Lettre n°57-Décembre 2016-disponible sur omc.ceis.eu

Brève du mois

« Cyber was the tool to use in the disinformation war. The overaching campaign is the information war.», Léo Taddeo, ancien agent en charge des opérations spéciales cyber au FBI, au sujet de la réponse américaine au piratage du parti démocrate[1].

TABLE DES MATIERES

[1] http://www.nytimes.com/2016/12/15/us/politics/russia-hack-election-trump-obama.html

SERIOUS GAME : QUEL APPORT EN MATIERE DE SENSIBILISATION ET DE FORMATION A LA CYBERSECURITE ?

80 % des vulnérabilités exploitées par les attaquants informatiques ont une origine humaine. D'où le besoin vital de faire évoluer les comportements et, donc, de travailler sur la sensibilisation des personnes à l'hygiène et la sécurité numériques. Pour ce faire, de nombreuses solutions de « serious game » ont émergé ces dernières années. Si toutes partagent un objectif « sérieux », elles se différencient en revanche très nettement quant à leurs cibles, leurs contenus et les techniques de « gamification » utilisées.

Cette note n'aborde pas les solutions de « cyber range » ou environnements de simulation technique, même si ceux-ci peuvent aussi être utilisées dans le cadre d'exercices de sensibilisation et des programmes de formation.

Qu'est-ce qu'un *serious game* ?

Le jeu sérieux peut se définir simplement comme la combinaison d'un contenu, d'un objectif « sérieux » et d'une approche ludique (« jeu »). « *La vocation d'un* serious game *est d'inviter l'utilisateur à interagir avec une application informatique dont l'objectif est de combiner des aspects d'enseignement, d'apprentissage, d'entraînement, de communication ou d'information, avec des ressorts ludiques et/ou des technologies issus du jeu vidéo*. »[2]

Depuis les années 2000, de nombreux scientifiques expliquent en effet qu'un état d'esprit jovial stimule la créativité et l'innovation. Cela permet notamment de débarrasser l'individu des émotions qui le brident, telles que la honte ou une sensation exacerbée de responsabilité. Les systèmes de récompense / renforcement (aussi appelés systèmes hédoniques) propres aux jeux vidéo favorisent en outre l'apprentissage. Il s'agit en effet d'un système fonctionnel fondamental des mammifères, indispensable à la survie car il fournit la motivation nécessaire à la réalisation d'actions ou de comportements adaptés, y compris dans des situations de danger. Ainsi, si le terme de « jeu sérieux » peut sonner comme un oxymore, c'est sa double nature qui le rend si puissant : ensemble, ces éléments paradoxaux entraînent un engagement profond (aussi appelé état d'écoulement) dans lequel les participants perdent la notion du temps et font preuve de tolérance face aux ambiguïtés et aux incertitudes, et sont donc particulièrement constructifs.

[2] http://ja.games.free.fr/ludoscience/PDF/EtudeIDATE08_VF.pdf

Un marché florissant

L'essor du *serious game* dans les années 2000 est notamment à attribuer au Ministère américain de la défense. Selon un rapport de l'IDATE[3], il existerait même une véritable symbiose sur le marché américain entre le gouvernement et les industriels du *serious game*, notamment en raison des investissements majeurs consentis par les différents organismes liés au ministère de la Défense, notamment par la DARPA (Defence Advanced Research Projects Agency), la CIA et la NSA. Le Small Business Act impose en effet aux différents ministères de consacrer 10% de leur budget au développement des PME, ce qui a permis l'émergence de nombreux jeux sérieux, ce type de solution correspondant davantage aux petites structures. Une société comme Wombat Security Technologies, aujourd'hui identifiée comme l'un des leaders du marché dans le Magic Quadrant de Gartner, a ainsi reçu 850 000 dollars pour développer une plateforme de micro-gaming dédiée à la sensibilisation et la formation à la cybersécurité du personnel de l'US Air Force[4].

Toujours selon l'IDATE[5], le marché était estimé à plus de 4 milliards d'euros en 2015, et celui-ci doublerait d'ici à 2018[6]. Le marché français suivrait une tendance similaire, passant de 70 millions d'euros en 2014 à 125 millions d'euros d'ici 2018.

Estimations du marché français et mondial du serious game – source : IDATE

Les *serious games* sont ainsi utilisés dans nombre d'entreprises du CAC 40 ainsi que par certaines administrations publiques[7] pour accompagner des changements, qu'il s'agisse de sûreté, de qualité, de sécurité, de politique RH etc. Cette tendance est encore renforcée par le développement de la « conformité » à l'anglo-saxonne, puisque celle-ci vise notamment à se prémunir contre les comportements à risque des salariés et à prouver, grâce au suivi de *Key Performance Indicators*, que l'on a mis en œuvre les outils nécessaires.

---

[3] http://ja.games.free.fr/Introduction_au_Serious_Game.pdf

[4] http://www.forbes.com/sites/oliverchiang/2010/10/08/wombat-security-makes-videogames-that-teach-cybersecurity-awareness-nabs-750000-us-airforce-contract/#22c65356a469

[5] http://www.ludoscience.com/files/ressources/10213---Serious-Games.pdf

[6] http://fr.slideshare.net/Hekfir/2014-05-serious-game-timeinteraction-games

[7] http://www.latribune.fr/technos-medias/electronique/20141119tribfe3179ee2/le-cac-40-de-plus-en-plus-accro-aux-jeux-video.html

Parmi les avantages des jeux sérieux cités par les directions RH et formation : la transformation du salarié en « acteur » de sa propre formation, l'immersion du participant grâce à une mise en situation réaliste et immersive, la capacité à rendre attractifs des sujets perçus comme rébarbatifs, ou tout du moins éloignés des préoccupations « business », la possibilité de rejouer la formation autant de fois que souhaité, ce qui transforme l'outil de formation en dispositif d'entraînement, l'absence de jugement extérieur, et donc de pression.

Panorama des solutions du marché

La cybersécurité, et plus simplement l'hygiène numérique, offrent donc un terrain de choix pour le *serious gaming*. Il s'agit en effet, tout d'abord, de travailler sur les comportements quotidiens des utilisateurs, afin d'éviter qu'ils ne deviennent malgré eux les complices d'une fuite de données, d'un sabotage informatique, d'un chantage etc.

Le tableau ci-dessous dresse une liste non exhaustive de sociétés et de solutions spécialisées. Si la plupart sont d'origine américaines, quelques acteurs français émergent toutefois comme Conscio Technologies ou Getzem Secure. Les Pays-Bas apparaissent aussi en pointe sur le sujet avec une forte implication du Gouvernement qui a lancé, avec un consortium d'entreprises, un jeu sérieux baptisé ThreatBattle destiné à la sensibilisation à la cybersécurité[8].

Nom de l'entreprise	**Observations**	**Site web**
B4 Communication	Propose un jeu baptisé Security Game.	https://www.securitygame.biz/
BeOne Development	Propose différents formats : vidéos, e learning, outils de simulation (solution BePhished).	https://www.beonedevelopment.com/
BIG (Business Interactive Games)	Start-up franco-américaine spécialisée dans les *decision game*. Propose un environnement de simulation décisionnelle sur la cybersécurité.	http://www.bi-games.com/cc/
Blackfin	Filiale de Symantec proposant des formations	http://www.blackfinsecurity.com/

[8] http://arno.uvt.nl/show.cgi?fid=136774

security	techniques et des campagnes de sensibilisation.	
Conscio technologies	Deux solutions phare : RapidAwareness (campagnes de sensibilisation clés en main sur 5 thématiques) ou prestations sur mesure avec Sensiwave.	http://www.conscio-technologies.com/
Crisotech	Spécialisée dans la gestion de crise. Solution « Keep it safe » sur la sûreté de l'information. Le participant est placé dans la peau de l'attaquant.	http://crisotech.com/fr/nos-produits/keep-it-safe/
Daesign / CIGREF	*Serious game* Keep an eye out. Développé par Daesign pour le compte du CIGREF avec des contenus élaborés par l'INHESJ.	http://www.daesign.com/portfolio/serious-game-securite-informatique/
Digital defense	Outre des prestations d'audit et de pentesting, propose aussi une plateforme de sensibilisation	https://www.digitaldefense.com/
Digitec Interactive	A lancé en septembre 2016 NetDefense Pro, jeu en ligne destiné aux PME.	https://www.netdefensepro.com/
Gaming Works	Spécialisée dans les *business game*. Propose Ocean's 99, jeu d'une journée pour 8-12 participants sur la cybersécurité et la résilience.	http://www.gamingworks.nl/
Getzem secure	Propose le *serious game* Info-Sentinel. Le joueur y joue le rôle d'un	http://www.info-sentinel.com/

	enquêteur. A notamment été utilisé par Safran ou Engie.	
Global Learning systems	Propose notamment des jeux de rôle pour les fonctions IT.	http://www.globallearningsystems.com/
Inspired eLearning	Propose Phishproof pour des campagnes de phishing de sensibilisation.	http://www.inspiredelearning.com/
Junglemap	A lancé le concept de « *nanolearning* » se traduisant par des enseignements de 2 à 4 minutes répétés de nombreuses fois.	http://www.junglemap.com/
Knowbe4	Simulateur de *ransomware* baptisé RanSom pour savoir si son poste de travail est vulnérable à différents types de *ransomware*.	https://www.knowbe4.com/
MediaPro	Un environnement de sensibilisation complet avec une librairie de situations permettant de personnaliser le support de sensibilisation.	https://www.mediapro.com/courses/cyber-security-awareness-training/
Optiv security	Plateforme de e learning interactif baptisée CyberBot.	https://www.optiv.com/
Phishline	Simulation de phishing mail, téléphone, SMS ou d'attaques par clés USB.	http://www.phishline.com/
PhishMe	L'un des leaders des solutions de sensibilisation anti-phishing avec Phishme simulator.	https://phishme.com/
Popcorn	Spécialisée dans le *story telling* et la mise en scène	http://popcorntraining.com/

training	d'histoires réelles.	
PwC	Game of Threats™ a pour objectif de sensibiliser les comités exécutifs et de tester les processus de gestion de crise.	http://www.pwc.fr/fr/vos-enjeux/cybersecurite/game-of-threats.html
Secure Mentem	Ont créé un programme spécifique dans le cadre du National Cyber Security Awareness Month aux Etats-Unis.	http://www.securementem.com/
Security Innovation	Large scope de sensibilisations et de formations de la sécurité applicative pour les développeurs jusqu'à la sensibilisation du management. Réalise également des hackatons associant équipes de développement et experts sécurité pour qualifier des systèmes.	https://www.securityinnovation.com/
Security Mentor	Un concept simple : "brief, frequent, focused"	http://www.securitymentor.com/
SparkCognition	Spécialisée en intelligence artificielle. A développé avec Circadence une plateforme de simulation et d'entrainement.	https://sparkcognition.com/ https://communityimpact.com/austin/news/2015/08/20/northwest-austin-tech-start-up-creates-cyber-warriors/
Terranova WW.	Offre une plateforme de sensibilisation complète mais également un outil de simulation de phishing.	https://terranovacorporation.com/fr/
The security Awareness Co.	Offre comprenant des quizz, des vidéos de sensibilisation, du e-learning.	http://www.thesecurityawarenesscompany.com/

WisdomTools	Solution DIGI Cybersecurity for business	http://www.wisdomtools.com/
Wombat Security Technologies	Propose une plateforme de sensibilisation complète ainsi qu'un outil de simulation de phishing. A fourni une plateforme à l'US Air Force.	https://www.wombatsecurity.com/
Valtech	Agence de formation en marketing digital. Propose un programme de formation sur la sécurité des objets connectés destiné à aider les développeurs et les architectes à comprendre les problèmes de sécurité.	http://www.valtech-training.fr/formation/developpement-web/objets-connectes/
CyberCiege	*Serious game* financé par l'US Navy. Développé dès 2004 par Rivermind. Utilisé par les agences fédérales américaines. Modèle : SimCity. Cible : les fonctions IT.	http://cyberciege.com/
SANS	Propose Netwars, une suite de scénarios interactifs pour professionnels de l'IT.	http://www.sans.org
Kaspersky	Propose Kaspersky Interactive Protection Simulation (KIPS), un jeu de simulation en équipe. Objectif : faciliter les échanges entre CxO, busness, IT.	https://ws.kips.site/
TrendMicro	Propose un jeu en ligne sur les attaques ciblées visant les entreprises. Le joueur est placé dans la peau du DSI d'une entreprise fictive, « The	http://targetedattacks.trendmicro.com/cyoa/fra/ http://www.trendmicro.fr/newsroom/pr/le-jeu-trend-micro-lance-un-jeu-de-simulation-pour-sensibiliser-aux-enjeux-des-attaques-cibles-pour-les-entreprises/

	Fugle », et doit prendre les bonnes décisions quant à la sécurité de l'entreprise, peu avant le lancement d'un produit majeur.	

Source : Gartner et CEIS

Comment choisir une solution ?

Au plan fonctionnel, la plupart des acteurs proposent des *serious game* sous la forme de *e-learning*, alternant phases de mise en situation, résolution de problèmes et apports théoriques, s'intégrant dans des plateformes LMS (*Learning Management System*) pour gérer des campagnes de sensibilisation complètes. Nombreux sont également ceux proposant des outils de simulation de *phishing* permettant d'organiser des campagnes de *phishing* simulées.

Certaines proposent cependant des concepts innovants en termes de micro-gaming permettant d'intégrer des périodes de formation très courtes dans la vie professionnelle des utilisateurs. Quelques-unes, comme Business Interactive Games, offrent également des environnements de simulation doublés de scénarios permettant de faire interagir les participants. Ces « business games » permettent, grâce à des modèles (d'entreprises, de marchés…) et à un moteur d'analyse sophistiqué, de mesurer les performances de chaque participant ou de chaque équipe en fonction des décisions prises par les joueurs. Leur intérêt réside donc non seulement dans la sensibilisation ou la formation des participants, mais aussi dans le brainstorming et l'évaluation de politiques ou de dispositifs de sécurité.

Des jeux purement « papier » offrent enfin un intérêt certain en favorisant la discussion entre les participants et les experts sécurité.

Pour choisir une solution adaptée, il est ainsi possible d'utiliser la grille d'analyse suivante :

- L'objectif : s'agit de sensibilisation ? De formation ? D'entrainements réguliers ?
- La cible : top management ? Fonctions IT ? Métiers ?
- Le périmètre thématique, qu'il soit technologique (APT, phishing, ransomware…) ou contextuel (sécurité en déplacement, sécurité au bureau…) ;
- Les techniques de gamification (mécanique de progression sous la forme de points, de badges…) ;
- Le niveau d'immersion ;
- Le niveau d'interaction attendu : e-learning individuel ? Jeu collectif ?
- L'intérêt du scénario et la qualité du « storytelling », l'intérêt étant de placer le joueur dans une situation inattendue et donc de le pousser à penser différemment ;
- Le niveau d'intelligence : simple enchainement d'actions simples ou capacité d'analyse sophistiquée, voire d'apprentissage ?
- Le support et le mode de diffusion : plateforme SaaS, solution « on-premise », jeu « papier » ;
- Le niveau de personnalisation possible (utile pour personnaliser le jeu en fonction de l'environnement « métier »).

Si les solutions de *serious game* peuvent contribuer de façon importante à la stratégie de cybersécurité d'une organisation, la solution ultime pourrait consister en la « gamification » des outils informatiques quotidiens et des processus clés d'une entreprise pour favoriser l'intégration de la sécurité dans la vie réelle. Digital Guardian, spécialisée dans les solutions de Data Loss Prevention, propose ainsi de décerner aux utilisateurs qui respectent la politique de sécurité de l'entreprise des récompenses[9] : l'utilisateur qui envoie ainsi 500 emails sans violer la politique de sécurité se voit ainsi promu « general data defender ».

Cyber Strategia : le jeu de stratégie de la Réserve citoyenne cyberdéfense

Développé par un groupe de réservistes citoyens, Cyber Strategia est un jeu de stratégie de « plateau » destiné à faire découvrir au plus grand nombre les enjeux de cybersécurité et de cyberdéfense. Pour privilégier la discussion et l'interaction directe entre les joueurs, le parti pris des concepteurs est de parler d'informatique sans informatique… Disponible à partir de mi-janvier 2017, ce jeu sera exclusivement distribué par le Ministère de la défense et les différents souscripteurs ayant financé l'opération, parmi lesquels l'ANSSI et différentes entreprises spécialisées en cybersécurité.

[9] https://techcrunch.com/2016/03/31/meeting-cybersecurity-challenges-through-gamification/

QUALIFICATION D'UN SI : LES APPORTS DU CONCEPT RED TEAM / BLUE TEAM ?

En ces temps de disette budgétaire, la qualification d'un Système d'Information est un exercice coûteux et chronophage : de la rédaction du plan de tests à la réception des résultats, elle peut durer des mois selon la complexité du SI à valider. Pourtant, lors de la réception d'un SI, les phases de qualification sont nécessaires. La menace n'est en effet plus exclusivement externe, aussi nécessite-t-elle de vérifier toutes les barrières de sécurité, y compris celles dédiées aux zones d'exploitation du système, afin de vérifier l'ensemble des données sensibles (l'extraction de données critiques par exemple, d'un utilisateur lambda ou par un administrateur avec des accès privilégiés).

La sécurité d'un système d'information d'un point de vue défensif consiste à mettre en place les mesures de sécurité actives et passives nécessaires à la protection du système. Malheureusement, la mise en place de ces mesures ne signifie pas que celles-ci soient toutes effectives, voire même qu'elles répondent aux besoins propres de protection du SI. Aussi est-il indispensable de qualifier et de vérifier la robustesse d'un système et de contrôler sa réaction face à différents niveaux d'attaque. Il est cependant inévitable que dans la vie de celui-ci l'efficacité des mesures de sécurité va s'affaiblir.

L'objectif d'un *pentest* « standard », comme il en existe depuis des années, est de lister un grand nombre de vulnérabilités sans lien concret entre elles, puis de les énumérer dans un rapport type « audit approfondi » de sécurité. Cette démarche n'est souvent pas exhaustive, car elle n'aborde qu'une partie du système d'information, le plus souvent celle dont le niveau d'exposition est le plus critique (l'accès Internet par exemple).

Quels sont les apports du concept *Red Team / Blue Team*, plébiscité outre atlantique, et quels en sont les clés de réussite ?

Les origines du concept

Pour contourner ces problèmes de budget et de calendrier, pour former et améliorer l'efficacité des équipes d'administrateurs qui auront la charge de gérer le système d'information, le département de la Défense a développé un concept de *Red Team / Blue Team*[10].

Les exercices de cybersécurité *Red Team / Blue Team,* tirent leur nom de leur origine militaire. Dès la fin des années 90, les experts du DoD ont ainsi commencé à utiliser cette approche pour tester les systèmes d'information. L'idée est simple : un groupe de professionnels de la sécurité, une équipe rouge, attaque un système d'information, alors qu'un groupe adverse, l'équipe bleue, essaye de le défendre. D'abord utilisé pour tester la sécurité physique des sites sensibles tels que les installations nucléaires, le concept a ensuite été décliné pour tester la robustesse d'une architecture de sécurité informatique et de l'organisation humaine autour de celle-ci.

[10] http://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blue-team.html
http://www.csoonline.com/article/2122440/emergency-preparedness/red-team-versus-blue-team--how-to-run-an-effective-simulation.html

Le terme « équipe rouge » est traditionnellement utilisé pour identifier des groupes hautement qualifiés et organisés. Cette équipe, dotée des mêmes compétences et des mêmes outils qu'un pirate informatique, agit comme rival fictif et / ou ennemi des forces « régulières » qui constituent l'équipe bleue.

Dans cette approche initiale l'objectif de l'équipe attaquante est de tracer un chemin partant d'une personne malveillante, interne ou externe, et allant jusqu'à la réalisation d'une ou plusieurs actions critiques au sein du système d'information ciblé (appelé aussi « exploit » dans le jargon des hackers).

Les actions de la *Red Team* et de la *Blue Team*

Adopter la mentalité d'un attaquant dans les phases de conception d'un système peut aider efficacement une organisation à améliorer ses chances de se protéger contre des menaces toujours changeantes. Dans les faits, il n'est plus question de lancer quelques outils automatiques pour tester la présence de portes ouvertes à l'aide d'un scanner de vulnérabilités, mais d'aller plus loin dans la démarche, en utilisant ces portes ouvertes de la même manière qu'un hacker peut le faire pour s'introduire dans un système. Dans cette approche, l'équipe rouge doit montrer à l'équipe bleue que les données sensibles à protéger sont bien accessibles par un chemin qu'elle ne protège pas, c'est le principe des chemins d'attaque.

Concrètement, les activités hostiles de l'équipe rouge se présentent sous la forme de tests de pénétration sophistiqués dont les résultats constituent une évaluation fiable des capacités défensives d'une organisation et du niveau de robustesse des barrières de sécurité. L'équipe rouge, dont l'action est strictement encadrée, engage des opérations offensives pour évaluer le niveau de vulnérabilité du système. Ces exercices permettent d'améliorer de façon continue son niveau de sécurité. L'équipe rouge tente de contourner les mesures prévues. Elle s'appuie sur sa propre expertise et sur une base d'outils pour explorer toutes les façons possibles de planifier et de mener une attaque. L'objectif est d'avoir la vision et la même approche que des assaillants potentiels. Généralement, l'équipe rouge peut être amenée à :

- Accéder à des informations sensibles ou classifiées ;
- Bloquer un système en montrant l'impact sur la productivité ;
- Atteindre à la chaîne de production pour les systèmes SCADA (Supervisory Control and Data Acquisition) ou ICS (Industrial Control System) ;
- Infecter durablement et profondément dans les systèmes (*malware/botnet*).

L'équipe rouge peut aussi recevoir une tâche très spécifique, comme par exemple, évaluer l'accès aux données sensibles stockées dans une base de données. Dans un tel scénario, le groupe agit comme un agent de menace externe, cherchant d'abord à « reconnaître » la cible et à identifier ses points faibles, qu'il s'agisse de vulnérabilités concernant les personnes, les processus ou les technologies (PPT ou People, Process and Technology). Pour essayer de contourner ces mesures de protection, les membres de l'équipe rouge doivent évaluer rapidement le potentiel de l'équipe bleue à gérer son système. Ils doivent pouvoir évaluer les procédures tactiques, techniques, et organisationnelles adverses, mises en œuvre. L'équipe rouge doit aussi maîtriser l'utilisation d'outils offensifs (par exemple, *Meterpreter* ou *Metasploit*) et scanners de ports (*Nmap*), connaître les principales techniques d'attaque (comme les injections SQL), utiliser des langages de script, reconnaître les commandes du routeur et du pare-feu, etc.

Pendant ce temps, l'équipe bleue est chargée de préparer sa défense. Bien que le rôle de l'équipe rouge soit généralement défini, celui de l'équipe bleue (et donc celui des analystes et des gestionnaires du Centre de

Supervision de la Sécurité) est dans un premier temps plus flou, ces derniers ne sachant pas *a priori* à quoi s'attendre et quelles parties du système surveiller précisément.

L'équipe bleue est censée comprendre toutes phases d'une réponse aux incidents :

- Maîtriser sa propre boîte à outils ;
- Identifier les schémas de trafic suspects ;
- Isoler les indicateurs de compromission ;
- Utiliser correctement un IDS ;
- Effectuer des analyses et des tests d'intégrité sur les différents systèmes d'exploitation.

L'objectif permanent de l'équipe bleue est de bloquer, détecter et atténuer les attaques de l'équipe rouge. Elle essaye de contrer en temps réel les attaques en corrigeant les nouvelles vulnérabilités identifiées par la *Red Team*. Elle améliore aussi de manière continue la politique de sécurité et alimente le dossier de vulnérabilités résiduelles. La formation des administrateurs est donc indispensable pour cette phase de qualification. D'autres actions de vérification régulière consistent à accéder aux données générées par chaque élément logiciel du système (les journaux comprenant des alertes). Un outil de corrélation permet d'obtenir des informations sur l'analyse du trafic et des flux de données, mais il permet surtout d'interpréter les comportements anormaux et, bien évidemment, de mettre en évidence les menaces et les vulnérabilités sur le système.

Sur le volet surveillance, il s'agira pour l'équipe bleue d'évaluer :

- L'efficacité et la performance des outils de supervision de sécurité du SOC ;
- La pertinence des mesures de réaction que vont déclencher l'équipe bleue dans le cas d'une crise majeure.

Les outils de centralisation et de traitement des incidents de sécurité sont en effet paramétrés à partir d'une stratégie de surveillance définie en amont pour chaque type de déploiement d'un SI et en fonction de la criticité de la mission. Si les outils réagissent peu, l'équipe bleue doit contrôler toute la chaine de remontée des journaux ou puiser dans une base de journaux bruts pour comprendre le manque d'information. Elle pourra ensuite paramétrer les mesures de sécurité pour couvrir les vulnérabilités identifiées lors des tests. Dès qu'un problème est identifié, un re-paramétrage des outils et processus du SOC doit être réalisé, jusqu'à rendre efficiente la stratégie de surveillance vis-à-vis du niveau d'attaque de l'équipe rouge.

Qualifier un SI par l'approche *Red Team / Blue Team* : une opportunité pour former efficacement les opérateurs ?

Au sein de l'OTAN par exemple, lors des exercices de cybersécurité, l'approche *Red Team / Blue Team* est parfaitement intégrée. Les activités de validation d'architectures de sécurité d'un système d'information s'adaptent aux nouvelles tendances en adoptant cette démarche. Les systèmes alliés sont régulièrement testés par une équipe rouge identifiée, pour mesurer la performance des principales barrières de sécurité mises en œuvre. Dans ce type d'exercice, l'équipe attaquante doit être en mesure de montrer qu'une combinaison d'actions (allant du recueil d'information auprès d'une personne vulnérable et ayant accès au système cible) à l'exploitation de vulnérabilités techniques peut mettre à mal le système d'information d'une armée alliée, jusqu'à se propager sur l'ensemble des systèmes connectés.

L'approche *Red / Blue Team* a aussi l'avantage de :

- Qualifier rapidement la livraison d'un système de communication équipé de nombreux COTS ;
- Vérifier le niveau de sécurité de son architecture, et la robustesse des interfaces vers les systèmes alliés sans passer par une phase d'audit complexe ;
- Corriger dans la foulée les vulnérabilités détectées sans refaire des audits complémentaires ;
- Faire monter en compétence la *Blue Team* dans le SOC.

Ces tests sont l'occasion unique d'évaluer de façon exhaustive l'efficacité des processus d'un Centre Opérationnel de Sécurité à moindre coût et dans un lapse de temps réduit. Pour une attaque réelle, entre la détection d'un incident et la mise en œuvre d'une stratégie de réaction, il peut en effet s'écouler plusieurs heures sans que l'attaque puisse être détectée.

La formation des équipes passe aussi par une synchronisation des actions lors de la phase de préparation de l'exercice. A chaque phase de tests de l'équipe rouge, l'équipe défensive re-paramétre le système pour apporter des améliorations régulières (personnalisation des règles du pare-feu, mise à jour des sondes de détection d'intrusion par exemple), sans remettre en cause le fonctionnement du système. Une veille active des journaux des serveurs de noms (DNS) peut aussi s'avérer rapidement indispensable, car ce service est très sensible aux attaques. Ces actions prioritaires permettent de former les administrateurs à exploiter efficacement les règles de sécurité.

L'approche *Red Team / Blue Team* permet également, à condition que les actions couvrent l'ensemble des fonctions du SI, de raccourcir la démarche de qualification et surtout de la rendre plus efficiente. Les tests peuvent être lancés lors de la conception de l'architecture du système afin d'apporter facilement des améliorations. L'architecture doit être suffisamment bien stabilisée, elle doit être représentative du système dans une version quasi définitive.

La phase la plus appropriée est souvent choisie par le chef du projet juste avant ou après la livraison du système, afin d'enclencher une démarche d'homologation ou de certification. C'est aussi à ce moment précis que la démarche se complexifie, car il est difficile de modifier la politique de sécurité ou d'ajouter des mesures complémentaires sans déclencher des coûts supplémentaires non prévus contractuellement.

Les clés du succès

Comme nous l'avons vu plus haut, les deux équipes doivent accomplir des tâches complexes. L'efficacité de l'équipe rouge dépend tout d'abord de sa capacité à adopter une posture agressive. Il est ainsi souhaitable que ses membres ne soient pas choisis parmi ceux qui ont contribué (ou contribuent toujours) à la défense de l'infrastructure de l'organisation ciblée. Cela risquerait d'engendrer un conflit d'intérêts qui étoufferait l'effort de créativité « hostile ».

Un état d'esprit « extérieur » est indispensable. Il est donc intéressant d'externaliser ce type d'opération ou de s'appuyer sur du personnel non impliqué dans la conception du système. En effet, un vrai assaillant s'affranchira de toutes les règles en vigueur et de toute barrière psychologique. Outre les aspects techniques, les tests doivent également se concentrer sur le point le plus faible du système de sécurité : l'être humain. L'équipe rouge doit mettre en œuvre un certain nombre de pièges pour s'introduire sur le

système, comme les pièces attachées aux courriers électroniques malveillants ou une clé USB laissée à l'abandon. Si l'entreprise ou l'organisation a déjà émis sa propre politique de sécurité, les efforts de l'équipe rouge seront proportionnels. Il s'agira alors de mesurer le niveau d'implication des employés vis-à-vis de cette politique, d'évaluer le niveau de sensibilisation et la discipline des employés, ainsi que la capacité de l'entreprise à appliquer les règles.

Dans ce type d'exercice, l'équipe rouge est là pour aider et non pour entraver la sécurité d'un système. Les deux équipes ont donc besoin de travailler ensemble : l'équipe rouge a pour objectif de servir l'équipe bleue. La relation symbiotique entre *rouge et bleu* amplifie l'efficacité de la démarche de qualification, en améliorant constamment les compétences et les processus des deux équipes. Il s'agit aussi d'établir une communication efficace, de partager les stratégies et les moyens employés, bénéfiques aux deux équipes. Cette relation inclut, par exemple, des explications détaillées sur la façon dont l'équipe rouge a contourné l'IDS ou sur la méthode utilisée par l'équipe bleue pour détecter les signaux faibles. Chacun cherche donc à repousser les limites et à faire mûrir la sécurité du SI. Une telle approche suppose ainsi que les procédures de défense et d'attaque sont partagées à la fin de chaque session.

Alors que l'automatisation peut s'avérer utile, l'équipe bleue ne doit pas se fier uniquement à la technologie. Des deux côtés, l'intuition humaine, l'expertise et l'habileté sont fondamentales. Les techniques d'ingénierie sociale sont ainsi nécessaires pour tester toute la chaine de management de la sécurité. De telles simulations visent ainsi à reproduire une situation d'urgence réelle et à améliorer la capacité des équipes à repousser une agression. Dans le même temps, les membres de l'équipe bleue sont formés et doivent détecter, s'opposer et affaiblir les efforts de l'équipe rouge.

Le succès de l'approche *Red Team vs Blue Team* réside dans l'interaction et la rétroaction mutuelle. L'équipe bleue doit considérer les activités de l'équipe rouge comme l'opportunité de comprendre les tactiques de l'assaillant potentiel. C'est aussi l'occasion pour cette dernière de tester les mesures de réaction et d'évaluer les outils de gestion des incidents.

Si le SOC ne constate pas d'éléments de compromission lors de ces exercices, ceci peut être dû à des insuffisances techniques et organisationnelles dans la configuration des règles de surveillance. Mais il peut aussi s'agir de méthodes d'attaques très ciblées ou inconnues passant « en dessous du radar ». Dans tous les cas, une stratégie de surveillance bien définie est indispensable. Elle permettra une bonne configuration des outils et assurera une détection automatique, à partir de signatures d'attaques connues ou à partir d'une base d'évènements déjà rencontrés. Ces évènements et ces incidents de sécurité relevés dans la phase de qualification constituent le socle et l'historique sur lesquels s'appuiera l'équipe bleue pour exploiter le système dans sa phase de production.

Les limites d'une telle démarche

Les potentielles dérives d'une telle démarche sont multiples : les modifications effectuées par l'équipe rouge peuvent entraver irrémédiablement le fonctionnement du système si les outils utilisés ne sont pas maitrisés. Ces modifications peuvent aussi laisser des portes dérobées, utiles à des attaques réelles. Ainsi, si l'équipe rouge est mal préparée ou équipée d'outils trop intrusifs qu'elle ne maitrise pas (laissant des codes « dormants » sur les machines par exemple), il est préférable de ne pas lancer une telle démarche ou de prévoir une sauvegarde du système avant de lancer ces types de tests. Ce problème se pose moins aujourd'hui, car les nouveaux SI sont généralement équipés de machines virtuelles, ce qui rend la création

de sauvegardes initiales du système relativement aisée. Le système testé doit si possible être déconnecté du système d'information de l'entreprise.

Pour un système complexe, il est nécessaire de l'intégrer dans un environnement de simulation pour en déterminer les performances limites. Cette démarche est particulièrement appréciable pour simuler différents moyens de protection dans le but de former les équipes en charge de sa gestion. La flexibilité de l'environnement de simulation peut aussi apporter une gamme d'outils complète et maitrisée à l'équipe rouge.

La mise en place d'un plan d'attaque et la présentation des outils (de leur efficacité) doivent être réalisées en amont auprès du responsable du projet et des RSSI (ou aux responsables de la chaine SSI pour un ministère). Cette phase peut être longue et durer potentiellement plusieurs jours selon la complexité du système à tester. Elle nécessite en outre de mettre en place un niveau d'attaque gradué, qu'une organisation non étatique peut difficilement obtenir, les ressources en cyber-sécurité devenant rares.

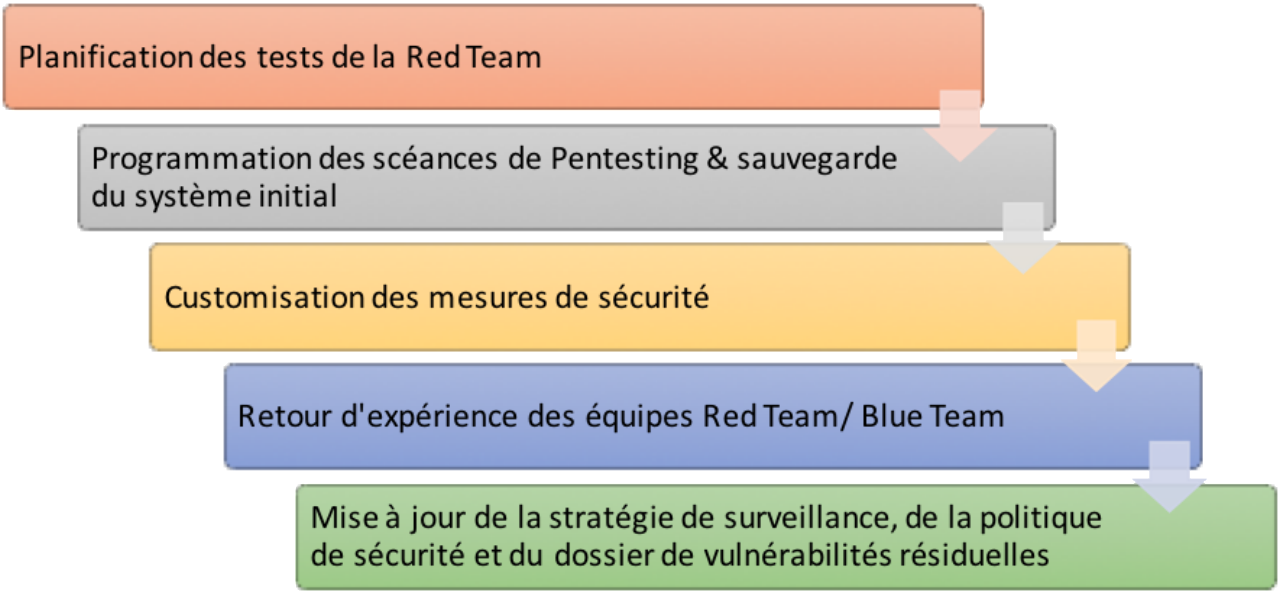
La qualification d'un prestataire jouant le rôle d'une *Red Team* s'avère également nécessaire, mais encore faut-il que l'équipe en charge de cette qualification soit pertinente pour pouvoir apprécier les capacités d'action d'une *Red Team*.

Conclusion

Engager une démarche de qualification de la sécurité d'un SI par l'approche *Red Team / Blue Team* permet de réduire les coûts. Elle permet aussi d'accélérer considérablement la formation des administrateurs d'un SOC et de réduire de manière tangible les vulnérabilités et les failles du système. Cette approche peut être déclinée à partir des étapes détaillées sur le schéma ci-dessous, certaines étapes pouvant être répétées de manière à complexifier les actions de la *Red Team*.

Avant de systématiser une telle démarche, il est important de dimensionner les ressources et mesurer les capacités des équipes rouge et bleu. Il faut également noter que ces gains de temps et de coûts ont une contrepartie : il est difficile de trouver ou former une équipe rouge compétente sur l'ensemble des technologies présentes sur le SI. Cette équipe doit disposer d'outils performants, qu'ils proviennent d'Internet ou de développements « maison ».

Les compétences techniques et les outils ne feront cependant pas tout. Cette approche requiert aussi une grande confiance dans l'équipe rouge. Il s'agit, en effet, de s'assurer que les tests réalisés par cette équipe ne laissent pas une porte ouverte définitive sur le système. La réponse sera dans ce cas principalement juridique : pour une qualification externalisée chez un prestataire, même agréé pour ce type de tests, il s'agira ainsi de définir précisément les limites et les responsabilités de chaque partie. Doit-on imposer à l'équipe rouge des pénalités pour chaque vulnérabilité ou chaque porte dérobée « oubliée » qui serait ultérieurement découverte ? L'exhaustivité des tests d'intrusion et le temps passé par les deux équipes seront les principales variables d'ajustement pour la réussite d'une telle démarche.



La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com