JANVIER 2023

LIVRE BLANC

MANQUE DE RESSOURCES EN CYBERSÉCURITÉ : QUELLES SOLUTIONS ?

GLIMPS

TABLE DES MATIÈRES

Déploiement du télétravail, complexité des SI :

un contexte favorable aux cyberattaques

Un peu plus de deux ans après le début de la pandémie, l'heure est à un premier bilan. Déploiement du télétravail, recours au cloud, environnements informatiques de plus en plus complexes… Gérer son système d'information (SI) nécessite d'avoir plus massivement recours à une nouvelle génération d'outils, à l'image des SOC et des SIEM.

La tendance de fond observée depuis quelques années ne se dément pas : les incidents critiques ne cessent de croître au sein des organisations. En 2021, 54% des entreprises françaises ont été attaquées et les rançongiciels ont augmenté de 95% [Cybermalveillance.gouv.fr 2022 ; CESIN 2022 ; Stoïk, 2022]. Toutes les organisations ; tous les secteurs sont impactés, générant d'importants changements dans l'approche des DSI en termes de sécurité.

Dès 2020, un contexte pandémique favorable à l'abaissement des barrières de sécurité

Comment expliquer ce qui s'apparente bel et bien à une rupture ? Le contexte a souvent été évoqué – à raison – afin d'expliquer cette évolution [Deloitte, 2020]. Dès les premiers mois de l'année 2020, la pandémie mondiale de la Covid-19 a entraîné un recours massif au télétravail, et donc à la digitalisation des usages. Au sein de chaque foyer, une interpénétration nouvelle a été observée entre les univers professionnels et personnels. Les entreprises ont dû revoir les organisations et lever de nombreuses barrières. Le résultat ne s'est pas fait attendre : autrefois conçu comme un château-fort, le Système d'Information (SI) a vu ses murs protecteurs s'abaisser et la sécurité informatique s'en est trouvée fragilisée. Dès le mois de juin 2020, le National Cyber Security Center démontrait que 350 cas de cyberattaques (hameçonnage, attaques directes contre les organisations, sites web vérolés…) avaient été recensés en Suisse pour le seul mois d'avril, contre 100 à 150 en temps normal. Tendance comparable en Europe tout comme en Amérique du Nord, où près d'un collaborateur sur deux (47%) se fait piéger par le phishing [Tessian, 2020]…

Des environnements informatiques de plus en plus complexes

Ce contexte a eu d'importantes répercussions sur les évolutions techniques qui étaient alors amorcées au sein des entreprises. En l'espèce, la pandémie ainsi que les changements opérés dans les pratiques professionnelles ont contribué à accélérer les tendances qui s'esquissaient, en lien avec la complexification croissante des environnements informatiques. Nouveaux outils, nouveaux services, nouvelles applications... Les organisations se sont mises à avoir de plus en plus recours à des produits spécialisés afin de perfectionner leur système informatique. Cette prolifération d'outils et d'applications nouveaux a modifié la donne stratégique : désormais, les DSI doivent assurer la sécurité de chacun des composants, au risque de mettre en péril l'intégralité de leur SI... Un véritable défi à relever, que 44% des entreprises estiment primordial [McKinsey, 2020]. Située au second rang des préoccupations des organisations (après la protection des données), cette sécurité a un coût non négligeable et oblige les entreprises à d'importants efforts. Et dans près de 8 cas sur 10 (78%), les experts de la cybersécurité et IT indiquent que la sécurité des télétravailleurs est de plus en plus difficile à assurer [Splunk, 2022].

Pénurie d'ingénieurs en cybersécurité

Les observateurs le savent : l'essor du cloud n'est pas pour rien dans la technicisation de plus en plus fine des Systèmes d'Informations, pour ne pas dire dans leur complexification (voir encadré page suivante). Celui-ci s'articule avec une pénurie structurelle de professionnels. En France, le déficit d'ingénieurs spécialisés en cybersécurité a fait l'objet à l'automne 2021 d'un plan national soutenu par l'Etat [Les Echos, sept. 2021], peu avant l'ouverture du Campus Cyber en février 2022. Principal acteur mondial, Microsoft estimait récemment que ce manque de compétences humaines constituait le principal problème lié à la sécurité informatique. « Il manque près de 15 000 personnes, experts en cybersécurité en France, pour laquelle nous recherchons des profils extrêmement variés. », déclare ainsi Jean-Christophe Pitié, COO de Microsoft France [Clubic, 2022]. Une tendance que l'on retrouve dans bien d'autres pays à l'échelle mondiale [ICS2, 2021] et qui est appelée à se confirmer dans les mois et les années à venir. Car selon les prévisions, le secteur de la cybersécurité connaîtra en France une croissance de 8 à 10% dans les 5 prochaines années [Les Echos, sept. 2021].

Sophistication des attaques

La sophistication accrue des attaques est l'autre grand phénomène du moment. Conjoncturel celui-ci, il repose sur des techniques de piratage continu, clandestines et très poussées afin d'atteindre le cœur du système informatique et y demeurer pendant une longue période. Si elles visent tout particulièrement des structures à haute valeur (Etats, grands groupes...), ces APT (Advanced Persistent Threats), ou menaces persistantes avancées concernent par extension toutes les organisations, publiques comme privées, quels que soient leur taille et leur champ d'activité. Leur objectif : subtiliser des informations précieuses et nombreuses sur une longue période en effectuant des mouvements latéraux qui permettront d'observer de l'intérieur les vulnérabilités du SI.

Elles viennent s'ajouter à la longue liste de menaces qui pèsent sur la cybersécurité des entreprises, et dont le facteur humain est un élément essentiel...

Face à ce contexte nouveau, les entreprises agissent. Observé depuis quelques années, le déploiement des SOC (Security Operations Center) et des SIEM (Security Information and Event Management) font pleinement partie des réponses qui sont désormais apportées. Offrant aux entreprises une nouvelle génération de fonctionnalités de détection, d'analyse et de réponse, ils impliquent au sein des entreprises des enjeux à la fois techniques et organisationnelles, en lien avec la stratégie globale de l'organisation.

La « cloudification » des SI

Entre 2019 et 2021, les structures privées comme publiques sont passées de 72% à 88% de recours au cloud, et les bureaux virtuels ont gagné quatre points de pourcentage (86%). Cela pose d'importants défis en termes de sécurité : plus l'infrastructure se ramifie, plus elle se révèle vulnérable. Difficile, dès lors, d'identifier une attaque, encore plus d'y répondre.
Selon une analyse effectuée par Kaspersky, 6 organisations sur 10 estiment que le déficit de visibilité sur l'infrastructure SI est le défi le plus courant auquel elles sont actuellement confrontées [Kaspersky, 2020].

Cyberattaques : un coût pour les organisations

En hausse depuis 2 ans, les cyberattaques sont de plus en plus considérées par les entreprises comme le risque le plus menaçant pour leur activité. En 2022, une entreprise sur dix témoigne avoir été victime d'un ransomware, et 62% des organisations impactées déclarent avoir payé la rançon demandée [Hiscox, rapport 2022 sur les cyber-risques]. Quant au coût moyen d'une cyberattaque, qu'il faut bien entendu rajouter au paiement de la rançon, il est évalué à quelque 51 000 € selon l'assureur Hiscox pour une entreprise moyenne. Ce montant comprend à la fois des coûts directs (enquête technique, notifications d'intrusion aux clients, sécurisation des données post-incident, relations publiques, mise en conformité règlementaire, honoraires d'avocat, frais de justice, amélioration des dispositifs de cybersécurité) et des coûts indirects (perturbation ou interruption d'activité, perte de propriété intellectuelle, perte de confiance, dépréciation de la valeur de la marque, augmentation des primes d'assurance et du coût de la dette). Il est bien sûr plus élevé pour les ETI, et encore plus encore pour les grands groupes.

Le SOC : des enjeux techniques...

mais surtout humains !

Face à des attaques malveillantes de plus en plus fréquentes et de plus en plus techniques, le SOC et le SIEM offrent une visibilité globale sur les incidents. Ils obligent également les organisations à se poser des questions majeures en termes d'organisation humaine.

Attaques malveillantes à répétition, complexité des systèmes d'information, essor des technologies cloud, télétravail, mondialisation des relations professionnelles... Depuis quelques années, les organisations optent pour le déploiement d'un SOC (*Security Operations Center*).
Objectif : détecter, analyser et intervenir en cas d'incident cyber. Pour ce faire, le SOC relève d'une articulation subtile de dispositifs technologiques et de processus. Il procède également d'une organisation humaine dédiée, tout en nécessitant une réflexion amont approfondie.

Une combinaison de dispositifs technologiques

La conception technique d'un SOC renvoie à des choix qu'il convient d'opérer sur les outils ainsi que sur les contrats à passer. À ce stade, un ensemble de questions se posent. Concernant la collecte de données, il s'agit d'identifier et de localiser les outils qui composent le SI existant : IDS/IPS, pare-feu, détection de fuite de données, boitiers de chiffrement, antivirus, anti-spam, contrôles d'accès et d'identité... À chaque outil sa mission, pour ne pas dire ses objectifs de sécurité. Pour ce qui relève des opérations de supervision, une étude de conception doit permettre d'affiner un choix sur l'outil majeur ainsi que sur ses satellites associés. Il s'agit là d'assurer la réception, le tri, la qualification et la priorisation, le suivi ainsi que le traitement des incidents de sécurité. À noter que ces éléments se doivent d'être adaptés (et adaptables) aux contraintes de l'organisation, qu'elle soit privée ou publique. Il s'agit notamment de considérer la comptabilité avec le (ou les) SIEM (*Security Information and Event Management*) mis en œuvre, d'évaluer la capacité du SOC à prioriser les incidents en rapport avec une échelle de gravité pour l'entreprise, de jauger de l'adaptabilité des circuits d'escalade et de communication, ou encore de prévoir les échanges et interactions avec d'autres SOC.

À ces choix inhérents aux outils techniques s'en ajoutent d'autres, liés aux processus ainsi qu'aux règles appelées à régir la sécurité du système d'information. De nature organisationnelle, ces process traitent notamment de la gestion de crise, des astreintes, des escalades. Ils garantissent la bonne intégration du SOC avec l'ensemble des processus IT de l'organisation.

Une organisation humaine *ad hoc*

De tels processus renvoient de facto à l'organisation humaine qui les sous-tend. Emmenées par un responsable SOC, des équipes sont en effet spécifiquement dédiées à la détection, à l'analyse, à la réaction, au signalement ou encore à la prévention des incidents liés à la cybersécurité. Elles se composent en général d'analystes de niveaux 1 et 2, ainsi que d'ingénieurs cybersécurité (niveau 3). Les analystes de niveaux 1 et 2 sont en quelque sorte des « chasseurs ». Leur motivation quotidienne est de débusquer des attaquants via des investigations poussées. Pour cela, ils observent et interprètent les différentes remontées d'alertes issues du centre de supervision : analyse de logs de sécurité en provenance du SIEM, analyse de flux réseau, mise en place de règles de corrélation pour la détection, gestion des incidents. Ces analystes effectuent également une veille sur les menaces et les vulnérabilités (avec rédaction de bulletins d'alerte), et réalisent un reporting ainsi que des actions de documentation (participation aux rapports de suivi d'activité ainsi qu'au fonds documentaire du SOC). Pour leur part, les ingénieurs sécurité de niveau 3 font montre d'une expertise plus poussée, notamment sur les méthodes d'attaque. Ces spécialistes sont en capacité de se pencher sur des signaux faibles, de réaliser des recherches exploratoires sur l'ensemble des événements auxquels ils sont confrontés, voire de faire du « reverse ». Outre de compétences techniques, ils font montre de fortes qualités relationnelles et de synthèse.

Le responsable du SOC s'acquitte de son côté des missions managériales globales de l'ensemble des analystes. Il est la clé de voûte des Service Level Agreements du SOC, garant de la bonne application des processus (gestion des incidents, optimisation des traitements, suivi des demandes de changements), de la cohérence ainsi que de la stratégie technique du SOC. C'est lui qui définit et suit les indicateurs de performance ainsi que la mise en place des tableaux de bord, lui qui anime les revues (hebdomadaires, mensuelles), lui encore qui rédige les rapports d'activités ou encore les messages préformatés d'alertes.

Loin d'être un acte anodin de type « plug and play », la mise en place d'un SOC au sein d'une organisation implique donc bien une forte réflexion amont ainsi qu'une approche méthodique.

Quelle gouvernance ? Quelles mesures de protection ? Quelles modalités de détection et de réaction ? Quelles remédiation et reconstruction en cas d'attaque réussie ? Autant de questions majeures, qui doivent s'accompagner d'un indispensable sponsorship interne tant le déploiement d'un SOC relève d'une opération d'envergure transverse. Mais c'est surtout le facteur humain qu'il convient de prendre en considération, dans la mesure où l'action quotidienne et pérenne des équipes SOC se révèle de la plus haute importance pour la sécurité de l'entreprise, et donc de sa pérennité.

Pourquoi les SOC et les SIEM sont nécessaires

Depuis plusieurs années, le déploiement des SOC et des SIEM permet aux organisations qui adoptent ce type de réponse de faire face à la recrudescence ainsi qu'à la puissance des attaques dont elles font l'objet.
Sept risques sont plus particulièrement à observer, auxquels les SOC répondent :

1- L'augmentation de la surface d'attaque : celle-ci est liée tout à la fois à l'essor du cloud, à la complexification des chaînes d'approvisionnement numérique et à des écosystèmes étendus en raison de l'essor des actifs.

2- Agrandissement de la chaîne d'approvisionnement numérique : d'ici à 2025, les spécialistes prévoient que 45% des organisations feront face à des attaques sur leurs chaînes d'approvisionnement en logiciels. Cela représente trois fois plus qu'en 2021.

3- Plus d'attaques sophistiquées sur la gestion des identités et des accès : l'usage abusif des justificatifs d'identité est devenu un moyen d'attaque primaire. À ce jour, les organisations ont pu apporter des réponses techniques afin de rendre l'authentification des utilisateurs plus performante, mais la question culturelle des comportements demeure.

4- Des responsabilités cyber de plus en plus diluées : face à une surface d'attaque en expansion, les organisations sont confrontées à un essaimage des décisions et des responsabilités. Cette complexité fait évoluer le rôle du RSSI : d'expert technique, le voici désormais gestionnaire exécutif des risques : une véritable refonte de leur rôle.

5- L'erreur humaine : celle-ci demeure un facteur et un enjeu, bien au-delà des progrès techniques. Pour ce faire, les organisations développent des programmes de sensibilisation. Les structures les plus à la pointe vont au-delà en investissant dans des programmes holistiques de comportement et de culture de la sécurité.

6- Les fournisseurs : ceux-ci sont désormais pleinement intégrés à l'écosystème numérique de leurs clients, notamment par souci d'efficacité et de réduction de la complexité. Cette extension augmente d'autant les risques, appelant des réponses globalisées.

7- Le maillage de la cybersécurité : complexe, celui-ci nécessite une approche en termes d'architecture générale du SI. Plus intégrée, celle-ci vise à sécuriser l'ensemble des actifs, que ces derniers soient localisés sur site, au sein du cloud ou dans des centres de données.

Source : Gartner, "Top Trends in Cybersecurity 2022", mars 2022

« Le SOC permet d'améliorer sa détection et ses réponses »

Le premier est consultant en cybersécurité ; le second occupe les fonctions d'architecte en cybersécurité. Lidao Bilesh et Mickaël Sardinha travaillent tous deux au sein de CAPFI, une ESN fondée en 2005 autour du conseil, des infrastructures IT et Sécurité, de la Data Science et du Big Data, de l'ingénierie digitale et de la finance. Témoignage d'experts.

Qu'est-ce qu'un SOC et comment fonctionne-t-il ?

Lidao Bilesah : Il existe plusieurs définitions du Security Operations Center. Pour nous c'est un ensemble qui comporte plusieurs éléments. Ce que l'on peut dire en premier lieu c'est qu'un SOC est une solution technique qui va permettre à l'organisation d'améliorer sa détection et ses réponses. C'est également un ensemble de processus qui vont faire gagner en réactivité lorsqu'il y a des alertes. Le SOC améliore par ailleurs les process. Et je rajouterai un tout dernier élément : le facteur humain. Souvent, les DSI oublient ou minimisent cette dimension. Or, ce sont bien les experts qui gèrent les alertes.

Mickaël Sardinha : Les solutions techniques des équipes SOC ne sont pas autonomes : il faut quelqu'un pour les gérer, voire mobiliser une équipe. Pendant longtemps, les DSI ont été habituées à apporter des réponses en grande partie technique : on avait un problème, alors on déployait un pare-feu par exemple. Avec les SOC, la ressource humaine est bien plus importante. Je dirai même que le côté humain n'a jamais été aussi important qu'aujourd'hui en matière de cybersécurité. Les équipes d'administration doivent travailler avec des équipes chargées des alertes.

Comment expliquer un tel changement ?

Mickaël Sardinha : Pour ma part, je pense que le changement le plus important a été le mouvement vers les services SaaS. Cela a d'emblée posé des problématiques importantes, liées à des solutions techniques que l'on ne voyait pas. Un firewall ne détecte rien lorsque l'on travaille dans un café… Le SOC va permettre de couvrir un maximum de surface d'attaque : le SaaS bien sûr, mais aussi par exemple la partie nomade – avec les mobiles, voire les tablettes. Le tout en sachant que l'on conserve la partie interne !

Le déploiement des SOC est donc lié à l'augmentation de la surface d'attaque ?

Mickaël Sardinha : En effet. Il y a quelques années, les pirates de l'intérieur, ceux que l'on appelle les insiders, étaient les plus nombreux. Mais le monde cyber est devenu bien plus large, notamment en raison de la pandémie. Cela a accéléré le phénomène, en lien avec l'essor du nomadisme et de celui du mode SaaS. Il y a eu une augmentation franche de ces derniers services : serveurs de fichiers, serveurs

mail, migrations vers Office 365… Les organisations ont découvert la facilité de ne pas avoir en responsabilité la partie maintenance. Mais cela a accéléré les malware…

Lidao Bilesah : Nous avons également pu observer qu'avec la crise sanitaire, les projets de transformation numérique étaient devenus plus liés à la dimension business. Là aussi, il en a résulté une extension de la surface d'attaque pour les cybercriminels. Ces derniers se sont adaptés à un nouveau contexte, et dans de nombreux cas ils se sont concentrés sur la faille humaine. Car il y a toujours une faille de ce type dans une organisation, et celle-ci est toujours exploitable ! Face à cela, les équipes de défense se sont elles aussi réorganisées. Avec le SOC, elles ont pu s'adapter au nouveau mode opératoire des cybercriminels, exploiter les informations sur les stratégies développées, les techniques, les outils… Pour les DSI, cela demande du temps, mais aussi une expertise spécifique ainsi que des profils particuliers liés aux connaissances les plus pointues sur les menaces.

Pour les DSI, le virage des SOC a-t-il été facile à prendre ?

Mickaël Sardinha : Il faut tout d'abord dire que toutes les organisations ne disposent pas d'un SOC ou d'un SIEM. Ensuite, replaçons tout cela dans le contexte de l'Internet, dont la portée a incroyablement augmenté ces dernières années. Actuellement, 1,2 milliard de personnes ont accès au Net. Les clients, les usagers sont partout, et les attaquants potentiels également. Cette explosion du nombre d'usagers de l'Internet démultiplie mécaniquement les failles, les incidents, les erreurs. Des adolescents de 14 ans peuvent trouver sans peine des malwares et ainsi faire très mal à une organisation. Tout cela oblige à mettre en place des équipes entières, dédiées, car il y a beaucoup de travail.

Lidao Bilesah : Dans ce contexte, monter une équipe pérenne, au sein de la DSI, peut se révéler long et fastidieux. Chaque entreprise a sa propre culture interne, et parfois elle ne passe pas par la cybersécurité – alors qu'elle le devrait. Ensuite, recruter est devenu très compliqué : les compétences manquent à l'appel, et cela prend énormément de temps. Un recrutement peut ainsi durer 6 à 8 mois, car il y a des offres à profusion et les demandeurs sont rares. Mais une fois que l'on a recruté on n'est pas au bout de ses peines : il faut encore maintenir les collaborateurs à jour techniquement. Et les sujets de formation sont partout : sur le mobile, le SaaS…

Plaidez-vous pour la mise en place d'un SOC interne ou d'un SOC externe ?

Mickaël Sardinha : Il n'y a pas de réponse claire à cette question car cela dépend de l'entreprise. Il faut aussi voir les implications. Le SOC interne est plutôt réservé à de grosses structures, ou à des sociétés qui disposent de moyens financiers conséquents. Car un SOC géré par une équipe interne pose inévitablement des questions liées à la gestion financière et humaine : outre les formations professionnelles indispensables, il faut encore prendre en charge les carrières, leur évolution, les périodes de vacances, les arrêts maladie… Lorsqu'elle est choisie, cette option peut être intéressante pour l'entreprise : les experts sont rapides à agir, connaissent parfaitement leur matrice de risque et celle-ci est bien ciblée sur les applications métiers. Pour sa part, le SOC externe s'adresse à des structures différentes, et répond à des enjeux spécifiques.

Lidao Bilesah : L'avantage que peut avoir un SOC externe vient du fait que le sous-traitant peut garantir un service égal et complet 365 jours par an, 7 jours sur 7. Ce sous-traitant aura également une plus grande facilité à répondre à certaines problématiques dans la mesure où il les aura déjà rencontrées sur d'autres missions. Un SOC externalisé permet d'avoir des réflexes, et ainsi de faire face à des process et des réponses plus rapidement que des équipes internes. Il reste la solution la plus évidente pour des PME et pour les ETI, particulièrement pour des sous-traitants de l'Etat.

Le SIEM, pilier du SOC

Depuis leur création au début des années 2000, les SOC ont subi de profondes modifications. Afin de répondre à des attaques de plus en plus élaborées et complexes, dans les années 2010, les équipes de sécurité opérationnelle se sont modernisées.
Les SIEM (Security Information and Event Management) et les SOAR (Security Orchestration, Automation and Response) ont indéniablement participé de cette évolution. Depuis 10 ans, ils rendent possible l'industrialisation de la surveillance en simplifiant l'analyse des nombreuses sources d'événements de sécurité (proxy, console antivirus, firewall notamment) et en automatisant les réponses aux incidents de sécurité. Le SIEM permet également de corréler les (nombreux) événements qui proviennent des équipements tout comme des applications de plus en plus nombreuses. Ce faisant, les SIEM et les SOAR nécessitent un niveau de compétence accru pour les équipes dédiées à la sécurité opérationnelle. Celles-ci doivent en effet éviter l'écueil d'une mauvaise implémentation des contrôles, voire d'une méconnaissance des scénarios de menaces réels.

Vers un SOC 2.0 augmenté grâce à l'eXtended Malware Analysis Platform

En 2023, il n'est plus possible de s'en tenir aux versions traditionnelles des SOC et des SIEM. Confrontées aux enjeux de cybersécurité actuels, ces solutions se doivent d'être consolidées par l'IA et le Machine Learning, mais également par des solutions de type Reverse Engineering et d'eXtended Malware Analysis Platform. Explications.

Historiquement versée dans la Recherche & Développement, l'économie française repose en partie sur la qualité de son ingénierie. Dynamique et encore faiblement concentré, le secteur fait l'objet de toutes les attentions – pour ne pas dire de toutes les protections. Afin de préserver les entreprises nationales des cyberattaques, et pour continuer de s'imposer dans l'industrie 4.0, l'Etat a récemment accéléré sa stratégie cyber : à l'horizon 2025, la filière vise un chiffre d'affaires de 25 Md€, soit trois fois plus qu'actuellement [France 2030].

SOC 1.0 : une architecture devenue obsolète

Cette modernisation devrait permettre aux entreprises ainsi qu'aux organisations publiques, toutes tailles et tous secteurs confondus, d'accélérer un peu plus encore la modernisation de leurs outils. Le passage à des SOC dits « 2.0 » fait pleinement partie de cet objectif. Car de nombreux *Security Operations Centers* reposent actuellement sur une architecture dépassée. Outils de plus en plus modernes, applications nouvelles, complexité du SI, environnements multicloud et cyberattaques à la fois plus nombreuses et plus performantes composent un environnement nouveau. Fonctionnant désormais avec des moyens de détection obsolètes, notamment avec des solutions qui reposent sur l'agrégation de volumes importants de Log et de systèmes de détection à signatures, les SOC « anciens modèles » obligent les équipes d'analystes sécurité à multiplier les efforts afin d'extraire les données manuellement, et ce à partir d'un nombre réduit et limité de sources. Les résultats n'en valent plus la chandelle tant ils sont imprécis, ôtant toute visibilité aux SOC Team et générant pour l'entreprise des coûts importants et inutiles.

L'IA et le Machine Learning : automatiser la détection

Comment détecter les attaques de ransomware, lesquelles reposent de plus en plus sur les déplacements subreptices des cybercriminels au sein même du système d'information ? Avec les nouveaux SOC et les SOAR, la détection est de plus en plus automatisée. Bénéficiant à la fois de l'intelligence artificielle (IA) et du Machine Learning, elle repose sur deux grands piliers : l'EDR (Endpoint Detection Response, détection sur les postes et les serveurs) et le NDR (Network Detection & Response, solution qui permet de contextualiser la menace de sécurité). Ceux-ci génèrent la visualisation de l'intégralité des éléments constitutifs de l'infrastructure, notamment sur les environnements IT et IoT. Avec ces nouvelles fonctionnalités, le SOC de nouvelle génération déploie, grâce à l'automatisation du SOAR, une sorte de filet de surveillance sur tous les assets présents dans les environnements physiques ainsi que le cloud. Ce SOC plus moderne permet de concentrer son attention sur la méthodologie de l'attaquant, et plus particulièrement sur son comportement, plutôt que sur l'usage de son attaque (signature). Il devient ainsi possible de détecter des attaques jusqu'alors inconnues.

Le concept code : reconnaître les nouvelles menaces

Mais ces technologies nouvelles, pour modernes qu'elles soient, sont encore loin de détecter les menaces persistantes avancées que constituent les APT (Advanced Persistent Threats), voire de lever le voile sur l'enchaînement des actions qui occasionnent les dommages portés au SI. Comme le rappelle le spécialiste Olivier Gesny, directeur de l'innovation au sein de PR0PH3CY (ex Silicom) dans la Revue Défense Nationale, « la cyberdéfense doit étendre ses capacités d'actions et de perception pour être en mesure de traiter d'égal à égal avec l'attaquant dont la palette d'actions est nettement plus riche » [Revue Défense Nationale, 2019].

L'eXtended Malware Analysis Platform est indéniablement l'un des éléments qui permet d'ores et déjà aux SOC ainsi qu'aux SIEM de franchir une marche significative en termes de détection et de réponse (voir pages suivantes). Particularité de cet outil : il offre une vision globale sur le système d'informations, notamment grâce au concept code. Cette dernière technologie joue un rôle particulier dans la mesure où c'est elle qui identifie de manière automatisée, au sein d'un malware, la « narration » de celui-ci, c'est-à-dire sa grammaire. « Nous reconnaissons les nouvelles menaces grâce à la manière avec laquelle les malwares sont codés », explique à ce sujet Frédéric Grelot, l'un des ingénieurs à la base de cette invention, vice-président en charge de la Recherche au sein de la start-up GLIMPS.

[Infoprotection, mars 2022]. « Pour être plus précis, nous recourons à l'apprentissage profond (Deep Learning) pour reconnaître non pas les nouveaux virus eux-mêmes mais leurs 'concept codes', à savoir la manière avec laquelle leur algorithme est codé : les codes de communication réseau, les codes de chiffrement, les codes de paiement en Bitcoin, etc. ».

Et cela fonctionne ! Face à des fichiers à la fois nombreux et disséminés, le concept code propose des

informations centralisées et pertinentes, qui vont permettre à l'eXtended Malware Analysis Platform de collecter des informations majeures qui permettront aux équipes sécurité de mieux réaliser leur travail.

Le concept code : tout est affaire d'histoire, voire de conte pour enfants !

L'analogie entre le concept code et les contes que l'on raconte aux enfants permet de mieux saisir les caractéristiques de cette technologie nouvelle qu'est le concept code. Car si les contes pour la jeunesse racontent une même histoire (de Boucle d'Or au Petit Chaperon rouge), celle-ci se décline auprès des enfants dans toutes les cultures et dans de nombreuses langues. C'est à ce niveau que se situe la spécificité du concept code : il se focalise sur l'histoire contée et non sur les mots ni la grammaire employée. Ce faisant, cette technologie permet de repérer un scénario identique à 80, 90 ou 95%, dans plusieurs malwares qui pourtant sont rédigés de manières différentes. C'est donc bien l'histoire qui est au cœur du concept code... mais aussi à la base des émotions des enfants face aux contes et légendes.

Désassembler le code : l'apport du Reverse Engineering

La conceptualisation du code repose sur le Reverse Engineering automatique. Celui-ci permet de désassembler le code, c'est-à-dire de le traduire en langage compréhensible, avant d'en identifier les concepts. Ce processus se fait en plusieurs étapes, qui sont similaires à l'apprentissage de la lecture pour tout être humain : prise de connaissance des lettres d'un alphabet afin de former des phrases, puis apprentissage de la grammaire. Le point ultime de l'apprentissage étant l'assimilation de l'histoire qui se trouve narrée, avec ses concepts et ses différentes idées.

Cap sur une notion nouvelle :

« l'eXtended » Malware Analysis Platform

Pour autant qu'ils soient fiables en termes de détection, les SOC constituent des solutions automatisées qui se révèlent de plus en plus limitées. Un nouvel outil se dessine : la XMAP, eXtended Malware Analysis Platform, dans une version plus étendue que les sandbox actuelles.

Les spécialistes connaissent et utilisent les nombreux points positifs des SOC. Articulés avec le SIEM et le SOAR, les Security Operations Centers collectent et analysent les données, avant de permettre leur remédiation. Mais ces SOC sont dans certains cas peu équipés en solutions, générant des « trous dans la raquette » en matière de détection. Problème : cette dernière en devient hétérogène… « Aujourd'hui, un SOC va devoir collecter des fichiers un peu partout – stations blanches, NAS, etc. – et ainsi se disperser. Ou bien, il va démultiplier les antivirus, ce qui pour l'entreprise entraîne un coût important », avertit Frédéric Grelot, ingénieur au sein de la start-up GLIMPS.

Malware Analysis Platform : une solution globale

Ce constat plaide pour le développement d'une solution globale : la Malware Analysis Platform. Particularité de cette dernière : sa propension à centraliser les solutions et les données, et ainsi à offrir aux DSI une visibilité d'ensemble sur ce qui est en train de se passer au cœur même de l'architecture du système d'informations. À l'heure actuelle, afin de tendre vers ce résultat, de nombreuses directions informatiques optent pour la solution nouvelle de la sandbox. Désignant un outil qui permet d'exécuter un malware afin d'en observer le comportement et en extraire des indicateurs, cette option propose de l'exécution dynamique aux équipes en charge de la sécurité. « Mais la sandbox se révèle très chère, nécessite de longs temps d'exécution et génère soit peu d'informations, soit beaucoup de données. Résultat : au mieux on se retrouve noyé dans les informations, au pire on en est sevré… », indique Frédéric Grelot.

L'apport du concept code en faveur d'une eXtended Malware Analysis Platform

Une détection ultra-rapide et complète est cependant possible grâce au concept code. En partie articulable à la sandbox mais aussi avec le SOC, cette technologie émergente permet de détecter en un temps de record des attaques sur un spectre le plus large possible.

« Avec le SOC, nous disposons d'un outil… mais ils nous manque la fiabilité de la détection ainsi que la dimension globale et synthétique d'une analyse avancée qui repose sur l'automation. Autant d'éléments que la solution du concept code permet », poursuit Frédéric Grelot.
Particularité de cette solution nouvelle, qui confine à la notion d'eXtended Malware Analysis Platform (plateforme étendue) : elle remonte de manière systématique et fiable les informations sur les SIEM et le SOAR (outil d'orchestration, d'automatisation et de réponse) afin de générer l'analyse. L'ensemble du mouvement s'effectue en un temps record : 4 à 5 secondes, contre plusieurs minutes (voire quelques heures) pour les solutions actuelles. Dès qu'une détection est effectuée, l'analyse avancée est prête ! Une rapidité qui peut être salvatrice pour les entreprises ainsi que pour les organisations publiques, particulièrement dans le contexte actuel.

Vers un acteur dédié à la détection et à l'analyse ?

Ceci pour indiquer combien la détection et l'analyse sont en passe de devenir les deux axes d'un véritable métier, lequel repose sur des compétences et des technologies d'automation à haute valeur ajoutée. En l'espèce, l'externalisation des compétences paraît de mise. Plutôt que se référer au savoir-faire partiel et parcellaire d'un ensemble d'acteurs disséminés au sein de l'écosystème informatique, il semble de plus en plus évident que l'avenir sera à la responsabilisation d'un acteur dédié dont la détection et l'analyse de malware constitueront le cœur de l'expertise. Nous rejoignons ici la notion d'XDR, outil de détection des menaces de sécurité et de réponse aux incidents qui repose sur le modèle SaaS. Spécifique à chaque fournisseur et intégrant nativement un ensemble de produits de sécurité dans un système d'opérations de sécurité cohérent, celui-ci unifie les détections et offre aux équipes de sécurité tout à la fois « *de la flexibilité, de l'évolutivité et des possibilités d'automatisation* » [Forrester Resarch, Palo Alto Networks]. Reposant sur l'association partenariale d'un ensemble d'acteurs spécialisés, ce type de plateforme a récemment fait l'objet d'une déclinaison à l'échelle française avec l'«Open XDR Platform», créée au moment des Assises de la sécurité 2021 (*voir encadré page suivante*). Son atout maître : l'automatisation de la réception et du traitement des alertes.

Une organisation humaine plus efficiente

Un tel niveau de spécialisation et de technicité ne peut qu'avoir un effet bénéfique sur les équipes DSI internes. Confrontés à des ransomwares de plus en plus élaborés, utilisant des outils à entrées multiples et soumis à une information devenue pléthorique, les ingénieurs informatiques se trouvent de plus en plus sommés d'avoir recours à des solutions manuelles, chronophages et dont les résultats sont plus qu'incertains. Parfois démunis, voire soumis à un fort stress, ils trouvent dans les solutions de Reverse Engineering, de concept code et d'IA des leviers leur permettant d'alléger leur quotidien. « *Il est clair que les DSI ont beaucoup de temps à gagner en s'appuyant sur l'intelligence artificielle et le Machine Learning* » conclut Frédéric Grelot. « *Ces solutions nouvelles mobilisent la réflexion humaine sur des données véritablement consolidées, globalisées*

et synthétiques. Elles permettent ainsi à l'organisation d'apporter une meilleure réponse à incident. » Et également à cette dernière d'effectuer au final d'importantes économies budgétaires, tout en bénéficiant d'une protection optimale.

Concept code : une technologie validée scientifiquement

La technologie du concept code a récemment fait l'objet d'un article scientifique [C&ESAR 2021].
Co-signé par Frédéric Grelot, Marie Salmon et Sébastien Larinier, cet article a permis de comparer deux méthodes d'analyse des binaires : l'une, manuelle, assurée par les experts de l'école d'ingénieurs du monde numérique ESIEA ; l'autre, automatique, par les ingénieurs de la start-up GLIMPS. Au final, la recherche automatisée et la technologie du concept code sont validés par l'approche académique manuelle : celle-ci montre que l'automatisation en rétro-ingénierie est non seulement fiable, mais aussi bien plus rapide que l'approche classique.

Open XDR Platform : une offre complète de cybersécurité en France

C'est lors des Assises de la sécurité 2021 que plusieurs acteurs français ont annoncé la mise en place de l'OPEN XDR Platform. Constituant une offre de confiance dans le domaine de la détection et de réponses étendues, celle-ci repose sur la collaboration de 7 participants et constitue le signe selon lequel l'écosystème de la cybersécurité français travaille main dans la main face aux importantes menaces qui pèsent sur les organisations. Parmi les structures participantes se trouvent HarfangLab (solution EDR certifiée par l'ANSSi, l'Agence Nationale de la Sécurité des Systèmes d'Information), SEKOIA. IO (brique de Cyber Threat Intelligence), Pradeo (Mobile Application Security Testing), Vade (filtrage d'emails), Gatewatcher (Network Detection & Response), Wallix (Sécurisation des accès) et GLIMPS (eXtended Malware Analysis Platform). Selon Grégoire Germain, fondateur de HarfangLab, « *les briques sont autonomes et les clients peuvent les choisir en fonction de leurs besoins* » [Lemondeinformatique.fr]. Objectif final : proposer une offre de confiance aux entreprises privées comme aux structures publiques.

GLOSSAIRE

Concept code :

La conceptualisation du code est une technologie récente consistant à identifier de manière automatisée, au sein d'un malware, la « narration » de celui-ci. Après avoir été désassemblé grâce au Reverse Engineering, le code livre ainsi l'histoire dont il est le détenteur, par-delà les chiffres qui le composent et qui en sont tout à la fois les mots et leur grammaire. Le concept code établit ainsi qu'une histoire est identique à une autre à 5%, 10% ou 15%, permettant de stopper net la progression d'un malware.

EDR :

Un logiciel EDR (Endpoint Detection & Response) constitue une solution de sécurité destinées aux « points terminaux » (endpoints). Il vient palier les déficiences de certains antivirus en détectant des attaques inconnues mais également en initiant des correctifs automatiques. Des fonctionnalités avancées permettent aux EDR de réaliser des investigations à distance.

Intelligence artificielle :

L'IA est un ensemble de technologie différentes qui fonctionnent ensemble dans le but de permettre aux machines de percevoir, comprendre, agir et apprendre à des niveaux d'intelligence tendant à celle des humains. Plusieurs sous-ensembles technologiques font partie de l'IA, tels que le traitement automatique du langage naturel (NLP) ou le Machine Learning (ML).

Machine Learning :

Le Machine Learning constitue l'une des formes de l'Intelligence Artificielle, une sous-catégorie de celle-ci visant à automatiser le processus de création de modèles analytiques. Le Machine Learning permet aux machines de s'adapter à de nouveaux scénarii de manière autonome. Il permet notamment une gestion intelligente du Big Data, ce qui dans le cadre de la recherche de malwares est un atout précieux.

NDR :

Une solution NDR (Network Detection and Response) traite les menaces de sécurité en les contextualisant. Pour ce faire, elle analyse le trafic réseau et inspecte en temps réale les communications du réseau. Les menaces sont ainsi détectées et disséquées, particulièrement les activités à risque ainsi que les comportements anormaux. Cette solution peut notamment se révéler utile lorsque l'organisation dispose d'alarmes mal contextualisées.

Reverse Engineering :

La rétro-ingénierie est la technique grâce à laquelle un système peut être désassemblé. Dans le champ des systèmes informatiques, cette étude et cette analyse peuvent être appliquées aux malwares. La Reverse Engineering logicielle consiste ainsi à inverser le code machine d'un malware afin de le ramener au sein du code source dans lequel il a été écrit. La rétro-ingénierie permet de récupérer ce code source, et ainsi d'identifier le contenu malveillant d'un programme.

GLOSSAIRE :

Suite

SaaS :

Ce terme signifiant « Software as a Service » désigne une solution applicative hébergée dans le cloud et exploitée par un tiers en dehors de l'organisation (entreprise privée ou structure publique). Ce modèle comprend une architecture multi-tenant qui permet aux utilisateurs comme aux applications de partager une infrastructure et une base de code uniques et communes, avec maintenance centralisée. Le SaaS facilite la personnalisation, la mise à jour des logiciels et un meilleur accès. Il invalide les coûts d'acquisition de matériel, d'approvisionnement et de maintenance, de licence et de support.

SOC :

Le *Security Operations Center* constitue une plateforme de supervision et d'administration de la sécurité du système d'information. Il comprend des outils de collecte, de corrélation d'événements ainsi que d'intervention à distance. Il se compose à la fois des équipements techniques et de personnes dédiées, nécessaires afin de garantir la supervision de la sécurité informatique mais également pour intervenir le plus rapidement possible en cas d'incident ou d'attaque.

SIEM :

Cet outil de Security Information and Event Management permet la gestion des événements ainsi que des informations liées à la sécurité des organisations. Reposant sur la comparaison des événements aux règles et moteurs d'analyse, mais aussi sur l'indexation et l'analyse, il représente pour l'ensemble des organisations une nouvelle génération de fonctionnalités de détection, d'analyse et de réponse. Historiquement, le SIEM est l'outil utilisé par les SOC afin de surveiller les infrastructures des entreprises.

SOAR :

Ce terme signifie Security Orchestration, Automation and Response. Comme sa traduction le laisse supposer, il désigne un outil d'orchestration, d'automatisation et de réponses aux incidents de sécurité informatique.

XDR :

Cet acronyme (pour eXtended Detection and Response) désigne un outil de collecte qui corrèle des données situées à plusieurs niveaux : email, endpoint, serveur, cloud et réseau. XDR permet ainsi une détection plus rapide de la menace, mais également des gains de temps concernant l'enquête et la réponse donnée au moment d'effectuer l'analyse de sécurité.

RÉFÉRENCES BIBLIOGRAPHIQUES

BOERO Alexandre, « *Il manque plus de 15 000 experts de la cybersécurité en France* », Clubic, 21 juin 2022
https://www.clubic.com/pro/entreprises/microsoft/actualite-427680-il-manque-plus-de-15-000-experts-de-la-cybersecurite-en-france-microsoft.html

CESIN, *Baromètre de la cybersécurité des entreprises*, 7e édition, année 2021, 17 janvier 2022
https://www.cesin.fr/actu-7eme-edition-du-barometre-annuel-du-cesin-enquete-exclusive-sur-la-cybersecurite-des-entreprises-francaises.html

CYBERMALVEILLANCE.GOUV.FR, *Rapport d'activité 2021*, 8 pars 2022
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2021

GARTNER, *Top Trends in Cybersecurity 2022*, mars 2022
https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

GESNY Olivier, « Capter l'IA de demain au regard des enjeux de cyberdéfense », *Revue Défense Nationale*, 2019/5, n° 820, pp. 38-42
https://www.cairn.info/revue-defense-nationale-2019-5-page-38.htm?contenu=article

GRELOT Frédéric, LARINIER Sébastien et SALMON Marie, « Automatisation de l'analyse des binaires : de la collecte source ouvert à la Threat Intelligence », 16 novembre 2021, salon C&AESAR 2021.
URL : https://conf.researchr.org/details/cesar-2021/call-for-papers/14/Automatisation-de-l-analyse-de-binaires-de-la-collecte-source-ouverte-la-Threat-I

HISCOX Assurances, *Rapport 2021 sur la gestion des cyber-risques*, avril 2021
https://www.hiscox.fr/courtage/blog/rapport-hiscox-2021-sur-la-gestion-des-cyber-risques

RÉFÉRENCES BIBLIOGRAPHIQUES

Suite

KASPERSKY, *A Resilient Cybersecurity Profession Charts the Path Forward*, (ISC)2 Cybersecurity Workforce Study, 2021
https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

MOTELLA Clotilde, « Le coût réel d'une cyber-attaque pour votre PME », SFR Business, 19 octobre 2021
https://www.sfrbusiness.fr/room/securite/cout-reel-cyberattaque-pme.html

PALO ALTO NETWORKS, « What is XDR ? », 2018
https://www.paloaltonetworks.com/cyberpedia/what-is-xdr

PERELAFOUINE, « La transformation du SOC », 20 juin 2022
https://perelafouine.com/la-transformation-du-soc/

PWC, « La cybersécurité fait face à une pénurie de talents constante »,
https://www.pwc.fr/fr/decryptages/securite/la-cybersecurite-fait-face-a-une-penurie-de-talents-constante.html

STOÏK, « La tendance à l'aggravation de la cybercriminalité se confirme », 28 avril 2022
https://www.stoik.io/cybersecurite/chiffres-cles

Web : https://www.glimps.fr
Linkedin : https://linkedin.com.company/glimpsre
Twitter : https://twitter.com/GlimpsRe
Email : contact@glimps.re