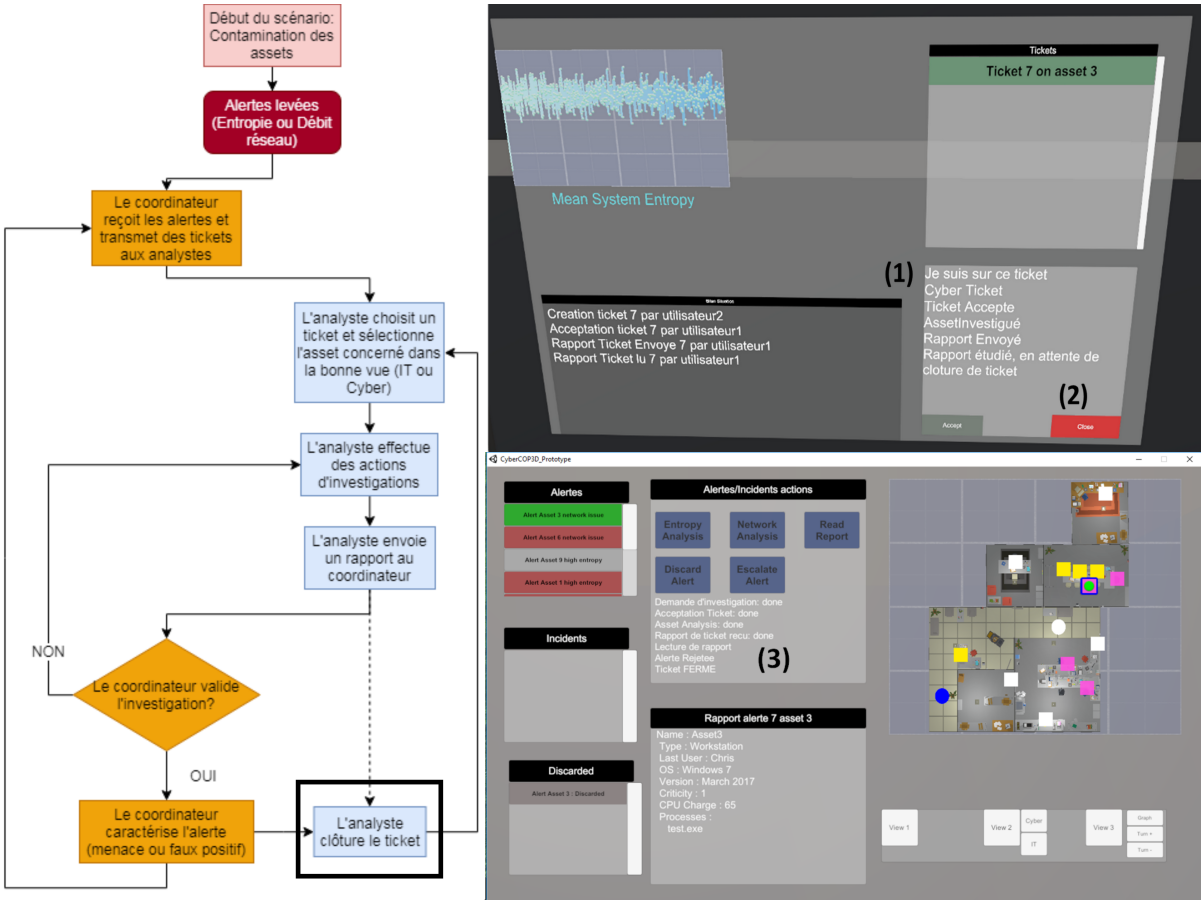


FIGURE 5.9 – (1) Mise à jour des informations du ticket sur le tableau de bord. L'analyste peut alors (2) fermer le ticket, ce qui (3) met à jour l'affichage du coordinateur.

Cette phase a été implémentée et testée avec succès lors de démonstrations et salons industriels. Pour faciliter l'exécution de cette phase, nous avons restreint l'interaction avec les assets qui ne sont pas concernés par des alertes et nous avons proposé des *feedbacks* visuels permettant de localiser les assets infectés (via un système de particules) ainsi que l'état d'avancement des analyses (sur la minicarte du coordinateur). Ces *feedbacks* découlent de choix de développement et peuvent être facilement modifiés en fonction des retours utilisateurs.

Le déroulement de la phase deux de notre scénario sera décrite dans la partie suivante.

5.1.2 Phase de corrélation d'alertes

Le déroulement de la phase de corrélation est décrit par le schéma 5.10. Cette phase a été développée d'après des retours d'experts sur l'importance de la corrélation d'informations lors de l'analyse d'alertes, mais elle n'a malheureusement pas pu être implémentée faute de temps et de retours utilisateurs.

La phase deux du scénario commence lorsque toutes les alertes et tickets sont traités par le coordinateur et l'analyste. Le coordinateur peut alors sélectionner plusieurs incidents (alertes escaladées) et demander à l'analyste de croiser les informations entre ces derniers via un ticket incident. L'objectif de cette phase est de définir si les incidents ont une origine commune ou s'ils sont indépendants.

L'analyste sélectionne le ticket incident, puis les assets correspondants. Cette sélection multiple lui permet d'accéder à une autre interface, qui lui permet à son tour de sélectionner les informations similaires entre les assets. Cette sélection d'informations peut être automatisée si l'utilisateur a besoin d'aide ou alors être effectuée manuellement (croisement d'informations de système d'exploitation, de processus etc...). Une interface de graphe 3D peut être proposée à l'analyste pour lui faciliter la tâche ; cette interface permet de mieux voir les liens entre différents assets.

Une fois que l'analyste a recueilli les informations qu'il juge nécessaires à la gestion des incidents, il transmet un rapport au coordinateur, contenant les liens de corrélation entre les incidents. Le coordinateur peut alors regrouper les incidents au sein d'un méta-incident si ceux-ci lui semblent liés (s'ils concernent des ordinateurs ayant le même système d'exploitation par exemple), ou tout simplement mettre à jour les informations des incidents. Le scénario se termine quand tous les incidents ont été soit regroupés soit inspectés.

Ces deux phases du scénario sont complémentaires et permettent à des utilisateurs soit de se pencher sur l'analyse d'alertes, soit sur la corrélation d'informations.

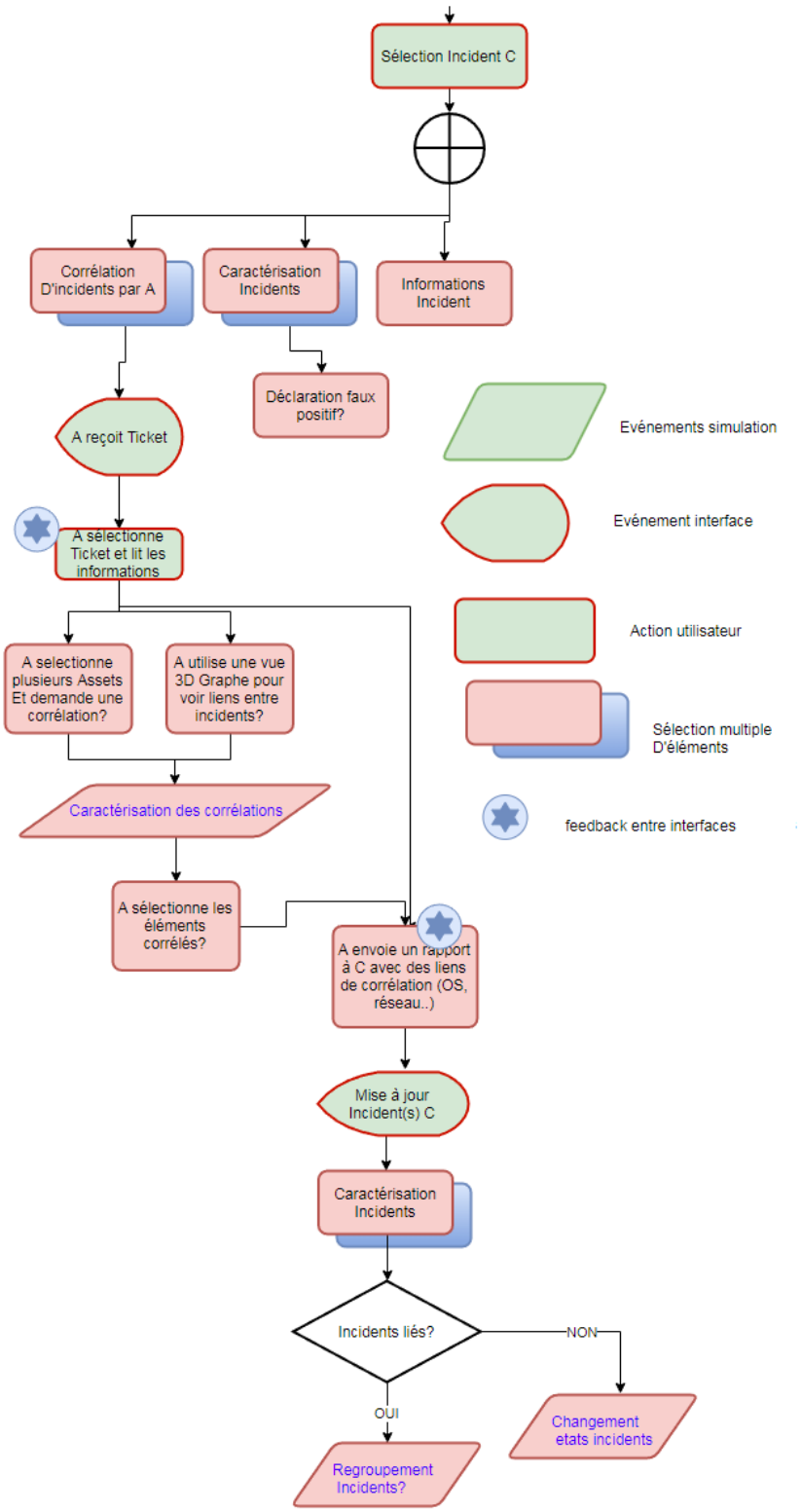


FIGURE 5.10 – Déroulement de la phase de corrélation d'alertes de notre scénario. L'objectif est de croiser les informations entre les alertes afin de déterminer si elles proviennent d'une même cause.

Bien que le scénario global ait été validé par nos partenaires industriels, nous nous sommes rendu compte que son déroulement était long et complexe, surtout pour des utilisateurs non familiarisés avec les Environnements Virtuels ou les tâches demandées. Le scénario, bien que linéaire et relativement simple, pouvait perdre l'utilisateur devant la masse d'informations et d'actions disponible. Une campagne de tests à la fois sur le scénario et sur les techniques d'interaction avait été proposée, mais nous n'avons pas pu accéder à assez d'experts pour proposer un protocole d'évaluation complet.

C'est pour cela que nous avons décidé d'effectuer une évaluation de l'utilisabilité d'un EV mono-utilisateur pour l'analyse d'alertes.

Scénario d'utilisation du CyberCOP 3D

Nous avons proposé un scénario collaboratif en deux phases, une phase d'analyse d'alertes et une phase de corrélation d'incidents. La phase d'analyse consiste à examiner les ordinateurs d'un réseau afin de déterminer s'ils sont infectés ou non par le rançongiciel WannaCry. La phase de corrélation, elle, consiste à croiser les informations de plusieurs alertes afin de déterminer si elles sont liées entre elles. Nous avons pu implémenter et tester la phase d'analyse mais pas la phase de corrélation. Un prototype fonctionnel de notre EVC a été présenté et testé, prototype dans lequel des utilisateurs peuvent réaliser la phase d'analyse d'alertes de notre scénario collaboratif.

5.2 Évaluation de l'utilisabilité du CyberCOP 3D

La cybersécurité étant un domaine sensible et les SOCs des environnements où les personnels analysent activement des alertes pouvant avoir des conséquences dramatiques, il n'est pas aisé de recruter des participants pour effectuer des expérimentations collaboratives. De plus, l'immersion dans un EV demande une phase d'adaptation et de familiarisation, et si les utilisateurs ne sont pas à l'aise avec les dispositifs immersifs cela peut entraîner des biais d'évaluation.

C'est pour cela que nous avons décidé dans un premier temps de mener une évaluation mono-utilisateur de l'utilisabilité d'un EV pour la cybersécurité. Ce type d'évaluation permet de juger un système dans son ensemble afin de déterminer s'il peut être utilisé correctement par des utilisateurs. L'avantage de l'évaluation de l'utilisabilité est qu'elle est simple à mettre en place (l'analyse se fait entre autres via des questionnaires utilisateurs comme le *System Usability Scale* (SUS) [12]) et qu'elle peut servir de support à des évaluations comparatives entre plusieurs solutions jugées utilisables. Par exemple, à l'issue d'une évaluation de l'utilisabilité d'une interface, nous pouvons proposer une évaluation comparée de différentes versions de cette interface.

Pour effectuer cette évaluation, nous avons du simplifier notre scénario d'utilisation afin que notre EVC soit utilisable par des utilisateurs non-experts en cybersécurité et nous avons proposé un protocole d'évaluation permettant de comparer différents types d'environnements virtuels.

5.2.1 Simplification du scénario

Le prototype d'Environnement Virtuel Collaboratif (EVC) que nous avons développé pour implémenter notre modèle CyberCOP 3D contient de nombreuses fonctionnalités telles qu'une gestion de la collaboration entre utilisateurs, des interfaces 2D et 3D immersives, des *feedbacks* d'interactions et plusieurs vues sur l'environnement.

Nous nous sommes rendu compte après des tests pilotes que ces fonctionnalités nécessitaient une prise en main relativement longue qui impactait la réalisation du scénario collaboratif. De plus, il n'a pas été possible d'effectuer des expérimentations auprès des personnels des SOCs.

Nous avons donc décidé à la fois de simplifier le scénario d'utilisation et de limiter les fonctionnalités présentes dans notre EVC afin de proposer un protocole d'évaluation qui soit accessible aux utilisateurs non familiarisés avec la cybersécurité ou la Réalité Virtuelle.

Nous nous sommes focalisés sur la procédure d'analyse d'alertes, à savoir la phase une de notre scénario présenté précédemment.

Notre scénario a donc été transformé pour être réalisable par un utilisateur seul, qui endosse le rôle d'analyste. Les actions à effectuer ont été limitées à la sélection et la caractérisation des alertes, via une investigation d'assets soit infectés par WannaCry soit effectuant des actions déclenchant des faux positifs.

L'utilisateur, immergé dans un EV, dispose de trois vues pour réaliser la tâche d'analyse : une vue IT, une vue Cyber et une vue Alerte. Contrairement aux deux premières qui sont présentes dans notre modèle CyberCOP 3D, la vue Alerte (Figure 5.11) a dû être rajoutée. Cette vue additionnelle permet d'obtenir les informations et d'agir sur les alertes, pour remplacer le système de *ticketing*, non nécessaire à une application mono-utilisateur.

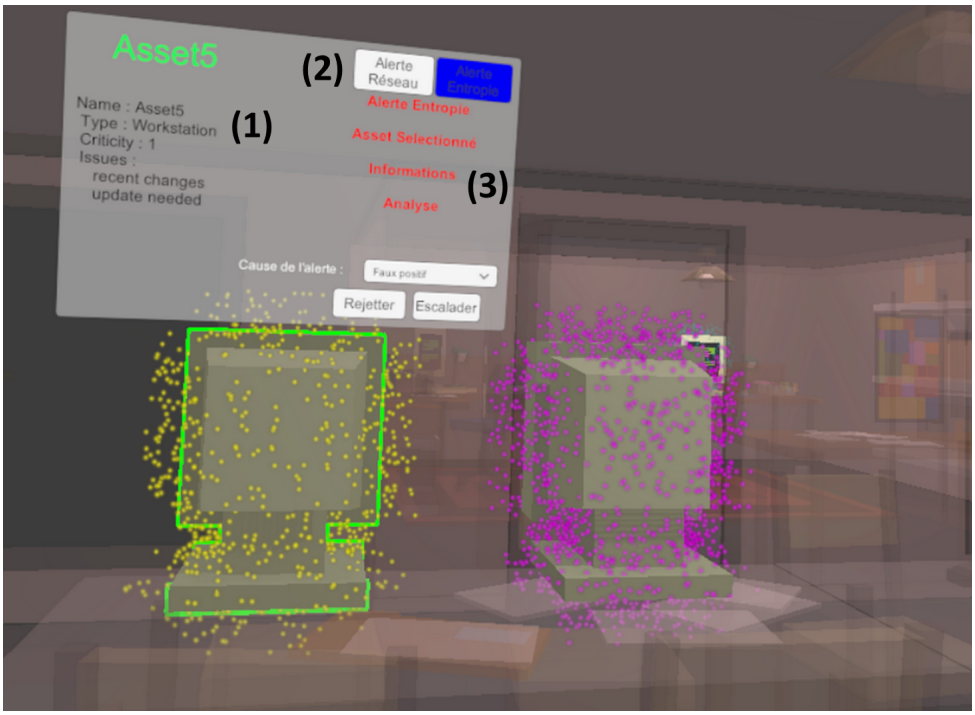


FIGURE 5.11 – Vue alerte qui remplace le système de *ticketing*. Cette vue contient (1) des informations sur l'asset et sur (2) les alertes le concernant. Le texte rouge (3) correspond à l'historique d'actions déjà effectuées sur l'alerte sélectionnée, en l'occurrence l'alerte entropie.

La sélection d'alertes s'effectue dans la vue alerte, et l'utilisateur doit ensuite basculer dans la vue IT ou la vue Cyber afin de poursuivre son investigation. Dans la vue correspondant à l'alerte (vue IT pour alerte entropie et vue Cyber pour alerte réseau), l'utilisateur peut récupérer les informations de l'asset et effectuer une analyse automatique d'anomalies (Figure 5.12). Enfin, pour caractériser l'alerte, il devra alors retourner dans la vue alerte.

Les indices d'infection par WannaCry sont disponibles sous la forme de processus ou de *threads* tournant sur les machines : "WannaCypt0r.exe", "Etern4lBlue" et "DoublePuls4r". Des indices concernant les faux positifs sont sous la même forme ("cryptor.exe, backuploaded.exe), et une analyse automatique est fournie à l'utilisateur afin de l'aider dans sa caractérisation. L'analyse automatique d'anomalies sur les assets donne un pourcentage d'anomalie, sous forme de probabilité d'infection de l'ordinateur. Nous avons fait en sorte que cette valeur soit supérieure ou égale à 50% si l'asset est infecté. Le scénario proposé est représenté sur la Figure 5.13.

Ce scénario d'évaluation dure une quinzaine de minutes et ne nécessite pas de connaissances préalables en cybersécurité. Une scène d'entraînement a aussi été développée, afin de permettre aux utilisateurs de se familiariser avec les dispositifs immersifs (en l'occurence, un casque de réalité virtuelle Oculus CV1).

Notre protocole d'évaluation sera présenté dans la section suivante.

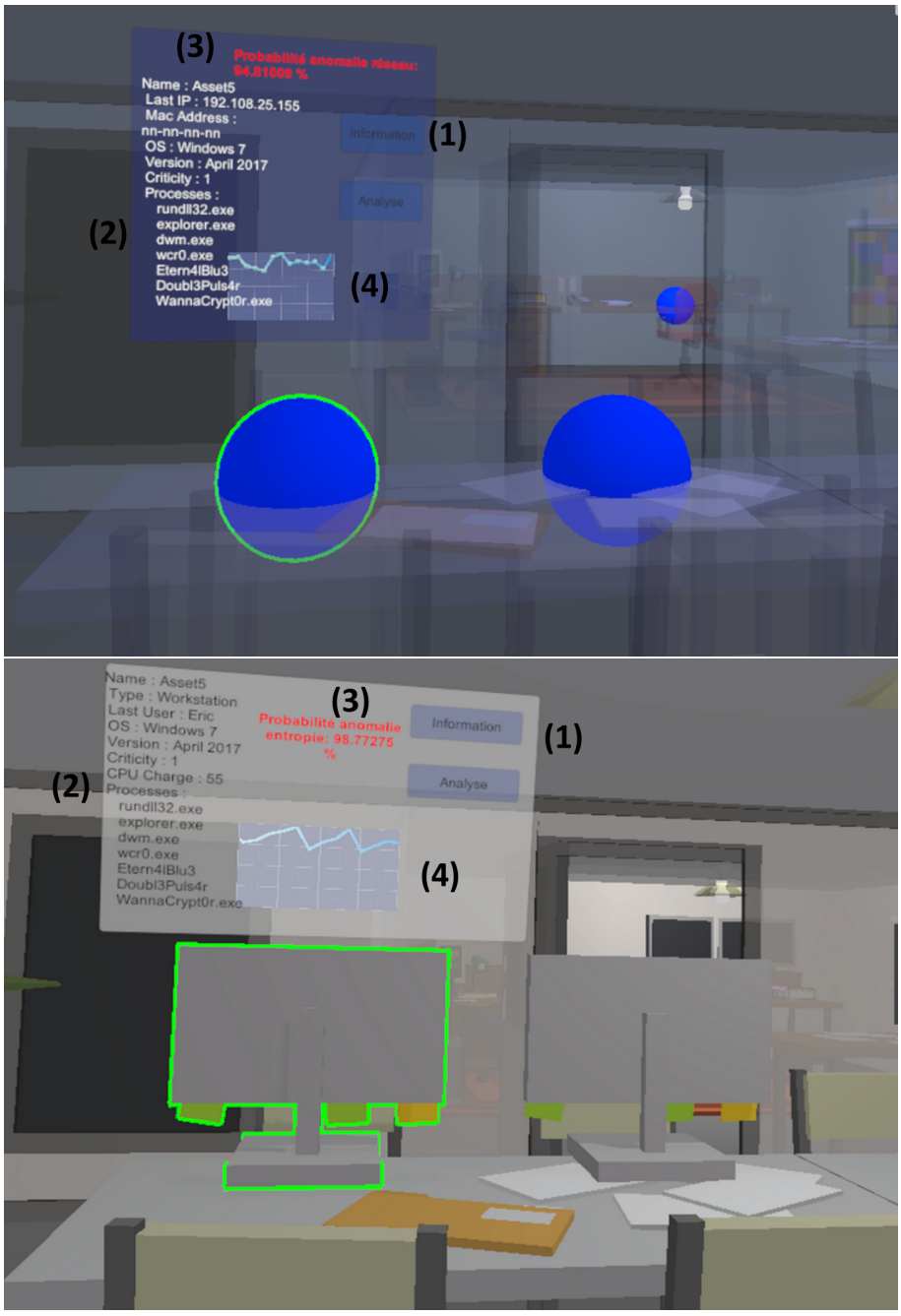


FIGURE 5.12 – Vue Cyber (en haut) et vue IT (en bas). Ces vues contiennent (1) les actions d'analyse, (2) des informations relatives à l'asset, (3) le résultat de l'analyse d'anomalies et (4) une visualisation des métriques d'entropie et de débit réseau, en fonction des vues.

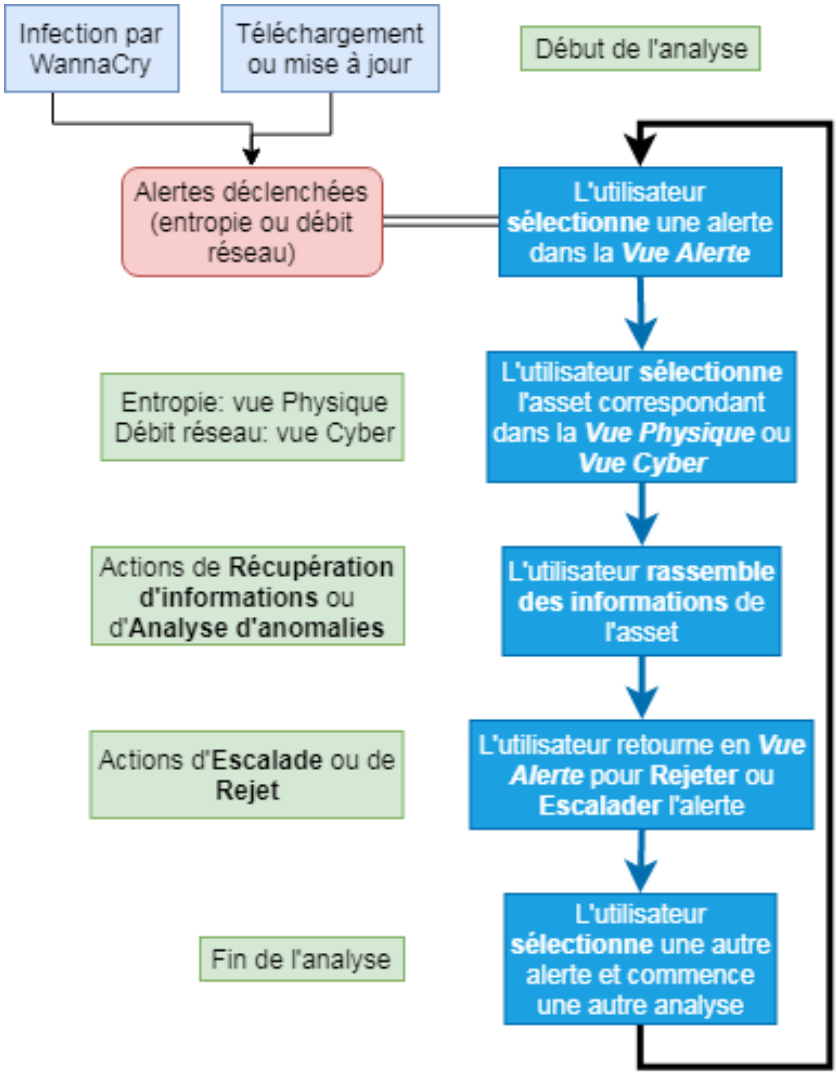


FIGURE 5.13 – Scénario simplifié pour notre étude de l'utilisabilité d'un environnement virtuel pour l'analyse d'alertes. Dans ce scénario, l'analyste agit seul pour étudier les alertes et les caractériser.

5.2.2 Protocole d'évaluation

Notre évaluation de l'utilisabilité d'un EV pour la cybersécurité s'appuie sur la réalisation d'un scénario d'analyse d'alertes. Nous avons souhaité comparer l'utilisabilité de trois types d'environnements différents (Figure 5.14) :

— Un environnement réaliste (concret) où les assets sont situés dans des locaux d'entreprise. Ces environnements sont utilisés dans le cadre de formations, mais peu présents en cybersécurité.

— Un environnement abstrait représentant les données sous forme de graphe 3D dont les liens correspondent à la topologie réseau. Ce type d'environnement est de plus en plus utilisé en *Immersive Analytics*.

— Un environnement mixte mêlant à la fois une visualisation abstraite sous forme de graphe et la représentation 'bureautique' concrète. Cet environnement va à l'encontre de notre approche de séparation des données en plusieurs vues, mais nous avons décidé de l'évaluer afin de voir s'il pouvait être considéré comme utilisable.

Notre objectif était de faire effectuer des tâches similaires aux utilisateurs dans ces trois environnements et d'évaluer leurs préférences. Afin de limiter l'effet d'apprentissage entre les trois réalisations, nous avons alterné l'ordre des deux premiers environnements testés, à savoir l'environnement concret et l'environnement abstrait. Les utilisateurs ont donc effectué les expérimentations dans la condition Concret-Abstrait-Mixte (CAM) ou dans la condition Abstrait-Concret-Mixte(ACM).

Nous pensions que les utilisateurs trouveraient l'environnement concret plus ludique mais qu'ils seraient également plus performants dans l'environnement abstrait tandis que l'environnement mixte serait jugé trop complexe. Nous avions défini trois scénarios présentant des similarités afin que les tâches soient différentes dans chaque environnement pour éviter un effet d'apprentissage. Ces scénarios contenaient les mêmes assets infectés mais positionnés différemment dans les environnements. Pour chaque scénario, les utilisateurs devaient caractériser onze alertes, dont deux faux positifs.

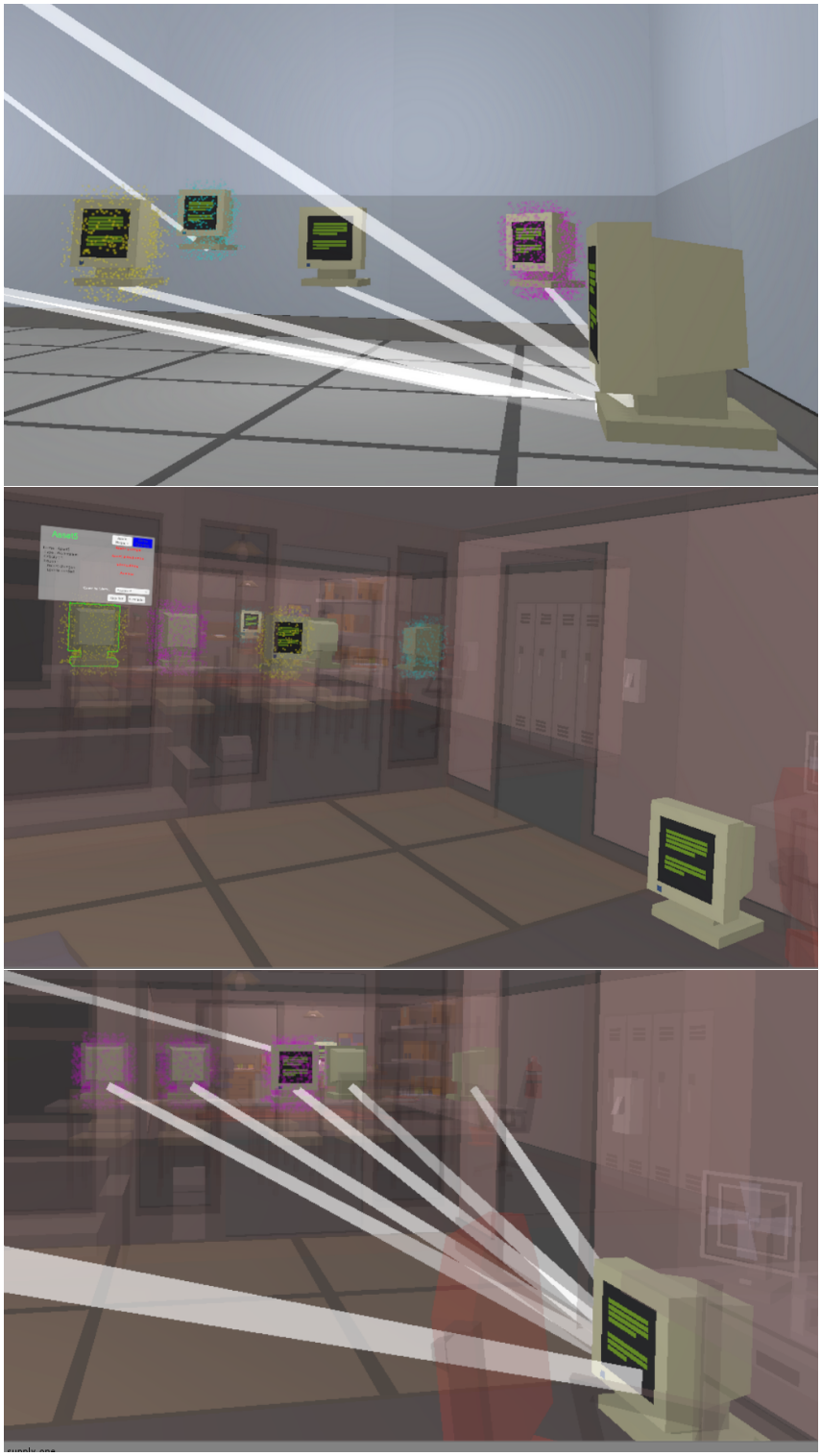


FIGURE 5.14 – Environnements Abstrait, Concret et Mixte proposés aux utilisateurs lors de l'évaluation de l'utilisabilité.

TABLE 5.1 – Protocole expérimental de notre évaluation de l'utilisabilité.

Déroulé	**Durée (mn)**
Accueil et signature consentement	15
Scène tutoriel	10
Scène d'expérience en réalité virtuelle : trois fois	10 x 3
Questionnaire utilisabilité et Cyber Situational Awareness : trois fois	5 x 3
Questionnaire final	5
Questionnaire Expérience Utilisateur	5

L'expérimentation durait un peu plus d'une heure. Nous fournissions une fiche de consentement expliquant les objectifs de notre étude, ainsi que les conditions de traitement et stockage des données.

Les utilisateurs effectuaient ensuite une session d'entraînement en environnement virtuel d'une quinzaine de minutes où ils apprenaient à se déplacer et interagir. Puis, une fois le tutoriel terminé et qu'ils se sentaient prêts, ils commençaient l'expérimentation soit par l'environnement concret, soit par l'environnement abstrait (conditions CAM ou ACM).

La session d'entraînement s'effectuait dans le même environnement que la première expérimentation (abstrait ou concret), pour faciliter cette dernière.

À l'issue de la première session, les utilisateurs devaient remplir un questionnaire d'utilisabilité tiré d'une traduction du *System Usability Scale* (SUS) [12], ainsi que des questions concernant leurs analyses. Le questionnaire SUS nous a permis d'établir un score d'utilisabilité tandis que les questions sur les analyses nous ont permis de caractériser leur compréhension de l'environnement et de la tâche.

Une fois le questionnaire rempli, les utilisateurs recommençaient l'analyse d'alertes dans les environnements virtuels restants et répondaient aux questionnaires entre chaque session. Une fois le troisième questionnaire rempli, ils devaient alors remplir un questionnaire synthétique sur les trois environnements, et un autre concernant l'adoption de la technologie immersive et le ressenti physiologique, inspiré quant à lui par les travaux de Katy Tcha-Tokey [121].

La fiche de consentement présentée aux utilisateurs sera présentée dans les annexes. La table 5.1 présente notre protocole d'évaluation.

Simplification du scénario et protocole d'évaluation

Afin d'effectuer une évaluation de l'utilisabilité de notre implémentation du modèle CyberCOP 3D avec des utilisateurs non familiarisés avec la cybersécurité et la Réalité Virtuelle, nous avons proposé un scénario simplifié réalisable par un seul utilisateur en une quinzaine de minutes. Notre protocole consistait à réaliser un scénario d'analyse d'alertes dans trois environnements différents, un environnement concret, un environnement abstrait et un environnement couplant les représentations concrètes et abstraites. L'objectif était d'évaluer l'utilisabilité de ces environnements. Entre les analyses, les utilisateurs devaient remplir des questionnaires d'utilisabilité SUS ainsi que des questions relatives à la tâche d'analyse. Une scène d'entraînement était fournie au début de l'expérimentation et un questionnaire final concernant la préférence entre les interfaces, l'adoption de la technologie et le ressenti physiologique clôturait l'évaluation.

5.3 Résultats de l'évaluation

Nous avons effectué notre expérimentation durant un mois et recueilli les résultats de trente utilisateurs, pour la plupart étudiants en informatique. Les utilisateurs étaient pour la plupart non familiarisés avec les technologies immersives et la cybersécurité, mais familiarisés avec les jeux vidéos.

La durée moyenne totale d'un passage était d'une heure et trente minutes, et tous les utilisateurs ont réussi les scénarios d'analyse.

Sur les Figures que nous allons présenter, la marge d'erreur provient de l'écart-type. Les valeurs de p données proviennent d'analyses de variance de type ANOVA à 95%.

5.3.1 Résultats utilisabilité et adoption

Les environnements abstrait, concret et mixte ont respectivement obtenu des scores d'utilisabilité SUS de 76.41, 72.42 et 77.33 sur 100 (Figure 5.15 à gauche), ce qui signifie qu'ils sont considérés comme utilisables (le seuil d'utilisabilité d'une interface est fixé à 70/100 pour le test SUS).

Il n'y a pas eu de différences significatives dans les scores d'utilisabilité des environnements entre les utilisateurs ayant commencé l'expérimentation par l'environnement abstrait (condition ACM) et les utilisateurs ayant commencé par l'environnement concret (condition CAM) (Figure 5.15). Les résultats des analyses de variance de type ANOVA à 95% entre les deux conditions et pour les environnements abstrait, concret et mixte donnent respectivement $p = 0.81$, $p = 0.71$ et $p = 0.69$.

Les utilisateurs ont préféré l'environnement mixte couplant vues abstraites et concrètes. Les conditions ACM et CAM de passage de l'expérimentation (à savoir débuter par l'environnement abstrait ou concret) n'ont pas eu d'effet sur les préférences utilisateurs. Contrairement à ce que nous pensions, la complexité de cet environnement n'a pas été un facteur limitant pour la plupart des utilisateurs, mais le fait que ce dernier est été toujours exploré en troisième session a peut-être influencé leur choix (Figure 5.16).

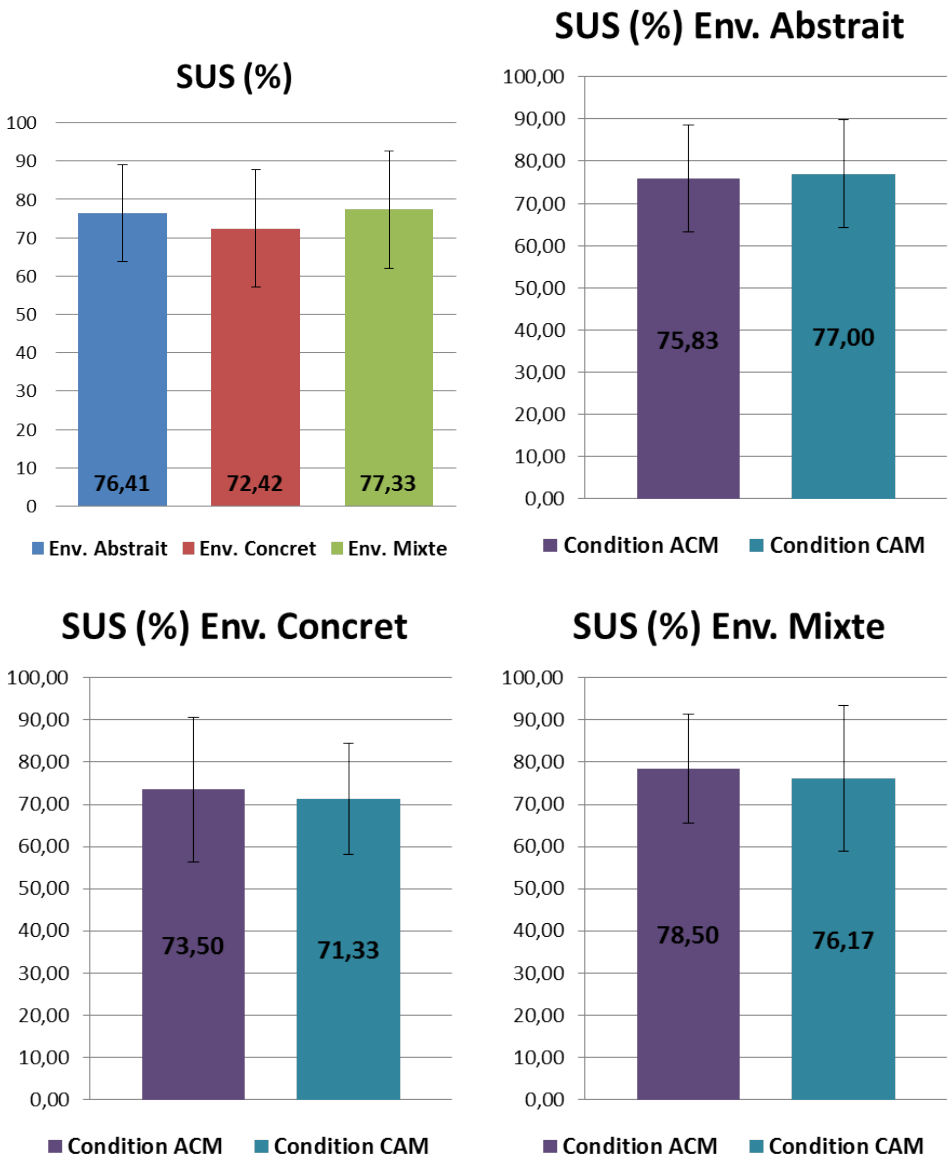


FIGURE 5.15 – Scores SUS pour les différents types d'environnements en moyenne et en fonction des conditions. Les scores sont supérieurs à 70/100 et il n'y a pas d'effets liés à la condition.

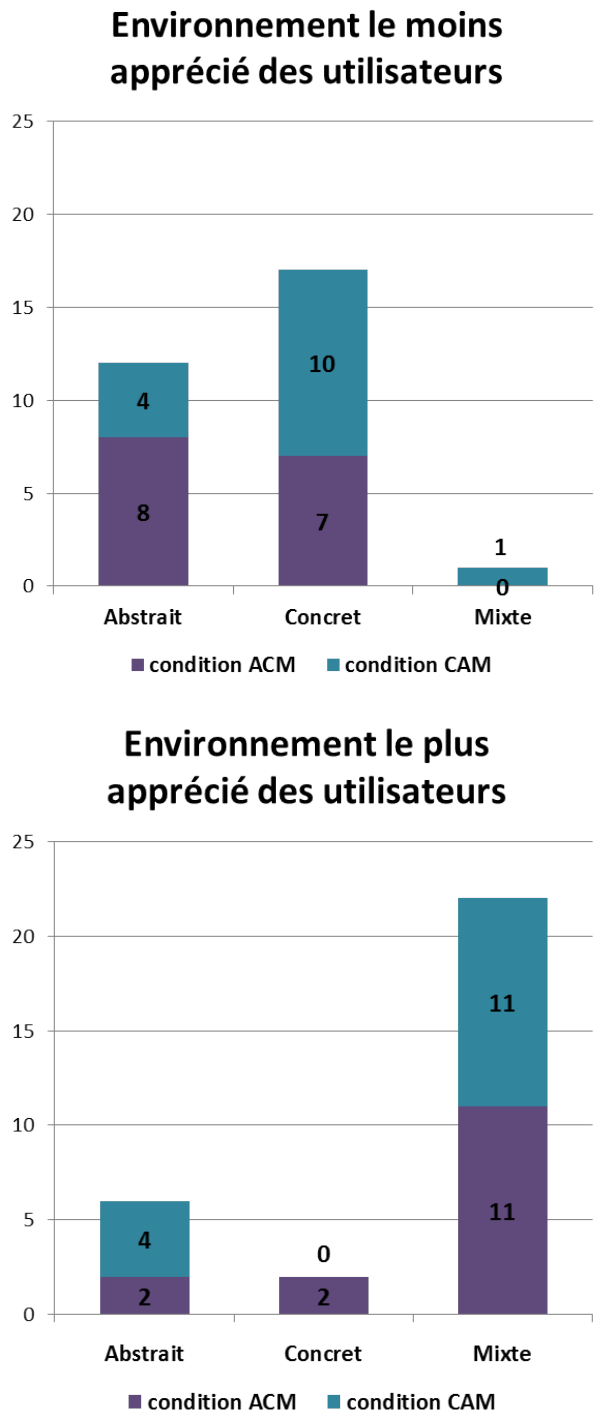


FIGURE 5.16 – Appréciations utilisateurs des différents environnements en fonction des conditions. L'environnement mixte fut préféré, sans effet de condition.

La moyenne des scores aux questions concernant les troubles physiologiques était de 2.9/10 : ce qui veut dire que les utilisateurs n'ont pas éprouvé de malaise durant les expérimentations, bien que nous ayons constaté que six utilisateurs (trois des cinq utilisateurs âgés de plus de trente-cinq ans, deux utilisateurs de moins de ving-cinq ans et un utilisateur entre ving-cinq et trente-cinq ans) ont eu un ressenti plus important que les autres.

Les utilisateurs ont considéré qu'ils pourraient acquérir aisément les compétences requises pour utiliser cet environnement virtuel (score moyen de 8/10), avec un effet significatif de l'âge (score moyen de 5.8/10 pour les plus de trente-cinq ans).

Les dispositifs immersifs ont été considérés comme agréables et potentiellement utilisables au travail. Les environnements et la technologie immersive ont dans l'ensemble été jugés pertinents, avec des scores aux questions concernant l'adoption des technologies et l'expérience utilisateur au dessus de 6 sur 10 (Figure 5.17).

Questions relatives à l'expérience utilisateur	Score moyen
1. Je me suis senti(e) fatigué(e) durant mon interaction avec l'environnement virtuel.	3,43/10
2. J'ai ressenti des maux de tête durant mon interaction avec l'environnement virtuel.	3,1/10
3. J'ai ressenti une fatigue visuelle durant mon interaction avec l'environnement virtuel.	4,03/10
4. J'ai eu des nausées dans l'environnement virtuel.	2,8/10
5. J'ai eu une impression de lourdeur dans la tête durant mon interaction avec l'environnement virtuel.	2,66/10
6. Je me suis senti(e) étourdi(e) lorsque j'ouvrais les yeux durant mon interaction avec l'environnement virtuel.	2,56/10
7. J'ai ressenti des vertiges durant mon interaction avec l'environnement virtuel.	2,43/10
8. Si j'utilise de nouveau le même environnement virtuel, mon interaction avec l'environnement sera claire et compréhensible pour moi.	8,56/10
9. J'arriverai aisément à acquérir les compétences requises pour utiliser cet environnement virtuel.	8,03/10
10. Utiliser ces périphériques d'interaction (casque Oculus, manette et/ou clavier) de réalité virtuelle est une mauvaise idée.	2,3/10
11. Les périphériques d'interaction (casque Oculus, manette et/ou clavier) de réalité virtuelle pourraient rendre mon travail plus intéressant.	6,83/10
12. J'aimerais bien utiliser ces périphériques d'interaction (casque Oculus, manette et/ou clavier) de réalité virtuelle dans mon travail.	7,1/10

FIGURE 5.17 – Score moyen des réponses aux questions concernant l'expérience utilisateur. Acceptation générale des interfaces immersives (questions 9,11 et 12) et peu d'impacts physiologiques (questions 1 à 7).

5.3.2 Effets sur la CSA et l'apprentissage

Un score d'analyse a été attribué aux utilisateurs en fonction de la justesse de leurs caractérisations d'alertes. un score de huit sur onze signifie par exemple qu'ils ont bien caractérisé huit alertes (faux positifs inclus) sur les onze présentes dans les scénarios.

Les utilisateurs ont en moyenne eu un score élevé durant les expérimentations (moyenne supérieure à 8.5/11) (Figure 5.18 à gauche). Nous avons constaté que le temps d'analyse d'alertes était sensiblement plus élevé dans l'environnement concret que dans les environnements abstraits et mixtes ($p = 4.10^{-4}$).

Les utilisateurs ont analysé plus rapidement les alertes dans l'environnement mixte, bien qu'il n'y ait pas de différences significatives des durées d'analyse entre les environnements abstraits et mixtes ($p = 0.1$). L'environnement mixte étant toujours exploré en dernier, l'adaptation à l'expérimentation ainsi qu'une familiarité avec la tâche peuvent expliquer ce résultat (Figure 5.18 au centre).

En revanche, nous n'avons pas constaté de différences concernant la distance parcourue dans les différents environnements ($p = 0.59$) (Figure 5.18 à droite).

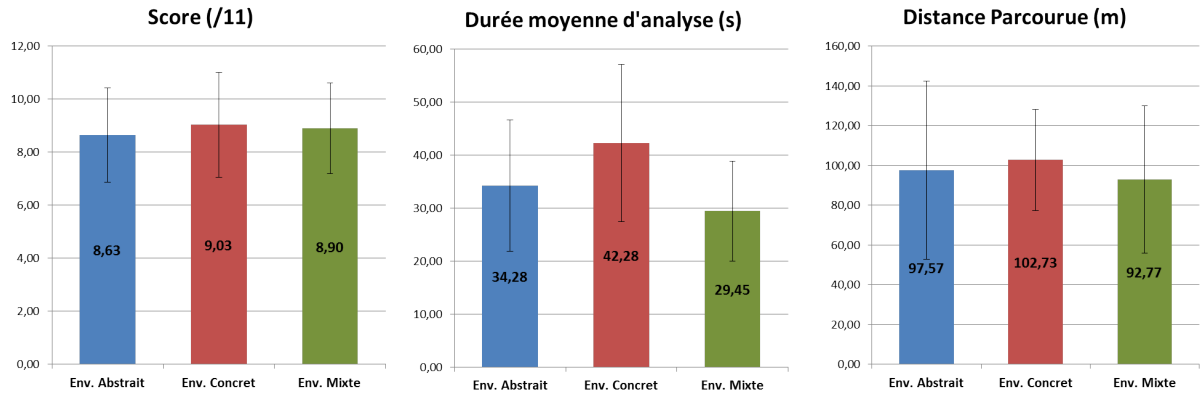


FIGURE 5.18 – Résultats des utilisateurs en fonction des interfaces. Les utilisateurs ont caractérisé de manière correcte huit alertes sur onze en moyenne, et ont passé moins de temps à analyser les alertes dans les environnements mixtes et abstraits que dans l'environnement concret. Peu de différences entre les environnements concernant les distances parcourues.

Bien que nous n'ayons pas constaté d'amélioration significative des scores ou des temps d'analyse durant les sessions successives, le nombre de données utilisées pour caractériser les alertes a évolué au cours du temps : les utilisateurs ont de plus en plus utilisé les données à leur disposition, avec une préférence pour la liste des processus et l'analyse automatique d'anomalies, qui étaient les sources de données les plus accessibles et qui donnaient des informations souvent catégoriques sur la présence de WannaCry (Figure 5.19).

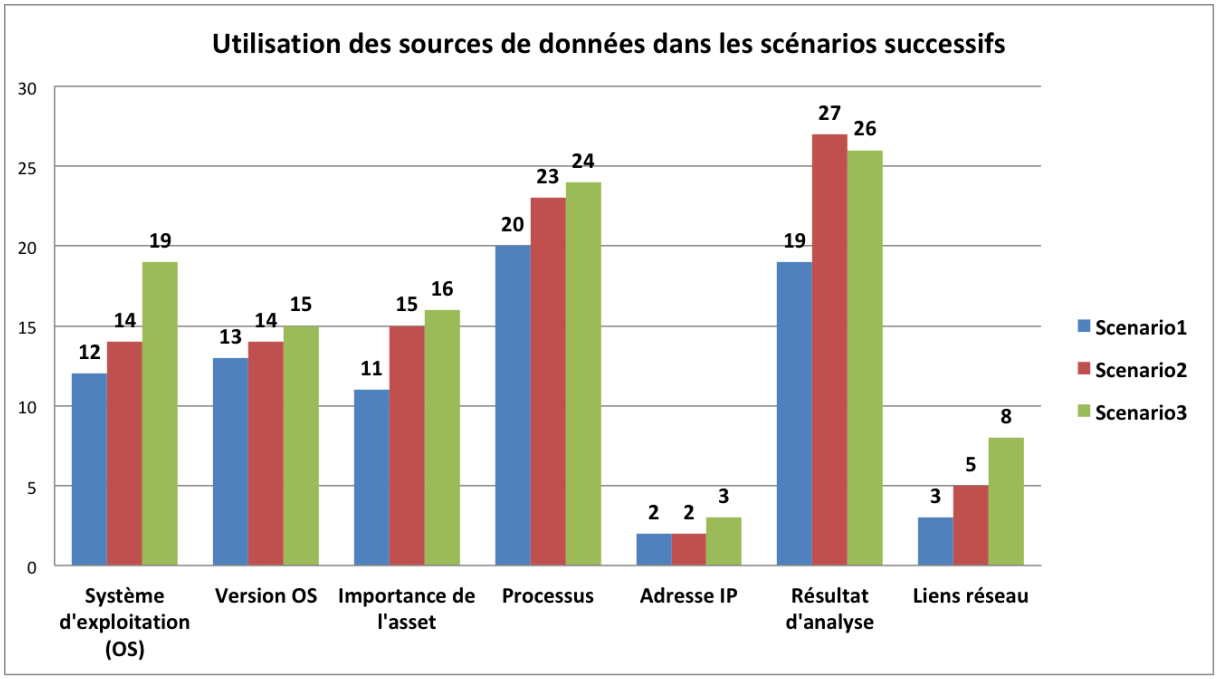


FIGURE 5.19 – Utilisation des données par les utilisateurs au fur et à mesure des expérimentations. Les utilisateurs ont de plus en plus utilisé les données à leur disposition (progression du nombre d'utilisations entre les scénarios 1 et 3) et ont utilisé en majorité les résultats d'analyse et la liste des processus pour caractériser les alertes.

Les réponses aux questions relatives à la tâche demandée n'ont pas beaucoup évolué entre les sessions, même si les utilisateurs ont considéré avoir mieux compris les alertes au fur et à mesure des expérimentations (Figure 5.20).

Questions relatives aux expérimentations successives	Score scénario 1	Score scénario 2	Score scénario 3
1. Je pense avoir compris ce qu'on attendait de moi	3,7/5	**4,2/5**	4,0/5
2. Je pense avoir compris les alertes	3,0/5	3,6/5	**3,8/5**
3. Je pense avoir répondu de manière pertinente aux alertes	2,9/5	**3,3/5**	**3,3/5**
4. J'ai éprouvé de la difficulté à naviguer entre les vues	1,8/5	**1,5/5**	1,7/5
5. Je pense que toutes les alertes provenaient d'une même attaque informatique	2,4/5	2,6/5	2,6/5
6. Je pense que les alertes étaient déclenchées par des événements indépendants	3,2/5	3,0/5	3,0/5
7. Les données des différentes vues étaient facilement accessibles	4,3/5	**4,5/5**	**4,5/5**
8. J'ai trouvé la situation crédible	4,1/5	4,0/5	**4,2/5**
9. J'ai ressenti un malaise physiologique lors de l'expérimentation	**1,9/5**	**1,7/5**	**1,9/5**
10. Je pense que cette interface est pertinente pour une utilisation par des experts en cybersecurité	3,9/5	4/5	**4,1/5**

FIGURE 5.20 – Score moyen des réponses des utilisateurs aux questions concernant les tâches d'analyse successives. Les utilisateurs n'ont en moyenne pas trop ressenti de malaise physiologique (Q.9), ont trouvé que les données étaient accessibles (Q.7) et qu'ils avaient compris les alertes (Q.2).

Nous n'avons pas constaté d'effet des familiarités ou de l'âge sur la réalisation des différentes sessions et sur la compréhension des situations. Les effets observés semblent être dus au faible nombre d'utilisateurs dans les différentes catégories.

5.3.3 Remarques qualitatives et/ou limites de l'étude

Durant les expérimentations, nous avons pris des notes concernant la réalisation des tâches par les utilisateurs ainsi que leurs remarques éventuelles.

Nous nous sommes rendu compte durant les expérimentations que si les résultats d'analyse d'anomalie étaient proches de 50%, les utilisateurs doutaient de la présence de WannaCry, bien que "WannaCrypt0r.exe" fût visible dans la liste des processus si l'asset était infecté.

De la même manière, nous nous sommes aperçus que nos interfaces graphiques n'affichaient que les six premiers processus des ordinateurs, et donc que les informations disponibles étaient parfois incomplètes, ce qui troublait les utilisateurs (Figure 5.21).

FIGURE 5.21 – Liste incomplète des processus tournant sur un asset (à gauche) et liste complète (à droite).

L'incomplétude des données n'était cependant pas détectée, les utilisateurs pensant simplement que certains processus ne se retrouvaient pas sur toutes les machines.

Aucun utilisateur n'a remarqué que les assets étaient les mêmes entre les scénarios et que seules leurs positions dans l'espace changeait. Par exemple, l'asset numéro 10 contenait toujours une fausse alerte mais n'était jamais au même endroit.

Des utilisateurs ont fait remarquer que bien que la navigation entre les vues fut aisée, une interface 2D contenant des informations sur les alertes aurait pu être proposée dans l'environnement virtuel. De la même manière, une interface d'aide nous a été suggérée, les utilisateurs étant souvent perdus durant la première session d'expérimentation.

Certains utilisateurs ont noté que les données n'étaient pas sensiblement différentes entre les vues, ce qui pourra à l'avenir être corrigé.

Beaucoup d'utilisateurs n'ont pas traité les alertes une par une mais en ont sélectionné

plusieurs afin de corréler des informations. Le fait que les assets soient parfois regroupés dans une même salle a facilité cette corrélation, dans les environnements concret, abstrait ou mixte.

Résultat de l'expérimentation

Nous avons effectué notre évaluation auprès de trente sujets, principalement étudiants en informatique. Les scores d'utilisabilité des environnements ont été supérieurs à 70/100, ces derniers sont donc considérés comme utilisables. Les utilisateurs ont préféré l'environnement couplant vues concrète et abstraite des données et ont moins apprécié l'environnement concret, contrairement à nos attentes. La sensation de malaise physiologique ressentie durant l'exploration des EV a été peu ressentie, dans l'ensemble les utilisateurs ont apprécié leur expérience. Les utilisateurs ont bien caractérisé plus de huit alertes sur les onze proposées dans les scénarios, et nous avons noté une progression des utilisateurs durant les différentes sessions. Les utilisateurs ont pour la plupart traité plusieurs alertes à la fois contrairement à nos attentes.

5.4 Conclusion sur l'instanciation et l'évaluation du CyberCOP 3D

Nous avons développé un prototype d'Environnement Virtuel Collaboratif (EVC) basé sur notre modèle CyberCOP 3D et sur un scénario d'analyse collaborative du rançongiciel WannaCry. Cet EVC a été présenté à nos partenaires industriels durant divers événements. Ils ont apprécié ses fonctionnalités mais nous n'avons malheureusement pas pu le faire tester à un panel suffisant d'experts en cybersécurité afin d'effectuer des évaluations collaboratives. De plus, la phase de corrélation de notre scénario n'a pas pu être implémentée, faute de temps et de retours utilisateurs sur la première phase du scénario.

Nous avons donc développé une version mono-utilisateur de notre environnement et de notre scénario afin d'effectuer une analyse de l'utilisabilité auprès d'utilisateurs non familiarisés avec la cybersécurité ou les interfaces immersives. Les utilisateurs devaient analyser onze alertes dans trois environnements virtuels différents, à savoir un environnement abstrait représentant les données sous forme de graphe 3D, un environnement bureautique concret et un environnement mixte, couplant les deux précédents.

Les utilisateurs ont considéré l'environnement mixte comme le plus utilisable (même si les trois environnements ont eu un score d'utilisabilité supérieur à 70/100), et ils ont bien caractérisé en moyenne huit alertes sur les onze.

D'autres évaluations sont à prévoir, notamment une comparaison 2D/3D, une évaluation de la collaboration (si possible avec des utilisateurs ayant déjà effectué l'expérimentation sur l'utilisabilité), et une évaluation avec des utilisateurs experts en cybersécurité.

Conclusion et perspectives

Conclusion

L'objectif de cette thèse était d'étudier les utilisations potentielles d'Environnements Virtuels Collaboratifs (EVC) pour l'analyse de l'état de sécurité d'un système informatique. Cette analyse, appelée aussi la *Cyber Situational Awareness* (CSA), peut se faire en utilisant des outils d'analyses de données ou des outils d'entraînement à des situations de cybersécurité.

Durant notre étude des modèles et outils pour la CSA, nous avons constaté que la collaboration est souvent mise de côté car difficile à caractériser et évaluer, et qu'il n'existe que peu d'outils immersifs permettant d'acquérir cette CSA, tandis que dans d'autres domaines, les dispositifs de Réalité Virtuelle sont de plus en plus utilisés pour analyser des données ou pour faciliter l'apprentissage de compétences.

Nous soutenons que l'utilisation d'EVC pour la cybersécurité est pertinente car ces derniers peuvent participer à l'acquisition de la CSA via des environnements de visualisation de données ou des environnements d'entraînement, et donc être utilisés pour analyser l'état de sécurité des systèmes informatiques.

De plus, les possibilités techniques offertes par les ordinateurs actuels nous permettent de développer des environnements dits de *Collaborative Immersive Analytics*, capables d'afficher énormément de données ou d'immerger plusieurs utilisateurs dans des environnements réalistes.

Afin de mieux comprendre les pratiques collaboratives en cybersécurité et les besoins des analystes, nous avons proposé un protocole d'analyse de l'activité collaborative au sein des Security Operations Centers (SOCs), centres de surveillance en continu de réseaux d'entreprises, de nos partenaires industriels. Bien que notre analyse se soit retrouvée bloquée par l'irruption du rançongiciel WannaCry en mai 2017, nous avons pu proposer un modèle de l'activité, le CyberCOP 3D, pouvant être implémenté dans un EVC afin de permettre à des utilisateurs d'analyser l'état de sécurité d'un réseau. Nous nous sommes inspirés du rançongiciel WannaCry pour proposer un scénario d'utilisation d'analyse d'alertes prenant en compte les fonctionnalités de notre modèle.

En nous basant sur notre modèle CyberCOP 3D, nous avons proposé une architecture événementielle permettant de bâtir des EVC pour l'analyse collaborative d'alertes en cybersécurité. Cette architecture nous a permis de développer un prototype d'EVC ainsi qu'un moteur de scénario permettant à des utilisateurs non familiarisés avec les moteurs de jeu de proposer des procédures collaboratives d'analyse d'alertes.

Ce prototype a été présenté à nos partenaires industriels, mais malheureusement nous n'avons pas pu le faire tester aux personnels des SOCs afin d'obtenir leurs retours et avis. De plus, comme nous avions implémenté un nombre important de fonctionnalités, l'évaluation de notre EVC par des experts n'était pas envisageable dans les SOCs, en raison du manque de temps que les personnels pouvaient consacrer à une étude collaborative.

Nous avons donc effectué une analyse de l'utilisabilité d'un environnement virtuel pour l'analyse d'alertes informatiques auprès de sujets non experts en cybersécurité. Cette étude nous a permis de mettre en évidence l'utilisabilité de tels environnements ainsi que l'adoption des technologies immersives quant à la sensibilisation aux problématiques cyber.

Cette thèse a donc apporté des contributions sur les points suivants :

— Proposition d'un protocole d'analyse de l'activité collaborative au sein des structures de cybersécurité comme les *Security Operations Centers* (SOCs).
— Proposition d'un modèle de l'activité collaborative des SOCs, le CyberCOP 3D, ayant pour objectif de transposer les pratiques des SOCs dans un Environnement Virtuel Collaboratif (EVC).
— Proposition d'un scénario collaboratif d'analyse d'alertes informatique pouvant être instancié dans un EVC et basé à la fois sur le modèle CyberCOP 3D et sur une modélisation du rançongiciel WannaCry.
— Développement d'une architecture événementielle et d'un moteur de scénario simplifié afin d'implémenter notre scénario collaboratif d'analyse d'alertes.
— Proposition d'un protocole d'évaluation de l'utilisabilité d'un environnement virtuel pour l'analyse d'alertes informatique.

Dans la partie suivante nous présenterons les perspectives à ces travaux de thèse.

Perspectives

Les perspectives à ces travaux de thèse concernent des aspects théoriques de l'analyse de l'état de sécurité des systèmes informatiques, des aspects techniques du développement d'EVC pour la cybersécurité et des aspects expérimentaux de l'évaluation de ces environnements.

Perspectives théoriques concernant l'analyse de l'état de sécurité des systèmes

Nous pensons qu'il faudrait affiner notre modèle afin de pouvoir le comparer aux études existantes des SOCs. Pour cela, il faudrait compléter l'étude que nous avons effectuée au sein des SOCs des partenaires industriels de la chaire Cyber CNI par des interviews des personnels ainsi que par des analyses de situations d'entraînement.

Dans un second temps, l'élaboration d'un modèle collaboratif de l'analyse de l'état de sécurité d'un système informatique s'appuyant sur notre modèle CyberCOP 3D pourrait être envisagée. En effet, ces modèles sont encore rares et notre approche basée sur l'analyse de l'activité collaborative pourrait permettre de proposer un changement des processus d'analyse d'alertes, comme l'ont proposé Crémilleux *et al.* [28].

Perspectives techniques du développement d'un EVC basé sur le modèle CyberCOP 3D

L'architecture que nous avons utilisée pour implémenter notre modèle CyberCOP 3D pourrait être étendue afin d'être encore plus modulaire et générale, en proposant par exemple un découplage entre l'affichage des informations sur les différentes interfaces utilisateurs et les événements utilisateurs, via un module d'événements *interface*. De plus, des retours utilisateurs d'experts en cybersécurité permettraient à la fois de modifier le moteur de scénarios, les différentes interfaces 2D ou immersives ainsi que les mécanismes de la gestion de la collaboration.

Le couplage d'un EVC basé sur le modèle CyberCOP 3D avec un outil de Cyber Range existant pourrait permettre d'une part la proposition de scénarios réalistes d'analyse au sein de l'EVC et d'autre part un pilotage des exercices de l'outil de Cyber Range directement au sein de l'environnement immersif. Ce couplage pourrait à terme permettre de proposer des situations d'entraînement collaboratives adaptées aux experts et aux non experts en cybersécurité.

L'intégration de données provenant d'outils d'analyse de données actuels comme les *Security Information and Event Management systems* (SIEMs) ou les *Intrusion Detection Systems* (IDS) à un EVC pourrait favoriser le monitoring immersif des systèmes informatiques. L'utilisation d'algorithmes de traitement de données adaptés aux représentations

immersives pourrait faciliter la représentation 3D des grands volumes de données issus des SIEMs.

L'utilisation d'outils de scénarisation existants et de techniques de gamification exploitables en EV pourrait faciliter l'emploi d'un EVC pour la CSA et pourrait aussi permettre une modification des procédures d'analyses existantes dans les SOCs.

Le développement d'une application de Réalité Augmentée basée sur le modèle Cyber-COP 3D pourrait aider au monitoring ou à l'entraînement en situation physique réelle.

Perspectives expérimentales de l'évaluation du modèle Cyber-COP 3D

L'évaluation de l'utilisabilité d'un environnement virtuel pour la cybersécurité par des experts en cybersécurité pourrait être envisagée, afin d'en comparer les résultats avec ceux de notre étude faite sur des sujets non experts.

Une étude comparative d'interfaces 2D, 3D desktop ou 3D immersives pour l'analyse de l'état de sécurité d'un système informatique pourrait permettre de mettre en évidence les apports des interfaces immersives par rapport aux interfaces actuelles. Staheli *et al.* [115] ont proposé en 2014 une revue des méthodes d'évaluation d'outils de visualisation pour la cybersécurité, et il pourrait être intéressant de compléter cette revue par un ajout des méthodes d'évaluations des outils immersifs de visualisation.

Une étude de l'impact de la durée de transition entre les vues de notre EVC (qui est actuellement instantanée) permettrait de déterminer si ce facteur aide les utilisateurs à mieux comprendre les différentes facettes des données représentées.

L'EVC que nous avons développé pourrait être utilisé afin d'implémenter des représentations de données 3D immersives, sous forme de graphe 3D ou autre, dont l'efficacité serait évaluée sur la base des scénarios d'analyse d'alertes que nous avons proposés.

Résumé des contributions

Publications Scientifiques

Conférences internationales

Résumé étendu : Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand, et al.. **Why should we use 3D Collaborative Virtual Environments for Cyber Security ?**. IEEE Fourth VR International Workshop on Collaborative Virtual Environments (IEEEVR 2018), Mar 2018, Reutlingen, Germany. (hal-01770064)

Article long : Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand, et al.. **From Cyber Security Activities to Collaborative Virtual Environments Practices through the 3D CyberCOP Platform.** International Conference on Information Systems Security, Dec 2018, Bengaluru, India. pp.272-287. (hal-01892161)

Article long : Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand, et al.. **3D CyberCOP : a Collaborative Platform for Cybersecurity Data Analysis and Training.** 15th International Conference on Cooperative Design, Visualization and Engineering, Oct 2018, Hangzou, China. pp.176-183. (hal-01831965)

Article collectif : Simon Foley, Fabien Autrel, Edwin Bourget, Thomas Cledel, Stéphane Grunenwald, et al.. **Science hackathons for cyberphysical system security research : putting CPS tesdbed platforms to good use.** CPS-SPC 2018 : Workshop on Cyber-Physical Systems Security and Privacy, Oct 2018, Toronto, Canada. pp.102 - 107, (hal-01911182)

Communications informelles

Rencontres doctorales : Alexandre Kabil. **CyberCOP3D : Visualisation Collaborative et Immersive pour la cybersécurité.** 29ème conférence francophone sur l'Interaction Homme-Machine, AFIHM, Aug 2017, Poitiers, France. 4 p. (hal-01577868)

Autres contributions

- Premier prix thèse 3.0 défi RCC (thèse en 180 secondes) organisé durant l'European Cyber Week en 2017.
- Présentation d'une application immersive et collaborative durant le Forum International de la Cybersécurité (FIC) en 2018 à Lille.
- Présentation et démonstration des travaux de thèse durant les *IT Risk & Cyber defense Days 2019* au Campus BNP Paribas.
- Présentation et démonstration des travaux de thèse dans les locaux d'EDF pour les événements suivants :
  - Journée Cyber EDF, forum de présentation de la cybersécurité aux personnels EDF.
  - Réunion avec des personnels EDF travaillant sur la visualisation 3D pour les environnements industriels.
  - Présentation de la Chaire Cyber CNI à l'EDF Lab Saclay.
- Présentation et démonstration des travaux de thèse dans les locaux de la Société Générale pour les événements suivants :
  - La Cyber Tech Week, forum de présentation de la cybersécurité aux personnels de la Société Générale.
  - La convention de la filière SSI, intéressée par les travaux de la Chaire Cyber CNI.
  - Présentation *Coffee and Learn* aux personnels de l'équipe outil du SOC.

BIBLIOGRAPHIE

[1] Pierre ABEL, Pascal GROS, Cristina Russo DOS SANTOS, Didier LOISEL et Jean-Pierre PARIS, « Automatic construction of dynamic 3d metaphoric worlds : An application to network management », in : *Visual Data Exploration and Analysis VII*, t. 3960, International Society for Optics et Photonics, 2000, p. 312-323 (cf. p. 35).

[2] J. M. AHREND, M. JIROTKA et K. JONES, « 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)*, juin 2016, p. 10, DOI : 10.1109/CyberSA.2016.7503279 (cf. p. 29, 30).

[3] Merete ASK, Petro BONDARENKO, John Erik REKDAL, André NORDBØ, Pieter BLOEMERUS et Dmytro PIATKIVSKYI, « Advanced persistent threat (APT) beyond the hype », in : *Project Report in IMT4582 Network Security at GjoviN University College* (2013) (cf. p. 79).

[4] Ruth AYLETT et Sandy LOUCHART, « Towards a narrative theory of virtual reality », in : *Virtual Reality* 7.*1* (2003), p. 2-9 (cf. p. 50).

[5] Camille BAROT, « Scénarisation d'environnements virtuels. Vers un équilibre entre contrôle, cohérence et adaptabilité. », thèse de doct., 2014 (cf. p. 64).

[6] Tim BASS et al., « Multisensor data fusion for next generation distributed intrusion detection systems », in : *Proceedings of the IRIS National Symposium on Sensor and Data Fusion*, t. 24, 28, Citeseer, 1999, p. 24-27 (cf. p. 14, 15).

[7] Mark BILLINGHURST, Maxime CORDEIL, Anastasia BEZERIANOS et Todd MARGOLIS, « Collaborative immersive analytics », in : *Immersive Analytics*, Springer, 2018, p. 221-257 (cf. p. 61, 62).

[8] Cyril BOSSARD, Gilles KERMARREC, Cédric BUCHE et Jacques TISSEAU, « Transfer of learning in virtual environments : a new challenge ? », in : *Virtual Reality* 12.*3* (2008), p. 151-161 (cf. p. 64).

[9] Rozenn BOUVILLE, « Interopérabilité des environnements virtuels 3D : modèle de réconciliation des contenus et des composants logiciels », thèse de doct., 2012 (cf. p. 53).

[10] J Boyd, « A discourse on winning and losing [Briefing slides] », in : *Maxwell Air Force Base, AL : Air University Library.(Document No. MU 43947)* (1987) (cf. p. 11).

[11] Jeffrey M Bradshaw, Marco Carvalho, Larry Bunch, Tom Eskridge, Paul J Feltovich, Chris Forsythe, Robert R Hoffman, Matt Johnson, Dan Kidwell et David D Woods, « Coactive emergence as a sensemaking strategy for cyber operations », in : *ICST (Institute for Computer Science, Social Informatics, and Telecommunications Engineering) Transactions of Security and Safety. Special section on The Cognitive Science of Cyber Defense Analysis (in press, 2012)* (2012) (cf. p. 20, 21).

[12] John Brooke et al., « SUS-A quick and dirty usability scale », in : *Usability evaluation in industry* 189.*194* (1996), p. 4-7 (cf. p. 137, 144).

[13] Cédric Buche, Ronan Querrec, Pierre De Loor et Pierre Chevaillier, « Mascaret : A pedagogical multi-agent system for virtual environments for training », in : *International Journal of Distance Education Technologies (IJDET)* 2.*4* (2004), p. 41-61 (cf. p. 64).

[14] Wolfgang Büschel, Jian Chen, Raimund Dachselt, Steven Drucker, Tim Dwyer, Carsten Görg, Tobias Isenberg, Andreas Kerren, Chris North et Wolfgang Stuerzlinger, « Interaction for immersive analytics », in : *Immersive Analytics*, Springer, 2018, p. 95-138 (cf. p. 59).

[15] Simon Butscher, Sebastian Hubenschmid, Jens Müller, Johannes Fuchs et Harald Reiterer, « Clusters, trends, and outliers : How immersive technologies can facilitate the collaborative analysis of multidimensional data », in : *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ACM, 2018, p. 90 (cf. p. 61, 62).

[16] Yohann Cardin, « L'analyse de l'activité comme préalable à la conception d'un environnement virtuel de formation. Le cas d'une formation à la gestion d'incendies en milieu urbain chez les sapeurs-pompiers », thèse de doct., UBO, 2016 (cf. p. 64, 76).

[17] Julien Casarin, Nicolas Pacqueriaud et Dominique Bechmann, « UMI3D : A Unity3D Toolbox to Support CSCW Systems Properties in Generic 3D User Interfaces », in : *Proceedings of the ACM on Human-Computer Interaction* 2.*CSCW* (2018), p. 29 (cf. p. 55, 86).

[18] Tom Chandler, Maxime Cordeil, Tobias Czauderna, Tim Dwyer, Jaroslaw Glowacki, Cagatay Goncu, Matthias Klapperstueck, Karsten Klein, Kim Marriott, Falk Schreiber et al., « Immersive analytics », in : *Big Data Visual Analytics (BDVA), 2015*, IEEE, 2015, p. 1-8 (cf. p. 61).

[19] Siming Chen, Cong Guo, Xiaoru Yuan, Fabian Merkle, Hanna Schaefer et Thomas Ertl, « Oceans : Online collaborative explorative analysis on network security », in : *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, ACM, 2014, p. 1-8 (cf. p. 31, 32).

[20] Elizabeth F Churchill et Dave Snowdon, « Collaborative virtual environments : an introductory review of issues and systems », in : *Virtual Reality* 3.*1* (1998), p. 3-15 (cf. p. 54, 55).

[21] Guillaume Claude, Valérie Gouranton et Bruno Arnaldi, « Roles in collaborative virtual environments for training », in : 2015 (cf. p. 65).

[22] Philippe Coiffet, *Mondes imaginaires : les arcanes de la réalité virtuelle*, Hermès, 1995 (cf. p. 51).

[23] Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson et Thuy D. Nguyen, « A Video Game for Cyber Security Training and Awareness », in : *Comput. Secur.* 26.*1* (fév. 2007), p. 63-72, issn : 0167-4048, doi : 10.1016/j.cose.2006.10.005, url : http://dx.doi.org/10.1016/j.cose.2006.10.005 (cf. p. 41, 42).

[24] Gregory Conti, John Nelson et David Raymond, « Towards a cyber common operating picture », in : *Cyber Conflict (CyCon), 2013 5th International Conference on*, IEEE, 2013, p. 1-17 (cf. p. 12, 31).

[25] Maxime Cordeil, Andrew Cunningham, Tim Dwyer, Bruce H Thomas et Kim Marriott, « ImAxes : Immersive axes as embodied affordances for interactive multivariate data visualisation », in : *Proceedings of the 30th Annual ACM Symposium on User Interface Software and Technology*, ACM, 2017, p. 71-83 (cf. p. 61).

[26] Jérémy Cormier, « Mobiliser une analyse de l'activité comme aide à la conception et à l'évaluation d'un Environnement Virtuel pour l'Apprentissage Humain : un exemple en implantologie dentaire », thèse de doct., Brest, 2012 (cf. p. 64).

[27] Ben Cowley, Darryl Charles, Michaela Black et Ray Hickey, « Toward an understanding of flow in video games », in : *Computers in Entertainment (CIE)* 6.*2* (2008), p. 20 (cf. p. 64).

[28] Damien Crémilleux, Christophe Bidan, Frédéic Majorczyk et Nicolas Prigent, « Enhancing Collaboration Between Security Analysts in Security Operations Centers », in : *International Conference on Risks and Security of Internet and Systems*, Springer, 2018, p. 136-142 (cf. p. 159).

[29] Anita D'Amico et Kirsten Whitley, « The real work of computer network defense analysts », in : *VizSEC 2007*, Springer, 2008, p. 19-37 (cf. p. 23).

[30] D Mellet d'Huart, « Virtual Environment for training : An art of enhancing reality », in : *ITS*, 2002 (cf. p. 64).

[31] Anita DAmico, Laurin Buchanan, Drew Kirkpatrick et Paul Walczak, « Cyber Operator Perspectives on Security Visualization », in : *Advances in Human Factors in Cybersecurity*, Springer, 2016, p. 69-81 (cf. p. 77, 184).

[32] Erica De Vries, « Les logiciels d'apprentissage : panoplie ou éventail ? », in : *Revue française de pédagogie* (2001), p. 105-116 (cf. p. 63).

[33] Berthier Denis, *Méditations sur le réel et le virtuel*, 2004 (cf. p. 49).

[34] Dorothy E Denning, « An intrusion-detection model », in : *IEEE Transactions on software engineering 2* (1987), p. 222-232 (cf. p. 14).

[35] Martin Dodge et Rob Kitchin, *Atlas of cyberspace*, t. 158, Addison-Wesley London, 2001 (cf. p. 57).

[36] C. Donalek et al., « Immersive and collaborative data visualization using virtual reality platforms », in : *2014 IEEE International Conference on Big Data (Big Data)*, oct. 2014, p. 609-614, doi : 10.1109/BigData.2014.7004282 (cf. p. 61).

[37] Steve Dübel, Martin Röhlig, Heidrun Schumann et Matthias Trapp, « 2D and 3D presentation of spatial data : A systematic review », in : *2014 IEEE VIS International Workshop on 3DVis (3DVis)*, IEEE, 2014, p. 11-18 (cf. p. 57).

[38] Thierry Duval, Cédric Fleury, Bernard Nouailhas et Laurent Aguerreche, « Collaborative exploration of 3d scientific data », in : *Proceedings of the 2008 ACM symposium on Virtual reality software and technology*, ACM, 2008, p. 303-304 (cf. p. 61).

[39] Mica R Endsley, « Measurement of situation awareness in dynamic systems », in : *Human factors* 37.*1* (1995), p. 65-84 (cf. p. 12, 18).

[40] Mica R Endsley et Erik S Connors, « Foundation and Challenges », in : *Cyber Defense and Situational Awareness*, Springer, 2014, p. 7-27 (cf. p. 19).

[41] Manuel Esteve, Israel Pérez, Carlos Palau, Federico Carvajal, Javier Hingant, Miguel A Fresneda et Juan P Sierra, « Cyber Common Operational Picture : A Tool for Cyber Hybrid Situational Awareness Improvement », in : *North Atlantic Treaty Organization (NATO) Science and Technology Organization (STO), Technical Report STO-MP-IST-148* (2016) (cf. p. 31, 33).

[42] Renée E Etoty et Robert F Erbacher, *A survey of visualization tools assessed for anomaly-based intrusion detection analysis*, rapp. tech., ARMY RESEARCH LAB ADELPHI MD COMPUTATIONAL et INFORMATION SCIENCES DIRECTORATE, 2014 (cf. p. 27, 28).

[43] Antti Evesti, Teemu Kanstrén et Tapio Frantti, « Cybersecurity situational awareness taxonomy », in : *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, IEEE, 2017, p. 1-8 (cf. p. 85).

[44] Vitaly Ford, Ambareen Siraj, Ada Haynes et Eric Brown, « Capture the flag unplugged : an offline cyber competition », in : *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*, ACM, 2017, p. 225-230 (cf. p. 40).

[45] Philippe Fuchs, *Le traité de la réalité virtuelle*, t. 2, Presses des MINES, 2006 (cf. p. 48).

[46] Ruben Jesus Garca-Hernandez, Christoph Anthes, Markus Wiedemann et Dieter Kranzlmuller, « Perspectives for using virtual reality to extend visual data mining in information visualization », in : *2016 IEEE Aerospace Conference*, IEEE, 2016, p. 1-11 (cf. p. 57).

[47] Stéphanie Gerbaud, Nicolas Mollet et Bruno Arnaldi, « Virtual environments for training : from individual learning to collaboration with humanoids », in : *International Conference on Technologies for E-Learning and Digital Entertainment*, Springer, 2007, p. 116-127 (cf. p. 65).

[48] Stéphanie Gerbaud, Nicolas Mollet, Franck Ganier, Bruno Arnaldi et Jacques Tisseau, « GVT : a platform to create virtual environments for procedural training », in : *2008 IEEE Virtual Reality Conference*, IEEE, 2008, p. 225-232 (cf. p. 64).

[49] Nicklaus A Giacobe, « Application of the JDL data fusion process model for cyber security », in : *International Society for Optical Engineering (SPIE)*, t. 7710, 2010, 77100R (cf. p. 16).

[50] William Gibson et Jean Bonnefoy, *Neuromancien*, Éditions J'ai lu, 1985 (cf. p. 57).

[51] Steven R Gomez, Vincent Mancuso et Diane Staheli, « Considerations for Human-Machine Teaming in Cybersecurity », in : *International Conference on Human-Computer Interaction*, Springer, 2019, p. 153-168 (cf. p. 20).

[52] Magdalena Granåsen et Dennis Andersson, « Measuring team effectiveness in cyber-defense exercises : a cross-disciplinary case study », in : *Cognition, Technology & Work* 18.*1* (2016), p. 121-143 (cf. p. 39).

[53] P Gros, P Abel, R Dos Santos, D Loisel, N Trichaud et JP Paris, « Experimenting service-oriented 3D metaphors for managing networks using virtual reality », in : *Laval Virtual–Virtual Reality International Conference*, mai 2000 (cf. p. 35).

[54] Robert Gutzwiller, *Situation Awareness in Defensive Cyberspace Operations : An Annotated Bibliographic Assessment Through 2015*, rapp. tech., NIWC Pacific San Diego United States, 2019 (cf. p. 21, 27).

[55] R. Hackathorn et T. Margolis, « Immersive analytics : Building virtual data worlds for collaborative decision support », in : *2016 Workshop on Immersive Analytics (IA)*, mar. 2016, p. 44-47, doi : 10.1109/IMMERSIVE.2016.7932382 (cf. p. 61).

[56] Cristin M Hall, Sonya AH McMullen, David L Hall, Mac J McMullen et Barton K Pursel, « Perspectives on visualization and virtual world technologies for multi-sensor data fusion », in : *Information Fusion, 2008 11th International Conference on*, IEEE, 2008, p. 1-6 (cf. p. 34).

[57] Juho Hamari, Jonna Koivisto, Harri Sarsa et al., « Does Gamification Work ?-A Literature Review of Empirical Studies on Gamification. », in : *HICSS*, t. 14, 2014, 2014, p. 3025-3034 (cf. p. 64).

[58] Balázs Péter HÁMORNIK et Csaba KRASZNAY, « Prerequisites of Virtual Teamwork in Security Operations Centers : Knowledge, Skills, Abilities and Other Characteristics », in : *Academic and Applied Research in Military and Public Management Science* (2017), p. 73 (cf. p. 71, 76, 89, 91).

[59] Warren Harrop et Grenville Armitage, « Real-time Collaborative Network Monitoring and Control Using 3D Game Engines for Representation and Interaction », in : *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, VizSEC '06, Alexandria, Virginia, USA : ACM, 2006, p. 31-40, isbn : 1-59593-549-5, doi : 10.1145/1179576.1179583, url : http://doi.acm.org/10.1145/1179576.1179583 (cf. p. 34).

[60] Charlotte Hoareau, Ronan Querrec et Franck Ganier, *Recommandations ergonomiques pour le guidage de l'apprenant en EVAH*, 2015 (cf. p. 64).

[61] Daisuke Inoue, Masashi Eto, Koei Suzuki, Mio Suzuki et Koji Nakao, « 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*, VizSec '12, Seattle, Washington, USA : ACM, 2012, p. 72-79, isbn : 978-1-4503-1413-8, doi : 10.1145/2379690.2379700, url : http://doi.acm.org/10.1145/2379690.2379700 (cf. p. 36).

[62] Jason Jerald, *The VR book : Human-centered design for virtual reality*, Morgan & Claypool, 2015 (cf. p. 51).

[63] W Lewis Johnson et Jeff Rickel, « Steve : An animated pedagogical agent for procedural training in virtual environments », in : *ACM SIGART Bulletin* 8.*1-4* (1997), p. 16-21 (cf. p. 65).

[64] Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand et Christophe Ponchel, « 3D CyberCOP : a Collaborative Platform for Cybersecurity Data Analysis and Training », in : *15th International Conference on Cooperative Design, Visualization and Engineering*, sous la dir. d'Yuhua Luo, Cooperative Design, Visualization, and Engineering, in proceedings of CDVE 2018 (15th International Conference on Cooperative Design, Visualization and Engineering), Springer, p. 176-183, Hangzhou, China, October 21-24, 2018, Hangzou, China : Springer, oct. 2018, p. 176-183, url : https://hal.archives-ouvertes.fr/hal-01831965 (cf. p. 96).

[65] Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand et Christophe Ponchel, « From Cyber Security Activities to Collaborative Virtual Environments Practices through the 3D CyberCOP Platform », in : *International Conference on Information Systems Security*, proceedings of ICISS 2018, 14th International Conference on Information Systems Security, Bengaluru, India, déc. 2018, p. 272-287, url : https://hal.archives-ouvertes.fr/hal-01892161 (cf. p. 96).

[66] Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand et Christophe Ponchel, « 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, url : https://hal.archives-ouvertes.fr/hal-01770064 (cf. p. 57).

[67] J Keiriz, Olusola Ajilore, Alex D Leow et Angus G Forbes, « Immersive analytics for clinical neuroscience », in : *Proceedings of the IEEE VIS Workshop on Immersive Analytics*, 2017, p. 1454-1 (cf. p. 61).

[68] Christa Kelleher et Thorsten Wagener, « Ten guidelines for effective data visualization in scientific publications », in : *Environmental Modelling & Software* 26.*6* (2011), p. 822-827 (cf. p. 57).

[69] Tero Kokkonen, « Architecture for the Cyber Security Situational Awareness System », in : *International Conference on Next Generation Wired/Wireless Networking*, Springer, 2016, p. 294-302 (cf. p. 16).

[70] Alfred Korzybski, *Une carte n'est pas le territoire : prolégomènes aux systèmes non-aristotéliciens et à la sémantique générale*, Éditions de l'Éclat, 1998 (cf. p. 57).

[71] Matthias Kraus, Niklas Weiler, Daniel A Keim, Alexandra Diehl et Benjamin Bach, « Visualization in the VR-Canvas : How much Reality is Good for Immersive Analytics in Virtual Reality ? », in : *2nd Workshop on the Creation, Curation,*

Critique and Conditioning of Principles and Guidelines in Visualization at IEEE VIS, 2018 (cf. p. 61).

[72] Kaur Kullman, Noam Ben Asher et Char Sample, « Operator Impressions of 3D Visualizations for Cybersecurity Analysts », in : *European Conference on Cyber Warfare and Security*, Academic Conferences International Limited, 2019, p. 257-XVIII (cf. p. 36).

[73] Kaur Kullman, Jennifer Cowley et Noam Ben-Asher, « Enhancing Cyber Defense Situational Awareness Using 3D Visualizations », in : *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, Academic Conferences et publishing limited, 2018, p. 369 (cf. p. 36).

[74] Oh-Hyun Kwon, Chris Muelder, Kyungwon Lee et Kwan-Liu Ma, « A study of layout, rendering, and interaction methods for immersive graph visualization », in : *IEEE transactions on visualization and computer graphics* 22.7 (2016), p. 1802-1815 (cf. p. 63).

[75] Lauri Laaperi et Jouko Vankka, « Architecture for a system providing a common operating picture of critical infrastructure », in : *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on*, IEEE, 2015, p. 1-6 (cf. p. 16).

[76] B. Laha, K. Sensharma, J. D. Schiffbauer et D. A. Bowman, « Effects of Immersion on Visual Analysis of Volume Data », in : *IEEE Transactions on Visualization and Computer Graphics* 18.4 (avr. 2012), p. 597-606, issn : 1077-2626, doi : 10.1109/TVCG.2012.42 (cf. p. 57).

[77] O. M. Latvala, T. Keränen, S. Noponen, N. Lehto, M. Sailio, M. Valta et P. Olli, « Visualizing network events in a muggle friendly way », in : *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, juin 2017, p. 1-4, doi : 10.1109/CyberSA.2017.8073400 (cf. p. 36, 37).

[78] Ralph Lengler et Martin J Eppler, « Towards a periodic table of visualization methods for management », in : *IASTED Proceedings of the Conference on Graphics and Visualization in Engineering (GVE 2007), Clearwater, Florida, USA*, 2007 (cf. p. 59, 60).

[79] Pierre Lévy, *Qu'est-ce que le virtuel ?*, Éditions La Découverte, 1995 (cf. p. 46, 57).

[80] Yanyan Li et Mengjun Xie, « Platoon : A Virtual Platform for Team-oriented Cybersecurity Training and Exercises », in : *Proceedings of the 17th Annual Conference on Information Technology Education*, ACM, 2016, p. 20-25 (cf. p. 38).

[81] Thomas Lopez, Pierre Chevaillier, Valérie Gouranton, Paul Evrard, Florian Nouviale, Mukesh Barange, Rozenn Bouville et Bruno Arnaldi, « Collaborative virtual training with physical and communicative autonomous agents », in : *Computer Animation and Virtual Worlds* 25.*3-4* (2014), p. 485-493 (cf. p. 65).

[82] Domitile Lourdeaux, « Réalité virtuelle et formation : conception d'environnements virtuels pédagogiques », thèse de doct., 2001 (cf. p. 63).

[83] Domitile Lourdeaux, Philippe Fuchs et Jean-Marie Burkhardt, « An intelligent tutorial agent for training virtual environments », in : 2002 (cf. p. 65).

[84] Robert Luh, Stefan Marschalek, Manfred Kaiser, Helge Janicke et Sebastian Schrittwieser, « Semantics-aware detection of targeted attacks : a survey », in : *Journal of Computer Virology and Hacking Techniques* 13.*1* (2017), p. 47-85 (cf. p. 79).

[85] Mirco Marchetti, Fabio Pierazzi, Alessandro Guido et Michele Colajanni, « Countering Advanced Persistent Threats through security intelligence and big data analytics », in : *2016 8th International Conference on Cyber Conflict (CyCon)*, IEEE, 2016, p. 243-261 (cf. p. 79).

[86] Kim Marriott, Jian Chen, Marcel Hlawatsch, Takayuki Itoh, Miguel A. Nacenta, Guido Reina et Wolfgang Stuerzlinger, « Immersive Analytics : Time to Reconsider the Value of 3D for Information Visualisation », in : *Immersive Analytics*, sous la dir. de Kim Marriott, Falk Schreiber, Tim Dwyer, Karsten Klein, Nathalie Henry Riche, Takayuki Itoh, Wolfgang Stuerzlinger et Bruce H. Thomas, Cham : Springer International Publishing, 2018, p. 25-55, isbn : 978-3-030-01388-2, doi : 10.1007/978-3-030-01388-2_2, url : https://doi.org/10.1007/978-3-030-01388-2_2 (cf. p. 57, 58).

[87] Kim Marriott, Falk Schreiber, Tim Dwyer, Karsten Klein, Nathalie Henry Riche, Takayuki Itoh, Wolfgang Stuerzlinger et Bruce H Thomas, *Immersive Analytics*, t. 11190, Springer, 2018 (cf. p. 61).

[88] Raffael Marty, *Applied security visualization*, Addison-Wesley Upper Saddle River, 2009 (cf. p. 25, 26).

[89] Sten Mäses, Liina Randmann, Olaf Maennel et Birgy Lorenz, « Stenmap : Framework for Evaluating Cybersecurity-Related Skills Based on Computer Simulations », in : *Learning and Collaboration Technologies. Learning and Teaching*, sous la dir. de Panayiotis Zaphiris et Andri Ioannou, Cham : Springer International Publishing, 2018, p. 492-504, isbn : 978-3-319-91152-6 (cf. p. 39).

[90] Barry McGuinness et Louise Foy, « A subjective measure of SA : the Crew Awareness Rating Scale (CARS) », in : *Proceedings of the first human performance, situation awareness, and automation conference, Savannah, Georgia*, t. 16, 2000, p. 286-291 (cf. p. 17).

[91] Sean McKenna, Diane Staheli et Miriah Meyer, « Unlocking user-centered design methods for building cyber security visualizations », in : *Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on*, IEEE, 2015, p. 1-8 (cf. p. 76, 89, 90).

[92] Wim Mees et Thibault Debatty, « An attempt at defining cyberdefense situation awareness in the context of command & control », in : *Military Communications and Information Systems (ICMCIS), 2015 International Conference on*, IEEE, 2015, p. 1-9 (cf. p. 11).

[93] M. C. K. Michel, N. P. Helmick et L. M. Mayron, « Cognitive cyber situational awareness using virtual worlds », in : *2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, fév. 2011, p. 179-182, doi : 10.1109/COGSIMA.2011.5753440 (cf. p. 34).

[94] Savita Mohurle et Manisha Patil, « A brief study of wannacry threat : Ransomware attack 2017 », in : *International Journal of Advanced Research in Computer Science* 8.5 (2017) (cf. p. 79).

[95] Julien Murphy, Edward Sihler, Maureen Ebben, Lynn Lovewell et Glenn Wilson, « Building a Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL) », in : *Proceedings of the International Conference on Security and Management (SAM)*, The Steering Committee of The World Congress in Computer Science, Computer . . ., 2014, p. 1 (cf. p. 38).

[96] A. Nagarajan, J. M. Allbeck, A. Sood et T. L. Janssen, « Exploring game design for cybersecurity training », in : *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, mai 2012, p. 256-262, doi : 10.1109/CYBER.2012.6392562 (cf. p. 41).

[97] Kara Nance, Brian Hay, Ronald Dodge, Alex Seazzu et Steve Burd, « Virtual laboratory environments : Methodologies for educating cybersecurity researchers », in : *Methodological Innovations Online* 4.3 (2009), p. 3-14 (cf. p. 38).

[98] Olivier Nannipieri et Philippe Fuchs, « Pour en finir avec La Réalité : une approche socio-constructiviste de la réalité virtuelle », in : *Revue des Interactions Humaines Médiatisées (RIHM)= Journal of Human Mediated Interactions* 10.1 (2009), p. 83-100 (cf. p. 47, 50).

[99] Huyen Nguyen, Peter Marendy et Ulrich Engelke, « Collaborative framework design for immersive analytics », in : *2016 Big Data Visual Analytics (BDVA)*, IEEE, 2016, p. 1-8 (cf. p. 61).

[100] Patrick O'Leary, Sankhesh Jhaveri, Aashish Chaudhary, William Sherman, Ken Martin, David Lonie, Eric Whiting, James Money et Sandy McKenzie, « Enhancements to VTK enabling scientific visualization in immersive environments », in : *Virtual Reality (VR), 2017 IEEE*, IEEE, 2017, p. 186-194 (cf. p. 59).

[101] Cyril Onwubiko, « Understanding cyber situation awareness », in : *Int. J. Cyber Situat. Aware* (2016) (cf. p. 17, 20).

[102] Timea Pahi, Maria Leitner et Florian Skopik, « Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers. », in : *ICISSP*, 2017, p. 334-345 (cf. p. 13).

[103] MB Parish et B Madahar, « Understanding Cyberspace Through Cyber Situational Awareness », in : *The Defence Science and Technology Laboratory : Wiltshire, UK* (2016) (cf. p. 12).

[104] Lévy Pierre, « Cyberculture », in : *Rapport au Conseil de l 'Europe. Odile Jacob* (1997) (cf. p. 46, 47).

[105] Ronan Querrec, Cédric Buche, Eric Maffre et Pierre Chevaillier, « SécuRéVi : virtual environments for fire-fighting training », in : *5th virtual reality international conference (VRIC'03)*, 2003, p. 169-175 (cf. p. 64).

[106] Kjetil Raaen et Ivar Kjellmo, « Measuring latency in virtual reality systems », in : *International Conference on Entertainment Computing*, Springer, 2015, p. 457-462 (cf. p. 51).

[107] Prashanth Rajivan et Nancy Cooke, « Impact of Team Collaboration on Cybersecurity Situational Awareness », in : *Theory and Models for Cyber Situation Awareness*, sous la dir. de Peng Liu, Sushil Jajodia et Cliff Wang, Cham : Springer International Publishing, 2017, p. 203-226, isbn : 978-3-319-61152-5, doi : 10.1007/978-3-319-61152-5_8, url : https://doi.org/10.1007/978-3-319-61152-5_8 (cf. p. 27, 29).

[108] A. Sethi et G. Wills, « Expert-interviews led analysis of EEVi - A model for effective visualization in cyber-security », in : *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, oct. 2017, p. 1-8, doi : 10.1109/VIZSEC.2017.8062195 (cf. p. 24, 25).

[109] Aneesha Sethi, Federica Paci et Gary Wills, « EEVi-framework for evaluating the effectiveness of visualization in cyber-security », in : *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, 2016, p. 340-345 (cf. p. 23, 76).

[110] Ankit Shah, Rajesh Ganesan, Sushil Jajodia et Hasan Cam, « A methodology to measure and monitor level of operational effectiveness of a CSOC », in : *International Journal of Information Security* 17.*2* (2018), p. 121-134 (cf. p. 74).

[111] Hadi Shiravi, Ali Shiravi et Ali A Ghorbani, « A survey of visualization systems for network security », in : *IEEE Transactions on visualization and computer graphics* 18.*8* (2012), p. 1313-1329 (cf. p. 29).

[112] Ronell Sicat, Jiabao Li, JunYoung Choi, Maxime Cordeil, Won-Ki Jeong, Benjamin Bach et Hanspeter Pfister, « Dxr : A toolkit for building immersive data visualizations », in : *IEEE transactions on visualization and computer graphics* 25.*1* (2018), p. 715-725 (cf. p. 59, 60).

[113] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, Daesung Moon et Jong Hyuk Park, « A comprehensive study on APT attacks and countermeasures for future networks and communications : challenges and solutions », in : *The Journal of Supercomputing* (2016), p. 1-32 (cf. p. 79).

[114] Mel Slater, « A note on presence terminology », in : *Presence connect* 3.*3* (2003), p. 1-5 (cf. p. 49).

[115] Diane Staheli, Tamara Yu, R. Jordan Crouser, Suresh Damodaran, Kevin Nam, David O'Gwynn, Sean McKenna et Lane Harrison, « Visualization Evaluation for Cyber Security : Trends and Future Directions », in : *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, VizSec '14, Paris, France : ACM, 2014, p. 49-56, isbn : 978-1-4503-2826-5, doi : 10.1145/2671491.2671492, url : http://doi.acm.org/10.1145/2671491.2671492 (cf. p. 160).

[116] Georgiana Subaşu, Livia Roşu et Ion Bădoi, « Modeling and simulation architecture for training in cyber defence education », in : *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, IEEE, 2017, p. 1-4 (cf. p. 37, 38, 42).

[117] Sathya Chandran Sundaramurthy, Jacob Case, Tony Truong, Loai Zomlot et Marcel Hoffmann, « A tale of three security operation centers », in : *Proceedings of the 2014 ACM workshop on security information workers*, ACM, 2014, p. 43-50 (cf. p. 76).

[118] Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G. Bardas et S. Raj Rajagopalan, « 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)*, Denver, CO : USENIX Association, 2016, p. 237-251, isbn : 978-1-931971-31-7, url : https://www.usenix.org/conference/soups2016/technical-sessions/presentation/sundaramurthy (cf. p. 76, 85).

[119] George P Tadda et John S Salerno, « Overview of cyber situation awareness », in : *Cyber situational awareness*, Springer, 2010, p. 15-35 (cf. p. 21, 22).

[120] Clark Taylor, Pablo Arias, Jim Klopchic, Celeste Matarazzo et Evi Dube, « CTF : State-of-the-Art and Building the Next Generation », in : *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, 2017 (cf. p. 39, 40).

[121] Katy TCHA-TOKEY, Olivier CHRISTMANN, Emilie Loup-Escande et Simon Richir, « Proposition and Validation of a Questionnaire to Measure the User Experience in Immersive Virtual Environments », in : *The International Journal of Virtual Reality* 16.*1* (2016), p. 33-48, URL : `https://hal.archives-ouvertes.fr/hal-01404497` (cf. p. 144).

[122] Jacques Tisseau, « Réalité virtuelle et complexité », in : *Expérimentation in virtuo des systemes complexes. Manifeste scientifique du Centre Européen de Réalité Virtuelle, France* (2004) (cf. p. 47).

[123] Jacques Tisseau, « Réalité virtuelle : autonomie in virtuo », in : *Habilitationa diriger des recherches, Université de Rennes* 1 (2001) (cf. p. 49).

[124] Alissa Torres, « Building a World-Class Security Operations Center : A Roadmap », in : (2015) (cf. p. 70, 72).

[125] Michael Tyworth, Nicklaus A Giacobe, Vincent Mancuso et Christopher Dancy, « The distributed nature of cyber situation awareness », in : *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference on*, IEEE, 2012, p. 174-178 (cf. p. 20).

[126] Margaret Varga, Carsten Winkelholz et Susan Träber-Burdin, « Cyber Situation Awareness », in : *Cyber Security Science and Engineering (STO-EN-IST-143)* (2016), p. 1-18 (cf. p. 23, 24).

[127] Margaret Varga, Carsten Winkelholz et Susan Träber-Burdin, *The Application of Visual Analytics to Cyber Security*, 2017 (cf. p. 23).

[128] Jorge A Wagner Filho, Carla Maria Dal Sasso Freitas et Luciana Nedel, « VirtualDesk : a comfortable and efficient immersive information visualization approach », in : *Computer Graphics Forum*, t. 37, 3, Wiley Online Library, 2018, p. 415-426 (cf. p. 61).

[129] Bing Wang et Klaus Mueller, « Does 3D really make sense for visual cluster analysis ? yes ! », in : *3DVis (3DVis), 2014 IEEE VIS International Workshop on*, IEEE, 2014, p. 37-44 (cf. p. 57).

[130] William Winn, « A conceptual basis for educational applications of virtual reality », in : *Technical Publication R-93-9, Human Interface Technology Laboratory of the Washington Technology Center, Seattle : University of Washington* (1993) (cf. p. 63).

[131] David Zeltzer, « Autonomy, interaction, and presence », in : *Presence : Teleoperators & Virtual Environments* 1.*1* (1992), p. 127-132 (cf. p. 49).

[132] Zequn Huang, Chien-Chung Shen, S. Doshi, N. Thomas et Ha Duong, « Fuzzy sets based team decision-making for Cyber Situation Awareness », in : *MILCOM 2016 - 2016 IEEE Military Communications Conference*, nov. 2016, p. 1077-1082, doi : 10.1109/MILCOM.2016.7795473 (cf. p. 21).

[133] Chen Zhong, Awny Alnusair, Brandon Sayger, Aaron Troxell et Jun Yao, « AOH-Map : A Mind Mapping System for Supporting Collaborative Cyber Security Analysis », in : *2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, IEEE, 2019, p. 74-80 (cf. p. 31, 32).

[134] Chen Zhong, John Yen, Peng Liu, Rob F. Erbacher, Christopher Garneau et Bo Chen, « Studying Analysts' Data Triage Operations in Cyber Defense Situational Analysis », in : *Theory and Models for Cyber Situation Awareness*, sous la dir. de Peng Liu, Sushil Jajodia et Cliff Wang, Cham : Springer International Publishing, 2017, chap. 2, p. 128-169, isbn : 978-3-319-61152-5 (cf. p. 14, 17).

[135] Zengsheng Zhong, Ying Zhao, Ronghua Shi, Yingshuai Sheng, Junrong Liu, Hua Meng et Dan Lin, « A user-centered multi-space collaborative visual analysis for cyber security », in : *Chinese Journal of Electronics* 27.*5* (2018), p. 910-919 (cf. p. 31, 33, 91).

[136] Fangfang Zhou, Wei Huang, Ying Zhao, Yang Shi, Xing Liang et Xiaoping Fan, « Entvis : a visual analytic tool for entropy-based network traffic anomaly detection », in : *IEEE computer graphics and applications* 35.*6* (2015), p. 42-50 (cf. p. 29, 30).

[137] Ying Zhu, « Introducing google chart tools and google maps api in data visualization courses », in : *IEEE computer graphics and applications* 32.*6* (2012), p. 6-9 (cf. p. 59).

[138] Carson Zimmerman, « Ten strategies of a world-class cybersecurity operations center », in : *MITRE corporate communications and public affairs. Appendices* (2014) (cf. p. 70, 73, 74).

[139] Michael Zyda, *Networked virtual environments : design and implementation*, Addison-Wesley, 1999 (cf. p. 52, 54, 55).

Annexe 1

Fiche de consentement

Cette fiche de consentement a été utilisée lors de notre évaluation de l'utilisabilité présentée dans le Chapitre 5.2.

Fiche de consentement éclairé pour la participation à une expérimentation en réalité virtuelle

Nom de la recherche : 3D Cyber COP

- **Étudiant-chercheur :**
  - Alexandre Kabil, Doctorant
    - IMT Atlantique / Lab-STICC

- **Chercheurs responsables :**
  - Thierry Duval, Professeur
    - IMT Atlantique / Lab-STICC
  - Nora Cuppens, Directrice de recherche
    - IMT Atlantique / Lab-STICC

Organismes subventionnaires : Chaire Cyber CNI

Préambule

Nous vous proposons de participer à un projet de recherche en Sciences de l'Information et de la Communication. Avant d'accepter de participer et de signer ce formulaire, veuillez prendre le temps de lire, de comprendre et de considérer attentivement l'information qui suit ou demander qu'on vous la lise.
Ce formulaire peut contenir des mots que vous ne comprenez pas. Nous vous invitons à poser toutes les questions que vous jugerez utiles à l'étudiant-chercheur ou aux autres membres du personnel affectés au projet de recherche afin de vous expliquer tout mot ou renseignement qui n'est pas clair pour vous. Si vous décidez de participer, nous vous demandons de signer ce formulaire. Un exemplaire vous sera remis.

Nature et but du projet de recherche

La numérisation croissante des entreprises améliore certaines pratiques mais augmente de façon exponentielle les vecteurs d'attaques informatiques.
Les conséquences de ces dernières sont multiples, allant de la perte d'informations à l'arrêt de services mettant en danger des vies humaines.
La difficulté de la sécurisation des systèmes informatiques (ou cybersécurité) provient de l'hétérogénéité des données et situations à analyser pour éviter des conséquences critiques.
La réalité virtuelle peut favoriser la compréhension de cyber-attaques en proposant des visualisations adaptées aux besoins et des situations d'entraînement plus immersives.
Notre étude consiste à analyser l'utilisabilité d'un environnement virtuel pour la compréhension d'une situation de potentielle attaque informatique. Bien que les dispositifs d'immersion et d'interaction tels que les casques de réalité virtuelle soient de plus en plus utilisés dans divers domaines pédagogiques, scientifiques ou ludiques, la sécurité informatique est encore frileuse quant à leur utilisation.

Cette étude propose de comprendre quelles sont les représentations de données les plus pertinentes permettant à un utilisateur non expert de déterminer si un réseau informatique est sujet à une attaque ou si les informations recueillies sont des faux positifs.

Nature de la participation demandée et déroulement du projet de recherche

Après avoir signé le présent formulaire, vous commencerez par un tutoriel vous permettant de prendre en main le simulateur.

L'expérimentation en réalité virtuelle consiste à analyser l'état de sécurité d'un système informatique. Vous devrez investiguer des alertes sur des postes de travail et déterminer :

- si les alertes sont des faux positifs ou alors sont la conséquence d'attaques informatiques,
- si les alertes proviennent d'une même attaque informatique ou sont indépendantes.

Pour ce faire, vous aurez à votre disposition trois vues complémentaires vous permettant de récupérer des informations sur les 'assets' du système informatique. Vous devrez ensuite caractériser les alertes, à savoir les **escalader** si vous considérez qu'il s'agit d'attaque ou les **rejeter** s'il s'agit de faux positifs.

La situation simulée est celle d'une potentielle infection du Rançongiciel Wannacry, qui a sévi durant le printemps 2017.
Wannacry s'attaquait aux ordinateurs sous **Windows 7** n'ayant pas reçu le **correctif de sécurité d'Avril 2017**.
Ce rançongiciel chiffre les données du poste de travail, ce qui augmente **la métrique d'entropie** de ce dernier. De plus, il se propage à la manière d'un ver informatique en profitant de failles système, ce qui augmente **la métrique de débit réseau**.
Il est à noter que ces métriques augmentent aussi lors d'un chiffrement programmé des données et lors des sauvegardes, ce qui déclenche des alertes qui doivent alors être considérées comme des **faux positifs**.

Vous allez effectuer des analyses dans trois environnements différents (trois tests). Après chaque analyse, vous devrez répondre à des questions concernant la situation que vous avez analysée et à un questionnaire sur l'utilisabilité des systèmes et sur la 'Cyber Situational Awareness', la capacité à comprendre une situation d'incidents en cybersécurité. Enfin, un questionnaire sur les expérimentations et un autre sur votre expérience utilisateur vous seront fournis .

Le tableau suivant récapitule les étapes de l'expérimentation et donne un ordre de grandeur de la durée des étapes :

Déroulé	**Durée (mn)**
Accueil et signature consentement	15
Scène tutoriel	10
Scène d'expérience en réalité virtuelle : trois fois	10 x 3
Questionnaire utilisabilité et Cyber Situational Awareness : trois fois	5 x 3
Questionnaire final	5
Questionnaire Expérience Utilisateur	5

Risques et avantages

Participer à cette étude peut vous exposer à un risque de cybersickness sur un très court terme, assimilable au mal des transports, car vous allez porter un casque de réalité virtuelle. Votre participation à cette recherche pourrait donc occasionner certains inconvénients de courte durée sur votre système visuel : fatigue et/ou inconfort visuel. Dans ces cas, vous aurez un espace pour vous détendre, vous reposer et vous hydrater. Vous pouvez cesser l'entrevue et l'expérience à tout moment. L'étudiant-chercheur principal vous offrira de poursuivre l'entrevue et l'expérience à un autre moment si vous le désirez.

Les résultats obtenus pourraient contribuer à l'avancement des connaissances en Sciences de l'Information et de la Communication.

Participation volontaire et possibilité de retrait

Votre participation à ce projet de recherche est entièrement volontaire. Vous êtes donc libre de refuser d'y participer. Vous pouvez également cesser de participer à ce projet à n'importe quel moment, sans avoir à donner de raisons, en faisant connaître votre décision à l'étudiant-chercheur du projet.
De même, l'étudiant-chercheur du projet de recherche peut mettre fin à votre participation, sans votre consentement, notamment si vous ne respectez pas les

consignes du projet de recherche ou s'il existe des raisons administratives d'abandonner le projet.
Si vous vous retirez ou êtes retiré(e) du projet, l'information déjà obtenue dans le cadre de ce projet sera conservée aussi longtemps que nécessaire pour assurer l'intégrité de l'étude et respecter les exigences réglementaires.
Toute nouvelle connaissance acquise durant le déroulement du projet qui pourrait affecter votre décision de continuer d'y participer vous sera communiquée sans délai verbalement et par écrit.

Confidentialité

Durant votre participation à ce projet, l'étudiant-chercheur recueillera et consignera dans un dossier de recherche les renseignements vous concernant, mais sans jamais que votre nom soit mentionné. Seuls les renseignements nécessaires pour répondre aux objectifs scientifiques de ce projet seront recueillis.
Tous les renseignements recueillis demeureront strictement confidentiels dans les limites prévues par la Loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. Toutes les mesures seront prises pour s'assurer de la confidentialité de votre dossier, s'il est consulté et toute information collectée demeurera confidentielle. Afin de préserver votre identité et la confidentialité des renseignements, vous ne serez identifiée que par un numéro de code. La clé du code reliant votre nom à votre dossier de recherche sera conservé par l'étudiant-chercheur.
L'étudiant-chercheur du projet utilisera les données à des fins de recherche dans le but de répondre aux objectifs scientifiques du projet décrit dans la présente lettre d'information et de consentement.

Les résultats pourront être publiés dans des revues spécialisées ou faire l'objet de discussions scientifiques, mais il ne sera pas possible de vous identifier.
À des fins de protection, notamment afin de pouvoir communiquer avec vous rapidement, vos noms et prénoms, vos coordonnées et la date de début et de fin de votre participation au projet seront conservés pendant un an après la fin du projet dans un répertoire à part conservé et maintenu par l'étudiant-chercheur.
Vous avez le droit de consulter votre dossier de recherche pour vérifier les renseignements recueillis et les faire modifier au besoin, et ce, aussi longtemps que l'étudiant-chercheur du projet ou l'établissement détiennent cette information.
Cependant, afin de préserver l'intégrité scientifique du projet, vous pourriez n'avoir accès qu'à certains de ces renseignements, une fois votre participation terminée.

Droit du sujet de recherche

En acceptant de participer à ce projet, vous ne renoncez à aucun de vos droits ni ne libérez les chercheurs ou l'établissement (IMT Atlantique) de leur responsabilité civile et professionnelle.

Communication des résultats généraux

Les résultats globaux de cette étude pourront être à votre disposition sur demande, après la fin du projet. La demande devra être faite par écrit auprès de l'étudiant-chercheur.

Personnes Ressources

Si vous avez des questions concernant le projet de recherche ou si vous éprouvez un problème concernant votre participation au projet, vous pouvez communiquer avec l'étudiant-chercheur:

Alexandre Kabil, ***doctorant***

IMT Atlantique

655 Avenue du Technopôle, 29280 Plouzané

alexandre.kabil@imt-atlantique.fr

Si vous avez des questions au sujet de vos droits en tant que participant à une étude de recherche ou si vous avez des plaintes à formuler, vous pouvez communiquer avec l'étudiant-chercheur dont le contact est mentionné ci-avant.

Fait à, le:

Signature du participant:

Annexe 2

Questionnaire SOCs

Le questionnaire suivant a été transmis aux personnels des SOCs des partenaires industriels de la chaire Cyber CNI. Il provient d'un article de D'Amico *et al.* [31].

Questionnaire sur la visualisation pour la cybersécurité

Inspiré de Cyber « **Operator Perspectives on Security Visualization** » d'Anita D'Amico, Laurin Buchanan, Drew Kirkpatrick and Paul Walczak

Ce questionnaire a pour objectif d'établir les préférences de cyberanalystes.

Il nous donnera une base de référence des besoins en visualisation et nous orientera donc sur nos choix de développement.

Afin de ne pas déformer l'étude précédente, les questions et titres de chapitres seront en anglais.

La section 1 contient des phrases générales sur le travail des cyberanalystes, tandis que les sections 2 et 3 contiennent respectivement des phrases générales concernant les visualisations et des phrases spécifiques.

Les questions suivantes sont là pour nous permettre de caractériser les réponses. Elles ne sont pas obligatoires.

Années d'expérience en cybersécurité : ◯ **0 à 5 ans** ◯ **5 à 10 ans** ◯ **10 ans et +**

Age : ◯ **- de 18 ans** ◯ **entre 18 et 25 ans** ◯ **entre 26 et 35 ans** ◯ **entre 36 et 45 ans** ◯ **plus de 45 ans**

Rôle au sein de la structure (remplir champ textuel si autre rôle) :

◯ **Analyste L.1** ◯ **Analyste L.2** ◯ **Analyste L.3**

◯ **SOC Manager** ◯ **Responsable outils** ◯ **Autre**

Les réponses possibles au questionnaire sont les suivantes :

0 : Cannot Respond *(si la question ne vous concerne pas ou que vous n'avez pas d'avis dessus)*

1 : Strongly Disagree

2 : Disagree

3 : Neither

4 : Agree

5 : Strongly Agree

Section 1 : Assertions about the work of defensive cyber operators

1. Some operators limit their inspection of data to *no more than a single day's data* to perform their job.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

2. Some operators search through more than a day's or even a few weeks' worth of data *within their own site* for unusual events or trends.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

3. Some operators search through more than a day's or even a few weeks' worth of data, *including data from external sites*, for unusual events or trends.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

4. Cyber operators often *associate several pieces of information together and add a hypothesis* for why these events are all related.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

5. In many cases, the *attacker-related data is intermingled with a substantial amount of other data*. It can be challenging to find the relevant amidst the irrelevant data.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

6. When analyzing an event or incident, the operator needs to assess the technical impact of the event or incident on the rest of the network. That is, s/he needs to determine what other resources on the network may have been impacted by the malicious activity.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

7. When analyzing an event or incident, the operator needs to assess the *operational impact* of the event or incident. That is, to determine what specific operations, missions, or users may have been impacted by the malicious activity.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

8. Operators often have several monitors on their desks, each depicting different data.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

9. The information displayed on the operator's monitor(s) is his or her *primary view* into whether there is a suspicious event or cyber incident, and of the activities of the attacker.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

10. One of the most important cognitive skills that operators leverage is their ability to mentally fuse data from different sources.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

11. An important feature of the operator's workflow is the series of questions thats/he asks as s/he moves through the analytic process: "Is this legitimate activity?" "How often has this source IP connected to our network?" "Has this destination IP been sending out unusually large payloads?"

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

12. Operators in all roles regularly engage in educating or communicating to others the results of their analyses, via daily briefings at a CERT, on electronic bulletin boards shared by fellow operators, or in training sessions.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

13. Operators are often required to explain why they formed certain hypotheses or took certain actions; this may require the presentation of knowledge that may not be available to all concerned.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Section 2 : General assertions about the state of cyber security visual presentations

1. Classic security tools, such as firewalls and intrusion detection systems, have over time added reporting capabilities and dashboards that are making use of data visualization techniques like charts and graphics.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

2. In general, the visual presentations of data in current cyber security tools do not have adequate interactivity to support data exploration.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

3. When designing visualizations for defensive cyber operators, the designer should assume that *at least two* monitors are available, and use the extra display for depicting different types of information.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

4. Most cyber security visual displays are fairly basic, such as pie charts or bar graphs.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

5. Some cyber security visual displays require several hours to learn how to use effectively. But if the operator learns how to use them, their value is worth the investment of time.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

6. Visualizations are more likely to be added-on to security products later in their design or production, rather than integrated early in the design process.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

7. Visual data presentation is an effective method for training others. For example, if a new operator is unfamiliar with the network topology, and the topology is a critical component of the operator's decision making, then a visual depiction of parts of the network topology can help the new operator learn the topology more rapidly.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

8. Visual data presentation is an effective method for communicating findings to colleagues or laypersons, and/or for documenting decisions for review or justification.

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Section 3 : Specific assertions about the state of cyber security visual presentations

1. Visualizations should interface to multiple data sources, and provide the operator with a common framework for viewing them.

   ◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

2. The distinct tasks and cognitive requirements of each analysis role and analytic stage indicate a need for *role-based visualization aids*.

   ◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

3. The exploration of voluminous data, and the discovery of patterns within that data, can be enabled through visual data presentation.

   ◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

4. A visualization system designed for defensive cyber operators should be able to draw data from various databases or delimited files, and fuse it into a single visualization.

   ◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

5. The data access and visualization system should provide the operator with the opportunity to save data files, visualization workspaces and any reports created with these files, using the analytic question he is trying to answer as the common reference point.

   ◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

6. In formulating and testing hypotheses to explain suspicious activity, operators look at, reorder, highlight, and filter out data from large datasets, looking for patterns and trends.

   ◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

7. To facilitate examination of data from multiple perspectives, visualization systems should provide multiple, coordinated views of the same dataset. When the operator reorders, highlights, or filters data in one view, the other views should automatically morph to correspond to the changes.

   ◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

8. As operators work their way through data, they apply filters either by specifying criteria for accessing data from the database, or by temporarily filtering data at the display.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

9. Operators typically apply a series of filters to reduce data — for example, first filter out all connections where bytes returned = 0, then filter data between .mil IP addresses, then temporarily hide any connections to CNN.com. However, if they get interrupted or distracted, as they are likely to do in a noisy environment, they can lose track of where they are in the exploration of the data.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

10. A simple graphic or table of the filters applied to the data and the displays aids situational awareness by helping operators reorient after distractions.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

11. Visual data presentation can facilitate the rapid comprehension of a sequence of interconnected events, improving understanding of complex relationships.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

12. Threat analysis may be facilitated by *animations and visual replay of events across the network*, from which cyber operators can deduce the progression, speed, or direction of an attack.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

13. By visually depicting the historical activity pattern of a specific attacker, the operator can forecast the next likely action of that attacker.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

14. Visualizations that *combine several types and dimensions of data* may enhance the operator's ability to see patterns and time trends across multiple data sets.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

15. A visualization of the *connections between various entities* can help the operator gain insight into the attacker's activities.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

16. An *animation of a possible path that an attacker could have taken* can help the operator gain insight into the *attacker's activities*.

◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

17. A visualization of the *connections between various entities* and an *animation of a possible path* that an attacker could have taken can help the operator *communicate the sequence of the attacker's actions to others*.

◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

18. Visual data presentation can be very useful for *ad hoc* types of exploration, as certain patterns are easily comprehended when presented graphically.

◯ 0 ◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

DOCTORAT BRETAGNE LOIRE / MATHSTIC

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Titre : CyberCOP 3D : visualisation 3D interactive et collaborative de l'état de sécurité d'un système informatique

Mots-clés : Environnement virtuels collaboratifs, Cybersécurité, Cyber Situational Awareness

Résumé : L'objectif de la thèse était d'étudier l'utilisation d'Environnements Virtuels Collaboratifs (EVC) pour l'analyse de l'état de sécurité de systèmes informatiques, aussi appelée la Cyber Situational Awareness (CSA). Après avoir étudié les modèles et outils de la CSA, nous avons pu visiter les Security Operations Center (SOCs) de quatre partenaires industriels de la Chaire Cyber CNI, afin de mieux cerner les besoins et attentes des cyber analystes. Ces visites ont été effectuées dans le cadre d'un protocole de l'analyse de l'activité collaborative et nous ont permises de proposer un modèle, le CyberCOP 3D. En nous basant sur notre modèle ainsi que sur une modélisation du rançongiciel WannaCry, nous avons développé un EVC pour la cybersécurité ainsi qu'un moteur de scénarisation simplifié permettant à des utilisateurs de concevoir leurs propres scénarios d'analyse d'alertes. Nous avons effectué une évaluation de l'utilisabilité d'un environnement virtuel pour l'analyse d'alertes auprès d'utilisateurs non-experts en cybersécurité.

Title: CyberCOP 3D: Interactive and Collaborative 3D visualization of a system's security state

Keywords: Collaborative Virtual Environments, Cybersecurity, Cyber Situational Awareness

Abstract: The aim of this thesis was to study the use of Collaborative Virtual Environments (CVE) for the analysis of the state of security of computer systems, also called Cyber Situational Awareness (CSA). After studying CSA's models and tools, we have had the opportunity to visit the Security Operations Centers (SOCs) of four industrial partners of the Cyber CNI chair, in order to better understand the needs and expectations of cyber analysts. These visits were made as part of a collaborative activity analysis protocol and have allowed us to propose a model, the 3D CyberCOP. Based on this model and a model of the WannaCry ransomware, we have developed a CVE and a simplified scenario engine that allows users to design their own alert analysis scenarios. We have also performed a usability evaluation of a virtual environment for alert analysis, with a panel of novice users.