expert

Avec le SIC, la cybersécurité passe à la défense active

Submergé d'informations, le SOC peine à faire face à la multiplication et à la dangerosité grandissante des cybermenaces. C'est pourquoi le SIC propose de changer de paradigme et d'adopter une posture résolument proactive, fondée sur le renseignement et la préparation des plans de remédiation et de reconstruction, afin de limiter les conséquences d'attaques désormais inévitables.

Le monde digital, vers lequel la crise sanitaire a poussé les entreprises à accélérer leur transition, est un monde d'opportunités, mais aussi de menaces.
En 2020, le nombre de victimes de cyberattaques ayant sollicité l'aide de l'ANSSI a ainsi été multiplié par quatre, et beaucoup d'entreprises se rendent désormais à l'évidence : la question n'est plus de savoir si elles seront attaquées, ni même si des malfaiteurs parviendront à pénétrer leurs systèmes, mais comment faire pour en minimiser les conséquences.

Tout est une question de temps. Il est inenvisageable que des *ransomware* puissent paralyser l'activité durant plusieurs jours, et quand l'offensive survient, chaque seconde compte. La défense doit donc ériger des protections, mais aussi établir des plans de remédiation et de reconstruction rapide.
Partagés avec tous les acteurs concernés, qui devront agir de façon coordonnée dans l'urgence, ces plans doivent être testés, rôdés et sans cesse actualisés. Pour cela, il est indispensable d'anticiper les menaces afin de pouvoir s'y préparer. Autrement dit, passer d'une logique de réaction à une logique d'anticipation.
Ce changement de paradigme, c'est celui qui conduit du SOC (*Security Operation Center*) au SIC (*Security Information Center*).

> ***Quand l'offensive survient, chaque seconde compte. La défense doit donc ériger des protections, mais aussi établir des plans de remédiation et de reconstruction rapide."***

Richard Nadolski,
Directeur du Business Développement
Sogeti

Frédéric De Maury,
Commercial Avant-Vente,
Global Cybersecurity Practice
Capgemini

3 points à retenir

• Le réalisme impose d'admettre que l'entreprise ne pourra parer toutes les cyberattaques, et qu'elle doit adopter une défense qui lui permette de minimiser les dégâts.

• Fondé sur le renseignement (Threat Intelligence), le SIC permet d'anticiper les menaces, et donc de mieux s'en prémunir et se préparer à leurs conséquences.

• L'automatisation, l'intelligence artificielle et une organisation repensée pour favoriser l'échange d'informations sont les clés du dispositif.

Le SOC, dépassé par la complexité

Tels qu'ils sont généralement conçus et mis en œuvre, les SOC sont de moins en moins capables de faire face aux évolutions rapides du paysage des menaces.
D'un côté, le système d'information est de plus en plus complexe, hétérogène et ouvert, avec notamment l'essor du télétravail, de l'Internet des objets et des environnements hybrides et multi-clouds.
De l'autre, les attaques sont de plus en plus nombreuses et, pour certaines, particulièrement professionnelles et sophistiquées. Au total, le SOC est submergé d'informations. Si l'on ajoute à cela la pénurie de compétences en cybersécurité, il devient quasiment impossible de séparer le bruit des menaces réelles, puis de répondre à chacune de façon adéquate.

Dispositif intégré de bout en bout, du renseignement à la remédiation, le SIC propose de dépasser ces limites en adoptant une posture proactive qui permet de devancer les menaces plutôt que de subir les flots de données de surveillance. Pour cela, le SIC repose sur quatre piliers complémentaires : **la *Threat* Intelligence**, **l'automatisation** et **l'orchestration**, **l'intelligence artificielle**, et **l'organisation**.

Threat intelligence

Pour se prémunir et se préparer, il faut d'abord identifier les menaces et les comprendre. C'est pourquoi le renseignement sur les menaces (*Threat* Intelligence) est au cœur du SIC. La *Threat* Intelligence s'organise selon quatre niveaux : stratégique (analyse de haut niveau des actifs, des périmètres et des risques), tactique (étude des modes d'action des assaillants), opérationnel (élaboration des plans de mitigation) et technique (définition des indicateurs de compromission et paramétrage des systèmes). La collecte d'informations sur laquelle tout repose doit être la plus large et décloisonnée possible : interne à l'entreprise, sur les web, *deepweb* et *darkweb*, auprès de partenaires, de pairs et des autorités dans le cadre de programmes de coopération et d'échange (ISAC…), voire provoquée au moyen de leurres (*deceptive security*).

Automatisation/orchestration

Pour donner aux équipes le temps de collecter, d'analyser et d'exploiter ces informations malgré des ressources limitées, l'automatisation est incontournable. Elle permet en particulier de traiter le bruit et de réduire considérablement le nombre de faux positifs, très chronophages. De surcroît, elle permet de réduire les coûts, et donc de dégager les moyens pour la transformation. Enfin, l'automatisation (des tâches) doit être associée à l'orchestration (des plans d'action).

En règle générale, les analystes voient d'un bon œil ces évolutions car l'automatisation les décharge de tâches peu gratifiantes, et leur permet de se concentrer sur les cas les plus intéressants et de monter en compétences.

Intelligence artificielle / Machine Learning

L'intelligence artificielle apparaît comme un maillon essentiel au fonctionnement du SIC, tant pour la détection précoce d'attaques (analyse comportementale type UEBA) que pour l'enrichissement, la contextualisation, l'aide à la priorisation ou encore la prise en charge (couplée au SOAR) d'un premier niveau de réponse. Sans elle, et le Machine Learning en particulier, il semble difficile en effet, d'identifier les signaux faibles caractéristiques des menaces au milieu du bruit et de lancer aussitôt les actions appropriées en tenant compte du contexte.

Organisation

Alors que le SOC est le plus souvent organisé de façon pyramidale, pour faire escalader les menaces les plus sérieuses vers des niveaux croissants d'expertise, le SIC est construit sur un modèle concentrique, où les spécialistes du CERT (*Computer Emergency Response Team*), au centre, diffusent les connaissances de la *Threat* Intelligence aux analystes qui les entourent.
Une possibilité est de croiser cette organisation avec une spécialisation par périmètres technologiques (IoT, cloud…) afin de renforcer encore les compétences, et donc l'anticipation.

Aujourd'hui, la plupart des grandes entreprises disposent d'un SOC, mais très peu ont encore basculé vers un SIC, car ceci nécessite au préalable un certain niveau de maturité. Pour l'atteindre, et pouvoir amorcer le processus de transition, il faut commencer par accroître ses connaissances sur les menaces (qui, pourquoi, comment), sur les cibles potentielles (systèmes, actifs critiques) et sur leur sécurisation (*Continuous Security Assessment*). Enfin, il faut mesurer la performance du SOC à travers sa capacité de détection et sa couverture défensive (en s'appuyant, par exemple, sur le référentiel ouvert *Mitre Att&ck*).

S'il reste encore beaucoup de chemin à parcourir jusqu'au SIC, les entreprises sont de plus en plus nombreuses à reconnaître avec réalisme la pertinence de ce modèle de défense active, fondé sur le renseignement, l'anticipation et la préparation. Tout simplement parce que les faits – et les menaces – ne leur laissent pas le choix.