kaspersky BRING ON THE FUTURE

Threat Intelligence : optimiser les avantages

Threat Intelligence : un outil essentiel dans la défense proactive contre les menaces

Selon une analyse de Kaspersky, le marché mondial de la Threat Intelligence (TI) représentait 1,386 milliard de dollars américains en 2022, avec un taux de croissance annuel composé de 15,8 % entre 2022 et 2025.

Pour de nombreuses organisations (en particulier celles qui sont vulnérables aux attaques ciblées et aux menaces persistantes avancées (APT), la TI est un outil essentiel pour assurer une défense proactive contre les menaces.

Cependant, si les utilisations et les avantages des technologies de l'information sont nombreux et variés, il en va de même pour leurs sources, à tel point qu'essayer d'identifier ce qui fonctionnera le mieux pour votre organisation particulière peut être un défi en soi. Quels sont donc les points à surveiller en 2023 et comment faire en sorte que la TI apporte le maximum d'avantages à votre entreprise ?

Éviter d'aggraver les problèmes existants

Pour vous aider à vous y retrouver dans les différentes options, la chose la plus importante à garder à l'esprit est que la TI qui n'est pas adaptée ou personnalisée aux spécificités de votre entreprise peut aggraver vos problèmes.

Dans de nombreuses organisations, les analystes de la sécurité passent aujourd'hui plus de la moitié de leur temps à trier les faux positifs au lieu d'identifier les menaces et d'y répondre de façon proactive, rallongeant ainsi considérablement les délais de détection. Alimenter vos opérations de sécurité avec des données vagues ou inappropriées augmentera le nombre de fausses alertes et aura une incidence négative importante sur vos capacités de réponse ainsi que sur votre sécurité dans son ensemble. Comment éviter cela ?

Évaluation des sources commerciales de TI

Bien qu'il n'existe pas de critères universellement reconnus pour évaluer les offres commerciales de TI, les éléments à prendre en compte sont les suivants :

- Parmi un large éventail de fournisseurs, recherchez une technologie de l'information qui vous permette de mieux comprendre votre propre paysage de menaces, par exemple grâce à une analyse détaillée des menaces historiques et émergentes ciblant votre secteur d'activité, votre zone géographique ou votre entreprise, afin d'améliorer les performances de fonctions telles que la gestion des vulnérabilités, la recherche de menaces, la réponse aux incidents et bien d'autres encore.
- Si vous avez déjà mis en place des contrôles et des processus de sécurité et que vous souhaitez combiner les technologies de l'information avec les outils que vous utilisez et connaissez déjà, recherchez des méthodes de livraison, des mécanismes d'intégration et des formats qui permettent une intégration harmonieuse des technologies de l'information dans vos opérations de sécurité existantes.
- Privilégiez également les informations dont la portée est globale. Comme les cyberattaques sont sans frontières, le fournisseur fournit-il des informations à l'échelle mondiale et rassemble-t-il des activités en apparence incohérentes pour les intégrer dans des campagnes cohérentes ? Les informations de ce type vous aideront à prendre plus de mesures appropriées.
- Si vous êtes à la recherche d'un contenu plus stratégique pour éclairer votre planification de la sécurité à long terme, recherchez un fournisseur de TI ayant fait ses preuves en matière de découverte et d'investigation continues de menaces complexes dans votre zone géographique et/ou votre secteur d'activité. La faculté du fournisseur à adapter ses capacités de recherche aux particularités de votre entreprise est également cruciale.

Utilisation d'une plateforme de TI

Une plateforme de Threat Intelligence (TIP) vous aide à agréger, gérer et rendre opérationnelle la Threat Intelligence, ce qui est vital lorsque vos outils de sécurité utilisent une Threat Intelligence provenant de sources multiples. Plus particulièrement, une plateforme de TI doit vous permettre de faire ce qui suit :

- Répondre plus efficacement aux menaces en vérifiant tout indicateur de menace que vous jugez suspect, qu'il s'agisse d'un fichier, d'un hachage de fichier, d'une adresse IP ou d'une adresse Internet.
- Vous pouvez analyser les fichiers pour détecter les menaces complexes, évasives et de type APT.
- Envoyer des adresses IP, des hachages de fichiers, des noms de domaines ou des adresses Internet que vous considérez comme suspects, afin de valider et de hiérarchiser rapidement les alertes et les incidents à l'aide de niveaux de risque et d'informations contextuelles permettant de déterminer quelles sont les menaces réelles.
- Vous pouvez recevoir des rapports réguliers relatifs au fonctionnement de certains fichiers ou de certaines adresses Internet spécifiques.
- Automatiser les flux de travail de sécurité en connectant vos applications avec la plateforme de TI.

Comment Kaspersky peut vous aider

Le portefeuille de Threat Intelligence de Kaspersky couvre une gamme complète de scénarios de sécurité, notamment la prévention, la détection, l'enquête, la réponse et les rapports stratégiques, qui peuvent tous être adaptés aux besoins des organisations individuelles. Notre équipe Global Research and Analysis Team (GReAT) est un groupe d'élite d'experts en sécurité qui, grâce à l'infiltration de communautés fermées et de forums obscurs dans le monde entier, a découvert et disséqué plus de 50 attaques ciblées parmi les plus sophistiquées au monde. Par ailleurs, nos connaissances et notre expérience approfondies dans tous les domaines de la cybersécurité font de nous le partenaire de choix des plus grandes autorités de police et administrations au monde, comme INTERPOL et les CERT majeurs.

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

Reconnu. Indépendant. Transparent. Nous nous engageons à construire un monde plus sûr où la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Pour en savoir plus, rendez-vous sur kaspersky.fr/about/transparency

Proven. Transparent. Independent.