Lettre n°60 - Mars 2017 - disponible sur omc.ceis.eu

Brève du mois

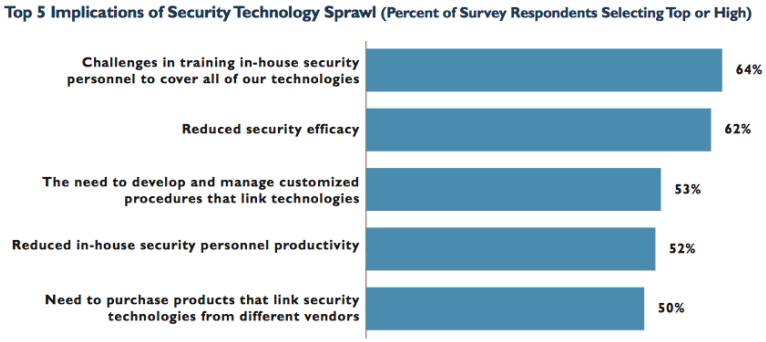
« The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether »[1] - Conclusion du rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans le cadre de la lutte anti-terroriste.

Table des matières

[1] https://theintercept.com/2014/10/15/un-investigator-report-condemns-mass-surveillance/

LUTTE INFORMATIQUE DEFENSIVE : LE ROLE-CLE DES CYBER RANGE EN MATIERE D'ENTRAINEMENT

En matière de sécurité informatique, les organisations sont confrontées à la persistance des cyber-attaques, combinées à la montée en puissance de nouvelles menaces. Parallèlement, elles ne sont pas suffisamment préparées à anticiper les incidents et à y apporter les réponses adéquates. En témoigne l'étude Global Information Security Workforce[2] menée par Frost & Sullivan en 2015, en partenariat avec ISC3 et Booz Allen Hamilton qui souligne que la formation du personnel demeure le défi premier, se traduisant par un investissement conséquent de la part des organisations.



Source : Global Information Security Workforce Study (2015)

Les Cyber Range, environnements de simulation informatique, dédiés non seulement à l'expérimentation des technologies, mais également à la formation par la pratique et à l'entraînement du personnel, constituent une réponse pertinente à ce défi. Initialement développés dans un cadre militaire4, les Cyber Range intéressent aujourd'hui l'ensemble de l'écosystème de cybersécurité. Pouvant offrir des conditions d'entrainement proches du réel, tant dans les topologies réseau reconstituées que dans les technologies de sécurité déployées, ils fournissent un environnement d'affrontement informatique permettant une nouvelle approche de la formation axée sur l'opérationnel. Comment fonctionnent ces environnements ? Quels sont les principaux acteurs du secteur ? Quelles sont les technologies utilisées ?

Caractéristiques-type d'un Cyber Range

Au plan technique, un Cyber Range se caractérise par les éléments suivants :

- Un environnement de simulation informatique multiniveaux. Il est dit « hybride » lorsqu'il permet également de connecter des équipements physiques (routeur, sonde, automate industriel…) ou des *appliances ;*
- Des topologies réseau. L'environnement permet de reproduire de façon relativement fidèle des topologies réseau constituées de plusieurs milliers, voire dizaine de milliers de postes. S'il est

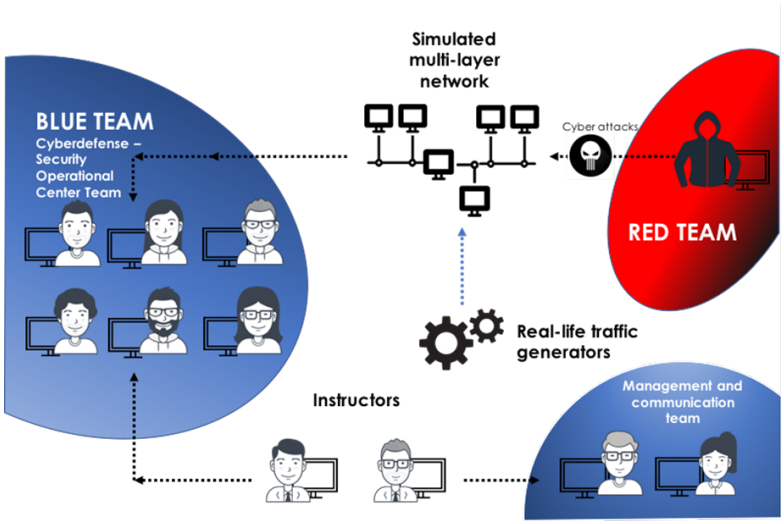
2 https://www.cybercompex.org/fileSendAction/fcType/0/fcOid/445471828686010375/filePointer/445471828686010530/fodoid/445471828686010527/frostsullivan-ISC2-global-information-security-workforce-2015.pdf

3 Organisation mondiale à but non-lucratif, fondée en 1989 et dédiée à l'éducation

4 Le terme « range » étant utilisé en anglais pour désigner un stand de tir, soit un environnement d'entraînement spécifique

basé sur un système de virtualisation traditionnel, la nouveauté réside dans le fait que les administrateurs peuvent créer et configurer très facilement des architectures réseau et des machines grâce à un *back office* adapté ;

- Des technologies de sécurité. Celles-ci peuvent couvrir toute la chaine de lutte informatique défensive depuis les firewalls, les IPS/IDS, les SIEM etc. ;
- Des générateurs de trafic réseau. Ceux-ci injectent dans l'environnement du trafic légitime mais aussi illégitime pour créer le « bruit » inhérent à tout réseau et reproduire le plus fidèlement possible la réalité du terrain.



Source : Bluecyforce

Au plan humain, les Cyber Range s'articulent généralement autour de deux équipes distinctes :

- La « red team », composée de hackers éthiques professionnels, appartenant généralement à l'organisation du Cyber Range. Ceux-ci reproduisent des attaques ciblées et d'ampleur et de complexité croissante, de nature à challenger la défense en fonction de sa marge de progression tout au long de l'entrainement ;
- La « blue team », chargée de la défense des réseaux et systèmes d'information, qui est donc constituée des stagiaires participant au programme d'entrainement.

A la frontière entre les moyens techniques et humains, le Cyber Range devra également mettre en œuvre une pédagogie spécifique, c'est-à-dire les parcours, les contenus et les méthodes permettant de transmettre aux stagiaires non seulement un savoir (les connaissances), mais également un savoir-faire (les capacités) et un savoir-être (les attitudes) répondant aux besoins des organisations clientes en matière de lutte informatique défensive.

Panorama des Cyber Range existants

Les offres de Cyber Range se sont largement développées ces dernières années. Pour un panorama complet du marché, il convient de distinguer les fournisseurs de technologies des prestataires de formation et d'entrainement agissant dans un cadre interne (par exemple un ministère de la défense ou une université) ou au profit de clients extérieurs.

Les fournisseurs de technologies

Différents équipementiers proposent des Cyber Range ou environnements de simulation dédiés à la cybersécurité (voir tableau ci-dessous) : Diateam (France), Cyber Test Systems (France), Cyberbit5 (Israël), Ixia (États-Unis), Ravello Systems6 (États-Unis) et Sypris (États-Unis).

Sociétés	Type d'acteurs	Prestations proposées
CYBERBIT (filiale ELBIT SYSTEMS) Amérique du Nord, Asie et Europe	* Secteur public * Fournisseurs de services * Monde académique * Organisations	Plateforme Cyberbit Range dont les nouvelles fonctionnalités ont été annoncées fin 2016 : * Une formation destinée aux dirigeants d'entreprise * Utilisation du matériel SCADA + protocole ICS/SCADA * Scénarios adaptés aux besoins clients
CYBER TEST SYSTEMS Amérique du Nord, Amérique du Sud, Asie, Moyen-Orient et Europe	* Fabricants d'équipements réseau * Fournisseurs de services haut débit et mobile * Intégrateurs de systèmes * Entreprises * Entrepreneurs de défense * Gouvernements	* Technologie : boitier générateur de trafics légitimes et malveillants (Cyber Test Systems Network Traffic Generator - CTS-NTG), associé à une solution logicielle en charge du contrôle de ce boitier * Des scénarios incluant des attaques ICS/SCADA, des attaques DDoS, DoS, des botnet command-and-control (C&C) communications, etc.
DIATEAM Sur site ou en ligne	* Initialement pour le compte de la Direction Générale de l'Armement, Maîtrise de l'Information (DGA MI) * Aujourd'hui ouvert aux acteurs publics comme privés	Plateforme HNS (Hybrid Network Simulation) adaptée à la formation et l'entraînement cyber, à la gestion des crises cyber, aux extensions ICS/SCADA
IXIA Sur site ou dans les locaux d'Ixia (Ixia's Cyber Defense Academy) - Californie, Royaume-Uni et Singapour	* Cyber Warriors * Organisations publiques * Entreprises souhaitant défendre leurs infrastructures critiques, leur société ainsi que leur réseau Prérequis informatiques : bonne compréhension TCP/IP, routeurs, pare-feu, IDS/IPS, SIEM	* Plateforme tout-en-un de test de sécurité et de performance * Formation et entraînement du personnel à des exercices pratiques relevant de niveaux de difficulté croissants : niveau intermédiaire dans les locaux d'Ixia (3 jours) ou niveau avancé sur site (3 jours ou 5 jours (mêmes sessions que les 3 jours + 2 jours de travaux pratiques sur des scénarios opérationnels)) - Jour 1 : fondamentaux du Cyber Range, des outils de test au Learning Management System (LMS) - Jour 2 : serveurs d'infrastructures critiques et vues d'ensemble des simulateurs d'application - Jour 3 : attaques par des logiciels malveillants, attaques IP, activités de reconnaissance etc.
RAVELLO SYSTEMS (Start up rachetée par Oracle) + SIMSPACE	Entreprises	On-demand Cyber Range * Technologie : Virtual Clone Network (VCN), totalement isolée et indépendante d'internet * Solution : cloner le réseau de l'entreprise dans le Cloud plutôt que d'utiliser le réseau actuel

5 A noter que Cyberbit est l'acteur le plus visible sur internet

6 Oracle a annoncé en février 2016 l'acquisition de la start-up Ravello Systems, tournée sur le Cloud, pour 500 millions de dollars

SYPRIS Electronics (filiale de Sypris Solutions)	* Secteur privé * Propriétaires et exploitants d'infrastructures d'information critiques	* Accent mis sur la Cyber santé des infrastructures d'information critiques * Modélisation et simulation permettant de configurer des environnements virtuels personnalisables, du serveur unique à l'interface extranet/Web * API qui permet l'extension des fonctionnalités par un tiers * Plateforme de formation virtuelle (PFV)

Comme le montre ce tableau, les différents fournisseurs de Cyber Range cherchent à répondre à des besoins variés : tests de performance, validation de solutions, réalisation de tests d'intrusion en environnement fermé, mise en place de *proof of concept*, entrainement…

Cyber Test Systems se positionne ainsi en équipementier grâce à des solutions de génération de trafic7, alors que Cyberbit fournit un environnement clé en main basé sur une infrastructure Cloud privée permettant aux utilisateurs de s'entraîner à n'importe quel moment et à n'importe quel endroit. La plateforme offre plusieurs scénarios d'attaque, intégrant par exemple des attaques par ransomwares. Même offre intégrée pour Diateam avec sa plateforme HNS, version la plus poussée d'HYNESIM[8] (Hybrid Network Simulation), qui propose à chacun de ses clients un véritable Cyber Range privé. Ixia, autre acteur bien connu du marché, propose de son côté sa solution BreakingPoint Storm pour simuler des attaques DDoS9, tandis que Ravello Systems10 permet à ses clients de choisir des topologies réseau déjà configurées, d'adapter l'une de ces dernières, ou de construire son propre réseau personnalisé en fonction de ses besoins et de la durée souhaitée. Enfin, Sypris met en avant un système personnalisable et rapide, extensible en nombre d'utilisateurs, facile d'intégration à d'autres équipements et réseaux, et ayant une architecture ouverte.

Les Cyber Range fermés

Les premiers Cyber Range ont été créés pour des besoins strictement militaires. Au plan multilatéral, c'est le cas, par exemple, de l'Estonian Defence Forces Cyber Range (EDF) mis en place pour l'OTAN et utilisé pour les exercices Locked Shields ainsi que Cyber Coalition. Côté américain, Lockheed Martin a gagné en 2014 un contrat de cinq ans concernant le National Cyber Range (NCR), originellement développé par la DARPA11, et utilisant la plateforme Ixia BreakingPoint. Thalès a, de son côté, monté le centre virtuel d'évaluation et d'entraînement en cybersécurité du Cybercommando du ministère de la Défense (DCC) néerlandais en s'appuyant sur la plateforme HNS de Diateam. La plupart des acteurs du secteur tirent ainsi parti de l'expérience acquise auprès des forces armées. C'est par exemple le cas de SimSpace qui, avec la plateforme de Ravello Systems, fournit aux entreprises une technologie similaire à celle utilisée dans les centres d'entraînement les plus sophistiqués. Sypris exploite de son côté le même registre au plan marketing en présentant son offre comme un véritable sport d'équipe et de combat au sein duquel

7 A l'occasion de la conférence Ignite de Palo Alto Networks, qui s'est tenue du 3 au 6 avril 2016 à Las Vegas, un Cyber Range utilisant la plateforme Cyber Test Systems fut mis en place

8 HYNESIM (GPLV2) pour un usage personnel ou académique et HYNESIM PRO pour un usage professionnel

9 Sur un système BreakingPoint Storm, il est ainsi possible de simuler jusqu'à 90 millions de sessions TCP/IP simultanées

10 La nouvelle offre Cyber d'évaluation, de test et d'entraînement de Ravello Systems et SimSpace a été annoncée en août 2015

11 Defense Advanced Research Projects Agency

les stagiaires entrent dans une compétition en temps réel par le biais d'exercices dynamiques12 et doivent résoudre des challenges de sécurité de difficulté progressive.

Les écoles et universités, qui misent de plus en plus sur la formation continue et l'entrainement, constituent un autre débouché important. Aux États-Unis, l'Université de Californie du Sud s'est déjà dotée d'un Cyber Range et l'Université de San Diego a prévu, dans le cadre de l'ouverture d'un master en cybersécurité, de mettre à la disposition de ses étudiants et partenaires industriels un *training center*. Cette installation permettra à 30 personnes, divisées en deux équipes, de simuler des attaques en ligne et d'apprendre à se défendre13. Depuis 2012, le Michigan Cyber Range (MCR)14, qui regroupe plusieurs organisations dont des universités américaines15, entraîne également les étudiants et professionnels de l'informatique. Le MCR a d'ailleurs initié depuis janvier 2013 un accord avec Mile2, développeur et fournisseur de certifications Cyber Sécurité, de formations certifiées *Ethical Hackers*, *Digital Forensic*, *Penetration Testing*, etc. Le personnel du MCR a notamment mené le 15 octobre 2014 l'exercice « Power Phoenix ». Celui-ci, qui concernait un environnement SCADA compromis, fut mené avec des représentants de deux entreprises d'électricité et de la police de l'État du Michigan.

A Singapour, l'École Polytechnique a lancé en octobre 2013, en collaboration avec eCop, EC Council, Ixia ainsi que ST Electronics (Training & Simulation Systems16), l'Académie Cyber Sécurité qui s'appuie désormais sur un Cyber Range. Ce projet est partie intégrante du National Cyber Security Masterplan 2018 qui a pour objectif de renforcer la sécurité et la résilience de l'infrastructure informatique critique et d'augmenter le bassin d'experts en sécurité informatique à Singapour. La plateforme utilisée est la plateforme Ixia BreakingPoint Storm.

Côté français, le centre commun de gestion de crise cybernétique (C4) de l'ENSIBS à Vannes propose un Cyber Range unique en France, tant dans la forme, grâce à des locaux dédiés, que sur le fond, du fait des contenus pédagogiques et de l'utilisation de la plateforme HNS de Diateam. La mise en place de ce dispositif aura nécessité 1,3 million d'euros17 et 2 ans de préparation. Depuis 2016, ce centre est utilisé à la fois pour la formation des étudiants de l'ENSIBS et pour la formation professionnelle grâce à la création d'un groupement opérateur baptisé BlueCyForce.

---

12 Capture the Flag exercices, exercices pratiques de modélisation et de simulation de systèmes de contrôle industriels (ICS), des attaques réseau ou génération de malwares

13 Selon The San Diego Union-Tribune

14 https://www.merit.edu/cyberrange/

15 Ann Arbor, Michigan (pour le staff Merit) + 4 environnements physiques sur les campus de l'Université de l'Est du Michigan (Ypsilanti), de l'Université Ferris State (Big Rapids), de l'Université du Nord (Marquette) et de la 110ème Attaque Wing Facility (Battle Creek) - base de la Garde nationale

16 ST Electronics (Training & Simulation Systems) fournit des solutions de modélisation et de simulation sur-mesure à des fins de formation, de simulation et de divertissement ludo-éducatif pour des clients issus de la sphère commerciale ou de la défense.

17 L'UBS ayant apporté la contribution la plus significative à hauteur de 37,29%

Les Cyber Range accessibles au public

Les centres d'entrainement accessibles au public permettent à un client de bénéficier d'une formation opérationnelle prodiguée dans les locaux de l'opérateur. On peut notamment relever les offres d'Airbus Defence and Space, de BlueCyForce, de Cisco, de Cyberbit, de Cybergym, d'IBM X-Force, de QA, de Raytheon ou encore de SANS.
Le tableau ci-dessous présente ces différentes offres de façon détaillée.

La plupart de ces acteurs proposent des offres complètes combinant environnement de simulation

Sociétés	Type d'acteurs	Prestations proposées
AIRBUS DEFENCE AND SPACE CyberSecurity Training Centre Dans les locaux d'Airbus DS ou sur site Trois centres européens (Paris, Newport et Munich)	Offre diversifiée de formation adaptée à tous niveaux, du manager à l'expert	1 à 3 jours de sessions : * Cyber Awareness : formation de sensibilisation à destination de l'ensemble du personnel d'entreprise * Cyber Portfolio : formation accompagnant le déploiement des solutions et produits Airbus DS (SOC) * Entraînements spécifiques : Red team/Blue team, coaching DSI/RSSI, etc.
BLUECYFORCE Paris et Vannes	Ouvert à tous les professionnels selon un parcours pédagogique adapté, de la sensibilisation à la gestion de crise	* Formation et entrainement via des sessions de 1 à 5 jours * Différents niveaux, de yellow à black belt * Approche intégrant le facteur humain
CISCO Cyber Range Service Sur site ou dans les locaux d'entraînement de Cisco	Equipes de sécurité d'une société	* Petit format : ateliers de 3 jours limités à 12 personnes, couvrant jusqu'à 8 technologies * Large format : ateliers de 5 jours limités à 12 personnes, couvrant jusqu'à 12 technologies * Management et travail d'équipe mis en avant
CYBERBIT & ETA (Electronic Technology Associates) ETA Cyber Range Baltimore, Maryland, US	Professionnels de la Cybersécurité	"Premier centre de formation en direct et autonome aux US" (opéré par ETA) Communiqué du 21 septembre 2016
Cyberbit Cyber Training Range NI CYBERSECURITY Toranomon, Tokyo, Japon	Organisations, principalement gouvernementales et financières	Plateforme d'entrainement et de simulation permettant aux stagiaires d'utiliser leur propre réseau, leurs outils informatiques, etc.
CYBERGYM (Israel Electric Corporation + CyberControl) CyberGym's Training Arena Israël	Organisations financières, infrastructures critiques et entreprises industrielles	* Centre opérationnel conçu avec une attaque (red team) / une défense (blue team) / ainsi qu'une équipe management et debrief (white team) * Approche sportive
CYBERGYM EUROPE Cybergym Europe's Training Arena Prague, République Tchèque	Entreprises (spécialistes IT, opérateurs, ingénieurs, managers, etc.)	* Différents programmes adaptés aux besoins * Approche intégrant le facteur humain * Red, blue & white teams (idem que CYBERGYM Israël)
IBM X-Force Command Center 75 Binney Street, Cambridge, MA	CISO + son équipe ou personnel non technique (membres du conseil d'administration, étudiants, etc.)	Les participants apprennent à se préparer et à répondre à des cyber attaques : malwares, ransomwares et autres scénarios réels.
QA Dans les Cyber Labs QA, Royaume-Uni	Entreprises (équipes commerciales, marketing, *penetration testers*…), forces de l'ordre, et gouvernements.	* Cyber Range high-tech axé sur le management de crise Cyber * Formations publiques, privées ou sur-mesure * Exercices pratiques (Capture the Flag, *Digital Forensics*, etc.) adaptés au profil client * Cours accrédités par les principaux fournisseurs : Cisco, Kaspersky, EC-Council, Microsoft, etc.
The Raytheon Cyber Operations, Development and Evaluation (CODE) Center Locaux de Raytheon's Global Solutions Center, États-Unis	Entreprises, services militaires et agences du gouvernement	* Tests de pénétration et exercices pratiques red team/blue team * Utilisation des derniers outils, techniques et malwares pour tester et évaluer les systèmes et réseaux * Exercices force-contre-force
SANS En ligne ou emplacement souhaité du client ou sur site : Amérique du Nord, Amérique du Sud, EMEA, APAC	Entreprises et gouvernements	* SEC562 (intégrant la gamme cinétique SANS CyberCity) * SEC562.4 : Cryptographie et protocoles ICS * SEC562.3 : Contrôle du système SCADA (notamment) * SEC652.5 : Pen test * SEC562.6 : Exercices force-contre-force

technique et contenus pédagogiques. SANS a ainsi conçu avec NetWars18 CyberCity une offre inter-entreprises privilégiant l'apprentissage par la pratique dans un mode « inter entreprises ». S'appuyant sur la reconstitution d'une ville physique miniature (échelle 1:87), cet environnement représente ainsi une distribution électrique contrôlée par SCADA et des infrastructures classiques en milieu urbain (eau, banque, etc.). Les participants doivent défendre ces dernières, menacées par des cyber-attaques, et utiliser des tactiques offensives pour en reprendre le contrôle.

Source : SANS

Idem pour Raytheon, dont le centre CODE permet de recréer une réplique précise d'un système en seulement quelques heures (contrôle du trafic aérien, réseaux électriques, centres d'opération de sécurité, etc.) adaptée à des prestations « intra entreprises ». L'environnement peut ainsi intégrer les capacités informatiques de l'entreprise, des clients et des partenaires, qui apprendront à maîtriser les dernières techniques de protection en matière de sécurité.

De son côté, le Français BlueCyForce19 propose les deux options, inter comme intra, avec des sessions de sensibilisation pour les managers ainsi qu'une formation opérationnelle combinée à un entraînement pour les experts. Même chose pour IBM X-Force, qui a testé son Cyber Range avec ses clients de novembre 2016 à janvier 2017, avant de l'ouvrir à la communauté business, de nature à être référencé comme le premier Cyber Range commercial. Même si la communication opérée par le groupe va dans ce sens, certaines sources le présentent cependant surtout comme une opération de sensibilisation destinée aux clients IBM.

Autre initiative intéressante, celle de NI Cybersecurity, fournisseur japonais de services de sécurité, dont le Cyber Range, utilisant la plateforme israélienne Cyberbit, propose une offre automatique d'attaque qui pourrait contribuer à la préparation des Jeux Olympiques de 202020. Toujours en Asie, NEC Corporation a annoncé le 27 janvier 2016 le lancement officiel d'une seconde « Cyber Security Factory » à Singapour (la première ayant été installée en 2014 au Japon). La plateforme Sypris qui y est utilisée propose : des modules de cours intégrant des laboratoires de simulation, répartis sur 5 niveaux ; des défis liés à la sécurité (sécurité des applications Web, sécurité des applications mobiles, cryptographie, sécurité des

---

18 NetWars représente un ensemble de scénarios pratiques d'apprentissage interactif : NetWars continuous, NetWars Experience, NetWars Cybercity, DFIR NetWars continuous, DFIR NetWars, NetWars courses). NetWars CyberCity correspond à l'offre la plus aboutie de SANS, à destination des guerriers et pros infosec

19 Composé des sociétés Diateam et CEIS, le GIE BlueCyForce exploite à compter d'avril 2017 un nouveau centre d'entrainement situé en plein Paris.

20 "I am confident that the initiative, led by Ni Cybersecurity, powered by our Range platform, will contribute to Japan's cyber readiness for the 2020 Olympic Games, and for years to follow". Adi Dar, Cyberbit's General Manager http://ir.elbitsystems.com/phoenix.zhtml?c=61849&p=irol-newsArticle&ID=2243187&ind=0

réseaux, forensics, etc.) ; et des exercices dynamiques en équipe couvrant 4 domaines (attaque/défense, capture the flag, prise de contrôle de botnet, tests de pénétration).

Source : Sypris

Quels critères différenciant ?

Pour choisir une offre d'entrainement dans un Cyber Range la plus adaptée à ses besoins, différents critères doivent être étudiés :

- La neutralité. Lorsqu'ils sont opérés par des éditeurs de solutions ou des intégrateurs, les Cyber Range n'intègrent généralement que des solutions sécurité « maison », ce qui est forcément très limitatif.
- L'adaptabilité. Le Cyber Range, ainsi que les contenus, doivent pouvoir s'adapter rapidement au contexte métier du client. Pour ce faire, SANS a privilégié une approche quantitative en offrant une grande diversité de scénarios préalablement établis dans le cadre de sa Cybercity et via son moteur de recherche « *Find the training you need* »21, disponible sur son site internet, qui permet à n'importe quel utilisateur de trouver dans les plus brefs délais le cours, le lieu, la date, ou le type d'entraînement souhaité. Une autre approche, plus qualitative, consiste à construire, dans un modèle de prestation « intra entreprises », une topologie réseau représentative du contexte client et un scénario adapté au niveau des stagiaires. C'est l'option choisie par BlueCyForce où la Red Team va « doser » ses attaques pour faire progresser les stagiaires, à l'image du « sparring partner » en boxe, sans dérouler des scénarios figés.
- L'infrastructure technique. Quelques solutions sont aujourd'hui déployables en mode « Cloud », privé ou public. Cyberbit Range est basé sur une infrastructure Cloud privée, tandis que SimSpace VCN utilise les capacités d'Amazon Web Services (AWS) et de Google Cloud afin de fournir des Cyber Range pré-configurés et déployés sur demande au sein d'environnements isolés.
- La dimension offensive. Certains offreurs n'ont pas oublié l'héritage militaire du concept. Qu'il s'agisse d'Ixia, de Ravello Systems, de Sypris, des Cyber Range Cybergym (Israël + Europe) ou de BlueCyForce, tous ont axé leur offre sur la notion de « combat » et le dépassement de soi (savoir-être au-delà des connaissances techniques et savoir-faire).

21 https://www.sans.org/find-training

LA STANDARDISATION DE LA CYBER THREAT INTELLIGENCE : OBJECTIFS ET ENJEUX DES STANDARDS DE PARTAGE

Selon une étude menée par IT-Harvest, le taux de croissance annuel du marché de la Cyber Threat Intelligence (CTI) est estimé à 85% depuis 2015. Il était évalué à 460 millions de dollars en 2016 et s'élèverait à 1,5 milliard en 2018. Ce marché en plein développement est aujourd'hui composé d'un large panel d'offreurs comme FireEye, Intel471 ou encore Flashpoint Intel. Ces derniers proposent des **flux d'information sur les cybermenaces** très différents les uns des autres, tant par le fond que par la forme : indicateurs de compromission, remontées de signaux faibles provenant du Clear/Deep/Dark Web, veilles sur les vulnérabilités ou encore rapports sur des modes opératoires d'attaques.

Tout l'enjeu pour ces différents fournisseurs de CTI, et pour leurs clients finaux que sont les responsables sécurité des systèmes d'information et les équipes de type CSIRT, CERT ou SOC, managés ou non, consiste à rendre intelligible ces différents flux en les rendant interopérables et « actionnables » grâce à un langage ou à des attributs communs.

Afin de répondre à cette problématique, un ensemble d'initiatives a vu le jour depuis 2012. Si des standards comme STIX et TAXII se sont imposés comme des références, tous n'ont pas rencontré le même succès auprès des différents acteurs de CTI.

Qu'est-ce que la Cyber Threat Intelligence ?

Une **cybermenace** se matérialise par la combinaison de trois facteurs, à savoir : une **intention de nuire**, une **capacité d'attaque** et une **opportunité à exploiter**, c'est-à-dire une vulnérabilité de nature technique ou humaine. Ainsi, trois principales cybermenaces aux motivations différentes sont susceptibles de cibler tous types d'organisations : les **hacktivistes** poussés par une idéologie, les **cybercriminels** motivés par l'appât du gain et enfin, les **groupes sponsorisés par un État** (à ne pas confondre avec la notion d'APT22) dont la finalité des actions menées est l'espionnage.

La **Cyber Threat Intelligence** est une activité dont le double objectif final est l'étude et la surveillance de ces cybermenaces. Pour ce faire, les offreurs de flux d'information de type CTI se basent sur deux approches :

- La première approche est l'**analyse des attaques passées** qui permet de caractériser ces dernières par des **marqueurs techniques** (signatures de malware, adresses IP, noms de domaine malveillants, etc.). Le but pour le défenseur est de se prémunir et de bloquer au plus vite une campagne qui se renouvellerait via l'utilisation de ces marqueurs techniques. Cette approche est la plus utilisée par les offreurs et constitue une **posture de « réponse »** pour les consommateurs de CTI.
- La deuxième approche est la surveillance **directe des attaquants**. L'objectif est de se placer en amont d'une cyberattaque et de détecter des éléments permettant d'**identifier sa préparation** : émergence d'un mobile, définition d'objectifs, choix d'un mode opératoire, acquisition de capacités ou encore organisation de ressources humaines. Cette approche témoigne d'une **posture d'anticipation** face à une cyberattaque et demande d'être au plus proche de la cybermenace,

notamment **en surveillant et en infiltrant les lieux qu'elle fréquente** (réseaux sociaux, IRC, plateformes underground du Dark Web comme les places de marché ou les forums restrictifs).

Ces deux approches permettent de remonter de nombreuses informations relatives aux cybermenaces qui peuvent être réparties selon quatre types de CTI23 :

- **Stratégique** : ce sont en général des analyses de très haut niveau mais peu techniques et destinées à des décisionnaires. Cela peut-être par exemple des rapports sur des adversaires qui ciblent un secteur donné.
- **Tactique** : ce sont souvent des documents (de type whitepapers) qui donnent des informations sur les outils et méthodologies utilisés par les cybermenaces (analyse de malware, contournement d'anti-virus, outils utilisés pour mener des attaques DDoS, etc.).
- **Opérationnel** : l'objectif est d'anticiper une attaque en étant au plus près de l'attaquant (exemple : tweet d'un groupe hacktiviste qui publie une liste de leurs futures cibles). La disponibilité des informations est fonction du niveau de sophistication de la cybermenace (hacktiviste – cybercriminel – groupe sponsorisé par un État).
- **Technique** : il est composé d'indicateurs de compromission (IPs, URLs, noms de domaine, listes de hashs, etc.) qui permettent d'identifier et donc de bloquer une attaque en cours. Cette information a cependant une durée de vie limitée et reste souvent peu fiable, non-contextualisée et disponible en trop grande quantité pour être traitée de manière efficiente.

Ainsi, l'approche « analyse des attaques passées » permet de couvrir les niveaux de CTI tactique et technique, alors que l'approche « surveillance directe des attaquants » se concentre sur l'opérationnel. Les fournisseurs de CTI positionnés sur ces deux approches produisent des flux d'information très diversifiés de par leur contenu et leur nature. Si ces données sont nécessaires pour anticiper et bloquer une cyberattaque, leur intégration au sein d'un système d'information représente néanmoins un défi.

23 https://www.cpni.gov.uk/cyber-security

Standards les plus utilisés

Afin de répondre à cet enjeu, de nombreux standards d'uniformisation des flux ont vu le jour au cours des dernières années. En 2015, l'ENISA recensait ainsi 36 standards et outils, dont certains ont rencontré un franc succès24.

Le premier type de standard à avoir été proposé est **le format de modélisation des informations**. L'objectif est qu'un émetteur puisse communiquer à l'ensemble de ses destinataires les données collectées à partir d'un support et dans un format défini. Le plus connu d'entre eux, **OpenIOC25**, est le standard historique créé par MANDIANT pour échanger des IOC. À la base, OpenIOC est un format (en XML) utilisé par les outils de la société mais qui a été rendu open-source pour permettre un usage par tous. Un fichier OpenIOC décrit les symptômes à rechercher pour identifier une menace.

D'autres formats ont également été proposés**26**, comme **SNORT** qui permet de détecter des menaces se propageant sur le réseau, ou encore **YARA** qui se focalise sur les caractéristiques intrinsèques d'un fichier et est particulièrement pertinent pour identifier des souches de familles de code malveillant.

Ces formats de modélisation rencontrent cependant une limite : ils ne se concentrent que sur un événement et ne donnent pas d'information quant à la cybermenace à l'origine de l'attaque. D'autre part, leur façon de modéliser un événement n'est pas uniforme puisqu'il varie suivant la typologie de la cybermenace et les capacités déployées.

D'où l'intérêt de **STIX27** (*Structured Threat Information Expression*) qui est un langage permettant de partager, à partir d'un format standard, des informations liées à des cybermenaces. Ce standard propose donc un niveau de représentation au-dessus des autres formats évoqués précédemment puisqu'il a pour vocation de permettre de modéliser un attaquant plutôt que de se concentrer sur un événement particulier causé par celui-ci. Les acteurs utilisant STIX peuvent entre autres décrire et modéliser les concepts suivants :

- ***Attack Pattern*** : mode opératoire de l'attaquant ;
- ***Threat Actor*** : individus, groupes ou organisations agissant avec une intention malveillante ;
- ***Malware*** : logiciel malveillant utilisé pour compromettre la confidentialité, l'intégrité ou la disponibilité du système d'information de la cible ;
- ***Tool*** : logiciel légitime utilisé par les cybermenaces dans le cadre de leurs attaques ;
- ***Vulnerability*** : vulnérabilité présente dans un logiciel qui est exploitée directement par un attaquant afin de compromettre un système d'information ;
- ***Indicator*** : indicateur utilisé pour détecter et bloquer une activité suspecte ou malveillante sur le système d'information.

Si STIX est le composant principal et permet de modéliser complétement un événement, le standard **TAXII** (*Trusted Automated eXchange of Indicator Information*) permet quant à lui de **transporter des données de type STIX**. Il décrit l'échange d'information et implémente des modèles de partage comme la « Source centrale », le « Hub de partage » et le « Peer to Peer ».

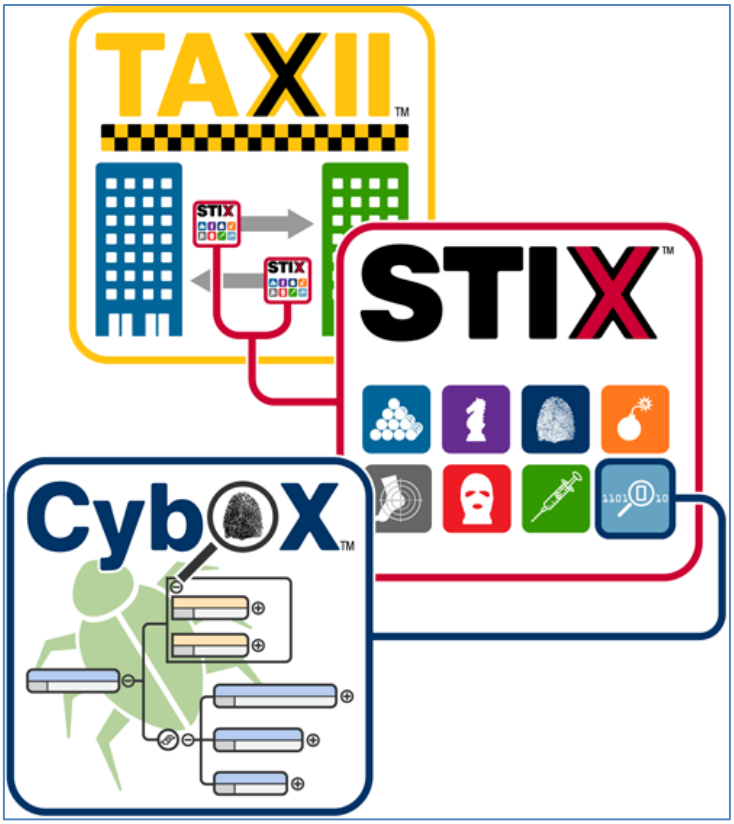
---

24 https://www.enisa.europa.eu/news/enisa-news/new-guide-by-enisa-actionable-information-for-security-incident-response

25 https://www.cert-ist.com/pub/files/Forum2015-03-BOURGEOIS_FILLETTE_ZANDONA-ThreatIntel&PilotIOC.pdf

26 http://connect.ed-diamond.com/MISC/MISC-079/Threat-intelligence-et-APT

27 https://oasis-open.github.io/cti-documentation/stix/about



Organisation des standards TAXII, STIX et CybOX[28]

Les plateformes de Threat Intelligence

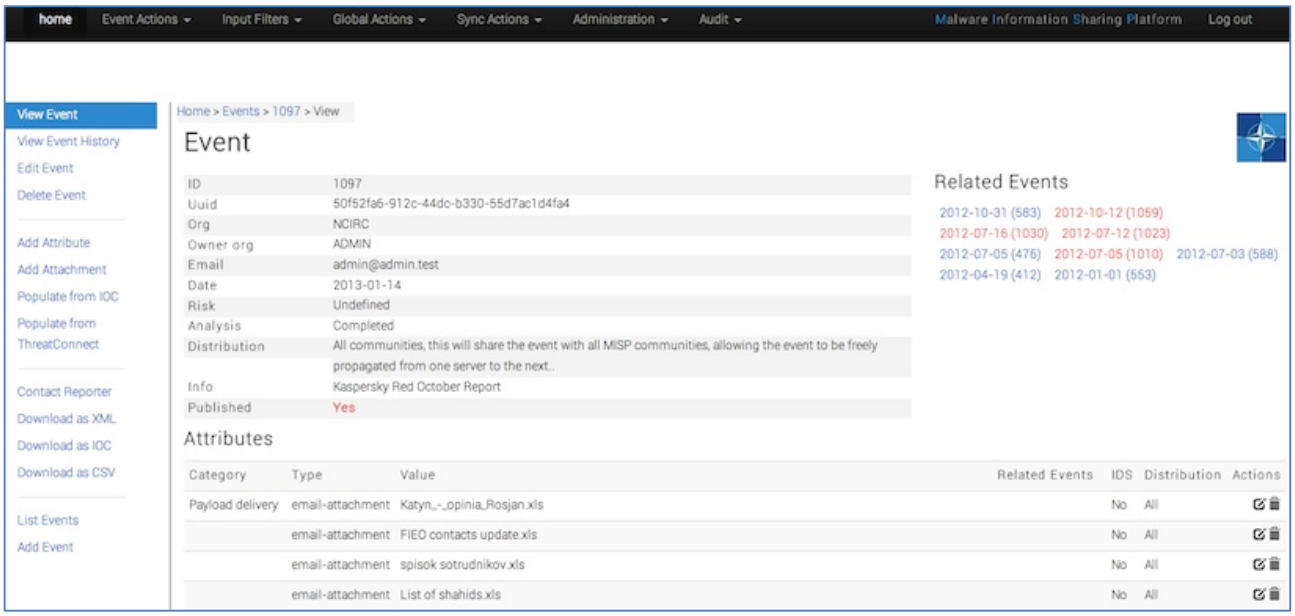
Pour faciliter la capitalisation et la corrélation des données, un nouveau type d'acteur s'est immiscé dans le marché de la Cyber Threat Intelligence en jouant un rôle de relais entre les producteurs et les consommateurs de flux d'information. Les ***« Threat Intelligence Platform »*** collectent les informations à partir de diverses sources, puis les intègrent au sein d'une plateforme afin de maximiser la valeur des différents flux via leur corrélation et contextualisation.

MISP[29] (*Malware Information Sharing Platform and Threat Sharing*) est une solution open-source permettant la collecte, le stockage, la distribution et le partage d'IOC liés aux malware. Cet outil à vocation communautaire permet à divers organismes de partager les indicateurs de compromission identifiés lors des activités de SOC et campagnes de réponses à incidents (CERT et CSIRT). Elle rencontre un franc succès auprès de la communauté européenne. D'un point de vue plus technique, MISP est une plateforme d'échange d'IOC où chaque acteur peut entrer et organiser ses IOC afin de les publier pour les partager aux autres acteurs présents sur ce portail. La diffusion est effectuée par emails chiffrés via GPG et la plateforme elle-même est régulièrement auditée afin d'en assurer sa sécurité. MISP fournit des fonctionnalités pour

28 Note de l'auteur : le langage CybOX (Cyber Observable eXpression) a directement été intégré dans la version 2.0 de STIX. Ce langage est l'un des concepts que peut modéliser un utilisateur de STIX, à savoir la description d'un événement.

29 http://www.misp-project.org/

favoriser les échanges d'informations, mais aussi l'intégration de l'information par les IDS (Intrusion Detection System), les outils d'analyse de logs et les SIEMs (Security Information and Event Management).



Plateforme MISP

D'autres initiatives d'origine privée rencontrent également un réel succès, comme celle de la société ThreatQuotient dont « *la plateforme agit comme une bibliothèque universitaire des menaces à disposition des SOC. Elle est reliée à plusieurs sources (feeds), Open Source ou des remontées issues de l'industrie (pharmacie, finance, etc.)* 30». Cette plateforme ne remplace pas un SOC ou un CERT mais vise à automatiser un certain nombre d'actions manuelles.

Conclusion

Les formats de modélisation des flux se sont majoritairement concentrés sur le niveau technique de la CTI à travers la démocratisation des indicateurs de compromission. Un standard comme STIX ou une plateforme de type MISP ont cependant introduit la notion de contexte (par conséquent de CTI stratégique et opérationnelle) afin d'appréhender les cybermenaces dans leur globalité et pas uniquement sur un mode réactif et technique, à savoir la cyberattaque en elle-même. Il est en effet primordial pour les défenseurs d'adopter une posture d'anticipation en plus de la posture de réponse à incident : l'offre et les solutions techniques sont d'ores et déjà disponibles et gagnent progressivement en maturité.

30 http://www.silicon.fr/threatquotient-agence-de-renseignement-des-menaces-en-mode-automatique-143488.html

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
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.eu