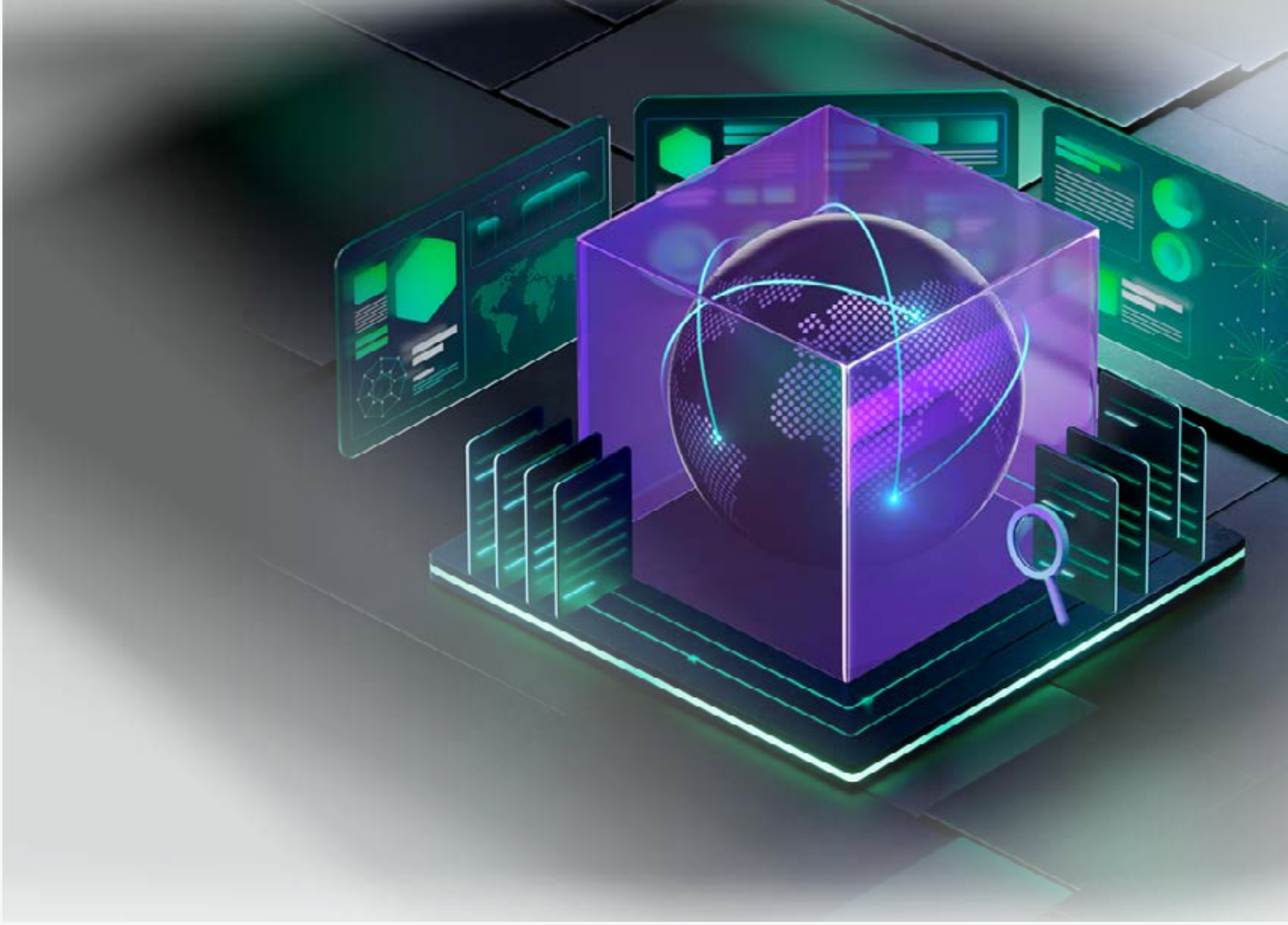


Kaspersky Threat Intelligence

Évaluation des sources de Threat Intelligence

kaspersky BRING ON THE FUTURE

Plus d'informations sur kaspersky.fr
#bringonthefuture

Introduction

Avec l'expansion des surfaces d'attaque et la sophistication croissante des menaces, se contenter de réagir à un incident n'est pas suffisant. Les environnements de plus en plus complexes offrent de multiples opportunités aux attaquants. Chaque secteur, chaque entreprise dispose de ses propres données spécifiques à protéger, et utilise son propre ensemble d'applications, de technologies, etc. Par conséquent, il existe de multiples méthodes possibles pour lancer une attaque, avec de nouvelles méthodes émergeant chaque jour.

Au cours des dernières années, les frontières entre les différents types de menaces et les différents types de cybercriminels se sont estompées. Les méthodes et les outils représentant auparavant une menace pour un nombre limité d'entreprises se sont considérablement étendus. On peut citer par exemple le groupe Shadow Brokers, qui a divulgué du code, mettant ainsi des vulnérabilités avancées (prétendument développées par la NSA) à la disposition de groupes criminels qui n'auraient autrement pas eu accès à ce type de code sophistiqué. Mentionnons aussi l'émergence des campagnes de menaces ciblées avancées (APT), qui se concentrent non pas sur le cyberespionnage, mais sur le vol d'argent pour financer les autres activités du groupe APT. Et la liste est longue.

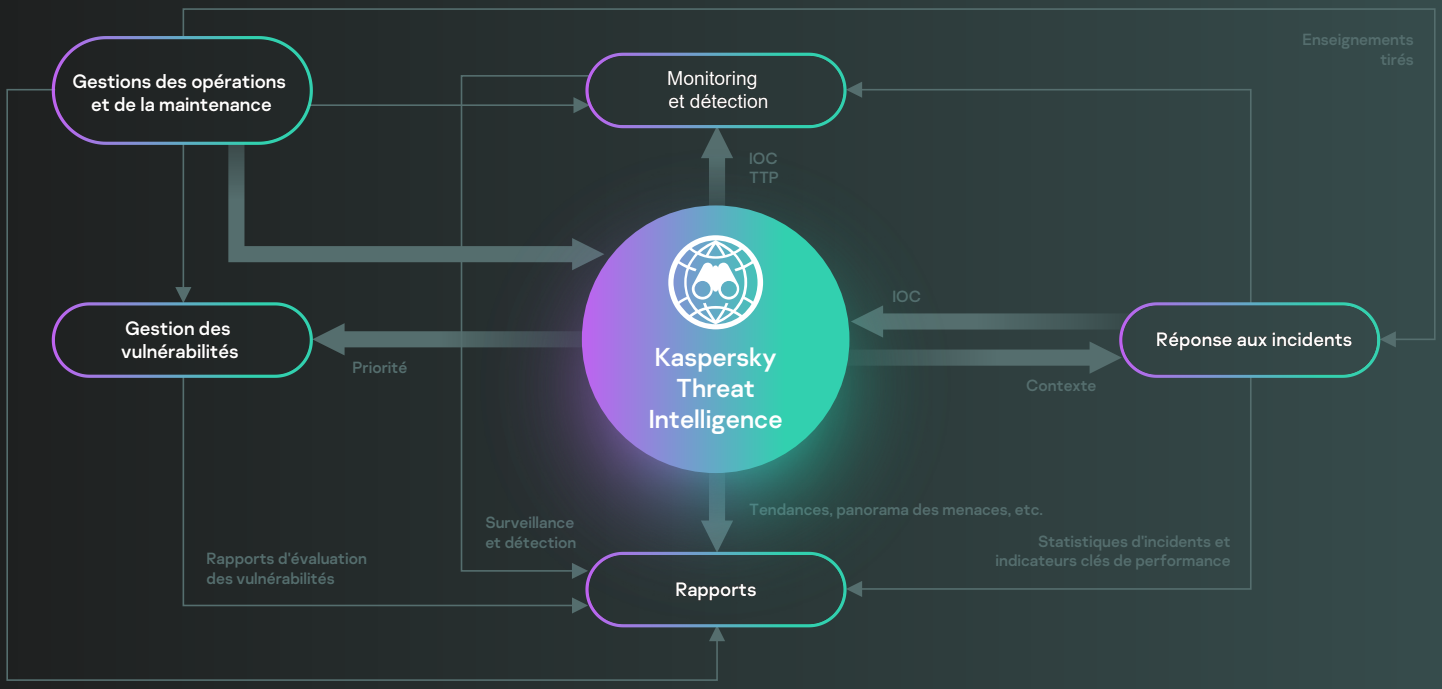
Une nouvelle approche est nécessaire

Les méthodes et les outils représentant auparavant une menace pour un nombre limité d'entreprises se sont considérablement étendus.

Les entreprises subissant toujours plus d'attaques ciblées et sophistiquées, il est clair qu'une défense efficace nécessite de nouvelles méthodes. Pour se protéger, les entreprises doivent adopter une approche proactive, adapter constamment leurs contrôles de sécurité à l'environnement à risques en constante évolution. Le seul moyen de faire face à ces changements consiste à développer un programme efficace de Threat Intelligence.

La Threat Intelligence est d'ores et déjà un composant clé des opérations de sécurité établies par les entreprises de différentes tailles, sur l'ensemble des secteurs et des zones géographiques. Disponibles dans des formats interprétables à la fois par des machines et par des humains, les informations de Threat Intelligence peuvent fournir aux équipes de sécurité des données pertinentes tout au long du cycle de gestion des incidents et leur permettre de prendre des décisions stratégiques éclairées (figure 1).

Cependant, la demande croissante en matière de Threat Intelligence externe a donné lieu à une abondance de fournisseurs de solutions de Threat Intelligence, chacun proposant un éventail de services différents. Sur un marché étendu et compétitif proposant une multitude d'options complexes, il peut être déroutant, voire extrêmement frustrant de choisir la solution adaptée à son entreprise.



Graphique 1

Opérations de sécurité reposant sur la Threat Intelligence

La Threat Intelligence non adaptée aux besoins qui vous sont propres peut empirer les choses. Dans de nombreuses entreprises, 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 créera un impact négatif majeur sur vos capacités de réponse, ainsi que sur la sécurité de votre entreprise dans son ensemble.

Où trouver des solutions d'information appropriées ?

Comment évaluer les nombreuses sources de Threat Intelligence, comment identifier les plus adaptées à votre entreprise et comment les exploiter efficacement ? Comment naviguer parmi la multitude de fournisseurs qui revendiquent tous la solution la plus efficace ?

Ces questions, bien que légitimes, ne sont pas les premières que vous devez vous poser. Attirées par les messages criards et les promesses ambitieuses, de nombreuses entreprises croient qu'un fournisseur externe peut leur fournir une sorte de vision à rayons X superpuissante, omettant totalement le fait que les informations les plus précieuses résident dans le périmètre de leurs propres réseaux d'entreprise...

Les données des systèmes de détection des intrusions et de prévention, les pare-feu, les journaux d'applications et les journaux des autres contrôles de sécurité peuvent en dire long sur ce qui se trame dans le réseau d'une entreprise. Elles peuvent identifier des schémas d'activité malveillante spécifique à l'entreprise. Elles peuvent permettre de différencier un utilisateur ordinaire et un comportement réseau et contribuer à suivre l'activité d'accès aux données.

Graphique 2

Mise en œuvre de la Threat Intelligence externe

Mettez-vous dans la peau d'un attaquant

Pour concevoir un programme efficace de Threat Intelligence, les entreprises, et notamment celles qui disposent d'un SOC, doivent adopter le mode de pensée d'un criminel en identifiant et en protégeant les cibles les plus probables. Exploiter pleinement les avantages d'un programme de Threat Intelligence nécessite de comprendre clairement en quoi consistent les ressources principales et quels sont les ensembles de données et les processus d'entreprise indispensables pour atteindre les objectifs de l'entreprise. L'identification de ces « joyaux de la couronne » permet aux entreprises d'établir des points de collecte de données autour d'elles pour cartographier les données collectées avec les informations disponibles en externe. En tenant compte des ressources limitées dont disposent généralement les département de sécurité des informations, établir le profil d'une entreprise dans sa globalité est un projet de grande envergure. La solution consiste à adopter une approche basée sur les risques et à se concentrer en premier lieu sur les cibles les plus probables.

Une fois les sources de Threat Intelligence internes définies et mises en œuvre, l'entreprise peut envisager d'ajouter des informations externes à ses flux de travail existants.

Une question de confiance

Les sources externes de Threat Intelligence présentent différents niveaux de fiabilité :

Les données open-source sont disponibles gratuitement, mais manquent souvent de contexte et renvoient un nombre important de faux positifs

Les sources commerciales de Threat Intelligence sont bien plus fiables, même si leur accès peut être coûteux

Il est judicieux de commencer par accéder aux communautés de partage spécifiques au secteur, comme le centre FS-ISAC (Financial Services Information Sharing and Analysis Center). Ces communautés fournissent des informations extrêmement précieuses, même si elles sont souvent clôturées et si une adhésion est nécessaire pour y accéder

Le principe directeur du choix des sources de Threat Intelligence doit privilégier la qualité à la quantité. Certaines entreprises estiment que plus elles intégreront de sources de Threat Intelligence, plus elles gagneront en visibilité. C'est parfois vrai. Par exemple en ce qui concerne les sources ultra-fiables, y compris les sources commerciales, qui fournissent des informations de Threat Intelligence adaptées au profil de menaces spécifique à l'entreprise. Mais le risque d'inonder vos opérations de sécurité d'informations non pertinentes demeure élevé.

Le chevauchement d'informations fournies par des fournisseurs de Threat Intelligence spécialisés peut être insignifiant. Leurs sources de renseignements et leurs méthodes étant différentes, les informations qu'ils fournissent présenteront des spécificités. Par exemple, un fournisseur bénéficiant d'une présence étendue dans une région donnée fournit davantage de détails sur les menaces émanant de cette région, alors qu'un autre fournit plus de précisions sur des types spécifiques de menaces. Ainsi, donner accès aux deux sources peut être bénéfique. Utilisées ensemble, elles peuvent contribuer à obtenir une image plus globale, à bloquer les menaces et à répondre aux incidents plus efficacement. Gardez toutefois à l'esprit que ces types de sources fiables requièrent également une évaluation préalable prudente pour garantir que les données fournies répondent aux besoins spécifiques et aux cas d'utilisation de votre entreprise, comme les opérations de sécurité, la réponse aux incidents, la gestion des risques, la gestion des vulnérabilités, la red team, etc.

Points à prendre en considération lors de l'évaluation des offres commerciales de Threat Intelligence

Il n'existe pas encore de critères courants pour évaluer les offres commerciales de Threat Intelligence, mais voici quelques points à prendre en considération :

Cela suppose que votre entreprise dispose déjà de contrôles de sécurité avec les processus associés prédéfinis. Utilisez la Threat Intelligence avec les outils que vous connaissez et maîtrisez déjà. Recherchez les méthodes de livraison, les mécanismes d'intégration et les formats qui garantissent une intégration transparente de la Threat Intelligence dans vos opérations de sécurité existantes

Privilégiez les informations dont la portée est globale. Les attaques n'ont que faire des frontières. Une attaque ciblant une entreprise en Amérique latine peut être lancée depuis l'Europe, et inversement. Le fournisseur se procure-t-il les informations dans le monde entier et réunit-il des activités apparemment incohérentes dans des campagnes cohérentes ? Les informations de ce type vous aideront à prendre les mesures appropriées

C'est le contexte qui permet d'exploiter les données. Les indicateurs de menaces sans contexte n'ont aucune valeur. Cherchez des fournisseurs qui vous aident à répondre à la question « Quel est l'intérêt ? ». Le contexte des relations (par exemple, les domaines associés aux adresses IP ou aux URL détectées depuis l'emplacement de téléchargement du fichier spécifique, etc.) ajoute de la valeur, dynamise les investigations sur les incidents et optimise la définition de leur portée grâce à la détection dans le réseau d'indicateurs de compromission associés et récemment acquis

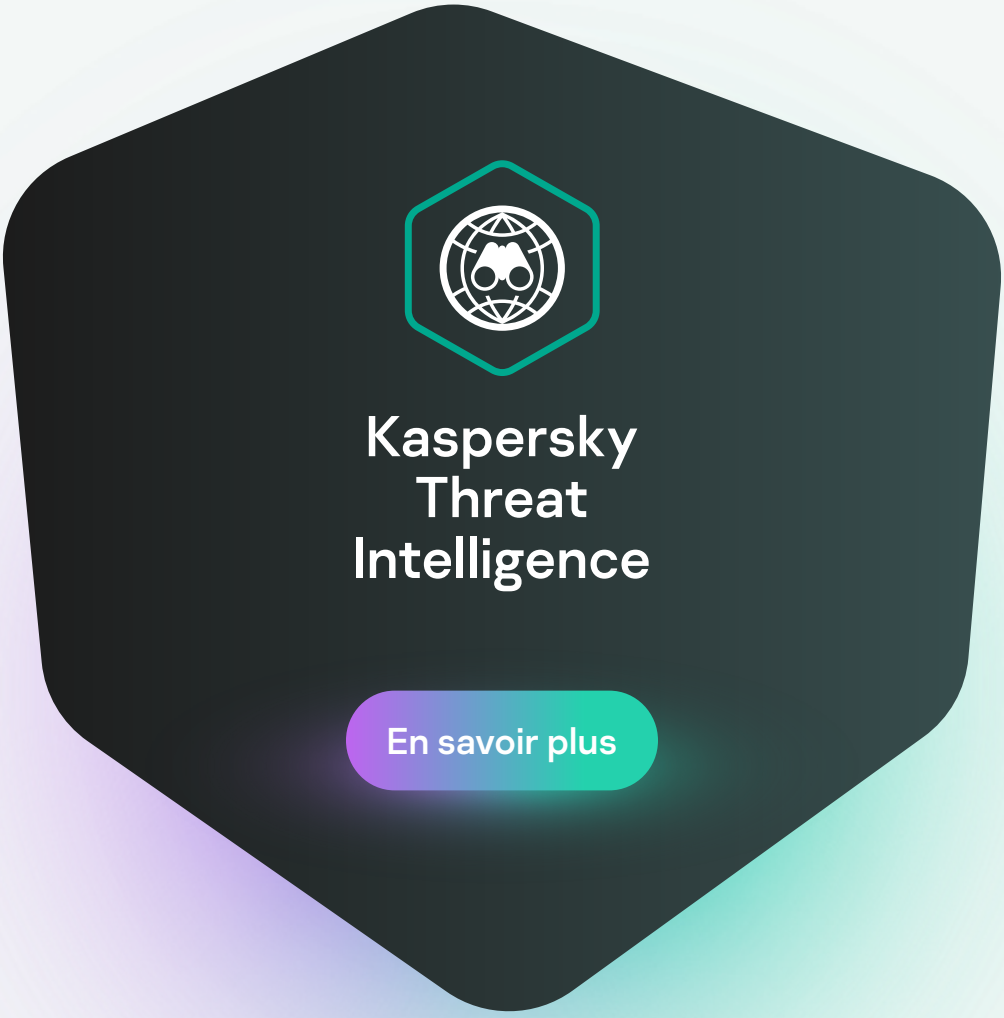
Si vous recherchez un contenu plus stratégique pour votre planification de sécurité à long terme, par exemple :

- Vue d'ensemble des tendances des attaques
- Techniques et méthodes utilisées par les attaquants
- Motivation
- Attributions, etc.,

optez pour un fournisseur de Threat Intelligence reconnu pour détecter constamment des menaces complexes et mener des investigations dans votre zone géographique ou votre secteur. La capacité du fournisseur à adapter ses capacités de recherche aux spécificités de votre entreprise est également cruciale

Conclusion

Kaspersky travaille sur la recherche des menaces depuis maintenant plus de 20 ans. Avec plusieurs pétaoctets de données sur les menaces à exploiter, des technologies avancées de machine learning et une équipe unique d'experts partout dans le monde, Kaspersky vous aide en vous proposant les informations sur les dernières menaces du monde entier, et vous permet de préserver votre immunité, même en cas de cyberattaques qui ne sont pas encore détectables.



www.kaspersky.fr