N°1 - 18€
3ÉME TRIMESTRE 2020

LE JOURNAL DES RISQUES CYBER

www.l1focr.com

L'1FO CR

- **Conformité :** les conséquences de l'annulation de Privacy Shield
- **Techno :** l'analyse d'ORC, outil open source de collecte des données forensiques fourni par l'ANSSI
- **Outils :** Appliances firewall ou l'essor de la virtualisation
- **Menaces :** Emotet, le retour
- **Projets :** Campus Cyber, ça se précise !

ENDPOINT DETECTION AND RESPONSE

Qu'attendre de l'EDR pour protéger un parc informatique ?

Comment la région Grand Est a maîtrisé sa plus grande cyberattaque

L'1FO-CR

38 rue Jean-Jaurès 92800 Puteaux – France
Tél. : +33 (0)1 74 70 16 30 | Fax : +33 (0)1 40 90 70 81
contact@pcpresse.com

RÉDACTION
Guillaume Périssat (rédacteur en chef délégué)
avec Bertrand Garé et la collaboration
de Julien Alis, Isabelle Cantero, Eric A. Caprioli,
Marina Casas, Alain Clapaud, Paul-Olivier Gibert,
Christophe Guillemin, Claude Marson
et Thierry Thaureaux.
redaction@pcpresse.com

CHEF DE STUDIO
Franck Soulier
Illustrations vectorielles : Designed by Freepik

PUBLICITÉ
Tél. : +33 (0)1 74 70 16 30 | Fax : +33 (0)1 40 90 70 81
pub@pcpresse.com

VENTE AU NUMÉRO
France métropolitaine 18 € TTC (TVA 5,5%)

ABONNEMENTS
France métropolitaine 60 € TTC (TVA 5,5%)
Toutes les offres : visiter pcpresse.com,
rubrique s'abonner.
Pour toute commande d'abonnement d'entreprise
ou d'administration avec règlement
par mandat administratif, adressez votre bon
de commande à : PC Presse - L'1FO-CR,
service abonnements, 38 rue Jean-Jaurès
92800 Puteaux – France
ou à abonnements@pcpresse.com

IMPRESSION
Imprimé en France par SIB (62)
Dépôt légal : 3ème trimestre 2020

L'1FO-CR est publié par PC PRESSE, S. A.
au capital de 130 000 euros, 443 043 369 RCS
Nanterre. Siège social : 38, rue Jean-Jaurès,
92800 Puteaux, France.
ISSN en cours

Un magazine du groupe PCpresse,
DIRECTEUR GÉNÉRAL, DIRECTEUR
DE LA PUBLICATION : Michel Barreau

Édito

Les indicateurs sont au rouge. Il y a deux fois plus de cas que voici quelques semaines. Nous ne sommes pas préparés pour faire face à une recrudescence massive. Les comportements individuels et collectifs se dégradent. Les mesures de protection et d'hygiène sont négligées. De quoi parlons-nous ? De l'épidémie de Covid-19 ? Bien sûr, mais pas seulement ! Tout ce qui vient d'être écrit peut s'appliquer de la même manière à la cybersécurité et aux risques cyber. Les similitudes sont flagrantes et les conséquences, si elles ne portent pas sur la vie humaine – du moins pour le moment – peuvent être particulièrement graves pour une économie déjà sous perfusion. Imaginons maintenant une cyberattaque visant un hôpital comme cela a déjà pu se produire encore récemment. Quelles pourraient être les conséquences pour la vie des patients, dans une période de pandémie ?
Il est plus urgent que jamais que les professionnels de la sécurité, acteurs comme utilisateurs, tirent la sonnette d'alarme et alertent sur la nécessité d'une mobilisation massive, à l'échelle internationale. C'est dans tous les cas le message que nous essaierons de faire passer dans cette publication.

La Rédaction

Sommaire

Invalidation du Privacy Shield : trois questions à Luc d'Urso, CEO du Groupe Atempo.Wooxo

Qu'est-ce le Privacy Shield ?
Le Privacy Shield (en français *« bouclier de protection des données »*) est un accord dans le domaine du droit de la protection des données personnelles, qui a été négocié entre l'Union européenne et les États-Unis d'Amérique. L'Union Européenne avait reconnu en Août 2016, le Privacy Shield conforme à la Directive Européenne de Protection des Données Personnelles en vigueur.
Ce *« bouclier de protection des données »* permettait aux entreprises américaines d'apporter des garanties « suffisantes » en matière de mesures de protection des données personnelles provenant d'Europe.

Invalidation du Privacy Shield, quels impacts pour les entreprises européennes ?
Le Privacy Shield était un mécanisme d'auto-certification puisque les entreprises américaines s'engageaient à respecter ces obligations pour être inscrites dans la liste des entreprises certifiées.
La Directive Européenne de Protection des Données Personnelles a été remplacée par le RGPD adopté par le Parlement Européen en avril 2016 et entrée en vigueur dans les 27 Etats membres de l'UE en mai 2018. Le 16 juillet dernier la Cour de justice de l'UE (CJUE) a rendu un arrêt dans l'affaire connue sous le nom de Schrems II (C-3111-18), dans laquelle les mécanismes de transfert de données personnelles entre l'UE et les États-Unis ont été contestés.

Quelles alternatives et solutions proposées aux entreprises pour être en conformité ?
La meilleure option consiste à opérer un rapatriement des données concernées et en confier le traitement à des fournisseurs 100% européens. Ces solutions existent :
European Champions Alliance – Cartographie et Buyers Guide disponibles : https://european-champions.org/focus-group-cybersecurity
PlayFranceDigital – Cartographie disponible : www.lesacteursdunumerique.fr/
Innovalead – Guide des Solutions alternatives : https://innovalead.fr/Les-solutions-DigitalWorkplace-alternatives

* Le 16 juillet 2020, la Cour de Justice de l'UE (CJUE) a annulé le Privacy Shield. Les entreprises ayant transféré leurs données vers l'une des +5000 solutions américaines (applications SAAS, hébergeurs ou autres services cloud) signataires du Privacy Shield, sont depuis la mi-juillet dans l'illégalité et doivent se mettre à la recherche de solutions leur permettant de revenir rapidement dans le cadre légal.

Miria garantit la performance et le succès de la migration de vos données vers de nouveaux services 100% européens

La FRENCH TECH FT120
HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY
MEMBRE DU GIP ACYMA CYBERMALVEILLANCE.GOUV.FR Assistance et prévention du risque numérique
FRANCE CYBER SECURITY
FRANÇAISES UTILISÉ PAR LES ARMÉES FRANÇAISES

N°1 EUROPEAN SOFTWARE VENDOR FOR DATA PROTECTION

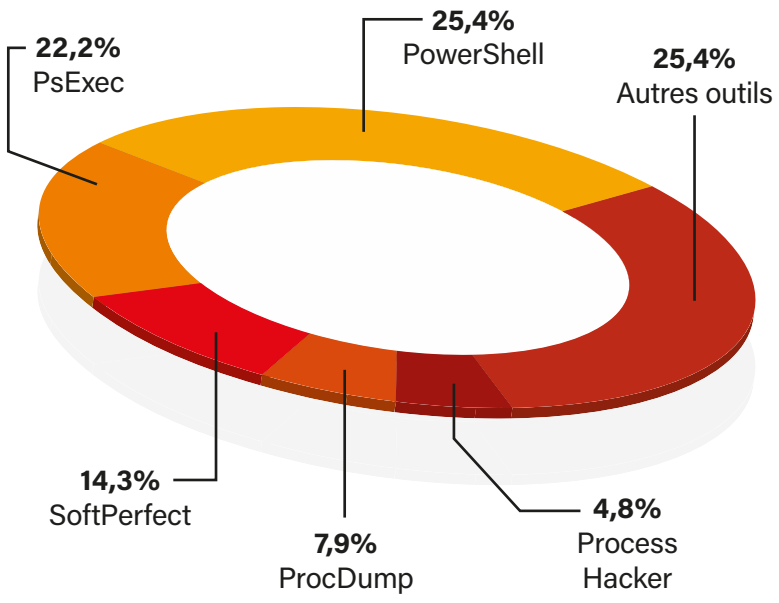
WWW.ATEMPO.COM

L'argument qui a primé étant que la législation américaine ne permet pas de garantir réellement une protection des données personnelles en provenance de l'UE qui soit conforme au Règlement Européen sur la Protection des Données (RGPD).
Les entreprises ayant transféré leurs données vers l'une des quelques cinq mille solutions américaines (applications SAAS, hébergeurs ou autres services cloud) signataires du Privacy Shield, sont depuis la mi-juillet dans l'illégalité et doivent se mettre à la recherche de solutions leur permettant de revenir rapidement dans le cadre légal.

Revenons sur cette décision et ses impacts pour les entreprises européennes :
L'argument qui a motivé l'annulation est que la législation américaine ne permet pas de garantir réellement une protection des données personnelles en provenance de l'UE qui soit conforme au RGPD.
Cette décision n'empêche donc pas les entreprises soumises au RGPD de transférer des données à caractère personnel vers les Etats-Unis, mais elle invalide la base légale sur laquelle la grande majorité de ces transferts étaient réalisés. Les mécanismes permettant les transferts devront donc être strictement encadrés par des clauses contractuelles types (CCT) garantissant la conformité desdits mécanismes au RGPD. Dans la pratique, ces entreprises s'exposent à des amendes conséquentes en cas de non-conformité avérée des mécanismes utilisés et l'appel en responsabilité des entreprises américaines paraît illusoire.

TABLEAU DE BORD

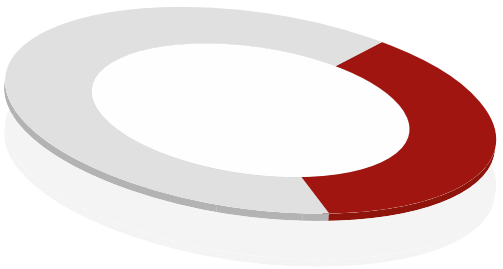
Rapport Kaspersky : un tiers des attaques est mené via des outils bien connus



Dans son rapport mondial Incident Response Analyst concernant l'année 2019, Kaspersky souligne que 30% des cyberattaques sur lesquelles a enquêté son équipe Global Emergency Response impliquaient des logiciels administratifs et de gestion authentifiés. Ce sont surtout les logiciels de monitoring qui paraissent la cible des hackers. Kaspersky cite PSExec et SoftPerfect Network Scanner mais également PowerShell. Pour Bertrand Trastour, Head of B2B, Kaspersky France, Afrique du Nord, de l'Ouest et Centrale, *« pour éviter de se faire détecter et rester invisible le plus longtemps possible sur le réseau de l'entreprise ciblée, les attaquants utilisent fréquemment des logiciels qui sont normalement développés pour les activités quotidiennes, comme le traitement des tâches liées à l'administration réseau et les diagnostics système. En effet, grâce à ces outils, les attaquants peuvent recueillir des informations sur le réseau de l'entreprise et effectuer des actions parallèles à celles des administrateurs, comme modifier les paramètres des logiciels et ceux des appareils, ou mettre en place des actions malveillantes (crypter les données des clients par exemple). Utiliser des logiciels authentifiés et légitimes peut également aider les pirates à rester inconnus des analystes sécurité, car souvent l'attaque n'est détectée qu'une fois les dommages causés. S'il n'est pas possible pour l'entreprise d'exclure ces outils de monitoring et de gestion - car ils permettent son bon fonctionnement - la mise en place de systèmes d'authentification et de détection permet de repérer les activités suspectes sur le réseau et les attaques complexes à des stades plus précoces ».*

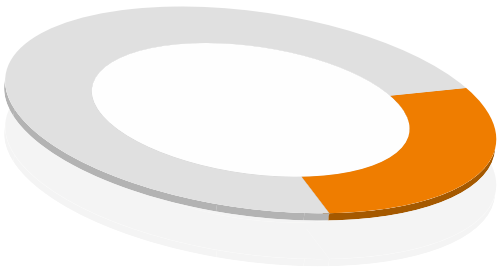
Enquête HackerOne Les RSSI sous pression et leurs budgets aussi !

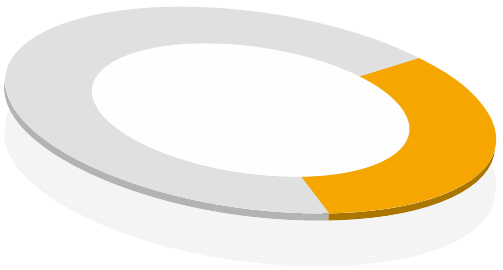
La plateforme de sécurité collaborative HackerOne a mené une enquête sur les défis des RSSI à l'ère de la pandémie de Covid. Cette enquête a été confiée à Opinion Matters qui a interrogé quelque 1400 RSSI et DSI d'entreprises de plus de 1000 employés en France, Allemagne, Royaume-Uni, Australie, États-Unis, Canada et Singapour au mois de juillet 2020. Concernant les seuls RSSI français 70% d'entre eux (66% au niveau mondial) estiment que suite à la pandémie leur entreprise est plus exposée aux violations de données. Pourtant 30% des RSSI français indiquent que les budgets de sécurité au sein de leur organisation ont été négativement impactés par la crise (25% au niveau mondial).
Selon Marten Mickos, PDG de HackerOne, *« la crise liée au COVID-19 a fait basculer pratiquement tous les aspects de notre vie en ligne. La pression pour répondre aux exigences du travail à distance et aux demandes des clients en matière de services numériques a considérablement élargi les surfaces d'attaque, laissant les équipes de sécurité à bout de souffle. Dans ce contexte d'urgence, de plus en plus d'organisations ont pris conscience des avantages de recourir à une communauté de hackers pour se protéger contre les activités malveillantes ».*
HackerOne indique une augmentation de 56% des inscriptions de hackers sur sa plateforme depuis mars dernier.



36%
des RSSI français ont observé une augmentation des attaques contre leurs systèmes informatiques.

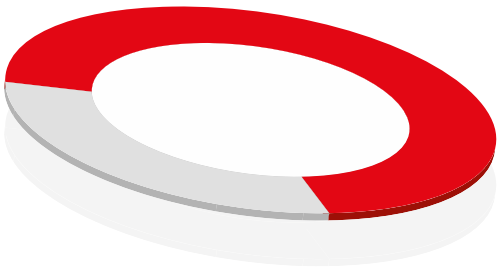
28%
des RSSI français affirment que les initiatives de transformation numérique se sont multipliées.





33%
des RSSI français sont plus enclins à accepter des rapports sur la sécurité de l'information de la part de chercheurs tiers.

70%
des RSSI français estiment que leur entreprise est plus exposée aux violations de données.



Rançongiciel : 18% des victimes capitulent

Le dernier rapport de l'assureur Hiscox apporte à la fois la possibilité d'être optimiste ou pessimiste selon les points observés dans le rapport. Ainsi le nombre des attaques a diminué fortement de 61 à 39 %. En revanche l'intensité des attaques est en hausse.
Les pertes liées à ce type d'attaque ont été multipliées par 6. Les rançongiciels connaissent une recrudescence importante (+ 19 %). Enfin 18 % des victimes capitulent et paient la rançon.
Le rapport fait le point aussi sur les conséquences de ces attaques et les impacts à long terme qu'elles peuvent avoir. 15 % des entreprises indiquent avoir plus de mal à attirer des clients. 11 % constatent des pertes de clients ou de partenaires commerciaux (12 %). Ces points s'ajoutent à l'arrêt brutal de l'activité, les conséquences en termes d'image et de réputation.
Frédéric Rousseau, en charge du marché Cyber chez Hiscox indique, qu'en moyenne, 80% des entreprises ayant perdu leurs données informatiques après une cyberattaque font faillite dans les 12 mois.

Cryptomonnaies : Ledger attaqué

Les plateformes d'échange de cryptomonnaies sont fréquemment la cible d'attaques. Quand le Bitcoin était à son plus haut, les tentatives étaient quotidiennes, et régulièrement couronnées de succès, les hackers volant ici et là l'équivalent de quelques centaines de milliers de dollars en devises virtuelles. Le rythme a quelque peu diminué mais l'industrie reste une proie particulièrement alléchante pour les cybercriminels. Ledger, entreprise française spécialisée en cryptowallets, des systèmes de stockage de cryptomonnaie, n'y a pas échappé. La société annonce avoir été victime d'une intrusion dans ses serveurs. C'est par le biais de son programme de bug bounty que Ledger a été informé, en juillet dernier, d'une potentielle vulnérabilité sur son site web. Aussitôt signalée, aussitôt corrigée.

Néanmoins, se penchant sur cette faille, l'équipe de Ledger découvre, une semaine environ après les faits, que celle-ci a été exploitée, permettant à un tiers non autorisé d'accéder à une base de données. L'entreprise prévient : les informations de paiement et les fonds stockés n'ont pas été affectés. Les pirates ont eu accès à une base de données marketing et e-commerce, *« utilisée pour envoyer des confirmations de commande et des e-mails promotionnels »*. Un accès obtenu via une clé API, désactivée depuis.

S'y trouvaient principalement un million d'adresses email d'utilisateurs, mais aussi *« un sous-ensemble comprenant également les coordonnées et les détails de la commande tels que le prénom et le nom, l'adresse postale, l'adresse e-mail et le numéro de téléphone »*. Ces dernières données concernent 9500 utilisateurs. En réaction, Ledger a prévenu la Cnil puis a fait appel à Orange CyberDefense *« pour évaluer les dommages potentiels de la violation de données »*.

Ledger surveille les places de marché bien connues des hackers afin d'y repérer la vente de ces données, et explique avoir réalisé et planifié la réalisation de plusieurs pentests. Une plainte a en outre été déposée, tandis que les utilisateurs affectés ont été notifiés.

Phishing **LinkedIn**

Le laboratoire de recherche de Zscaler a découvert dans le courant du mois d'août un schéma d'attaque. Ce labo dénommé ThreadLabZ a constaté un fort trafic ayant pour origine un site malicieux utilisant LinkedIn pour bâtir un schéma d'ingénierie sociale afin de voler des identifiants d'utilisateurs et de placer des codes malicieux sur leurs publications. Les attaquants utilisaient un site légitime chez un hébergeur connu, Yola, pour stocker leur contenu malveillant. Les codes malveillants semblent en relation avec le malware Agent Tesla et un code encore inconnu et pas encore vu en action. Le but semble être le vol d'informations et leur exfiltration via SMTP.

L'appât premier consistait en une page reprenant le logo de LinkedIn qui prétendait proposer des emplois dans toutes les régions du monde pour une compagnie appelée « Jobfinders 3ee ». Un lien invitait à télécharger un fichier ZIP qui contenait les binaires .Net infectés.

Une deuxième étape, sous la forme d'une page LinkedIn, demandait encore plus d'informations personnelles comme le numéro de téléphone et le pays.

L'attaque se déroule ainsi en plusieurs phases et vise spécifiquement des utilisateurs LinkedIn. L'exfiltration des données se réalisait sur des adresses mails spécifiques comme « linkedin.job » ou « linkedin.office » qui semblent avoir été créées spécifiquement pour cette attaque selon les chercheurs du laboratoire.

Comment la région Grand Est a maîtrisé sa plus grande cyberattaque

En février dernier, en plein premier tour des municipales, le SI de la région Grand Est était paralysé par le ransomware Dridex. Pendant plus d'une semaine, environ 2 000 agents n'avaient plus accès à leurs outils numériques. Une attaque sans précédent pour ce type d'administration locale, mais plutôt bien maîtrisée par les équipes en place. Retour sur une gestion de crise « exemplaire » qui pourrait devenir un cas d'école.

« *Toutes les mesures ont été prises pour gérer cette attaque qui peut encore entraîner quelques retards dans les réponses que nous apportons* ». C'est par ce tweet que Jean Rottner, Président de la région Grand Est, confirmait le 20 février dernier la cyberattaque dont était victime son administration. Un « piratage » d'abord évoqué par la presse locale, dont le quotidien L'Union. « *Mails et logiciels en rade, réseau wifi et internet inaccessibles… Tous les ordinateurs des agents et des élus de la région Grand Est sont quasiment inutilisables depuis vendredi* », indiquait ainsi le journal rémois dans son édition du 19 février. « *De Strasbourg à Châlons-en-Champagne, il n'est plus possible de travailler normalement* », confiait un observateur au quotidien. « *Certains agents ou élus reçoivent encore des messages, d'autres n'y ont plus accès* », précisait pour sa part une élue. Un agent confiait qu'il n'était « *plus possible pour les collègues de badger à leur arrivée au travail car le programme relié aux badgeuses a été atteint* ».

La cyberattaque de la région Grand Est est notable à plus d'un point. Tout d'abord, elle est une des rares affectant une région, soit la plus large administration territoriale française. Et pas n'importe laquelle : la région Grand Est, fusion des anciennes régions Alsace, Champagne-Ardenne et Lorraine, à la sixième place hexagonale en termes de population (5,5 millions d'habitants). Ses services administratifs comptent environ 7 500 agents dont 2 000 au siège qui utilisent un poste de travail informatique quotidiennement. La « surface d'attaque » était donc relativement large.

Autre point notable : l'incident est survenu dans un contexte particulier, celui du premier tour des élections municipales de février 2020. « *Il fallait communiquer rapidement afin d'éviter des communications divergentes* », indique Nicolas Brossard, consultant chez Advens, société de sécurité qui a accompagné la région Grand Est dans la gestion de crise et la remédiation.

Élément de timing plus avantageux pour la collectivité : cette période correspondait aussi au début des vacances scolaires. « *Cela en a considérablement réduit l'impact. Des agents en congés sont revenus une semaine plus tard et ont pu reprendre leur travail sans aucun problème* », indique Pierre Gundelwein, DSI de la région Grand Est. « *L'attaque est également survenue une veille de week-end, dans la nuit du 13 au 14 février, vers minuit. Cela a aussi réduit les conséquences, puisque pendant deux jours, peu de personnes travaillaient* ».

Dernière spécificité de cette cyberattaque : sa gestion par la région Grand Est serait « *exemplaire* », estime Advens. « *Tous les bons réflexes ont été pris, tant sur le plan de la communication que de la technique. Si l'attaque n'a pas été déjouée, elle a été maîtrisée et son impact considérablement réduit. Cela ne se passe pas toujours comme ça !* », souligne Nicolas Brossard.

80 serveurs bloqués en une nuit

Le point d'entrée de l'attaque reste flou. « *Nous suspectons l'arrivée d'un e-mail comportant une pièce jointe zippée vérolée. Mais nous n'écartons pas non plus une faille dans l'infrastructure Citrix, utilisée par des clients légers* », indique Pierre Gundelwein.

Si le "patient zéro" n'a donc pas été clairement identifié, l'arme des cybercriminels a en revanche été rapidement reconnue : il s'agissait du malware Dridex, utilisé le plus souvent pour le vol d'informations d'identification bancaires (lire encadré). « *Après avoir infecté plusieurs sessions de travail Citrix, le malware est remonté jusqu'à l'annuaire AD (Active Directory) en quelques heures* », indique Julien Vallée, manager au sein du Computer Security Incident Response Team (CSIRT) d'Advens. Une fois dans l'annuaire, le code malveillant a cryptolocké les services d'authentifications et les accès aux différentes applications, dont la messagerie et les services dans le cloud. Il a ensuite poursuivi sa propagation sur le SI. Le 14 février, à 8 heures du matin, les 80 serveurs Windows de la collectivité étaient paralysés. « *Nous disposons également de serveurs sous Linux qui ont échappé à l'attaque. Ils hébergent la plupart de nos applications métiers, notamment pour les RH, les finances ou les fonctions administratives. Le logiciel libre est un avantage dans ce type de situation* », indique Pierre Gundelwein. En 2019, la région Grand Est a ainsi décroché le niveau 4, sur une échelle de 5, du label Territoire Numérique Libre de l'Adulact (Association des Développeurs et Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales).

Surtout que le niveau de sécurité du SI de la région Grand Est était dans la moyenne, sans être excessivement élevé. Selon la DSI, il était simplement « correct ». Qu'est-ce qui a fait la différence ? « *La réactivité de la DSI et la bonne coordination des équipes ont été déterminantes* », poursuit Advens. « *Nous avons également profité d'un avantage technique : la présence d'outils d'accès à distance au SI. Cela a grandement facilité et accéléré la remédiation car nous n'avions pas besoin d'envoyer des équipes sur le terrain. Tout a été réalisé à distance* ».

> **« *A priori, nous n'avons eu aucun vol de données à déplorer, mais nous restons prudents.* »**
>
> Pierre Gundelwein,
> DSI de la région Grand Est.

Si les applications métiers ont donc été épargnées, l'accès à la messagerie et à la plupart des outils bureautiques, dont Office 365, était en revanche impossible. Les données hébergées sur les serveurs de fichiers étaient également inaccessibles.

Dans la journée du 14, la région Grand Est prévient les autorités, dont l'ANSSI ainsi que la police judiciaire. Pierre Gundelwein présente également la situation au président du conseil régional et au directeur général des services. Entre-temps, une demande de rançon est reçue par la région Grand Est (le montant n'est pas public). Par principe, la région refuse de payer et prépare sa riposte. La DSI contacte alors la société Advens. « *Nous avions réalisé plusieurs prestations pour la région Grand Est. Nous avions donc déjà une relative connaissance de leur SI* », explique Julien Vallée. Une équipe de 8 personnes est mobilisée à la DSI ainsi que cinq du côté d'Advens. La première opération consiste à faire un point sur la situation, avec un inventaire complet de l'architecture réseau, des outils de sécurité et aussi des moyens humains. Étape suivante : identifier le type d'attaque. « *Nous avons collecté tous les logs des solutions de sécurité, dont les antivirus et les VPN* », poursuit Julien Vallée. Les suspicions vont rapidement porter sur Dridex dont le mode de propagation est reconnaissable, en ciblant d'abord l'AD.

Par mesure de précaution, dès le 14, l'ensemble du SI est « débranché », l'accès aux différents services est bloqué tout comme le partage réseau. L'écriture via le protocole SMB (Server Message Block) est également coupée. « *Cela nous a permis d'endiguer la propagation du code malveillant* », indique-t-on à la DSI. L'ensemble des mots de passe administrateurs sont également changés en urgence, car l'une des actions de Dridex est de collecter les mots de passe dans l'annuaire.

Une première tentative d'attaque le 12 février

Le lendemain, toute l'attention se porte sur les récentes sauvegardes du SI, dont la dernière date du jeudi soir, quelques heures avant l'attaque. « *Il faut vérifier ces sauvegardes pour éviter qu'elles ne soient elles-mêmes compromises. Ce n'est donc pas forcément la toute dernière qui est utilisée pour la restauration* », indique-t-on chez Advens.

Parallèlement, l'analyse des logs de sécurité se poursuit et révèle une première activité de Dridex datant du 12 février à midi. Une autre attaque est également décelée à 13 heures, le même jour, mais exploitant un autre logiciel malveillant : Cobalt Strike. « *Peut-être que l'attaque Dridex n'était qu'un écran de fumée, pour faire diversion, et que la réelle attaque était celle via Cobalt Strike. C'est un scénario possible* », poursuit-on chez Advens.

Au vu de ce premier historique d'attaques, la DSI et Advens décident d'utiliser une sauvegarde antérieure au 12 février, celle du 11 février pour les serveurs applicatifs. Elle sera progressivement déployée sur le SI pendant plusieurs jours. « *Nous avons commencé par restaurer l'AD et le contrôleur de domaine* », indique Pierre Gundelwein. Le 17 février, la messagerie est de nouveau accessible tout comme l'application "Teams" d'Office 365. Le même jour, un nouvel outil de sécurité est déployé : l'EDR (Endpoint Detection

and Response) de l'éditeur Cybereason. « *Un EDR exploite classiquement une base virale et de l'analyse comportementale, mais y ajoute de l'intelligence artificielle permettant d'identifier tous les usages anormaux des machines connectées au SI* », résume Julien Vallée. Grâce à cet EDR, Advens analyse les exécutions suspicieuses pour « *remonter le fil d'Ariane des infections* » et isoler les machines potentiellement infectées. Le 17 février, un renforcement des règles des firewalls est également réalisé.

Pas de vol de données

Entre les mesures bloquant la propagation du virus et celles visant à restaurer les données, les services sont progressivement rouverts le 20 février. Environ cinq jours plus tard, le SI retrouve son fonctionnement normal. « *Grâce à l'EDR nous avons pu suivre la disparition progressive des souches virales Dridex avant de rouvrir le SI* », indique Advens.

Quel aura été l'impact de cette attaque ? « *A priori, nous n'avons eu aucun vol de données à déplorer, mais nous restons prudents* », souligne Pierre Gundelwein. Par mesure conservatoire, il a demandé à tous les utilisateurs de changer leurs mots de passe à chaque réouverture de services. La principale conséquence de l'attaque est donc le blocage du SI, entre le 14 et le 20 février, qui a considérablement compliqué le travail des 2 000 agents du siège, mais aussi de 169 élus et des 180 membres du Ceser, le conseil économique, social et environnemental régional. « *Cela s'est traduit par des retards dans certains traitements de dossiers, par exemple des demandes d'aides et de subventions. Certaines instances n'ont également pas pu se tenir. Elles ont donc été reportées* », indique la DSI.

Suite à l'incident, divers renforcements de la sécurité du SI ont été engagés. Tout d'abord, l'EDR Cybereason a remplacé progressivement les antivirus, trop hétérogènes. Cet EDR est aujourd'hui opéré et supervisé en permanence par Advens afin de réagir au plus vite en cas d'autre incident. Les firewalls ont également été re-paramétrés et l'infrastructure Citrix mise à jour. Enfin, la sécurité de l'AD a été renforcée.

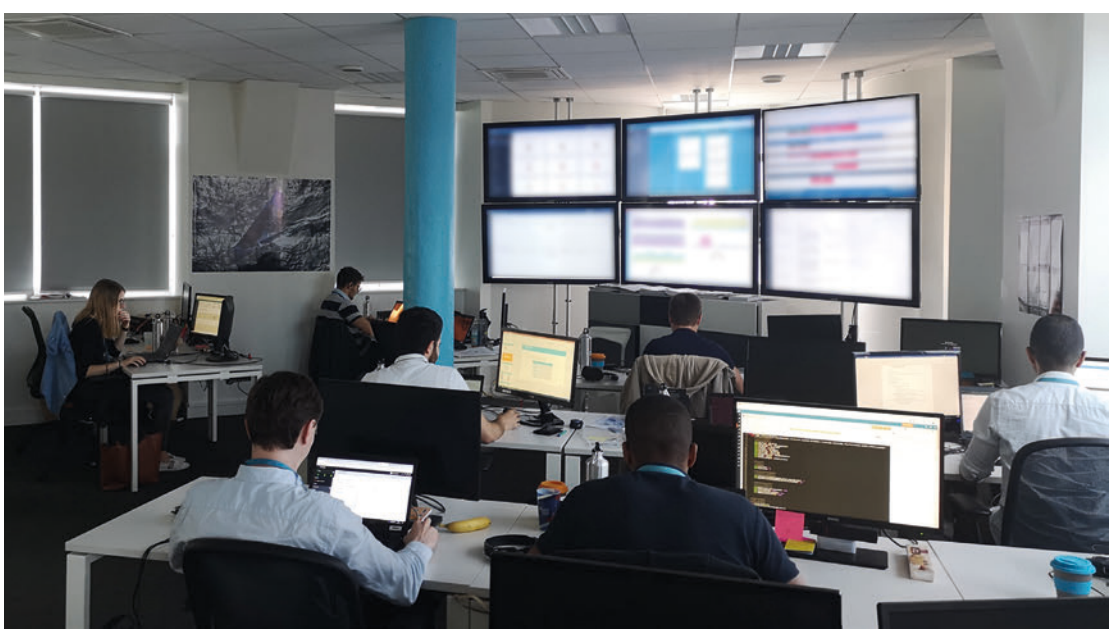
Dernière étape en date : la région Grand Est a porté plainte auprès de la police judiciaire début juin. Un dépôt qui n'a pu être réalisé précédemment à cause du confinement lié à l'épidémie de Covid-19. L'enquête révélera peut-être l'identité des attaquants, qui reste pour l'instant inconnue. « *Dridex est utilisé pour tellement de groupes de cybercriminels, qu'il est difficile de savoir auquel nous avons eu affaire* », indique la DSI.

Une communication de crise « réaliste »

Parallèlement à la gestion technique de l'incident, la région Grand Est a dû communiquer très rapidement sur la cyberattaque, relatée par la presse locale dès le 19 février. « *Un des piliers d'une bonne gestion de crise est la communication* », souligne Pierre Gundelwein. « *Une cellule de crise a été mise en place dès le dimanche 16 février. Elle a produit un état quotidien de la situation, transmis aux différentes directions. Une page web spécifique a également été publiée sur notre intranet pour tenir informés les agents. Nous avons misé sur une communication la plus transparente possible* ». Résultat : « *Nous n'avons pas eu de frictions à déplorer. Les agents étaient plutôt compréhensifs.* »

Jean Rottner s'est exprimé sur le sujet lors de la commission permanente de l'assemblée du 14 février, le jour même de l'attaque. Et en externe, il a donc évoqué l'incident sur Twitter le 20 février. « *Nous nous sommes positionnés en victime, ce qui était le cas. Nous avons expliqué que nous avions été agressés et que nous faisions le nécessaire pour endiguer l'attaque et rétablir les services dans les meilleurs délais* », précise Pierre Gundelwein qui estime avoir bénéficié d'un fort soutien de sa direction générale.

« *La région Grand Est a tenu un discours réaliste, en restant sur des éléments factuels, que ce soit en interne comme en externe, ce qui était la bonne option* », précise pour sa part Nicolas Brossard d'Advens. « *Cette communication a permis d'éviter des frictions en interne et une exploitation par des opposants politiques, qui n'était pas impossible en période électorale. Pour les équipes opérationnelles, cela a permis de réduire la pression médiatique, qui peut freiner nos interventions. Nous avons pu travailler dans de saines conditions* ».



Le SOC d'Advens, qui compte plus d'une cinquantaine d'experts, a participé au pilotage à distance de la crise et à sa remédiation.

Dridex cible la plateforme Windows

Apparu en 2014, Dridex (alias Bugat ou Cridex) est un cheval de Troie initialement utilisé pour le vol d'informations d'identification bancaires. Son usage a ensuite été décliné dans des domaines tels que l'espionnage industriel et, plus rarement, l'attaque de structures publiques. Selon un récent rapport de la société de sécurité Check Point, ce malware a déjà contaminé 3 % des entreprises mondiales. « *Dridex cible la plateforme Windows et est diffusé via des campagnes de spam (...) Il contacte un serveur distant, envoie des informations sur le système infecté et peut également télécharger et exécuter des modules supplémentaires pour le contrôle à distance* », précise Check Point qui l'a hissé, en avril dernier, à la troisième place de son classement des malwares les plus utilisés au monde (derrière XMRig et Jsecoin).

« *Sa fonctionnalité première est celle d'un stealer, c'est-à-dire le vol de codes d'accès de banque en ligne, afin que les attaquants puissent réaliser des virements frauduleux depuis des comptes en banque compromis* », observe pour sa part l'ANSSI, dans un rapport paru en mai dernier. Son usage pour des demandes de rançon est permis par sa grande modularité. Il intègre en effet plusieurs éléments, qui s'accumulent au fil de ses nombreuses mises à jour, dont un loader, un keylogger, un spammer et un dérivé du code malveillant Pony pour le vol de codes d'accès. « *Dridex est aussi susceptible de télécharger les rançongiciels BitPaymer et DoppelPaymer en tant que seconde charge utile* », précise l'ANSSI.

Les principaux développeurs de Dridex seraient des membres d'Evil Corp, un groupe cybercriminel russophone, actif depuis 2014. Il cible principalement le secteur de la finance, de la distribution et des institutions gouvernementales et est à l'origine de la récente attaque du CHU de Rouen (lire CyberRisques n°1, p. 6).

Les collectivités territoriales : des proies faciles ?

Cette cyberattaque n'est pas la première ayant touché la région Grand Est. « *En analysant les logs de sécurité, nous avons trouvé des traces d'attaques survenues trois à six mois avant celle de Dridex, notamment par injection SQL. Mais rien de comparable avec celle de février 2020* », confie Julien Vallée. En 2015, la région Lorraine avait également subi une attaque par déni de service. Il s'agissait alors d'une opération menée par les Anonymous, en lien avec le site d'enfouissement de déchets nucléaires de Bure (Meuse). « *Il y a eu une erreur sur la personne. Les Anonymous ont attaqué la Lorraine soi-disant pour sa prise de position en faveur de ce site d'enfouissement, ce qui était faux* », se souvient Pierre Gundelwein.

Au-delà de la région Grand Est, les attaques ciblant les collectivités territoriales se multiplient en France. Une des dernières en date a pris pour cible la métropole Aix-Marseille-Provence ainsi que la ville de Marseille. Survenue en mars dernier, cette attaque par rançongiciel a duré plus d'un mois (nous reviendrons sur cet incident dans un prochain numéro).

Les petites collectivités ne sont pas épargnées. Au début du confinement, les attaques par ransomware visant des communes de taille intermédiaire ont globalement augmenté, a constaté la plateforme nationale cybermalveillance.gouv.fr. « *Bon nombre de collectivités ont mis en place le télétravail dans l'urgence, ce qui a augmenté le risque de failles dans la sécurité du SI* », explique Jérome Notin, directeur général de cette émanation de l'ANSSI qui s'adresse aux collectivités et aux entreprises. « *Les collectivités territoriales ne sont clairement pas à l'abri des cyberattaques et elles peuvent même représenter des proies faciles, car elles n'ont pas toujours les moyens de se protéger* », poursuit le responsable. « *Pour autant, il reste difficile d'évaluer si la plupart de ces attaques sont ciblées. Il semble plutôt que les cybercriminels fassent de la "pêche au chalut", donc de manière très large et sans cibles précises. Dans les mailles du filet, il y a parfois une collectivité, sur laquelle ils lancent ensuite une attaque, sans savoir réellement de qui il s'agit* ».

Un avis partagé par Nicolas Brossard d'Advens. « *Oui, la "pêche au chalut" semble être la pratique la plus courante. Dans le cas de la région Grand Est, rien ne prouve que l'attaquant connaissait, a priori, cette administration. Il ne savait probablement pas qu'il s'attaquait à une grande administration française* ».

Selon Jérôme Notin, un des indicateurs démontrant la prédominance d'attaques non ciblées est le montant des rançons, qui est en général déconnecté de la réalité. C'était le cas de la région Grand Est, dont la rançon était donc « incohérente », comme l'a indiqué la DSI. « *Il y a d'autres exemples similaires. L'année dernière, dans le sud de la France, une attaque a touché une PME et une collectivité territoriale, le même week-end. L'entreprise a reçu une demande de rançon de 130 000 euros alors que la collectivité s'est vue réclamer : 5 000 euros !* »

Une culture de la cybersécurité à développer

Cette multiplication d'attaques de collectivités n'est pas sans poser problème. Car l'impact peut être potentiellement très large, du fait des nombreuses responsabilités des administrations locales françaises. « *Une collectivité gère des services clés de l'administration publique couvrant le domaine économique, la santé, les transports... et bien entendu les services aux citoyens. Bloquer les outils numériques servant à assurer ces missions peut avoir un impact majeur sur un territoire. Un impact souvent bien plus grave que l'attaque d'une entreprise* », souligne Jérôme Notin.

Il rappelle donc l'importance de développer la culture de la cybersécurité au sein des administrations locales. Une culture qui ne serait pas si répandue. Dans cette optique, Cybermalveillance.gouv.fr propose un kit gratuit de sensibilisation, pouvant être utilisé par des collectivités. Il rappelle les fondamentaux de la cybersécurité et les bonnes pratiques que doivent adopter les agents. La ville de Vannes a par exemple diffusé massivement ce guide en 2019. « *La sensibilisation des agents est des un principaux leviers du renforcement de la cybersécruité dans les collectivités. Bien entendu, nous recommandons également la mise en place de solutions de sécurité, certifiées par l'ANSSI. Enfin, il faut développer les échanges d'informations entre les DSI des collectivités, pour que les expériences des uns puissent profiter aux autres* », conclut-il.

Christophe Guillemin

Quelles conséquences pour les entreprises après l'annulation du Privacy Shield ?

Par **Isabelle Cantero** et **Eric A. Caprioli**,
avocats associés de la société d'avocats Caprioli & Associés

Dans l'attente de nouvelles négociations entre la Commission européenne et les autorités américaines, les transferts de données à caractère personnel vers les entreprises US relevant du Privacy Shield (Google, AWS, Microsoft, Facebook,...) sont suspendus voire désormais interdits selon le Comité Européen à la Protection des données (CEPD).

La protection des données personnelles a pris une importance inégalée depuis que le RGPD est entré en application le 25 avril 2018. Nonobstant la répression pénale, les sanctions pécuniaires en cas de manquement avéré aux obligations prescrites sont désormais substantielles. Dans le cadre de ce règlement, le transfert de données personnelles en dehors de l'UE a été consolidé. Néanmoins, on pouvait s'interroger sur la validité des instruments mis en place antérieurement par la Commission européenne (décision d'adéquation, clauses contractuelles-types). Cela est d'autant plus important que de nombreux services numériques (ex : hébergement et SaaS dans le cloud) émanent d'entreprises américaines et sont utilisés par de très nombreux organismes européens. C'est dans ce contexte que la Cour de Justice de l'Union Européenne (CJUE) a rendu son arrêt du 16 juillet 2020.

Cadre juridique du transfert des données hors de l'UE

Les décisions dites d'adéquation de la Commission européenne permettent de transférer librement des données personnelles à partir du territoire de l'UE vers les pays tiers suivants : Andorre, Argentine, Canada (entreprises commerciales), Iles Féroé, Guernesey, Ile de Man, Japon, Jersey, Nouvelle Zélande, Suisse et Uruguay. Une telle décision d'adéquation résulte du constat selon lequel le pays destinataire des données présente un niveau de protection équivalent à celui de l'UE. Spécifiquement, la décision d'adéquation entre les USA et l'UE, à savoir le Safe Harbor (ou sphère de sécurité) conclu en juillet 2000 (décision 2000/520), était de nature sectorielle et ne visait que certaines entreprises américaines relevant de la Federal Trade Commission. Une décision de la CJUE a invalidé le Safe Harbor le 6 octobre 2015 (affaire Schrems c/. FaceBooks). Dans la foulée de cette invalidation, les négociations avec les USA ont repris pour aboutir à l'adoption d'une nouvelle décision d'adéquation sectorielle le 12 juillet 2016 portant sur le Privacy Shield (bouclier de protection).
Faute de décision d'adéquation, les exportateurs européens de données à caractère personnel, c'est-à-dire les responsables du traitement ou les sous-traitants, doivent adopter des outils permettant d'apporter des garanties appropriées, à savoir les clauses contractuelles types de la Commission européenne, les règles d'entreprise contraignantes (Binding Corporate Rules) ou encore l'adhésion à un code de conduite. En pareille hypothèse, l'adoption de ces outils ne nécessite pas non plus d'autorisation préalable de la part de l'autorité de contrôle nationale (en France la CNIL).

Comment répondre à la problématique suite à l'invalidation ?

Afin de pouvoir continuer à transférer les données de ses utilisateurs européens vers Facebook Inc, après l'invalidation du Safe Harbor, Facebook Ireland a eu recours aux clauses contractuelles types (CCT) de la Commission européenne (Décision 2010/87/UE de la Commission du 5 février 2010, modifée par la Décision d'exécution (UE) 2016/2297 du 16 décembre 2016). Or, ce qui est en cause, ce sont les programmes de surveillance de masse (PRISM et UPSTREAM) ainsi que les règlementations extraterritoriales américaines notamment le Foreign Intelligence Surveillance Act « FISA » et le Décret présidentiel EO-12333, ou encore le Patriot Act. Ces textes permettent à certaines agences gouvernementales fédérales (FBI, NSA, CIA, ATF, FDA) d'accéder aux données personnelles qui ont été transférées vers des opérateurs américains (métadonnées et contenus des communications), que ces derniers soient aux USA ou dans l'UE. Sont ainsi invoquées les exigences relatives à la sécurité nationale. Or, on était en droit de se demander si la limitation du pouvoir conféré aux autorités publiques américaines permettait de garantir le respect d'un niveau de protection des données personnelles transférées équivalent à celui de l'Union européenne.

Que dit la décision de la CJUE du 16 juillet 2020 ?

Le même plaignant que pour le Safe Harbor, M. Schrems, demandait à la CJUE d'interdire à Facebook Irlande de procéder au transfert de ses données personnelles vers les États-Unis. Pour ce faire, il arguait que le droit des USA n'apportait pas les garanties suffisantes de protection des données stockées aux USA en raison des activités de surveillance des agences gouvernementales qui y sont pratiquées.
Sur le plan des fondements juridiques, la décision de la CJUE s'appuie sur le RGPD (art. 45) et sur la Charte des droits fondamentaux de l'Union européenne (art. 7, 8, 47 et 52). Pour ce faire, le raisonnement procède en deux temps : validation conditionnelle des CCT et invalidation du Privacy Shield.
Premièrement, la **Cour de justice a jugé que la décision de la Commission européenne relative aux clauses contractuelles types pour le transfert de données personnelles vers des sous-traitants établis dans des pays tiers était valide.** Mais, il reste que cette validation est conditionnelle dans la mesure où la Cour impose au responsable du traitement ou au sous-traitant établis dans l'UE de **prendre des mesures supplémentaires dans le cas où la réglementation du pays de l'importateur des données comporterait des mesures contraires aux clauses types.** A défaut, le responsable du traitement ou le sous-traitant, et, à titre subsidiaire, l'autorité de contrôle compétente ***« sont tenus de suspendre ou de mettre fin au transfert de données vers le pays tiers concerné »***.
Deuxièmement, **la CJUE a invalidé la décision d'adéquation portant sur le Privacy Shield**, dans la mesure où elle a estimé qu'elle était incompatible avec les exigences d'adéquation fixées par le RGPD. Tout d'abord, la Cour juge que les programmes de surveillance massive menés par les autorités américaines apportaient des **limitations de la protection des données personnelles transférées depuis l'UE et qu'elles étaient non conformes aux exigences minimales attachées au principe de proportionnalité.** Par ailleurs, la CJUE estime que **cette règlementation ne confère pas non plus aux personnes concernées de droits opposables aux autorités américaines devant les tribunaux.** Enfin, la Cour remet en cause **le mécanisme de médiation prévu par le Privacy Shield** étant donné que cet accord **ne permet pas de garantir aux non américains le droit à un recours effectif à accéder à un tribunal impartial**.

La position du Comité Européen à la Protection des données (CEPD)

Dans la foulée de la décision de la CJUE, le CEPD donne sa position sur les principales conséquences de cet arrêt dans ses FAQ publiées le 23 juillet 2020.

1) **Les transferts de données vers les entreprises américaines relevant du Privacy Shield** (Google, AWS, Microsoft, FaceBook,...) **sont interdits.** Aucune période de grâce, n'est accordée suite à l'arrêt de la Cour.

2) S'agissant des **clauses contractuelles types**, la portée de l'arrêt de la CJUE va au-delà des transferts vers les USA ; il incombe à l'exportateur et à l'importateur de données d'évaluer si le niveau de protection du pays tiers concerné est substantiellement équivalent à celui de l'UE afin de déterminer si les garanties appropriées pourront être respectées en pratique.

3) Toutes les garanties appropriées prévues par le RGPD sont impactées en ce compris les BCR, même si ces dernières ont été validées par le CEPD...

4) Pour les USA comme pour tout autre pays tiers dont la règlementation n'assure pas un niveau de protection adéquat, les **transferts de données doivent être suspendus ou définitivement arrêtés si des mesures de protection complémentaires n'ont pas été adoptées ou si les dérogations prévues par l'article 49 du RGPD ne sont pas applicables** (consentement explicite, spécifique et informé des personnes concernées).
Les mesures complémentaires dans l'hypothèse où les CCT ou les BCR n'assureraient pas un niveau de garantie suffisant peuvent se traduire en termes juridiques, techniques (ex : chiffrement des données) ou organisationnels pour les transferts de données vers des pays tiers. L'évaluation et la fourniture de mesures de protection complémentaires incombent exclusivement à l'exportateur de données et à l'importateur de données.

5) **Dans l'hypothèse où il est décidé de maintenir le transfert** vers un pays tiers (ex : Chine, Inde) dont la règlementation n'assure pas un niveau de protection adéquat (sans mesures complémentaires ou dérogation applicable), **le responsable du traitement doit en informer l'autorité de contrôle ;** étant précisé que cette dernière pourra interdire ledit transfert !

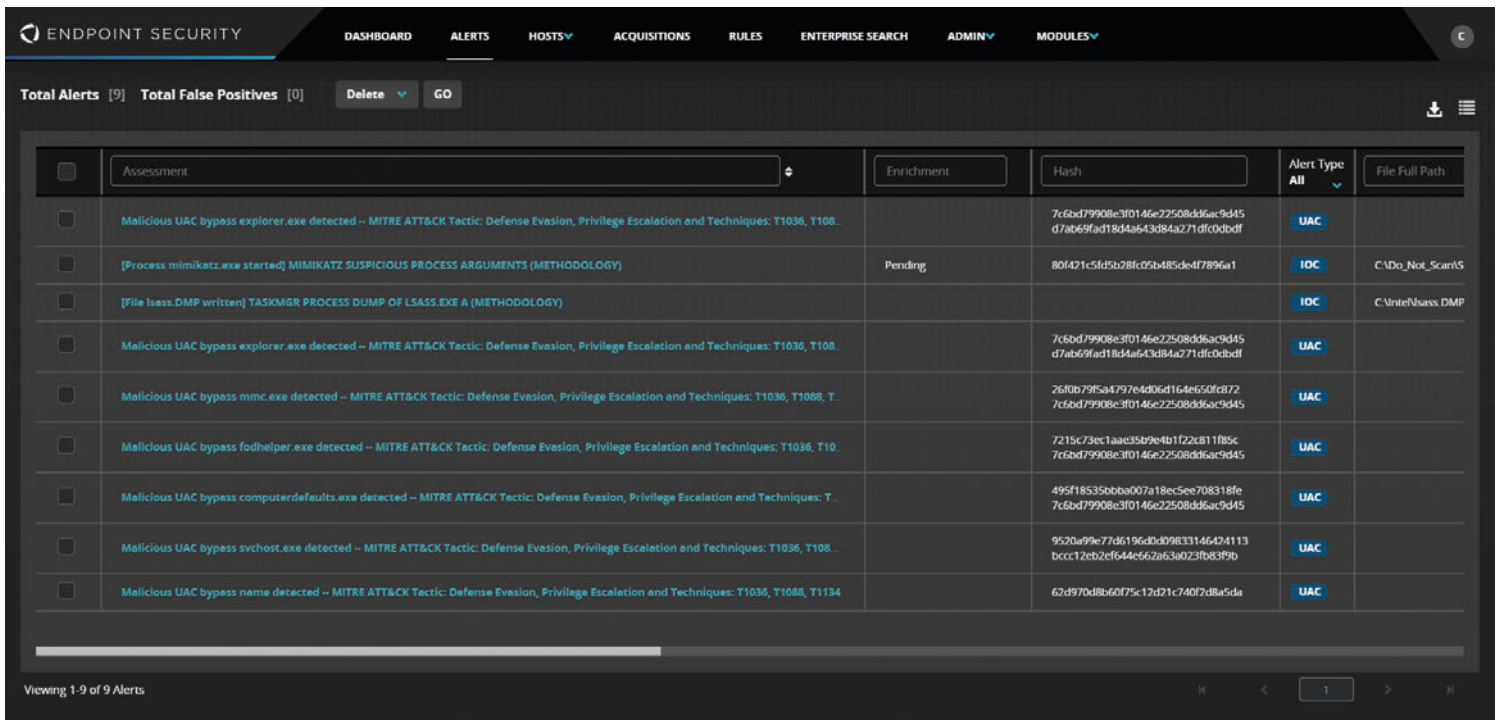
6) Pour les transferts de données résultant de sous-traitance en chaîne, **le responsable du traitement doit négocier un avenant ou une clause supplémentaire au contrat de sous-traitance afin d'interdire les transferts.**

7) **Il est urgent que** les diverses autorités de contrôle se concertent sur le sujet.
En fin de compte, l'Accountability prend un virage important en faisant peser sur les exportateurs de données une bien lourde responsabilité...
En attendant, la Commission européenne a relancé les négociations avec les autorités américaines en vue d'un nouvel accord, conforme au RGPD afin de lever les irrégularités.
En conséquence de quoi, à date : Wait and see !

Eric A. CAPRIOLI & Isabelle CANTERO
Avocats associés, Caprioli & Associés,
Société d'avocats membre
du **réseau JURISDEFI**

DOSSIER

Quel rôle doit jouer l'EDR pour protéger un parc informatique ?



Les EDR, tout comme les antivirus Next-Gen, sont aujourd'hui devenus synonymes de machine learning sur les machines. Une solution technique relativement légère sur les postes, mais qui permet d'aller au-delà de la détection des malware sur base de signatures.

Détecter toute tentative d'infiltration sur les postes utilisateurs notamment et tuer dans l'œuf toute attaque, c'est la promesse des EDR (Endpoint Detection & Response). L'approche qui s'appuie sur la puissance du cloud et le machine learning est séduisante, mais pose question en termes de fuites de données et de son positionnement par rapport au SOC.

Avec une croissance attendue de 28,8% par an sur la période 2018 à 2025 selon The Insight Partners, le marché des EDR est une mine d'or pour les éditeurs et tous veulent leur part du gâteau. L'EDR est présenté par les éditeurs venus du monde de l'EPP (Endpoint Protection Platform) comme une évolution logique des offres d'antivirus « NextGen » ou comme un composant à part entière d'une infrastructure de cybersécurité pour les gros fournisseurs qui, à l'image de l'acquisition de Carbon Black par VMware en 2019, se sont rués sur cette niche de marché en train d'exploser.

Des solutions majoritairement portées par le Cloud

Comme l'indique son acronyme, toute solution EDR se doit de fournir des solutions de détection, avec des moteurs de détection directement issus du monde de l'EPP avec de l'antivirus à base de signature, des moteurs de Machine Learning et de la reconnaissance comportementale pour générer des alertes dès lors que des process ou des services se mettent subitement à fonctionner de manière anormale. Une majorité de ces solutions mettent en œuvre des ressources cloud pour centraliser les données collectées sur les points afin de faire tourner les modèles qui vont permettre de repérer les attaques en cours ou même les signaux précurseurs d'une attaque en préparation.

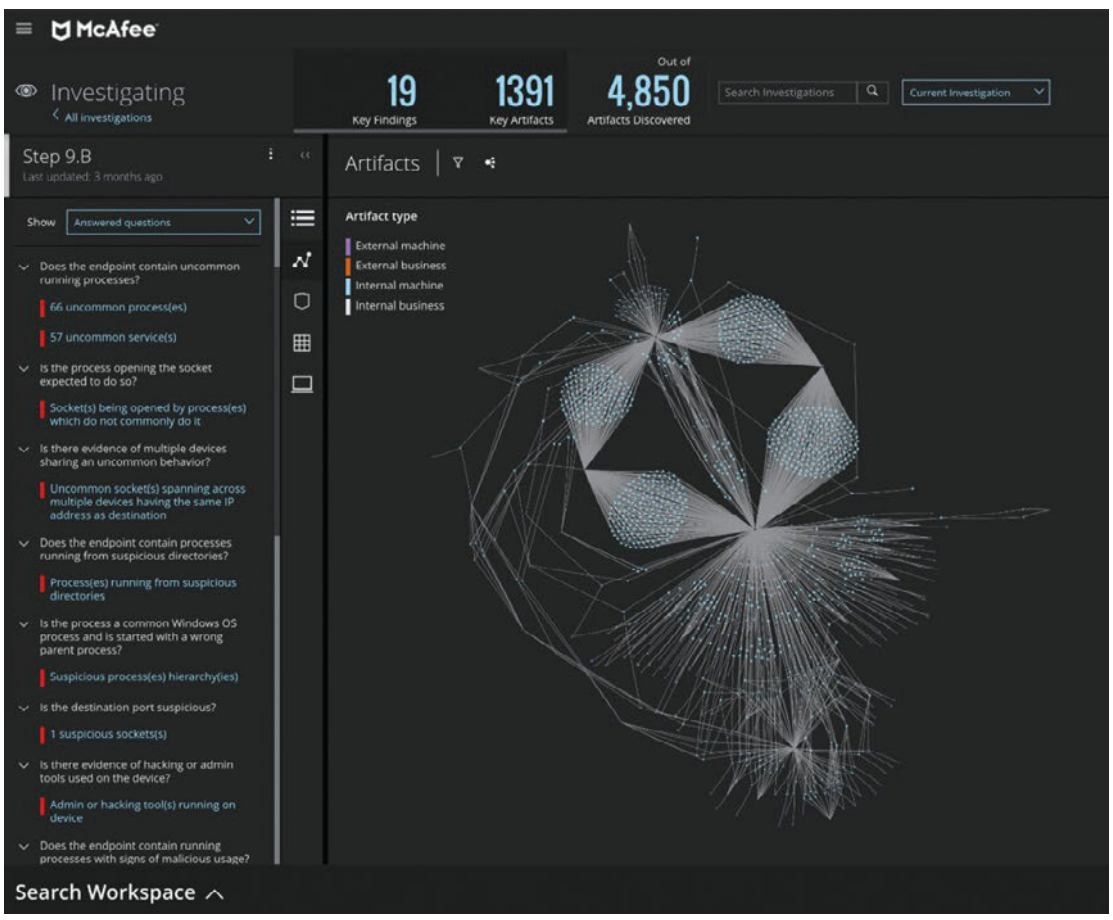
Cette approche mutualisée est ardemment défendue par CrowdStrike, un éditeur créé en 2011 par deux anciens VP de McAfee qui ont souhaité repenser la protection endpoint en partant d'une feuille blanche. Joël Mollo, directeur général Europe du Sud de CrowdStrike souligne : « *Les fondateurs de CrowdStrike sont partis sur une approche 100% cloud, une approche qui permet de mutualiser la surveillance réalisée pour l'ensemble de nos clients. Cela a permis de constituer une communauté dans la gestion des menaces, ce que nous appelons le Threat Graph. Cela représente d'une certaine manière un SOC mondialisé mutualisé et qui permet à toute entreprise qui ne dispose pas de SOC en propre de bénéficier de l'action de notre équipe Overwatch.* »

Pour CrowdStrike, l'autre atout d'une approche cloud est de pouvoir s'appuyer sur un agent logiciel très petit qui peut être déployé sur un parc sans nécessiter le reboot des machines. L'éditeur revendique 20 millions de postes déployés à ce jour.

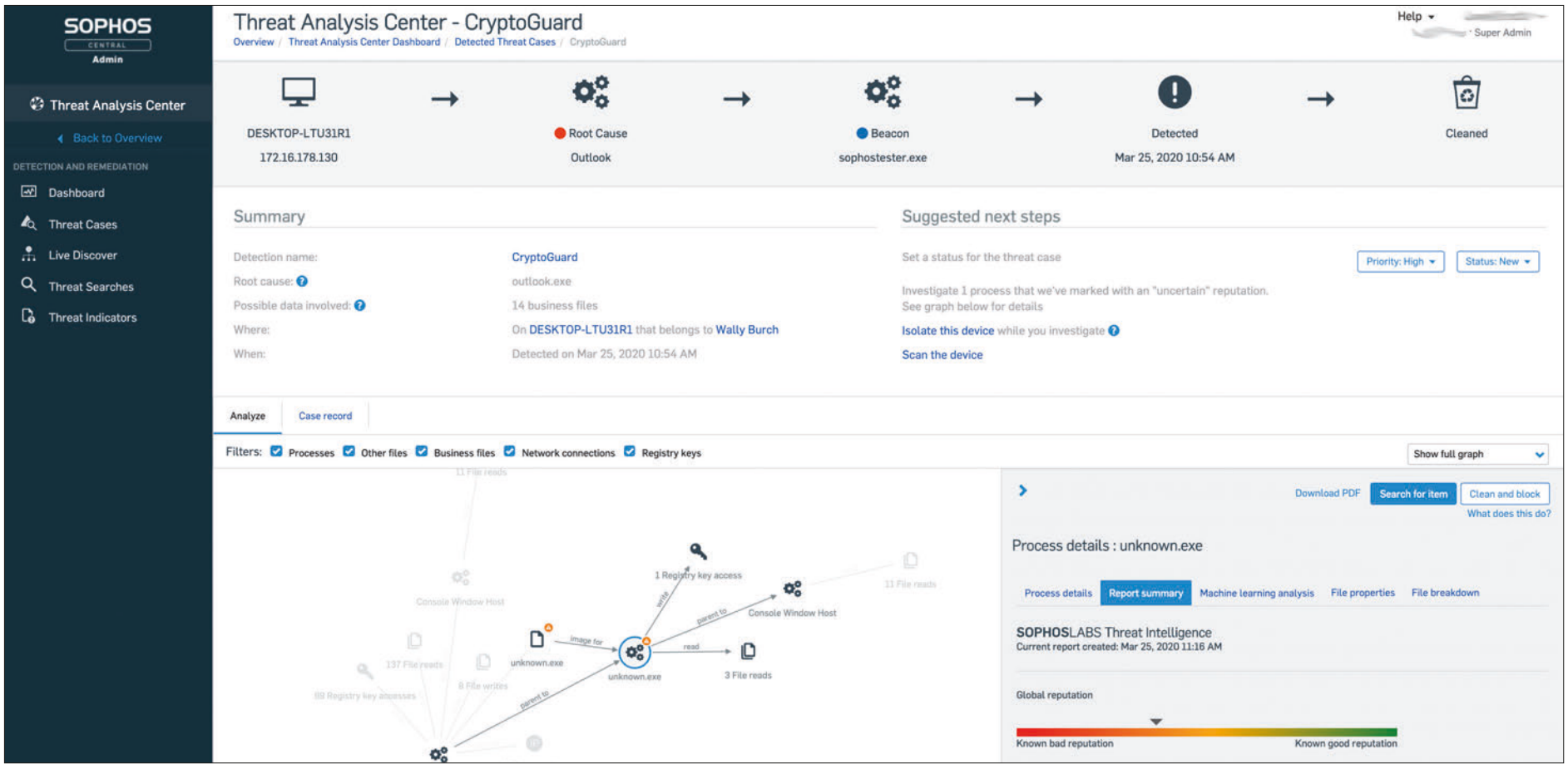
De par ses capacités de stockage et de traitement virtuellement infinies, le cloud se prête particulièrement à la collecte de données de fonctionnement de centaines de milliers de postes et pour faire tourner des modèles de Machine Learning sur ces énormes volumes de données. De facto, de plus en plus d'éditeurs privilégient maintenant une approche « cloud-only ». Ceux-ci assurent à leurs clients que seules des métriques de fonctionnement sont rapatriées sur leurs serveurs cloud, mais dans certains cas, ce type d'assurance ne suffit pas. C'est bien évidemment le cas d'entreprises liées à la défense nationale et de certains ministères. « *Beaucoup de nos concurrents sont de type* « cloud-first » *voire même* « cloud-only », *or notre historique fort avec le monde gouvernemental et défense nous a poussé à proposer notre EDR en mode cloud, en mode on-premise, mais aussi dans un mode totalement déconnecté* » explique David Grout, CTO EMEA de FireEye. « *Notre solution peut ainsi être déployée sur un navire militaire ou pour protéger un site militaire sans que des données ne remontent vers l'éditeur.* » 60% à 70% ont été achetés par des clients finaux de l'éditeur, 15% ont fait le choix des services managés par FireEye et 15% utilisent la solution à l'occasion d'un incident de sécurité, en tant qu'outil de forensic.

« L'EDR est un excellent complément des outils du SOC »

Julien Coulet, co-fondateur d'Excube, pense que « *Les projets et la gestion des SOC sont complexes et les résultats ne sont pas toujours à la hauteur des attentes. Ceci s'explique notamment par une approche très empirique : concentrer une quantité de données souvent colossale que l'on analyse au travers d'algorithmes statiques. En parallèle à cela, on assiste actuellement à l'apparition de sondes intelligentes sur des verticaux d'infrastructures. Par exemple, c'est le cas d'Alsid pour*



C'est la partie sans doute la plus spectaculaire d'un EDR. L'interface d'investigation permet à l'analyste de se livrer à l'autopsie de l'attaque. Elle permet notamment de retrouver de manière interactive quels étaient les signaux faibles de l'attaque qui ont échappé aux briques de sécurité en place.



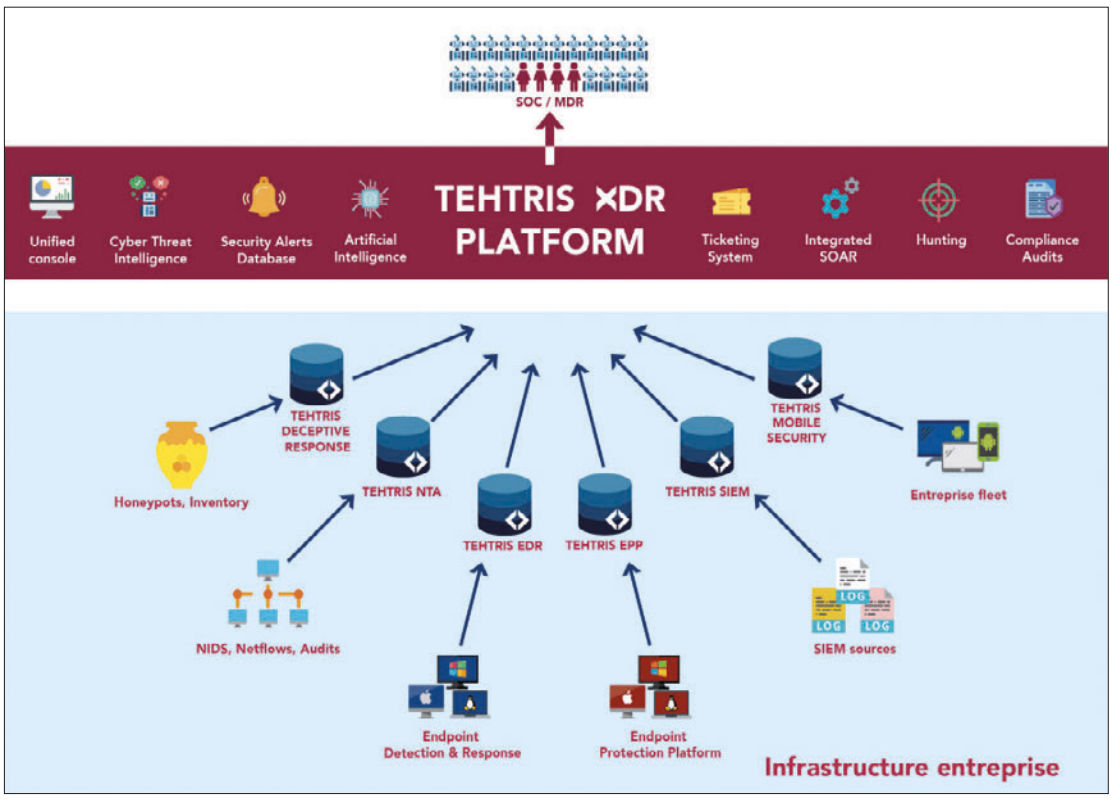
Un EDR est intimement lié à un service de Threat Intelligence afin de détecter puis aider l'analyste dans sa recherche sur un incident de sécurité.

les Active Directory, Vectra pour la partie réseau et des EDR pour la partie postes de travail. Cette approche présente plusieurs avantages, notamment en simplifiant la collecte de données. La collecte du bon niveau de détails des données est toujours problématique pour les SOC, en particulier lorsque le système d'information est complexe et le nombre de postes élevé. L'EDR se déploie au travers des mécanismes de télédistribution et donne ensuite accès à des alertes déjà préqualifiées par l'outil, ce qui simplifie l'implémentation des règles de détection statiques.»

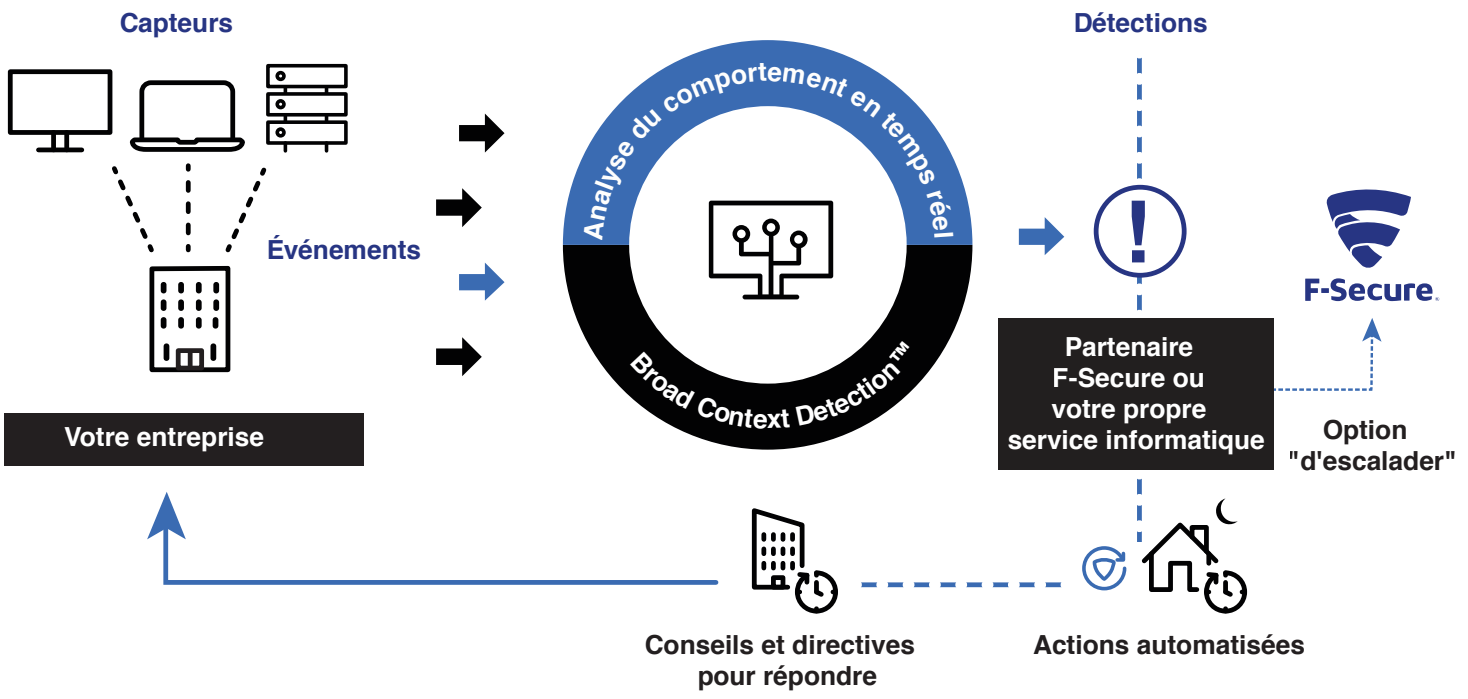
Jusqu'où externaliser la protection des postes clients ?

Ce qui différencie fondamentalement un EDR d'un antivirus «NextGen», c'est bien le "R", c'est-à-dire la Response ou plutôt la Remédiation. Les EDR implémentent des outils qui vont permettre d'une part de repérer très rapidement dans le parc quels sont les postes victimes d'une attaque et lancer des mesures correctives sur l'ensemble de ces machines. Les éditeurs proposent souvent une offre de service de «Threat Hunting» couplée à l'outil, leurs analystes de sécurité venant aider l'entreprise qui fait face à une attaque avérée. Des éditeurs tels que FireEye interviennent auprès des entreprises et parfois des assureurs pour réaliser l'analyse d'attaques qui ont fait des dégâts dans l'entreprise mais ce recours peut aller beaucoup plus loin. Ainsi, un géant mondial du e-commerce a confié à CrowdStrike la protection de 800 000 endpoints. *«Ils ont fait le choix de se centrer sur leur métier et ne souhaitaient pas consacrer des ressources internes sur la sécurisation des endpoints. C'est pour cela qu'ils nous en ont confié la sécurité.»*

Même les acteurs venus du monde de la protection endpoint musclent aujourd'hui le volet service de leur offre qui leur permet une montée en gamme opportune en termes de revenus. Ainsi Sophos a considérablement musclé son offre de service avec l'acquisition de Rook Security en juin 2019. *«Nous avons mis en place une offre MTR (Managed Threat Response) de surveillance des logs générés par nos EDR en 24/7»* explique Bruno Leclerc, directeur des ventes de Sophos France. *«Outre les algorithmes d'IA qui traitent 400 000 menaces / jour, une analyse humaine reste indispensable. Nous avons des labs répartis sur 3 continents afin de travailler sur les logs de nos clients sous contrat. Il ne s'agit pas seulement de faire de l'alerting, mais bien de prendre la main sur les équipements de nos clients pour identifier l'attaquant mais surtout lancer une remédiation pour placer des postes en quarantaine, lancer des scripts pour contrer l'attaque. L'alerting n'est qu'un premier pas, ce qui compte, c'est l'action !»*



A la différence de l'EDR qui n'analyse que les données glanées au niveau des postes clients (endpoints), le XDR corrèle des données issues de multiples sources, dont les données réseau, les logs, etc.



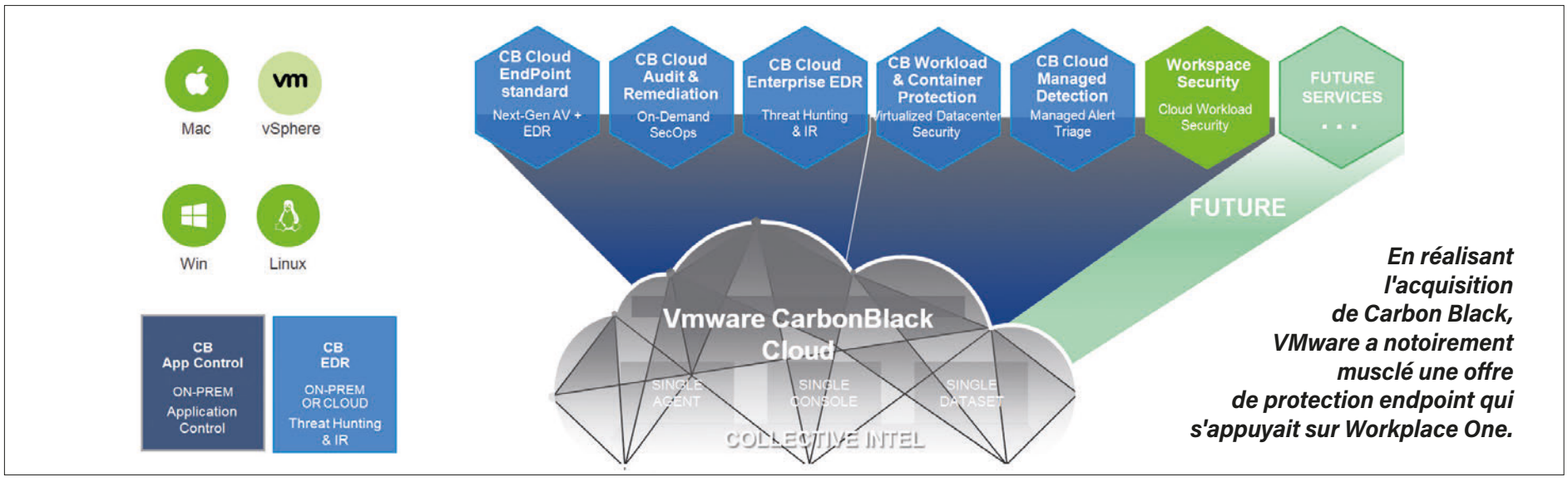
Dans le schéma de fonctionnement de l'EDR F-Secure, les experts en sécurité de l'éditeur ont un SLA de 2 heures pour analyser une menace qui a été «escaladée» auprès de son service de Threat Intelligence.

Autre approche, celle de VMware qui, en mettant la main sur Carbon Black, a rapproché l'EDR de ce dernier à son offre de gestion des postes de travail Workspace One (ex-Airwatch). Ghaleb Zekri, architecte au sein de l'équipe SDDC et expert cybersécurité chez VMware, souligne les interactions entre les deux solutions : « *Des actions de remédiation peuvent être engagées au niveau du client Next-Gen AV, la partie antivirus de la solution afin de casser la chaîne d'attaque, ce que l'on appelle la* « kill chain ». *Carbon Black peut aussi alerter d'autres systèmes notamment Workspace One qui gère notamment l'identification des utilisateurs. Cette notification permet à l'entreprise de réajuster la posture de sécurité de ses utilisateurs et par exemple verrouiller l'accès VPN d'un utilisateur s'il s'avère que celui-ci a ouvert un email suspect.* » De plus, VMware a fusionné sa solution de protection des charges de travail AppDefense avec Carbon Black. « *Plutôt que de chercher les attaques elles-mêmes, l'idée est de se concentrer sur le comportement habituel des applications et générer une alerte en cas de déviation par rapport à ce comportement. Carbon Black est maintenant capable d'exploiter ce scoring comportemental des applications et cela permet à la solution d'avoir une longueur d'avance et prendre une action dès qu'un comportement inattendu est détecté.* »

EDR, le complément naturel du SOC

Cette montée en puissance de l'EDR pose la question de son positionnement vis-à-vis du SOC lui-même. Initialement limités aux seuls endpoints, les outils d'investigation de certains EDR peuvent aussi analyser des données glanées dans le réseau et leur rôle se rapproche des SIEM habituellement mis en oeuvre dans les SOC. « *Ce qui intéresse le plus les grands comptes, c'est l'ouverture de nos API* » souligne ainsi Bruno Leclerc. « *La console de management est en quelque sorte un SIEM intégré. De plus, disposer d'une telle console unifiée dans le cloud représente une importante source d'économie en termes d'administration.* » Pour une entreprise qui ne dispose pas des moyens d'opérer un SOC, le recours à un service managé est une solution intéressante estime Bruno Leclerc : « *Pour le midmarket, la problématique est différente. Bien souvent les PME n'ont pas les ressources humaines en interne pour exploiter les capacités d'un EDR. Une bonne interface graphique ne suffit pas et une offre de service va leur donner accès à des compétences en mode managé.* »
Faut-il voir dans l'EDR le SOC du pauvre ? Sans doute pas, mais l'EDR reste un moyen pour une entreprise ne disposant pas de SOC de commencer à s'outiller et de mettre en place une organisation pour aller vers les concepts du SOC. « *L'EDR peut être présenté à une direction comme une évolution naturelle de l'antivirus, une évolution logique apportant des fonctionnalités additionnelles très différentes* » explique Julien Coulet, co-fondateur d'Excube. De même, certains éditeurs et consultants poussent les entreprises à investir dans des EDR en les présentant comme un remplaçant possible du SOC, une position à laquelle de nombreux acteurs s'opposent, dont Dagobert Levy, vice president South EMEA de Tanium : « *Il ne faut pas tomber dans le travers de considérer l'EDR comme le remplaçant du SOC. Ce n'est pas du tout le cas, l'EDR est un outil qui doit se mettre au service du SOC mais n'a certainement pas vocation à s'y substituer.* »
Pour Palo Alto Networks, l'EDR a clairement un rôle à jouer vis-à-vis du SOC, notamment pour dégrossir le travail de tri des analystes. « *Selon les chiffres de Gartner, un SOC moyen recueille plus de 170 000 alertes par semaine mais les analystes ne sont en capacité d'en traiter que 10% environ* » argumente Eric Antibi, senior manager et directeur technique de Palo Alto Networks. « *Les SOC n'ont pas les capacités humaines à corréler toutes les informations reçues et au-delà de ce chiffre, on se rend compte que lorsqu'une attaque a réussi, on peut retrouver les premiers signaux faibles annonciateurs de l'attaque plusieurs mois avant son exécution.* » L'éditeur estime qu'avec les bons mécanismes de corrélation de données, le nombre d'alertes pourra être réduit et l'équipe SOC sera plus efficace et mieux à même de prévenir les attaques et traiter les signaux faibles. « *Les SIEM ont bien évidemment toujours un rôle à jouer, mais le XDR et Cortex XDR ont un rôle à jouer dans l'enrichissement et le filtrage des alertes.* » Ainsi, si le XDR est complémentaire au SOC dans les grands groupes qui en disposent, pour des entreprises dont les moyens sont plus modestes, Cortex XDR peut suffire, avec le client XDR sur les postes clients et les firewalls qui alimentent le Data Lake Cortex, un moyen d'améliorer la posture de sécurité de l'entreprise sans avoir à investir dans un SIEM et la mise en place un SOC.
Adopté en tant que simple évolution de l'antivirus ou en tant que brique à part entière d'un écosystème cybersécurité, l'EDR est en train de s'imposer comme une solution de sécurité majeure à l'aube de la généralisation des nouvelles approches de type "zero-trust". A chaque RSSI de lui accorder le rôle qui sera le plus en phase avec sa propre stratégie de sécurité.

Alain Clapaud



En réalisant l'acquisition de Carbon Black, VMware a notoirement musclé une offre de protection endpoint qui s'appuyait sur Workplace One.

Ce qu'en pensent **les éditeurs**

« Un EDR doit pouvoir dialoguer avec d'autres briques de sécurité »

BRUNO LECLERC, DIRECTEUR DES VENTES DE SOPHOS FRANCE

« La valeur ajoutée de notre offre EDR tient dans le fait qu'elle peut dialoguer avec d'autres éléments de sécurité. Depuis 2015, nous avons développé un protocole SynSec pour Synchronised Security qui permet d'élever le niveau de sécurité car on va interroger l'ensemble des briques de sécurité Sophos, au niveau de la messagerie, de la mobilité, du WiFi et des firewalls. Si le firewall détecte un endpoint qui cherche à contacter un Command&Control, celui-ci va pouvoir bloquer le poste de travail et bloquer tous les autres postes qui ont un même flux réseau. D'autres acteurs ont repris cette approche aujourd'hui et le Gartner réfléchit à l'acronyme XDR pour référencer ce type d'approche, mais une interopérabilité entre les offres est difficile à imaginer entre acteurs en concurrence frontale. Notre réflexion vis-à-vis de l'ouverture aux autres acteurs porte plus sur l'accès aux IOC qu'à vouloir convaincre les autres acteurs à implémenter SynSec dans leurs solutions. »

« Un EDR ne doit pas être un outil fermé »

DAVID GROUT, CTO EMEA DE FIREEYE

« L'entreprise doit pouvoir utiliser les API de son EDR afin de créer ses propres investigations. Nos utilisateurs sont les gens qui opèrent les SOC. Ce sont des analystes qui mènent des levées de doute et des investigations. Certains SOC cherchent simplement dans leur EDR un outil pour créer leurs propres business cases d'investigation. D'autres font le choix du service managé FireEye. Nous travaillons alors pour eux sur la levée de doute et la chasse proactive des marqueurs de compromission (IOC). Enfin, il nous arrive de nous livrer à des investigations chez les entreprises victimes d'une attaque. Nous déployons l'EDR sur le réseau de l'entreprise puis nous menons le volet forensic de l'attaque pour son compte. C'est une prestation à réaliser dans un délai très court. »

« La Threat Intelligence est l'activité historique de CrowdStrike »

JOËL MOLLO, DIRECTEUR GÉNÉRAL EUROPE DU SUD DE CROWDSTRIKE

« Nous appliquons la règle 1/10/60 : 1 minute pour détecter une tentative d'attaque, moins de 10 minutes pour qu'un analyste caractérise la menace et 60 minutes pour éradiquer la menace et empêcher tout mouvement latéral. Cela nous permet de proposer à nos clients une cyberassurance avec une garantie jusqu'à 1 million de dollars si des données sont perdues en cas d'attaque. CrowdStrike compte plus de 5 000 clients dans le monde et un millier sont sous licence Falcon Complete. »

« Les sources de données de l'EDR doivent aller au-delà des seuls endpoints »

ERIC ANTIBI, SENIOR MANAGER CHEZ PALO ALTO NETWORKS

« Nous avons été les premiers à non pas parler d'EDR, mais de XDR. Le terme est devenu une catégorie du marché en tant que tel depuis. La nuance entre EDR et XDR, c'est que la source d'information qui va alimenter le Data Lake ne va pas être uniquement le endpoint, mais de multiples sources. Le endpoint est un vecteur d'attaque privilégié par les hackers, cependant un problème majeur dans la détection d'une attaque est d'avoir une vue globale de la situation, corréler des informations issues des endpoints mais aussi du réseau et même du cloud. C'est une approche qui est complémentaire à celle du SIEM. »

« Inutile de déployer un EDR si on n'a pas une bonne connaissance de sa surface d'attaque »

DAGOBERT LEVY, VICE PRESIDENT SOUTH EMEA DE TANIUM

« Beaucoup d'entreprises ont lancé un projet de déploiement d'EDR en négligeant un prérequis important : une bonne connaissance de sa surface d'attaque. On ne peut protéger que ce que l'on connaît et dans beaucoup de cas il faut atteindre une couverture maximale du SI avec les outils existants avant de songer à ajouter une nouvelle couche de sécurité. Il faut aussi se méfier de l'EDR de type "boîte noire". Cette approche peut conduire à noyer l'équipe de sécurité sous des milliers de détections, avec des milliers de faux positifs à traiter chaque jour. C'est la raison pour laquelle il est nécessaire de customiser l'outil en fonction de son activité et de l'intégrer avec l'existant, notamment le SIEM si on en dispose déjà. Un tel déploiement est structurant pour les 3 à 5 années à venir. Dans ce laps de temps l'entreprise va gagner en maturité, progresser, la surface d'attaque va évoluer en parallèle. L'approche "boîte noire" peut rapidement s'avérer inadaptée dans la durée. »

Les **principaux EDR** du marché

Bitdefender	Gravity Zone Ultra	Bitdefender implémente une trentaine de couches de protection dans son client ainsi que sa technologie ERA (Endpoint Risk Analytics). L'EDR s'appuie notamment sur le framework ATT&CK du MITRE.
BlackBerry Cylance	CylanceOPTICS	Alors que CylancePROTECT permet de contrer les attaques de malware, CylanceOPTICS ajoute une brique d'IA pour la détection des attaques et des outils d'investigation et réponse à incident.
Check Point Software	SandBlast Agent	L'agent destiné aux endpoint de Check Point implémente de multiples fonctions, donc les fonctions clé d'un EDR. A noter qu'il joue aussi le rôle de VPN, de chiffrement des contenus.
Cisco Systems	Advanced Malware Protection (AMP) for Endpoints	L'EDR Cisco est disponible en déploiement on-premise ou cloud pour les terminaux Windows, Mac, Linux ainsi que Android et iOS.
CrowdStrike	CrowdStrike Falcon	Approche 100% cloud privilégiant la mutualisation des indicateurs de sécurité. L'offre Falcon Overwatch met à disposition l'équipe de Threat Hunting de l'éditeur.
Cybereason	Cybereason EDR	S'appuyant sur le framework ATT&CK du MITRE, la solution implémente un antivirus Next-Gen et un EDR avec des données in-memory pour investiguer les graphes d'attaque.
Digital Guardian	Digital Guardian Endpoint Detection and Response	Editeur spécialisé dans la prévention contre les pertes de données, Digital Guardian propose un service managé d'EDR à son catalogue.
ESET	Enterprise Inspector	ESET Enterprise Inspector vient compléter la solution EPP d'ESET avec notamment le Threat Monitoring des postes ainsi que l Threat Hunting réalisé par les experts ESET.
F-Secure	F-Secure Rapid Detection & Response	Disponible pour Windows Desktop et Server ainsi que MacOS, l'offre F-Secure stocke ses données en Europe, dans le datacenter d'AWS en Irlande.
FireEye	FireEye Enpoint Security	L'offre intègre 4 modules de protection : anti-virus, machine leaning, comportemental, protection contre le vol d'identifiants déployables au travers de la console de supervision de l'outil.
Fortinet	FortiEDR	Fruit de l'acquisition d'enSilo en 2019, FortiEDR vient s'intégrer à la Fortinet Security Fabric, le framework de communication des différentes briques de sécurité de l'éditeur.
GoSecure	GoSecure EDR	Editeur canadien acquis par CounterTack en 2018, GoSecure propose un EDR on-premise ou cloud avec notamment un connecteur vers SAP HANA.
Kaspersky	Kaspersky EDR	Module de la suite Kaspersky Endpoint Security for Business, Kaspersky EDR est complété d'une offre de Threat Hunting en 24/7 de l'éditeur ainsi que de l'outil de détection d'APT YARA.
Malwarebytes	Malwarebytes Endpoint Protection and Response	Malwarebytes Endpoint Protection and Response met en oeuvre le Linking Engine et le Ransomware Rollback, des technologies de remédiation propres à l'éditeur.
McAfee	MVISION EDR	L'offre logicielle MVISION EDR est déployable via la plate-forme de gestion McAfee ePolicy Orchestrator on-premise ou via la plate-forme SaaS McAfee MVISION ePO. Le logiciel est complété d'une offre de service managé McAfee Managed Detection and Response.
Microsoft	Microsoft Defender ATP	Avec la version Advanced Threat Protection de Defender, Microsoft propose une suite EDR complète dédiée à Windows 10 et qui offre un jeu d'API complet.
Nucleon Security	Nucleon Smart Endpoint	Editeur français, Nucleon Security propose une solution de gestion des vulnérabilités ainsi qu'un EDR "souverain" qu'il destine notamment aux PME et ETI.
OpenText	OpenText Security Suite	Issue de l'acquisition de Guidance Software, l'EDR EnCase Enpoint Security fait partie du portefeuille applicatif d'OpenText.
Palo Alto Networks	Cortex XDR	La solution XDR de l'éditeur est capable d'analyser les données issues de endpoints mais aussi des firewalls, y compris s'ils ne sont pas d'origine Palo Alto Networks.
Panda Security	Panda Adaptive Defense	Panda unit EPP et EDR dans son offre Panda Adaptive Defense, avec une approche basée sur une classification de 100% des processus actifs des postes clients.
RSA	RSA NetWitness Endpoint	La solution réunit à la fois l'EDR, le NDR (détection et réponse réseau), SIEM, UEBA et SOAR (Orchestration et automatisation) sur une même plateforme.
SentinelOne	SentinelOne ActiveEDR	La solution stocke par défaut 30 jours d'activité, un délai qu'il est possible d'étendre, fournit un jeu d'API ainsi que le support du streaming Kafka pour exporter ses données vers un Data Lake.
Sophos	Intercept X avec EDR	Sophos a intégré la fonction EDR à son offre Intercept X en 2018. Elle implémente le protocole SynSec qui permet d'élever le niveau de sécurité de l'ensemble des briques de sécurité Sophos en cas d'alerte.
Symantec	Symantec EDR 4	Anciennement dénommé Advanced Threat Protection (ATP), Symantec EDR est une solution cloud couplée à une offre de service s'appuyant sur les SOC de l'éditeur.
Tanium	Tanium Threat Response	Expert de la visibilité et du contrôle des postes de travail et serveurs, Tanium exploite son logiciel client pour proposer des fonctions d'EDR.
Tehtris Security	Tehtris EDR	La solution d'EDR de l'éditeur français Tehtris peut fonctionner en mode on-premise ou cloud et peut s'interfacer à la plateforme XDR de l'éditeur. Son agent est disponible sous Windows, MacOS, Linux et Android.
Trend Micro	Smart Protection for Endpoint	Solution complète de protection des postes de travail comprenant gestion des vulnérabilités, chiffrement, protection des mobiles, prévention des pertes de données...
VMware	Carbon Black Cloud	L'offre d'EDR Carbon Black est venu renforcer l'offre Workplace One de VMware et a intégré sa solution AppDefense.
WatchGuard	WatchGuard Threat Detection and Response (TDR)	Spécialiste de la sécurité réseau WatchGuard correle les données de ses appliances Firebox et celles glanées par ses agents Host Sensor pour délivrer le service cloud d'EDR ThreatSync.

Modélisation de la sécurité : comment faire du vent avec de vrais problèmes

Les grandes entreprises ont souvent recours aux techniques de modélisation pour traiter d'un problème donné. Leur objectif est d'harmoniser la perception des équipes vis-à-vis de ce problème et d'imposer les bienfaits d'une pensée unique. Ce n'est pas pour autant que la modélisation soit systématiquement la meilleure approche possible. Dans le cas de la sécurité, avec des outils tels que CARTA, nous pensons justement qu'au minimum, la question mérite d'être posée.

La tendance est à la modélisation et plus précisément à celle de la sécurité. On cherche à décrire de manière exhaustive les tâches à exécuter, les comportements à traquer, de manière à rendre le SI, sinon insensible aux attaques venues de l'extérieur, pour le moins le plus imperméable possible en cas d'opération malveillante et capable de réagir avec le maximum d'efficacité.

Il y aura deux grandes approches. Celle qui consiste à modéliser les opérations, ressources et comportements dans le cadre d'un référentiel, comme le font Cobit 5 et CARTA du Gartner, avec le risque de se perdre dans des descriptions théoriques, sans liens avec le terrain et celle qui consiste à s'approcher au plus près des réalités techniques et d'en déduire un « modus operandi » spécifique du domaine traité, pour la messagerie, pour les accès Cloud, etc. C'est ce que proposent les EDR.

En gros, les outils de type CARTA seront parfaits pour concevoir de beaux Powerpoint en couleurs, mais n'apporteront pas grand-chose, dès lors que l'on passera aux travaux pratiques.

Le danger d'une telle méthodologie étant qu'elle peut devenir une cible et non plus un outil.

C'est en tout cas le point de vue que nous défendons ici. L'approche des EDR, nous semble mieux coller à la réalité des besoins. C'est d'ailleurs ce qui remonte du terrain, CARTA n'étant pas une réussite, malgré le nom de son sponsor, alors qu'il existe de plus en plus de produits EDR, tels que SentinelOne, qui exploite un mécanisme d'IA ou CrowdStrike Falcon Insight. On peut y voir un signe.

L'art de vendre du vent

Certains consultants, soucieux de trouver de nouveaux débouchés pour leurs équipes et désireux d'attacher leurs clients par des liens forts, ont choisi une fois de plus le domaine de la sécurité IT pour sévir. L'idée est géniale…

Ils élaborent une méthodologie, avec un glossaire pour savoir de quoi on parle, des bonnes pratiques pour se distinguer des autres intervenants, qui n'ont pas été touchés par la grâce, édifient de beaux schémas avec des modèles à N couches (sans un modèle à N couches, ça ne fait pas sérieux), établissent un cheminement qu'il faut absolument emprunter, sinon on n'y arrivera pas et surtout ils prévoient des paliers de certification, auxquels les clients avec force dollars, vont se soumettre pour avoir le sentiment d'appartenir au cénacle des « gens qui savent ». Même s'il y a un fond de vérité, ne serait-ce qu'à travers les bonnes pratiques proposées, tout cela n'est somme toute que du vent, disons une brise, destinée à donner une sorte de « cadre légal » à certains domaines du TI : le développement et la sécurité, entre autres et une légitimité à des équipes qui veulent se positionner dans la hiérarchie de leur entreprise.

C'est un peu comme les diplômes. En général, ils ne servent à rien, si ce n'est pour entrer « quelque part », mais une fois en place, on se rend compte qu'ils n'apportent pas grand-chose de concret. On exagère à peine…

C'est exactement ce qui se passe dans le domaine de la sécurité, où l'on voit fleurir des méthodologies et outils de modélisation théoriques, les consultants ayant pris soin de rappeler que le TI est une catastrophe sécuritaire mondiale, que les Russes et les Chinois sont prêts à nous envahir, fortement aidés il est vrai par les Coréens du nord, sans qui une attaque ne saurait être prise au sérieux et qu'il ne faut pas se demander si notre système d'information va exploser, mais quand cela va se produire.

Évidemment dans ce contexte, tout ce qui peut rassurer les clients est bon à prendre et s'il vous prenait l'envie d'inventer une nouvelle méthode fondée sur l'alignement des astres et les cycles de reproduction des hannetons du Baloutchistan oriental, nul doute que vous auriez beaucoup de succès.

Vous l'avez compris, nous sommes quelque peu sceptiques sur le sujet (…), convaincus que la solution est plus dans une approche rationnelle de la protection, avec des gens qualifiés aux bons endroits et un traitement technique des problématiques. Et pas dans un verbiage fumeux bourré d'évidences.

Nous pensons certes, qu'il peut être intéressant de répertorier les failles dans un modèle à N couches, mais qu'il faut surtout inculquer des techniques de programmation et de conception d'architectures, pour éviter justement ces failles. Autrement dit traiter le mal à la racine, plutôt que de passer son temps à poursuivre un ennemi, qui de toute façon a toujours une bataille d'avance.

Il y a, chaque jour, plus de 50 000 virus nouveaux, chevaux de Troie, Rootkits et produits qui exploitent des failles, connues ou pas (attaques « zero day »). Et on ne voit pas très bien comment faire face à la déferlante, si ce n'est en fermant tous les accès de notre SI, ce qui est évidemment impensable. Nous avions bien suggéré de remplacer la quasi-totalité des protocoles en activité sur Internet : TCP, IP, CMIP, DNS, SMTP, SNMP, etc., mais il semble que cela soit trop tard, un peu compliqué à faire et que la facture pour construire un nouvel ordre sur Internet, soit inenvisageable. Dont acte.

Il nous faut donc faire contre mauvaise fortune bon coeur, « faire avec » et nous organiser en conséquence. D'où la prolifération des marchands de rêves.

Demain…

On a tous conscience qu'il y a intérêt à mettre de l'ordre dans notre approche sécuritaire du TI. Car c'est souvent n'importe quoi, tant du point de vue des comportements, que des outils. Mais nous ne sommes pas convaincus qu'une « pure » solution de modélisation, qui n'est rien d'autre qu'un catalogue de bonnes intentions, pourra changer quoi que ce soit à la gravité de la situation.

Non pas que l'approche CARTA ne soit pas séduisante, mais elle n'est pas suffisamment concrète, les vrais problèmes se situant à la source, dans les faiblesses des briques protocolaires et les comportements suicidaires des usagers.

Le seul intérêt de ce référentiel est qu'il dresse un inventaire des problèmes à traiter. Il indique ce qu'il faut faire, mais ne dit pas comment le faire.

Quant à savoir s'il faut perdre du temps à se faire certifier, la réponse est dans la question… Au fond, l'histoire se répète. N'a-t-on pas déjà dit la même chose au sujet d'ITIL ?

La modélisation carta du gartner

Le cabinet américain Gartner a publié en 2014 un référentiel de modélisation applicable à la sécurité.

Il s'agit de CARTA (« *Continuous Adaptive Risk and Trust Assessment* »), qui consiste à mettre en place une approche prédictive de la sécurité, fondée sur l'analyse permanente (!!!), le Machine Learning et l'évaluation constante du contexte. Évidemment si l'on fait intervenir le Machine Learning et l'Intelligence Artificielle, dans cette affaire, nul doute que ça ira beaucoup mieux.

Ce qui est sûr, c'est que le Gartner était très optimiste lors de l'annonce de CARTA, puisque le consultant prévoyait qu'en 2020, 25 % des grandes compagnies auraient adopté son modèle (ils étaient 5 % en 2017). Ramené aux réalités concrètes du terrain, il serait étonnant que CARTA dépasse les 10 % et encore parmi ces 10 %, il y a bon nombre d'entreprises qui sont prêtes à tout accepter, à condition que le logo du Gartner apparaisse. Qui n'a d'autre but que de servir de parapluie à leurs propres décisions. Si le Gartner a dit, donc… Pour la petite histoire, CARTA est donc une méthode d'analyse continue, fondée sur la modélisation des « assets » (ressources), dont on évalue de

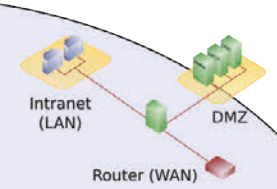
(suite en page 16)

LEMARSON 2020

Cet article est extrait de l'ouvrage LeMarson 2020 ouvrage de référence sur les tendances et technologies IT/TI (plus de 500 pages format A4, 1,5 kg !). Créé en 2015, le service LeMarson (www.lemarson.com) propose de nombreux dossiers qui concernent les problématiques du TI. Il comporte aussi des formations vidéos longue durée : Big Data, Tendances Informatiques, NoSQL, projets agiles, applications, etc, des webinaires chaque semaine sur invitation, des séminaires en direct multi-sessions : IA, Blockchain, objets communicants, un accompagnement technique des clients, etc.… Exclusivement en français, le service est dirigé par Claude Marson. Il est disponible sur abonnement.

Sécurité périmétrique

Firewall périmétrique



DeMilitarized Zone
Zone démilitarisée bornée par deux firewalls, dans laquelle on place les élements sensibles exposés à l'extérieur

Détecteur d'intrusion avec firewall (IPS) ou sans (IDS)

Anti malware
Détecte et supprime les malwares d'une machine, sur la base d'une bibliothèque de signatures. Placé dans la DMZ.

Honeypot
Technique qui consiste à attirer des attaques sur des ressources contrôlées pour les identifier et les neutraliser

Sécurité des réseaux

Sécurité de la messagerie
Ressources pour sécuriser les messages sortants et détecter les anomalies des messages entrants

NAC pour identifier qui se connecte sur le réseau et d'où il le fait.

Protection VoIP
Système de protection contre les intrusions, passées par unh protocole de téléphonie logicielle

VPN
Lien direct et sécurisé pour accéder à distance aux ressources du TI. Avec des fonctions d'isolation, de chiffrement et d'authentificat

Proxy
Ressoure qui permet à un client interne d'accéder à des serveurs externes (Web) sans dévoiler son identité.

Serveur d'accès aux ressources réseaux
Radius...

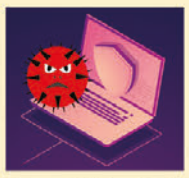
Reverse Proxy
Permet à un usager externe d'accéder à un serveur Web interne (inverse du proxy)

NBA
Anlayse comportementale des équipements réseaux, fondée sur les protocoles spécifiques de communication inter-équipements : switchs, routeurs, frontaux...,

Sécurité des réseaux "sans-fil"
L'ensemble des outils qui permettent de sécuriser les réseaux Wi-Fi et cellulaires.

Sécurité "endpoints" : serveurs, postes de travail

Endpoint Detection and Response
L'ensemble des outils qui permettent de surveiller le comportement des postes de travail et serveurs (endpoints), en permanence et de manière prédictive



Firewall du desktop
Pare-fu intégré à l'OS ou fourni en add-on sur le poste de travail. Relativement peu connu et souvent mal paramétré.

Gestion des patchs
Logiciels d'aide à la gestion patchs : postes de travail et serveurs

IDS/IPS dédié host
Détecteur IDS/IPS attaché à une machine hôte, avec fonctions de firewall et proxy

Anti-malware
installé sur un poste de travail. Peu efficace.

Conformité FDCC
(Federal Desktop Core Configuration)
Ensemble des recommandations émises par le "National Institute of standards and Technology).

Sécurité applicative

Revue de code orientée sécurité
Outils de détection des faiblesses sécuritaires d'une application. Souvent intégrés à des produits de revue de code. plus complets.

WAF ("Web Application Firewall")
Pare-feu dédié aux applications Web, orienté analyse des paquets HTTP et HTTPS et des autres protocoles applicatifs d'Internet.

Sécurisation des bases de données
Outils qui surveillent l'usage sécuritaire des bases de données, remontent les alertes et mettent en oeuvre les parades. Les outils sont soit intégrés aux SGBD, soit fournis en addons.

Modélisation des faiblesses
Outils qui modélisent en amont les faiblesses potentielles des applications, pour servir de base aux tests de pénétration.

Footprinting
Toutes les techniques qui visent à acquérir des informations sur les cibles, y compris applicatives.

Recommandations d'écriture
Ensemble de recommandations pour l'écriture d'un code sécurisé. La distinction est faite entre les langages script et objet.

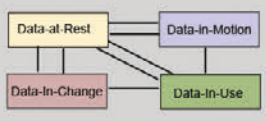
Tests de pénétration
Solutions qui simulent les pénétrations illicites dans le système d'information, de manière à améliorer ses protections.

Sécurité des données

DLP (Data Loss Protection)
Permet de se protéger contre la perte ou le vol de données sensibles.

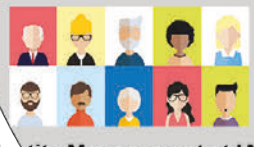
PKI
Architecture à clés publiques. Attribution de certificats, pour garantir l'identité d'une entité.

"Data Cleansing"
Outils de nettoyage automatique des données, liés aux critères de qualité retenus.



DAR, DIU, DIM
Protection des données, en usage ou en transit dans les mobiles

Customer Identity & Access Management
Gestion des données clients avec respect des contraintes règlementaires



Identity Management et IAM
Gestion des identités et solutions intégrées, l'identité prise au sens d'une donnée sensible

Modélisation des données
et annuaires
Dans une optique sécuritaire : données sensibles, liens...
Des outils tels qu'UML, Merise...

Technologies génériques

Fido
Détection d'un mobile, par la combinaison d'une clé privée et d'une donnée biométrique

Chiffrement
Technologies pour assurer la confidentialité des données. Systèmes symétriques, asymétriques ou mixtes

Sécurité du Cloud
Technologies spécifiques de protection des ressources serveurs et données dans le Cloud

OAuth
Protocole pour accéder aux ressources "patrimoniales" d'un utilisateur

SSO et WebSSO
Authentification unique des usagers

Identité des objets et IRM
Les objets reçoivent une identité, qui peut être administrée par un IRM (Identity Rights Management)

Biométrie
Technologies pour reconnaître une entité par ses caractéristiques physiques

(suite de la page 15)

manière prédictive et continue le comportement. Autrement dit, en fonction du contexte qui n'arrête pas de changer, avec de nouvelles menaces et faiblesses, on cherche à modéliser la capacité de réaction et d'opposition aux attaques et aux dysfonctionnements.
Le Gartner liste cinq points clés, à prendre en compte, pour y parvenir. D'abord réaliser un inventaire de toutes les ressources et effectuer des mises à jour systématiques et automatiques, dès que les modifications interviennent. Vieux « serpent de mer » que l'on a connu avec les CMDB de l'approche ITIL, si ce n'est que l'on se concentre ici sur la sécurité.
On sait, « grâce » au CMDB, qu'il est très difficile de garantir les remontées temps réel des modifications et qu'il reste toujours une part importante de saisies manuelles à effectuer.
Modéliser ensuite les relations entre les ressources, de manière à anticiper sur les effets collatéraux d'une attaque menée sur une ressource bien précise : machine, réseau, poste de travail, fichiers, etc.
Là encore on est exactement dans le même contexte que le CMDB et l'on sait que si l'idée est effectivement très séduisante, elle est difficile à mettre en oeuvre.
Evaluer de manière continue les vulnérabilités des systèmes et les prioriser pour les prendre en charge. L'idée que recommande le Gartner étant de se focaliser sur les vulnérabilités les plus criantes, celles qu'exploitent réellement les criminels. Évidemment, on ne va pas suggérer le contraire…
Comme toujours, il faut démontrer que l'approche CARTA est pertinente, aussi allons-nous nous armer de métriques qui démontreront le bien-fondé de l'approche.
Le dernier point concerne l'adaptabilité du modèle CARTA, qui doit être remis en cause régulièrement, chaque mois, au minimum une fois par trimestre. C'est le coeur de la méthode, s'adapter aux évènements et être proactif pour anticiper sur les nuisances.
Une fois ces prérequis respectés, la modélisation CARTA est censée répondre à quatre grands objectifs : prédire les aléas sécuritaires, sur un modèle donné, prévenir les incidents, de manière continue, ce qui n'est pas pareil que de se contenter de les prédire, prioriser les faiblesses pour mieux s'opposer aux attaques et répondre aux changements de contextes.
Personne ne pourra dire que ce ne sont pas de bonnes idées, sauf à être de mauvaise foi, mais ce n'est pas parce qu'elles sont « rangées » dans un modèle CARTA, qu'elles seront plus faciles à mettre en oeuvre.

Les liens avec les EDR

Dans un domaine plus limité, le Gartner et d'autres consultants, nous suggèrent depuis 2013, une approche différente de la modélisation des actions sécuritaires, focalisée sur les « endpoints », serveurs et postes de travail, les EDR (*« Endpoint threat Detection and Response »*).
Ces EDR, qui ressemblent par certains aspects à CARTA, sont basés comme celle-ci sur la récupération en temps réel, d'un maximum d'informations ayant trait à la sécurité des endpoints. Qui vont leur permettre de remplir une triple mission : détecter, investiguer et remédier.
Cette-fois, on n'est plus dans un référentiel de type CARTA, mais dans une chronologie de bonnes pratiques. C'est beaucoup plus concret et proche des problématiques à traiter, que la seule modélisation.
La détection se fera en temps réel et de manière intelligente, selon une escalade à quatre niveaux : recherche de présence de l'anomalie dans d'autres sources recherche de signatures connues recherche d'attributs comportementaux ou d'écarts de comportements et si les attributs ne sont pas reconnus, confinement et « sand boxing » Pour ce qui est de l'investigation, deuxième volet EDR, elle sera intuitive, avec recherche des IOC (indicateurs de compromission) ou IA (Indicateurs d'attaques), sur les « endpoints » : date de création, hash, noms de fichiers, taille, etc., qui auront pu être compromis et sur la recherche d'événements caractéristiques, telle qu'une augmentation anormale des privilèges ou une escalade horizontale, le code s'exécutant sur des machines tierces, dans le Cloud par exemple ou dans un botnet.Quant à la remédiation, autrement dit l'organisation des parades, son principe consiste à prioriser les interventions des équipes, grâce à l'évaluation de la criticité des alertes. On pourra alors supprimer les process malveillants, quand ce sera possible, mais aussi isoler le réseau, mettre le process en quarantaine, voire revenir à une version plus saine des fichiers et de l'OS… ou décider de le traiter quand on aura le temps.
En comparant CARTA et les EDR, on voit bien qu'il y a d'incontestables zones de recouvrement. Les deux référentiels pouvant d'ailleurs se concevoir conjointement. La vraie différence tient à ce que CARTA est un modèle global de sécurité de l'entreprise, à 8 000 pieds d'altitude par rapport aux problèmes concrets des clients, alors que l'EDR propose un cheminement d'actions à effectuer, de manière très précise, en se focalisant sur les serveurs et les postes de travail.
De ce fait, il est beaucoup plus utile. Et n'a pas ce côté abstrait, que certains trouvent décalé…

Emotet, le retour

Ce n'est plus le cheval de Troie bancaire que l'on a connu mais plutôt désormais un vecteur d'attaques opéré par un groupe appelé TA542 lequel a des « clients » qui exploitent des trojans tels que Dridex, Qbot et TrickBot distribués sous forme de seconde charge utile. Emotet doit donc être détecté au plus tôt sur les postes infectés car sa présence laisse prévoir d'autres intrusions. Les premiers courriers d'hameçonnage contiennent la plupart du temps des fichiers joints de type PDF ou Word. L'ANSSI a lancé une alerte le 7 septembre sur la recrudescence d'Emotet en France avec quelques recommandations : ▸ Sensibiliser les utilisateurs à ne pas activer les macros dans les pièces jointes et à être particulièrement attentifs aux courriels qu'ils reçoivent et réduire l'exécution des macros. ▸ Limiter les accès Internet pour l'ensemble des agents à une liste blanche contrôlée. ▸ Déconnecter les machines compromises du réseau sans en supprimer les données. ▸ De manière générale, une suppression / un nettoyage par l'antivirus n'est pas une garantie suffisante. Seule la réinstallation de la machine permet d'assurer l'effacement de l'implant.

Pour Matt Walmsley, expert cybersécurité et directeur Europe de Vectra, *« chercher à identifier et à comprendre qui sont les opérateurs d'Emotet ainsi que leurs motivations fait partie du puzzle et c'est le rôle des forces de l'ordre. Mais le plus utile et le plus durable pour la sécurité reste de comprendre les tactiques et les techniques qu'ils utilisent et d'anticiper la manière dont elles pourraient être atténuées pour protéger les cibles du Trojan.*

« Dans le cas d'Emotet, il s'agirait notamment de détecter l'utilisation abusive de comptes à privilèges, les mouvements latéraux sur le réseau local (pour les PME par exemple) et les comportements signalant la présence d'outils de commande et de contrôle (C&C). Les équipes de sécurité doivent être de plus en plus agiles, car le temps est leur ressource la plus précieuse pour faire face aux attaques de logiciels malveillants. Une détection et une réponse précoces sont essentielles pour reprendre le contrôle et arrêter les attaquants avant qu'ils ne puissent se propager dans l'organisation, et qu'ils volent ou empêchent l'accès aux données. »

Trois mesures clés pour le retour au bureau

Sur la base d'une enquête menée auprès de son club d'utilisateurs, SailPoint a identifié trois mesures clés que doivent prendre les équipes IT et sécurité alors qu'un nombre croissant d'employés ont commencé à retourner à leur bureau en septembre :

▸ Mettre à jour et vérifier continuellement les identités des utilisateurs afin d'aligner les droits d'accès aux fonctions de chacun. Utiliser des politiques intégrées de conformité et de traçage des groupes de travail pour s'assurer que chaque utilisateur a les droits d'accès adéquats dès son recrutement en qualité d'employé et de sous-traitant, lorsqu'il change d'affectation, est promu ou quitte l'entreprise.

▸ S'assurer d'autorisations d'accès appropriées aux applications, fermer des accès sur la base d'analytiques en temps réel, et contrôler les actions des utilisateurs. Utiliser le machine learning et les plus récents outils d'IA pour gérer toutes ces procédures à la fois pour les applications hébergées sur site et dans le cloud.

▸ Passer d'une protection des données basée sur un périmètre de sécurité à un processus basé sur l'identité. Identifier propriétaires des données et la plate-forme pour classer et cataloguer les données de façon intelligente. Ceci à la fois pour les données structurées et non structurées.

Appliances firewall : l'essor de la virtualisation

Devant l'essor du Cloud et de la virtualisation, que deviennent les appliances de filtrage ? Nous avons voulu faire un point de situation, en interrogeant quelques parties prenantes du secteur...

Le pare-feu a été l'un des premiers éléments de la sécurité des réseaux. Au départ déployés dans les années 90 avec des simples listes de filtrages d'adresses IP, ces équipements empilent aujourd'hui les fonctionnalités : terminaison SSL/TLS, antivirus, filtrage applicatifs, authentification des utilisateurs, data-leak prevention, deep packet inspection...

Ce que proposent les éditeurs aujourd'hui

Chez tous les éditeurs, on note une volonté de proposer à leurs clients des solutions unifiées de gestion de leur sécurité, avec une simplicité d'administration. Depuis les années 2010 nous avons constaté un fort déplacement du traitement et du stockage des données vers le Cloud. Que deviennent ces équipements dans un contexte multi-réseau et de forte virtualisation ? Pour le savoir, nous avons demandé à différents éditeurs de présenter leurs dernières nouveautés : Sophos, Fortinet, Stormshield, Watchguard, pour la partie appliance, et Zscaler, pour l'offre « pure player » Cloud.
Quel est l'état de la menace aujourd'hui ? Sophos a publié un rapport, «*The State of Ransomware 2020* », qui précise que l'année dernière une entreprise sur deux dit avoir rencontré un cas de ransomware sur son réseau. Le Sophos Lab, qui analyse des milliers de fichiers suspects tous les jours, nous parle de « Maze ransomware », ou encore de « Lockbit », cette menace nouvelle génération qui combine chiffrement des données, vol d'informations et menace de divulgation.
Sophos propose le concept de sécurité synchronisée qui permet de corréler tous les événements collectés, au niveau firewall et endpoints, pour produire des réponses automatisées aux menaces. Le point central de management est la console « Sophos Central », déployée dans le Cloud, pour laquelle Sophos annonce un taux de disponibilité de 99,99%.
Selon Patrice Clair, directeur avant-vente de Sophos France, il y a deux points de sécurisation du réseau: au niveau du poste de travail avec Sophos Intercept X et, au niveau du filtrage LAN/WAN, Sophos propose le XG firewall, qui a une fonctionnalité d'IPS (intrusion prevention system). Comme le rappelle Patrice Clair : *« aujourd'hui plus de 80% du trafic réseau est chiffré. L'interception SSL est primordiale pour analyser le trafic ».*

Le déchiffrement SSL est essentiel

Même son de cloche chez WatchGuard : pour Jérémie Schram, ingénieur avant-ventes, *« 80% du trafic utilisateur est chiffré, le déchiffrement SSL est donc essentiel. Les équipements doivent être dimensionnés en conséquence. »* WatchGuard propose le « Firebox » (physique), le « Firebox Cloud » (cloud public) et le « FireboxV » (virtualisé). Avec deux niveaux de licences : « Basic Security » et « Total Security ». La philosophie de WatchGuard est

Patrice Clair, directeur avant-vente de Sophos France.

Hervé Schauer (HS2)

« La protection périmétrique est caduque »

Aujourd'hui à la tête du cabinet de conseil HS2, Hervé Schauer a été l'un des pionniers de ces technologies dans les années 80. Nous lui avons demandé de dresser un bref panorama de ces évolutions technologiques, et sa vision du futur !

L'1FO-CR : M. Schauer, vous êtes un expert reconnu en sécurité des systèmes d'information. Pourriez-vous nous décrire l'historique du firewall, et dans un contexte de virtualisation, quels sont les gains opérationnels et les mesures de sécurité à déployer ?

Hervé Schauer : *« Tout d'abord je ne suis pas spécialiste et justement je ne trouve pas de spécialistes Cybersécurité Azure ou AWS pour dispenser des formations. En effet J'ai coinventé le proxy firewall en 1991 avec Christophe Wolfhugel. Cela a été présenté à Usenix à Baltimore en 1992.*
Lors de l'avènement des réseaux dans les années 80, la sécurité passait par le mot de passe pour authentifier l'utilisateur. En 1986 Bull a couplé un lecteur de carte à puce au PC et en 1988 je prédisais que tous les claviers auraient un lecteur de carte à puce et que nous nous authentifierions avec. Raté. Il a fallu attendre les ports USB, des bus série comme le lecteur de carte à puce, mais pour une authentification par un facteur autre que le mot de passe, ce sont les ordiphones qui le permettent enfin, c'est récent, il aura fallu 30 ans.
Dans l'intervalle TCP/IP a pris le pas sur Novell Netware et la sécurité d'accès aux applications totalement défaillante, que ce soit sur des PC de l'époque ou des stations de travail Unix (rlogin, NFS et les Yellow Pages de Sun, etc). Puis en 1988 TCP/IP a quitté le réseau local pour passer en inter-sites et le vers Morris a montré les conséquences. Il fallait pouvoir échanger avec Telnet et FTP, voir avec X11 ou SQL, entre entreprises distinctes, et aucun moyen d'authentifier les flux n'existait. Donc en 1989 Network Systems (devenu StorageTek puis EMC) a inventé le filtrage IP sur un contrat Darpa, et il a été programmé dans Wellfleet (devenu Bay Networks puis Nortel) en 1991, puis dans CISCO IOS aussi en 1991. J'ai co-inventé le proxy firewall sur un contrat CNES en 1991, afin d'aller au-delà du filtrage IP en identifiant et authentifiant l'utilisateur en coupure dans la communication. Pas de brevet, de là tous les éditeurs ont repris le principe, les firewalls ont permis la protection périmétrique et l'expansion d'Internet de 1994 à nos jours.
En 1999 j'ai fais des présentations aux USA et même dispensé un "Short Course" à la conférence SANS à Orlando sur "The doom of the firewall" pour démontrer que la protection périmétrique était insuffisante et qu'il fallait impérativement cloisonner les réseaux. C'était le paroxysme de la sécurité dans le réseau, qui n'a cessé de se développer des années 2000 à nos jours. En 2003 des réflexions chez Cisco ont mené à la création du Jéricho Forum qui a fait une campagne en 2004 pour la déperimétrisation. J'ai répondu en 2005 avec une présentation ci-jointe à la JSSI de l'OSSIR que ce n'était pas pour tout de suite. Cédric Blancher m'a emboité le pas avec une présentation plus complète à SSTIC en 2008.
Mais quand j'ai clamé haut et fort aux Assises de la Sécurité toujours en 2008, appellé à l'improviste à la conférence plénière à la tribune, que "le RSSI allait survivre au DSI", j'ai fait scandale, il y a beaucoup de DSI invités aux Assises, pas que des RSSI, j'ai froissé du monde. Pourtant, le directeur cybersécurité des années 2020 va prendre l'importance et le grade qu'ont eu les DSI dans les années 2000 et 2010.
Maintenant les applications sont dans le cloud, elles seront gérées majoritairement par les métiers directement, localement, plus par une DSI centralisée, les DSI sont un service d'accès à Internet et de gestion d'annuaires (eux-mêmes dans le cloud), comme les gestionnaires de téléphonie l'étaient avant eux. Les applications utilisent des webservices dans tous les sens, seuls les auditeurs en cybersécurité retracent quel composant appelle quel composant, les DSI ne savent plus. Et les utilisateurs sont hors du réseau protégé, chez eux avec la crise sanitaire, avec des appareils divers et personnels...
La protection périmétrique est donc caduque, la sécurité doit être mise au plus proche des données auxquelles l'utilisateur réclame l'accès. Google a très bien expliqué comment il le faisait en 2017 et maintenant c'est sous le terme "ZeroTrust" que ce mouvement est popularisé. »


Mathieu Bonenfant, directeur marketing et de produit chez Stormshield.

là aussi de proposer une simplicité d'administration. Ils proposent également une plateforme de « CTM » (Cyber Threat Management). Leurs appliances sont capables de faire de la détection d'intrusion, de l'antivirus, de l'inspection protocolaire TLS. L'objectif consiste à proposer du« best of breed » avec un déploiement modulaire, pour coller aux besoins spécifiques de leurs clients.
Finalement, l'inspection SSL n'est-elle pas trop consommatrice de ressources ? Zscaler dit répondre à ce besoin, en effet selon Ivan Rogissart (responsable des ingénieurs avant-vente pour l'Europe du sud, Zscaler): un proxy est indispensable au niveau architecture pour obtenir des performances satisfaisantes. L'avantage de Zscaler, pure player du Cloud, est de pouvoir répondre à la demande grâce à son infrastructure multi tenant et le cas échéant d'upgrader son infrastructure. Pendant la crise pandémique, certains clients ont vu leurs connexions VPN multipliées par 10 ou 20. Zscaler a doublé ses infrastructures pour absorber la montée en charge en quelques jours.

Analyse fine des protocoles industriels

Stormshield, seul éditeur de solutions de firewalls en France et 1er éditeur européen, fait aussi de la terminaison HTTPS sur ses équipements, nous explique Mathieu Bonenfant, directeur marketing et de produit. « *Stormshield, filiale d'Airbus, est issu de la fusion de Arkoon et Netasq. Nous avons un centre de threat intelligence, pour identifier les menaces et proposer des contre-mesures. Nos équipements de filtrage de la gamme SNS sont tous équipés en standard de filtrage d'URL, d'analyse anti-malware, de terminaison HTTPS, de prévention d'intrusion et de VPN. Les PME activent souvent un maximum de fonctionnalités sur le même équipement. Les grandes entreprises et administrations vont plutôt utiliser nos firewalls en connexion intersites, avec la fonction VPN* ».
« *Notre stratégie, poursuit Mathieu Bonenfant, est d'accélérer notre développement vers la protection des réseaux d'automates industriels, qu'on appelle* « réseaux OT » *(Operational Technology).* »

Sur ces infrastructures, il y a trois types de contraintes : contraintes matérielles du fait des conditions environnementales (résistance aux vibrations, à l'humidité, aux variations de températures,...), maintien de la sûreté de fonctionnement et prise en charge des protocoles de communication industriels. Par exemple quand on met un firewall qui est en segmentation réseau, Stormshield sait faire une analyse très fine des protocoles industriels, et déterminer qu'une commande qui est passée est légitime ou non. Cela a été mis en œuvre récemment, par exemple chez leur client SNCF Réseau: Stormshield a mis en place une segmentation IT/OT et une analyse protocolaire pour sécuriser les zones industrielles.

La configuration du firewall, étape clé

Comment s'opère la détection de binaires ? D'après Jérémie Schram (WatchGuard) : « *Pour sécuriser une appliance, qu'elle soit virtualisée ou non, la configuration du firewall va être aussi importante que la robustesse de la solution elle-même. Le client a par ailleurs une grande part de responsabilité en ce qui concerne sa sécurité : les qualités du produit et de l'intégrateur ne peuvent pas suffire si le client refuse certains mécanismes.* »

Pour analyser les binaires, WatchGuard est en partenariat avec Lastline (qui vient d'être racheté par VMware) sur la partie sandboxing, avec Bitdefender pour la partie anti-virale, et enfin avec Cylance (une société BlackBerry) pour la partie analyse de fichiers basée sur l'IA.
Sophos n'est pas en reste et propose de l'IA et une corrélation d'évènements de sécurité via son « Sophos Lab ».
Fortinet est un autre acteur historique avec la solution Fortigate. Christophe Auberger est Cybersécurité évangéliste France. Selon lui, la philosophie de Fortinet est de protéger ses clients contre l'ensemble des

risques cyber au travers d'une plateforme intégrée, unifiée et automatisée, appelée « Fortinet Security Fabric ». Le pare-feu nouvelle génération, FortiGate, peut être déployé en mode appliance ou en mode virtualisé, sur tout type de plateforme (AWS, Azure, GCP).
Fortinet propose aussi le «*Zero-trust Network Access* »: la transformation numérique fait que l'on ne peut plus avoir de zones de confiances dans le réseau. On va donc valider l'ensemble des personnes qui se connectent sur le réseau. C'est plus de que l'authentification. On va savoir qui se connecte à partir de quoi et où, et s'il en a le droit ou pas. Cela fonctionne sur du filaire, sur du wireless. Ces fonctions peuvent êtres portées par un pare-feu nouvelle génération, par un système d'authentification, ou déployées sur un Cloud. Voilà typiquement une bonne réponse aux risques engendrés par le cyber et la virtualisation.
Une tendance intéressante est le partage d'informations sur la « threat intelligence » en back end. Tous les éditeurs possèdent des laboratoires d'analyses de binaires, et prétendent pouvoir détecter en temps réel un malware chez un client, le remonter dans leur propre lab pour analyse, puis distribuer rapidement sa signature à tous leurs autres équipements. C'est ce qu'on a constaté en opérations dans de nombreux cas. Le facteur de mutualisation de la sécurité dans ce cas semble fonctionner à fond, avec une amélioration globale des systèmes de signature.

Où en est-on de la virtualisation des appliances ?

Selon Patrice Clair (Sophos), 80% des XG firewalls sont vendus en mode appliance, et 20% en mode virtualisé. Pour lui les avantages du Cloud vont être de pouvoir faire du scale up ou scale down rapidement. Mais in fine, c'est la politique de sécurité décidée par le client qui va déterminer le niveau de sécurité.
Idem chez Fortinet, où Christophe Auberger nous parle d'un ratio 80/20 entre les appliances et la virtualisation. Fortinet propose le FortiGate (Firewall), FortiManager (console d'administration), FortiAnalyser pour l'analyse des logs et FortiSIEM pour la partie SIEM, qui sont disponibles « on-premise » ou en mode « Cloud » (notamment AWS).

Jérémie Schram, WatchGuard.

Christophe Auberger est Cybersécurité évangéliste France pour Fortinet.

Il note également : « *Aujourd'hui il y a un engouement pour le SD-WAN* » (software-defined wan). Il poursuit : « *On trouve de la 5G, du MPLS... L'intérêt du SD-WAN est d'avoir un réseau agile, flexible, évolutif. Cela ne doit pas se faire au détriment de la sécurité.* ».
Concernant Stormshield, Mathieu Bonenfant précise « *90% de nos appliances sont encore vendues en mode hardware. Le risque avec la virtualisation, c'est qu'Il faut pouvoir maîtriser l'ensemble des composants, or un équipement virtualisé va être dépendant de l'hyperviseur et du hardware sous-jacent. De plus l'administration d'un hyperviseur peut être consommateur de ressources pour certaines entreprises. C'est pourquoi les clients se tournent de préférence vers des machines virtuelles déployables dans Azure ou AWS.* ». Stormshield propose des solutions virtualisées depuis 2010 et depuis 2018 des instances « élastiques » qui permettent d'allouer à chaud des ressources en VRAM ou VCPU.

Des appliances compatibles avec les « majors »

Tous les éditeurs affirment avoir des appliances compatibles avec les trois majors : AWS, GCP, Microsoft Azure. Il n'est plus question de parler d'indépendance des données, mais de haute disponibilité, et avec les milliards investis par ces 3 éditeurs américains, le dimensionnement des infrastructures semble garanti.
Reste qu'on nous évoque l'existence de milliers de machines virtuelles hébergées en datacenter sur une seule machine physique (ou appliance). Techniquement se pose alors la question de la confidentialité des instances, et de la disponibilité du serveur. AWS, Google Cloud proposent des solutions dédiées en surcouche de virtualisation. Les éditeurs d'appliances ont eux aussi pris en compte ces problématiques.
Qu'en est il de la sécurité des appliances elles-mêmes ? Off-the-record, on nous parle de noyaux linux « custom », de pentests réguliers et de partenariats avec l'Anssi.
A savoir que les produits Stormshield de la gamme SNS, sont qualifiés au niveau standard de l'Anssi (diffusion restreinte). « *C'est un investissement important,* souligne Mathieu Bonenfant, *qui permet de démontrer la robustesse de nos technologies. Le process d'évaluation lié à la qualification s'appuie notamment sur du test de vulnérabilités, de l'audit de code source mais aussi de l'audit organisationnel* ». Ce qui semble nécessaire pour satisfaire aux exigences de leurs nombreux clients « OIV » et administrations. Stormshield revendique plus de 15000 clients et un réseau de 800 intégrateurs.

La sécurité de bout en bout

Pour Jérémie Schram (WatchGuard), « *les solutions les plus simples ne doivent pas être délaissées au profit des solutions de pointe, elles restent fondamentales : il faut penser à la visibilité, à la configuration des équipements (fine-tuning). Il faut penser aux failles humaines, il faut penser à patcher son infra contre les dernières CVE.* »
Selon Christophe Auberger (Fortinet), pour parer aux risques engendrés par la virtualisation, « *il faut intégrer la sécurité dès la conception du système, du réseau virtuel. Peu importe l'environnement de destination, Cloud ou physique, il faut déployer la sécurité en même temps qu'on déploie le projet. C'est la sécurité de bout en bout. On cherche à sécuriser la donnée. Le plan de sécurité doit être unifié. Il doit être imposé par la donnée. Quand on déploie sur Azure, AWS, quand on augmente la capacité du datacenter interne, il faut prendre en compte la sécurité de bout en bout. Le plan de sécurité doit être unifié et basé sur la donnée qu'on cherche à protéger* ».

Les **conseils** d'un intégrateur

Nous avons également recueilli le point de vue d'un intégrateur avec le partage d'expérience de Orange Business Services (OBS) sur ses offres d'hébergement et de virtualisation dans un contexte multi-Cloud.
Pour ses offres de confiance, OBS s'appuie sur l'expérience de Orange CyberDefense.

Selon Cédric Prevost, directeur « Solutions de confiance » au sein de la BU Cloud, OBS propose des offres de Cloud « Orange » et s'intègre aussi dans des offres de Cloud tierces parties. il faut penser les solutions de sécurité dans un monde « multi-cloud ». OBS a des offres de Cloud souverain, et, pour répondre aux besoins de ses clients « OIV » (« opérateurs d'importance vitale »), a développé une offre « CCOE » : Cloud Center Of Excellence, pour s'intégrer chez le client et offrir des services d'accompagnement des opérations Cloud.
Pour Christophe Dernys, directeur Build Solutions de confiance au sein d'Orange CyberDefense, « *Orange CyberDefense est le bras armé d'Orange en cybersécurité.* » Ils comptent 3000 experts, et 700 millions d'euros de chiffre d'affaires. Leur métier va être de préserver voire d'améliorer le MCS (Maintien en conditions de sécurité) de leurs clients, par l'accompagnement en sécurité, par l'intégration de solutions Cloud (y compris équipements de filtrage par exemple), et enfin par l'intégration de cyber-SOC pour détecter les menaces en temps réel chez leurs clients.
OBS propose deux offres de services « Cloud » : Flexible engine qui est un cloud public avec un hub de service sur une souche openstack, proche de Zscaler, et Flexible computing advance qui est un cloud public sur souche technologique VMware.
Le niveau suivant, c'est quand un client veut protéger en autonomie un service hébergé chez eux. C'est ce qu'on appelle « cyber protection express » (CPE).
En matière de technologies de filtrage, OBS va proposer des solutions Stormshield, Fortinet, Vadesecure... « *Il n'y a pas que des solutions open source. Tout est mis en œuvre et opéré par les équipes orange. Cela apporte toutes garanties possibles d'indépendance* » nous explique Christophe Dernys.

Quelles sont les tendances dans la virtualisation ?

« *On voit une vraie tendance à accumuler plusieurs instances de firewalls sur une même appliance. Avant les clients se retrouvaient avec 4 ou 5 clusters pour sécuriser des zones différentes. Aujourd'hui les clients investissent sur une grosse infrastructure physique, et ils virtualisent les firewalls, tous sur une même appliance physique. Sur un même boîtier hardware, on va avoir un firewall qui sécurise les accès web, les réseaux partenaires. Donc différentes zones de sécurité sur une même appliance* ».
« *Dans ce contexte, l'étanchéité est essentielle pour sécuriser le trafic* « est -ouest » *(interne au datacenter). Cette étanchéité va être garantie, soit par l'appliance propriétaire, soit par des éditeurs spécialisés. On peut citer Trend micro deep security, ou encore Aqua security qui sont capables de sécuriser les microservices.* »
Mais selon Christophe Dernys « *la grande tendance c'est les micro services. On explose les systèmes en différents services* ». « *Le vrai risque c'est le risque de rebond. Usurper un niveau d'authentification et rebondir sur d'autres machines plus sensibles. Avec les micros services cela peut prendre encore plus de proportions* ». C'est dans ce contexte que OBS propose des tests d'intrusion réguliers à tous ses clients Cloud.
Pour Cédric Prevost : « *la vraie sécurité des applications cloud, et donc l'efficacité de la protection des réseaux dans un contexte de virtulisation, cela va être le* « cloud native » *qui va permettre le* « security by design ». *Il faut penser la sécurité et l'intégrer dès le début du projet* ».

Pour sécuriser la console de management, l'accès aux appliances, Il faut sécuriser l'authentification des users. Comme l'explique Ivan Rogissart (Zscaler): on va utiliser l'IdP (identity provider) de nos clients pour les authentifier sur nos solutions. Cela permet d'obtenir un niveau de gestion d'identité et d'accès satisfaisants. Ce sera par exemple du SAMLV2 avec de l'authentification multifacteur.

Même constat chez Zscaler : « *Pour répondre aux problématiques de sécurisation des services cloud, La politique de sécurité de Zscaler est de l'authentification et du multitenant. Il y a des rôles et des permissions basées sur l'identité pour gérer les privilèges de la personne. Toutes les actions sont loggées* » nous explique Ivan Rogissart.

Selon lui Zscaler permet d'adresser deux problématiques: les applications se déplacent vers le cloud. De plus les utilisateurs ne se connectent pas toujours depuis le LAN, mais depuis des tablettes, mobiles, pc portables, différents réseaux.

Zscaler a été créé en 2008. Dans ces conditions de « data in motion », il faut des solutions spécifiques qui dépassent la sécurité périmétrique.

A partir de 2010, Zscaler a deployé ses solutions de sécurité dans des datacenters en mode SaaS. Aujourd'hui Zscaler dispose de 150 datacenters répartis dans le monde. Ils traitent 100 milliard de connexion quotidiennement (30 milliards il y a 3 ans), avec 2 offres de service : Zscaler internet access, pour la protection internet (à destination de services logiciels « SaaS »), et Zscaler private access, pour faire accéder des utilisateurs authentifiés à des applications hébergées dans un cloud privé (Zscaler security Cloud).

Selon Ivan Rogissart, aujourd'hui la tendance est au SD-WAN, qui donne une intelligence de routage. Cela permet de sélectionner les réseaux et d'avoir un accès plus rapide aux applications.

Le cœur du métier de Zscaler est de s'occuper du filtrage pour « nettoyer » le trafic. Cela permet de vérifier qu'il n'y a pas de malware (IDS) et qu'il n'y a pas de « data leaks » (DLP). Dans ce contexte l'interception HTTPS est primordiale pour analyser le trafic.

Visualiser le risque Zero Day

Un exemple de détection de malware: pendant la crise virale « NotPetya » et « Wannacry », Zscaler a activé la « cloud sandbox » gracieusement pour leurs clients. Ils ont pu bloquer un grand nombre d'attaques pendant 120 jours, le temps pour les attaques basées sur des variantes de s'estomper. Certains clients ont gardé l'offre de « cloud sandbox » même après la crise car elle leur a permis de visualiser le risque des « Zero days » circulant dans leur SI.

A noter que cette fonctionnalité de « sandbox » est disponbile également chez Stormshield, WatchGuard, et tous les éditeurs du marché... Dans ce contexte, comment choisir entre ces solutions ? Fortinet nous annonce avoir remporté un important contrat chez un fournisseur de logements de vacances & loisirs. A regarder le communiqué, on voit que toute la gamme de solutions est prévue pour le déploiement : « *FortiGate, FortiMail, FortiClient (...)* ». C'est l'un des arguments forts des éditeurs, qui, pour déployer leur « sécurité unifiée » avec corrélations d'évènements, vont proposer l'ensemble de leurs solutions.

De ces nombreux entretiens nous retiendrons quelques tendances. En premier lieu la notion de sécurité périmétrique se transforme vers une notion de protection de la donnée pour les utilisateurs. On va ainsi vers une protection « contextuelle ».

Ensuite, il faut souligner un fort développement du SD-WAN. Enfin, le déchiffrement HTTPS reste bien entendu indispensable.

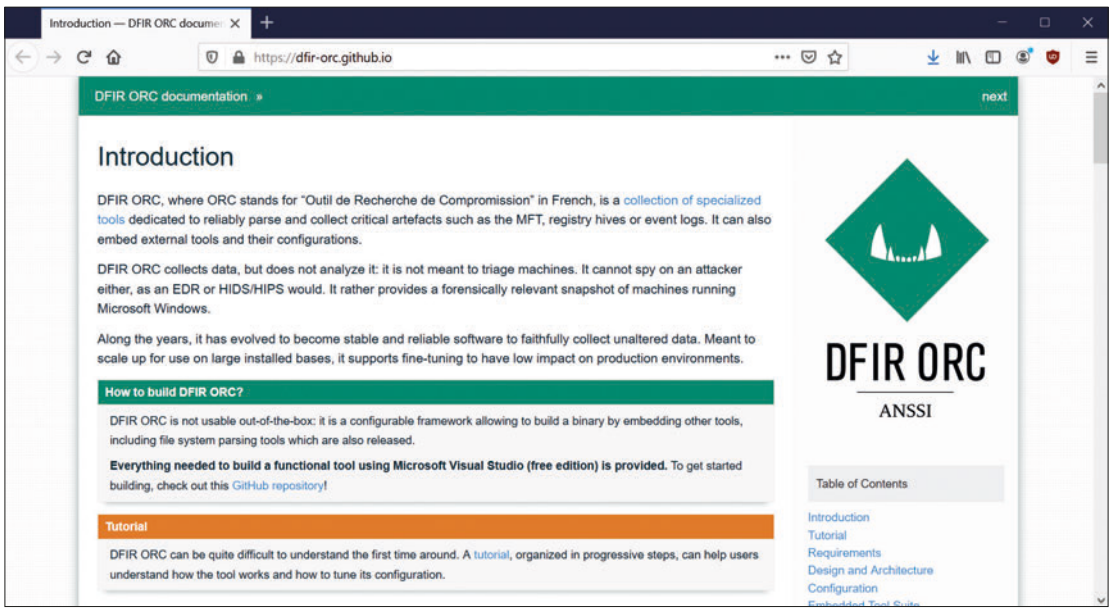
Au final on voit que dans un contexte de mobilité des données et des utilisateurs, de virtualisation, de pervasivité des réseaux, l'évolution des menaces nécessite plus que jamais des équipements de filtrage « intelligents » et une coopération entre les éditeurs du marché.

Julien Alis

Ivan Rogissart, responsable des ingénieurs avant-vente pour l'Europe du sud chez Zscaler.

L'ANSSI a publié dans l'open source le code d'ORC, son outil de collecte de données forensiques

L'Agence nationale pour la sécurité des systèmes d'information (ANSSI) a publié fin septembre 2019 sur son compte GitHub les sources de DFIR ORC, conçu pour récupérer les données criminalistiques dans les parcs Windows. Dans quelles conditions peut-il être exploité ? Comment le mettre en œuvre et le configurer ?



Vous trouverez sur le compte GitHub de l'Anssi (https://github.com/DFIR-ORC/dfir-orc) les sources d'ORC ainsi que la documentation de l'outil.

ORC (pour Outil de Recherche de Compromission) a été conçu en 2011 et n'a cessé depuis d'évoluer pour regrouper un ensemble d'outils permettant la recherche, l'extraction et la mise à disposition de données forensiques, tout cela dans un environnement Microsoft Windows (uniquement). DFIR Orc (DFIR veut dire Digital Forensics and Incident Response) est capable de récolter des données sur des parcs de très grande taille.

Il a été développé dans le cadre de la lutte contre les APT (Advanced Persistent Threats), des attaques caractérisées par leur haut niveau de furtivité et de continuité d'infection. Elles sont le plus souvent le fruit du travail de groupes de pirates très organisés, capables d'exploiter rapidement des failles de sécurité inconnues (les fameuses Zero-day), ce qui rend leur détection d'autant plus complexe. L'outil, intégralement libre, est aujourd'hui publié par l'agence à l'usage des acteurs et des professionnels de la « communauté » (entendez par là tous ceux qui s'intéressent à la problématique de la cybersécurité). C'est donc pour faire face à ces fameux APT, apparus il y a près de 10 ans, que l'Anssi a adapté sa méthodologie et son outillage. DFIR ORC est directement issu de cette démarche et n'a cessé de se développer depuis afin de mieux s'adapter aux besoins en matière d'investigation et de réponse à incident. Créé et utilisé de longue date par les équipes de l'Anssi, le logiciel de collecte DFIR ORC a été conçu afin de fonctionner de façon décentralisée et à grande échelle. « *Après 8 ans d'usage, DFIR ORC a été utilisé sur plus de 150 000 postes dans le cadre de nos activités opérationnelles en matière de réponse à incident.* » dixit François Deruty, le sous-directeur Opérations de l'Anssi. En s'engageant dans une démarche claire d'ouverture avec la communauté de la sécurité numérique, l'Anssi souhaite aujourd'hui partager cet outil mature qu'elle utilise au quotidien depuis plusieurs années. Elle veut profiter ainsi de l'émulation de la communauté et l'a pour cela publié sous licence LGPL 2.1+.

A qui s'adresse DFIR ORC ?

DFIR ORC s'adresse aux professionnels de la sécurité informatique soucieux d'acquérir les données nécessaires à la réponse aux incidents de sécurité de façon fiable, mais aussi à tous les développeurs qui souhaiteront s'en inspirer ou contribuer à son développement. ORC peut être déployé sur l'intégralité d'un parc Microsoft Windows, tout en minimisant l'impact sur son fonctionnement normal. Il assure ainsi la collecte des informations souhaitées en respectant de grandes exigences en termes de fiabilité, de qualité et de traçabilité, sans modifier la configuration des machines analysées et en réduisant au maximum les risques d'altération des données collectées.

DFIR ORC permet donc de disposer d'une vision de l'état du parc au moment de la collecte. Son rôle s'arrête là. Il n'a pas été conçu pour analyser les données collectées. Cette tâche reste celle de spécialistes disposant de leur méthodologie propre et d'outils adaptés. DFIR ORC est un outil modulaire, configurable, capable d'embarquer d'autres outils, ceux proposés par l'agence mais pas seulement. Avec la publication dans l'Open Source d'ORC, l'Anssi partage le code source, la procédure de compilation ainsi que des exemples de configuration de l'outil. Tous ces éléments permettent la génération d'un outil fonctionnel adapté à l'usage souhaité, comme montré un peu plus loin dans cet article. « *À travers DFIR ORC, nous avons l'ambition de contribuer activement à la vie de la communauté de la réponse à incident, en lui permettant de s'approprier et de développer l'outil à sa manière* », précise François Deruty, sous-directeur Opérations à l'Anssi.

Connaissez-vous le mystère du logo de l'Anssi ? Non ? Et bien cherchez, alors...

Un seul objectif : le partage de connaissances

L'Anssi, encore une fois, souhaite encourager l'émergence d'une communauté publique de développeurs et d'utilisateurs de l'outil, ceci en vue de favoriser sa montée en maturité et de créer de nouvelles fonctionnalités. L'agence continuera bien entendu à développer de son côté DFIR ORC et publiera régulièrement des mises à jour accessibles à tous. L'Anssi invite tous les acteurs de la communauté à enrichir dès à présent ce projet en collaboration avec ses équipes, comme pour tout bon projet open source. L'agence soutient également le projet de Campus de la cybersécurité, porté

Commandes de compilation

Les versions 32-bit et 64-bit devraient toutes deux être compilées pour garantir un maximum de compatibilité avant le déploiement. Dans le terminal pour développeur de Visual Studio (et non dans le cmd classique de Windows), tapez les **commandes suivantes** :

```
git clone --recursive https://github.com/dfir-orc/dfir-orc.git
cd dfir-orc
mkdir build-x86 build-x64
cd build-x86
cmake -G "Visual Studio 16 2019" -A Win32 -T v141_xp -DORC_BUILD_VCPKG=ON ..
cmake --build . --config MinSizeRel -- -maxcpucount
cd ../build-x64
cmake -G "Visual Studio 16 2019" -A x64 -T v141_xp -DORC_BUILD_VCPKG=ON ..
cmake --build . --config MinSizeRel -- -maxcpucount
```

Cela change un peu si vous utilisez VS 2017 au lieu de VS 2019. L'option « -T v141_xp » de l'avant-dernière ligne permet d'assurer la compatibilité avec Windows XP SP2 et les versions ultérieures de Windows (et antérieures à Windows 10). Vous pouvez donc l'omettre si ce n'est pas nécessaire dans votre cas de figure. L'option ORC_BUILD_VCPKG=ON compilera les packages vcpkg dans le répertoire external/vcpkg.

par Michel Van Den Berghe (lire article dans ce numéro), visant à réunir et à renforcer l'ensemble des acteurs de l'écosystème français de la cybersécurité. L'agence apportera au projet son expertise en matière de sécurité numérique. « *Le Campus de la cybersécurité offre une belle opportunité pour décloisonner les activités publiques et privées. Il jouera un rôle important de catalyseur et de vitrine internationale du dynamisme et de l'engagement de l'écosystème français* », selon Guillaume Poupard, directeur général de l'Agence de sécurité. L'Anssi est convaincue de l'importance de s'ouvrir à d'autres écosystèmes, notamment ceux de l'enseignement et de la recherche pour répondre au défi du passage à l'échelle de la sécurité numérique en France. « *Le concept même de cybersécurité doit évoluer, afin d'être perçu favorablement par toutes et tous. Les professionnels de la sécurité numérique doivent assumer un rôle de conseil et d'accompagnement des projets, surtout les plus innovants en la matière.* » Il faut viser l'intégration de la sécurité dès le début des projets logiciels. L'objectif avoué est d'assurer une compatibilité entre les usages et la sécurité, sans pour autant freiner l'innovation. « *La politique de la terreur a trouvé ses limites ! Nous devons aller vers une sécurité numérique toujours plus ambitieuse, à la hauteur des menaces, mais également plus positive, en phase avec les usages numériques modernes. Nous devons collectivement prioriser l'accompagnement et le conseil au plus près des projets, en associant tous les décideurs et responsables, dont les préoccupations naturelles ne sont pas encore la cybersécurité* », a encore déclaré Guillaume Poupard.

Des outils spécifiques de collecte, mais pas d'analyse

Ces outils sont clairement destinés aux professionnels de la sécurité informatique et n'ont rien de grand public. Ils ne peuvent d'ailleurs pas être utilisés tels quels et nécessitent un fichier de configuration adapté (au format XML). Ils permettent de connaitre l'état à un instant t d'un parc, mais ne s'occupent, encore une fois, que de récupérer des données, pas de les analyser. L'Anssi assure qu'ORC réalise ses opérations « *en minimisant l'impact sur le fonctionnement normal d'un parc Microsoft Windows* » et « *les risques d'altérations des données collectées* ». ORC ne modifie ainsi pas la configuration des machines analysées.

De l'open source, encore et encore

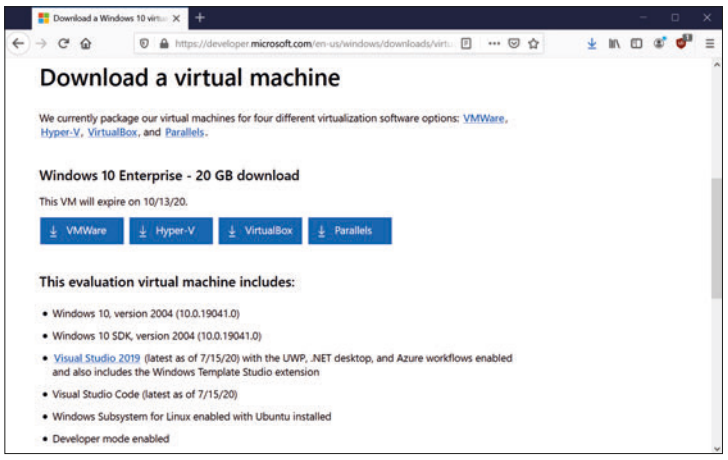
L'Anssi s'investit en effet plus massivement que jamais dans le logiciel libre ces dernières années. ORC est publié sous licence LGPL 2.1, une licence open source particulièrement souple puisqu'elle permet de lier sans contrainte le code open source à du code propriétaire. La version fournie est la 10. Le choix de l'agence de libérer les sources n'est en effet pas anodin. Elle veut prolonger un cercle vertueux déjà initié avec d'autres outils comme le système d'exploitation Clip OS (cf encadré) ou WooKey, un projet de disque externe sécurisé (https://wookey-project.github.io/architecture.html), pour ne citer qu'eux. C'est aussi une bonne méthode pour créer une émulation autour de ses outils dédiés à la sécurité et permettre, par exemple, de repérer de nouveaux talents. En dehors de ces sorties relativement récentes, le dépôt GitHub de l'agence de sécurité (https://github.com/DFIR-ORC/dfir-orc) compte actuellement plus d'une quarantaine de projets open source, la plupart sous licence GPL 3.0 et d'autres sous licence BSD.

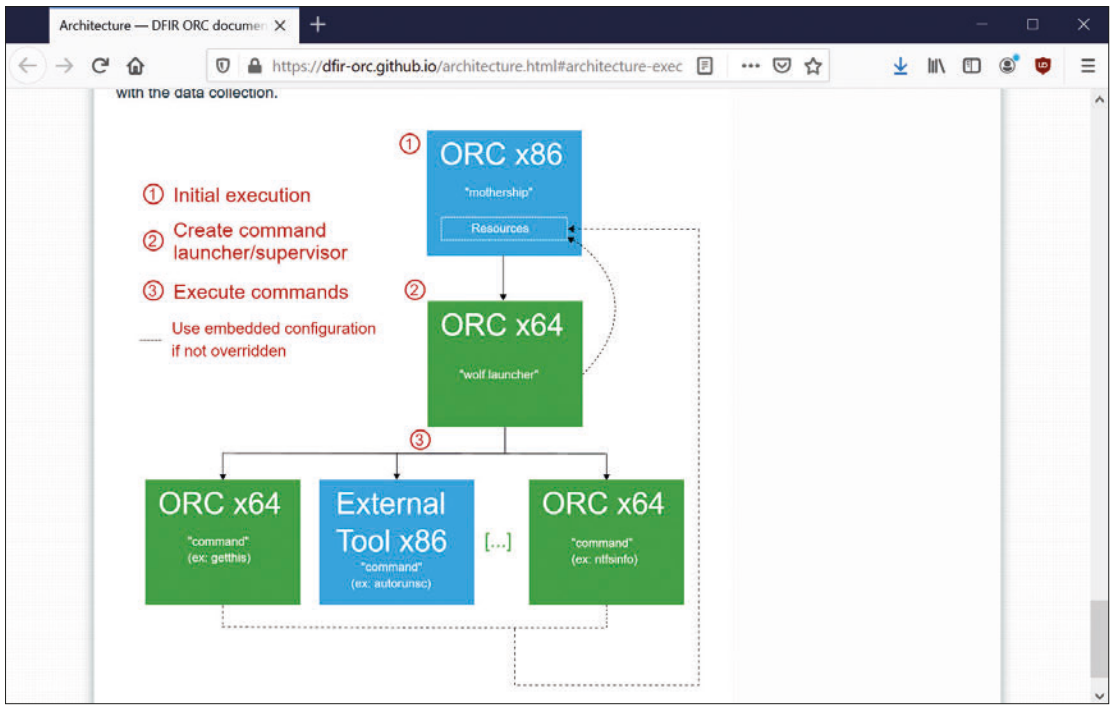
Vous pouvez gagner beaucoup de temps en ce qui concerne la configuration de l'environnement de compilation en téléchargeant des machines virtuelles pour développeurs prêtes à l'emploi depuis cette adresse : https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/

Configuration du logiciel DFIR ORC

Pour configurer DFIR ORC, il faut :

- des fichiers de configuration au format XML, enregistrés dans le répertoire config ;
- des éléments à intégrer (particulièrement les binaires 32 et 64 bits de DFIR-Orc), stockés dans le répertoire tools.





Un binaire non configuré contient tout ce qui est nécessaire pour orchestrer la collection d'artefacts, comme illustré à l'adresse https://dfir-orc.github.io/architecture.html#architecture-exec

Les configurations données ici comme exemple utilisent l'outil Autorunsc des Sysinternals. Pour les reproduire, vous devez le télécharger et le placer dans le répertoire tools. Vous le trouverez, avec le reste de la suite, à l'adresse https://docs.microsoft.com/en-us/sysinternals/. Ne le récupérez surtout pas à une autre adresse, non gérée par Microsoft, comme Softonic ou autres sites malveillants. Vous risqueriez fort d'avoir un petit « cadeau » à l'intérieur. Le répertoire tools doit, par conséquent, contenir les fichiers suivants :

- DFIR-Orc_x64.exe
- DFIR-Orc_x86.exe
- autorunsc.exe

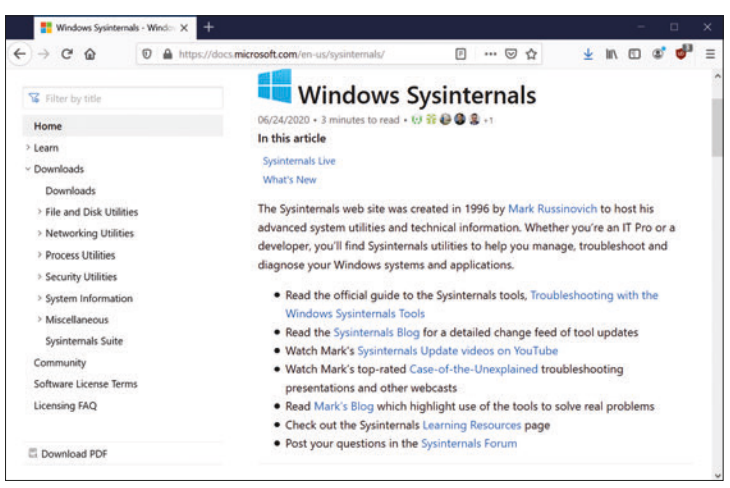
Enfin, pour générer un exécutable DFIR-Orc configuré, vous devez exécuter le script *.\Configure.cmd* sur un système Windows depuis un terminal Windows cmd classique ou powershell en mode Administrateur, comme on dit chez Microsoft. Le binaire généré est créé dans le répertoire output.

Outils nécessaires à la compilation d'ORC

Voici les quelques outils indispensables pour compiler OrRC:

- Visual Studio version 2017 ou ultérieure (ce sera bien plus simple avec VS 2019) ou, éventuellement, les vstools (https://visualstudio.microsoft.com/fr/downloads/);
- CMake de Kitware version 3.12 ou supérieure ou la version intégrée à Visual Studio ;
- Clang Format de LLVM version supérieure à 8.0.0 ou la version intégrée à Visual Studio 2019 16.3 (ou ultérieure).

L'environnement de compilation peut être défini rapidement (et donc facilement) en employant des machines virtuelles pour développeurs de Microsoft (https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/). Vous pouvez importer le dossier de configuration prédéfini .vsconfig disponible à l'adresse https://github.com/DFIR-ORC/dfir-orc/blob/master/.vsconfig directement depuis l'outil Visual Studio Installer.



Pour reproduire l'exemple de cet article tiré du tutoriel officiel d'ORC, vous devez télécharger l'outil Autorunsc.exe des sysinternals depuis le site de Microsoft.

ClipOS

L'Anssi avait ouvert en 2018 le code source de son système d'exploitation « durci » Clip OS. Celui-ci a pour rôle de séparer les activités triviales des plus sensibles, en partant du cœur du système jusqu'à l'interface utilisateur. Cette action avait été réalisée dans le cadre du plan d'action de l'Open Government Project. Utilisé par l'administration et des opérateurs dits « d'importance vitale » (OIV) depuis plusieurs années, il a été complétement réécrit. Son principe est simple : il offre deux environnements de travail séparés, l'un pour la navigation Internet classique et les opérations banales, l'autre pour obtenir et traiter des documents sensibles. Dans le jargon de l'Anssi, ces deux « cages » sont de niveau « bas » et « haut ». Cette séparation est au cœur de Clip OS, qui cloisonne autant que possible les processus, en leur retirant tous les privilèges qui peuvent l'être. La racine du système est impossible à modifier une fois celui-ci lancé. Les bureaux sont dupliqués et même le serveur audio et le copier-coller sont cantonnés à chaque niveau.

Options

Il est recommandé d'employer les options par défaut sauf pour ORC_BUILD_VCPKG qui doit être positionné sur ON afin que les dépendances soient construites automatiquement à l'aide de vcpkg. Pour connaître les valeurs par défaut de quelques options, parmi les principales, consultez le tableau ci-contre.

Le tutoriel officiel détaille en profondeur les étapes permettant d'obtenir un binaire DFIR ORC configuré et prêt à être déployé. Il explique quel code compiler, comment intégrer une configuration, comment modifier une configuration, quelle est la différence entre compilation et configuration. Tout doit être réalisé dans un environnement Microsoft Windows. Seule la première étape nécessite la compilation avec Visual Studio (l'édition gratuite, Community, est suffisante). Les binaires (programmes exécutables), qu'ils soient ou non configurés, requièrent des droits de niveau administrateur. Les commandes qui suivent doivent elles aussi être exécutées dans un terminal Powershell avec des droits de niveau administrateur. Il est possible – mais guère intéressant – de les adapter quelque peu pour les exécuter dans un terminal Windows classique (cmd) avec les mêmes droits.

Compilation

Cette étape est la seule qui requiert une compilation avec la chaîne d'outils (toolchain) de Microsoft. Les instructions pour compiler ces fichiers à partir du code source sont détaillées un peu plus haut. La compilation du code source pour *DFIR ORC* produit ce qui est appelé des binaires non configurés, nommés normalement DFIR-Orc_x86.exe (pour le 32-bit) et DFIR-Orc_x64.exe (pour la version 64-bit). Un binaire non configuré contient tout ce qui est nécessaire pour orchestrer la collection d'artefacts (comme illustré à cette adresse https://dfir-orc.github.io/architecture.html#architecture-exec). Il contient également la suite d'outils intégrés incluse par défaut.

Configuration

Après la première étape, plus aucune compilation n'est requise. Pourquoi est-il nécessaire de définir une configuration ? Un binaire est simplement un ensemble d'outils avec un moteur de recueil de données. Par conséquent, la liste des artefacts à récolter et la manière de le faire n'ont jusqu'alors pas été définis. C'est cette liste d'éléments à collecter qui représente précisément ce qu'est une configuration. L'étape décrite ci-dessous détaille comment obtenir un binaire configuré à partir d'un binaire non configuré et le dépôt des configurations existantes. Tout d'abord, il faut cloner la configuration par défaut, avec cette commande :

```
git clone https://github.com/dfir-orc/dfir-orc-config.git
cd dfir-orc-config
```

Ensuite, il faut copier les binaires non configurés DFIR ORC (DFIR-ORC_x86.exe et DFIR-ORC_x64.exe) dans le dossier tools grâce à ces commandes en powershell :

```
Copy-Item <Path>\dfir-orc\build-x86\MinSizeRel\DFIR-Orc_x86.exe .\tools
Copy-Item <Path>\dfir-orc\build-x64\MinSizeRel\DFIR-Orc_x64.exe .\tools
```

Afin d'illustrer la manière d'inclure des outils externes dans le framework DFIR ORC, voici un exemple de configuration utilisant autorunsc.exe qu'il faut bien évidemment télécharger depuis le site de Microsoft, comme mentionné plus haut.

```
Invoke-WebRequest https://live.sysinternals.com/autorunsc.exe -OutFile .\tools\autorunsc.exe
```

Puis exécutez la commande suivante, qui produit un binaire DFIR ORC configuré (nommé par défaut DFIR-Orc.exe) dans le répertoire de sortie :

```
.\Configure.cmd
```

Test de la configuration

Une fois que le binaire DFIR ORC configuré a été créé, vous pouvez le tester. Vous pouvez bien entendu l'utiliser pour exécuter un des outils intégrés, tout comme pour les programmes exécutables non configurés :

```
.\output\DFIR-Orc.exe NTFSInfo /out=C_drive.csv C:\
```

Cette commande va créer un fichier nommé C_drive.csv dans le répertoire courant avec l'énumération de la MFT (Master File Table) du volume C:. De manière similaire, GetThis peut être invoqué depuis la ligne de commande :

```
.\output\DFIR-Orc.exe GetThis /nolimits /sample=ntdll.dll /out=ntdll.7z C:\
```

Cette commande va créer un fichier appelé ntdll.7z dans le répertoire courant, contenant tous les fichiers ntdll.dll dans le volume C:. Cependant, les configurations ont été mises en place de telle sorte que les utilisateurs puissent écrire ces lignes de commande une fois pour toutes. Lorsqu'un outil est exécuté, ses résultats sont stockés dans un fichier d'archive. Le contenu de ces archives est déterminé par le fichier de configuration. Pour un binaire configuré donné, l'option keys liste toutes les archives qui peuvent être créées en fonction de la configuration intégrée. Voici ce que cela donne appliqué au binaire obtenu après exécution des précédentes instructions :

```
.\output\DFIR-Orc.exe /keys
```

Pour voir le résultat que produira cette commande, voir l'encadré ci-contre.

Thierry Thaureaux

À propos de l'Anssi

L'Agence nationale de la sécurité des systèmes d'information a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale. L'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité directe du Premier ministre. L'agence de sécurité gouvernementale s'ouvre clairement aux acteurs de l'écosystème numérique dans le but avoué de s'enrichir mutuellement en partageant les expertises, les capacités et les outils de chacun. L'Anssi s'est engagée dans une démarche open source, publiant de nombreux projets tels que OpenCTI, CLIP OS, WooKey ou, plus récemment, DFIR ORC. Suivant une logique d'ouverture, l'agence plaide pour le partage des données, en toute sécurité, afin d'accroître le niveau de connaissance de tous.

COMMENT PROTÉGER LES DONNÉES À CARACTÈRE PERSONNEL DE SES COLLABORATEURS TOUT EN FAVORISANT LE TÉLÉTRAVAIL ?

Par Marina Casas, Chargée de mission à l'AFCDP, et Paul-Olivier Gibert, Président de l'AFCDP.

Comment protéger les données à caractère personnel de ses collaborateurs tout en favorisant le télétravail ?

À l'heure où la crise sanitaire nécessite un recours massif au télétravail, qui semble devenir durablement une nouvelle norme, il ne faut pas perdre de vue les risques que cela implique pour les données personnelles des employés et la responsabilité des entreprises.

Quels sont les risques ?

Le télétravail permet au salarié de travailler hors des locaux de son entreprise, de façon volontaire, et en utilisant les technologies de l'information et de la communication de son entreprise (1).

En cas de circonstances exceptionnelles, ou de force majeure, le télétravail peut être imposé au salarié, sans son accord. Il est donc essentiel pour chaque organisme de mettre en œuvre un ensemble de règles concernant le télétravail, en vue de limiter les risques juridiques et relatifs à la sécurité des systèmes d'information et/ou des données.

En effet, pour éviter tout conflit d'intérêts entre le salarié et l'entreprise, il faut pouvoir permettre le cloisonnement entre vie privée et vie professionnelle dans un cadre de travail à domicile, tout en permettant au salarié d'avoir accès aux ressources professionnelles nécessaires pour travailler. De plus, l'entreprise doit se protéger de la compromission générale du système d'information de l'entreprise à distance, pour éviter toute fuite de données.

Quelles mesures préventives adopter ?

Le télétravail doit être encadré, dans la charte informatique de l'entreprise, annexée au règlement intérieur et/ou accord collectif pour lui donner une valeur contraignante, excepté dans le secteur public où le télétravail est fixé par arrêté. En l'absence de ces éléments, les parties peuvent formaliser un accord par tout moyen. Il faut ainsi prêter une attention toute particulière aux droits et obligations des salariés ainsi que des employeurs dans ce contexte de travail à distance. Cela nécessite une véritable analyse de risque, intégrant les aspects juridiques, techniques ainsi que les modalités de mise en œuvre du télétravail.

La charte informatique est essentielle puisqu'elle permet d'encadrer et de limiter ces risques. Elle facilite pour l'employeur le cloisonnement entre vie privée et vie professionnelle de ses salariés, en interdisant par exemple, l'utilisation des outils personnels à des fins professionnelles, ou au contraire, en rappelant les usages de base des outils informatiques à des fins personnelles (par exemple, inscrire dans l'objet d'un courriel l'indication « personnel » ou « privé »).

Pour des conditions plus spécifiques, le télétravail peut faire l'objet d'un guide détaillé, par exemple, sur les modalités de mise en œuvre en cas de circonstances exceptionnelles (horaires, etc.) combiné à la charte informatique. L'entreprise doit prévoir des assurances spécifiques en consultation avec les ressources humaines et être en mesure de mettre à disposition le matériel nécessaire pour le salarié afin de limiter l'utilisation de son propre matériel personnel.

Une procédure en cas de perte, de panne ou de vol du matériel et des données est recommandée.

La sensibilisation des salariés reste essentielle pour garantir la sécurité des données personnelles. Ils doivent notamment prêter une attention particulière aux accès à l'Internet, en particulier en cas d'usage du WI-FI public s'il leur est nécessaire.

En raison de la crise sanitaire actuelle, le télétravail se généralise, les entreprises s'efforcent de maintenir leur activité et peuvent perdre de vue les enjeux de cybersécurité liés au travail à distance et ceux de protection des données à caractère personnel. C'est là que le rôle du DPD/DPO (Délégué à la protection des données ou Data Protection Officer) prend tout son sens.

(1) Article L.1222-9 du Code du travail

Campus Cyber : ça se précise !

Le confinement n'a pas ralenti les travaux autour du projet du Campus Cyber, lieu qui doit rassembler l'écosystème français de la cybersécurité. Michel Van Den Berghe, a soumis au gouvernement cinq propositions de lieux dans la Petite Couronne parisienne, tandis que la structure juridique et de gouvernance du campus a été définie. Le projet est désormais suspendu à la décision gouvernementale.

La phase 2 du projet, lancée lors du FIC en début d'année, n'a pas été ralentie par la crise et les travaux pourraient démarrer en septembre prochain.

On pouvait penser que la crise sanitaire allait mettre un coup d'arrêt au projet de Campus Cyber porté par Michel Van Den Berghe. Au contraire, le confinement lui a permis d'avancer. Mandaté en juillet 2019 par le Premier ministre, alors Edouard Philippe, le patron d'Orange Cyber Defense avait pour première mission de mener une réflexion sur la faisabilité d'un tel projet, celui d'une structure capable de répondre aux problématiques posées en France par le milieu de la cybersécurité. Le secrétaire d'Etat au numérique, Cedric O, fixait trois objectifs : résoudre la pénurie de compétences en renforçant *« la sensibilisation et la formation »*, faciliter les interactions entre les différents acteurs de la cybersécurité en France, notamment par *« le partage et la mutualisation d'outils, de compétences et de données »* et enfin *« accompagner l'innovation publique et privée pour concourir au développement de la filière industrielle de cybersécurité, en cohérence avec le comité stratégique de filière sécurité »*.

Une soixantaine d'engagements fermes

Après une cinquantaine d'auditions, des discussions et des visites de campus similaires à l'étranger, Michel Van Den Berghe a remis fin 2019 son rapport de faisabilité au gouvernement, qui a étudié la question fin janvier, à la veille du FIC de Lille. Le projet entrait alors dans sa phase 2, celle de "l'opérationnalisation", pour reprendre les termes employés par le directeur de l'Anssi, Guillaume Poupard. Le patron d'Orange CyberDefense devait alors, au cours des deux mois à venir, recenser les organisations participatrices et les effectifs qu'elles veulent positionner dans ce lieu, de sorte à pouvoir enfin déterminer l'emplacement du campus. Il nous expliquait alors vouloir aller vite, visant un lieu déjà bâti, plutôt dans l'ouest parisien, avec une surface de 10 000 ou 15 000 m², à Paris même ou en proche banlieue et capable d'accueillir 500 à 1 000 personnes dès le premier trimestre 2021. Ce qui, considérant 10 mois de travaux pour *« aménager, câbler, cloisonner, sécuriser »* les lieux, laissait au porteur du projet jusqu'à avril pour présenter plusieurs options au gouvernement. Mais voilà, le 17 mars, la France se trouvait confinée, frappée par l'épidémie de Covid-19.

Pourtant, la crise n'a pas gêné outre mesure Michel Van Den Berghe. *« Nous avons profité du confinement pour réaliser une sorte de cahier des charges pour interroger les organisations intéressées sur le nombre de personnes qu'elles veulent y positionner, la typologie des équipes, les mètres carrés dont elles ont besoin... »* nous explique le CEO d'Orange CyberDefense. Résultat : une soixantaine de propositions d'engagement ferme, avec les "moteurs" du projet que sont Atos, Capgemini et Orange, des entreprises de taille moyenne à l'instar d'Advens et des startups, ainsi que des acteurs publics tels que l'Anssi et l'Acyma, des associations et même des groupes internationaux, plutôt européens, *« qui préfèrent prendre des bureaux au Campus Cyber plutôt que s'installer dans une tour de bureau anonyme »*. Car rappelons que ce campus ne sera pas une simple vitrine, occupée uniquement à l'occasion d'évènements quelques fois dans l'année, c'est du moins ce que souhaite Michel Van Den Berghe, et ce qui semble se concrétiser aujourd'hui.

Dans le vif du sujet

Le lieu sera avant tout un centre opérationnel où les acteurs publics et privés positionneront des équipes et des ressources. *« Bonne nouvelle, nous avons déjà des engagements forts de petites entreprises qui veulent y mettre toutes leurs équipes »* précise le patron d'OCD. Ainsi le Campus Cyber s'articulera autour de plusieurs grandes activités opérationnelles, à commencer par un "Observatoire de la menace cyber". *« Le marché numérique, et en particulier celui de la cybersécurité, est mené par trois composants : les hackers, la régulation et les modes. La France, si elle veut exister sur ce terrain, doit travailler sur la compréhension de la menace et je pense que nous avons une réelle expertise sur le sujet »* souligne Michel Van Den Berghe.

Par exemple, un groupe de travail intégrant de grandes banques réfléchit à la création d'un CERT inter-bancaire, CERT qui se positionnerait dans ce campus et qui agirait alors comme une zone neutre, où plusieurs acteurs habituellement en concurrence peuvent travailler ensemble. Des règles de bonne conduite viendront par ailleurs assurer la bonne entente entre tous ceux présents sur le campus, chacun pouvant en outre avoir sa "zone de confiance", avec un certain niveau de confidentialité quand bien même il se veut un lieu de partage. S'ajoute à cet observatoire des activités de formation, de recherche ou encore d'événementiel.

Ces activités, conjuguées à la soixantaine d'entreprises et d'administrations désireuses de s'installer dans le campus, aboutissent à un lieu de 17 000 à 20 000 mètres carré, où se côtoieront entre 800 et 1 000 spécialistes. Reste à définir le site approprié. *« J'ai visité plusieurs lieux et remis au gouvernement cinq propositions : trois à la Défense, une à Saint Ouen et une à Boulogne »* nous dévoile Michel Van Den Berghe. *« Pour chaque projet, nous sommes accompagnés par des promoteurs, des collectivités »*.

La structure juridique a elle aussi été choisie, une SAS jouera l'opérateur du Campus Cyber, tandis que la gouvernance sera assurée par le biais d'un « fonds de pérennité », un véhicule instauré par la loi PACTE, équivalent français des fondations d'actionnaires. Ne manque plus désormais que la décision politique qui entérinera le projet. Mais le dernier remaniement gouvernemental risque de retarder la mise en oeuvre du campus. *« J'attends maintenant la fumée blanche »* indique Michel Van Den Berghe. Une décision qui pourrait être prise par le président de la République lui-même.

Des Campus Cyber

La création du Campus Cyber ne sera néanmoins qu'une première étape. Au FIC, Michel Van Den Berghe nous expliquait se refuser à une démarche jacobine, mais pouvoir disposer, sur un même niveau, d'un réseau de campus. Il s'agit de "voir plus grand" avec dans la ligne de mire de nombreuses structures régionales. *« Nous avons des soutiens forts. La région des Hauts de France réfléchit à une unité satellite dédiée à la sécurisation des PME et PMI, tandis que les Pays de Loire sont sur la partie smart cities, et la Bretagne surtout tout ce qui touche à la défense et aux activités sensibles. Nous regardons à l'extérieur de Paris et avons déjà des accords tacites avec plusieurs régions »*".

L'un des projets actuellement présenté est de créer un premier campus cyber à deux jambes, l'une dans la proche banlieue de Paris pour les activités surtout tertiaires, c'est le projet qui attend le feu vert du gouvernement, et une autre sur le plateau de Satory, dans les Yvelines, pour la cybersécurité du secteur industriel et les activités qui exigent plus de surface. *« Il ne faut pas rater le coche, insiste Michel Van Den Berghe. Le secteur de la cybersécurité représente des milliers d'emplois à créer, nous avons besoin d'avoir de l'expertise, de créer des vocations »*. Et pour ce faire, le campus incarnerait un véritable totem, une marque attractive, tant et si bien que *« les experts demanderont à leurs dirigeants pourquoi ils ne sont pas au Campus Cyber »*. La volonté des industriels est réelle et le patron d'Orange CyberDefense se dit prêt à démarrer les travaux dès septembre prochain, de sorte à tenir le calendrier initial et d'avoir un lieu prêt à accueillir les entreprises dès la fin du premier trimestre 2021. Encore faut-il qu'une décision politique soit prise rapidement, mais le porteur du projet se veut confiant et espère *« pouvoir entrer dans le concret au moment des Assises de la Sécurité »*, qui se tiennent à Monaco du 14 au 17 octobre.

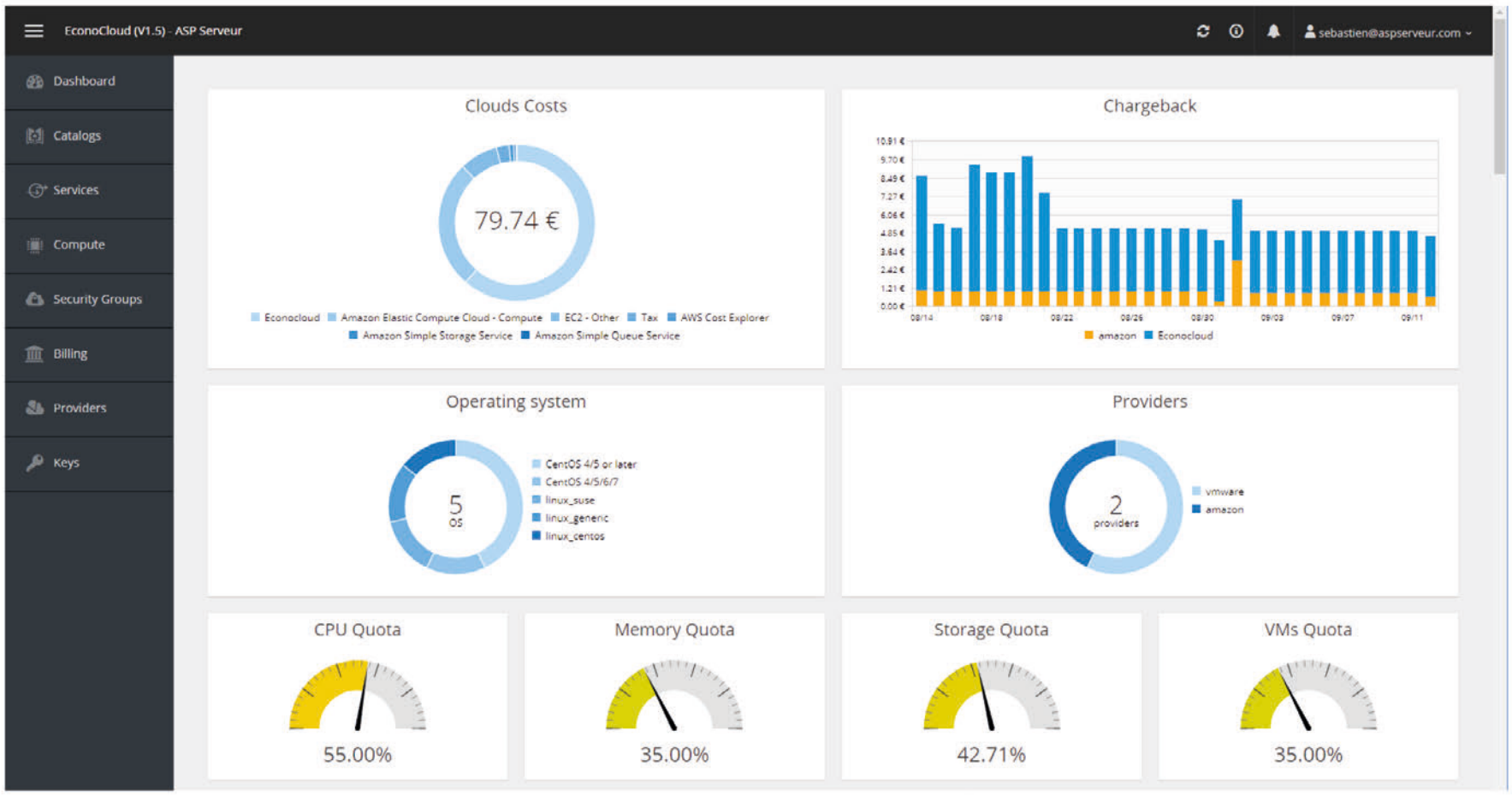
G. P.

Beer Sheva, l'exemple israélien

Parmi les structures servant d'inspiration au Campus Cyber français, l'exemple de Beer Sheva est l'exemple le plus fréquemment cité. Situé dans le désert du Neguev, ce centre dédié à la cybersécurité concentre les acteurs clés du secteur en Israël, privés et publics. On y trouve aussi bien un centre d'affaires, nommé Cyber Spark, où se regroupent la majeure partie des sociétés, que la chaire dédiée à la cybersécurité de l'Université Ben Gourion ou encore les locaux de la branche cyberguerre de l'armée israélienne. Plusieurs géants internationaux, à l'instar d'Oracle ou d'IBM, s'y sont également installés. Et si Beer Sheva semble surtout servir de vitrine à la cybersécurité israélienne, il est indéniable que tout l'écosystème profite de cette proximité physique et de l'émulation autour de ce lieu. L'écosystème français espère qu'il en ira de même au sein de son Campus Cyber.

econocloud

Votre Cloud Management Platform par Econocom



Connect

Permet nativement le multi-cloud et l'hybridation.
Connectez les principaux Cloud publics, hyperviseurs et orchestrateurs.

Manage

Vos ressources sont auto-découvertes.
Vous pouvez les administrer dans le portail unifié ou les présenter dans le catalogue de service en créant des templates.

Report

Le dashboard vous permet de consulter vos consommations et les coûts associés. Comparez et optimisez vos charges chez vos fournisseurs de Cloud.

Inscrivez-vous gratuitement à l'adresse econocloud.fr

ASPSERVEUR | ECONOCOM SAS. SIRET 45177725400033. 785 voie Antiope, 13600 La Ciotat. Email : info@econocloud.fr Tel : 0805 360 888

Démultipliez la puissance de votre cybersécurité

Nos solutions basées sur des technologies EDR permettent de prévenir et détecter les attaques complexes, à la vitesse de l'éclair, sans demander d'effort supplémentaire à votre équipe.

Kaspersky
Endpoint Detection
and Response

kaspersky BRING ON THE FUTURE *

kaspersky.fr