Threat Intelligence : quand, quoi et comment ?

kaspersky BRING ON THE FUTURE

Renseignements et données

Le monde croule sous les données, c'est une évidence.

Bon nombre d'organisations collectent de grandes quantités de données et d'informations sur les menaces, mais considèrent bien souvent que leur utilisation dans le cadre de leurs activités est difficile. La Threat Intelligence (TI), quant à elle, rassemble des données, des informations et des analyses détaillées, dans le but de fournir aux services de sécurité des informations pertinentes, précises et exploitables pour lutter contre les attaques et d'autres problèmes liés à la cybersécurité.

Ils y parviennent par la mise en contexte des données et des informations dont dispose déjà l'organisation, ainsi que par leur enrichissement à partir de renseignements, pour la plupart recueillis sur le Dark Web, sur les tactiques, les techniques et les procédures (TTP) utilisées par les acteurs de menaces déjà connus.

Grâce aux flux de données sur les menaces régulièrement mis à jour, aux rapports détaillés et aux services spécialisés, les équipes de sécurité peuvent mieux comprendre les motivations, les méthodes et les identités des pirates informatiques, optimiser leur prise de décision et réduire le risque de piratage de leur organisation.

Avec un large éventail de fournisseurs, les organisations peuvent également utiliser la Threat Intelligence pour améliorer leur compréhension du paysage des menaces (par exemple grâce à une analyse détaillée des menaces antérieures et nouvelles affectant leur secteur d'activité, leur pays ou même leur entreprise) et ainsi optimiser la qualité des activités, comme la gestion des vulnérabilités, le Threat Hunting, la réponse à incidents etc.

Comment en sommes-nous arrivés à cette situation ?

Le concept de TI remonte aux années 2000, avec l'apparition des listes de refus d'adresses IP et d'URL recueillies par des chercheurs en sécurité qui recherchaient manuellement les menaces et envoyaient des mises à jour quotidiennes à leurs clients et que les logiciels de protection comme les systèmes SIEM et les pare-feu de nouvelle génération (NGFW) utilisaient pour créer des alertes et des rapports.

Cependant, jusqu'en 2010, le développement du Dark Web et des activités malveillantes testait les limites des logiciels de protection disponibles, qui n'étaient pas conçus pour faire face au grand nombre d'indicateurs de compromission (IoC) reçus, et qui peinaient à identifier et à traiter tous les domaines malveillants, les adresses IP et les autres menaces.

Pour y remédier, le secteur de la cybersécurité a opté pour le Machine Learning et l'intelligence artificielle (AI), qui ont permis d'automatiser et de traiter les données à grande échelle. À l'aide de millions de capteurs, le flux de données a généré des milliards d'informations traitées et analysées au moyen d'outils de big data. Ces systèmes ont rapidement commencé à exécuter des opérations de détection complexes sur tous les types de menaces, et la technologie Big Data a donné lieu à la notion de TI.

À mesure que le marché devenait de plus en plus mature, en 2015, les experts en sécurité étaient en mesure de superviser la collecte de renseignements afin de réduire le nombre de faux positifs, et de mieux détecter les menaces et les modes d'attaque propres à leur organisation. Cette évolution s'est traduite par une détection et une réponse plus rapides, ainsi qu'un changement d'orientation pour repérer et hiérarchiser les vulnérabilités.

Puis, à partir de 2018, l'industrie de la TI a connu un véritable essor. Des centaines de nouvelles entreprises ont proposé des services axés sur la qualité des données afin de faciliter la prise de décisions et d'actions. Parallèlement, les organisations utilisatrices de produits et services informatiques ont commencé à les employer plus efficacement, notamment en adaptant leur collecte de données aux besoins en matière de sécurité.

Enfin, depuis 2019, le secteur s'est mis d'accord sur la signification de la TI définissant celle-ci comme un ensemble de sources multiples qui assurent la diffusion de données pertinentes et ciblées, pouvant être analysées et converties en renseignements susceptibles d'être utilisés instantanément ; pouvant être intégrées au fonctionnement de la sécurité d'une organisation par le biais d'un point d'entrée unique ; pouvant communiquer de manière transparente avec les systèmes de contrôle de sécurité déjà en place afin de fournir des informations uniques sur les menaces émergentes ; ainsi que pouvant servir aux équipes en charge de la sécurité à hiérarchiser les alertes, à optimiser les ressources et à prendre des décisions plus rapidement.

La TI rend aussi la cybersécurité plus proactive, grâce à des renseignements qui permettent de prédire et de prévenir efficacement les cyberattaques en amont, pour protéger l'organisation, et l'aider à identifier les risques et à définir ses buts opérationnels.

Quand et où utiliser la TI ?

Dans son étude sur es cybermenaces de 2021 (2021 SANS Cyber Threat Intelligence [CTI] Survey), l'institut SANS a révélé les résultats suivants :

Les usages de la CTI sont divers au sein d'une organisation, allant des usages stratégiques comme l'affectation des ressources et l'établissement de priorités aux applications tactiques comme le signalement des menaces et la réaction à ces dernières.

Les organisations continuent d'utiliser la CTI essentiellement sur le plan technique, notamment pour la détection et le blocage des menaces ainsi que les interventions en cas d'incident informatique, mais son utilisation se répand progressivement dans des zones comme le processus décisionnel et la sensibilisation des utilisateurs.

L'utilisation de la CTI à des fins de gestion des risques et d'établissement de priorités budgétaires a connu une augmentation constante au cours des dernières années.

Les informations relatives aux vulnérabilités ciblées par les pirates informatiques (76 %), les applications malveillantes exploitées par ces derniers (73 %) et les informations générales sur leurs pratiques (72 %) arrivent en tête des informations les plus utiles aux opérations CTI.

Voici les principales conclusions du rapport :

« La CTI ne concerne pas seulement les grandes entreprises. Cette année, un plus grand nombre de petites organisations ont adopté les programmes de CTI. Ce développement montre que la CTI est devenue un secteur où davantage d'organisations considèrent que les avantages valent l'investissement. Le renforcement de la sécurité à tous les niveaux, des décisions tactiques aux décisions stratégiques, est profitable aux organisations de toutes tailles et de tous secteurs d'activité.

« Les outils et les processus de la CTI s'automatisent progressivement, ce qui laisse plus de temps aux analystes pour se consacrer à des activités d'analyse de haut niveau plutôt qu'à des tâches répétitives de collecte et de traitement. Cette année, les analystes de la CTI incluent dans leurs analyses davantage d'informations en provenance des rapports de sécurité gouvernementaux et de médias. Cette évolution témoigne de la nécessité de disposer d'outils et de processus qui permettent de mieux intégrer cette source de données dans l'analyse et d'identifier la désinformation éventuelle susceptible d'avoir un impact négatif sur celle-ci ».

En plus du constat ci-dessus, les cas d'utilisation courants mis en évidence par d'autres analystes incluent notamment :

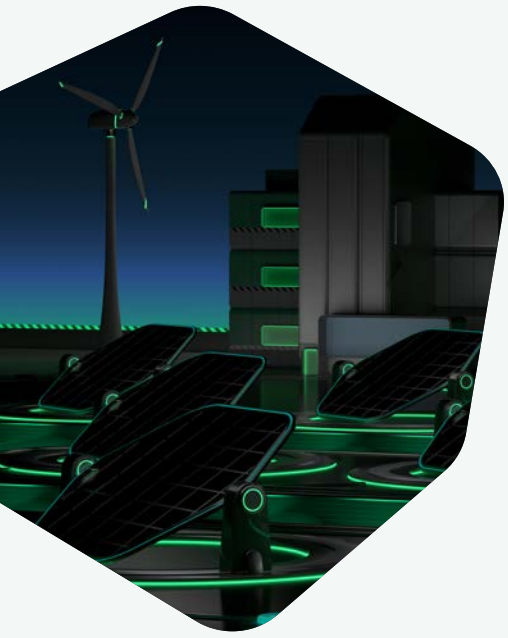
Si on se concentre sur des cas d'utilisation, comme le développement de la télémétrie, ils permettent un retour sur investissement rapide, en particulier pour les organisations et les équipes qui ont récemment mis en place un programme de TI.

Dans le cas des organisations exposées à de multiples menaces, l'utilisation de la TI permet de hiérarchiser les menaces selon le type et le niveau de risque, et ce en fonction des activités cybercriminelles déjà répertoriées et de l'impact éventuel sur l'organisation en cas de l'exploitation de ces menaces.

La TI permet de créer des stratégies de détection à partir de solutions de sécurité disponibles comme les SIEM ou l'EDR.

Vous pouvez enrichir la base de données d'incidents pour fournir des solutions comme les technologies SOAR, notamment par l'association d'un artefact IP ou binaire à une série de logiciels malveillants connus.

Vous pouvez vérifier la capacité de défense des systèmes existants en simulant des cyberattaques basées sur les profils de pirates informatiques connus.



Comment maximiser les bénéfices de la TI pour votre organisation ?

Les utilisations et les avantages de la TI sont nombreux et variés. Il en va de même pour ses sources, dans la mesure où essayer d'identifier ce qui fonctionnera le mieux pour votre organisation peut constituer un véritable défi à relever.

Pour vous aider à vous y retrouver dans les différentes options, il est essentiel de garder à l'esprit que la TI, non adaptée aux particularités de votre entreprise, risque d'accroître vos soucis.

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 ?

Vous possédez déjà la principale source de renseignements

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 votre réseau. Elles peuvent identifier des schémas d'activité malveillante propre à votre entreprise. Elles peuvent également permettre de différencier un utilisateur ordinaire et un comportement réseau et contribuer à suivre l'activité d'accès aux données.

Pour bénéficier au maximum de la TI, il convient donc de compléter et d'enrichir ces données, plutôt que de la considérer comme une source de données parmi d'autres.

Se mettre dans la peau d'un pirate informatique

Pour concevoir un programme efficace de Threat Intelligence, les organisations, et notamment celles qui disposent d'un centre d'opérations de sécurité (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 tel programme nécessite de comprendre clairement en quoi consistent ces ressources principales, et quels sont les ensembles de données et les processus d'entreprise indispensables pour atteindre les objectifs de votre organisation.

Identifier vos données les plus précieuses vous permet d'établir des points de collecte de données sur eux dans le but de cartographier ensuite les données collectées à l'aide d'informations relatives aux menaces externes et d'adopter une approche fondée sur le risque en privilégiant d'abord les cibles les plus vulnérables.

Mettre en place un programme de TI efficace

Dès que vos ressources informatiques en interne ont été définies et rendues exploitables, vous pouvez commencer à ajouter des informations externes aux flux de travail existants.

À supposer que votre entreprise ait déjà mis en place des mesures et des processus de sécurité et que vous souhaitiez utiliser la TI avec des outils que vous utilisez et connaissez déjà, recherchez des méthodes de livraison, des mécanismes d'intégration et des formats qui permettront une mise en œuvre harmonieuse de la TI dans le cadre de vos opérations de sécurité en cours.

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.

C'est le contexte qui permet d'exploiter les données. Les indicateurs de menaces sans contexte n'ont aucune valeur. Cherchez donc 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 d'un fichier particulier, 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'IoC associés et récemment acquis.

Si vous recherchez un contenu plus stratégique pour alimenter votre programme de sécurité sur le long terme, comme des analyses approfondies des stratégies de piratage informatique, des techniques et des méthodes utilisées par les criminels, leurs motivations et des attributions, recherchez un fournisseur de TI expérimenté en matière de détection et d'analyse des menaces complexes dans votre région 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

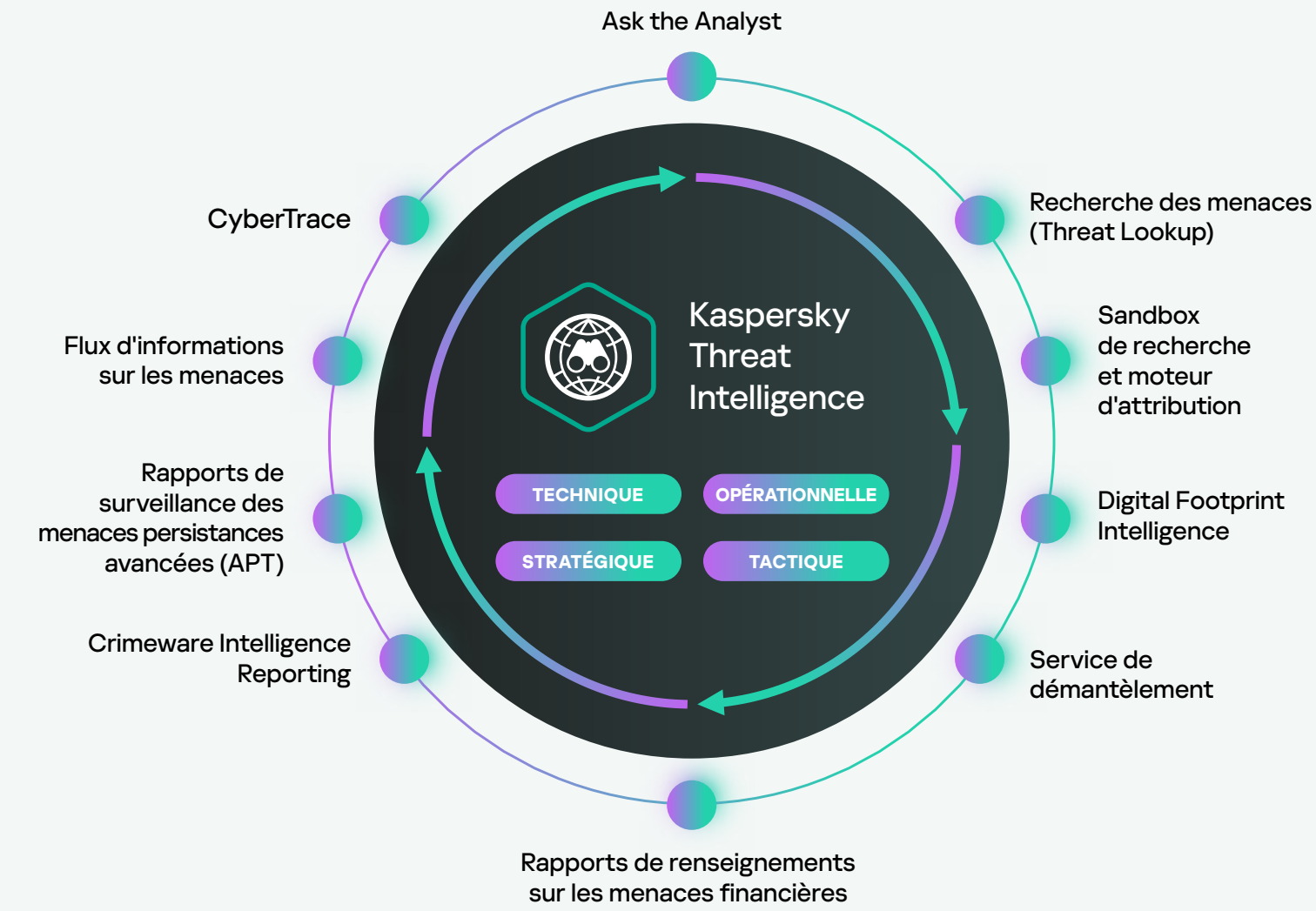
Une plateforme de Threat Intelligence (TIP) vous permet d'agréger, de gérer et d'opérationnaliser la TI, ce qui est vital lorsque vos outils de sécurité utilisent une TI provenant de sources multiples.

Une plateforme TIP devrait également faciliter le partage de la TI, tant publiquement qu'en privé avec d'autres organisations, et devrait permettre d'exporter et d'ingérer les TI à haut débit dans des formats lisibles par machine (MRTI), et vous fournir de l'aide :

- Vous pouvez répondre aux menaces plus efficacement en vérifiant les indicateurs de menace que vous jugez suspects, 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.
- Vous pouvez soumettre des adresses IP, des hachages de fichiers, des domaines ou des adresses Internet que vous jugez suspects, afin de confirmer et de prioriser rapidement les alertes et les incidents selon des niveaux de risque et des informations contextuelles pertinentes pour déterminer les véritables menaces.
- Vous pouvez recevoir des rapports réguliers relatifs au fonctionnement de certains fichiers ou de certaines adresses Internet spécifiques.
- Vous pouvez automatiser le flux de travail en matière de sécurité en connectant vos applications à la plateforme.

Comment Kaspersky peut vous aider

Kaspersky Threat Intelligence fournit des informations complètes, pertinentes, précises et exploitables sur l'ensemble du processus de prévention, de détection, de recherche, de traitement et des rapports stratégiques, qui sont tous adaptables aux besoins de votre organisation.



Notre gamme de services de TI inclut divers avantages concrets :

Le portail Kaspersky CyberTrace Threat Intelligence Portal assure l'intégration transparente des flux de données sur les menaces avec les solutions SIEM et aide vos analystes de la sécurité à exploiter plus efficacement la Threat Intelligence dans le cadre de leur flux de travail actuel sur les opérations de sécurité

Un large éventail de sources de données fournissant des informations sur les menaces actuelles dans le monde entier, y compris un inventaire des fichiers malveillants détectés par Kaspersky depuis plus de 25 ans

Un accès direct aux informations techniques, tactiques, opérationnelles et stratégiques fournies par notre équipe de chercheurs et d'analystes de renommée mondiale

Plus de 20 types de flux de données sur les menaces ; une sandbox développée en interne qui détecte les menaces sophistiquées et évasives ; et un moteur d'attribution des menaces qui fournit des informations détaillées sur les acteurs des menaces, nécessaires à la recherche des menaces APT

Une équipe dédiée d'experts en cybersécurité industrielle

En savoir plus sur la façon dont nous transformons les données en renseignements exploitables

www.kaspersky.fr