APIXIT
L'expertise augmentée

# SECURITY OPERATIONS CENTER (SOC)
# Pourquoi l'externaliser ?

LIVRE BLANC Mai 2020

# SOMMAIRE

# QUI SOMMES-NOUS ?

Expert reconnu des solutions de Connectivité, des Infrastructures Digitales, de la Digital Workplace et de la Cybersécurité, APIXIT vous propose un accompagnement sur l'ensemble de vos projets : audit, conseil, intégration et services managés.

L'usage est au coeur de notre proposition de valeur. Notre offre de service répond directement à vos enjeux métiers. Nos experts vous accompagnent ainsi sur l'ensemble du cycle de vie de vos projets. Animé par une solide culture de la performance, de l'innovation technologique et de la satisfaction client, les 330 collaborateurs du groupe APIXIT sont présents à travers toute la France.

# CONTACT


**Jean-Philippe GUILLEMIN**
Responsable développement d'activité Cybersécurité

**Nicolas Berchoux**
Directeur du Business Development

**Courriel :** communication@apixit.fr
**Tél. :** 01 64 86 97 97

# LA MENACE ÉVOLUE

Le taux d'incidents de sécurité informatique ne cesse d'augmenter graduellement depuis plusieurs années. Pas une semaine ne passe sans qu'une cyberattaque ne soit chroniquée dans la presse spécialisée.

**24 MILLIONS**

Nombre de nouveaux objets malicieux détectés en 2019

Source : Kaspersky

**1 FICHIER SUR 5**

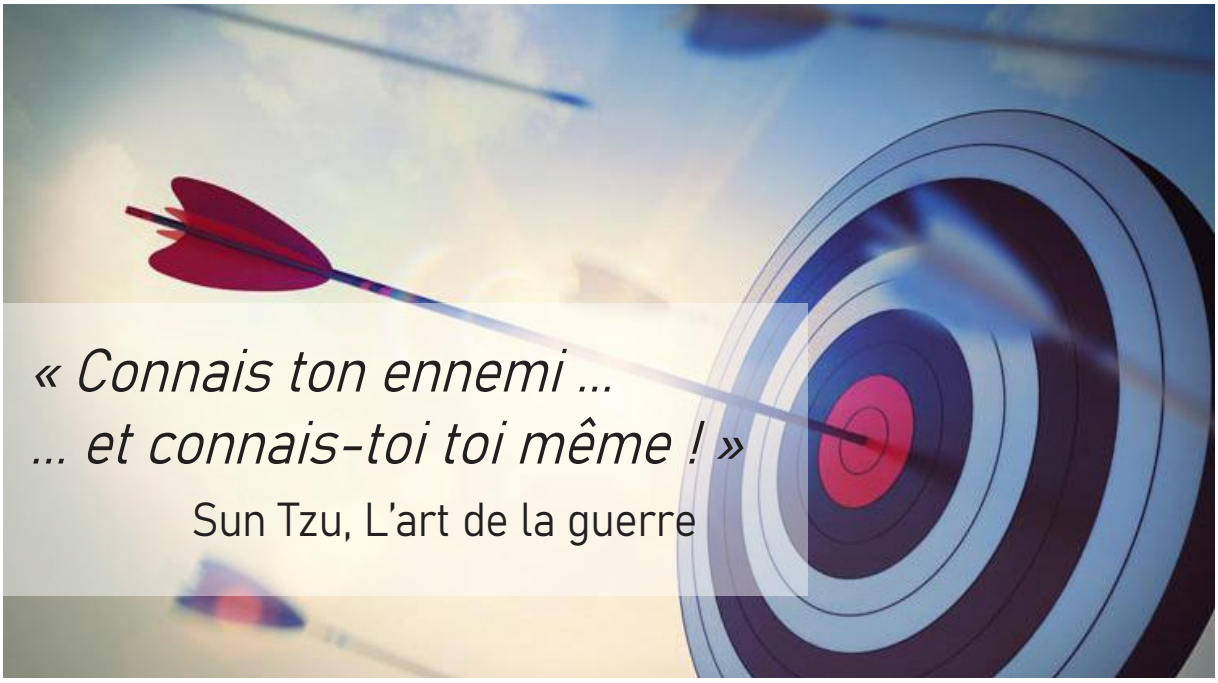
Est exposé du fait d'une sécurité informatique insuffisante

Source : Varonis

Désormais l'ampleur de certains incidents est telle que la presse généraliste s'en fait elle aussi l'écho. Selon une étude Thalès, en 2018, 1 entreprise sur 3 était confrontée à au moins une attaque informatique. Un constat édifiant à l'heure où la facture moyenne d'un incident s'élève à 8,6 millions d'euros *(BFM Business)*.

Pour ne pas rester fataliste face à cette réalité qui inquiète les dirigeants d'entreprise, il est nécessaire d'identifier les moyens pouvant être mis en œuvre pour limiter le phénomène.
Force est de constater que les moyens déployés par les entreprises sont, de façon générale, insuffisants : en atteste l'augmentation du nombre d'incidents dont il est question.
Pour paraphraser Sun Tzu *« Connais ton ennemi et connais-toi toi-même (…) »*. Pour bien combattre il faut avoir au préalable compris à qui on a affaire.

De fait, il est légitime de se demander ce qui provoque cette augmentation de la cyber-délinquance, question à laquelle nous allons commencer par proposer une explication, pour ensuite poser les bases d'une tactique de réponse à cette situation.




# CONNAIS TON ENNEMI

**Deux éléments ont drastiquement évolué ces dernières années : la « surface » d'attaque et les « moyens » d'attaque ; surface d'attaque désignant, dans la terminologie consacrée l'exposition de la cible à l'attaque, telle le nombre de portes dérobées d'un édifice réputé fermé.**

De facto : « tout » , et aussi « tout le monde », se connecte en permanence, à n'importe quelle heure, depuis n'importe quel lieu, vers des destinations connues ou inconnues, volontairement ou involontairement :

- ultra-nomadisme,
- digitalisation des usages,
- objets connectés,
- utilisation massive des web services,
- décentralisation entropique des données,

La surface d'attaque est de plus en plus grande et il semble difficile d'imaginer qu'elle va se réduire : on a plutôt de bonnes raisons de craindre qu'elle n'augmente.

Deuxième élément, les moyens d'attaque ont eux aussi subit une mutation progressive : les chevaux de Troie sont passés dans leur phase industrielle : le BotNet.

La facilité avec laquelle il est devenu possible de réaliser une attaque de grande ampleur va de pair avec un coût de mise en œuvre faible. En effet l'outillage est déjà déployé et prêt à l'emploi. Une simple connexion au DarkNet et quelques fractions de bitcoin suffisent à organiser des attaques variées allant de l'espionnage au rançonnage en passant par le déni de service.

Ainsi, il apparaît que l'explication la plus probable à l'emballement cybercriminel constaté au quotidien est la professionnalisation de cette forme de criminalité. Elle dispose en effet d'excellentes « conditions business » : une clientèle pléthorique, c'est-à-dire beaucoup de cibles potentielles ayant toutes une surface d'attaque importante, et un outil de production économique et performant : les BotNets.

Il n'est donc pas étonnant qu'un nombre de plus en plus important d'attaques passent au travers des mailles du filet, celles-ci étant de plus en plus larges. Les attaques sont de plus en plus nombreuses étant donné que leur mise en œuvre ne coûte presque rien, et peut rapporter beaucoup;

## ET CONNAIS-TOI TOI MÊME

**Quel est le point commun de presque toutes les entreprises en matière de lutte contre les menaces informatiques ? La réponse est : « Elles mettent en œuvre des mesures « passives ».**

Les firewalls, les anti-malwares, l'audit de code, les sondes de prévention d'intrusion, les sauvegardes, … La presque totalité des mesures couramment mises en œuvre appartiennent au domaine de la prévention passive ou sont utilisées dans ce cadre. De fait : la plupart des dispositifs de sécurité sont par essence destinés à prévenir automatiquement les attaques : ou leur mise en œuvre se limite à ce périmètre.

En effet, la masse et la diversité des alertes à traiter, qu'il s'agisse de nouvelles vulnérabilités, ou d'événements de sécurité a progressivement entraîné une « désensibilisation » des équipes IT. Déjà en 2008 : le Gartner Hype Cycle montrait l'abandon de la technologie IDS (Détection d'Intrusion) au profit de sa version « automatique » : l'IPS (Prévention d'Intrusion). En effet l'IDS nécessitait une charge d'exploitation trop importante que ne pouvaient pas assumer les équipes internes. L'IPS est une solution de prévention passive dans la mesure ou le plus souvent : on l'implémente, et on l'oublie.

Distinguons d'ailleurs « prévention passive », « prévention active », et les répercussions de ces deux approches en termes de traitement des incidents. La prévention passive s'efforce d'empêcher l'occurrence d'un évènement redouté en présupposant l'anticipation de tous les scénarios d'attaque.

Des mesures de prévention, souvent technologiques, sont mises en place en assumant les limites de leur efficacité (parfois en la surestimant). A l'inverse : l'approche de prévention active peut donner lieu à une « action » préventive : les vulnérab ilités identifiées vont engendrer la mise en œuvre de mesures de réaction préventive.

A titre d'illustration : construire un mur d'enceinte pour protéger un édifice est une mesure de prévention passive : y poster un vigile rend la prévention active. On imagine mal une forteresse sans vigiles.

Face à la publication d'une nouvelle vulnérabilité exploitable sur un service WEB : l'approche préventive passive consiste à avoir préalablement mis en place un dispositif automatique de « virtual patching » : un WAF (Web Application Firewall) par exemple.

L'approche « prévention active » consiste quant à elle à corriger la vulnérabilité dès son apparition. En effet, il n'est pas du tout certain que le WAF soit à 100% efficace pour empêcher l'attaque si elle se produit.

*« On imagine mal une forteresse sans vigiles. »*

Encore faut-il disposer d'une source d'alertes de vulnérabilités en temps réel, et d'une équipe d'experts capables de statuer sur sa criticité, de spécifier techniquement une remédiation, et d'accompagner les équipes d'exploitation pour implémenter les mesures de remédiation.

Il est également possible de citer l'exemple d'une attaque ransomware : la prévention classique « best practices » consiste à disposer de sauvegardes intégrales et temps réel. Cependant, sommes-nous toujours certains que toutes les données métier de valeur ont été sauvegardées ? Ne serait-il pas également important d'avoir corrigé, 30 jours plus tôt, la vulnérabilité publiée qui a été utilisée pour réaliser l'attaque ransomware afin de tout simplement : l'éviter ?

Les dispositifs préventifs automatiques ne doivent pas être négligés : il est bien entendu utile de conserver cette approche. C'est ce qui est mis en œuvre actuellement, de façon globalement satisfaisante, sur la plupart des systèmes d'information : réduire la taille des mailles du filet, réduire la surface d'attaque. Cependant, l'avalanche d'attaques déborde nos systèmes de prévention : il devient donc obligatoire de réagir aux attaques qui passent au travers des mailles de notre filet.
Ceci met en évidence la faiblesse essentielle de nos stratégies martiales face au cybercrime : elles sont très majoritairement passives ou implémentées selon une « approche » passive. Deux aspects essentiels sont négligés dans ce contexte de harcèlement cyber-délinquant : la détection et la réaction aux incidents de sécurité. Alors même qu'il est possible de disposer d'une partie de l'outillage permettant de détecter, et donc de réagir, cela n'inclue pas l'essentiel : une « équipe » de réponse aux incidents.

La « tactique martiale » utilisée face à cet ennemi indénombrable doit être adaptée. Si les outils de prévention sont toujours nécessaires, il faudra, pour faire basculer le rapport de forces, une équipe de maintien en conditions de sécurité : le SOC (Security Operations Center).

# POURQUOI UN SOC ?

## La réponse la plus entendue est celle de la protection du système d'information contre les menaces informatiques.

En 2020, la digitalisation des usages rend caduque le simple fait de se demander si le système d'information est essentiel à l'activité de l'entreprise.

Il est malgré tout difficile d'imaginer pouvoir consacrer des efforts financiers et opérationnels identiques pour protéger l'ensemble des ressources jusqu'à la moindre imprimante (notons au passage que cet exemple peut ne pas s'appliquer à toutes les entreprises car pour certaines un arrêt de la fonction impression peut se révéler critique).

Selon les contextes, l'intégralité du SI n'est pas essentielle à la continuité de l'activité de l'entreprise. La question du périmètre se pose donc. « Un SOC pour protéger quoi, et contre quelles menaces ? »

L'analyse de risque, qu'elle s'inscrive dans une démarche globale de système de management de la sécurité, ou qu'elle soit menée dans le cadre de la définition initiale du périmètre d'un SOC, est indispensable. Elle va devoir répondre aux deux questions précédentes, et ainsi permettre de concentrer les efforts sur les fonctions essentielles du système d'information.

Parmi les résultats en sortie d'analyse de risque, le SOC va principalement se focaliser sur les scénarios de menace, mais il convient de préciser que ceux-ci sont de deux types :
- Les scénarios de menace « métier »
- Les scénarios de menace « best practices »

*« En donnant un sens business aux alertes de sécurité traitées, le SOC devient SOC Métier. »*

***Jean-Marc ODET,***
***Directeur Commercial APIXIT***

Les entreprises, qu'elles soient grandes ou petites, ont au fil du temps empilé les briques fonctionnelles,. Les conséquences organisationnelles de ces mille-feuilles technologiques, notamment en matière de sécurité IT, sont multiples.

En cybersécurité plus qu'ailleurs, les solutions génèrent un nombre sans cesse croissant d'informations. Ces solutions doivent être suivies mais également maintenues à jour et adaptées aux besoins des architectures. Ces actions, accessoires à l'activité des entreprises, sont cependant très chronophages.

En outre, bien que la notion de cybersécurité soit très répandue, ce domaine est en proie à une pénurie criante d'expertise. Il est ainsi extrêmement compliqué pour une entreprise de se doter des expertises nécessaires à un niveau optimal d'actions. De même, ces profils sont très recherchés, de sorte qu'il devient compliqué de conserver les collaborateurs.

S'appuyer sur un expert semble donc la seule solution viable à terme. Elle assure à l'entreprise le meilleur niveau d'opérabilité, de maintien à jour et d'exploitation de son infrastructure de protection. Elle lui garantit un niveau d'expertise et de disponibilité difficilement égalables en interne.

En donnant un sens business aux alertes de sécurité traitées, le SOC devient SOC Métier. Il permet alors de corréler les décisions prises aux évènements liés à la PSSI. Il offre alors au Comité d'Exploitation des métriques compréhensibles, outils nécessaires à la prise de décision.

Les scénarios « métier » découlent directement de l'analyse de risque. Il peut s'agir, par exemple, de détecter une fréquence d'accès inhabituelle à certains fichiers pour une catégorie de personnel spécifique.

Les scénarios de menace « best practices » sont des scénarios de type « attaque virale », communs à toute entreprise : ils ne sont pas obligatoirement identifiés par l'analyse de risque car leur impact n'est le plus souvent pas ciblé. De plus, leur traitement n'appelle pas d'arbitrage : cela fait partie des bonnes pratiques : il faut les traiter !

D'une façon générale, on considère que les ressources à prendre en compte par le SOC en mode « best-practices » sont à minima :

- Les systèmes de contrôle d'accès du SI interne et de(s) cloud(s) (AD, IAM, NAC, …)
- Le cloisonnement du SI interne et de(s) cloud(s) (firewalls, CASB, systèmes de détection d'intrusion, …)
- La protection anti-malwares du SI interne et de(s) cloud(s) (AV, ATP, …)

Limiter le périmètre de surveillance, en termes composants surveillés, et en terme de scénarios de détection est primordial pour que le SOC soit à la fois pertinent, et performant : il faut se concentrer sur l'essentiel.

# LES DIFFÉRENTES ACTIVITÉS DE MAINTIEN EN CONDITION DE SÉCURITÉ

Un centre opérationnel de sécurité (SOC) répond à différentes nécessités opérationnelles de maintien en conditions de sécurité. Il peut s'agir d'une équipe et d'un outillage interne à l'entreprise, externe à l'entreprise, ou d'une combinaison appropriée des deux.

Si nous prenons du recul, l'objectif du SOC va être, dans l'ordre :

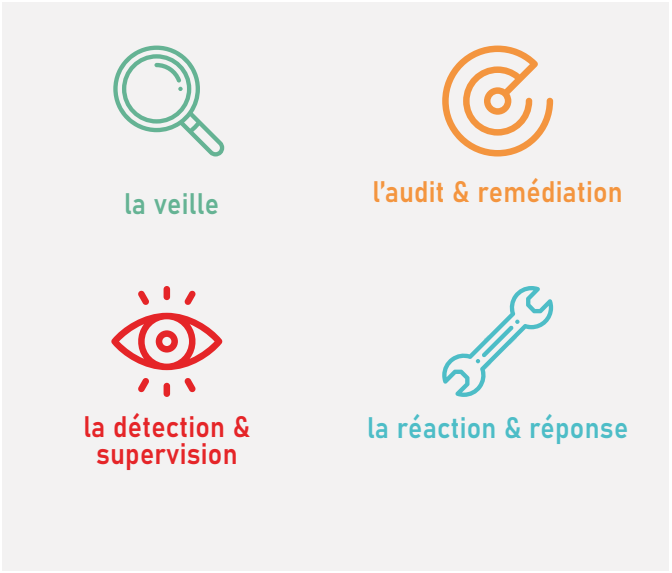
- D'anticiper un incident, idéalement afin d'empêcher qu'il ne se produise,
- Si l'incident n'a pu être évité : de limiter ou annuler ses impacts,
- Si les impacts n'ont pu être annulés, d'en limiter la durée : contribuer à un retour à la normale le plus rapide possible,
- D'effectuer une recherche de preuves associée à l'incident.

La recherche de preuves (prenant souvent le funeste nom d'« analyse post-mortem ») est une étape capitale.

Quand l'incident est inédit ou atypique, il s'agit de récolter des indices de compromission (IOC) afin de perfectionner les règles de détection.

Quand le préjudice le justifie : il s'agit de préparer les éléments à charge du dépôt de plainte (dans ce cas on perle de démarche forensique).

Le SOC ne doit pas se limiter à la seule activité de détection. En effet, différentes activités ont un rôle prépondérant aux différents stades d'un scénario d'attaque :




La veille et l'audit, deux activités de prévention active, permettent d'anticiper une attaque. C'est, rappelons-le, le premier objectif du SOC. En cas de succès, cela permet de ménager la charge de travail de l'activité détection.

La détection d'incident ou d'indices de compromission, si elle est réalisée efficacement, permet de limiter l'attaque (en impact et/ou en durée) et, de facto, la charge de l'équipe de réaction. Ceci afin de ne pas aller jusqu'à l'étape de réponse à l'incident,.

On constate que la veille et la détection donnent lieu à une réaction : remédier aux vulnérabilités pour la première ; réagir aux incidents pour la seconde.

# L'ACTIVITÉ VEILLE & AUDIT

## La veille se donne pour objectif de connaître le niveau de vulnérabilité du système d'information avant que les vulnérabilités ne soient utilisées à mauvais escient.

Il convient de distinguer les vulnérabilités « logicielles » des vulnérabilités dites de « de configuration ».

Surveiller les vulnérabilités logicielles est une démarche assez classique. Il s'agit d'inventorier les composants impliqués dans les différents scénarios de menace identifiés et de réaliser une veille quotidienne des bulletins de sécurité publiés pour ces composants.

L'outillage mis en œuvre est un flux d'information CVE (Common Vulnerabilities and Exposures), éventuellement agrégé avec des sources éditeurs : appelons ça le « flux CERT ». Si l'analyse du flux CERT est automatisable, l'intervention d'un cyber analyste est nécessaire. En effet il s'agit de valider la probabilité d'occurrence d'une attaque pour chaque vulnérabilité identifiée, ainsi que la faisabilité de mise en œuvre d'une remédiation.

Surveiller les vulnérabilités de configuration est moins évident à réaliser avec une réactivité satisfaisante (par exemple, à fréquence quotidienne), et il s'agit d'un point essentiel. Par exemple on va essayer de détecter une porte laissée ouverte par inadvertance : un port d'administration qui n'aurait dû être ouvert que temporairement.

Détecter les vulnérabilités de configuration repose sur l'audit, la recherche de mots clés et la fuite de données. Pour pouvoir le réaliser quotidiennement, il est nécessaire de l'automatiser et de le restreindre à l'essentiel. De fait, un scan de vulnérabilités est habituellement réalisé quotidiennement. Il est dit « scan de surface » (scan de ports, détection de mots de passe faibles).

Pour auditer complètement les vulnérabilités de configuration, un test d'intrusion est nécessaire. La fréquence d'audit va dépendre des enjeux associés et des moyens consacrés : le plus souvent, un test d'intrusion est réalisé à fréquence annuelle, complété par un scan de vulnérabilités complet à fréquence mensuelle ou trimestrielle.

# L'ACTIVITÉ DÉTECTION / SUPERVISION

## L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) définit l'activité de détection

La détection est la surveillance d'une liste d'éléments techniques permettant d'identifier un incident à partir d'un ou de plusieurs évènements dits « indices de compromission », et la notification immédiate des alertes ainsi générées.

Toujours selon l'ANSSI, une règle de détection peut être :

- Le résultat de l'occurrence d'un scénario de menace identifié à partir des journaux d'événements collectées sur certains composants,
- Le résultat d'une correspondance avec une signature d'attaque au sein d'un outil de détection (par exemple une sonde IDS, un antivirus).
- Une règle machine-learning basée sur un comportement identifié comme anormal.

Le niveau de gravité d'un incident découle de ses impacts prévisibles sur le système d'information. L'analyse de risques prouve encore ici son importance : c'est le seul moyen de classer objectivement les incidents et de leur affecter un niveau de priorité. En pratique le service de détection s'appuie sur un logiciel SIEM (Security Information & Event Management) dont le rôle est de transformer des événements en alertes. Les indices de compromission (éventuellement récoltés lors d'une analyse post-mortem, ou simplement best-practices), sont la base de la construction des règles de détection. Ces dernières permettent au SIEM de déclencher une alerte quand un ou plusieurs évènements correspondent au scénario de détection basé sur les IOC.

**Les sources d'événements sont variées :**

Les journaux d'évènements de certains composants identifiés comme pertinents pour le périmètre de détection considéré (voir par exemple la liste « best practice, ci-dessus)

- Les événements relatifs à la disponibilité des composants critiques (issus d'un monitoring SNMP par exemple),
- Les événements relatifs à l'intégrité de certaines ressources, issus d'outils de surveillance d'intégrité (« anti-defacing » permettant de détecter des modifications non prévues sur un site Web),
- Les événements relatifs à l'exposition aux menaces, issus d'un service de Cyber Threat Intelligence réalisant cette analyse.

Le volume de données collecté peut être important. Il l'est d'autant plus dans le cas d'une collecte de l'ensemble des journaux d'événements des composants surveillés pour constituer une base d'audit. Rappelons que les logs indexés dans le SIEM ne sont plus en format brut et incidemment, qu'ils ne constituent pas une preuve légalement recevable.

Aussi, seuls les logs utiles pour la détection des scénarios de menace identifiés sont généralement indexés et stockés dans la base de données du logiciel SIEM. Un filtrage est réalisé à cet effet : les autres logs (les logs de type « information » par exemple, ou les « access logs » d'un proxy) sont habituellement stockés en format brut sur un serveur d'archivage indépendant (communément désigné « puit de logs »). Cela permet d'optimiser la détection des incidents tout en conservant la possibilité d'accéder à l'intégralité des logs en cas d'analyse post-mortem.

Notons au passage que l'analyse des signaux faibles (concept introduit dans les années 1970 par Igor Ansof impliquant les évènements qui ne sont pas ostensiblement reliés à un scénario de menace, mais permettent de révéler des scénarios non prévus), ne doit pas être négligée. Pour prendre en compte ces évènements et les intégrer dans l'approche « best practice », il est de plus en plus frquent d'avoir recours aux technologies d'analyse comportementale utilisateur (dites UEBA : User Environment Behaviour Analytics).

Plus généralement, le machine learning, appliqué sur une grande quantité de données non-indexées, est l'intermédiaire permettant le raffinage de ce flux d'information gigantesque avant d'envoyer des alertes vers le SIEM.

Malgré ces optimisations, le volume de données indexé explose rapidement, ce qui explique une prédominance de l'utilisation de bases de données non-structurées, dites « data lakes » par les principaux logiciels SIEM de dernière génération.

Les architectures de collecte d'événements sont variées, selon que l'outillage et l'équipe sont internes au système d'information ou externes, selon que les ressources surveillées sont internes ou externes ou encore selon que les ressources sont accessibles via Internet ou non. Il est néanmoins possible de citer un certain nombre de bonnes pratiques qui restent valables dans tous les cas :

- Les flux de collecte sont chiffrés,
- Les relais de collecte et d'audit (scanner) sont isolés du système d'information de production surveillé,
- Les systèmes de notification sont isolés des bases de données d'analyse,
- L'ensemble des chaînes de liaison sont mandatées : l'architecture de collecte doit être irréprochable sur le plan de la sécurité logique,
- L'ensemble des composants impliqués dans la collecte et l'analyse sont redondés : l'architecture de collecte doit être irréprochable sur le plan de la continuité de service.
- Les logs doivent faire l'objet d'un tamponnage lors de leur acheminement jusqu'au système d'analyse, afin de prévenir tout risque de perte d'information.

Ainsi, par exemple, si le SOC est externe au périmètre surveillé, il sera nécessaire de déployer une zone démilitarisée, dite « enclave de collecte » au sein du système d'information. Dans le cas d'un service cloud, il sera possible d'utiliser Syslog over TLS, ou une API transportée via SSL.

# L'ACTIVITÉ DÉTECTION / SUPERVISION

## L'activité réaction et réponse est adossée aux activités de veille/audit et de détection/supervision.

En effet, qu'il s'agisse d'une alerte concernant une vulnérabilité identifiée par la veille ou d'un incident détecté, la raison d'être du service SOC est d'y réagir.

Cette réaction peut consister à :

- Notifier la vulnérabilité ou l'incident aux acteurs concernés, selon le plan de communication prévu,
- Remédier à la vulnérabilité / l'incident (ou limiter le risque / l'impact) selon la priorité qui y a été associée par l'analyse de risque,
- Déclencher un processus de gestion de crise.

Il peut arriver qu'un incident déborde les processus de veille et de détection. Par exemple, dans le cas d'une attaque en déni de service très rapide, cela signifie qu'il n'a pas été possible d'annuler ses impacts via les procédures de réaction prévues, ou via l'intervention réactive d'un expert.

Dans un tel cas, une collecte de l'ensemble des preuves sur l'incident est nécessaire. Celle-ci sera utile soit pour réaliser un dépôt de plainte ou pour comprendre l'événement afin d'adapter les

mesures de veille, de détection, ou de réaction.

Ces informations peuvent être de différentes natures :

- Réseau, permettant une étude du trafic réseau,
- Codes malveillants impliqués,
- Copies physiques de supports de stockage, permettant une étude discrète d'un système compromis sans risque d'altération des preuves,
- Fichiers de configuration.

L'analyse des informations collectées va permettre d'améliorer la compréhension de l'incident de sécurité, et d'en tirer les conclusions qui s'imposent dans le cadre de l'amélioration continue du Centre Opérationnel de Sécurité.

*Jean-Philippe Guillemin,*
*Consultant Cybersécurité APIXIT*

## RETOUR D'EXPEIRENCE

Voici une anecdote remontant à 2012. Un client contacte son SOC pour demander une investigation concernant une plainte reçue par son hébergeur : on l'accuse d'être à l'origine d'un flux de spam relativement important, et on s'apprête à couper son accès à Internet.

De fait, la stratégie de détection mise en place se focalisant sur les attaques en provenance de l'extérieur, le flux de spam « sortant » incriminé n'avait pas déclenché d'alerte : cela ne faisait pas partie du périmètre de détection. Un cyber analyste est donc envoyé sur site pour procéder à l'investigation.

L'analyse de l'intégralité des journaux et configurations du relai de messagerie ne révèle aucune trace d'émission massive de mails … mais on finit assez rapidement par découvrir que le proxy WEB, situé sur la même zone démilitarisée que le relais de messagerie (un proxy à l'origine trop rapidement configuré, en « open-relay ») était coupable du relayage des mails. Une simple correction de la configuration du Proxy à été réalisée, mettant fin à l'incident.

Cet exemple démontre l'importance de la définition initiale du périmètre de surveillance, et l'importance de l'équipe de réaction aux incidents. Il montre également l'importance de l'audit récurrent des configurations. Un scanner aurait détecté cette vulnérabilité bien avant qu'elle ne soit exploitée par des spammeurs, mais ce type d'audit récurrent n'avait, dans l'exemple, pas été souhaité.

# LE SOC EST UN TRAVAIL D'ÉQUIPE

## Selon le cabinet Gartner : les SOC sont des équipes de professionnels de la cybersécurité chargés de surveiller les cyberattaques et les comportements suspects sur les réseaux, ainsi que d'améliorer les contrôles et procédures de sécurité internes.

Dans le cadre de l'activité réaction, l'expérience de l'équipe SOC est primordiale, et en particulier : sa capacité de « partage » et de « capitalisation de compétences ».

Certains incidents ne requièrent pas systématiquement l'intervention d'un expert. Il peut en effet s'avérer nécessaire d'escalader à ce niveau lors de la première occurrence d'un incident dit « simple », afin de documenter la procédure de réaction.

Il est ainsi possible de confier par la suite aux techniciens de premier niveau le soin de traiter les occurrences suivantes de l'incident en respectant la procédure.

De même, certaines vulnérabilités sont intrinsèquement simples à corriger, s'il s'agit par exemple de fermer un service, ouvert par mégarde sur un routeur.

Incidemment on voit apparaitre la structure organisationnelle d'une équipe SOC :

1. Une équipe de techniciens de premier niveau (dits « N1 ») dont le rôle est de traiter 24 heures sur 24 un maximum d'incidents en mode industriel, de façon processée,

2. Une équipe de cyber-analystes experts (dits « N2 ») auxquels on va confier l'élaboration des stratégies de détection et de remédiation, ainsi que le traitement de cas complexes ou inédits, Cette équipe est également susceptible d'intervenir quelle que soit l'heure à laquelle se produit l'incident

3. Une équipe de consultants spécialisés en cyber sécurité défensive et offensive (dits « N3 ») qui vont se charger des analyses post-mortem, des analyses de code, et des tests d'intrusion.

L'équipe SOC s'inscrit donc dans un processus d'amélioration continue créant en permanence de nouveaux processus de réaction, et perfectionnant les anciens. Mais ce travail d'amélioration continue « interne » ne doit pas faire oublier une fonction essentielle : la gouvernance « globale » du service. L'importance de réaliser une analyse de risque initiale lors de la mise en place du SOC a déjà été évoquée. L'analyse de risque est une composante essentielle, et le point de départ de la gouvernance. Mais n'oublions pas qu'elle s'inscrit également de façon itérative dans l'amélioration continue du périmètre global de surveillance :

1. Planifier : analyse de risque initiale et la définition du périmètre SOC,

2. Développer : mise en place des activités de veille, détection, réaction

3. Contrôler : réalisation de Comités de Sécurité (COSEC) de revue du périmètre de surveillance, de bilan de traitement des incidents, d'audit des niveaux de services (SLA),

4. Adapter : mise à jour des fiches de traitement, adaptation du plan de communication, prise en compte de nouvelles sources d'indices de compromission, rectification des seuils de détection, …

Le pilotage de l'amélioration continue du SOC est en général confié à un consultant spécialisé (dit ROS : Responsable Opérationnel de Sécurité), rouage essentiel au fonctionnement optimal et pérenne des activités SOC.

Comme nous venons de l'illustrer, sans l'équipe SOC, l'outillage de veille, d'audit de vulnérabilités, et de détection, est une coquille vide, et ne peut pas atteindre son objectif : le passage d'une tactique de défense passive à une tactique de défense active. Pour que la tactique de défense soit active, l'humain est, jusqu'à preuve du contraire, nécessaire en dépit des progrès réalisés par les technologies de Machine Learning.

Enfin, comme le fait remarquer Peter Firstbrook, vice-président recherche de Gartner, l'équipe SOC doit rester en étroite collaboration avec les équipes métier : « si vous avez un gros incident de ransomware, quelqu'un aura la responsabilité de la relance des ac tivités, des relations publiques et juridiques ». Il est donc utile de rappeler l'importance du plan de communication associé aux activités SOC, et de noter à nouveau le rôle primordial de liaison/relation métier – SOC du Responsable Opérationnel de Sécurité.

# INTERNALISER LA FONCTION SOC : POSSIBLE ?

## Un SOC externalisé fait bénéficier l'ensemble des clients qui y souscrit, d'une base de connaissance et de procédures de traitement sans comparaison

Est-il possible d'internaliser la fonction SOC ? La réponse est oui, bien entendu. Néanmoins Bryce Austin, PDG de TCE Strategy, estime probable que seules les entreprises du Fortune 1000 ont la capacité d'implémenter un service SOC en interne. Les autres « sont plus susceptibles d'externaliser les capacités de SOC ».

Comme nous nous sommes efforcés de le montrer dans ce livre blanc : on ne peut évidemment pas se contenter de mettre en place un SIEM, ce dernier n'étant que l'un des nombreux outils nécessaires à la conduite des activités SOC.

De plus, l'exploitation d'un simple outil SIEM nécessite à minima une équipe de plusieurs experts en astreinte 24 heures sur 24. De fait, très peu d'entreprises sont en capacité d'y consacrer les budgets CAPEX et OPEX associés.

Le modèle économique d'un SOC externalisé repose sur la mutualisation des investissements et des opérations afin de les transformer en budget de fonctionnement réparti sur N clients. L'effet d'échelle est considérable compte tenu de cette mutualisation. Cela permet aux acteurs spécialisés de proposer des services de bonne qualité pour une fraction du budget de fonctionnement d'un SOC interne, et sans investissement ou presque.

Pour conclure, en considérant à nouveau l'importance de la capitalisation de compétences, il est clair qu'un SOC externalisé fait bénéficier l'ensemble des clients qui y souscrivt d'une base de connaissance et de procédures de traitement sans comparaison avec que ce que pourrait réaliser une équipe interne. Il est donc probable que les estimations communément admises concernant le nombre d'entreprises pouvant implémenter un service SOC en interne soient assez optimistes.

APIXIT
L'expertise augmentée

Ce Livre Blanc est un document d'information rédigé par la société APIXIT.
Il n'a pas vocation à servir de support de prestation de conseil.


**SIEGE SOCIAL**

Les Conquérants
Immeuble Annapurna
1 avenue de l'Atlantique
91940 LES ULIS

**RENNES**

Espace Jacques Cartier
CS 96031
35360 MONTAUBAN
DE BRETAGNE

**LILLE**

Village Créatif
10 rue de la Cense
59650 VILLENEUVE D'ASCQ

**QUIMPER**

3 allée Emile Le Page
29000 QUIMPER

**PARIS**

Immeuble AXIUM
22/24 rue du Gouverneur
Général Félix Eboué
92130 ISSY LES MOULINEAUX

**NANTES**

Les Espaces Océane
4 rue Jack London
44400 REZÉ

**REIMS**

13 rue Desbureaux
51100 REIMS

**TOULOUSE**

2 rue des Cosmonautes
31400 TOULOUSE

**LYON**

97, allée Alexandre Borodine
69800 SAINT-PRIEST

www.apixit.fr