kaspersky BRING ON THE FUTURE

Comment la Threat Intelligence peut-elle répondre aux besoins de votre organisation ?

Threat Intelligence : s'adapte à vos besoins

La Threat Intelligence implique la collecte de vastes volumes de données brutes sur les menaces actuelles ou potentielles visant une organisation, qui sont ensuite affinées à l'aide d'une combinaison d'algorithmes de machine learning et d'expertise humaine dans le but de produire des informations exploitables. Les centres d'opérations de sécurité (SOC) peuvent utiliser ces informations pour accroître leurs capacités de détection, d'enquête et de recherche des menaces afin de prévenir de futures cyberattaques.

Nombreux sont ceux qui ont présenté la Threat Intelligence comme un élément essentiel de la sécurité à l'ère des menaces avancées telles que les menaces persistantes avancées (APT) et les attaques de type « zero-day ». En effet, les organisations qui disposent d'une Threat Intelligence pertinente et de qualité peuvent acquérir une compréhension claire du paysage unique des menaces auxquelles elles sont confrontées, garder une longueur d'avance sur les pirates et mettre rapidement en place des mesures préventives. Face à une protection aussi efficace, les acteurs malveillants se tourneront vers des proies plus faciles.

Toutefois, si les flux de Threat Intelligence ne sont pas bien gérés ou si les renseignements sur les menaces sont de mauvaise qualité, ces « informations » peuvent en fait nuire aux SOC, en les submergeant de données non pertinentes. Les ressources en matière de sécurité, déjà très sollicitées, le sont encore plus, et le résultat net pour les organisations est négatif.

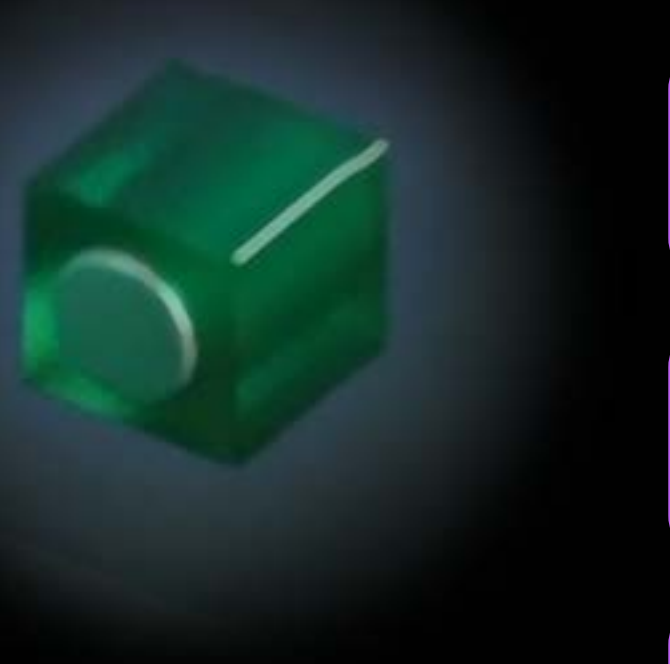
Examinons en détail ce qui se passe lorsque la Threat Intelligence n'est pas adaptée aux besoins d'une organisation. Nous verrons ensuite à quoi ressemble une Threat Intelligence de bonne qualité et sur mesure. L'analyse des deux aspects nous aidera à comprendre la véritable valeur de la Threat Intelligence sur mesure pour la sécurité des organisations.

Que se passe-t-il lorsque la Threat Intelligence n'est pas conçue sur mesure ?

Commençons par poser la question inverse : à quoi ressemble une Threat Intelligence non conçue sur mesure ?

Aujourd'hui, de nombreuses entreprises vendent une forme ou une autre de Threat Intelligence, dont le contenu et la qualité varient considérablement. Et si de nombreuses organisations considèrent la Threat Intelligence comme un élément essentiel de la sécurité, elles sont beaucoup moins nombreuses à considérer qu'elles parviennent à détecter efficacement les menaces externes.

Voici trois façons dont la Threat Intelligence peut s'avérer inutile :



Qualité médiocre – par exemple, d'immenses « données brutes » sur les activités criminelles compilées à partir de forums clandestins ou encore de vastes quantités d'informations indifférenciées sur les nouveaux programmes malveillants et les exploits logiciels. Bien que certaines informations puissent être exactes et pertinentes, de tels raz-de-marée de données peuvent accabler une organisation s'ils ne sont pas transformés en informations exploitables.

Inexactitude – des informations fausses ou trompeuses entravent une organisation, de même qu'un raisonnement et une analyse médiocres.

Non-pertinence – les informations peuvent être totalement exactes mais ne pas être pertinentes pour votre organisation, votre pays ou votre secteur d'activité. Comparez cela à un registre de police (le compte-rendu quotidien des événements dans un poste de police) : les renseignements non pertinents sont comme un registre de police concernant une ville d'un pays où vous n'êtes jamais allé et où vous n'avez pas l'intention de vous rendre.

Quel est le résultat net d'un tel manque d'informations ?

1. **Une augmentation du nombre de faux positifs.** Le simple fait d'introduire une série de données dans le système sans les avoir soigneusement examinées et affinées aura pour effet de déclencher les capteurs du réseau tel un arbre de Noël, générant une cacophonie que les analystes, déjà débordés, devront filtrer.

2. **Un faux sentiment de sécurité.** Vous pensez que vous êtes en sécurité parce que vous recevez beaucoup d'informations sur les menaces auxquelles vous êtes exposé. Or, ces informations sont en fait inutiles, et votre complaisance vous rend encore plus vulnérable.

3. **Des ressources mal orientées.** Lire des rapports de mauvaise qualité, examiner des faux positifs et mener des enquêtes inutilement approfondies fondées sur une catégorisation erronée des menaces (par exemple, penser qu'un incident est un APT au lieu d'un cybercrime ordinaire) sont autant de facteurs qui pèsent sur les précieuses ressources des équipes de sécurité.

À quoi ressemble donc une Threat Intelligence conçue sur mesure ?

Nous pouvons aborder cette question en appliquant l'analogie des catastrophes naturelles. Imaginez que les organisations soient comme des pays, chacun avec ses propres ressources, systèmes de défense et menaces. Les menaces ne sont pas les mêmes pour un pays côtier de faible altitude que pour un pays montagneux enclavé. Ces régions sont vulnérables à des forces différentes et ont des priorités différentes en matière de défense.

Cependant, si chaque pays a un paysage de menaces unique en fonction de sa géographie, de ses ressources et de ses défenses, les pays voisins sont confrontés à des menaces similaires. Les pays dont le cœur de métier est l'agriculture, par exemple, seront vulnérables aux inondations. Ces nations peuvent partager des informations et appliquer des stratégies défensives similaires, bien qu'il n'existe pas deux stratégies identiques.

Sur le plan organisationnel, les priorités défensives d'une startup fintech seront très différentes de celles d'une agence gouvernementale. Les outils adaptés à l'un ne seront pas utiles à l'autre.

En tenant compte de cette analogie, considérons la Threat Intelligence pour les organisations modernes.

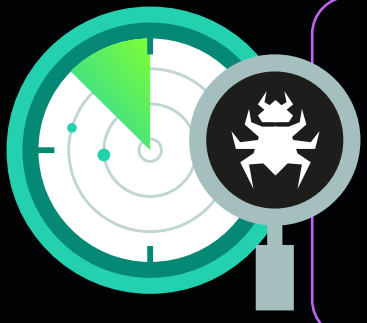
Sources internes

La première étape d'un système de défense contre les menaces intelligent et adapté consiste à évaluer l'infrastructure de sécurité de l'organisation du point de vue d'un pirate informatique potentiel : où sont les vulnérabilités et quelles sont les principales ressources, les « bijoux de la couronne » ? L'établissement du profil d'une organisation entière est un travail considérable, mais toutes les informations ne sont pas de même nature confidentielle. C'est pourquoi il est préférable d'adopter une approche fondée sur les risques, en se concentrant d'abord sur les cibles les plus vulnérables.

Une fois que les ressources sont identifiées, des points de collecte de données peuvent être mis en place autour d'elles et cartographiés à l'aide d'informations sur les menaces externes, tout comme la construction d'un barrage sur une rivière vulnérable. Vous pouvez également prévoir le chemin le plus probable qu'emprunteront les pirates informatiques et mettre en place des pièges et des pots de miel.

Ces sources internes de Threat Intelligence, y compris l'évaluation du trafic normal et la détection des anomalies, sont les plus précieuses, car elles sont les plus pertinentes pour l'organisation.

Le but est de mettre à profit la connaissance approfondie de ses propres ressources pour instaurer des mécanismes de défense sur mesure plutôt que des contrôles de sécurité génériques et traditionnels.



Sources externes

L'étape suivante consiste à se tourner vers l'extérieur et à observer ce qui se passe dans d'autres organisations de la même zone géographique et du même secteur. De nombreuses organisations ont tout à gagner à appartenir à des ISAO et des ISAC (Information Sharing and Analysis Organizations and Centers), qui facilitent l'échange de Threat Intelligence relative à des groupes hostiles touchant leurs pairs. Il existe aujourd'hui de nombreux fournisseurs commerciaux de Threat Intelligence, qui proposent aux organisations de leur fournir des informations en rapport avec les menaces particulières auxquelles elles sont confrontées.

Voici ce que l'on trouve habituellement dans ce type d'informations, qu'elles proviennent d'un service gratuit ou d'un fournisseur payant :

Types de menaces – risques auxquels sont confrontées des organisations similaires (par exemple, phishing ciblé, groupes APT, etc.). Il peut également s'agir de vulnérabilités découvertes dans les produits, appareils et infrastructures les plus utilisés dans une industrie donnée. Ces informations peuvent ensuite être exploitées. Par exemple, si des organisations comme la vôtre sont généralement la cible d'attaques de phishing, vous pouvez investir dans la formation du personnel et dans des mesures de défense contre le phishing.

Profils des cybercriminels – indicateurs de compromission particuliers ; tactiques, techniques et procédures (TTP) ; schémas d'attaque propres à des acteurs en particulier qui s'attaquent à une industrie donnée. Ces informations peuvent être utilisées immédiatement dans le cadre d'un exercice de recherche des menaces au sein de l'infrastructure de l'organisation. Il existe peut-être une compromission qui n'avait pas été remarquée. Elles peuvent également être utilisées pour bloquer les pirates informatiques et informer les analystes sur les modèles à surveiller.

Risques numériques – il s'agit des informations les plus précises possibles, puisqu'elles concernent des informations sur des organisations particulières qui circulent sur le Dark Web. Ces informations peuvent inclure des services vulnérables découverts sur le périmètre du réseau de l'organisation, des identifiants compromis ou un accès initial au réseau de l'organisation vendu sur des marchés clandestins. Une fois découverts, ces vecteurs d'attaque peuvent être rapidement bloqués.

Conclusion

Le suivi, l'analyse, l'interprétation et la lutte contre les menaces informatiques, en perpétuelle évolution, représentent un travail considérable. Dans tous les secteurs, les entreprises manquent de données actualisées et pertinentes pour gérer les risques liés aux menaces informatiques. Les connaissances et l'expérience approfondies de Kaspersky dans tous les domaines de la cybersécurité en font le partenaire de choix des plus grandes autorités de police et administrations au monde, comme INTERPOL et les CERT majeurs. Kaspersky Threat Intelligence vous donne accès instantanément aux informations techniques, tactiques, opérationnelles et stratégiques nécessaires pour atténuer ces cybermenaces, fournies par notre équipe de chercheurs et d'analystes internationaux.

Qu'il s'agisse des soins de santé, de la finance, des transports, de la vente au détail ou de l'industrie, les différents secteurs du monde ultra connecté d'aujourd'hui sont tous confrontés à des formes particulières de cybermenaces visant à exploiter les vulnérabilités propres à leur industrie. Cependant, toutes les entreprises modernes partagent deux points communs : la menace réelle d'une cyberattaque et la nécessité de disposer d'une Threat Intelligence sur mesure pour garder une longueur d'avance sur leurs adversaires.

Comme indiqué précédemment, de nombreux fournisseurs de Threat Intelligence ont récemment fait leur apparition sur le marché, proposant des informations qui peuvent varier à la fois sur le plan de la qualité et de la surface d'attaque pour laquelle elles ont été produites. Une organisation qui cherche à renforcer son programme de sécurité devrait donc trouver un fournisseur qui fournit des données de haute qualité pour les types particuliers de défis auxquels elle est confrontée. Si elle est pertinente, précise et adaptée aux besoins de l'organisation, une Threat Intelligence bien mise en œuvre peut permettre d'accéder à une infrastructure de sécurité robuste et cyber-résiliente tout en permettant de réaliser des économies considérables de temps, d'argent et de ressources.

En savoir plus sur Kaspersky Threat Intelligence

Kaspersky
Threat Intelligence

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique :
https://www.kaspersky.fr/blog/category/business/
Sécurité informatique pour les PME : https://www.kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : https://www.kaspersky.fr/enterprise-security
Portail de Threat Intelligence : opentip.kaspersky.com
Interactive Portfolio Tool (outil de catalogue interactif) :
https://media.kaspersky.com/fr/business-security/enterprise/KL-Enterprise-Catalogue.pdf

www.kaspersky.fr