Training - Tutorial - How to develop a cybersecurity policy

Véronique Legrand

le cnam
CyberSécurité

LES TD DU MODULE 2

VOTRE EFFORT….

le cnam

Ce document fait partie de l'Unité d'Enseignement SEC101 de 6 ECTS.

Les crédits ECTS représentent un apprentissage fondé sur des acquis d'apprentissage clairement définis ainsi que sur la charge de travail qui leur est associée. La valeur d'1 ECTS représente donc environ 25 à 30 heures de travail « étudiant » réparti entre du face à face, du suivi de TD, de la réalisation de TPs et de l'effort personnel, 1 UE à 6 ECTS représente donc à minima à 150 heures de travail au total. Certaines UE nécessitent plus d'effort que d'autres.
https://fr.wikipedia.org/wiki/Syst%C3%A8me_europ%C3%A9en_de_transfert_et_d%27accumulation_de_cr%C3%A9dits

Le module 2 PSSI représente donc 2 ECTS soient de 50 à 60 heures au total de travail, il se compose de :

- 4 cours comprenant 4 regroupements et du travail personnel estimés au total à 16 heures d'effort « étudiant » ,
- accompagnés de 3 TD
- -- TD1 : , si approfondis à 08:00
- -- TD2 : 14 ateliers : 5h30, si approfondi à 08:00
- -- TD3 : si approfondi à 08:00
- représentant au total 42 heures.

le cnam

TD1 05:45

Atelier 1-1	Atelier 1-2	Atelier 1-3	Atelier 1-4	Atelier 1-5	Atelier 1-6
Effort : 45'	Effort : 15'	Effort : 60'	Effort : 45'	Effort : 120'	Effort : 60'

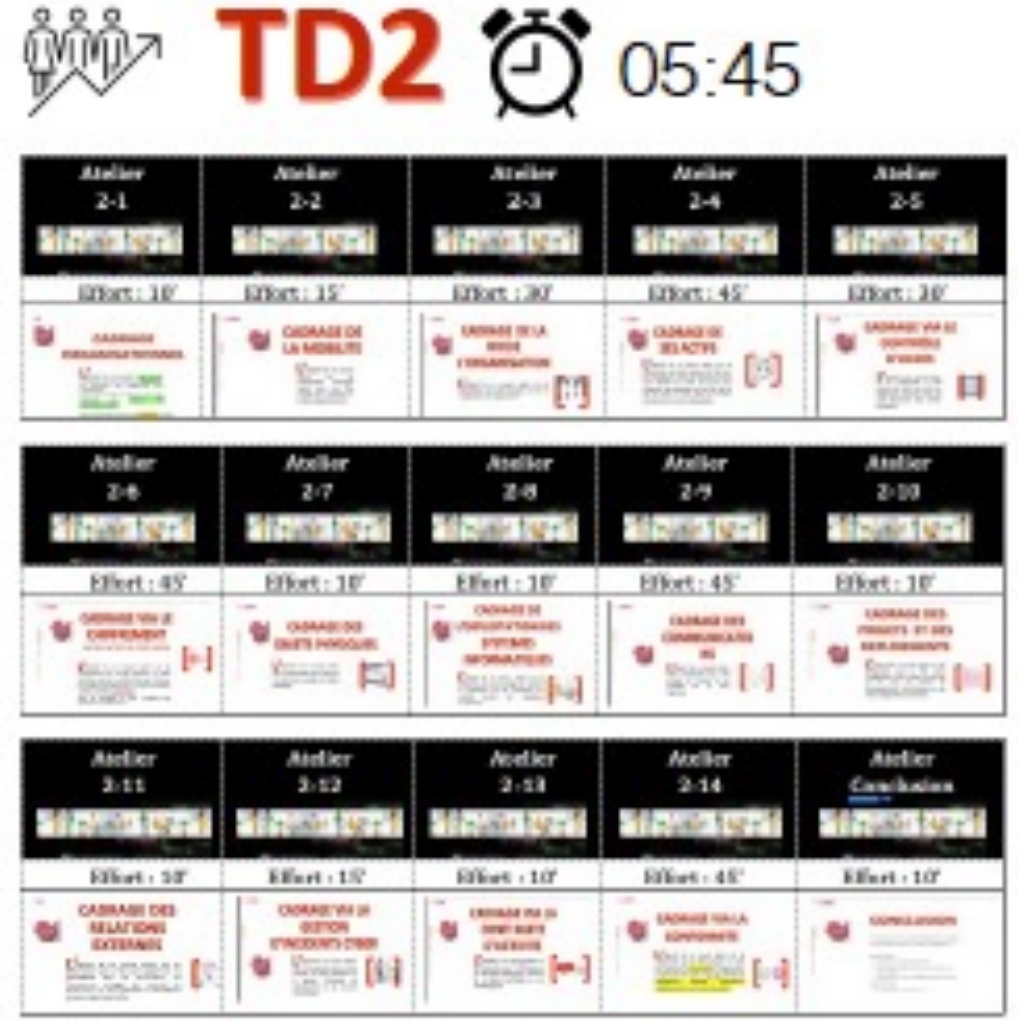
le cnam

TD2 05:45

02:10

02:00

01:30



le cnam

TD3

06:00

le cnam

MODULE 2 – PSSI - TD3

EN AUTONOMIE

OBJECTIFS PEDAGOGIQUES DU TD3

- Détecter des faiblesses d'une infrastructure à partir d'un énoncé
- Élaborer puis évaluer le scénario stratégique
- Identifier les vulnérabilités clés en le traduisant en scenarios opérationnels
- Identifier les exigences techniques correspondant à votre architecture.
- Corriger les faiblesses en sélectionnant les mesures de sécurité d'un référentiel

le cnam

SAVOIR-FAIRE

TRADUIRE LES EXIGENCES ET RÉDIGER

UPMC SORBONNE UNIVERSITÉS	Politique de Sécurité des systèmes d'information	Edition 1

2.16 Protéger les serveurs

Les serveurs hébergent des données sensibles et fournissent des services numériques. Ils représentent des biens essentiels pour le support des activités métiers des agents.

La sécurité des données (disponibilité, intégrité et confidentialité) et des services (disponibilité et intégrité) dépend du niveau de protection des serveurs qui les hébergent.

Les réseaux assurant l'accès aux données et aux services numériques doivent offrir des garanties de disponibilité et d'intégrité.

- Les environnements de développement, de tests et de production sont séparés.

le cnam

OBJECTIFS DU CAS D'ETUDE XGAME GL :

- Au fur et à mesure des ateliers, on apprend à mettre en œuvre les mesures de sécurité afin qu'elles soient adaptées :

1. au problème de vulnérabilité traité,
2. à l'étude de l'architecture technique de GL.

- Un élément déclencheur constitue souvent le point de départ du constat d'une faiblesse et des mesures correctives qui s'en suivent,
- Dans ce travail dirigé, l'énoncé de l'atelier 2 incorpore un élément nouveau du contexte de GL, dans notre cas, il s'agira d'une nouvelle menace.
- Vous apprendrez donc à la prendre en compte tout en vous familiarisant avec les outils et méthodes de l'élaboration des mesures et de leur rédaction

ÉTAPES ET OBJECTIFS DU TD3

le cnam

ATELIER 1 DÉCOUVRIR L'ÉNONCÉ

- appréhende un périmètre (les Actifs concernés)
- relever le contexte actuel de Gameluck,
- relever l'architecture technique
- choix d'une modélisation du problème.

ATELIER 2 ELABORER ET ÉVALUER LA STRATÉGIE DE L'AGENT MENAÇANT

- Principe d'un scénario stratégique
- Perception défensive : connaissance du contexte de l'entreprise (son écosystème, le contexte, l'architecture)
- Perception défensive : évaluation de la gravité de la menace

ATELIER 3 IDENTIFIER LES FAIBLESSES

- Exprimer un scénario opérationnel d'attaque
- En fonction de la cible donnée (ici les données d'innovation).

ATELIER 4 MODÉLISER L'AGENT MENAÇANT

- chemins d'attaques de l'attaquant,
- conclure sur les vulnérabilités.

ATELIER 5 EXTRAIRE LES ÉLÉMENTS À CORRIGER

- à partir des agents menaçants
- dans le contexte de Gameluck .

ATELIER 6 APPLIQUER LES MESURES : RECONFIGURER L'ARCHITECTURE

- sélectionner la mesure
- ajout d'un VLAN
- règles de firewall
- authentification.

le cnam

PRENEZ AVEC VOUS....

1 2 3 4

Les ateliers Gameluck présentent le cas d'étude de l'entreprise Gameluck, éditeur de logiciel de jeux videos, dont l'architecture technique est vulnérable.

Ces ateliers présentent l'utilisation conjointe de plusieurs outils et méthodes pour corriger cette architecture vulnérable:

- analyse de risque,
- référentiel ISO27002
- éléments de contexte donnés dans l'énoncé
- cahier des charges.

PRENEZ AVEC VOUS....

1. Le cahier des charges GameLuck
2. L'exemple de la PSSI UPMC (Université Pierre et Marie Curie)
3. L'exemple de la PSSI Université de Poitiers
4. L'ISO 27002

le cnam

UN JEU DE RÔLES

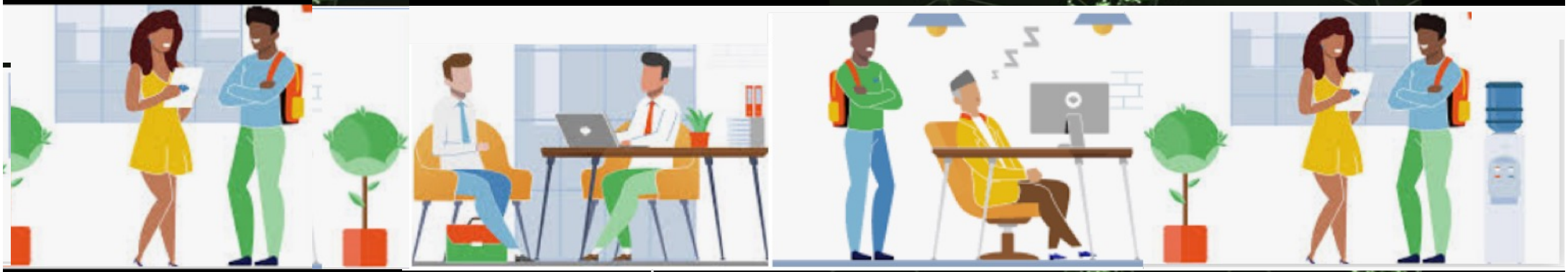
CONSULTANT APPELE PAR DIRIGEANT

Vous : vous êtes consultant, en charge de la mission de sécurisation de GL, vous avez pris connaissance du CdC de GameLuck et découvrez ces nouveaux éléments du contexte qui vous seront donnés par le dirigeant de GL au travers de l'énoncé.

DIRIGEANT

Atelier

1



le cnam

le cnam

ATELIER 1 GAMELUCK

ÉNONCÉ DU CAS D'ÉTUDE XGAME

Ce premier atelier a pour but de présenter les phases 0 (référentiel) & 1 (éléments stratégiques) ou de contexte pris en compte dans la correction des faiblesses.

OBJECTIF DE L'ANALYSE

XGAME

le cnam

ENONCE PAR LE DIRIGEANT

L'une des valeurs métier de GL repose sur son processus d'innovation, l'application XGame est l'une des applications coeur-métier de GL, elle est particulièrement sensible, puisque le jeu très attendu des Gamers, devrait très prochainement accaparer le marché.

Le résultat que nous recherchons sera une architecture technique plus robuste pour notre processus d'innovation.

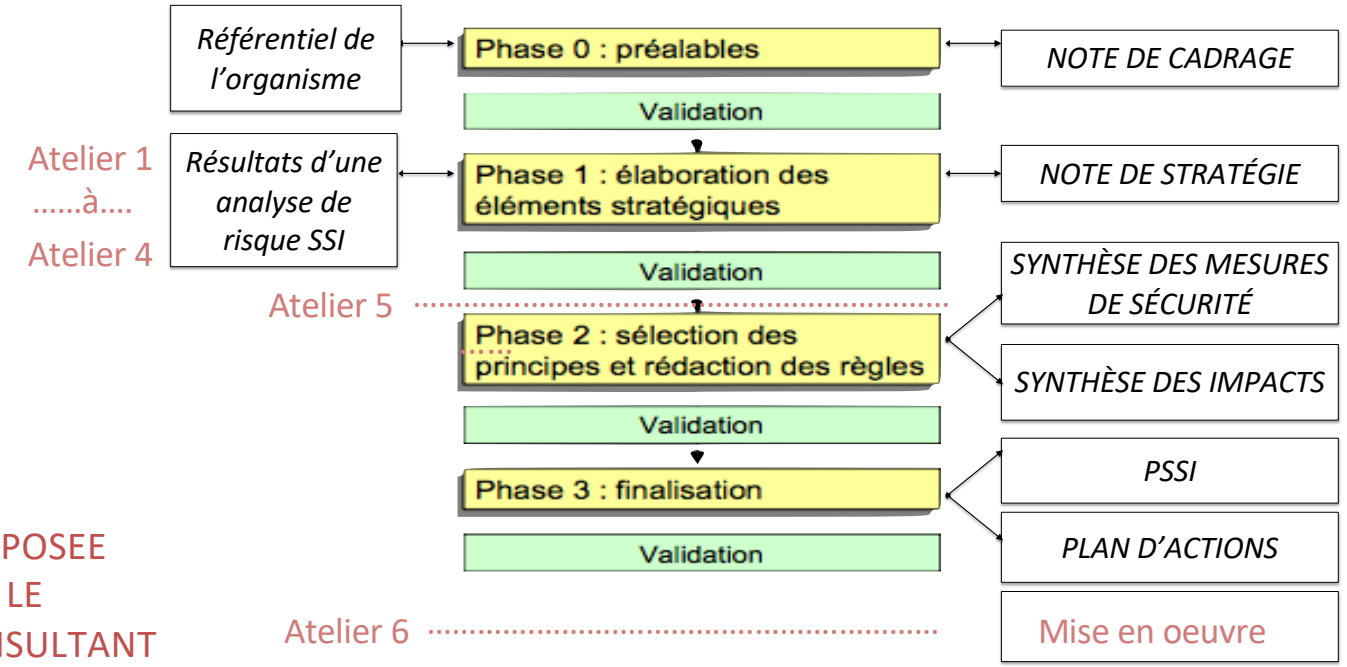
CONSULTANT

METHODE D'ANALYSE ANNONCEE

le cnam

Afin de faciliter la compréhension, la démarche suivra les étapes de la méthode EBIOS, abordée en cours et rappelée ici.

PROPOSEE PAR LE CONSULTANT



PROBLEME POSE

le cnam

ENONCE PAR LE DIRIGEANT

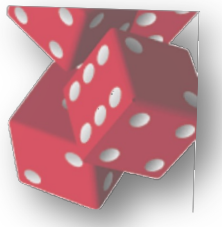
Fin 2021, Abim Velox, le super Gamer de GL conduit le nouveau projet de jeu video 3 D appelé XGame.

À peine cinq ans après son embauche chez GL, Abim Velox présente son tout nouveau scénario, hyper riche, avec une équipe bien plus étoffée qu'à ses débuts chez GL.

Abim Velox revient sur les devants de la scène avec la sortie de XGame. Le jeu a plein de belles nouveautés comme un jeu de plateforme en 3D, en réseau, hyper fluide et toujours avec cet univers très particulier, très riche et très pur.

Le logiciel est entré depuis quelques jours dans son dernier cycle de développement, la concurrence, de plus en plus vive, très à l'écoute, essaie d'obtenir de l'information sur ce nouveau logiciel de jeu afin d'anticiper sa sortie, les fêtes de Noel sont un enjeu de taille.

Nous vous demandons à vous notre conseiller d'étudier les mesures de sécurité adaptées à notre préoccupation actuelle, protéger notre processus « innovation » des éventuelles fuites ou de vols d'informations comme en 2017…



PROBLEME POSÉ

QUELS ÉLÉMENTS DE L'ARCHITECTURE TECHNIQUES (ACTIFS) SONT CONCERNÉS PAR XGAME ?

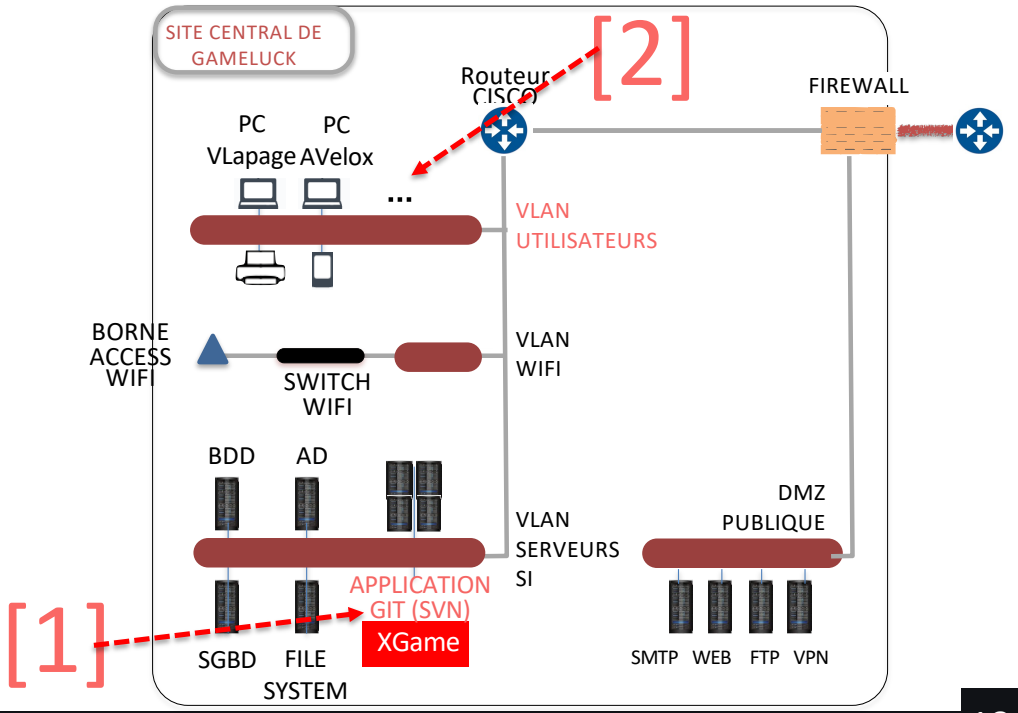
le cnam

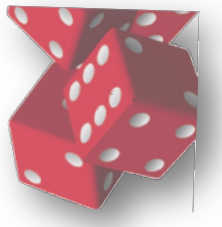
[1] l'application XGame est hébergée sur le GIT(SVN)* du service développement R&D.

[2] l'ensemble de l'équipe de développement travaille sur le VLAN « utilisateurs » à partir de leurs postes de travail .

Comme indiqué dans le cahier des charges

RELEVE PAR LE DIRIGEANT (AUDIT TECHNIQUE)





PÉRIMÈTRE RETENU

VALEURS MÉTIERS & BIENS SUPPORTS

le cnam

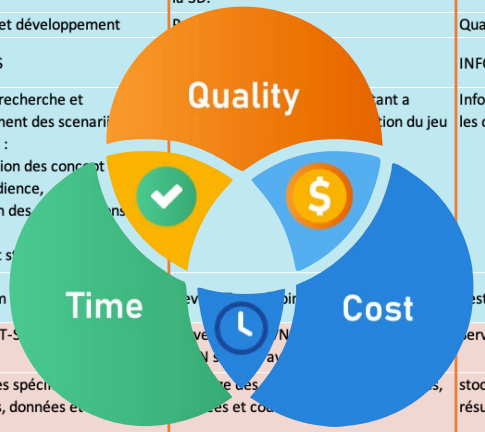
Voici le processus d'innovation de Gameluck avec les différents composants pour produire un jeu.

On voit les valeurs métiers (activités, sous-processus et processus), les biens supports de ces valeurs métiers et leurs responsables respectifs.

Notre intervention se situera à l'intérieur de ce périmètre, nous devons détecter les facteurs de la menace sur les activités de GameLuck !!!

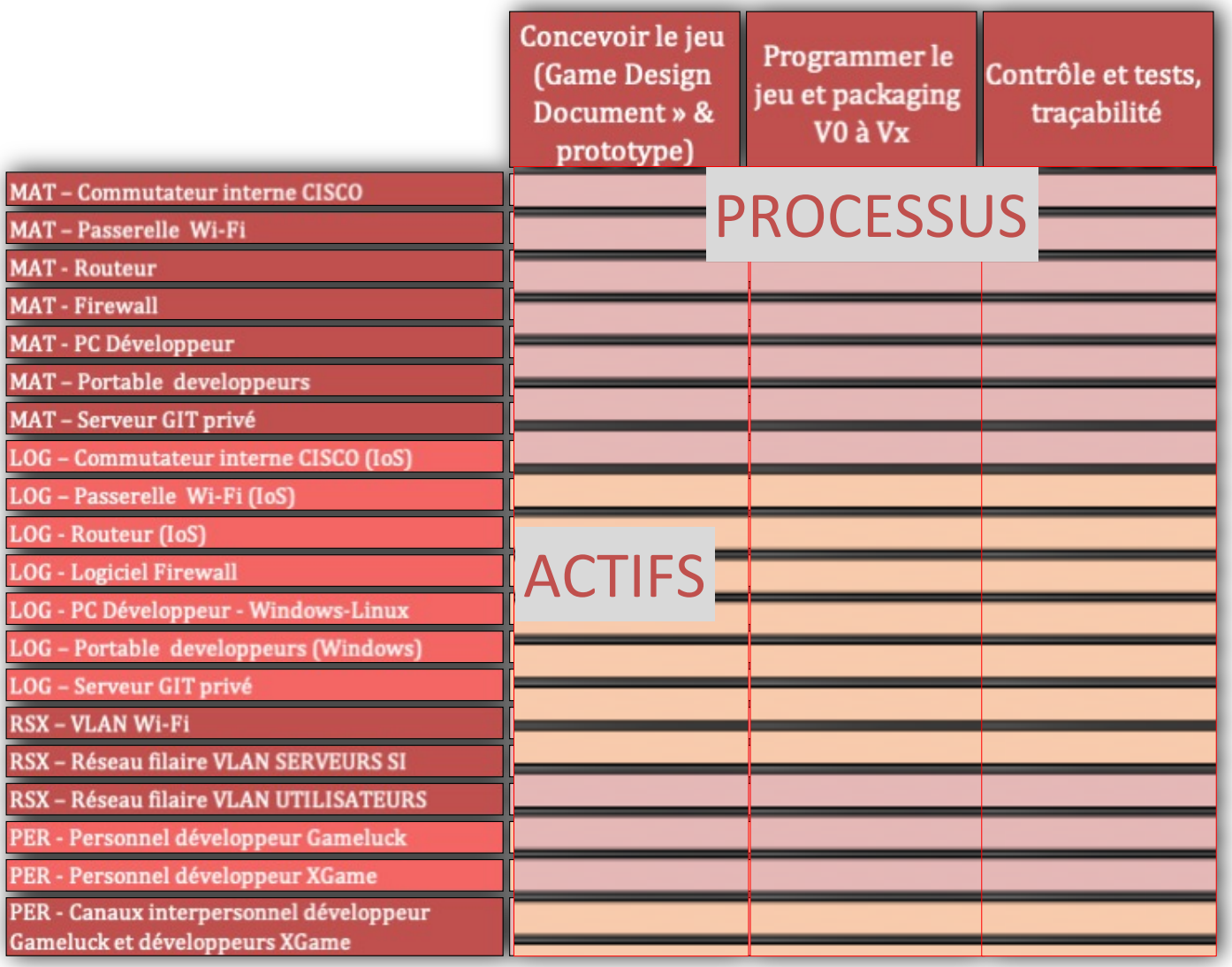
RELEVE PAR LE DIRIGEANT (AUDIT TECHNIQUE)

PROCESSUS "INNOVATION" DE GAMELUCK			
MISSION	Concevoir le jeu (Game Design Document » & prototype)	Programmer le jeu et packaging V0 à Vx	Contrôle et tests, traçabilité
DESCRIPTION GLOBALE	Cette activité permet de concevoir l'application en décrivant : le scénario du jeu, le genre, l'univers, l'audience visée, les objectifs, la mécanique, la stratégie marketing, elle permet également de produire une version de prototype (MVP).	Cette activité permet de produire le logiciel à l'aide de framework de programmation et langages. Abim Velox utilise Unity (propriétaire avec C#) et Godot Engine (moteur open-source et langage GDScript(python)), toutes les plateformes, et est capable de développer des jeux video 2D comme de la 3D.	Informations permettant d'assurer les controles qualité
DÉNOMINATION DE LA VALEUR MÉTIER	Recherche et développement		Qualité logicielle
NATURE DE LA VALEUR MÉTIER (PROCESSUS OU INFORMATION)	PROCESSUS		INFORMATION
DESCRIPTION	Activité de recherche et développement des scenari… nécessitant : - identification des concept… univers, audience, - production des … détaillées - partage et s…	…tant a …tion du jeu	Informations permettant d'assurer les controles qualité
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE)	Studio Team		…sts (Abim Velox et AdjarCarbon)
DÉNOMINATION DU/DES BIENS SUPPORTS ASSOCIÉS	Serveurs GIT-S…	…ve… …N… …av…	…erveurs GIT-SVN internes
DESCRIPTION	stockage des spéci… algorithmes, données e… logicielss	…re des …és et co… …s,	stockage des évènements et des résultats de tests
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE)	GSIT	GSIT	GSIT



le cnam

CARTOGRAPHIE DES ACTIFS

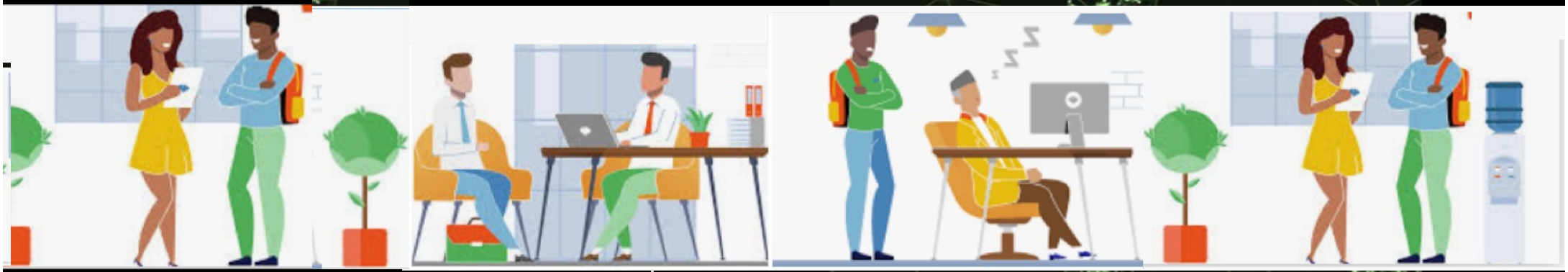


le cnam

CONCLUSION

L'atelier a permis de découvrir l'énoncé expliquant le contexte actuel de Gameluck, de rappeler l'architecture technique et de présenter comment on appréhende un périmètre à prendre en compte dans l'analyse de sécurité à effectuer.

Atelier 2



le cnam

le cnam

ATELIER 2 GAMELUCK AGENTS DE LA MENACE

Ce second atelier rappelle les menaces génériques qui pèsent sur Gameluck en fonction du périmètre retenu.

Il décrit ensuite un état de la menace qui pèse actuellement sur GameLuck, ses nouveaux enjeux et craintes, ainsi que quelques tendances pour mieux cerner cette menace.

Enfin, l'atelier montre un exemple de menace de type « signaux faibles » et comment l'analyse de risque peut prendre en compte ces agents menaçant particuliers.

CONSULTANT

ÉTAT DE LA MENACE

le cnam

1) À PARTIR DES ACTIFS ET DE L'ARCHITECTURE TECHNIQUE

La méthode EBIOS a fourni une liste générique des menaces par typologie de biens supports

TYPE		
M1. MAT-USG	MENACES SUR LES MATÉRIELS	Détournement de l'usage prévu d'un matériel
M2. MAT-ESP		Espionnage d'un matériel
M3. MAT-DEP		Dépassement des limites de fonctionnement d'un matériel
M4. MAT-DET		Détérioration d'un matériel
M5. MAT-MOD		Modification d'un matériel
M6. MAT-PTE		Perte d'un matériel
M7. LOG-USG	MENACES SUR LES LOGICIELS	Détournement de l'usage prévu d'un logiciel
M8. LOG-ESP		Analyse d'un logiciel
M9. LOG-DEP		Dépassement des limites d'un logiciel
M10. LOG-DET		Suppression de tout ou partie d'un logiciel
M11. LOG-MOD		Modification d'un logiciel
M12. LOG-PTE		Disparition d'un logiciel
M13. RSX-USG	MENACES SUR LES CANAUX INFORMATIQUES ET DE TÉLÉPHONIE	Attaque du milieu sur un canal informatique ou de téléphonie
M14. RSX-ESP		Écoute passive d'un canal informatique ou de téléphonie
M15. RSX-DEP		Saturation d'un canal informatique ou de téléphonie
M16. RSX-DET		Dégradation d'un canal informatique ou de téléphonie
M17. RSX-MOD		Modification d'un canal informatique ou de téléphonie
M18. RSX-PTE		Disparition d'un canal informatique ou de téléphonie
M19. PER-USG	MENACES SUR LES PERSONNES	Dissipation de l'activité d'une personne
M20. PER-ESP		Espionnage d'une personne à distance
M21. PER-DEP		Surcharge des capacités d'une personne
M22. PER-DET		Dégradation d'une personne
M23. PER-MOD		Influence sur une personne
M24. PER-PTE		Départ d'une personne
M25. PAP-USG	MENACES SUR LES SUPPORTS PAPIER	Détournement de l'usage prévu d'un support papier
M26. PAP-ESP		Espionnage d'un support papier
M27. PAP-DET		Détérioration d'un support papier
M28. PAP-PTE		Perte d'un support papier
M29. CAN-USG	MENACES SUR LES CANAUX INTERPERSONNELS	Manipulation via un canal interpersonnel
M30. CAN-ESP		Espionnage d'un canal interpersonnel
M31. CAN-DEP		Saturation d'un canal interpersonnel
M32. CAN-DET		Dégradation d'un canal interpersonnel
M33. CAN-MOD		Modification d'un canal interpersonnel
M34. CAN-PTE		Disparition d'un canal interpersonnel

ÉTAT DE LA MENACE

le cnam

Au regard de l'architecture technique exposée ci-dessus, nous avons analysé la source de menace sur les cibles.

Seront visés potentiellement :
- Le serveur GIT sur le VLAN Serveurs SI
- Les postes de travail de l'équipe d'Abim Velox sur le VLAN utilisateurs.

Menaces et vulnérabilités génériques

TYPE		
M1. MAT-USG	MENACES SUR LES MATÉRIELS	Détournement de l'usage prévu d'un matériel
M2. MAT-ESP		Espionnage d'un matériel
M3. MAT-DEP		Dépassement des limites de fonctionnement d'un matériel
M4. MAT-DET		Détérioration d'un matériel
M5. MAT-MOD		Modification d'un matériel
M6. MAT-PTE		Perte d'un matériel
M7. LOG-USG	MENACES SUR LES LOGICIELS	Détournement de l'usage prévu d'un logi
M8. LOG-ESP		
M9. LOG-DEP		
M10. LOG-DET		
M11. LOG-MOD		
M12. LOG-PTE		
M13. RSX-USG	MENACES SUR LES CAN INFORMATIQUES ET TÉLÉPHONIE	
M14. RSX-ESP		
M15. RSX-DEP		
M16. RSX-DET		
M17. RSX-MOD		
M18. RSX-PTE		
M19. PER-USG	MENACES SUR LES PERSON	
M20. PER-ESP		
M21. PER-DEP		
M22. PER-DET		
M23. PER-MOD		
M24. PER-PTE		
M25. PAP-USG	MENACES SUR LES SUPP PAPIER	
M26. PAP-ESP		
M27. PAP-DET		
M28. PAP-PTE		
M29. CAN-USG	MENACES SUR LES CAN INTERPERSONNELS	
M30. CAN-ESP		Espionnage d'un canal interpersonnel
M31. CAN-DEP		Saturation d'un canal interpersonnel
M32. CAN-DET		Dégradation d'un canal interpersonnel
M33. CAN-MOD		Modification d'un canal interpersonnel
M34. CAN-PTE		Disparition d'un canal interpersonnel

	Concevoir le jeu (Game Design Document » & prototype)	Programmer le jeu et packaging V0 à Vx	Contrôle et tests, traçabilité
MAT – Commutateur interne CISCO	M1 à M6	M1 à M6	M1 à M6
MAT – Passerelle Wi-Fi	M1 à M6	M1 à M6	M1 à M6
MAT - Routeur	M1 à M6	M1 à M6	M1 à M6
MAT - Firewall	M1 à M6	M1 à M6	M1 à M6
MAT - PC Développeur	M1 à M6	M1 à M6	M1 à M6
MAT – Portable developpeurs	M1 à M6	M1 à M6	M1 à M6
MAT – Serveur GIT privé	M1 à M6	M1 à M6	M1 à M6
LOG – Commutateur interne CISCO (IoS)	M7 à M12	M7 à M12	M7 à M12
LOG – Passerelle Wi-Fi (IoS)	M7 à M12	M7 à M12	M7 à M12
LOG - Routeur (IoS)	M7 à M12	M7 à M12	M7 à M12
LOG - Logiciel Firewall	M7 à M12	M7 à M12	M7 à M12
LOG - PC Développeur - Windows-Linux	M7 à M12	M7 à M12	M7 à M12
LOG – Portable developpeurs (Windows)	M7 à M12	M7 à M12	M7 à M12
LOG – Serveur GIT privé	M7 à M12	M7 à M12	M7 à M12
RSX – VLAN Wi-Fi	M13 à M18	M13 à M18	M13 à M18
RSX – Réseau filaire VLAN SERVEURS SI	M13 à M18	M13 à M18	M13 à M18
RSX – Réseau filaire VLAN UTILISATEURS	M13 à M18	M13 à M18	M13 à M18
PER - Personnel développeur Gameluck	M19 à M24	M19 à M24	M19 à M24
PER - Personnel développeur XGame	M19 à M24	M19 à M24	M19 à M24
PER - Canaux interpersonnel développeur Gameluck et développeurs XGame	M29 à M34	M29 à M34	M29 à M34

ÉTAT DE LA MENACE

le cnam

2) À PARTIR DU CONTEXTE ET DE L'HISTOIRE DE GAMELUCK

En 2015, je rencontrais dans un Game le célèbre développeur Abim Velox.

Séduit par son approche novatrice dans la conception des jeux video, je lui proposais de rejoindre GL, il accepta.

En 2016, Abim Velox créait la surprise avec son studio GameLuck et notre petite équipe, il sort le séduisant jeu ZGame, considéré par beaucoup comme l'un des jeux les plus révolutionnaires, son titre « Z » aura marqué les esprits avec son univers très particulier, ses couleurs choisies avec soin et sa musique envoûtante.

ÉTAT DE LA MENACE

le cnam

2) À PARTIR DU CONTEXTE ET DE L'HISTOIRE DE GAMELUCK

À peine cinq ans plus tard, Abim Velox revient avec son équipe un peu plus robuste pour la sortie de XGame, avec des belles nouveautés comme un jeu de plateforme en 3D toujours avec cet univers très particulier et un scénario hyper riche, et surtout un nouveau personnage, envoutant…

Le logiciel est entré depuis quelques jours dans son dernier cycle de développement, la concurrence, de plus en plus vive, est très à l'écoute et essaie d'obtenir de l'information sur notre nouveau logiciel de jeu afin d'anticiper sa sortie, les fêtes de Noel sont un enjeu de taille pour nous tous.

En 2017, l'année qui a suivi son arrivée à GL, Abim Velox portait son ZGame sur une plateforme 3D, il créa ainsi YGame, un jeu video de toute dernière génération, toujours avec ce même univers soigné.
Mais drame, à cette époque, YGame se voit quasi phagocyté par un jeu concurrent, HideWorks, également en 3D avec un univers assez proche de YGame. Malgré un scénario bien moins avancé, mais avec des moyens colossaux, YGame n'a pas résisté à l'époque,
Gameluck n'a jamais su si les ressemblances frappantes avec son jeu avaient été le fruit d'une concurrence trop à l'écoute. …

YGame est un jeu innovant, en plein développement

YGame est un jeu innovant, en plein développement

Images tirées de Attack on Titan 2 / A.O.T. 2 - Costumes Eren et Levi//Gamekult

Oui, c'est à ce moment là que je suis intervenu pour la première fois chez GL.

La presse venait de reléguer un peu durement quelques explications qui nous ont causé problèmes

Accueil > News > Cybersécurité

Gameluck, victime de chantage au vol de données

Sécurité : *Le groupe Egregor revendique l'attaque et a également menacé de divulguer le code source de YGame, un jeu de Gameluck.*

ZDNet

Par Catalin Cimpanu | Vendredi 16 Octobre 2017

Réactions 0 | Partager 18 | Tweeter | Partager | plus +

Oui, c’est à ce moment là que je suis intervenu pour la première fois chez GL.

La presse venait de reléguer un peu durement quelques explications qui nous ont causé problèmes

Un groupe cybercriminel utilisant le site de diffusion Egregor a divulgué des données qu'il prétend avoir obtenues à travers le piratage des réseaux internes de deux éditeurs majeurs de jeux vidéo, Gameluck et RubiWare.

Fuites de données

Les données ont été publiées mardi sur un site en .onion tenu par le groupe cybercriminel. Les détails sur la manière dont le groupe Egregor a obtenu les données restent flous. Cependant, dans de nombreux cas, les groupes se font également détecter et expulser des réseaux pendant le processus d'exfiltration des données, et les fichiers ne sont jamais chiffrés. Néanmoins, ils continuent d'extorquer les entreprises victimes, en demandant aux victimes de l'argent en échange, ils ne divulgueront pas les fichiers sensibles. Habituellement, lorsque les négociations échouent, les groupes rançongiciels affichent une fuite partielle des fichiers volés sur des sites dédiés désignés sous le nom de « leak sites ».
Ce mardi, des fuites de données concernant Gameluck et RubiWare ont été publiées sur le portail Egregor, assorties de menaces promettant la publication d'autres fichiers dans les jours à venir.

Images tirées de Attack on Titan 2 / A.O.T. 2 - Costumes Eren et Levi//Gamekult

Les hacktivistes sont également une menace.

Récemment, certains ont bloqué Titanfall, ils n'aiment pas les jeux video surtout quand ces derniers parlent « mal » des hackers !!!.

DES HACKERS ONT PRIS LE CONTRÔLE D'APEX LEGENDS… POUR SE PLAINDRE DES HACKERS DE TITANFALL

CITIZEN ERASED - 5 JUILLET 2021 0

Hacktivistes

C'est un drôle de dimanche qu'on passé les joueurs d'Apex Legends, hier : pendant une demi-douzaine d'heures, il a été **impossible de lancer une partie**. Et pour cause : **les serveurs de matchmaking du free-to-play ont été piratés**.

Coincés dans le lobby, **les joueurs d'Apex Legends** étaient invités à **visiter** SaveTitanfall.com, détaillant les revendications des pirates. Ce qui pouvait sembler être **un acte malveillant** de plus serait en réalité **un happening** pour mettre en lumière les soucis que rencontrent **le premier Titanfall**, pratiquement devenu injouable à cause **des tricheurs**, **bots** et **chutes des serveurs** qui peuvent parfois mettre des semaines à **revenir en ligne**.

> *Titanfall est une franchise bien-aimée par beaucoup, et les problèmes de pirates n'ont fait qu'augmenter. La communauté Titanfall supplie Respawn de résoudre ce problème depuis plus de trois ans, mais en vain. Aujourd'hui ce jeu est toujours en vente, tout en étant totalement injouable. Il est temps de parler.*

Le site serait en ligne **depuis quelques temps** maintenant, et les hackers — **encore non-identifiés** — ont trouvé que c'était une bonne idée de pirater **le jeu le plus populaire de Respawn Entertainment** pour rediriger un maximum de monde dessus. Reste à déterminer si le site a un lien avec **cette opération de détournement**.

> *Titanfall 1 est attaqué, alors Apex aussi.*

Dans les bonnes nouvelles, Respawn affirme que le piratage n'a pas mis en danger **les informations personnelles** des joueurs.

Images tirées de Attack on Titan 2 / A.O.T. 2 - Costumes Eren et Levi//Gamekult

ANALYSE DES AGENTS MENAÇANTS DE GL

EBIOS Risk Manager – Formation

le cnam

Nous devons connaitre les agents menaçants (quels sont-ils), leurs motivations (quels sont leurs objectifs ?), leurs chances de réussites ?

Nous devons évaluer leur chances de réussite à partir des éléments que nous connaissons :

- Statistique du fait, le même ou similaire dans le passé
- Quelles sont les circonstances et conditions générales et particulières du fait, à l'époque,
- Ces conditions sont-elles réunies actuellement ?
- Quel est le fait générateur à l'époque, existe-t-il UN TEL FAIT actuellement ?
- Observons nous des signaux faibles de TOUT OU PARTIE DE LEUR présence ?

Au vu de l'actualité passée et présente, nous pouvons poser ce tableau de synthèse.

SOURCE DE RISQUE	OBJECTIF VISÉ	MOTIVATION	MOYENS/RESSOURCES	PERTINENCE	on mesure les statistiques, les signaux faibles venant de l'extérieur et de l'intérieur, on note d'investiguer si besoin
concurrent	voler des informations pour empecher le jeu de sortir	très forte	importants	- des cas similaires dans l'actualité de 2017 - un marché lucratif à l'approche de noel - pas de signaux faible avérés - conditions présentes	
concurrent	voler des informations pour reproduire le jeu	très forte	importants	- des cas similaires dans l'actualité de 2017 - un marché lucratif à l'approche de noel - pas de signaux faible avérés - conditions présentes	
interne	voler des informations pour reproduire le jeu	faible	faible	- pas de cas similaires - besoin d'argent et l'approche des fêtes - pas de signaux faible avérés - pas de conditions présentes	
hactiviste	empecher la sortie de jeux video Sabotage	selon le contexte, signaux faibles à surveiller	importants par essence	- pas de hacking dans Xgame - les conditions ne sont donc pas réunies	https://www.warlegend.net/hack-matchmaking-apex-legends-triche-titanfall/

très forte : l'agent passera à l'acte, ses avantages sont plus élervé que ce qu'il encourt, les conditions sont réunies pour que le fait se produise de façon quasi certaine, le passé présente des faits similaires, des signaux faibles se sont manifestés, les facteurs de l'exploit sont présents
forte : l'agent passera probablement à l'acte, ses avantages sont équivalent à ce qu'il encourt, le fait se produit de façon règulière, les conditions de l'exploit sont quasi présentes, des signaux faibles sont possibles même s'ils sont difficiles à interpréter et qu'il peut etre une collecte d'informations supplémentaires est requise.
moyenne : l'agent voit une trop grosse différence entre ce qu'il tirera de son méfait et ce qu'il lui rapportera, néanmoins, le fait s'est produit dans le passé, certe 1 ou quelque fois, sans répétition systématique ou regle, attentif, aux signaux faibles néanmoins
faible : le fait s'est peu produit, les risques de l'agent sont trop élévés au regard de ce qu'il en tire, les facteurs de réussite d'une telle attaque ne sont pas réunis à notre connaissance.

ACTIONS POTENTIELLEMENT MENAÇANTES SUR L'ACTIVITÉ INNOVANTE DE GL

le cnam

Nous devons anticiper les actions qui pourraient menacer notre activité innovante.

Nous devons mieux comprendre contre quelles menaces nous devons nous protéger, prioriser celles qui auront un impact grave sur notre activité. Clairement, la conception de notre MVP est en jeu, ne pas exposer le MVP est notre priorité.

Mais nous devons mieux connaître la menace

VALEUR METIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIE D'IMPACT	GRAVITÉ SUR 4
R&D **Concevoir le jeu**	Vol d'informations ou fuites d'information en conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes	-Impacts sur le patrimoine intellectuel -Impacts financiers énormes en pleine période	4
R&D **Concevoir le jeu**	Perte ou destruction du prototype MVP	Impacts financiers impacts sur l'image et la confiance	3
R&D **Concevoir le jeu**	Perte ou destruction du prototype	- Impacts sur le patrimoine intellectuel - Impacts financiers énormes en pleine période	2
DevOpsTeam **Développer (coder) le jeu**	Perte ou destruction des informations	- en pleine période de vente de Noel	2

4 : le cout de l'impact est très élevé pour l'organisation, les dommages menance la continuité d'activité de façon irréversible, catastrophique, l'organisation passera pas le cap si cet événement se produit
3 : le cout de l'impact est élevé pour l'organisation, les dommages seront serieux sur l'activité, les finances, l'image et/ou les biens propres ou la propriété intellectuelle, l'organisation se relèvera néanmoins avec des traces.
2 : le cout de l'impact est moyen pour l'organisation, les dommages ne menacent pas la continuité d'activité, la santé des finances, l'image et/ou les biens propres ou la propriété intellectuelle
1 : le cout de l'impact est faible pour l'organisation, les dommages n(ont pas d'influence (p être faible) sur la continuité d'activité, la santé des finances, l'image et/ou les biens propres ou la propriété intellectuelle

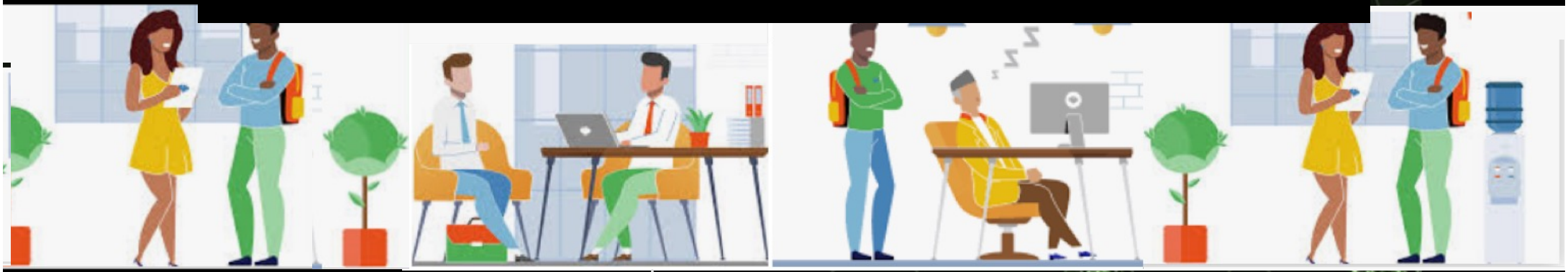
le cnam

CONCLUSION

L'atelier a permis de comprendre le contexte de Gameluck afin d'appréhender ensuite la menace, vous découvrez les éléments clé de la menace.

Vous allez apprendre comment générer un scénario stratégique qui vous permettre de comprendre et évaluer ce qu'il peut se passer.

Atelier 3



le cnam

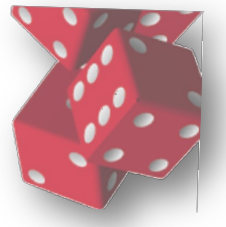
le cnam

le cnam

ATELIER 3 SCÉNARIO STRATÉGIQUE POUR XGAME

L'objectif de ce nouvel atelier est de déterminer les scénarii stratégiques sur le processus « innovation » de GameLuck avec son jeu XGame en cours de sortie.

Le travail présenté dans cet atelier sera la transformation en scénario stratégique, avec en entrée : les éléments de contexte de l'Atelier 1 et la méthode EBIOS pour vous guider, en sortie vous obtiendrez un scénario stratégique que pourrait emprunter l'agent menaçant.

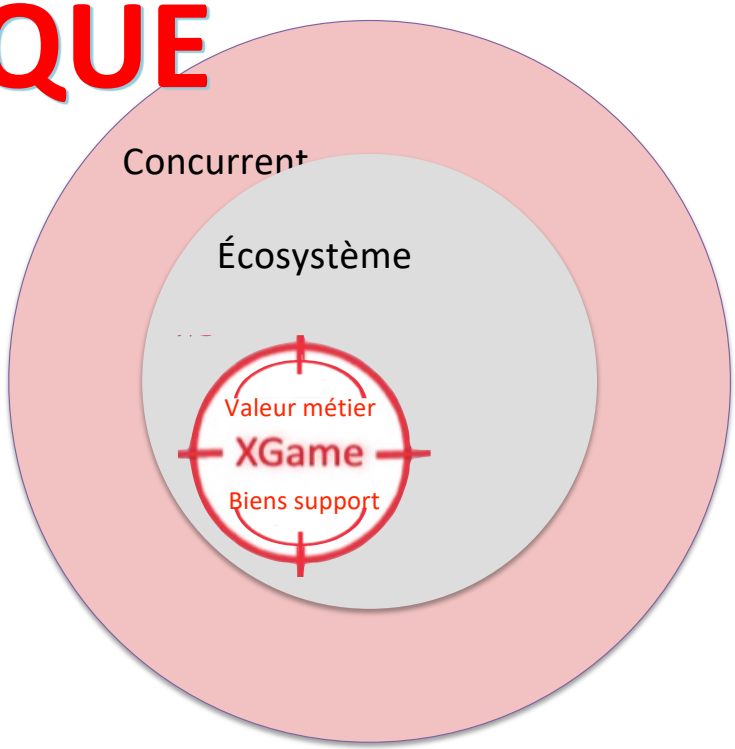


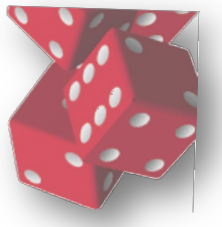
ÉLABORER UN SCÉNARIO STRATÉGIQUE

le cnam

Dans le scénario « concurrence » identifié lors de l'atelier précédent, il reste à identifier les différents éléments et leurs relations au niveau stratégique (c'est-à-dire ceux qui ont une valeur pour l'entreprise ou au contraire pour l'agent menaçant et qui seront également susceptibles de jouer un rôle dans le scénario d'attaque ou de défense).

On repèrera :
- 1/ les accès directs
- 2/ les vecteurs





ÉLABORER UN SCÉNARIO STRATÉGIQUE

le cnam

Identifier « cible » et « attaquant » potentiels :
- Le concurrent: c'est le 1er élément, il est de base dans le scénario que nous étudions,
- XGame : c'est la cible, il attire le concurrent

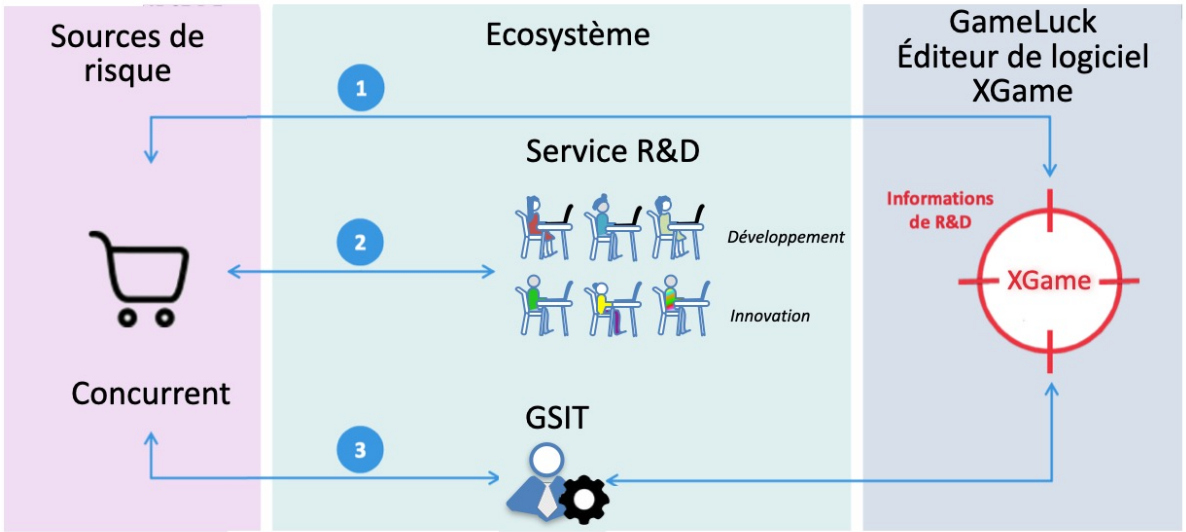
Poser les chemin d'attaque :

- Chemin d'attaque 1 : direct, le concurrent et XGame ont une relation directe (attirance), donc le concurrent peut atteindre directement XGame .

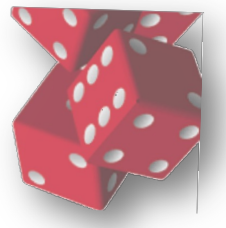
- Chemin d'attaque 2 : via un vecteur générique - l'écosystème - qui les sépare, l'écosystème est en lien direct avec la cible - XGame - via les développeurs innovation ou non qui peuvent accéder au GIT (code).

- Chemin d'attaque 3 : via l'écosystème également, tout ou partie de l'équipe du GSIT peut être approchée par le concurrent.

Objectif visé : voler les informations de R&D de Gameluck



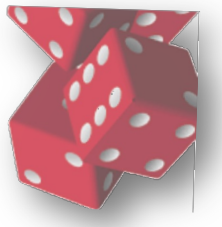
Scenarii stratégiques composés de 3 chemins d'attaques



GRAVITÉ

- REPRODUIRE LE JEU : 4 OU ROUGE : le concurrent peut voler les informations sur les savoir-faire de l'organisation pour reproduire le jeu
- BLOQUER LA PRODUCTION OU DIFFUSION COMMERCIALE DU JEU : 3 OU ORANGE : le concurrent peut détruire le prototype ou les informations en lien.

VALEUR METIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIE D'IMPACT	GRAVITÉ SUR 4
R&D **Concevoir le jeu**	Vol d'informations ou fuites d'information en conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes	-Impacts sur le patrimoine intellectuel -Impacts financiers énormes en pleine période	4
R&D **Concevoir le jeu**	Perte ou destruction du prototype MVP	Impacts financiers impacts sur l'image et la confiance	3



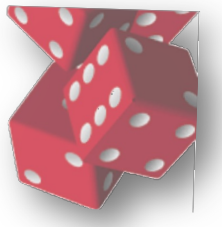
le cnam

PERTINENCE

ETUDE DE CAS DES CONCURRENTS AYANT VOLER DES INFORMATIONS POUR BLOQUER LA SORTIE DU JEU
MOTIVATION : TRÈS FORTE / MOYENS IMPORTANTS

ETUDE DE CAS DES CONCURRENTS AYANT VOLER DES INFORMATIONS POUR REPRODUIRE LE JEU
MOTIVATION : TRÈS FORTE / MOYENS IMPORTANTS

SOURCE DE RISQUE	OBJECTIF VISÉ	MOTIVATION	MOYENS/RESSOURCES	PERTINENCE
concurrent	voler des informations pour empecher le jeu de sortir	très forte	importants	- des cas similaires dans l'actualité de 2017 - un marché lucratif à l'approche de noel - pas de signaux faible avérés - conditions présentes
concurrent	voler des informations pour reproduire le jeu	très forte	importants	- des cas similaires dans l'actualité de 2017 - un marché lucratif à l'approche de noel - pas de signaux faible avérés - conditions présentes



ÉVALUER UN SCÉNARIO STRATÉGIQUE PAR SA GRAVITÉ

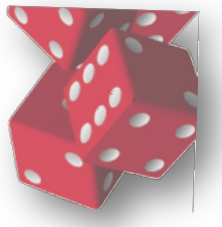
LES ENCADRÉS PERMETTENT D'ÉTABLIR LES LIENS ENTRE L'ÉVÈNEMENT LE PLUS REDOUTÉ ET LES OBJECTIFS VISÉS PAR L'AGENT MENAÇANT.

ETUDE DE CAS DES CONCURRENTS AYANT VOLER DES INFORMATIONS POUR BLOQUER LA SORTIE DU JEU
MOTIVATION : TRÈS FORTE / MOYENS IMPORTANTS/CAS SIMILAIRES

ETUDE DE CAS DES CONCURRENTS AYANT VOLER DES INFORMATIONS POUR REPRODUIRE LE JEU
MOTIVATION : TRÈS FORTE / MOYENS IMPORTANTS/CAS SIMILAIRES

VALEUR METIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIE D'IMPACT	GRAVITÉ SUR 4
R&D **Concevoir le jeu**	Vol d'informations ou fuites d'information en conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes	-Impacts sur le patrimoine intellectuel -Impacts financiers énormes en pleine période	4
R&D **Concevoir le jeu**	Perte ou destruction du prototype MVP	Impacts financiers impacts sur l'image et la confiance	3

SOURCE DE RISQUE	OBJECTIF VISÉ	MOTIVATION	MOYENS/RESSOURCES	PERTINENCE
concurrent	voler des informations pour empecher le jeu de sortir	très forte	importants	- des cas similaires dans l'actualité de 2017 - un marché lucratif à l'approche de noel - pas de signaux faible avérés - conditions présentes
concurrent	voler des informations pour reproduire le jeu	très forte	importants	- des cas similaires dans l'actualité de 2017 - un marché lucratif à l'approche de noel - pas de signaux faible avérés - conditions présentes



ÉVALUER UN SCÉNARIO STRATÉGIQUE PAR SA GRAVITÉ

LES ENCADRÉS PERMETTENT D'ÉTABLIR LES LIENS ENTRE L'ÉVÈNEMENT LE PLUS REDOUTÉ ET LES OBJECTIFS VISÉS PAR L'AGENT MENAÇANT.

ETUDE DE CAS DES CONCURRENTS AYANT DETRUIT POUR BLOQUER LA SORTIE DU JEU
MOTIVATION : PAS DE CAS

VALEUR METIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIE D'IMPACT	GRAVITÉ SUR 4
R&D **Concevoir le jeu**	Vol d'informations ou fuites d'information en conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes	-Impacts sur le patrimoine intellectuel -Impacts financiers énormes en pleine période	4
R&D **Concevoir le jeu**	Perte ou destruction du prototype MVP	Impacts financiers impacts sur l'image et la confiance	3

SOURCE DE RISQUE	OBJECTIF VISÉ	MOTIVATION	MOYENS/RESSOURCES	PERTINENCE
concurrent	voler des informations pour empecher le jeu de sortir	très forte	importants	- des cas similaires dans l'actualité de 2017 - un marché lucratif à l'approche de noel - pas de signaux faible avérés - conditions présentes
concurrent	voler des informations pour reproduire le jeu	très forte	importants	- des cas similaires dans l'actualité de 2017 - un marché lucratif à l'approche de noel - pas de signaux faible avérés - conditions présentes

2 SCÉNARIO DE GRAVITÉ « 4 » RETENUS

ETUDE DE CAS DES CONCURRENTS AYANT VOLER DES INFORMATIONS POUR BLOQUER LA SORTIE DU JEU
MOTIVATION : TRÈS FORTE / MOYENS IMPORTANTS/CAS SIMILAIRES

ETUDE DE CAS DES CONCURRENTS AYANT VOLER DES INFORMATIONS POUR REPRODUIRE LE JEU
MOTIVATION : TRÈS FORTE / MOYENS IMPORTANTS/CAS SIMILAIRES

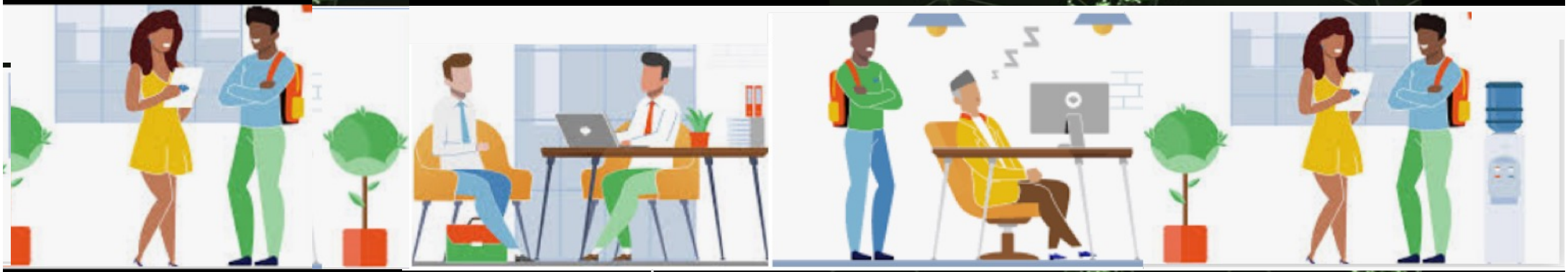
CONCLUSION

L'atelier a permis d'élaborer un scénario stratégique prenant en compte la connaissance de l'entreprise (son écosystème, le contexte, l'architecture) et d'évaluer la menace qu'il représente en fonction de sa gravité.

Vous allez apprendre comment générer un scénario opérationnel qui permettre de détecter les faiblesses, en dernier lieu, on apprendra à les corriger.

Atelier

4



le cnam

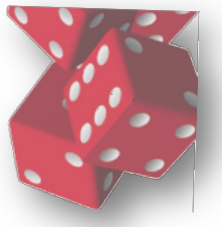
le cnam

ATELIER 4 GAMELUCK SCÉNARIO OPÉRATIONNEL POUR XGAME

L'objectif de ce nouvel atelier est de déterminer les scénarii opérationnels qui peuvent s'instancier à partir des scenarii stratégiques, cette fois, il s'agit de regarder comment l'attaquant peut opérer sur le processus « innovation » de GameLuck avec son jeu XGame en cours de sortie.

Le travail présenté dans cet atelier vise la transformation d'un chemin d'attaque (du scénario stratégique) en un scénario opérationnel plus technique.

En entrée, le travail utilise le chemin d'attaque en question, en sortie vous obtiendrez le mode opératoire technique suivi par l'attaquant.



Scénario opérationnel

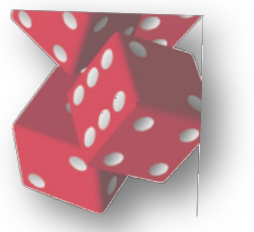
le cnam

Pour ce faire on utilise une chaine d'attaque type (cyber kill chain) proposée par la méthode EBIOS de l'ANSSI.

Des scénarios structurés selon une séquence d'attaque type

CONNAITRE	RENTRER	TROUVER	EXPLOITER
Corruption	Corruption	Corruption	Corruption
Reconnaissance externe	Intrusion depuis Internet	Reconnaissance interne	Pilotage et exploitation de l'attaque
	Intrusion ou piège physique	Latéralisation et élévation de privilèges	

Il est important de noter que ces étapes sont modulaires (par exemple selon si l'attaquant attaque directement ou par rebond via une partie prenante de l'écosystème)



Scénario opérationnel

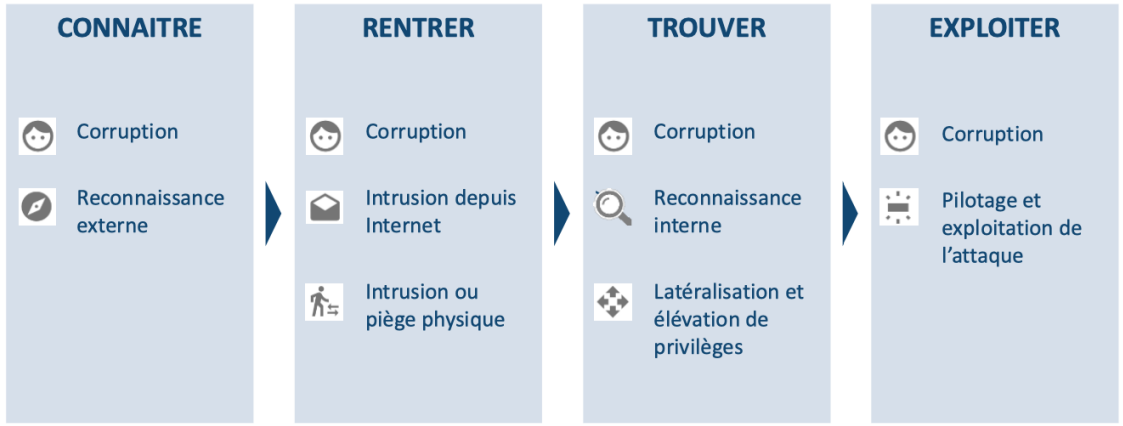
le cnam

1.3 Travail 2 : atelier « Scenario Opérationnel » 3 points

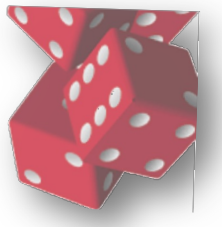
Phases scenario opérationnel	Actions malveillantes	Objectif l'attaque	de Pré-requis techniques nécessaires pour engager l'action	Gain de l'attaquant une fois l'action effectuée
CONNAITRE				
RENTRER				
TROUVER				

Corruption

Des scénarios structurés selon une séquence d'attaque type



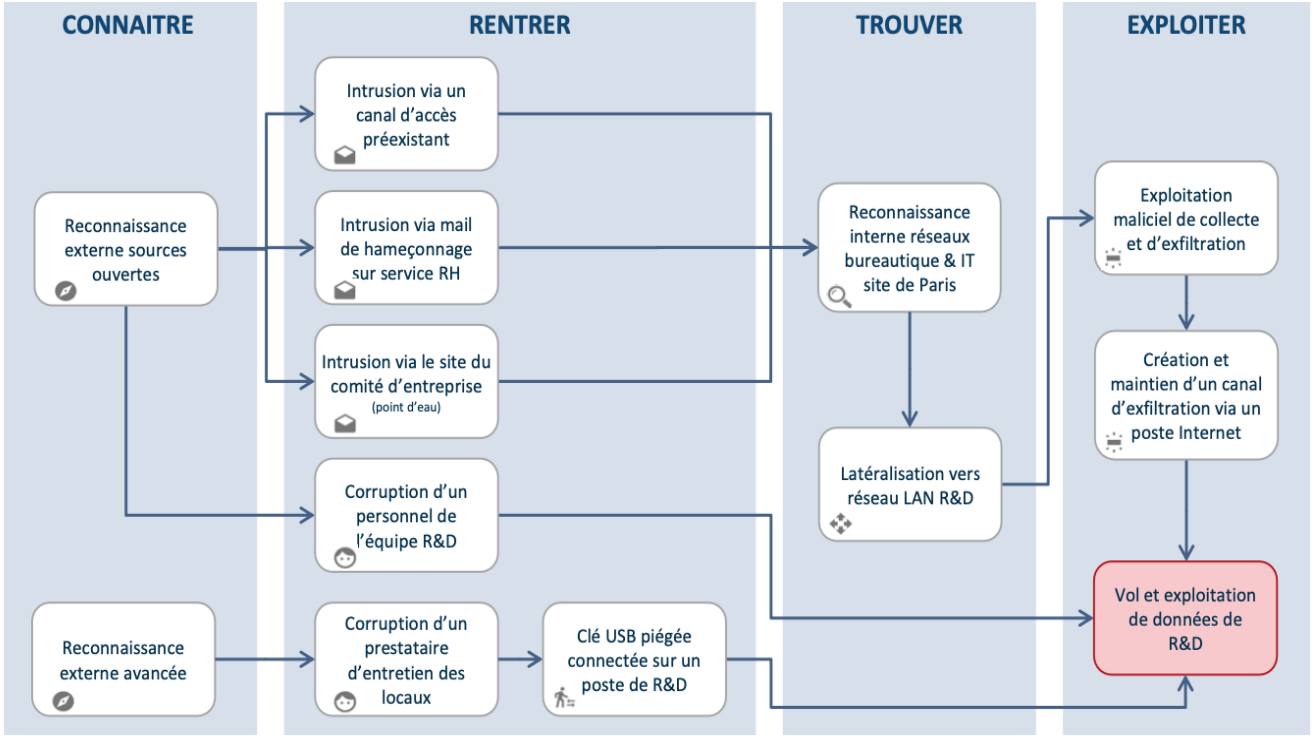
Il est important de noter que ces étapes sont modulaires (par exemple selon si l'attaquant attaque directement ou par rebond via une partie prenante de l'écosystème)

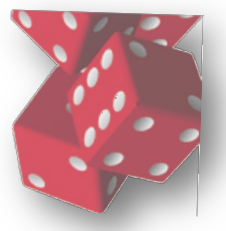


Description du scénario opérationnel

le cnam

Pour ce faire on utilise une chaine d'attaque type (cyber kill chain) proposée par la méthode EBIOS de l'ANSSI.
Voici la scénarisation de ce qu'il peut se passer.





Description du scénario opérationnel « Connaitre »

1.3 Travail 2 : atelier « Scenario Opérationnel » 3 points

Phases scenario opérationnel	Actions malveillantes	Objectif l'attaque	de Pré-requis techniques nécessaires pour engager l'action	Gain de l'attaquant une fois l'action effectuée
CONNAITRE				
RENTRER				
TROUVER				

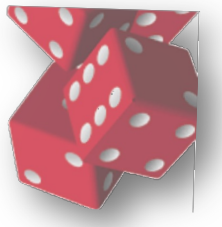
Tirer partie du salarié GL

Obj : Corruption

CONNAITRE	RENTRER	TROUVER	EXPLOITER
1/ Action de reconnaissance externe en source ouverte : réseau social pro, etc. Par exemple recherche de collaborateurs de GL et d'ancrages (points d'entrée). 2/ Vers une vulnérabilité prête ou à faire fléchir, par exemple tirer partie d'échanges avec un salarié de Gameluck .	Vers où peut aller l'attaquant pour « rentrer »?		

1 Quelles actions exerce l'attaquant ?

2

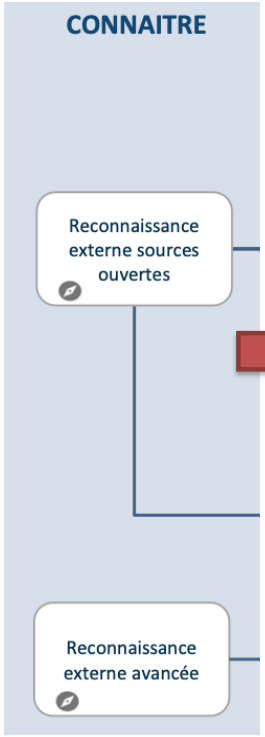


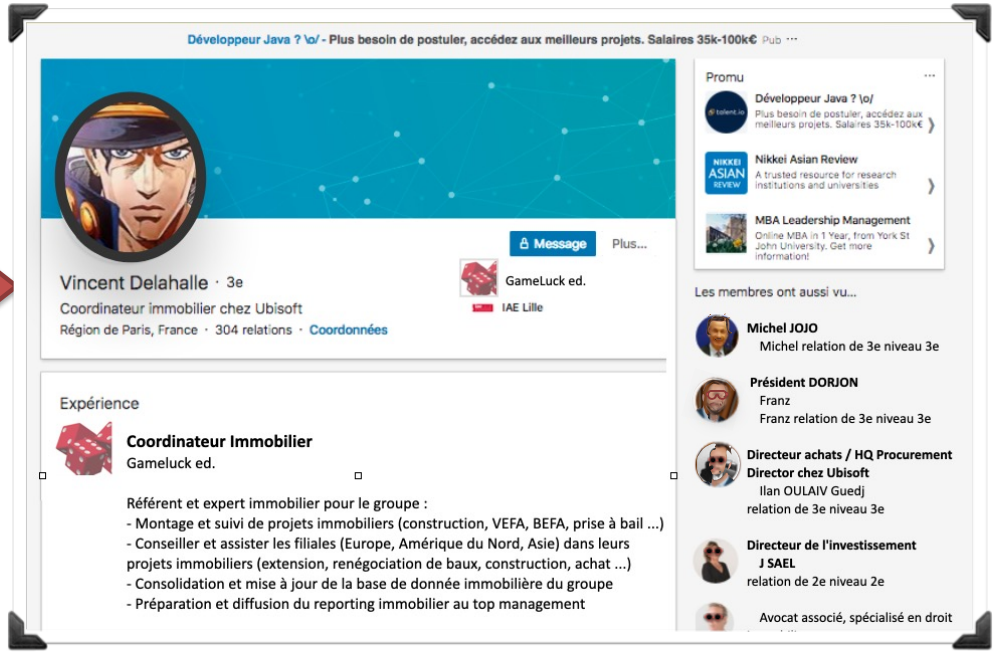
Description du scénario opérationnel « Connaitre » : reconnaissance en source ouverte

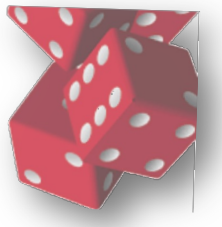
le cnam

Dans le cas de GL, il s'agit d'approches de collaborateurs GL par des cyber attaquants qui interagissent sur les réseaux sociaux professionnels et privés avec des personnes peu sensibilisées.

Vincent Lapage se fait approcher.



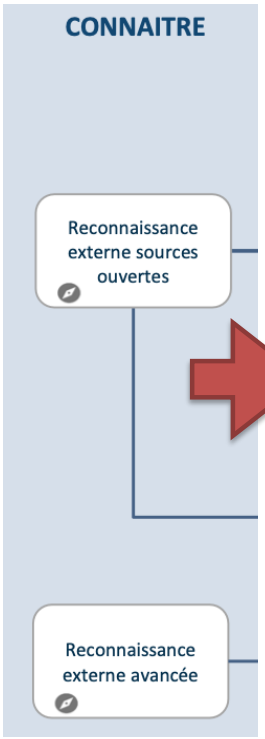


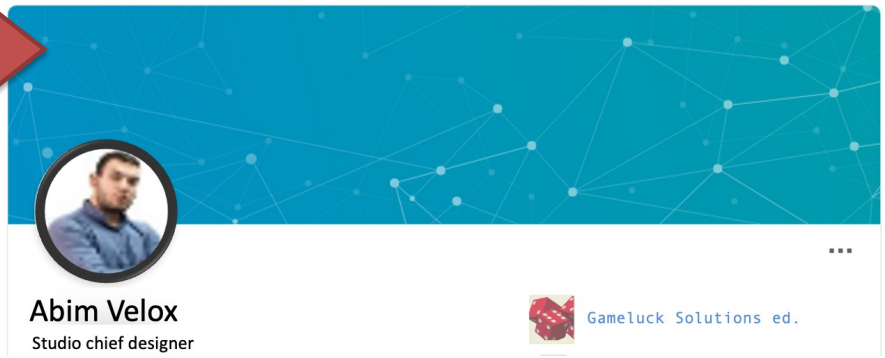


Description du scénario opérationnel « Connaitre » : reconnaissance en source ouverte

le cnam

Abim Velox se fait également « approcher » avec son équipe



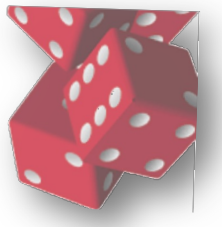


Autres pages consultées


Yvon Kerberosc
Studio designer
France


Tamara Brunschwik
Studio designer
France

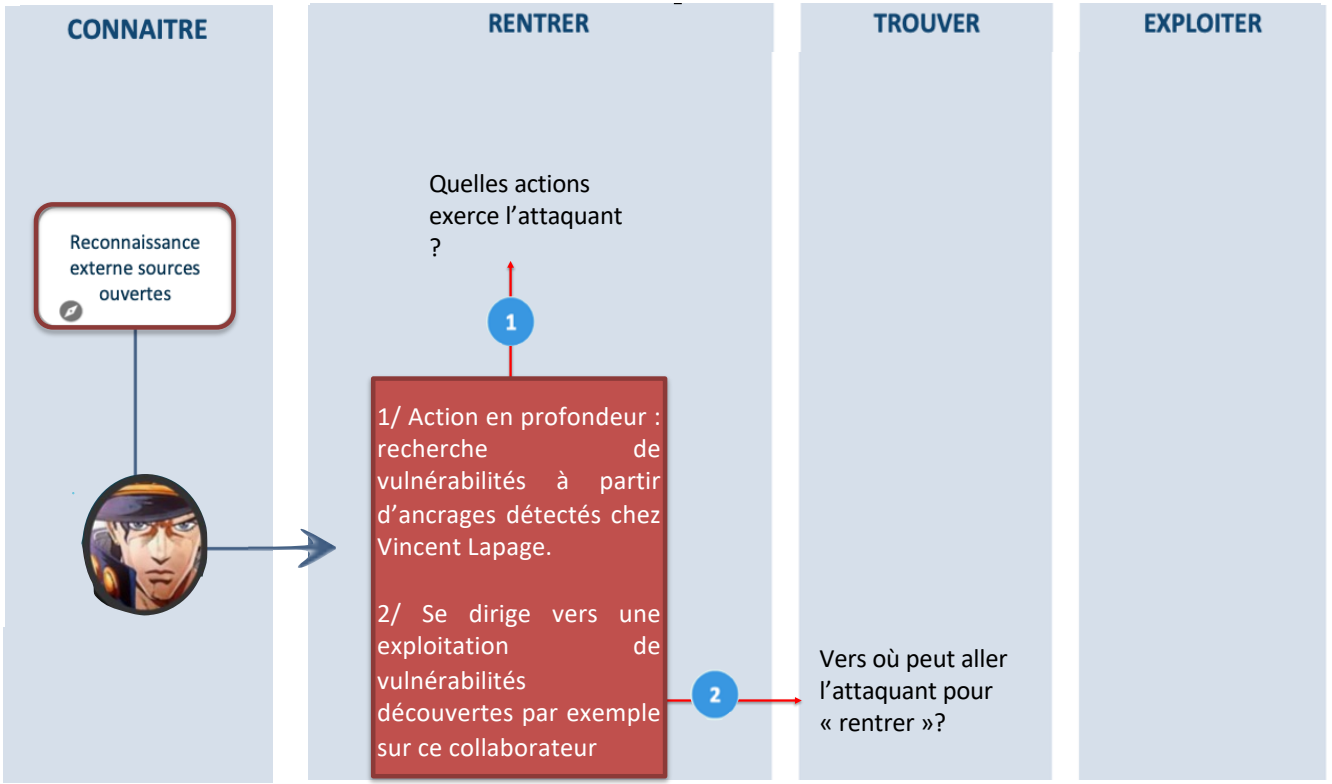

Yann Bartez
Studio developper
France

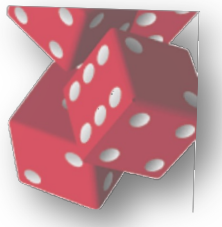


Description du scénario opérationnel « Rentrer »

le cnam

Une fois l'ancrage sur la cible Vincent Lapage, il devient possible de faire des actions soit en latéralisation sur ses collègues soit en profondeur en générant des actions pour rentrer dans le SI.

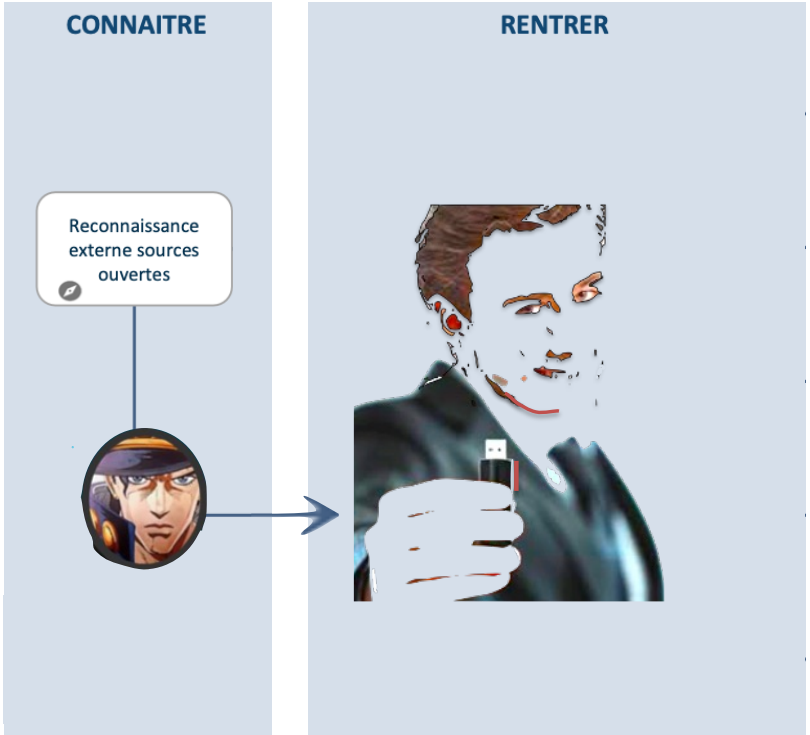


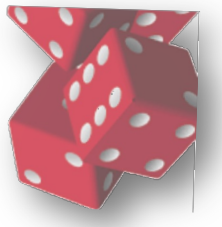


Description du scénario opérationnel « Rentrer »

le cnam

Par exemple l'attaquant offre à Vincent Lapage une clé USB préchargée avec un malware.



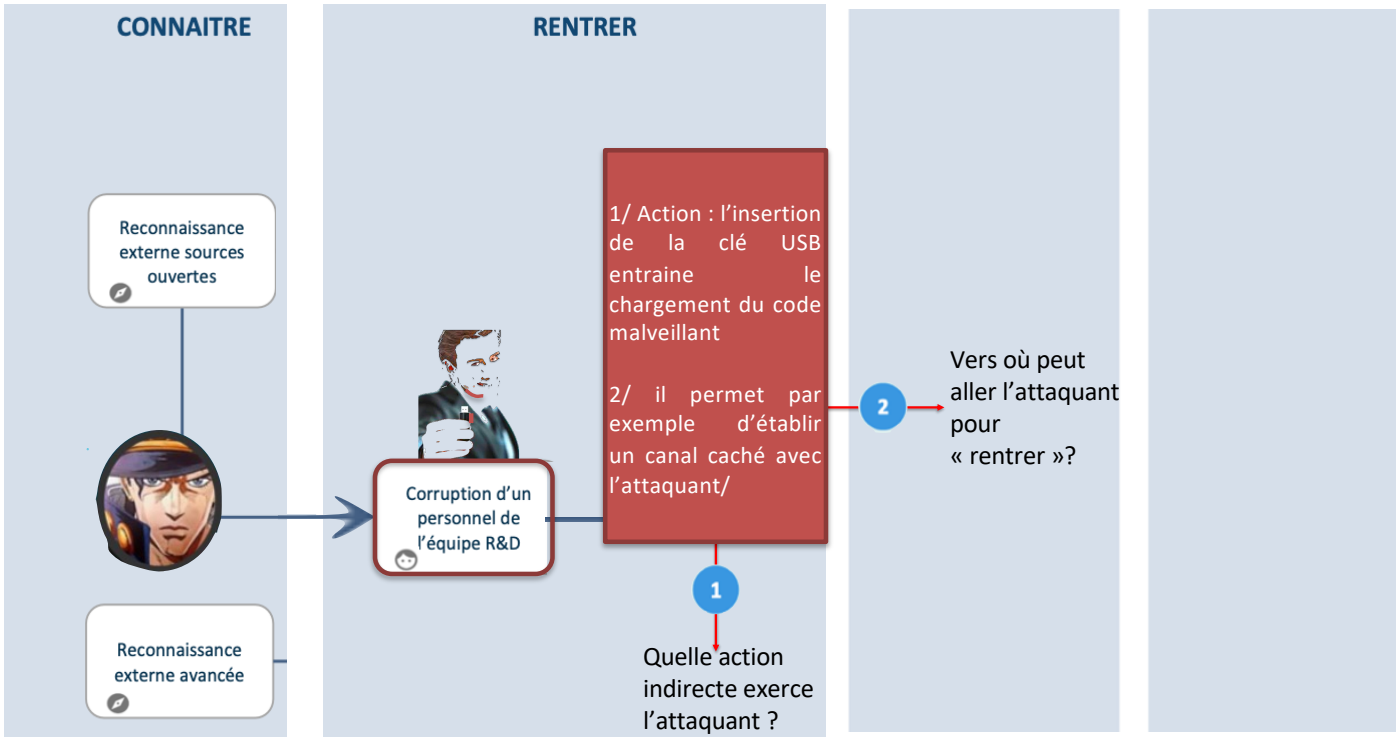


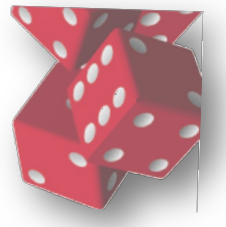
Description du scénario opérationnel « Rentrer »

le cnam

Une fois que Vincent Lapage accepte la clé USB, il va l'insérer dans son PC.

- Dès l'insertion de la clé, le poste de travail a les autorisation pour éxécuter automatiquement les programmes préchargés sur la clé (dont le code malveillant).

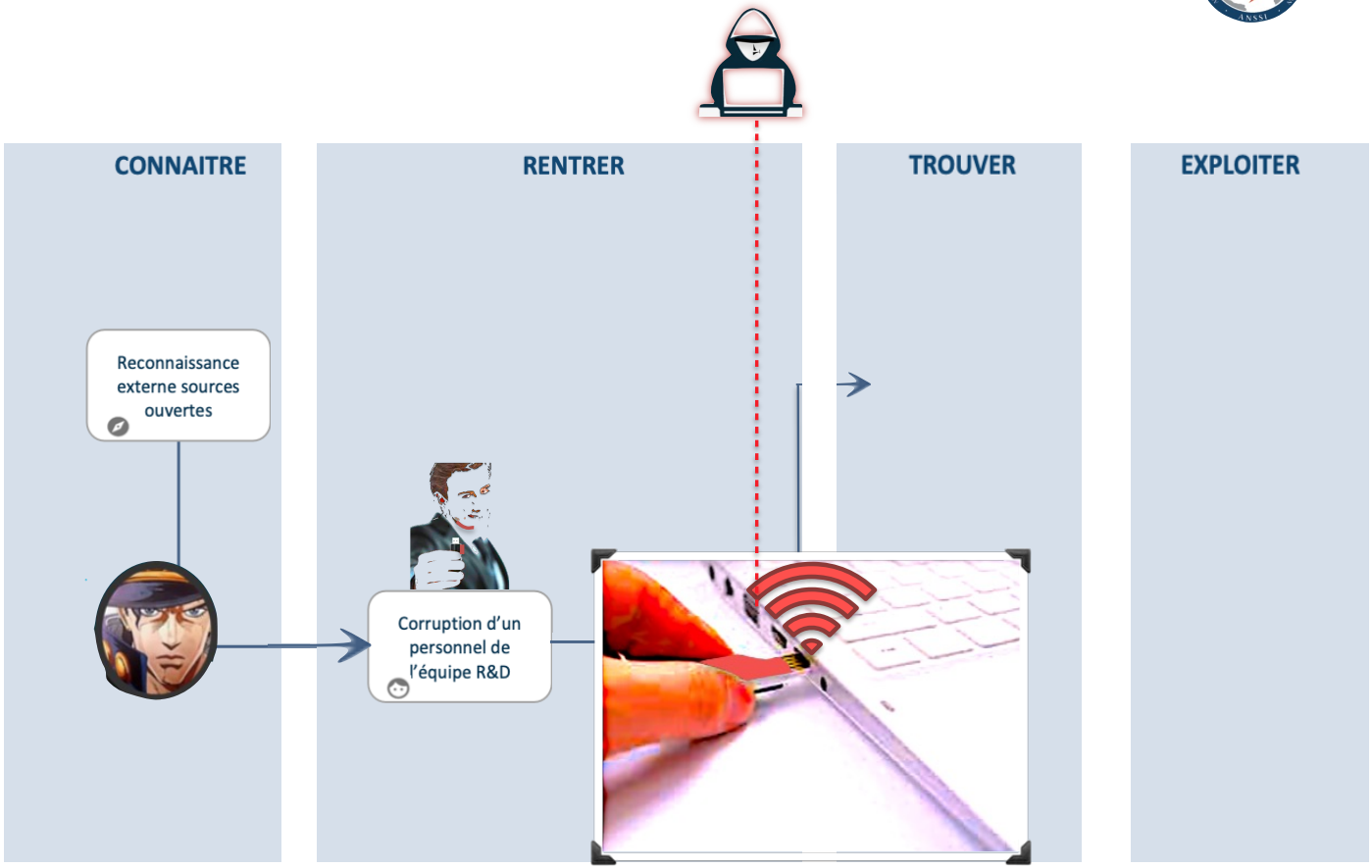


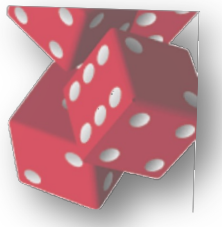


Description du scénario opérationnel « Rentrer »

le cnam

- De fait le programme malveillant hébergé sur la clé USB va s'exécuter et se propager et créer des liens et des canaux pour maintenir un canal d'exfiltration.





Description du scénario opérationnel « Trouver »

le cnam

Trouver : l'attaquant trouve le réseau et les systèmes internes, il peut les cartographier

CONNAITRE

Reconnaissance externe sources ouvertes

RENTRER

Corruption d'un personnel de l'équipe R&D

Clé USB piégée connectée sur un poste de R&D

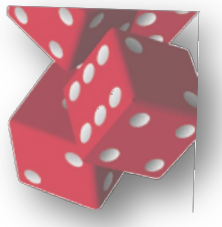
TROUVER

1/ Action : le canal permet à l'attaquant d'exécuter des commandes depuis le poste de Vincent Lapage

2/ Vers où ? De là, il peut par exemple explorer le réseau et les serveurs et le cartographier afin d'identifier des vulnérabilités.

2 → Vers où peut aller l'attaquant pour « rentrer »?

1 → Quelle action indirecte exerce l'attaquant ?

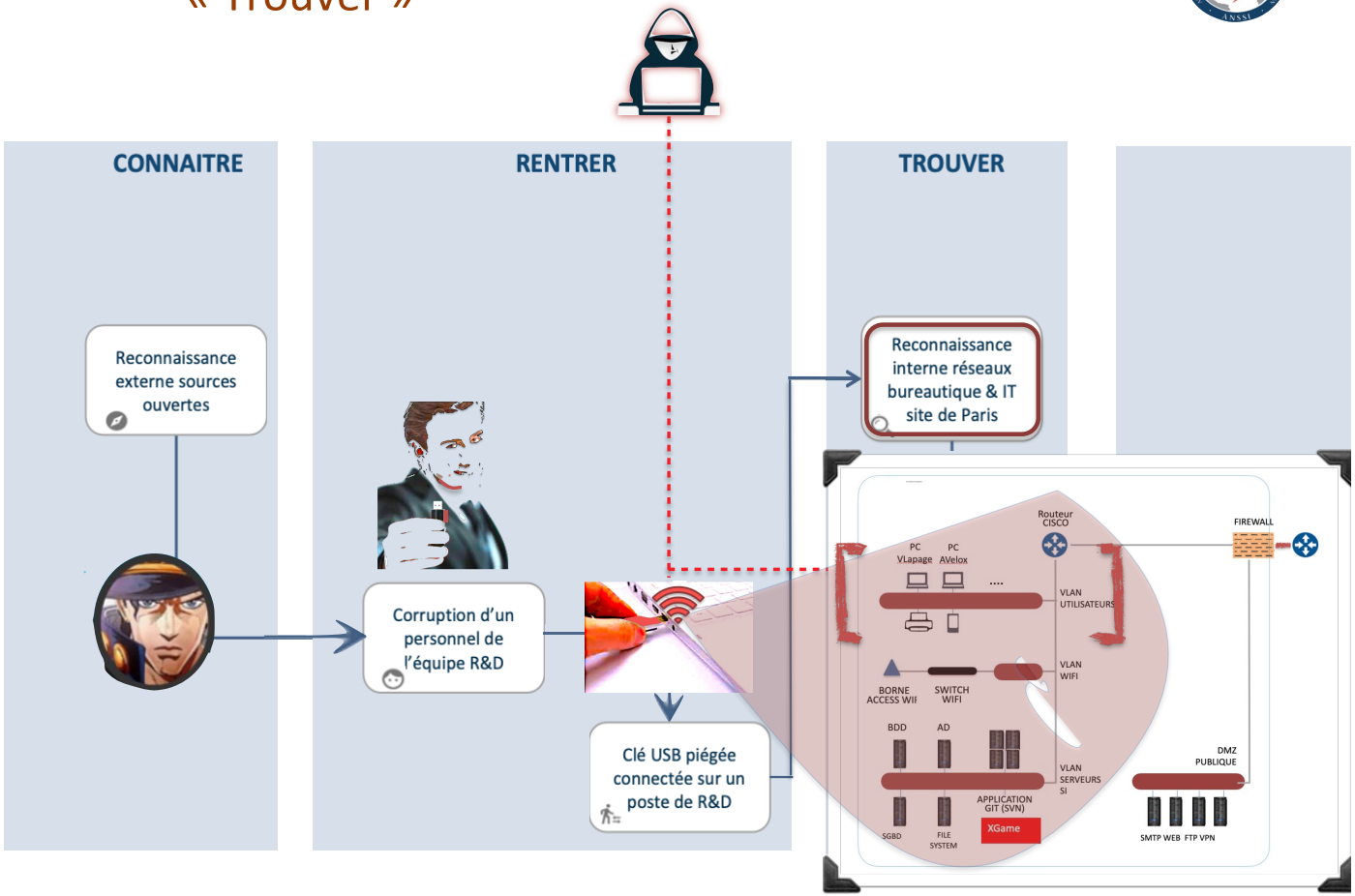


Description du scénario opérationnel « Trouver »

le cnam

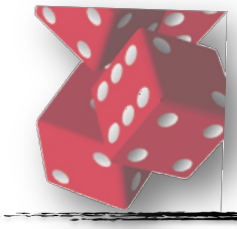
Une fois le canal établit, l'attaque se déroule en profondeur pour **trouver** les informations sur XGame, l'attaquant fouille et cartographie le réseau.

Il **trouve** les VLAN, les postes de travail du VLAN utilisateur et le VLAN Serveur



le cnam

Description du scénario opérationnel « Trouver »



Une fois le canal établit, l'attaque se déroule en profondeur pour trouver les informations sur XGame, l'attaquant fouille et cartographie le réseau.

Par exemple, l'attaquant **parcourt l**e VLAN Utilisateurs, il liste les postes de travail, certains noms de ces postes de travail reprennent le nom des développeurs notés dans Linkedin.

CONNAITRE

RENTRER

TROUVER

Reconnaissance externe sources ouvertes

Corruption d'un personnel de l'équipe R&D

Clé USB piégée connectée sur un poste de R&D

Reconnaissance interne réseaux bureautique & IT site de Paris

1/ Action : Avec sa présence sur le VLAN utilisateur depuis le poste de Vincent Lapage , explorer le VLAN est possible

2/ Vers où ? De là, il peut par exemple explorer les partages des postes de travail et le switch s'il est accessible

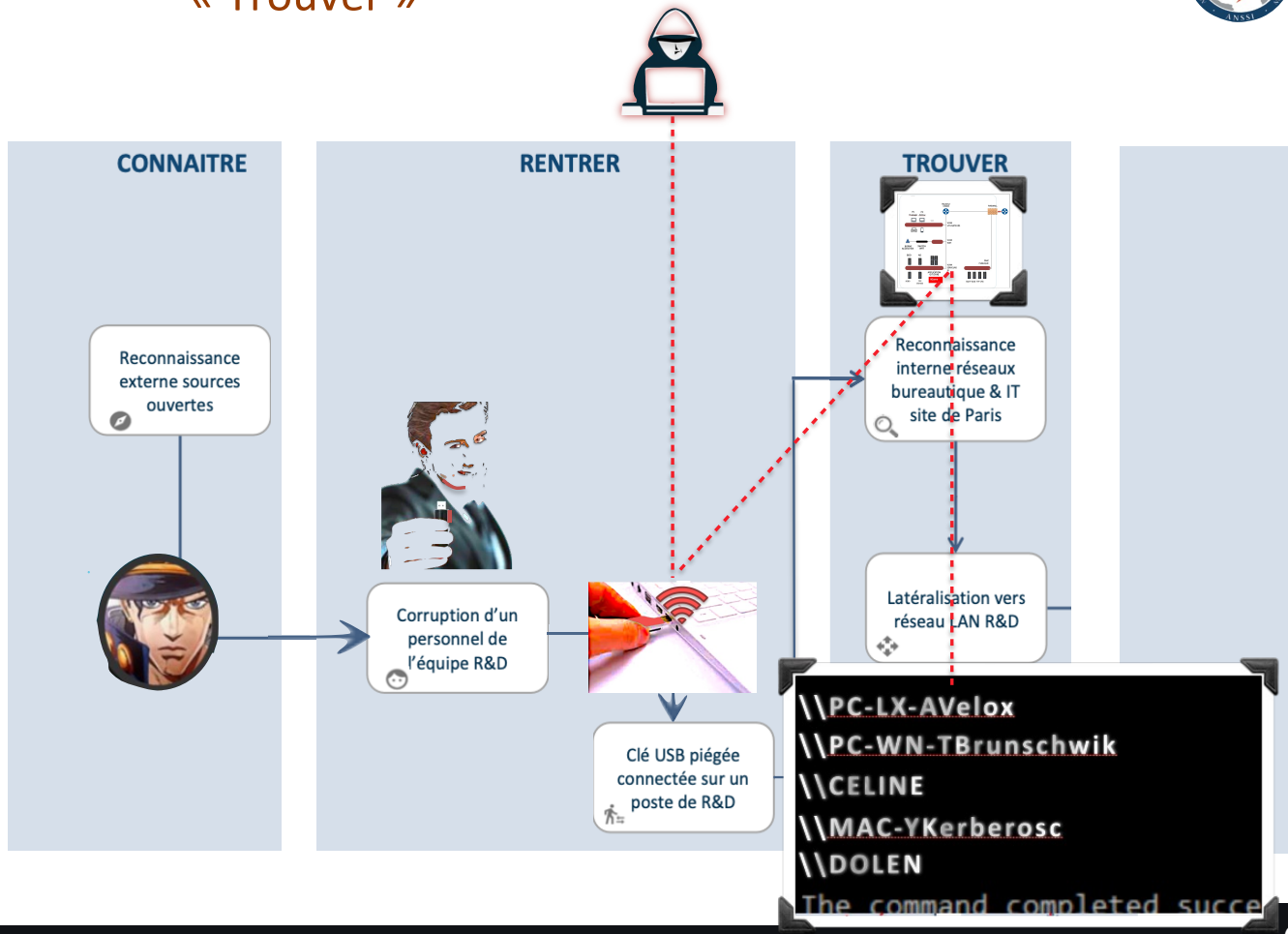
2 Vers où peut aller l'attaquant pour « rentrer »?

1 Quelle action indirecte exerce l'attaquant ?

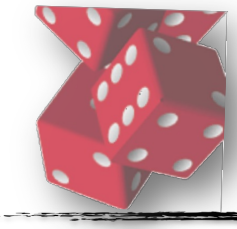
Description du scénario opérationnel « Trouver »

Une fois le canal établit, l'attaque se déroule en profondeur pour trouver les informations sur XGame, l'attaquant fouille et cartographie le réseau.

Par exemple, l'attaquant **parcourt l**e VLAN Utilisateurs, il liste les postes de travail, certains noms de ces postes de travail reprennent le nom des développeurs notés dans Linkedin (Kerberosc, Brunschwik,.)…

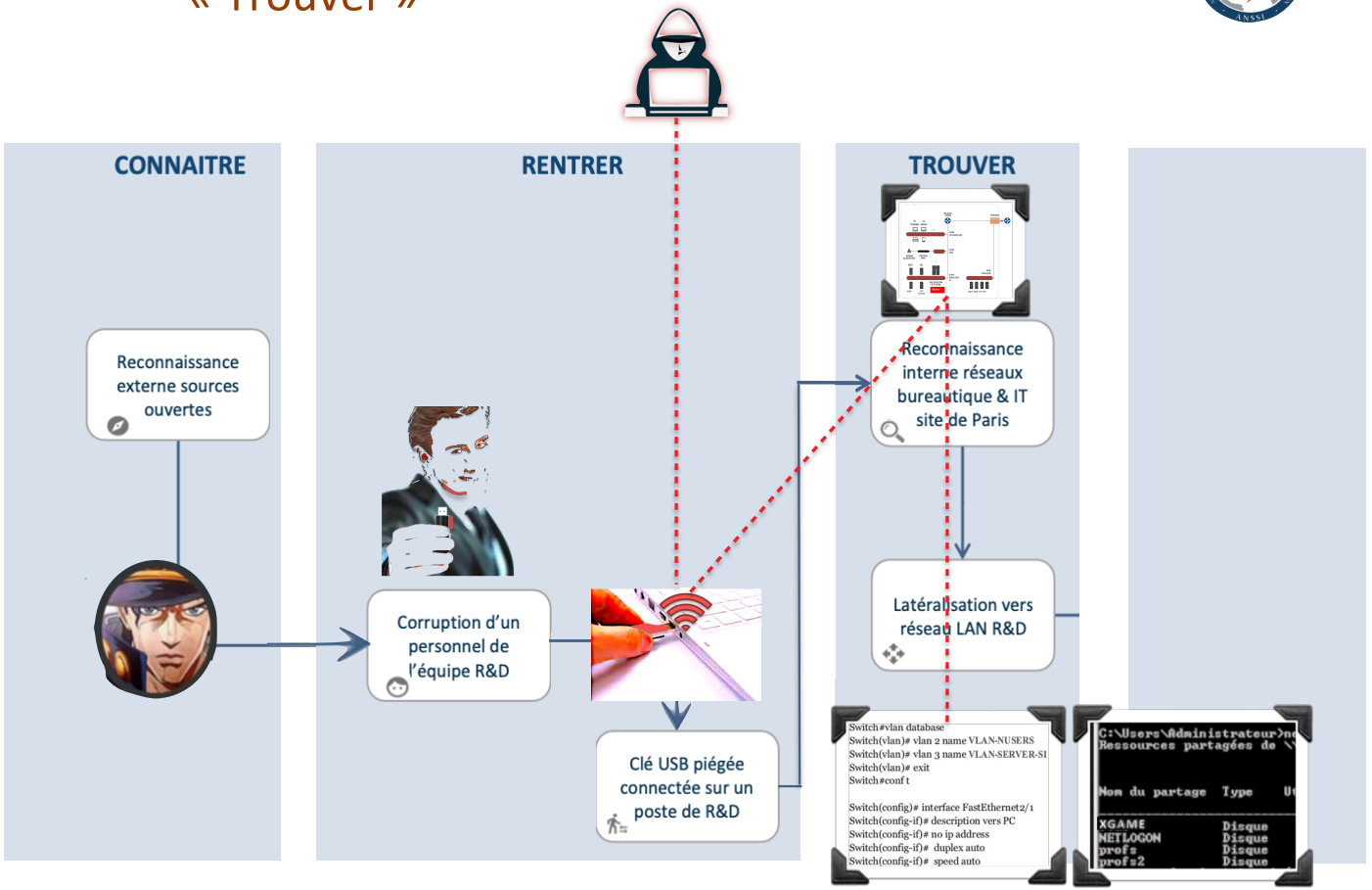


Description du scénario opérationnel « Trouver »

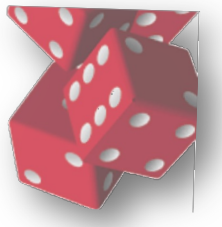


Une fois le canal établit, l'attaque se déroule en profondeur pour trouver les informations sur XGame, l'attaquant fouille et cartographie le réseau.

Par exemple, l'attaquant **parcourt l**e VLAN Utilisateurs, il liste les postes de travail, certains noms de ces postes de travail reprennent le nom des développeurs notés dans Linkedin (Kerberosc, Brunschwik,.)…

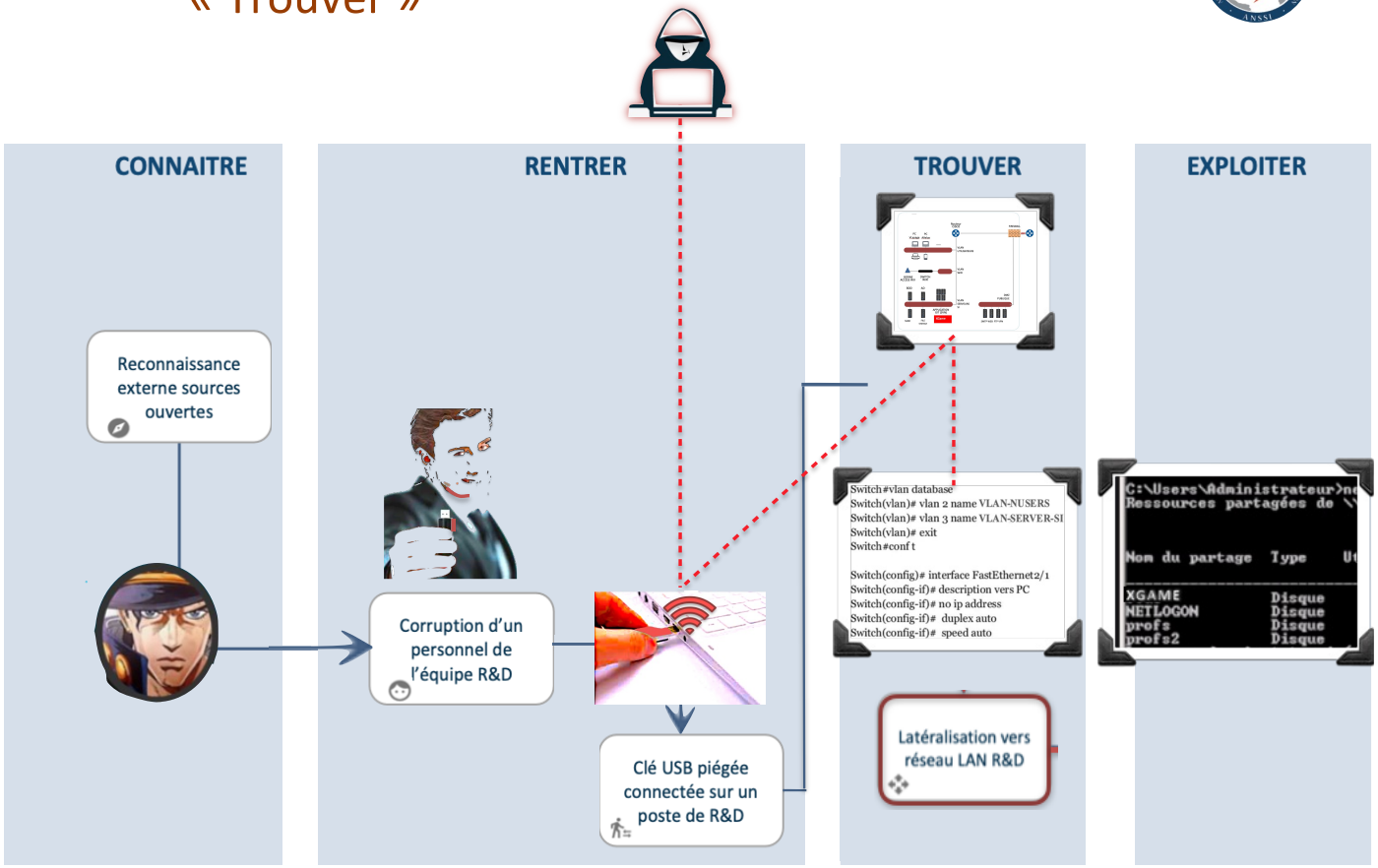


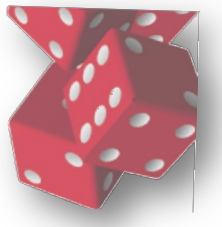
Description du scénario opérationnel « Trouver »



L'attaquant fouille encore les composants du réseau, trouve également sur la configuration du switch les VLAN USERS et Serveurs-SI.

Il découvre ensuite le serveurs GIT, puis les partages de fichiers dont XGAME accessible depuis le VLAN USERS (disponible pour les développeurs déposent leurs programmes.

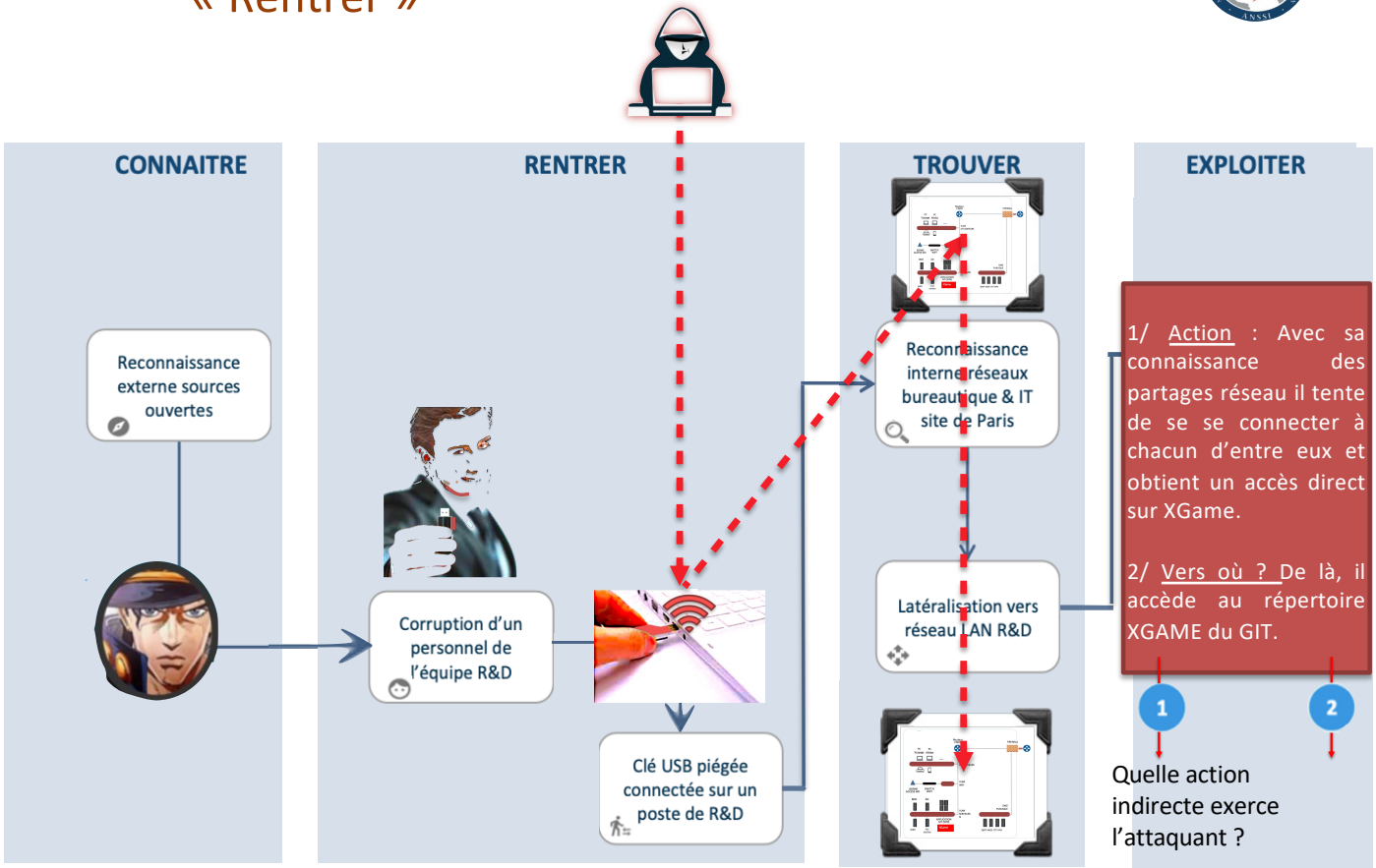


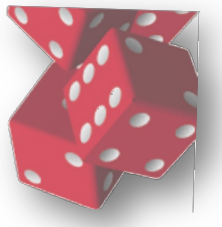


Description du scénario opérationnel « Rentrer »

le cnam

L'attaquant obtient un accès sur le serveur GIT via le partage de fichiers, il peut accéder aux codes source de XGame et les exfiltrer

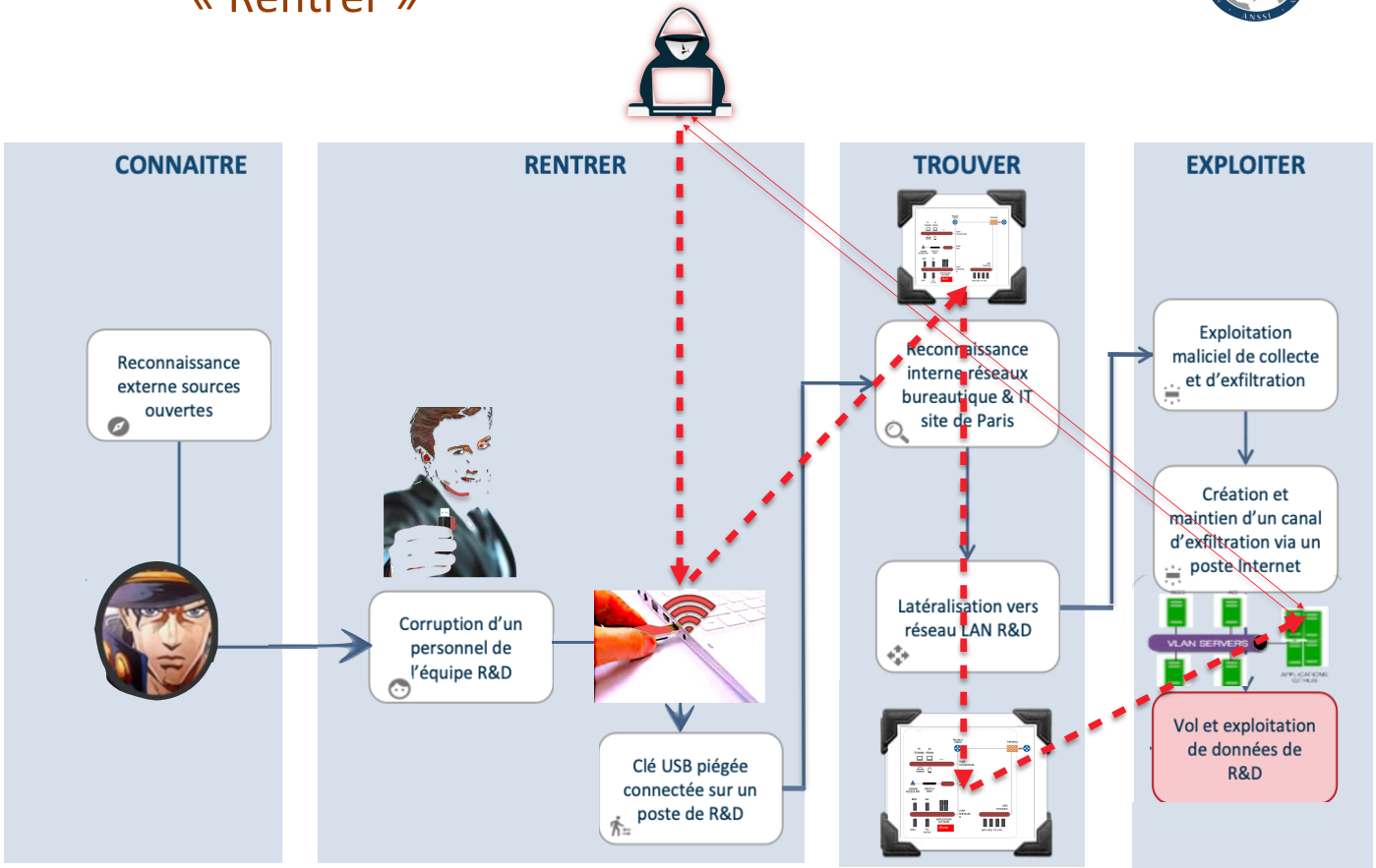


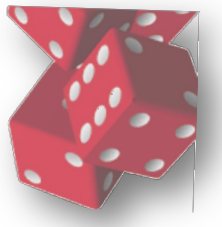


Description du scénario opérationnel « Rentrer »

le cnam

Une fois l'accès au GIT, l'attaquant peut établir un canal vers son serveur de collecte depuis le serveur GIT et exfiltrer les données.

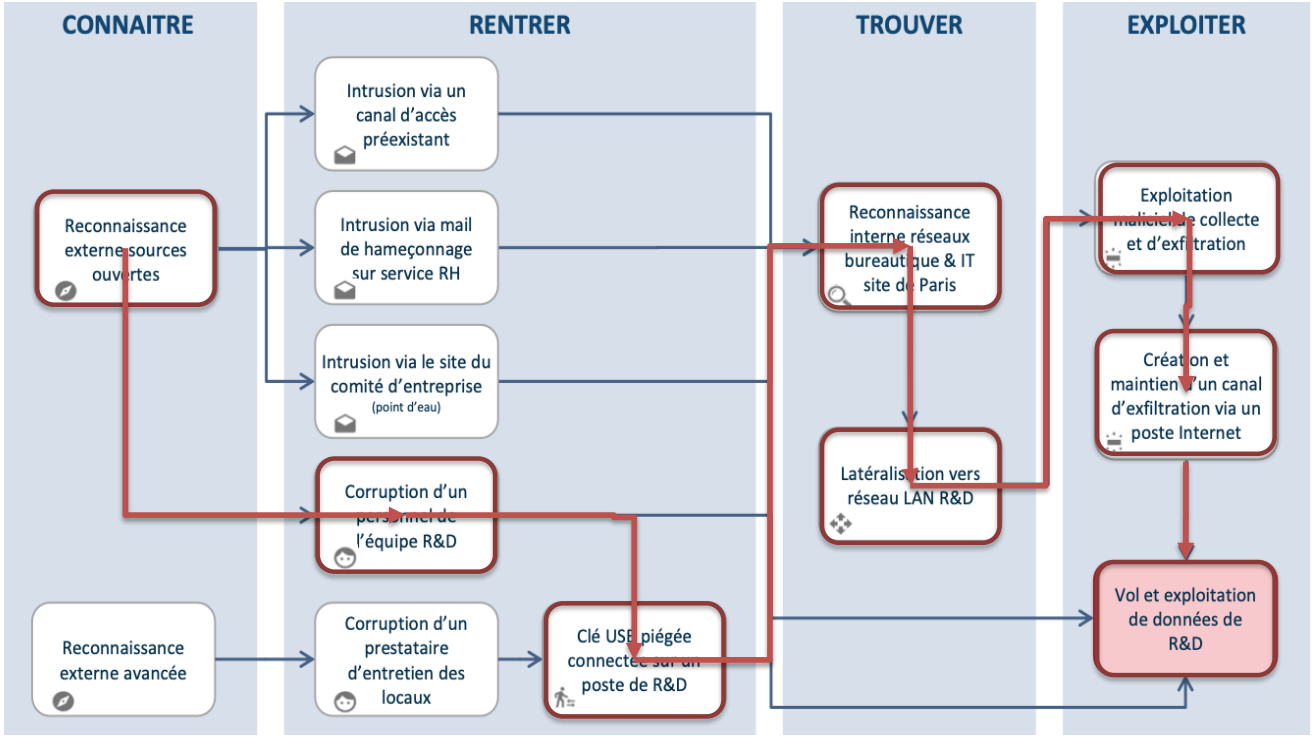




Description du
Synthèse du scénario opérationnel

le cnam

Pour ce faire on utilise une chaine d'attaque type (cyber kill chain) proposée par la méthode EBIOS de l'ANSSI.
Voici la scénarisation de ce qu'il peut se passer.



le cnam

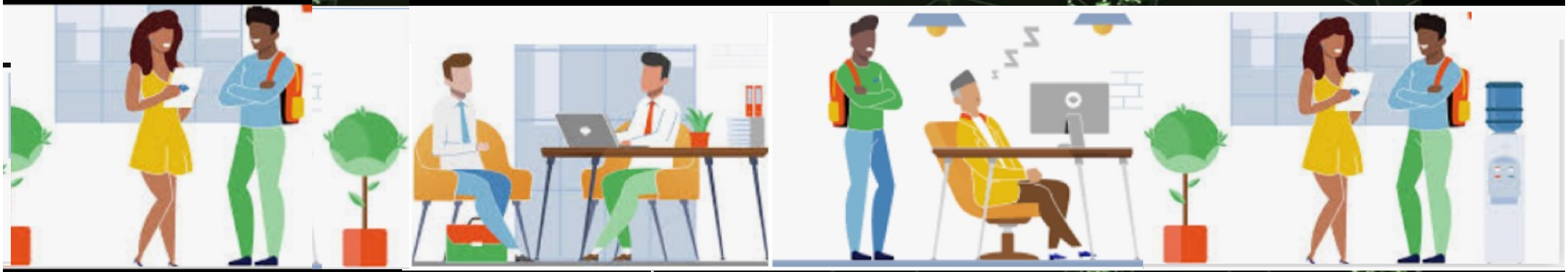
CONCLUSION

L'atelier a permis de comprendre les chemins d'attaques de l'attaquant, et de conclure sur les vulnérabilités.

Vous savez exprimer un scénario opérationnel d'attaque en fonction de la cible donnée (ici les données d'innovation).
Vous savez identifier les points faibles dans ce scénario opérationnel.

Vous allez apprendre comment sélectionner les mesures proposées dans le référentiel et correspondant à votre architecture.

Atelier 5



le cnam

ATELIER 5 GAMELUCK COMMENT SÉLECTIONNER LES MESURES DE SÉCURITÉ À PARTIR DU SCÉNARIO OPÉRATIONNEL DE XGAME

L'objectif de ce nouvel atelier est de montrer comment on sélectionne des mesures de sécurité à partir d'un référentiel (ISO 27002) en réponse au scénario opérationnel que l'on vient de découvrir.

Le scénario opérationnel présente plusieurs points de faiblesse, cet atelier ne traite que la réponse aux actions d'exploration du réseau interne.

Le travail présenté dans cet atelier se focalisera sur les mesures correctives liées à :

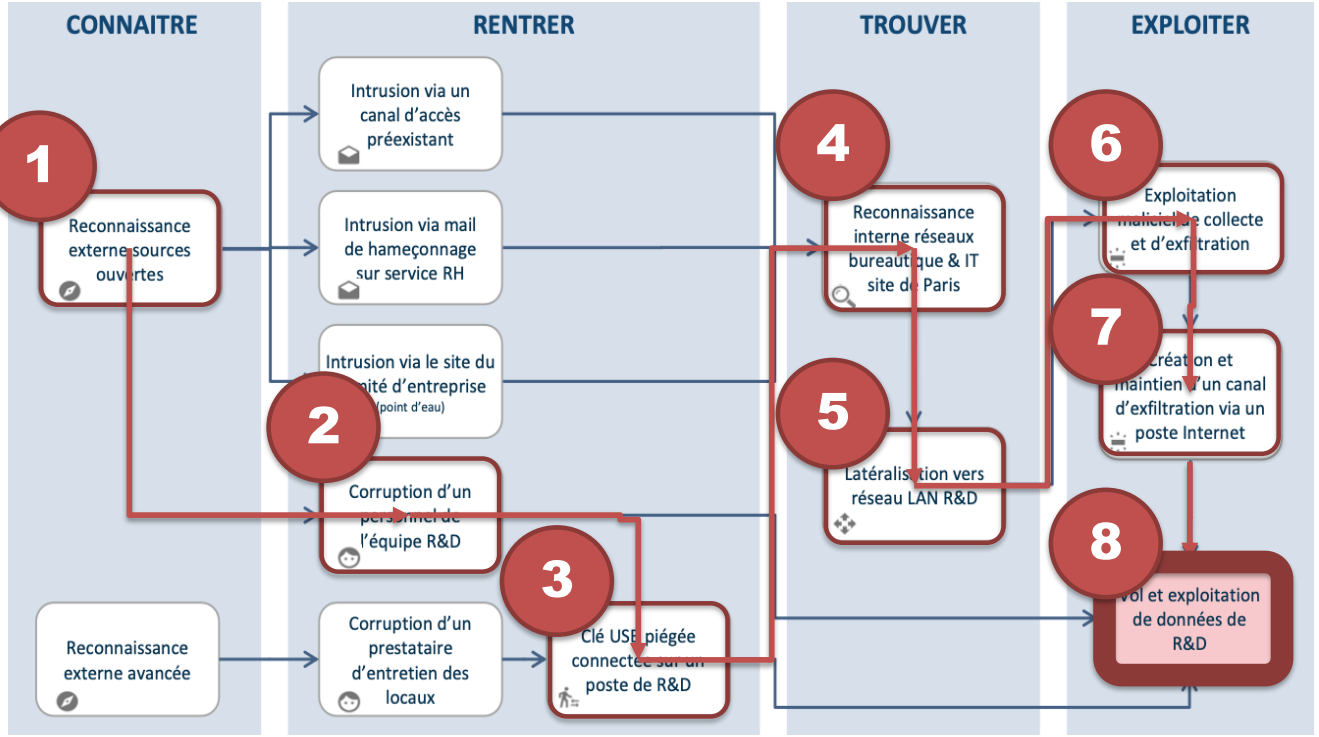
- la sécurité de l'exploitation qui fait que le service innovation et développement partagent les mêmes ressources,
- la sécurité des communications qui fait que les réseaux internes ne sont pas cloisonnés.

Le travail de cet atelier prend en entrée le scénario opérationnel et fournit en sortie un ensemble de mesures issues d'un référentiel, ici l'ISO27002.

Quels sont ces problèmes qui exposent les cibles ?

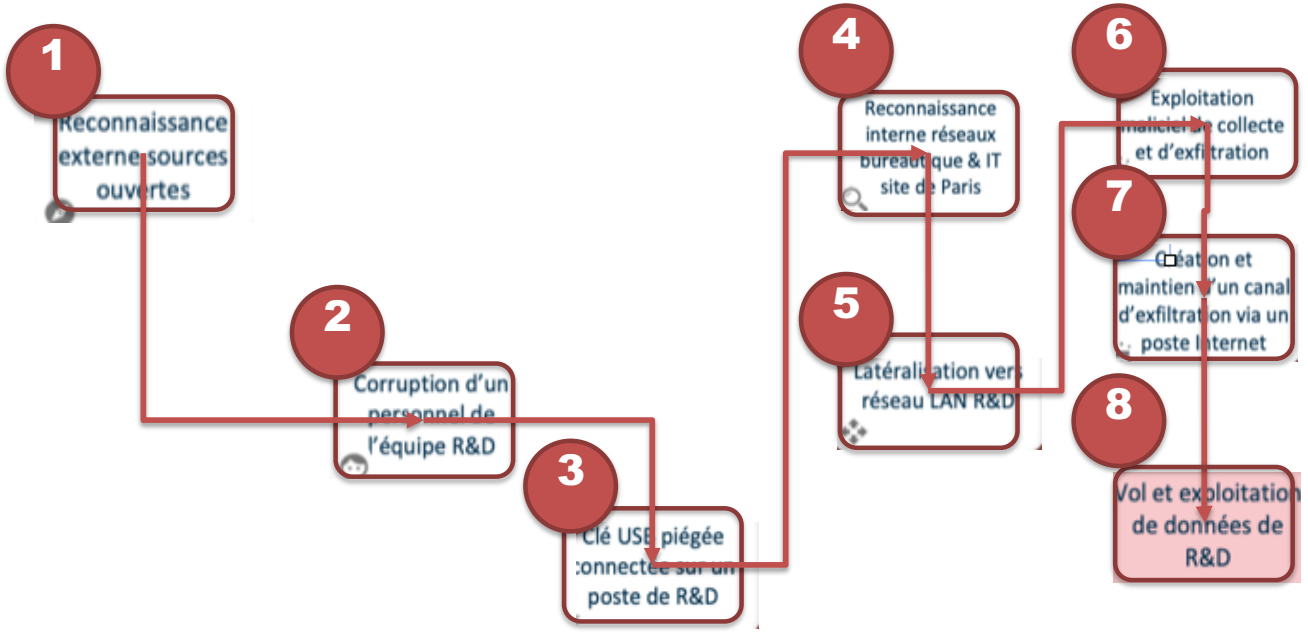
Nous constatons 8 problèmes dans le cas de la réalisation de ce scénario.

Cet atelier n'a pas pour objectif de corriger l'ensemble des problèmes, mais d'expliquer le principe mis en oeuvre pour 1 problème : le cas 5 comment empêcher l'attaquant de « trouver » ?



Problématiques

Cet atelier détaille le principe pour le problème 5 mais présentera une vue générale pour les 6,7,8



Quelles mesures de sécurité de l'ISO 27002 pourraient-être sélectionnées pour les problèmes 6,7,8 ?

6

« Exploitation maliciels de collecte et d'exfiltration »

L'attaquant injecte des maliciels pour mener à bien le transfert des données.

Mot-clé recherché dans la norme ISO27002 : «code malveillant »

Généralement l'ISO propose les mesures pour :

- 12.2 : protection contre les logiciels malveillants,
- 12.1.4 : Séparation des environnements de développement, de test et d'exploitation,
- 13.2.1 : des procédures de détection et de protection contre les logiciels malveillants lors des communications électroniques
- 6.2.1, 12.5.1, 12.6.1, 12.6.2, Restrictions liées à l'installation de logiciels, règles régissant l'installation de logiciels par les utilisateurs

7

« Création et maintien d'un canal d'exfiltration avec Internet »

L'attaquant établit un canal à partir du réseau interne.

Mot-clé recherché dans la norme ISO27002 : «maintien » « canal »

Généralement l'ISO propose les mesures pour se prémunir de canaux cachés :

- 12.2.1 : protection contre les logiciels malveillants,
- 13.2.1 : Maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure.
  - surveiller les ports réseaux ouverts,
  - surveiller le trafic vers l'extérieur,
  - bien connaître ses flux réseaux à l'aide d'une matrice de flux,
- 13.2.3 : messagerie électronique.

8

« Vol et exploitation de données de R&D »

L'attaquant peut substituer l'information directement car elle est accessible « en clair »

Mot-clé recherché dans la norme ISO27002 : « vol » & « données »

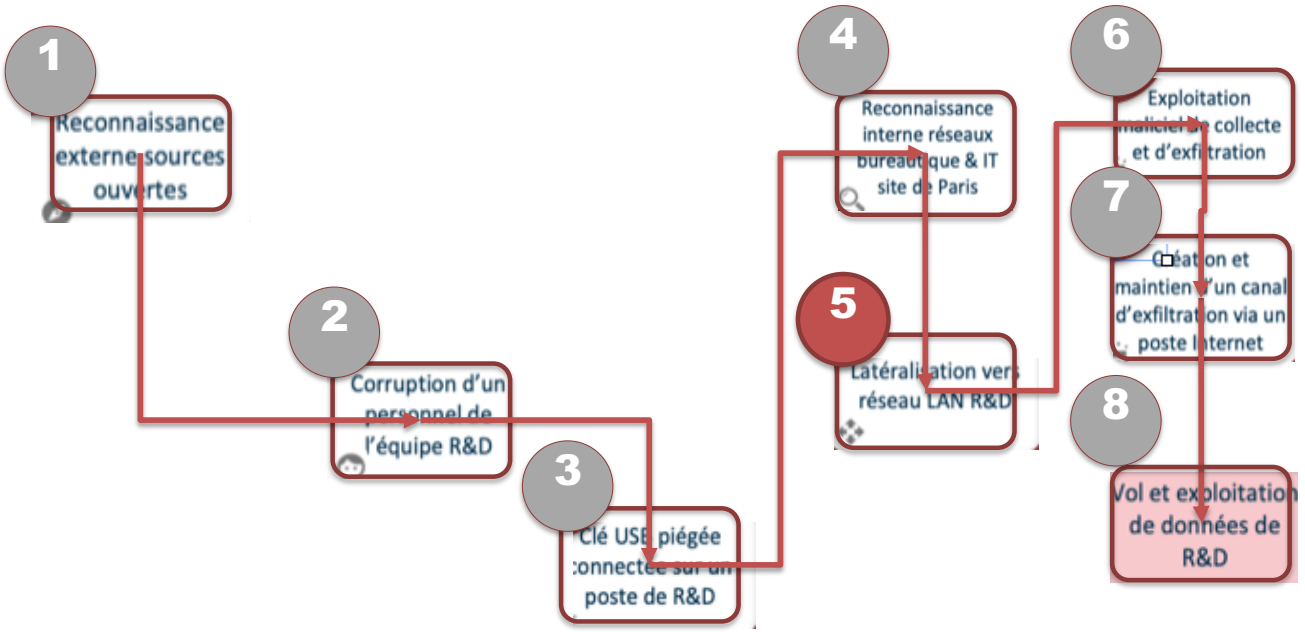
Généralement l'ISO propose ces classes de mesures de sécurité pour se prémunir du vol de données :

- **9.4.5 : restreindre l'accès au code source des programmes XGAME : Gestion des accès/habilitations et privilèges.**
- 10.1.1, Chiffrer le stockage des données internes,
- 10.1.1, 14.1.3 : Chiffrer les échanges de données internes,
- Sensibiliser les utilisateurs au traitement sécurisé des données,

Quelles mesures de sécurité pour le problème 5 ?

Nous nous intéressons au problème 5 : les tentatives d'accès aux réseaux internes LAN de la RD (latéralisation).

Ce problème constitue un vecteur clé utilisé par l'attaquant pour « trouver » les moyens d'accéder au données d'innovation.



Quelles mesures de sécurité pour le problème 5 ?

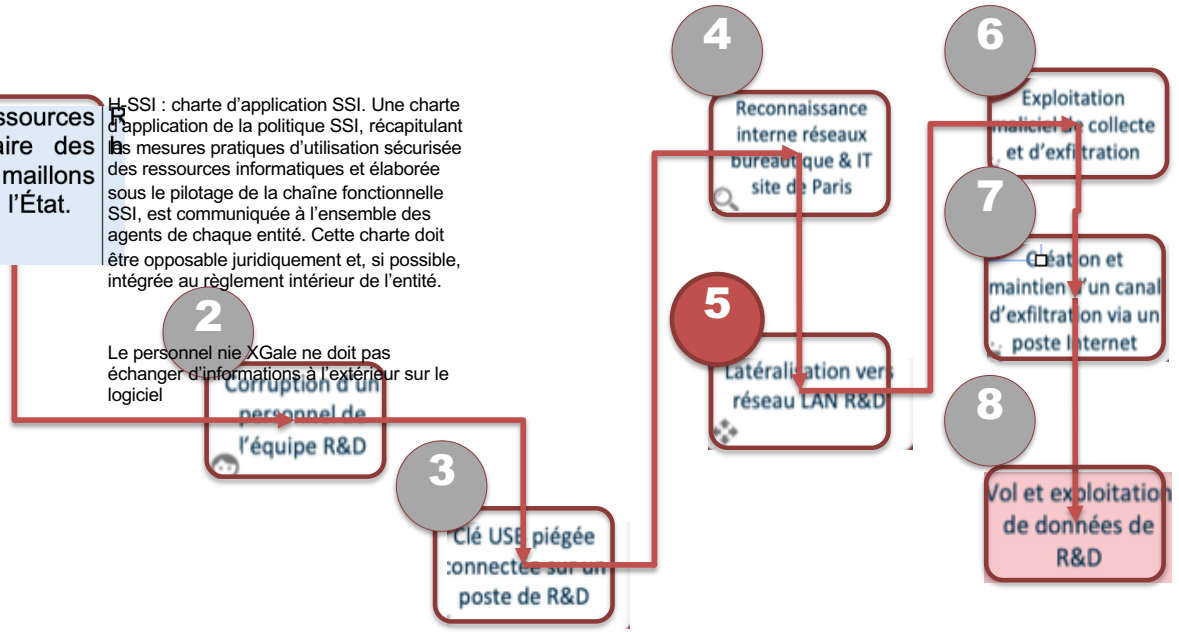
Ressources humaines

1.3 Travail 2 : atelier « Scenario Opérationnel » 3 points

Phases scenario opérationnel	Actions malveillantes	Objectif l'attaque	de Pré-requis techniques nécessaires pour engager l'action	Gain de l'attaquant une fois l'action effectuée
CONNAITRE				
RENTRER				
TROUVER				

Tirer partie du salarié GL

Obj : Corruption



Quelles mesures de sécurité pour se protéger des accès aux réseaux internes ?

le cnam

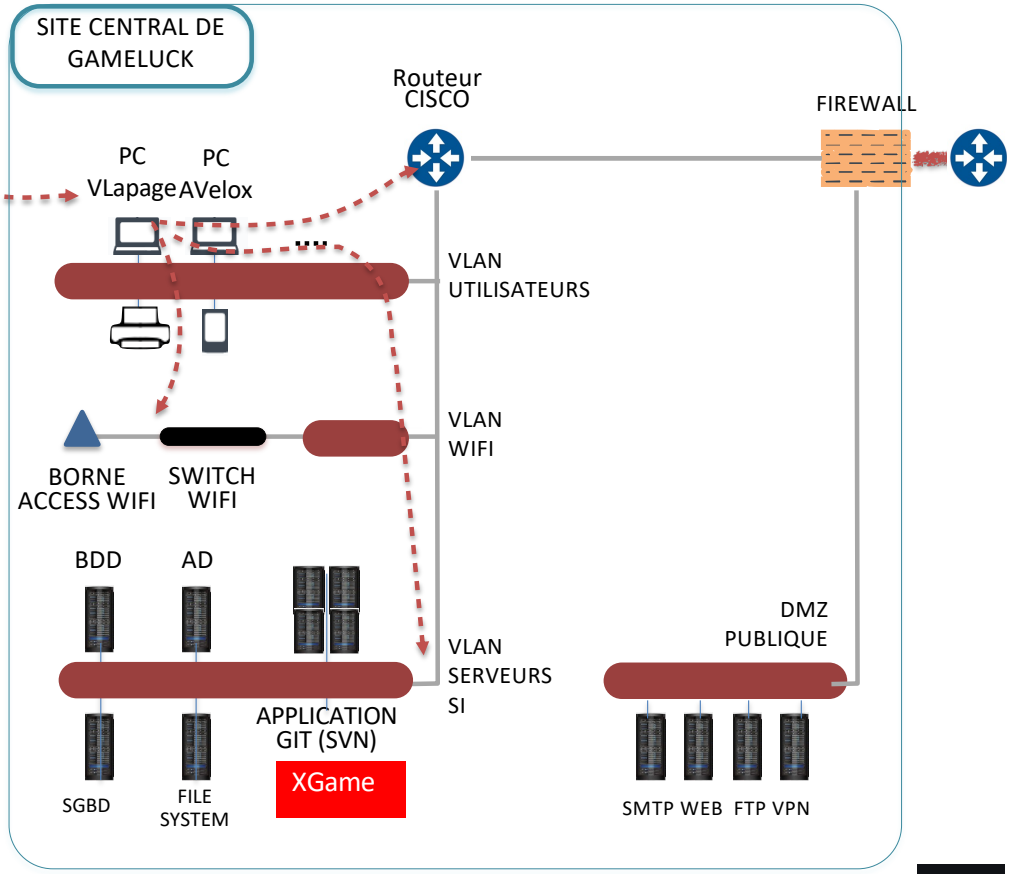
L'attaquant peut se déplacer (latéralisation) vers des sous-réseaux internes car il peut les « toucher » : tester leur présence (map, ping,…), obtenir leurs configurations et cartographier le réseau, scanner les vulnérabilités et les exploiter, lister les partages de fichier et y accéder,…,

```
Switch#vlan database
Switch(vlan)# vlan 2 name VLAN-NUSERS
Switch(vlan)# vlan 3 name VLAN-SERVER-SI
Switch(vlan)# exit
Switch#conf t

Switch(config)# interface FastEthernet2/1
Switch(config-if)# description vers PC
Switch(config-if)# no ip address
Switch(config-if)#  duplex auto
Switch(config-if)#  speed auto
```

```
C:\Users\Administrateur>ne
Ressources partagées de \\

Nom du partage  Type    Ut
-------------------------------
XGAME           Disque
NETLOGON        Disque
profs           Disque
profs2          Disque
```



Pour se protéger de tentatives d'accès aux réseaux internes LAN de la R&D :

5

Mot-clé recherché dans la norme ISO27002 : « réseaux internes » « réseau »

Généralement, les mesures de sécurité destinées à contrer ces tentatives d'accès aux réseaux internes sont :

- Clause **05** : des mesures de gouvernance de la cybersécurité,
- Clause **06** : des mesures fixant les responsabilités de la sécurité,
- Clause **12** : des mesures de sécurisation de l'exploitation informatique,
- Clause **13** : des mesures de sécurité de l'architecture de communication des réseaux.

le cnam

Généralement, les mesures pour bloquer les tentatives d'accès aux réseaux internes peuvent être :

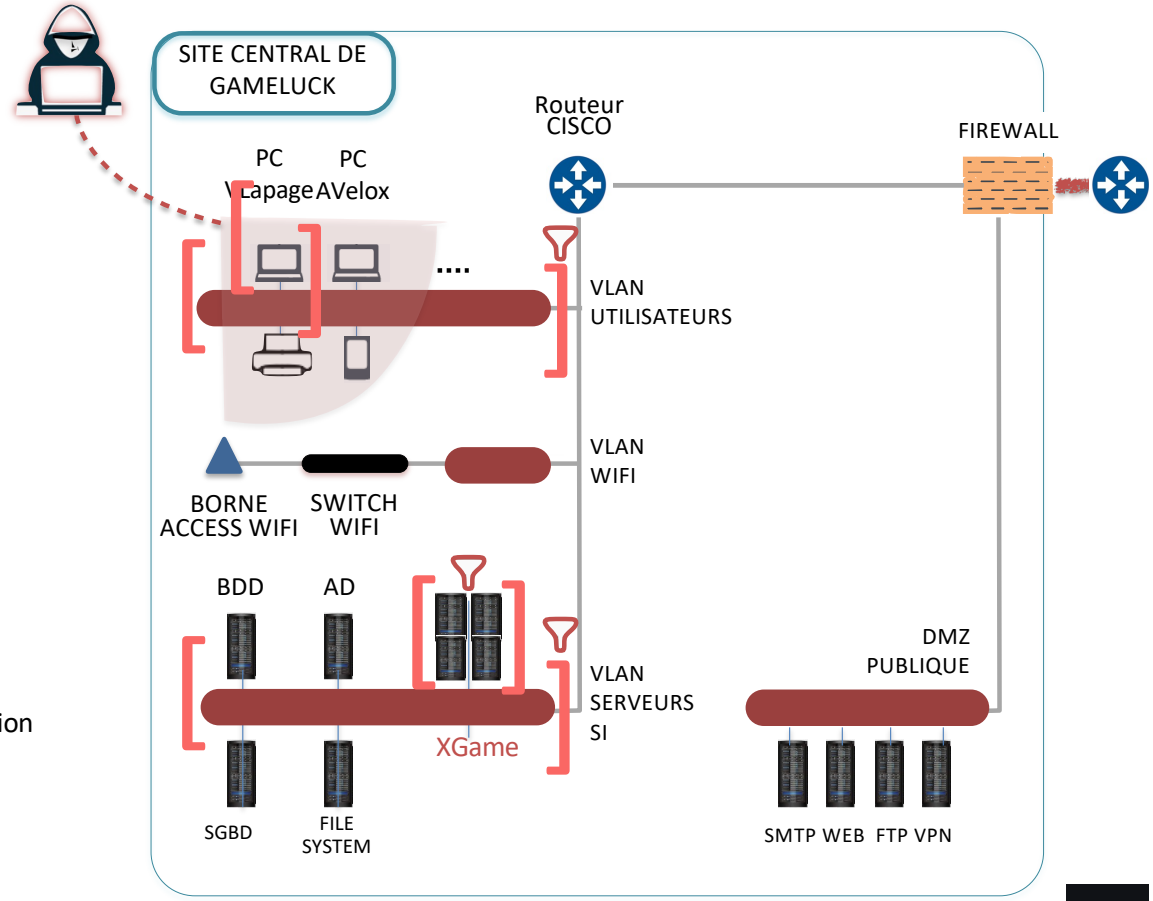
- Clause 13 : Les mesures en lien avec l'architecture de communication des réseaux.
- Clauses :
  - 13.1.1 : Contrôle des réseaux,
  - 13.1.2 : sécurité des services réseaux,
  - **13.1.3 : Cloisonnement des réseaux:**
    - **Confinement.**

Limitation du domaine de diffusion

Cloisonnement

Filtrage des accès

Le cloisonnement pour bloquer les tentatives d'accès aux réseaux internes



Mesures de sécurité organisées par niveau de complexité, statut et échéances

le cnam

Nous avons réalisé la sélection des mesures de sécurité en lien avec les risques évalués.
Le cloisonnement est une mesure essentielle de la défense en profondeur.
Il convient de mettre en place le cloisonnement :
- ☑ des services
- ☑ des réseaux.

MESURE DE SÉCURITÉ	RESPONSABLE	COMPLEXITÉ	ÉCHÉANCE	STATUT
GOUVERNANCE				
Sensibilisation renforcée des collaborateurs de Gameluck	RSSI	faible	fin février 2022	en cours
PROTECTION				
Protection renforcée des données de R&D sur le SI via un cloisonnement, le contrôle d'accès aux serveurs de fichiers et le chiffrement des données	GSIT	élevée	fin janvier 2022	en cours
Renforcement du contrôle d'accès physique aux bureaux de la R&D	Sécurité globale	moyenne	mi mars 2022	A lancer

Clause 12 - Sécurité liée à l'exploitation

- 12.1 Procédures et responsabilités liées à l'exploitation
  - Objectif: S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.
- 12.1.1 Procédures d'exploitation documentées
  - Mesure
  - Il convient de documenter les procédures d'exploitation et de les mettre à disposition de tous les utilisateurs concernés
- 12.1.2 Gestion des changements
  - Mesure
  - Il convient de contrôler les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information qui influent sur la sécurité de l'information.
- 12.1.3 Dimensionnement
  - Mesure
  - Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour garantir les performances exigées du système.
- **12.1.4 Séparation des environnements de développement, de test et d'exploitation**
  - **Mesure**
  - **Il convient de séparer les environnements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.**

Mesure à actionner chez GameLuck :
« restrictions : séparer les environnements »

Clause 13 - Sécurité des communications

- 13 Sécurité des communications
  - 13.1 Management de la sécurité des réseaux
  - Objectif: Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.
- 13.1.1 Contrôle des réseaux
  - Mesure
  - Il convient de gérer et de contrôler les réseaux pour protéger l'information contenue dans les systèmes et les applications.
- 13.1.2 Sécurité des services de réseau
  - Mesure
  - Pour tous les services de réseau, il convient d'identifier les mécanismes de sécurité, les niveaux de service et les exigences de gestion, et de les intégrer dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.
- 13.1.3 Cloisonnement des réseaux
  - Mesure
  - Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient cloisonnés sur les réseaux.

Mesure à actionner chez GameLuck :
« restrictions : cloisonner les réseaux »

le cnam

Comment avez vous défini l'objectif de sécurité ?

Comment identifier/associer les mesures afférentes aux objectifs ?

=> Mesures et objectifs de sécurité

le cnam

Comment identifier et définir l'objectif de sécurité

Depuis le plan de traitement des risques

Élaborer la réalisation du plan de traitement des risques

La suivre par les mesures de sécurité afin de pouvoir prononcer l'homologation de sécurité

Conclusion

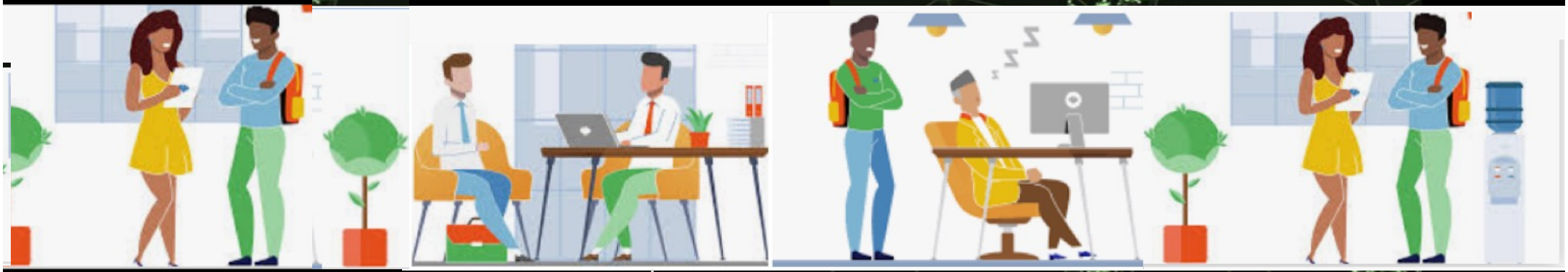
le cnam

L’atelier a permis d’extraire les éléments correctifs à partir des agents menaçants dans le contexte de Gameluck .

Vous allez découvrir l’application des mesures et leurs impacts sur l’architecture.

Atelier

6



le cnam

Atelier 6
Mise en place de mesures correctives techniques (réseau, systèmes d'exploitation, etc.) et organisationnelles

le cnam

L'objectif de ce nouvel atelier est d'apporter une réponse au scénario opérationnel que l'on vient de découvrir.

Le scénario opérationnel présente plusieurs points faibles, le travail présenté dans cet atelier se focalisera sur deux d'entre eux :

- L'exploitation
- L'exploration du réseau interne.

Cet atelier poursuit l'objectif de montrer comment on réalise la transformation d'une architecture existante « vulnérable » en une architecture « plus robuste ».

En entrée, vous aurez le scénario opérationnel en question, en sortie une mesure de sécurité corrective.

le cnam

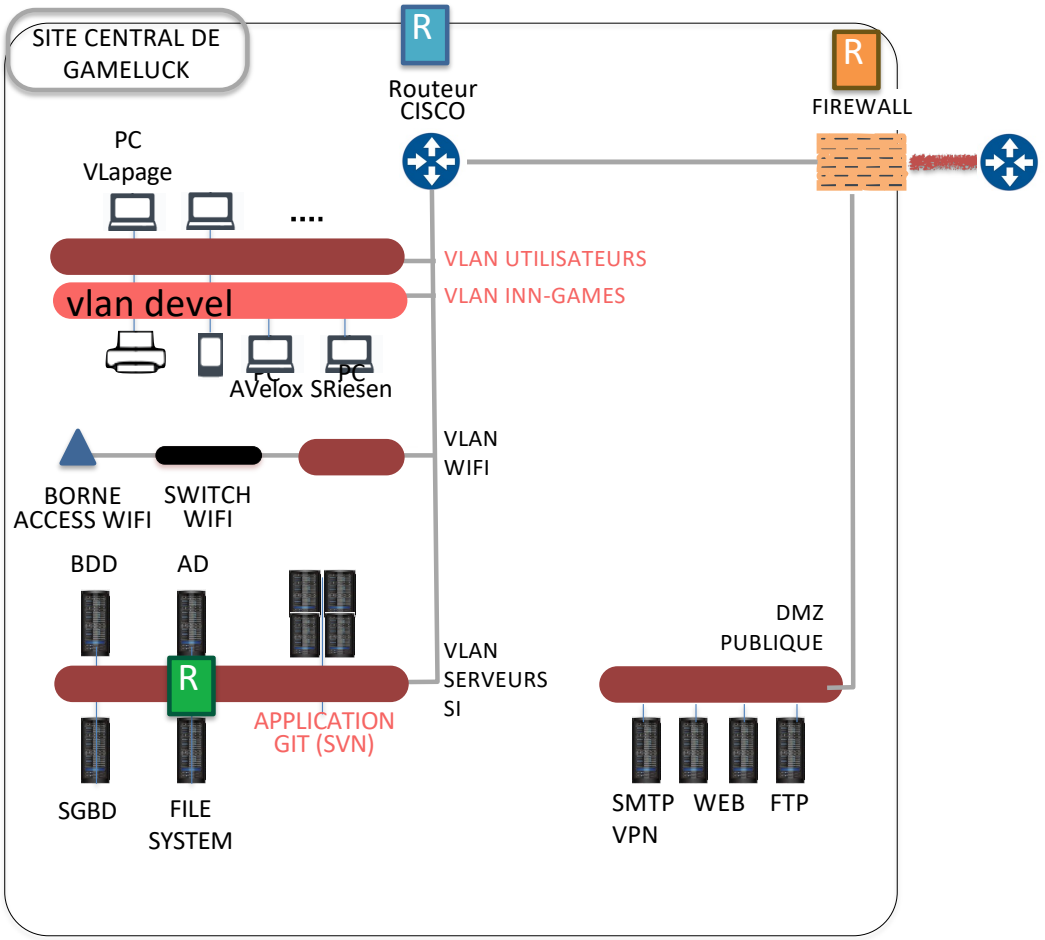
Nous présentons maintenant la mise en place des mesures afin de fournir l'architecture cible :

- Mesure "exploitation »
- Mesure « cloisonnement réseaux »

le cnam

12.1.4 Séparation des environnements de développement, de test et d'exploitation

- Mesure
- Il convient de séparer les environnements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation



R Règles d'authentification (= user appartient à Inn_Games)

R Règles de commutation (ex:domaine de Broadcast, @Mac)

R Règles de FW (matrice de flux)

Mesure « exploitation » ISO/IEC27002-12.1.4

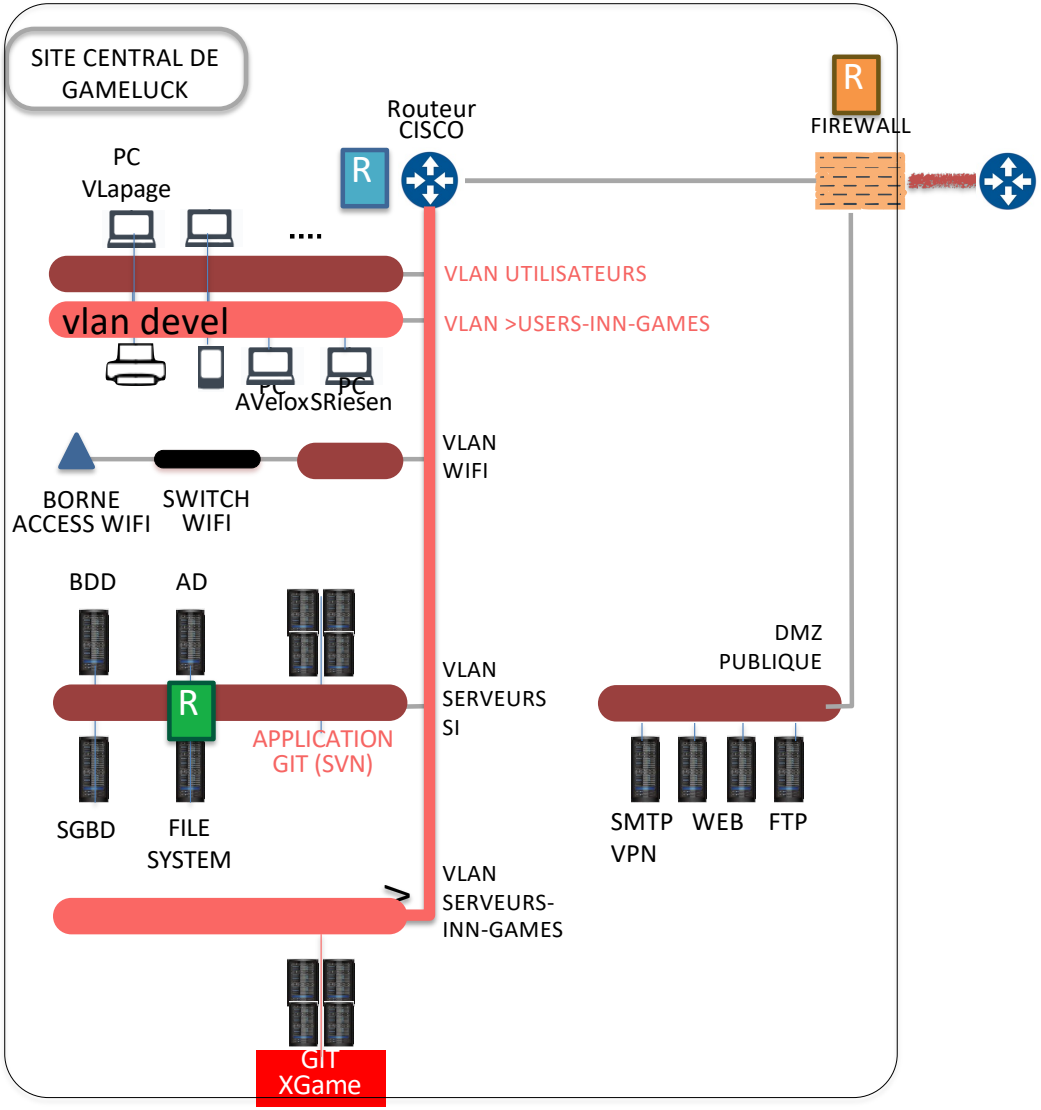
- La politique de sécurité sera :
  - « Il convient de séparer les environnements de développement et de tests pour réduire les risques d'accès non autorisés dans l'environnement d'innovation. »
- Risque :
  - Les utilisateurs Lapage, Velox et les autres partagent le même VLAN « utilisateurs ».
- Action :
  - Créer un VLAN dédié aux développeurs du service innovation, donc actuellement l'équipe de A. Velox.
  - L'avantage est de ne pas permettre d'infiltration ou d'accès d'un VLAN à un autre, et, de protéger les machines de l'équipe innovation d'éventuelles explorations réseau menées par les attaquants depuis les postes des utilisateurs des autres VLANs.

le cnam

13.1.3 Cloisonnement des réseaux

Mesure

Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient cloisonnés sur les réseaux.



R Règles d'authentification (= user appartient au conteneur AD Inn_service)

R Règles de commutation (ex:domaine de Broadcast, @Mac)

R Règles de FW : production d'une matrice de flux

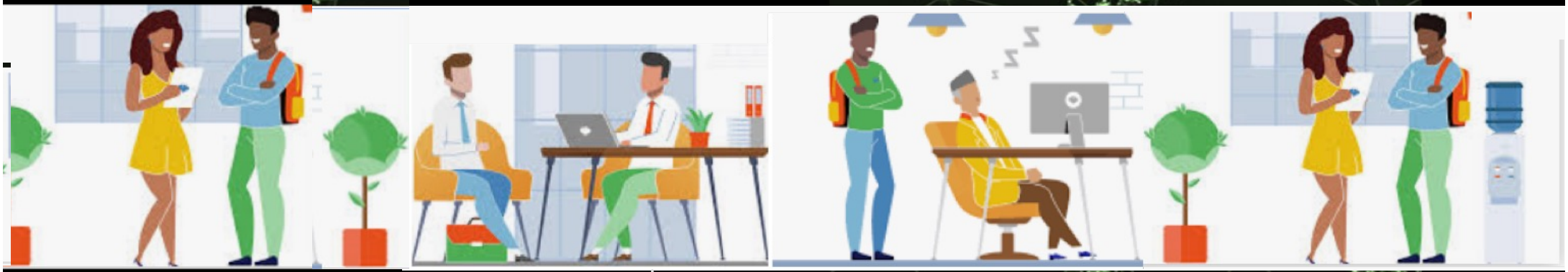
Mesure « exploitation »

- La politique de sécurité sera :
  - « Il convient de séparer les environnements pour réduire les risques d'accès non autorisés dans l'environnement d'innovation. »
- Risque :
  - Les utilisateurs Lapage, Velox et les autres partagent le même VLAN « utilisateurs ».
- Action :
  - créer un VLAN dédié aux développeurs du service innovation, donc actuellement l'équipe de A. Velox.
  - L'avantage est de ne pas permettre d'infiltration ou d'accès d'un VLAN à un autre, et, de protéger les machines de l'équipe innovation d'éventuelles explorations réseau menées par les attaquants depuis les postes des utilisateurs des autres VLANs.

Conclusion

L'exercice a permis de reconfigurer l'architecture par l'ajout d'un VLAN, la mise en place de règles de firewall et d'authentification.

Conclusion



le cnam

Conclusion générale

L'exercice a permis de comprendre l'intérêt des mesures de sécurité afin de corriger une architecture.

Pour y parvenir, vous avez déroulé les éléments de l'analyse de risque en ateliers 1,2,3 , le risque, la menace, vous avez ensuite sélectionné les mesures de sécurité tel qu'elles soient en cohérence avec l'architecture existante .

La prochaine étape sera de produire le document de la PSSI avec sa rédaction.

ALLEZ ….RÉDIGEZ LA PSSI

UPMC SORBONNE UNIVERSITÉS	Politique de Sécurité des systèmes d'information	Edition 1

2.16 Protéger les serveurs

Les serveurs hébergent des données sensibles et fournissent des services numériques. Ils représentent des biens essentiels pour le support des activités métiers des agents.

La sécurité des données (disponibilité, intégrité et confidentialité) et des services (disponibilité et intégrité) dépend du niveau de protection des serveurs qui les hébergent.

Les réseaux assurant l'accès aux données et aux services numériques doivent offrir des garanties de disponibilité et d'intégrité.

- Les environnements de développement, de tests et de production sont séparés.

Conclusion

le cnam

La prochaine étape sera de produire le document de la PSSI avec sa rédaction.