ThreatQuotient livre une bibliothèque universitaire automatisée des menaces

On parle beaucoup aujourd'hui de *threat intelligence*, c'est-à-dire de l'ensemble des actions de renseignement – d'origine et/ou d'intérêt cyber – permettant de prémunir toute entité d'une menace potentielle. Un marché du renseignement qui est très actif comme le montre le rachat probable du cabinet Lexsi par Orange Cyberdéfense. Parmi les acteurs qui vont animer ce marché, ThreatQuotient tente sa chance en France.

Start-up d'origine américaine, elle a recruté deux anciens de chez Cisco et SourceFire pour mener à bien cette aventure. Cyril Badeau et Yann le Borgne ont donc pour mission de faire connaître ThreatQ. « *La plateforme agit comme une bibliothèque universitaire des menaces à disposition des SOC (Security Operation Center, NDLR). Elle est reliée à plusieurs sources (feeds), Open Source ou des remontée issues de l'industrie (pharmacie, finance, etc.)* », précise Cyril Badeau. Est-ce que cela ne rentre pas justement en concurrence avec les SOC ou les CERT qui sont capables de faire remonter des événements de sécurité ou des alertes ? « *Non, il n'y a pas de remplacement des SOC ou des CERT, mais une automatisation des actions manuelles* », réplique le responsable.

Des renseignements de confiance et automatisés

Et c'est bien sur cette automatisation que mise ThreatQuotient. « *Il y a une industrialisation des réponses sur incident face à une automatisation des attaques, il faut donc bien comprendre l'ennemi et jouer sur son propre terrain* », reconnaît Cyril Badeau en citant les récentes offensives de ransomwares comme Locky. Ces derniers sont capables de muter rapidement avec de nouvelles adresses IP, d'autres serveurs C&C dont les domaines peuvent être générés par algorithme, etc. Il est donc essentiel de « *trouver une cohérence* » pour connaître les adversaires. Ainsi pour Locky, « *la plateforme permet d'agglomérer les données sur le spearphishing, quel xmailer a été utilisé, etc., de s'assurer que le regroupement des informations dispose d'un haut niveau de confiance et de les renvoyer au SOC, via un connecteur, qui peut les comparer avec un SIEM (Security Information and Event Management) et prendre des mesures plus rapidement* », décrit Yann Le Borgne.

En s'adressant au marché des SOC, ThreatQuotient est optimiste pour la France. « *Il y a environ 5% du marché qui est mature en matière de SOC sur lesquels nous allons nous focaliser, il y a moins besoin de pédagogie pour montrer ce que l'on apporte* », explique Cyril Badeau. Mais ce marché devrait progresser pour atteindre 50% d'ici 10 ans. *« Il sera difficile à l'avenir d'être un SOC managé sans intégrer de la threat intelligence »*, prophétise le dirigeant. Il devrait renforcer ses équipes d'ici la fin de l'année

A lire aussi :

Ralentir les hackers, la meilleure façon de les éloigner

Piratage des SCADA, cessez de prendre des selfies !