C O M M U N I Q U É D E P R E S S E

Rapport SANS Institute :
L'usage de la threat Intelligence se développe

Si l'utilisation de la Threat Intelligence pour améliorer la sécurité du SI des entreprises se poursuit, le rapport de SANS Institute montre qu'une mauvaise mise en œuvre et des équipes manquant de compétences sont souvent source d'échec.

Paris, le 5 mai 2017 - SANS Institute, référence mondiale en matière de formation, recherche et certification dans le domaine de la cybersécurité, publie les résultats d'une enquête portant sur la Cyber Threat Intelligence (renseignement sur la menace - ou CTI). Cette enquête [(1)] révèle qu'il existe encore un grand nombre d'obstacles à la mise en œuvre efficace de la CTI, dont : le manque de compétences des équipes, le manque de budget et de temps pour implémenter de nouveaux processus, un manque de moyens techniques pour intégrer la CTI, et un soutien limité de la part de la direction. Tous ces facteurs témoignent de la nécessité de renforcer la formation, mais aussi de disposer d'outils et de processus plus simples et plus intuitifs, capables de prendre en charge l'utilisation croissante de la CTI au sein des réseaux actuels.

« Les 60 % d'entreprises interrogées qui utilisent la CTI et 25 % qui envisagent de le faire à l'avenir montre que la Threat Intelligence continue de se démocratiser », déclare **Dave Shackleford, Instructeur SANS Institute**. *« Et le constat est plus que positif puisque parmi celles qui pratiquent la CTI, 78 % ont observé une amélioration de leur sécurité et de leurs capacités de réaction, un chiffre en hausse par rapport aux 64 % recensés lors de l'enquête de 2016. Les avantages de la CTI ne sont donc plus à démontrer, même si notre enquête démontre que de nombreux point d'amélioration peuvent être apportés afin que les entreprises pour profiter pleinement des avantages de la Threat Intelligence. »*

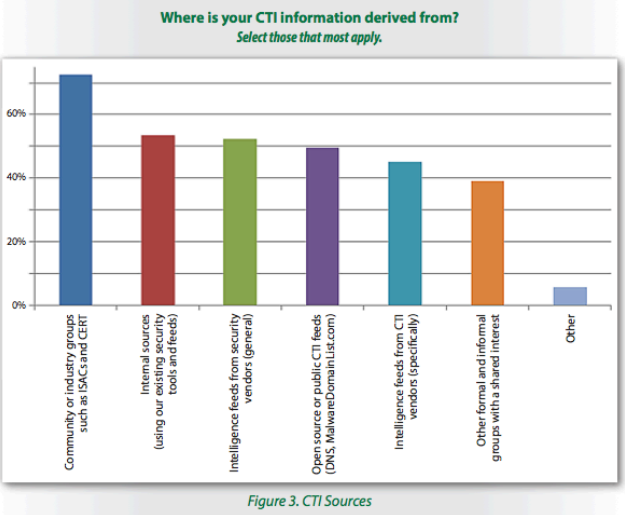

Figure 3. CTI Sources

Questionnées sur l'origine du renseignement sur la menace, 73 % des entreprises interrogées ont répondu « *Un groupe communautaire ou industriel, tel qu'un ISAC (Information Sharing and Analysis Center) ou un CERT (Computer Emergency Response Team)* ». Toutefois, de plus en plus d'entreprises optent pour un modèle hybride de la CTI combinant sources externes et internes.

Qui utilise la Threat Intelligence ?

47 % des entreprises interrogées indiquent disposer d'une équipe officiellement dédiée à la CTI, une nette progression par rapport à 2016 (28 %). Dans 9 % des entreprises, une seule personne est en charge de la CTI.

26 % des entreprises ne possèdent pas d'équipe dédiée, mais se partagent cette responsabilité. La plupart des entreprises ont mis en place une équipe interne (48 %), tandis que 47 % externalisent certains aspects de cette fonction. Seules 6 % sous-traitent entièrement la CTI. La tendance est clairement à une plus grande internalisation de la collecte et de la gestion du renseignement sur la menace.

Les réponses mettent en évidence la difficulté à recruter du personnel doté de compétences hautement spécialisées. Parmi les compétences les plus recherchées figurent une parfaite maîtrise des schémas d'attaques et des indicateurs de compromission (IOC), l'analyse des renseignements, la réponse aux incidents, ainsi qu'une connaissance des comportements normaux et anormaux.

Cette enquête montre une augmentation de l'utilité et de l'efficacité de la Threat Intelligence dans le cadre de la réponse aux incidents et des opérations de sécurité au cours des deux dernières années. 29 % des entreprises interrogées ignorent cependant dans quelles proportions l'usage de la Threat Intelligence a contribué à améliorer les fonctions de prévention et de détection. Il convient toutefois de noter qu'aucune entreprise n'a mentionné l'absence d'amélioration de ces fonctions. Contrairement à l'année dernière, le sentiment que des vols de sécurité aient bien été déjoués et que des menaces « inconnues » aient été détectées marque un changement très positif par rapport aux années précédentes.

Résultats clés :

- **Agrégation des données CTI** : les solutions SIEM sont les outils de prédilection pour la gestion de la Threat Intelligence et la plupart des entreprises y ont recours avec une interface utilisateur intégrée.

- **Reporting CTI** : 51 % des entreprises sont satisfaites de leurs rapports CTI, mais doivent néanmoins procéder à un nettoyage et à d'autres manipulations manuelles. Seules 14 % jugent les rapports excellents. 32 % avouent ne pas savoir comment exploiter les données CTI qu'elles reçoivent.

- **Niveau de satisfaction des éléments CTI**
  Les équipes sont pleinement satisfaites de la pertinence des informations sur les menaces (80 %), de la « propreté » et de la qualité des données (76 %), ainsi que du caractère opportun de la CTI et de la visibilité sur les menaces et sur les indicateurs de compromission (à égalité à 74 %).

  Les entreprises interrogées sont moins satisfaites des fonctions actuelles de machine learning et d'analyse (49 %), de l'identification et de la suppression des indicateurs de compromission obsolètes et autres données anciennes (61 %), et de la visibilité basée sur la géolocalisation (69 %).

- **Obstacles à une mise en œuvre efficace** : la majorité des entreprises interrogées (53 %) ont estimé que le manque de personnel formé et de compétences constituaient le principal obstacle à la mise en œuvre efficace de la Threat Intelligence. La moitié des entreprises ont déclaré que le manque de moyens financiers représentait un handicap majeur, tandis que 42 % ont cité le manque de temps.

Conclusion et perspectives

Cette année, les réponses à l'enquête du SANS Institute indiquent une amélioration aussi bien des outils, des technologies et des compétences CTI, que de l'intégration de cette discipline. Les équipes de sécurité reconnaissent plus que jamais les avantages offerts par la collecte et l'exploitation du renseignement sur la menace pour les opérations de sécurité et la réponse aux incidents.

Néanmoins, l'intégration de la Threat Intelligence avec d'autres outils et technologies n'en est encore qu'au stade embryonnaire. L'automatisation et l'analyse sont des domaines qui méritent d'être améliorés. Et il est encore difficile de trouver du personnel disposant des compétences requises.

« Au fur et à mesure que la Threat Intelligence se développe, on observe un besoin croissant de professionnels mieux formés, qui sachent non seulement exploiter les données récoltées, mais aussi mettre en place, intégrer et gérer des projets au sein des entreprises », précise **Dave Shackleford**. *« Notre rapport montre qu'il y a également un besoin d'indicateurs et de fonctions de reporting plus efficaces, notamment en raison d'un manque de temps et de budgets, un tiers des équipes ne bénéficiant pas du soutien de la direction. Tant que nous pourrons démontrer l'intérêt de la CTI dans la prévention, la détection et la réponse aux attaques actuelles, cette discipline gagnera en maturité et jouera un rôle plus important que jamais dans les programmes de cybersécurité. »*

(1) L'enquête a été menée au niveau international sur un panel de 600 professionnels de l'informatique évoluant dans un large éventail de secteurs : industries, banques, éducation, santé, nouvelles technologies et services publics.

Téléchargez l'étude dans son intégralité : ici

À propos de SANS Institute (@SANSInstitute)

Créé en 1989, SANS est la référence mondiale en matière de formation, recherche et certification dans le domaine de la cybersécurité. Les formateurs mondialement reconnus de SANS ont déjà formés plus de 140 000 professionnels, issus du secteur public et privé et enseignent chaque année plus de 60 cours qui s'alignent sur les rôles, responsabilités et disciplines majeur des équipes de sécurité. SANS Institute propose des cours qui sont alignés sur les 30 certifications techniques GIAC dans le domaine de la sécurité de l'information. GIAC (Global Information Assurance Certification) valide ainsi les compétences des professionnels de la sécurité de l'information, attestant que ceux qui sont certifiés ont les connaissances techniques nécessaires pour travailler dans des domaines clés de la cybersécurité.

SANS Institute développe et publie de nombreuses ressources mis à disposition gratuitement, y compris des bulletins d'information, des livres blancs et des webcasts (www.sans.org).

Les inscriptions à l'événement « SANS Paris 2017 » sont ouvertes : https://www.sans.org/event/paris-2017.

Contacts presse

Laëtitia Berché
Cymbioz
+33 1 42 97 93 30 / + 33 6 14 48 02 95
laetitia.berche@cymbioz.com
www.cymbioz.com