LES INDUSTRIELS DOIVENT SE DOTER D'UN CENTRE DE SURVEILLANCE CYBER

GILLES LÉVÊQUE
directeur des systèmes d'information (DSI) du groupe ADP (Aéroports de Paris)

Pour tirer pleinement profit de la transformation numérique des modèles d'affaires et des processus opérationnels, les entreprises doivent ouvrir leurs systèmes d'information et les interconnecter à leur écosystème (clients, fournisseurs, prestataires…). Les bénéfices induits par la numérisation des entreprises ne sont plus à prouver ; ils ne seront pérennes que si les données sont protégées et les systèmes qui les manipulent sécurisés.

Dans ce contexte de menace, l'ensemble des entreprises et notamment les plus sensibles doivent continuellement progresser dans leur niveau de cyberrésilience pour faire face à l'addition du crime ordinaire, qui a été le premier à saisir le potentiel de la transformation numérique de nos modes de vie, et de l'arme cyber utilisée par des États. Pour cela elles peuvent notamment s'appuyer sur les préconisations de l'ANSSI et de l'article 22 de la loi de programmation militaire du 18 décembre 2013, qui établit un certain nombre de règles de sécurité. Les actions de protection sont évidemment primordiales, mais elles ne sont pas infaillibles et doivent être complétées par la détection au plus tôt des attaques ou des tentatives d'attaque, sachant qu'il est démontré que dans la plupart des attaques réussies l'attaquant s'était introduit depuis plusieurs semaines, voire des mois, dans le système de l'entreprise visée pour cartographier son système d'information et rendre son attaque plus efficace et même imparable.

Le SOC, une tour de contrôle indispensable

Un des éléments majeurs de cette capacité de détection est le *Security Operations Center* (SOC). Véritable tour de contrôle cyber, ses missions principales sont la détection des anomalies, leur analyse et le déclenchement des mesures pour répondre à la menace, pour garantir la continuité de service de solutions numériques supervisées. Il s'agit d'un dispositif organisationnel mettant en œuvre des moyens humains avec des compétences spécifiques, proche de la *data science*, s'appuyant sur des outils et des technologies d'analyse puissants et innovants. En effet le SOC est un très grand consommateur de données (journaux, alertes, *logs*…) générées notamment par les composants du système à surveiller et souvent consolidées au travers d'un outil de collecte des événements de sécurité appelé SIEM (*Security Information and Event Management*).

Une mise en œuvre progressive

La construction d'un SOC est un projet d'envergure, transverse, avec des impacts opérationnels importants, dont la mise en place se fait progressivement. Elle nécessite premièrement de faire le choix du *make or buy*. Chaque entreprise apportera la réponse la plus appropriée en fonction de son contexte opérationnel, de sa taille, de ses moyens et de sa maturité, mais il me semble que, compte tenu des investissements nécessaires, la mutualisation des moyens et des compétences est un

REPÈRES

La cyberguerre est déclarée ! Si les attaques cyber sont assez anciennes, par exemple l'attaque Stuxnet en 2010 attribuée à la NSA en collaboration avec les services israéliens pour neutraliser les centrifugeuses iraniennes d'enrichissement d'uranium, les épisodes WannaCry et NotPetya de l'été 2017 ont marqué les esprits par leur ampleur. Au-delà des conséquences graves pour les cibles touchées, elles ont montré le risque d'une attaque large touchant l'ensemble du tissu économique. Certains parlent même de III[e] guerre mondiale, et Florence Parly, ministre des Armées, déclarait le 18 janvier 2019 que la cyberguerre avait commencé.

élément clé, d'où l'adossement à un partenaire de confiance. Compte tenu du côté « invasif » des outils du SOC (cartographie des systèmes, sondes pour la collection des données, droits donnés à l'opérateur…), il est conseillé de choisir un prestataire qualifié (ou en cours de qualification), notamment au travers de la démarche PDIS (prestataire de détection d'incidents de sécurité) de l'ANSSI qui vise à assurer la sécurité ainsi que la compétence des prestataires. Ce choix fait, il faut ensuite travailler en mode projet avec le prestataire retenu pour cartographier le ou les systèmes à protéger, définir les cas d'usage, collecter les données (*via* le SIEM), définir des seuils d'alerte et mettre en place les outils d'analyse.

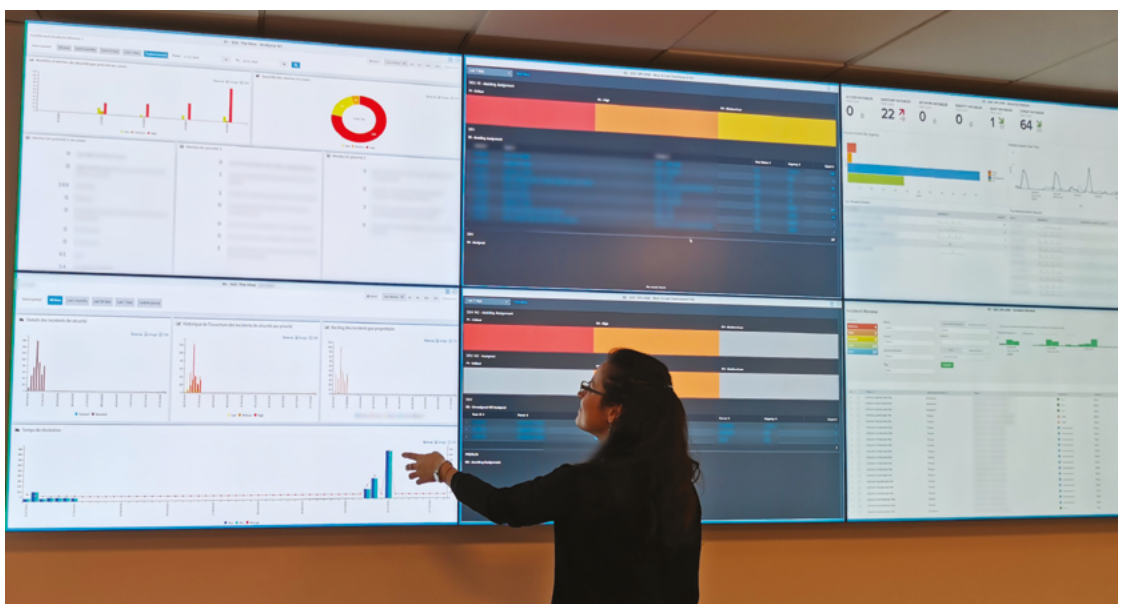
Une organisation en mouvement

Un SOC, c'est d'abord des moyens humains (opérateurs, *data scientists*, experts en sécurité informatique…) qui supervisent le comportement du système d'information, mènent des analyses de levée de doute ou d'investigation à la suite des alertes internes ou externes provenant par exemple de CERT (*Computer Emergency Response Team*) ou d'institutions comme l'ANSSI, détectent les anomalies et alertent les équipes gérant les systèmes impactés, répondent aux incidents de sécurité et administrent les outils pour les adapter en fonction de l'évolution de la menace et des systèmes à protéger. L'apport des nouvelles technologies de gestion de données massives (*big data*) et d'apprentissage (*machine learning*) est primordial. Le SOC doit en effet absorber et analyser une très grande quantité de données pour définir le comportement normal d'un système et détecter des anomalies aussi petites soient-elles. Les attaques malveillantes sont très souvent précédées du dépôt, par les attaquants, de codes ou scripts de faible taille cachés dans l'immensité des données échangées et stockées dans les SI des entreprises. Il est donc critique de détecter au plus tôt ces signaux faibles et de les corréler avec la vie du système surveillé. Les techniques de type *machine learning*, proches de l'intelligence artificielle, sont nécessaires pour modéliser le comportement « normal » du système et détecter les anomalies (connexion anormale d'un système (IP), accès à des ressources spécifiques, flux de données, horaires d'activité du système…) pouvant faire suspecter une attaque. L'anomalie est ensuite analysée et corrélée avec des événements de fonctionnement du système (panne, maintenance, activité métier…) pour déterminer s'il s'agit d'une action malveillante qu'il faut éradiquer immédiatement ou d'un fait de la vie courante du système qui viendra enrichir la base d'apprentissage du logiciel de surveillance.

Une extension de l'organisation interne

Le SOC doit réagir dans des délais très courts. Pour apporter l'expertise et la méthodologie requises au moment où l'organisation en a le plus besoin, même s'il est externalisé à un prestataire qualifié et certifié, le SOC doit être fortement lié avec les équipes internes et imbriqué avec les processus d'opération et de gestion du SI. C'est pourquoi, au-delà des compétences et de la capacité du prestataire, il est important de s'assurer que celui-ci saura adapter son organisation et ses services à la spécificité de son client en termes de risques cyber mais aussi son organisation, son périmètre technique et géographique ou encore son mode de fonctionnement. La mise en place d'un SOC requiert donc une implication forte des équipes internes et un soutien explicite de la direction pour accompagner le changement et assumer les dépenses récurrentes induites. Même si elles sont à mettre en perspective avec l'impact souvent destructeur d'une attaque cyber, la mise en place et l'opération d'un SOC peuvent être complexes et coûteuses.

"Un SOC, c'est d'abord des moyens humains."



Vue du SOC déployé par Hub One pour ses clients.