LIVRE BLANC

Cyber Threat Intelligence

COMMENT VOUS AIDE-T-ELLE À BIEN ALLOUER VOTRE BUDGET CYBERSÉCURITÉ ?

serenety
By xmco

Sommaire

Avant-propos.

L'AUGMENTATION DES MENACES CYBER, LA COMPLEXIFICATION DES ATTAQUES ET L'INTENSITÉ DE LEURS IMPACTS ONT RENDU OBLIGATOIRE LE FAIT DE SE TENIR INFORMÉ DU CYBER CONTEXTE DANS LEQUEL VOTRE ENTREPRISE ÉVOLUE.

Le renseignement sur les menaces cyber, aussi appelé Cyber Threat Intelligence permet de disséminer de l'information à l'ensemble de votre chaîne de défense. Qu'elles soient techniques ou contextuelles, la connaissance de ces informations permet de mieux anticiper, détecter et répondre aux menaces anciennes ou futures.

La Cyber Threat Intelligence permet donc d'avoir une vision globale de son environnement de menaces en surveillant son périmètre connu *(IPs, DNS ou mots-clés)* mais aussi des éléments inconnus que l'on retrouvera sur le Web, qu'il s'agisse du Web visible, du Deep Web ou du Dark Web.

Pour ce faire, de nombreuses techniques et méthodes sont utilisées et ont pour vocation d'aider les organisations à s'adapter à un contexte de menaces toujours plus mouvant et de répondre aux évolutions des techniques utilisées par les attaquants pour cibler leurs victimes.

Bien souvent ignorée par les dirigeants d'entreprise et les responsables informatiques, nous vous proposons ici, de démocratiser cette approche et de dépeindre comment toute entreprise, indépendamment de sa taille, peut en tirer parti.

1. Cyber Threat Intelligence, de quoi parlons-nous véritablement ?

DEVENUE INCONTOURNABLE ET POURTANT SI PEU COMPRISE, LA CYBER THREAT INTELLIGENCE REPRÉSENTE L'UNE DES PIERRES ANGULAIRES DES STRATÉGIES DE CYBERSÉCURITÉ.

En se plaçant du point de vue d'un attaquant, **l'analyse de la cybermenace permet à la fois de cartographier les failles de son système d'information et de les mettre en corrélation avec le mode opératoire des attaquants**.

Selon l'ANSSI, la Cyber Threat Intelligence *(CTI)*, implique l'ensemble des activités de **recueil, d'étude et de partage d'informations** liées à des attaques informatiques. Son but est de « **fournir des connaissances qualifiées et adaptées** à de multiples destinataires souhaitant protéger des systèmes numériques ».

La CTI et son ancêtre : le renseignement militaire.

COMMENT DÉFINIR LE RENSEIGNEMENT ?

Le renseignement se définit comme une donnée *(élément général et non contextualisé)* devenant une information *(équivalent de la matière brute contextualisée et confirmée)*. Au travers de l'analyse, l'information devient renseignement *(équivalent de la matière raffinée, directement actionnable, confirmée et vérifiée)*.

DONNÉE > INFORMATION > RENSEIGNEMENT

LE CYCLE DU RENSEIGNEMENT MILITAIRE.

Issu du cycle du renseignement militaire, le processus de recueil des informations s'organise en cinq phases.

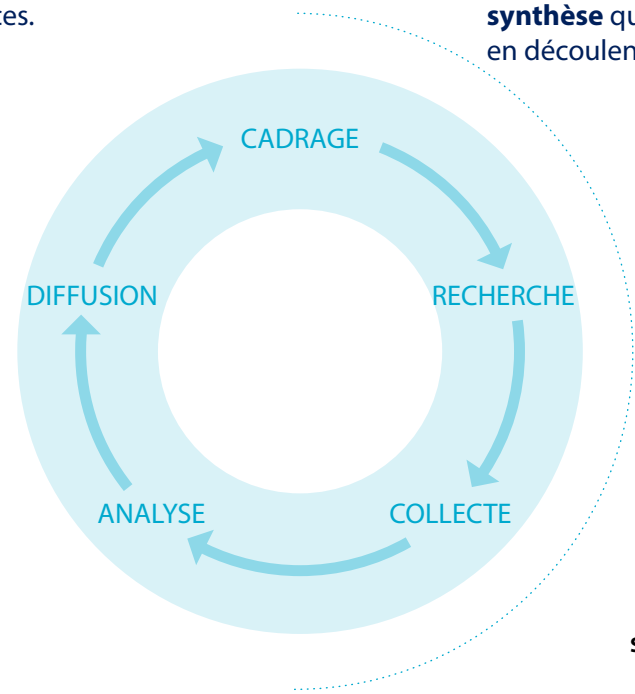
La phase de **CADRAGE a pour but de définir les attentes du projet de recherche d'information pour** cadrer le besoin initial. Il peut s'agir d'une phase pendant laquelle l'analyste va utiliser la méthode du QQQOCP *(Qui ? Quoi ? Quand ? Où ? Comment ? Pourquoi ?)*.

La période de **RECHERCHE est la phase de lancement des travaux durant laquelle l'analyste fait le tri entre les informations pertinentes et le reste**. Il s'agit également d'une phase pendant laquelle il identifie la fiabilité des sources.

La phase de **COLLECTE permet de recueillir toutes les informations qui ont été jugées pertinentes lors de la phase de recherche.**

La phase d'**ANALYSE**, au-delà d'être la plus longue, est également la plus cruciale de ce processus. Elle permet d'**analyser les différents éléments recueillis et de rédiger les notes de synthèse** qui en découlent.

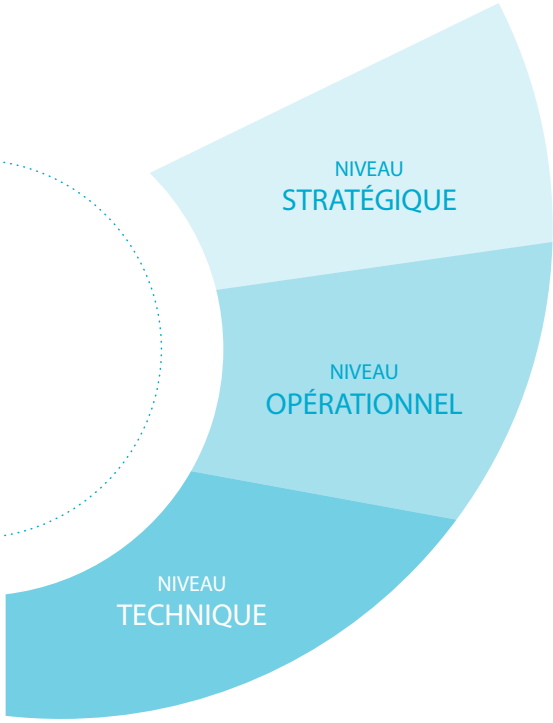
La phase de **DIFFUSION représente la période pendant laquelle le renseignement sera diffusé**. Il sera uniquement transmis aux personnes à qui il est destiné, de manière à limiter les risques de diffusion inopinée. Le format de diffusion diffère en fonction des cas et des besoins du commanditaire.



Comment définir la CTI aujourd'hui ?

La CTI est majoritairement présentée en trois catégories, correspondant chacune à une partie de l'analyse de la menace. L'ANSSI divise notamment la Cyber Threat Intelligence en trois axes :

1. Le **niveau stratégique** qui oriente les décideurs .
2. Le **niveau opérationnel** *(TTPs : Tactics, Techniques and Procedures)* qui aide à la priorisation des projets de sécurisation.
3. Le **niveau technique** *(IOCs : Indicator of Compromise)* qui alimente les outils de détection et de recherche de compromission.



1. LE NIVEAU TECHNIQUE DE LA CTI : LES INDICATEURS DE COMPROMISSION OU L'IDENTIFICATION DE LA MENACE AU SEIN DE SON SYSTÈME D'INFORMATION (SI).

Les informations techniques telles que les IoC *(indicateurs de compromission)* constituent la matière brute sur laquelle les autres niveaux de CTI viendront se baser. **Il s'agit d'adresses IP, de noms de domaines ou encore des hash de fichiers malveillants *(empreinte propre à chaque fichier)***. Identifiés au travers d'analyses, le simple fait de trouver l'un de ces marqueurs revient à identifier une compromission de tout ou partie de son système.

2. LE NIVEAU OPÉRATIONNEL DE LA CTI : TACTIQUES, TECHNIQUES ET PROCÉDURES OU LA COMPRÉHENSION DE LA LOGIQUE D'ATTAQUE.

Le niveau opérationnel, parfois confondu avec le niveau tactique se caractérise par l'utilisation des éléments issus du niveau technique pour en faire émerger une tendance et une analyse plus précise de la menace. **L'analyse de la tactique de l'attaquant permet ainsi de comprendre son but et sa manière d'opérer**.

Plusieurs grilles méthodologiques existent afin d'appréhender au mieux le mode opératoire des attaquants, parmi elles : la plus reconnue est la matrice **MITRE ATT&CK**. Au travers de ces onze étapes, **cette matrice permet d'identifier les différentes actions et angles d'attaque des criminels lors d'une tentative de compromission**.

Parmi les compromissions les plus courantes, les problèmes de configuration sont récurrents et très risqués car ils exposent les services d'une organisation. Un exemple concret d'application de la matrice **MITRE ATT&CK** peut être celui lié au mode opératoire Sandworm, présenté page suivante.

En analysant les techniques et tactiques utilisées par les attaquants du groupe Sandworm, on apprend notamment que :

[Initial Access] Le spear-phishing a été utilisé comme porte d'entrée au SI des cibles.

[Execution] Les commandes powershell, scripts et pièces jointes contenant des malwares ont ensuite été lancés pour exécuter du code malicieux dans le SI ciblé.

[Persistence] et [Privilege Escalation] Le groupe a ensuite utilisé des comptes légitimes existants afin de se maintenir dans le système et procéder à des élévations de privilèges permettant de compromettre davantage d'équipements .

[Defense Evasion] Afin d'éliminer ses traces et éviter d'être détecté, le groupe a utilisé un malware spécifique lui permettant d'effacer les données des machines compromises et de remettre à zéro les journaux d'évènements. Le groupe a également tenté d'imiter un autre groupe d'attaquants afin de brouiller les pistes.

Sans retracer toutes les étapes par lesquelles sont passés les criminels, les techniques listées plus haut ont finalement permis aux attaquants d'accéder aux informations qu'ils souhaitaient et de les récupérer. Au-delà des données exfiltrées, le groupe a également défacé environ 1 500 sites web et eu un impact très important sur certains services vitaux aux États-Unis.

Découvrir la matrice **MITRE ATT&CK** :

https://attack.mitre.org/matrices/enterprise/

3. LE NIVEAU STRATÉGIQUE DE LA CTI : L'ÉTUDE DES TENDANCES ET DES MENACES OU COMMENT CONNAITRE SES ADVERSAIRES POUR ANTICIPER SES ATTAQUES.

Une fois le mode opératoire et les éléments techniques liés identifiés, il est possible d'orienter sa stratégie de sécurité en conséquence. **En identifiant les angles d'attaque, les failles et vulnérabilités utilisées par les criminels, vous êtes en capacité d'identifier, d'une part, les menaces pesant sur vos SI, et d'autre part, les briques vulnérables dans celui-ci**.

Une organisation ciblée par du spear-phishing *(technique d'hameçonnage avancée)* nécessiterait sans doute d'orienter sa stratégie de cyberdéfense sur la sensibilisation de ses employés, mais également sur la mise en place de solutions dédiées au filtrage et à l'analyse du contenu des emails.

Cette analyse fine basée sur le contexte précis de l'entreprise est l'une des briques sur lesquelles peut se construire la vision globale de la sécurité des systèmes de l'entreprise.

Par exemple, l'analyse de la menace par secteur d'activité et par zone géographique vient ajouter des éléments de contexte permettant aux décideurs de se préparer aux attaques. **La connaissance des modes opératoires de certains groupes d'attaquants, de leurs origines géographiques ou encore de leurs cibles principales permet également d'ajouter des éléments déterminants dans l'analyse des menaces et d'orienter des décisions stratégiques à plus long terme**.

2. Les entreprises face au risque cyber, panorama des menaces en 2021.

UNE FOIS LES ENJEUX ET LES RISQUES POUR LES ENTREPRISES IDENTIFIÉS ET COMPRIS, LE PANORAMA DE LA MENACE CYBER PERMET DE POSER LES BASES DE L'UTILISATION DE LA CTI POUR ACCOMPAGNER SA STRATÉGIE DE SÉCURITÉ.

Le constat est clair : les attaques sont toujours plus fréquentes et sophistiquées. Le risque cyber est devenu un enjeu économique majeur pour toutes les entreprises et les faits d'actualité confirment cette tendance : rançongiciels, extorsions, fraudes au président, attaques opportunistes, phishing, fuites de données, tous ces termes inondent depuis quelques années les news des rubriques « tech » des sites d'actualités.

Au-delà de ce constat, l'élargissement de la surface d'attaque, avec notamment l'adoption du Cloud et l'augmentation des activités à distance, en particulier le télétravail, ont participé à cette multiplication des risques et des vulnérabilités auxquels se confrontent les entreprises.

3 vecteurs d'attaque privilégiés par les attaquants.

Il faut garder en tête que dans la plupart des cas, ces attaques sont principalement opportunistes. Une porte laissée ouverte par mégarde ou un simple manque d'attention lors de l'ouverture d'un email et les cybercriminels s'engouffrent dans la brèche.

LES ENTREPRISES SONT AUJOURD'HUI LA CIBLE DE TROIS CYBERMENACES MAJEURES :

1 **Des composants obsolètes, ou non maintenus à jour, exposés à tous vent**

2 **Des emails et pièces jointes piégées misant sur la crédulité des utilisateurs**

3 **L'utilisation d'identifiants** *(propre à l'entreprise ciblée ou à des partenaires)* **faibles, volés ou achetés sur le dark web** *(business email compromise)***.**

SHADOW IT, CLOUD ET MAITRISE DE SON EXPOSITION

Avec la généralisation du télétravail et l'utilisation massive des services Cloud et la contractualisation à outrance des solutions SaaS et des prestataires tiers par les entreprises, les DSI ont de plus en plus de mal à contrôler et surveiller l'exposition de leur SI. Comment assurer une sécurité adaptée et continue sans maitriser complètement votre périmètre ?

Les risques de Shadow IT tout comme le maintien en condition de sécurité du périmètre « connu » constituent l'une des causes principales de risques cyber.

Les attaquants ont bien pris en compte ces problèmes et continuent de réduire la fenêtre de tir entre la publication d'une vulnérabilité et son exploitation. Les attaquants profitent du temps nécessaire aux entreprises pour déployer les correctifs disponibles pour cibler en « ratissant large » via la réalisation de scans sur Internet. On peut noter que 5 produits affectés par des vulnérabilités importantes ont été particulièrement exploitées depuis le début de l'année : Exim *(serveur de messagerie)* / Pulse Connect Secure *(VPN SSL)* / Exchange / SonicWall SMA / F5 BIG-IP / VCenter *(voir seconde question)*.

LE SOCIAL ENGINEERING : L'UTILISATEUR EST-IL LE MAILLON FAIBLE DE LA CYBERSÉCURITÉ ?

Le phishing et les attaques de social engineering restent toujours aussi prisées par les attaquants.

Démarche simple abusant de la naïveté des victimes, les vols de mots de passe sont devenus une des portes d'entrée faciles pour les attaquants.

Pourquoi changer une attaque qui fonctionne et qui ne coûte presque rien ! Une simple réplication d'une mire Office365, un email indiquant « partage » un document Microsoft et le tour est joué, les pirates ont accès aux boites mail Office de leurs victimes. Elles rediffusent ensuite à tout le carnet d'adresses un autre email pour piéger un grand nombre de victimes jusqu'à tomber sur « le » compte d'un VIP ou du trésorier pour pouvoir, de manière plus ou moins astucieuse et visible, engendrer un paiement vers un pays exotique (fraude au président) ou accéder à des fichiers confidentiels qui seront pris en otages !

Pire encore, le spear-phishing ou l'ouverture d'une pièce jointe malveillante *(contenant une macro)* permettra, elle aussi, au pirate d'avoir un accès encore plus direct au réseau de la société victime de l'attaque...

Le sixième baromètre annuel du CESIN révèle que le phishing demeure le vecteur d'attaque **le plus fréquent pour 80% des entreprises**. De la même manière, un récent rapport sur l'état de la menace liée au phishing publié par Proofpoint indique que plus d'une entreprise française a subi une attaque réussie en 2020.

LE VOL OU LA RÉUTILISATION DE MOTS DE PASSE

Le dernier vecteur en vogue concerne la réutilisation des nombreux mots de passe que chacun utilise au quotidien, que ce soit dans son environnement personnel comme professionnel.
La multiplication des identifiants devient une véritable problématique à gérer. Les piratages massifs de sites non protégés facilitent ainsi l'échange et la revente de milliards de mots de passe qui se retrouvent du jour au lendemain dans la nature, prêts à être utilisés par les cybercriminels !

Ces attaques baptisées « password stuffing » et « password spraying » sont ensuite menées sur des cibles de choix et peuvent avoir un effet dévastateur.

Les collaborateurs sont donc une nouvelle fois à l'origine de ces mauvaises pratiques *(un mot de passe personnel partagé dans son environnement professionnel)* ce qui offre, par mégarde, encore un risque complémentaire aux autres.

Des tendances et évolutions influencées par la pandémie et l'accès au Cloud.

LE CLOUD ÉTEND SA TOILE ET LES MENACES

L'adoption du Cloud, considéré comme le principal vecteur de la transformation numérique des entreprises, est massive. Pour autant les risques liés au Cloud demeurent, ils s'en trouvent même amplifiés. **Une entreprise sur deux pointe le risque de ne pas maîtriser la chaîne de sous-traitance de l'hébergeur et le risque de rebond des attaques via ce dernier, ainsi que des difficultés dans le contrôle des accès**.

Une attention particulière doit être portée aux plateformes de collaboration, en particulier Microsoft 365, souvent associée à l'hébergement de menaces dans le Cloud.

Avec la pandémie, 97% des entreprises françaises ont étendu leur utilisation de Microsoft Office 365, mais 71% d'entre elles ont été victimes de 7 compromissions de compte utilisateurs légitimes en moyenne sur l'année 2020[1].

LA DÉMOCRATISATION DU TÉLÉTRAVAIL

C'est un effet inattendu de la pandémie, **la démocratisation du télétravail pourrait avoir involontairement créé une culture d'entreprise dans laquelle les collaborateurs sont réticents à signaler des problèmes de sécurité**.

Un collaborateur qualifié de non technique sur deux (48%)[2] serait réticent à signaler les menaces de sécurité auxquelles il serait confronté[3].

Faut-il pour autant leur jeter la pierre alors que la pandémie a créé une situation inédite à laquelle peu d'organisations étaient préparées ? Les entreprises ont généralisé l'usage des services Cloud, trop souvent sans former les utilisateurs. Et pour favoriser l'accès aux réseaux et aux données à partir d'équipements personnels et de connexions privées non sécurisées, elles ont assoupli les restrictions de sécurité.

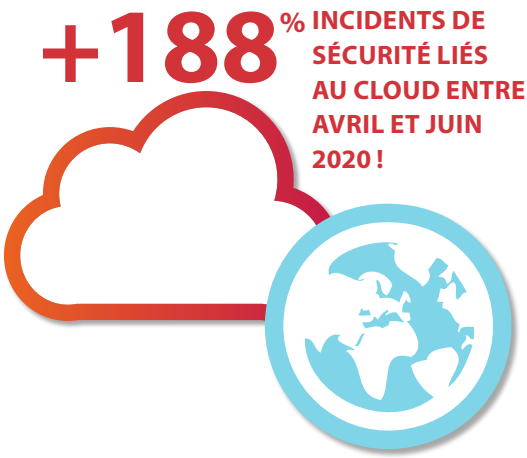
Un chef d'entreprise sur deux (54%)[4]reconnaît que les politiques de sécurité n'ont pas évolué convenablement face aux changements dans l'organisation du travail. Les collaborateurs distants se montrent également réticents à soulever les questions de sécurité. Voilà qui aura favorisé l'augmentation des surfaces d'attaque.

(1) Source Vectra. (2) Rapport de l'Unit42. (3) Étude « Building a Cyber Smart Culture » de Fujitsu (4) Source Check Point.

LA COVID-19 VECTRICE DE MENACES NUMÉRIQUES

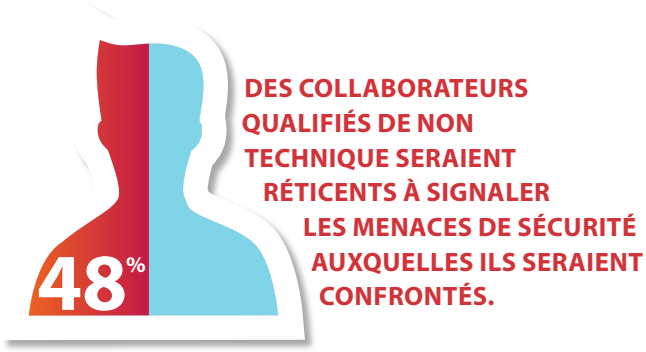
La pandémie a entraîné la plus grande migration de l'histoire vers le travail à distance. Les cyberattaquants se sont largement emparés de la crise sanitaire et des effets du Covid pour apporter de nouveaux risques. Et si les entreprises ont rapidement déporté une grande partie de leur charge de travail dans le Cloud pour répondre à la pandémie, elles ont depuis des difficultés à automatiser la sécurité dans le Cloud et à limiter les risques qui y sont liés.

Au niveau mondial, les incidents de sécurité dans le Cloud ont connu des pics liés à la crise Covid.



D'autre part, **la démocratisation du télétravail pourrait également avoir involontairement créé une culture d'entreprise rendant les collaborateurs réticents à signaler des problèmes de sécurité**. Malheureusement, les entreprises ont souvent généralisé l'usage des services Cloud sans proposer aux utilisateurs des formations adaptées.

L'assouplissement des mesures de sécurité pour faciliter l'accès aux réseaux et aux données à partir d'équipements personnels et de connexions privées non sécurisées est également source de nouvelles menaces.



LES MENACES SUR LES DISPOSITIFS MOBILES DE L'ENTREPRISE

Nous l'avons évoqué, la progression de la pratique du télétravail est un facteur d'augmentation du risque cyber. Cette pratique est à rapprocher de celle plus large de la mobilité. **En 2020, 97% des entreprises, soient quasiment toutes les entreprises, ont subi une attaque de malware *(application malveillante)* mobile au cours de l'année**[4]. Ces applications ont principalement été téléchargées par les employés via des spams les invitant à découvrir des informations liées à la crise Covid-19. À quoi servent ces malwares mobiles ? Principalement à dérober les identifiants bancaires mobiles *(Trojan bancaire)* ou à composer des numéros premium.

(4) Source Check Point.

De l'intrusion initiale à l'exécution d'un rançongiciel.

L'enchainement d'une intrusion, aboutissant très souvent à l'exécution d'un rançongiciel, suivent globalement le schéma suivant :

1. **Première étape**, les attaquants utilisent 3 vecteurs principaux comme porte d'entrée vers les systèmes d'informations des entreprises.

2. **Deuxième étape**, une fois installés sur le réseau, les attaquants pivotent puis progressent afin de trouver le moyen d'exécuter leurs logiciels et finalement exécuter le fameux rançongiciel, se répliquant ainsi sur tout ou partie du réseau.

3. **Troisième étape**, ces groupes font pression sur leurs victimes de différentes manières *(chiffrement des données, vols d'information, divulgation des informations les plus sensibles, revente éventuelle des données dérobées, délit d'initié pour manipuler le cours des actions, voir chantages auprès des collaborateurs ou des clients de la victime)*.

L'arme favorite des cybercriminels reste clairement le rançongiciel. Ce nouveau business extrêmement lucratif est désormais répandu chez tous les groupes de pirates. On ne compte plus le nombre de rançongiciels en circulation, ni le nombre de groupes spécialisés dans ce domaine.
Selon le CESIN, qui réunit les responsables sécurité des systèmes d'information des grandes organisations françaises, en 2020, **une grande entreprise sur cinq aurait été victime d'une attaque par rançongiciel**. Ces attaques dont le but est de bloquer les systèmes informatiques de la victime sous réserve que celle-ci verse une rançon. **De plus en plus organisés, les groupes d'attaquants proposent aujourd'hui des kits prêts à l'emploi pour déployer des rançongiciels**. Cette pratique du « rançongiciel as a service » passe la majorité du temps par un abonnement ou un partenariat entre les deux entités criminelles.

Les rançongiciels ont touché des centaines d'entreprises, des collectivités, le secteur de l'éducation et celui de la santé qui continuent d'en faire les frais chaque semaine, ainsi que les très grandes entreprises. Et malheureusement, le paiement des rançons (par la société victime ou par les cyberassurances) ne cesse de mettre de l'eau dans le moulin pour financer encore d'autres services cybercriminels.

Il faut maintenant se poser la question : pourquoi ? Comment les pirates arrivent-ils si facilement à pénétrer les réseaux informatiques des entreprises pour y déposer tranquillement un logiciel qui fait tant de dégâts.

Lutter contre une cybercriminalité organisée et financée !

L'organisation de l'écosystème des cybercriminels et des moyens/ressources mis à disposition pour les attaques augmente toujours, avec des attaques de plus grande envergure et de plus en plus liées à des états.

La professionnalisation des groupes présents sur le Dark Web se ressent également avec la revente de services toujours plus originaux. Leur organisation se rapproche d'une entreprise avec des gangs dédiés sur certains types de services, des personnes responsables du marketing et des ventes. La démocratisation des crypto-monnaies leur a notamment permis de monnayer plus facilement les reventes de services ou produits illicites.

L'activité du rançongiciel a généré plusieurs centaines de millions de dollars. Darkside, un des groupes les plus connus et actifs, aurait infecté 99 organisations dont 47 d'entre elles auraient réalisé un paiement avoisinant au total 90 millions d'euros selon le site DarkTracer.

Dernière actualité en date, une cyberassurance aurait, quant à elle, payé la plus grosse rançon de l'histoire, soit 40 millions de dollars...

Voilà déjà quelques raisons qui poussent à s'outiller et à comprendre les vecteurs d'attaques utilisés, à savoir comment les attaquants progressent sur un réseau pour identifier les modes opératoires utilisés. En effet, c**omme toute entreprise, les attaquants misent sur la maximisation du profit en automatisant autant que possible chaque étape d'une attaque. Leur but est de faire le plus de victimes dans le moins de temps possible tout en espérant générer le maximum d'argent à la sortie**. Leur « signature » d'intrusion, d'outils et de déplacement suit donc une industrialisation qui peut être identifiée et donc contrée...

Les entreprises, premières victimes des États-nations.

Autre phénomène moins connu, mais en forte augmentation, **le cyberespionnage représente une menace difficile à chiffrer mais considérée par 56% des RSSI comme élevée** et ce, particulièrement dans les secteurs stratégiques. Les conséquences des cyberattaques représentent pour les RSSI, des impacts considérables notamment sur le business (57%) comme sur la production (27%).

Parmi les menaces émergentes qui risquent de prendre de l'ampleur dans les années à venir se trouve le risque lié aux activités États-nations. Cette menace, dont on mesure rarement l'étendue, se livre dans l'ombre au travers d'une véritable cyberguerre, pour déstabiliser les États, mais pas seulement. Autre conséquence de la pandémie, ces derniers se sont engouffrés dans l'opportunité que représente la Covid-19 pour multiplier les attaques et élever les tensions de manière inquiétante.

Sont principalement concernés les entreprises (en particulier la chaîne logistique), la cyberdéfense, les médias, les institutions gouvernementales et les organismes de régulation et les infrastructures critiques. Ainsi les entreprises sont les premières victimes des incidents de sécurité liés aux États-nations, principalement de la surveillance, pour dérober des brevets et des données, dont les vaccins contre la Covid-19.

Ces menaces diverses ciblent les entreprises sur différents maillons de la chaîne de valeur. Qu'il s'agisse de la coupure de service avec des attaques par rançongiciel, de fraude ou d'usurpation d'identité avec des attaques de phishing ou même de compromission de systèmes au travers de campagnes organisées par des États-nations, les **entreprises sont aujourd'hui attaquées de toutes parts et n'ont pas toujours une visibilité optimale sur leur exposition et sur l'exploitation de leurs failles**.

Les politiques de sécurité interne ainsi que la protection des réseaux de l'entreprise ou des échanges au sein de réseaux sécurisés sont primordiales cependant ils sont aujourd'hui bien insuffisants.

Adopter la posture des attaquants en identifiant, d'un point de vue extérieur, ce qui peut être utilisé pour nuire et cibler l'entreprise est tout l'enjeu de la CTI. En connaissant vos failles et votre exposition, il est plus simple d'identifier les menaces et les risques induits par l'exploitation de ces failles.

3. Pourquoi la CTI est-elle importante ? Quels sont les enjeux et les risques pour le CODIR ?

Limiter les dérives de l'informatique hyperconnectée.

Nous l'avons évoqué plus tôt, l'évolution de l'informatique *(et par conséquent de la cybersécurité)* a pris un véritable tournant ces dernières années.

Il est rare de voir des entreprises maitriser, administrer et sécuriser seules leurs systèmes d'information. C'est un fait, **le monde hyperconnecté d'aujourd'hui repose sur des environnements informatiques de plus en plus « sur le Cloud » ou externalisés. Ces prestataires tiers et d'applications SaaS *(Software As A Service)* sont d'ailleurs toujours plus impliqués dans le traitement et la sécurité de données sensibles voire personnelles**.

Plus récemment, les nouveaux risques introduits par ces évolutions, les migrations vers les environnements agiles *(Office 365)* et le télétravail ont plongé les responsables de sécurité dans une approche encore plus stressante de la maitrise qui était, à l'époque uniquement « périmétrique ».

Séparer et cloisonner les données sensibles, durcir et sécuriser suffisamment ce système d'information non tangible tout en tenant compte du contexte et des nouveaux usages, est un véritable casse-tête qui impose également aux équipes chargées de la sécurité de prendre un virage différent pour se défendre des menaces.

Toutes les directions *(générales et informatiques)* ont pris conscience que la sécurité pour protéger ce patrimoine informationnel n'était plus une option. Ne pas avoir de budget pour adresser ce sujet ni s'entourer d'un responsable de la sécurité de l'information pour gérer une société de plus d'une soixantaine de salariés devient très risqué... ou pour certains acceptable jusqu'au jour où...

La sécurité a donc pris, peu à peu, une place conséquente à tous les niveaux et dans tous les secteurs d'une entreprise, mais les efforts pour anticiper et contrer les menaces sont encore hétérogènes. En effet, pour se défendre, il faut déjà savoir contre qui on se protège...

Les conséquences et les impacts d'une sécurité perfectible...

L'absence de sécurité et d'anticipation des risques engendre des conséquences très importantes pour l'entreprise. L'impact financier étant toujours la conséquence finale qu'il faudra affronter si un incident de sécurité survient.

LES CONSÉQUENCES SONT DIVERSES ET SURTOUT TRÈS SPÉCIFIQUES À L'ENTREPRISE, MAIS ON PEUT REGROUPER LES RISQUES EN QUELQUES CATÉGORIES. UN INCIDENT PEUT DONC AFFECTER :

• L'image de marque de l'entreprise engendrant potentiellement le risque de perdre des clients.

• L'activité en détériorant la qualité d'un service ou la capacité de le rendre à ses clients ou en passant du temps à résoudre cet incident.

• Le respect de lois, de réglementations ou de certifications comme pour le cas du rgpd et peut finir dans certains cas à l'interdiction d'exercer.

• La sureté des personnes.

• Le développement de l'entreprise lors d'exfiltration / espionnage de données de recherche confidentielles.

Amendes, pénalités, dommages et intérêts et perte de chiffre d'affaires sont souvent les conséquences induites par le manque d'anticipation de ces risques.

Cependant, depuis deux ans et avec la recrudescence des campagnes d'intrusion et de diffusion de rançongiciels, les directions prennent de plus en plus conscience de ces risques. Si une forte proportion d'entre elles ne disposent pas de mécanismes évolués pour détecter des attaques sophistiquées, la première étape reste de surveiller, de maitriser son périmètre exposé, de détecter les potentiels points d'entrée et de savoir réagir rapidement. Voilà ce que la Cyber Threat Intelligence opérationnelle permet d'apporter... Des solutions.

Pour toute entreprise, grande ou petite, qui se lance dans une opération de fusion/acquisition, nous recommandons fortement de dresser un portrait des risques cyber qui pèsent sur l'entreprise à acquérir. Il s'agit alors de faire de la Due Diligence.

En matière de cybersécurité, la Due Diligence est une opération qui permet d'identifier le risque associé à une entreprise tierce. Au cours de ce processus, les organisations recueillent des informations sur les efforts existants sur la protection des données stockées numériquement et s'il y a eu ou non une situation dans laquelle lesdites données ont été compromises.

Grâce à la Cyber Threat Intelligence, l'acquéreur prend donc connaissance d'éventuelles irrégularités que la société devra assumer après la fusion/acquisition.

LES AVANTAGES DE LA CTI APPLIQUÉE EN FUSION/ACQUISITION :

- Connaître le type de données traitées par l'entreprise et dans quelle mesure elles les protège.
- Comprendre le paysage des risques et identifier les menaces communes aux deux entreprises.
- Évaluer les risques de la transaction particulière avant d'engager sa responsabilité morale.
- Identifier s'il y a des problèmes qui peuvent justifier la restructuration de l'accord.

4. La nécessité de se placer du point de vue de l'attaquant.

L'avant/après WannaCry.

Il y a sans doute eu un avant et un après WannaCry. C'est en tous cas ce que l'on peut aisément penser lorsqu'on analyse l'évolution de la cybersécurité après cette attaque.

En mai 2017, WannaCry, un virus malveillant, s'est répandu sur des milliers d'ordinateurs pour chiffrer les données des utilisateurs et demander une rançon aux organisations ciblées. **L'un des tout premiers rançongiciel ayant fait parler de lui de manière si spectaculaire est également celui qui a fait prendre conscience aux entreprises du risque que les cybermenaces représentent sur leurs périmètres**. Plus de 150 pays touchés et des entreprises mises à l'arrêt pendant plusieurs mois parfois, WannaCry a infecté ses victimes au travers d'une faille de sécurité repérée et documentée par la NSA, mais n'ayant pas fait l'objet de mise à jour pour la corriger.

Cette étape majeure dans l'histoire récente de la cybersécurité a sans doute fait partie des éléments déclencheurs de l'analyse des menaces telles qu'on la connait aujourd'hui. La nécessité de comprendre son adversaire et sa manière d'opérer est aujourd'hui évidente pour tous.

Le discours a fini par évoluer transformant le « vais-je être attaqué ? » en « quand vais-je être attaqué ? ». Ainsi, le monde de la cybersécurité s'est organisé autour d'un objectif : anticiper les attaques pour diminuer leur occurrence et leur impact au maximum.

La communauté de la sécurité s'est organisée ces dernières années autour de la connaissance de l'environnement des menaces et de leur analyse. Pour ce faire, de nombreuses entreprises et organisations non gouvernementales notamment menées par des chercheurs en sécurité informatique ont créé des grilles de lecture permettant de mieux comprendre notre environnement de menaces.

C'est dans ce cadre que plusieurs matrices ont émergé, notamment la MITRE ATT&CK. Ayant pour vocation d'être un guide pour les experts dans l'analyse des cybermenaces, cette base de connaissances reposant sur « des observations réelles » met en avant les méthodologies spécifiques d'attaques et modèles de menaces utilisées par les cybercriminels pour cibler tant les institutions que les entreprises privées.

Séparée en 14 catégories renvoyant chacune à une technique d'attaque utilisée par les criminels, cette matrice permet de mettre en lumière les différentes méthodes utilisées par les attaquants tout au long d'une attaque informatique.

La nouvelle vision de la cybersécurité : se placer dans la posture d'un attaquant.

L'adoption de cette posture d'attaquant, externe aux organisations ciblées, renvoie à d'autres disciplines de la sécurité informatique et notamment aux tests d'intrusion. Cette méthode fait aujourd'hui partie intégrante des méthodes dont les organisations se dotent pour sécuriser leur environnement. **Quoi de mieux que d'identifier ses failles d'un point de vue extérieur, dans des conditions reprenant une réelle tentative d'attaque ?**

Il en est de même avec la Cyber Threat Intelligence. **En connaissant ses failles d'un point de vue externe et en identifiant celles pouvant être utilisées contre soi, il est plus simple d'y remédier et de maitriser son environnement.**

Un second axe de la Cyber Threat Intelligence fait également partie intégrante des stratégies de défense des organisations : l'association entre renseignement sur les groupes d'attaquants et victimologie. Les groupes d'attaquants et les conséquences de leurs actions font l'actualité depuis de nombreuses années et grâce à la structuration du domaine autour de ces enjeux, **les professionnels de la cybersécurité disposent aujourd'hui de nombreux outils pour se prémunir de ces attaques.**

Cette approche orientée « attaquant », concrète et efficace est plus tangible pour les directions générales. Elle permet de mettre en place un plan d'action et d'y associer des budgets. Présenter qui pourrait attaquer, leurs motivations et les possibles moyens permettant de mobiliser les entreprises face au risque cyber.

Les modèles, la boîte à outils de la Cyber Threat Intelligence.

MATRICE MITRE ATT&CK : COMPRENDRE COMMENT UNE CIBLE EST CONCRÈTEMENT ATTAQUÉE

Évoquée plus haut, la matrice MITRE ATT&CK ne permet pas seulement de **comprendre comment les criminels choisissent et ciblent leurs victimes, mais également de comprendre comment est attaquée concrètement une cible, une fois choisie**. Composée de 14 étapes reprenant les tactiques et techniques associées des groupes criminels, **cette matrice permet de cartographier les modes opératoires des attaquants et de mettre en lumière la chronologie des attaques**.

Au travers de la récupération d'indicateurs de compromission présents dans les environnements informatiques des victimes, leur analyse permet aux nombreux chercheurs et professionnels en sécurité informatique de mettre en lumière des patterns et biais relatifs aux groupes criminels. Ces patterns et biais permettent, bien qu'il soit extrêmement délicat d'attribuer une attaque à un groupe spécifique *(si celui-ci ne le revendique pas)* de pointer le curseur vers un groupe plutôt qu'un autre. Le but étant de créer une fiche d'identité du groupe reprenant ses tactiques et techniques d'attaque associées, son origine, ses attaques précédentes connues, ses liens avec d'autres groupes ou pays étrangers, etc.

MATRICE CYBER KILL CHAIN : COMPRENDRE LA CHRONOLOGIE DES ATTAQUES INFORMATIQUES

Ainsi, tout comme le ferait un agent de police en traquant un criminel dont les méfaits seraient régulièrement répétés, il est possible de dégager de ces analyses des éléments différenciant les groupes de criminels. L'une des matrices les plus utilisées dans ce cadre est la Cyber Kill Chain. Reprenant une partie des catégories de la matrice MITRE ATT&CK, cette « chaîne cybercriminelle » est reprise du terme militaire « kill chain » désignant une « chaîne de frappe » utilisée pour cibler un ennemi.

Complémentaire à la matrice MITRE ATT&CK, **la Cyber Kill Chain permet à une organisation d'identifier à chaque stade d'une attaque ciblée, la manière dont elle pourrait réagir et détecter cette attaque**.

À mi-chemin entre la posture de l'attaquant et la capacité de réaction des victimes, cette matrice est un outil indispensable à la compréhension de la chronologie des attaques informatiques.

LE MODÈLE EN DIAMANT POUR METTRE EN RELIEF LE RENSEIGNEMENT SUR VOS MENACES ET DRESSER VOTRE PROFIL DE CIBLE

Cependant, la connaissance des groupes et l'identification de leurs vecteurs d'attaque ne constituent qu'une partie des informations nécessaires pour se prémunir des futures attaques.

Le renseignement sur les victimes est la deuxième pierre angulaire de cette analyse. Utilisées par les criminels pour cibler les organisations, ces informations liées à la victimologie des cibles sont foncièrement liées à la connaissance des cibles dans leur ensemble.

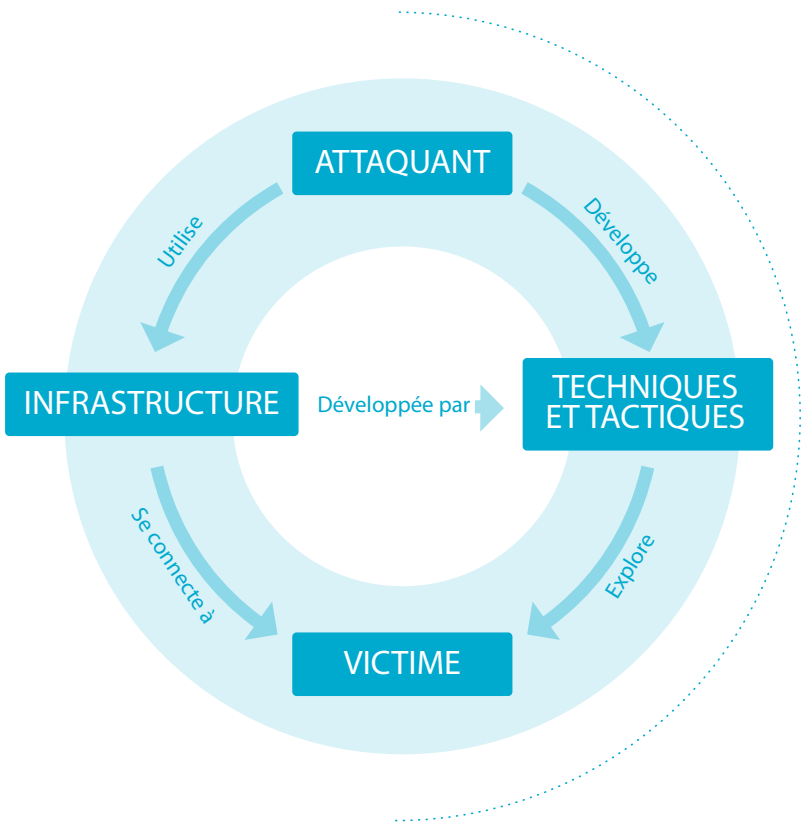
Son but est d'identifier des patterns de cibles, autrement dit, des types de cibles aux caractéristiques spécifiques et schémas d'attaque associés.

Cette posture d'analyse du point de vue des victimes est encore assez peu développée et l'une des matrices d'analyse les plus connues est sans doute le modèle en diamant *(ou « Diamond Model »)*.

Représenté comme un diamant, son but est de mettre en relief tout le renseignement sur la menace :

- Le profil de l'attaquant
- Les méthodes utilisées par l'attaquant
- Les informations liées à l'infrastructure de la cible
- Les informations publiques liées à la cible

Chacun de ces quatre éléments représente une partie de ce diamant dont les branches communiquent entre elles de la manière suivante :



L'intérêt de cette matrice se trouve principalement dans le fait qu'elle se positionne du point de vue de l'attaquant tout en étant spécifique à l'organisation ciblée.
Les autres matrices, notamment MITRE ATT&CK et la Cyber Kill Chain mettent en lumière les tactiques et techniques des attaquants en ne distinguant pas toujours les cibles les unes des autres. Le modèle en diamant en mettant en relief le renseignement sur les menaces *(Attaquant et Techniques et tactiques)* et sur les victimes *(Victime et Infrastructure)* permet de contextualiser les menaces en fonction d'une victime ou d'un groupe de victimes en particulier.

Enfin, au-delà de la victimologie propre à l'organisation dans son ensemble, **il est important d'identifier à un niveau plus bas, les personnes ou services les plus ciblés. C'est le principe du modèle VAP *(« Very Attacked Person »)* basé sur la surveillance et la sécurisation accrue des boites mail de personnes VIP ou de boites mail « alias » souvent ciblé par les criminels**. Lorsque l'on sait que les attaques par phishing et les fuites d'identifiants de connexion sont monnaie courante, l'identification des personnes à risque ainsi que de leurs informations exposées permet d'anticiper grandement les prochaines attaques.

Ces deux modèles permettent donc d'établir un niveau de risque de l'entreprise d'un point de vue cyber, répondant notamment aux questions suivantes :

- **Comment suis-je ou vais-je être attaqué ?**
- **Qui et quoi, au sein de mon organisation, est ou sera ciblé ?**
- **Comment prévenir ces attaques et diminuer leur risque d'occurrence et leur sévérité ?**

On peut donc identifier trois manières d'utiliser la CTI comme volet actionnable de sa stratégie cyber :

- **La mise en lumière de ses failles et vulnérabilités en adoptant une posture d'attaquant**
- **La connaissance des groupes d'attaquants, de leurs principaux buts et la compréhension de leurs modes opératoires et techniques d'attaques**
- **L'analyse des cibles permettant de mettre en avant le profil type des victimes**

Ces trois aspects se complètent et permettent aux organisations de créer une fiche d'identité de votre menace permettant ensuite d'adapter votre stratégie de cyberdéfense. Une fois ces analyses effectuées et votre carte d'identité de victime créée, comment concrètement mettre en place votre stratégie cyber au travers de la CTI ? Quels sont les éléments à prendre en considération dans le choix de votre prestataire de services CTI et comment peut-il m'accompagner dans la définition de mes objectifs et la compréhension de mes risques ?

5. Comment choisir son partenaire de Cyber Threat Intelligence en 11 points clés.

NOUS AVONS DRESSÉ UN PORTRAIT DE LA CYBER THREAT INTELLIGENCE, VOUS L'AVEZ COMPRIS, ELLE DEVIENT INÉVITABLE POUR GARANTIR UNE SURVEILLANCE GLOBALE DE VOTRE EXPOSITION.

L'un des principaux challenges pour les RSSI se trouve principalement dans la partie prévention, car contrairement aux opérations, celles-ci ne se passent pas au sein de son réseau. L'un des outils les plus adaptés est la CTI, qui lui permet d'obtenir une vision externe de son exposition et des risques associés. Vous vous poserez notamment les questions suivantes :

• Quels serveurs ou applications sont les plus exposées ?

• Quelle méthode utiliserait un attaquant pour s'introduire dans mon SI ?

MAINTENANT, VOUS VOUS DEMANDEZ CERTAINEMENT VERS QUEL PARTENAIRE VOUS TOURNER ? NOUS VOUS PROPOSONS 11 POINTS D'ATTENTION POUR BIEN LE CHOISIR.

1 Privilégiez un programme qui **surveille 24/7 votre surface d'attaque** *(périmètre connu)* **et votre surface d'exposition** *(périmètre inconnu)*.

2 Ne cherchez pas **une solution tout-en-un, mais une solution qui peut s'adapter à vos besoins**. Chaque entreprise est différente et les menaces qui les ciblent peuvent varier. Il est important de pouvoir intégrer autant d'assets que vous le souhaitez, car ils risquent d'évoluer et représentent la base de nos recherches.

3 **Si jamais vous souhaitez élargir votre stratégie de cyberdéfense en misant aussi sur une meilleure anticipation ou une réaction aux menaces, vérifiez les offres complémentaires du prestataire**.

a. Est-il capable de proposer des offres d'anticipation des menaces : un service de **veille en cybersécurité, de scan de vulnérabilités ou de surveillance du typosquatting** ?

b. Est-il capable de vous accompagner en cas d'incident *(dispose-t-il de la certification GIAC CFA Forensic Analyst qui atteste de sa capacité d'accompagnement)* ? S'il y a une menace ou un incident de sécurité, le prestataire qui vous en livre l'information sera plus réactif.

4 **Choisissez des prestataires qui se positionnent d'un point de vue extérieur et en posture d'attaquant**. Vous pourrez ainsi surveiller votre exposition, qu'il s'agisse d'assets ou de données non-maitrisées ou inconnus. Au travers d'une cartographie de votre périmètre, **une carte d'identité de votre organisation** pourra ainsi être régulièrement réalisée et vous permettre d'anticiper les risques liés au Shadow IT, aux fuites de données ou encore au dénigrement de votre marque.

5 **Optez pour des prestataires à même de vous apporter une définition dynamique de votre périmètre**. Les environnements sur lesquels reposent les systèmes dynamiques hébergés au sein d'un **Cloud sont en constante évolution**, il est donc primordial de disposer d'une boite à outils suffisamment sophistiquée pour réaliser une cartographie du SI dynamique de manière récurrente.

6 **Demandez à voir un exemple d'alerte**. Vous saurez juger de sa qualité, du contexte apporté. Une alerte bien rédigée permet une remédiation rapide et facile.

7 **Faites appel à un prestataire qui dispose d'un CERT**. C'est l'assurance pour lui d'avoir accès à certaines données et aux forums d'échanges d'information. Pour ce faire, les CERT se partagent des informations de manière privée et public sur les retours d'expérience des investigations réalisées. Ces échanges de données se font notamment grâce à des logiciels comme MISP, TheHive ou encore OpenCTI. L'accès à ces bases de connaissances permet à un programme de CTI d'être au fait des dernières attaques et méthodes de contournement.

8 Nous vous conseillons également **un service qui intègre une analyse manuelle pour éviter le bruit et les faux positifs qui peuvent augmenter le temps de traitement des alertes**.

9 **La solution idéale se trouve finalement dans le choix d'un service qui allie l'exhaustivité et la continuité des scans automatisés** sur le web et l'expertise humaine grâce à des **analyses manuelles**. C'est la combinaison de toutes ces informations qui permet de construire une cartographie des risques la plus exacte possible. Un RSSI peut ainsi avoir une vision exacte de ce qu'il maitrise et ne maitrise pas.

10 **Vérifiez que vous avez accès à un maximum de livrables**. Ils permettront de suivre vos menaces et évaluer vos risques en fonction de votre contexte spécifique.

a. Des synthèses managériales
b. Des recommandations
c. Des cartographies ponctuelles de votre surface d'attaque
d. Un indicateur de suivi du niveau de risque global
e. Un dashboard reprenant toutes vos statistiques
f. Un portail de gestion collaboratif
g. Une API pour une connexion à votre SOC

Les fonctionnalités sont variées ! Profitez des livrables mis à votre disposition pour vous faciliter le travail et avoir une meilleure vision de la sécurité de votre entreprise et des actions à mettre en œuvre.

11 **Pour aller plus loin dans votre connaissance des menaces, vous pourriez également demander à votre partenaire des investigations complémentaires**.

a. Est-il capable de vous fournir des notes d'analyse sur les groupes d'attaquants ? Pour identifier un attaquant qui aurait ciblé votre système ou qui le souhaiterait, **il est important de connaitre les méthodologies, les outils employés, les infrastructures utilisées par les attaquants. Ils peuvent s'accommoder à une étude comportementale des attaquants**.

b. Est-il capable de tester les nouvelles menaces pour voir si vous êtes exposé ? Une veille quotidienne des nouvelles vulnérabilités et failles type 0-day est indispensable afin d'identifier vos menaces. De la manière, un prestataire en capable de tester ces nouvelles menaces sur votre périmètre est indispensable à votre protection.

Pour conclure, connaitre votre exposition sur Internet est primordial. Un attaquant utilisera toutes les informations disponibles et ne se limitera pas aux sites vitrine. **Les ressources non maitrisées de type Shadow IT ou environnements de développement restent une cible privilégiée des attaquants**.

Afin de mieux anticiper les attaques, il est important aussi de considérer que l'attaquant est déjà présent. Connaitre les Tactiques Techniques et Procédures des attaquants est primordial pour bien paramétrer ses logiciels de défense. Il permettra également une plus grande efficacité en cas d'investigation numérique.

Si vous avez validé les 11 points de cette checklist, choisi le prestataire et mis en place le programme de CTI, c'est que vous avez accès à tout le renseignement concernant les menaces ! Ce renseignement est primordial pour établir votre stratégie de défense, prioriser vos choix de sécurité et adapter votre budget en conséquence.

6. Comment l'analyse fine de la CTI vous aide à répartir votre budget cybersécurité global ?

La CTI : un outil de pilotage par les risques pour les décideurs.

La démarche de Cyber Threat Intelligence permet aux dirigeants ainsi qu'à toute la filière « Sureté et Sécurité » de mieux connaitre l'environnement dans lequel leur entreprise évolue, et plus particulièrement les menaces qui pèsent sur cette dernière. **L'une des finalités de cette démarche est de permettre aux décideurs de mettre en place une stratégie de pilotage par les risques**. Cette approche rend exploitables et compréhensibles des données et des informations manipulées par l'entreprise, qui étaient jusqu'alors réservées aux équipes techniques opérationnelles. En effet, chaque société évolue dans un contexte spécifique, et sa cartographie des risques lui est donc propre. Il n'y a donc pas de règle universelle en termes de stratégie de pilotage et de réduction du risque.

Outil de gestion particulièrement important pour un décideur, **le budget de l'entreprise se doit donc d'être aligné avec la stratégie adoptée** pour être efficace. Pour cela, il est possible d'utiliser les renseignements délivrés par la CTI afin d'alimenter et de compléter l'analyse de risque, tant au niveau global de l'entreprise qu'au niveau plus spécifique *(filiale, projet, site, …)*.

L'apport de la démarche de CTI sera de rendre possible la contextualisation des risques à une entreprise particulière, selon différents éléments tels que :

- **L'environnement économique ou géopolitique dans lequel évolue l'entreprise**

- **Le profil d'attaquant pouvant la cibler :**
  - Les acteurs de la menace en présence
  - Le type d'attaques réalisées
  - Le mode opératoire utilisé *(schéma d'attaque)*

- **Et enfin, la victimologie de chacun des attaquants identifiés précédemment :**
  - Les secteurs d'activité ciblés
  - La localisation géographique des victimes
  - La fréquence d'attaque *(probabilité d'occurrence)*

NIVEAU LOCAL / MICROSCOPIQUE

Pour illustrer cela, commençons par détailler les apports d'une démarche de CTI au niveau « micro ». Différentes actions doivent être adoptées afin de poser des bases saines et de garantir l'identification de tous les risques pesant sur l'entreprise.

Celles-ci peuvent être classées selon 3 niveaux :

1. **La connaissance du panorama général de la menace**

2. **La contextualisation de ce panorama à l'environnement spécifique de l'entreprise**

3. **L'exploitation des données techniques interne à l'entreprise**

Focus : Identification des vulnérabilités de l'entreprise.

1. DISPOSER D'UN PANORAMA GÉNÉRAL DE LA MENACE À JOUR

La première action consiste à disposer d'une vision du panorama de la menace maintenue régulièrement à jour. Ainsi, réaliser une veille généraliste sur les groupes d'attaquants connus, leurs méthodes, les failles identifiées par les chercheurs ou les éditeurs permet à l'entreprise de savoir dans quel environnement elle opère et d'adopter des premières mesures de remédiation.
Cette démarche n'est néanmoins pas suffisante. Il est en effet nécessaire de transcrire ce contexte général dans le contexte spécifique de l'entreprise *(Suis-je réellement affectée par la faille CVE récemment corrigée et exploitée de manière opportuniste par les pirates ?)*.

L'objectif de ce volet est de disposer d'une vision claire de l'environnement de l'entreprise et d'identifier des risques existant au niveau microscopique.

2. CONTEXTUALISER LE PANORAMA DE LA MENACE À MON EXPOSITION RÉELLE

La collecte de ces renseignements actionnables permettra aux équipes opérationnelles *(DSI et SSI)* d'identifier concrètement les vulnérabilités affectant l'entreprise et étant recherchées par les attaquants.

L'identification des vulnérabilités pesant sur l'entreprise permettra ainsi aux équipes opérationnelles de remédier le plus rapidement possible, au cas par cas, aux évènements identifiés ponctuellement, tels que :

- L'enregistrement de nouveaux domaines utilisés pour tromper la vigilance des collaborateurs, des clients ou des partenaires de l'entreprise *(ingénierie sociale type arnaque au président, vol de données sensibles via du phishing, …)*

- L'identification de données sensibles appartenant à l'entreprise *(données techniques ou métier, rapports, …)*

- L'identification de composants sensibles publiquement exposés *(interface d'administration, base de données et autres partages ouverts sur Internet)*

- La mise en ligne de nouveaux sites vulnérables sans validation préalable du niveau de sécurité par les équipes des filières DSI / SSI *(Shadow IT)*

- L'identification d'équipement constituant l'infrastructure de l'entreprise affectés par une nouvelle menace *(0day)* exploitée massivement par les pirates pour obtenir un accès distant au SI de l'entreprise.

L'objectif de ce volet est d'anticiper au mieux l'exploitation d'une vulnérabilité affectant l'entreprise en aadoptant un point de vue externe et d'identifier des risques existant au niveau local / microscopique.

Focus : Identification des menaces ciblant l'entreprise.

1. CROISER LES DONNÉES TECHNIQUES AVEC LES MARQUEURS CIBLANT L'ACTIVITÉ DES PIRATES

Dans l'idéal, il est enfin important d'exploiter les informations disponibles au sein de l'entreprise *(logs, rapport d'incident, résultats d'investigation)* pour identifier les activités suspectes des pirates.
Ce type d'activité est classiquement réalisée par une équipe de type SOC au travers d'un SIEM.

Bien que ne permettant pas d'anticiper l'occurrence d'une menace, les renseignements issus de ces activités permettront de compléter l'analyse de risque au niveau global de l'entreprise.

L'objectif de ce volet est de compléter les aspects « connaissance de l'environnement » et « anticipation de la menace » en adoptant un point de vue interne à l'entreprise, toujours dans l'objectif d'identifier des risques existants au niveau local / microscopique.

2. POINT D'ÉTAPE : NIVEAU LOCAL / MICROSCOPIQUE

Il est d'ores et déjà possible de tirer une première conclusion après la présentation de ces trois axes de collecte de renseignement.

L'identification d'évènements isolés, ayant un impact localisé et dont l'occurrence ne peut malheureusement pas être anticipée, est primordiale pour l'entreprise.

Premièrement, cela permet à l'entreprise d'adopter des mesures efficaces et pragmatiques de réduction du risque.

Deuxièmement, en prenant du recul sur les résultats retournés au travers de cette démarche, l'analyse de ces incidents permettra d'identifier les services ou activités de l'entreprise les plus exposés *(filiale X ou Y, département RH ou DSI, etc.)* aux différents risques identifiés :

- Atteinte à l'image de l'entreprise
- Vols de données personnelles *(collaborateurs ou clients) ou métier (propriété intellectuelle, données stratégiques liées au pilotage de l'entreprise, …)*
- Fraude *(ciblant directement ou indirectement l'entreprise : cas des clients)*
- Perte de compétitivité et/ou de productivité
- Risques économiques et financiers
- Non-conformité avec la législation
- Risques liés aux nouvelles réglementations et changement de politiques

D'un point de vue de la stratégie à adopter, il est donc important de définir un premier budget correspondant à un fonds de roulement. Ce dernier permettra de garantir la production de renseignements contextualisés à la réalité de l'entreprise.

3. POINT D'ÉTAPE : NIVEAU GLOBAL / MACROSCOPIQUE

En complément de ces premières mesures ciblant l'occurrence d'évènements isolés, l'entreprise doit adopter une stratégie plus globale pour exploiter au mieux la CTI. En effet, la connaissance des menaces et des contextes opérationnels au niveau local permettra à un décideur de mieux adapter sa stratégie au niveau global.

Cette connaissance lui permettra par exemple d'influer sur :

- **L'organisation de l'entreprise** *(recrutement, redistribution des responsabilités entre les équipes, sensibilisation des équipes, …)*
- **L'organisation de son système d'information** *(architecture du SI, accès au SI, mise en place de nouvelle infrastructure pour répondre à un besoin particulier, …)*
- **L'exploitation de son système d'information** *(données disponibles, mais non exploitée, …)*

Focus : En réaction aux vulnérabilités identifiées.

Quelques exemples concrets issus de nos retours d'expériences :

L'identification régulière d'**interfaces d'administration ou de composants d'infrastructure sensibles accessibles publiquement** peut pousser à l'adoption de différentes mesures d'envergure telles que :

- La refonte de l'architecture du SI de l'entreprise.

- L'adoption d'une nouvelle organisation interne garantissant le respect « by design » de certaines contraintes sécuritaires.

L'identification d'un **nombre élevé de domaines suspects réutilisant l'identité de l'entreprise** peut pousser l'entreprise à adopter des mesures telles que :

- La mise sur liste noire des domaines suspects - pour bloquer l'accès à ces sites suspects ou les mails dans lesquels ces domaines sont mentionnés, pour protéger les collaborateurs.

- Le lancement de campagne de sensibilisation des collaborateurs à la menace représentée par les campagnes de phishing et autres arnaques au président.

- Le lancement ponctuel de campagnes de communications à destination des clients de l'entreprise afin de rappeler les méthodes d'accès « officielles ».

- L'enregistrement préventif des principaux domaines et de leurs déclinaisons.

- L'ouverture de dossier type UDRP auprès de l'ICANN afin de récupérer ces domaines.

L'identification régulière de **ressources *(sites)* de type Shadow IT** peut pousser à l'adoption de différentes mesures d'envergure telles que :

- La mise en place de campagne de communication interne pour rappeler les règles concernant le dépôt de noms de domaine, et la mise en ligne de nouveaux sites.

- La mise en place d'un processus interne pour le dépôt de noms de domaine et l'hébergement de nouveaux sites.

Enfin, l'identification d'un grand nombre de **fuites d'information provoquées par des partenaires** peut pousser l'entreprise à adopter des mesures telles que :

- La définition et l'adoption d'une politique de classification.

- L'ajout de clauses contractuelles relatives au Maintien en Condition de Sécurité *(MCS)* ou de confidentialité dans les process d'achat.

- La mise en place de politique et d'outils de DLP *(Data Leakage Prevention)*.

Focus : Identification des menaces de l'entreprise.

En complément des décisions stratégiques apportées pour répondre aux enjeux liés aux vulnérabilités, des réponses doivent également être formulées pour adresser les menaces identifiées.

Par exemple, l'identification d'un **groupe d'attaquant ciblant spécifiquement les entreprises ou ses parties prenantes *(fournisseurs, clients, …)* opérant dans mon secteur d'activité** peut pousser à l'adoption de différentes mesures d'envergure telles que :

- L'identification et l'exploitation de nouvelles sources *(logs)* au sein du système d'information, afin de disposer de la capacité d'identifier les traces d'activité spécifique à un acteur.
- L'adaptation de la PSSI de l'entreprise afin de refléter le risque existant, et les mesures de réduction du risque adoptées pour y répondre.

Remerciements :

Charles DAGOUAT
Adrien GUINAULT
Charlène GREL
Julien TERRIAC
et Paloma SIGGINI

À propos de

serenety
By xmco

Créée en 2010, Serenety est un service de Cyber Threat Intelligence, développé par le CERT-XMCO et à destination des organisations publiques et privées. Son objectif est d'identifier la surface d'attaque et la surface d'exposition des organisations surveillées au travers d'un outil simple d'utilisation et ergonomique. Il se distingue de ses concurrents par la corrélation de ses résultats issus des analyses automatiques des sources ouvertes surveillées et des investigations manuelles de son équipe d'experts qualifiés. Cette surveillance permet d'identifier les menaces et d'anticiper les risques notamment liés aux fuites de données, aux systèmes exposés et vulnérables ou encore à la compromission de comptes.

xmco

Cabinet de conseil indépendant en cybersécurité, XMCO a à cœur d'accompagner ses clients, de toute taille et de tous secteurs, dans l'anticipation des vulnérabilités, la détection des failles et la réponse à incidents. XMCO est qualifié PASSI sur l'ensemble des portées, ce qui confirme le cœur de métier historique : l'audit et les tests d'intrusion.

Retrouvez-nous

Sur notre site :

www.xmco.fr

Sur les réseaux sociaux :

Envie d'échanger ?

sales@xmco.fr

01 79 35 29 30