Threat intelligence : les entreprises craignent l'indigestion de données

Le Ponemon Institute a mené l'enquête (« *Value of Threat Intelligence* »). Le sondage sponsorisé par le fournisseur Anomali a été réalisé cet été auprès d'un échantillon de 1072 professionnels IT et responsables de la sécurité informatique basés en Amérique du Nord et au Royaume-Uni.

70% des répondants pensent que l'information sur les menaces (Threat Intelligence) est souvent trop volumineuse ou trop complexe. Ils sont presque aussi nombreux (69%) à estimer que leur entreprise n'a pas les compétences en interne ou les profils experts nécessaires pour définir et mettre en oeuvre les mesures qui s'imposent. Et 52% jugent que leur organisation ne dispose pas de technologies adaptées pour répondre à la sophistication des cyberattaques actuelles.

Résultat : moins de la moitié des professionnels interrogés (46%) pensent que les données sur les menaces sont effectivement utilisées pour répondre à une activité malveillante.

Trop de données, pas assez d'experts

« *Il y a trop de données pour vraiment les comprendre si vous avez des ressources limitées…, notamment si vous manquez d'analystes des menaces* », déclare dans les colonnes de *CSO* Travis Farral, directeur de la stratégie de sécurité d'Anomali. Cela peut devenir un casse-tête chronophage et coûteux.

L'étude montre également que les données sur les menaces sont encore peu partagées avec le top management et les membres du conseil d'administration. Seuls 31% des répondants disent que ces informations sont utilisées pour sensibiliser cadres dirigeants et administrateurs aux risques de sécurité auxquels les organisations sont confrontées aujourd'hui… La faute à la DSI ?

Lire aussi :

Les RSSI des grandes entreprises se sentent invincibles
Des services de Level 3 interrompus : une nouvelle attaque DDoS Mirai ?
Un hôpital anglais ferme pour traiter son virus… informatique

crédit photo © Ollyy-Shutterstock