Prevention First :

Les avantages de la Cyber Threat Intelligence (CTI) pour une défense proactive

Digital Security
Progress. Protected.

Table des matières

La véritable importance de la prévention

Il ne fait aucun doute que la prévention des cybermenaces est primordiale. Les organisations étant de plus en plus dépendantes du numérique, le risque associé aux cybermenaces augmente en conséquence. Tout le monde devrait en être conscient. Mais est-ce bien la réalité ?

Ces dernières années, nous avons assisté à des prises de conscience qui nous ont montré l'importance des mesures préventives pour la cybersécurité. Ces cas expliquent pourquoi il est risqué de lésiner sur la prévention : **pertes financières importantes**, **réputation ternie** qui peut prendre des années à se reconstruire, et même **répercussions juridiques** que personne n'a envie d'affronter. Ce sont de sérieuses conséquences que les cybermenaces peuvent entraîner si l'on ignore la prévention proactive.

> **« Lorsque les technologies préventives sont sapées, une détection et une réponse rapides sont les seules choses qui vous sépare d'une atteinte à la sécurité des données coûteuse et probablement très publique. »**

Source : *Forrester : Forrester Tech Tide™ : Cybermenaces : détection et réponse Zero Trust, Q3 2023*
H. Mullins et son équipe. 21 juillet 2023.

En privilégiant une approche centrée sur la prévention, les organisations peuvent protéger leurs systèmes et leurs données, et donc réduire le risque de compromission. Même si une attaque se produit, la prévention proactive réduit le temps que les équipes de sécurité doivent consacrer à la réponse aux incidents et leur remédiation. Cela permet non seulement d'assurer la continuité des activités des organisations, mais également d'instaurer un climat de confiance avec les parties prenantes.

Bien qu'une approche centrée sur la prévention soit cruciale pour les organisations de toutes tailles, certains **aspects** sont **particulièrement importants** pour les **grandes organisations** et les entreprises.

Ce sont notamment les suivants :

AMPLEUR DES ACTIVITÉS

Les entreprises mènent généralement des opérations complexes à grande échelle. Cela signifie qu'elles ont plus de données et de systèmes à protéger, ce qui en fait des cibles de choix pour les cybercriminels et augmente l'impact potentiel des cyberattaques.

CONFORMITÉ RÉGLEMENTAIRE

De nombreuses organisations et entreprises opèrent dans des secteurs soumis à des exigences réglementaires strictes pour la protection des données. L'absence de prévention des cyberattaques peut conduire à une non-conformité, ce qui entraîne des amendes élevées et des conséquences juridiques. La règle d'or est la suivante : il **vaut mieux investir dans la prévention** que de dépenser pour le rétablissement.

243 K$

était le coût moyen atténué d'une atteinte à la sécurité des données grâce à la mise en place d'un système de threat intelligence en 2024.

Source : *Rapport d'IBM sur le coût d'une atteinte à la sécurité des données en 2024*.

EXIGENCES COMPLEXES POUR L'INFRASTRUCTURE ET L'INTÉGRATION

Les entreprises disposent souvent d'infrastructures informatiques plus complexes, comprenant de multiples réseaux, applications et systèmes. L'administration de la cybersécurité sur l'ensemble de ces vecteurs peut s'avérer difficile et nécessiter des solutions sophistiquées de threat intelligence utilisées à bon escient dans l'ensemble de l'infrastructure de protection. Idéalement, une **CTI avancée doit englober** à la fois une **technologie** fiable et une **expertise humaine**.

4,45 M$

était le coût moyen d'une atteinte à la sécurité des données en 2023.

Source : *Rapport d'IBM sur le coût d'une atteinte à la sécurité des données en 2023*.

RÉPUTATION

De nombreuses organisations de ce type ont une clientèle importante et une réputation reconnue. Une cyberattaque peut nuire considérablement à leur image, éroder la confiance des parties prenantes et avoir un impact négatif sur leur position sur le marché ou au sein de la communauté. Cela peut sembler anodin à première vue, mais la réalité peut être beaucoup plus dramatique après un tel préjudice.

L'utilisation de **solutions de cyber threat intelligence** est un **moyen efficace d'adopter une approche centrée sur la prévention** qui permet d'atténuer ces dommages potentiels. Elles fournissent des informations en temps réel sur les menaces potentielles, ce qui permet aux organisations d'identifier et de réduire les risques avant qu'ils ne causent des dommages et, par conséquent, de conserver une longueur d'avance sur les cybercriminels.

Quels sont les défis réels ?

MENACES AVANCÉES (ZERO-DAY)

Fréquemment associées aux vulnérabilités zero-day, ces menaces consistent à utiliser du **code malveillant** par des attaquants avant qu'un correctif ne soit disponible. Ces vulnérabilités sont dites « zero-day » car il s'écoule zéro jour entre la découverte de la menace et la mise à disposition d'un correctif ou d'une protection dédiée.

Plus largement, les menaces zero-day peuvent contourner les mesures de sécurité traditionnelles. Les conséquences directes et assez désagréables de cette situation pour les organisations sont le risque **d'attaques non détectées**, **d'atteintes à la sécurité des données** et **de pertes financières qui en découlent**.

L'une des meilleures solutions à ce problème est l'adoption de la cyber threat intelligence qui permet d'identifier et d'atténuer les menaces zero-day en fournissant des informations fiables et utilisables sur les vulnérabilités émergentes et les techniques d'attaque les plus couramment observées, telles que l'obscurcissement de fichiers ou d'informations, l'accès à des identifiants à partir de bases de mots de passe, l'hameçonnage et l'exfiltration via des canaux de commande et de contrôle.

PÉNURIE DE TALENTS

Le secteur de la cybersécurité est confronté à une pénurie de professionnels qualifiés. Les organisations ont des difficultés à trouver et fidéliser des experts en renseignements et en analyse des menaces, ce qui a un impact profond sur leurs capacités de détection et de réponse aux menaces.

Ces lacunes peuvent inclure une surveillance minimale plutôt que 24 heures sur 24, une mauvaise analyse des alertes, des journaux et d'autres IoC, ou une réponse lente qui autrement aurait pu permettre de mieux atténuer les dommages. **Investir dans la formation**, l'**automatisation** et la collaboration avec des **fournisseurs de threat intelligence externes** peut atténuer la pénurie de talents et, par conséquent, vous permettre d'être plus résilient.

COMPLEXITÉ DES OUTILS UTILISÉS

Les organisations utilisent souvent plusieurs outils de sécurité, chacun ayant sa propre interface, son propre format de données et sa propre configuration. L'intégration de ces outils peut être une tâche assez complexe et délicate, et peut prendre beaucoup de temps. Les effets négatifs possibles sont une **diminution de l'efficacité**, de **mauvaises configurations** et le **ralentissement de la réponse aux incidents**.

En ce qui concerne l'administration d'une variété d'outils, les équipes de sécurité doivent souvent passer d'une interface à une autre, ce qui entraîne une perte de temps et des erreurs potentielles. Le défi de l'intégration est la complexité, qui augmente le risque de mauvaise configuration, notamment la mauvaise correspondance des données ou des mises à jour négligées. C'est également un défi pour la fluidité des flux d'informations, et lorsque les outils n'échangent pas les informations de manière transparente, les délais de réponse aux incidents augmentent inutilement.

L'adoption de plateformes unifiées de threat intelligence qui rationalisent et automatisent l'agrégation, la normalisation et le partage des données entre les différents outils constitue une première étape dans la résolution de ces problèmes. Elles servent de centre d'information et réduisent donc considérablement la complexité. L'utilisation de **formats standardisés** tels que JSON et STIX via TAXII est également très importante car elle garantit la compatibilité et facilite la mise en œuvre.

Dernier point, mais non des moindres, l'**automatisation** aide les équipes de sécurité à tirer parti des informations actuelles sur les menaces pour mieux protéger les réseaux. L'orchestration automatisée des flux de données entre les outils minimise les interventions manuelles et peut réduire les erreurs humaines.

LACUNES EN MATIÈRE DE CONFORMITÉ ET MANQUE DE CONNAISSANCES PRATIQUES

Les organisations moins matures peuvent avoir des difficultés à traduire la threat intelligence en mesures concrètes, en raison d'un écart entre les connaissances théoriques et l'application pratique. Les exigences de conformité peuvent également ne pas correspondre aux pratiques de sécurité, ce qui peut entraîner une **implémentation inefficace** de la threat intelligence, **le non-respect de la réglementation** ou même des opportunités manquées.

L'implémentation est inefficace lorsque les organisations collectent des données sur les menaces mais ne parviennent pas à les utiliser de manière effective. Le non-respect de la réglementation signifie que votre organisation ne s'aligne pas sur les pratiques et les normes actuelles de threat intelligence, ce qui, comme nous l'avons mentionné plus haut, peut avoir des conséquences juridiques. Enfin, l'aspect des opportunités manquées correspond principalement à la façon dont le manque de connaissances pratiques empêche les organisations de tirer pleinement parti de la threat intelligence pour des stratégies de défense proactives et préventives.

En déployant largement l'IA dans les flux de travail de prévention, le coût des atteintes à la sécurité des données était en moyenne de

2,2 M$

de moins

par rapport aux organisations qui n'utilisent pas l'IA dans les flux de travail de prévention.

Source : *Rapport d'IBM sur le coût d'une atteinte à la sécurité des données en 2024*.

Que pouvez-vous faire ? **Former les équipes de sécurité** à l'utilisation pratique de la threat intelligence, **coordonner les efforts de conformité avec les objectifs de sécurité** et accorder la priorité aux connaissances exploitables. Former régulièrement les équipes de sécurité à l'utilisation pratique de la threat intelligence et combler le fossé entre la théorie et l'application pratique.

Fournir de la threat intelligence dans un contexte qui correspond aux exigences de conformité spécifiques et met en évidence des connaissances exploitables. Enfin, il convient d'accorder la priorité aux activités de threat intelligence en fonction de l'évaluation des risques et des besoins en matière de conformité.

Qu'est-ce que la Cyber Threat Intelligence ?

La cyber threat intelligence guide votre réflexion et vos actions. Vous ne vous contentez pas d'attendre passivement et d'émettre des hypothèses sur les menaces auxquelles vous êtes confronté, mais **anticipez activement les menaces réelles** et recherchez des occasions de créer des défenses plus robustes contre elles. Cela permet d'élaborer des plans à court et à long terme, d'assurer la stabilité et la préparation, de renforcer la résilience et de progresser.

Dans le domaine de la cybersécurité, cette approche modifie le paradigme de la protection contre les menaces et façonne le processus décisionnel. L'utilisation active de la cyber threat intelligence est une méthode pratique pour faire face aux cybermenaces, qui permet aux organisations d'établir et de prendre en charge la bonne ligne de conduite et, par conséquent, de permettre à l'entreprise de prospérer.

La cyber threat intelligence comprend la **collecte**, l'**analyse** et la **contextualisation d'informations** sur les menaces potentielles et actuelles qui pèsent sur les systèmes d'informations d'une organisation. Il s'agit avant tout d'une approche proactive qui permet aux organisations d'identifier, d'évaluer et d'atténuer les risques posés par les cybermenaces.

La threat intelligence a considérablement évolué au cours de la dernière décennie, permettant aux organisations d'identifier et d'atténuer les cybermenaces de manière proactive. En utilisant des données de threat intelligence, elles peuvent également mieux comprendre leur profil de risque et élaborer des stratégies de sécurité globales qui les protègent contre les acteurs malveillants.

Source : *IDC : Les dimensions stratégique, opérationnelle et tactique de la threat intelligence : Le point de vue d'un fournisseur*, doc. n° US51451823, 29 décembre 2023, M. Soltysik et Ch. Kissel.

La threat intelligence peut provenir de différentes sources, telles que des sources ouvertes, des services de renseignement commerciaux, des agences de renseignement gouvernementales et des équipes internes. Pour que cette approche centrée sur la prévention soit correctement implémentée, la cyber threat intelligence doit être fondée sur des connaissances exhaustives. Cela signifie essentiellement que les organisations doivent s'appuyer sur la **combinaison** d'une **technologie** fiable et adaptée à votre organisation et l'**intelligence humaine professionnelle**.

Lorsqu'elle est conçue et mise en œuvre de manière professionnelle, elle permet non seulement d'assurer une prévention proactive, mais également de réduire la complexité. Elle devient indispensable. Compte tenu de la complexité croissante du paysage des menaces, il est vivement recommandé de l'utiliser.

La cyber threat intelligence peut vous aider à :

- Prendre des mesures proactives pour prévenir ou atténuer les cyberattaques.
- Focaliser les ressources limitées pour tenter d'atténuer les risques les plus importants.
- Catégoriser les événements et réduire les dommages causés par des attaques potentielles.
- Minimiser l'impact négatif global d'une attaque.
- Réagir efficacement aux incidents de sécurité.

En pratique, il existe de nombreuses situations en temps réel où la cyber threat intelligence peut s'avérer utile, notamment pour **inventorier les adresses IP** associées à des infrastructures malveillantes, les **TTP**, les **identifiants compromis** ou les **injections web** de code HTML ou JavaScript.

Rassemblement, **contextualisation**, **interprétation** et **actions ciblées** : ces quatre éléments sont les issues les plus favorables qu'une organisation peut escompter lorsqu'elle utilise la cyber threat intelligence.

ESET Threat Intelligence et ses avantages clés

ESET Threat Intelligence (**ETI**) se définit par son approche préventive de la cybersécurité qui a pour objectif d'accélérer la réactivité, d'améliorer la préparation et de mettre en œuvre des mesures proactives face aux différents types de cybermenaces.

> **« En ce qui concerne nos sources de threat intelligence, la qualité des renseignements d'ESET sur les menaces est l'une des deux meilleures, si ce n'est la meilleure. »**
>
> Administration anonyme, octobre 2023

Les principaux avantages d'ETI pour renforcer votre posture de cybersécurité sont :

SÉLECTION PRÉCISE ET HAUTEMENT UTILE

- Faible taux de faux positifs
- Qualité plutôt que quantité
- Dans un format lisible par l'homme

COUVERTURE GÉOGRAPHIQUE UNIQUE

- Par la propre télémétrie d'ESET
- Éventail unique de sources
- Une expérience inégalée sur le terrain

PARTENAIRE DE CONFIANCE POUR LA THREAT INTELLIGENCE

- + 30 ans dans le secteur
- Basée en Europe
- Entreprise privée

> **La visibilité d'ESET sur un ensemble unique de données est ce qui fait sa force dans le monde de la CTI.**
>
> Une entreprise du secteur de la défense, août 2023

Parmi les autres avantages :

EXPERTISE HUMAINE
Même si des systèmes sophistiqués et personnalisés sont utilisés pour recueillir et traiter les données relatives aux cybermenaces, l'expertise humaine reste cruciale. La raison en est que **les humains restent plus aptes à contextualiser** et **interpréter**. Les analystes de threat intelligence supervisent également les processus, et étudient et proposent des améliorations.

COMPRÉHENSION DES RISQUES
Comprendre signifie prévoir les menaces, atténuer les incidents et réduire l'exposition aux menaces existantes.

AMÉLIORATION DE LA RECHERCHE DES MENACES ET LEUR REMÉDIATION
Recherche proactive des cybermenaces qui ont pu échapper aux défenses initiales et éradication des menaces persistantes pour améliorer la posture de sécurité.

IDENTIFICATION DES COMPROMIS POTENTIELS
Identifiez les compromissions potentielles en **utilisant des règles YARA pour analyser les systèmes** et en vérifiant les réseaux.

SURVEILLANCE DES GROUPES DE PIRATES
Cela vous permet d'acquérir une **compréhension approfondie** des tactiques, des méthodes, voire des motivations des groupes de pirates. Vous pouvez ainsi en dégager un avantage.

ÉCONOMIE DE RESSOURCES
Un contenu adapté vous permet d'économiser des ressources précieuses.

AGILITÉ
Cela vous permet de prendre de meilleures décisions plus utiles et plus rapidement, à court et à long terme. Dans le premier cas, la solution peut proposer des **IoC très pertinents** en temps utile. Dans le dernier cas, elle peut **renforcer votre stratégie de renseignement** et de cybersécurité.

ETI est une **offre complète** qui comprend de nombreux outils permettant d'assurer un niveau élevé de cyberprotection. ETI peut être consommé sous forme de service étendu, fournissant des connaissances grâce à des **flux de données**, des **rapports sur les APT**, **ESET AI Advisor** et un **accès direct à des analystes** ayant une connaissance approfondie des menaces.

Flux de données ESET Threat Intelligence

ETI fournit des flux uniques aux organisations. Il s'agit de **flux de données couvrant les menaces potentielles ou réelles** pour la sécurité d'une organisation, fournissant des informations complètes et utilisables en temps opportun. Les flux de données d'ETI proviennent d'un ensemble d'environ 110 millions de capteurs via ESET LiveGrid® et d'un système automatisé de suivi des botnets, qui permet de réduire au maximum le nombre de faux positifs.

Il existe six flux ETI bien connus, qui fournissent ensemble une image holistique et permettent à votre organisation de bloquer rapidement les intrusions : **flux de fichiers malveillants**, **flux d'APT**, **flux de domaines**, **flux d'URL**, **flux d'adresses IP** et **flux de botnets**. Pour en savoir plus, consultez notre guide de l'acheteur sur la cyber threat intelligence.

Neuf nouveaux flux améliorent encore davantage les fonctionnalités d'origine d'ESET. Chacun de ces flux est créé quasiment en temps réel et la déduplication est effectuée toutes les 24 heures.

FLUX DE SMS FRAUDULEUX

Une escroquerie par SMS est un message texte frauduleux. Ce flux contient des informations ciblées sur les données, les URL et les domaines associés à des escroqueries courantes par SMS. Il est créé à partir de toutes les sources de domaines et d'URL d'ESET.

FLUX DE SMISHING

Le flux de smishing est similaire au flux d'escroqueries par SMS, sauf que l'activité frauduleuse utilise le smishing, une attaque d'ingénierie sociale basée sur de faux messages texte pour inciter les gens à télécharger des malwares, révéler des informations sensibles ou envoyer de l'argent à des cybercriminels.

Ces informations peuvent être utilisées pour obtenir une threat intelligence unique, réagir aux incidents ciblés, effectuer d'autres études, sensibiliser les collaborateurs et protéger les systèmes.

FLUX D'ESCROQUERIES AUX CRYPTOMONNAIES

Les escroqueries aux cryptomonnaies désignent toute pratique frauduleuse visant à inciter des individus à faire de mauvais investissements dans des cryptomonnaies, céder des biens ou révéler des informations sensibles.

Ce flux est considéré comme un sous-ensemble des flux de domaines et d'URL d'escroqueries contenant des informations ciblées sur les domaines et les URL d'escroqueries courantes aux cryptomonnaies, ainsi que sur les données associées. Il est créé à partir de toutes les sources de domaines et d'URL d'ESET.

→ FLUX D'URL D'HAMEÇONNAGE

Les URL d'hameçonnage dirigent les destinataires vers de faux sites web et tentent de les inciter à divulguer des données sensibles telles que des identifiants de connexion ou des informations financières. Le site web semble généralement familier et légitime, mais il abuse de votre confiance en « allant à la pêche » aux informations personnelles.

Le flux d'URL d'hameçonnage recueille des données brutes provenant de multiples sources. Les organisations peuvent intégrer ce flux dans leurs solutions de sécurité, notamment XDR/EDR, SIEM, SOAR et pare-feux, afin de se défendre de manière proactive contre les cybermenaces.

FLUX D'URL D'ESCROQUERIES

Les flux d'URL d'escroqueries constituent une menace sérieuse qui est particulièrement susceptible d'être efficace en raison d'une erreur humaine. Ces URL ont l'air réelles et dignes de confiance, mais sont en réalité malveillantes. Ce flux couvre les boutiques en ligne frauduleuses, les escroqueries à l'investissement, les escroqueries à la rencontre, et il vous aide également à détecter les URL frauduleuses au niveau du réseau.

Les utilisateurs peuvent l'intégrer aux contrôles de sécurité de leur réseau ou à d'autres outils d'analyse, tels que les TIP, les systèmes SIEM et les solutions SOAR, afin de protéger les collaborateurs contre les escroqueries.

« Les renseignements d'ESET se concentrent sur une partie du monde d'où émanent de nombreuses attaques récentes de ransomwares. Ils se sont avérés à la fois opportuns d'un point de vue opérationnel et permettent d'identifier ces menaces de manière unique. »

Jess Parnell, Vice-président des opérations de sécurité chez Centripetal, octobre 2023

→ FLUX DE PIÈCES JOINTES MALVEILLANTES

L'objectif principal de ce flux est de protéger les utilisateurs et les organisations contre les menaces potentielles posées par les pièces jointes des emails. Il s'agit de fichiers envoyés par email dans le but de compromettre ou d'endommager le système informatique du destinataire ou d'exfiltrer des informations sensibles.

Ces malwares nuisibles se font souvent passer pour des éléments apparemment inoffensifs, tels que des documents, des PDF, des images ou des fichiers audio. Lorsque des utilisateurs peu méfiants ouvrent ces pièces jointes, ils activent des malwares par inadvertance, tels que des ransomwares, des logiciels espions et des chevaux de Troie.

➜ Les pièces jointes imitent souvent des communications légitimes provenant de sources réputées, ce qui augmente la probabilité que les utilisateurs les ouvrent.

Le flux est mis à jour quotidiennement pour suivre l'évolution des menaces émergentes et est créé à partir des sources de télémétrie d'ESET centrées sur l'analyse des emails (côté client et côté serveur) en temps quasi réel. Les utilisateurs peuvent accéder à ces informations via TAXII et STIX, ainsi que différents outils de sécurité.

FLUX DE RANSOMWARES

Ce flux fournit des informations en temps réel sur les échantillons de ransomwares actuellement répandus, ainsi que sur leurs caractéristiques et leurs IOC. Il vous aide à comprendre quelles familles de ransomwares sont découvertes et vous permet de les bloquer de manière proactive avant qu'elles ne causent des dommages.

Il comprend des hachages d'échantillons de ransomwares et les données associées. Le flux est fréquemment actualisé et peut être filtré afin que les clients n'obtiennent que des données pertinentes avec de faibles niveaux de redondance.

FLUX DE MENACES POUR ANDROID

Une menace Android désigne tout malware ou toute activité malveillante ciblant les appareils Android, y compris smartphones, tablettes et autres appareils utilisant le système d'exploitation Android. Ces menaces sont conçues pour exploiter les vulnérabilités, voler des informations personnelles, espionner les activités des utilisateurs, afficher des publicités indésirables ou même verrouiller l'appareil pour obtenir une rançon. En utilisant le flux de menaces pour Android, vous pouvez rester informé de l'évolution de ces dangers et protéger vos appareils contre les attaques potentielles.

Il fournit des informations en temps réel sur les menaces pour Android actuellement répandues, ainsi que sur leurs caractéristiques et leurs IOC. Le flux vous aide à comprendre quels menaces pour Android sont découvertes et vous permet de les bloquer de manière proactive avant qu'elles ne causent des dommages.

FLUX D'INFOSTEALERS POUR ANDROID

Ce flux contient des informations ciblées sur les échantillons actuels et répandus d'infostealers pour Android et les données associées. Une fois installées, ces menaces peuvent compromettre la sécurité et la confidentialité des personnes et des organisations, entraînant des vols d'identité, des pertes financières et d'autres conséquences graves.

Les données fournies par ce flux vous aident à comprendre quelles familles d'infostealers pour Android existent et comment les bloquer de manière proactive.

Intégrations

Les intégrations sont essentielles pour renforcer la cybersécurité des organisations. En connectant nos données de threat intelligence avec des plateformes comme Elastic, Microsoft Sentinel, OpenCTI et ThreatQuotient, ESET facilite l'accès aux informations critiques. Ces intégrations **optimisent la détection et la réponse aux menaces**, en fournissant des **flux de données en temps réel** pour aider les organisations à conserver une longueur d'avance sur les cybermenaces et prendre en charge une approche **centrée sur la prévention**.

ESET assure la compatibilité en utilisant des normes telles que TAXII 2.1 et STIX 2.1 qui facilitent la consommation de nos données de threat intelligence par les différentes plateformes SIEM et SOAR. Cette approche permet aux organisations de disposer de données précises dans des formats courants afin de renforcer leurs mesures de sécurité avec un minimum d'efforts et un maximum d'efficacité.

ELASTIC SIEM

Les utilisateurs d'Elastic peuvent bénéficier des flux ESET Threat Intelligence pour surveiller les botnets, les URL, les adresses IP, les domaines et les fichiers malveillants, qui révèlent les activités cybercriminelles cachées et les opérations des groupes de pirates. Cette intégration améliore le produit SIEM d'Elastic, fournissant aux opérateurs de sécurité des données globales sur les menaces, moins de faux positifs et un précieux contexte. Les clients bénéficient de données en temps réel provenant des flux ESET, d'une couverture complète des menaces et d'informations hautement spécialisées s'appuyant sur les recherches exclusives d'ESET, fournies par l'intégration native d'Elastic.

MICROSOFT SENTINEL

L'intégration d'ESET avec Microsoft Sentinel améliore la détection et la réponse aux menaces en combinant les flux de données de threat intelligence d'ESET avec les outil de SIEM et SOAR de Sentinel. Les analystes des SOC peuvent utiliser le client TAXII de Sentinel pour accéder à des données sur les APT, les fichiers malveillants, les botnets, les domaines, les URL et les adresses IP. Cette collaboration a pour objectif d'améliorer la détection des menaces et les temps de réponse. Elle s'appuie sur la recherche réputée d'ESET, les contributions à MITRE ATT&CK et la coopération avec la CISA, EUROPOL et le FBI.

OpenCTI

OpenCTI offre une plateforme collaborative pour l'analyse, l'enrichissement et le partage des données sur les menaces. L'intégration d'ESET Threat Intelligence améliore les connaissances sur les menaces et leur détection. L'intégration peut utiliser soit le connecteur OpenCTI natif d'ESET, soit le connecteur OpenCTI TAXII2 pour ingérer les flux de données ESET, en automatisant l'importation de Bundles STIX 2 sans conversion. Même si vous n'utilisez pas notre connecteur ou notre plugin conçu pour la plateforme, l'intégration est étonnamment simple.

Les flux d'OpenCTI au format CSV permettent la génération automatique d'un fichier CSV, qui est mis à jour à des intervalles définis par l'utilisateur, ce qui facilite l'intégration avec des systèmes qui peuvent ingérer ce format. Les Collections TAXII de la plateforme sont mises en œuvre dans un serveur TAXII 2.1, permettant la création d'autant de Collections TAXII que nécessaire, ce qui est particulièrement utile pour l'intégration avec les systèmes modernes de cybersécurité. Enfin, la fonctionnalité Live Streams d'OpenCTI améliore le partage des données en temps réel en servant les Bundles STIX 2.1 comme des Collections TAXII avec des fonctionnalités avancées, pour ajouter un contexte enrichi aux données partagées.

THREATQUOTIENT

L'intégration d'ESET Threat Intelligence à ThreatQuotient améliore la détection et la réponse aux menaces. Après vous être connecté à ThreatQ Marketplace, vous pouvez télécharger le fichier d'intégration et configurer les clés de l'API dans votre instance ThreatQ. L'intégration utilise le service TAXII d'ESET Threat Intelligence pour accéder à des flux spécifiques, y compris les flux de botnets, de domaines, d'URL et de fichiers malveillants. Ces flux fournissent des ensembles STIX contenant des indicateurs, des malwares, des identités et des relations.

Rapports sur les auteurs de menaces

Les rapports d'ESET sur les menaces persistantes avancées (APT) représentent une source fiable de cyber threat intelligence qui couvre leurs auteurs et leurs activités. Ils fournissent des renseignements stratégiques, tactiques, techniques et opérationnels pour aider les organisations à **rechercher des menaces**, **enquêter** et **atténuer les incidents actifs**, et par conséquent, aider les organisations à devenir proactives et prédictives au lieu d'être réactives. La connaissance de l'adversaire aide les responsables de la sécurité à déterminer quelles menaces potentielles sont les plus susceptibles de devenir des menaces réelles pour leur organisation, et décider où investir et sur quoi se concentrer.

> **« ESET offre une perspective unique sur les activités des auteurs de menaces et fournit une analyse technique approfondie des malwares, de l'infrastructure et des TTP. L'équipe d'ESET est devenue un élément essentiel de notre capacité à combattre les différents auteurs de menaces qui opèrent dans notre région. Nous sommes reconnaissants de notre collaboration avec elle. »**

Agence de renseignements anonyme, septembre 2023

Une pratique très utile pour les organisations consiste à consolider toutes les données des rapports dans leur plateforme de threat intelligence. ESET offre un accès à son système interne MISP (plateforme de partage d'informations sur les malwares), qui contient toutes les données pertinentes et utiles. Les clients peuvent donc facilement le synchroniser avec leurs systèmes.

Les rapports sur les APT contiennent des informations contextuelles et d'autres détails pertinents. Ils se présentent sous la forme d'un ensemble avec plusieurs types d'informations : **rapports d'activité**, **rapports d'analyse technique**, **rapports mensuels**, **rapports de synthèse mensuels**, **flux de données sur les APT**, accès au serveur MISP d'ESET et aux analystes de menaces.

ESET AI Advisor

ESET AI Advisor est le complément parfait de la boîte à outils de l'analyste de sécurité, offrant une expérience fluide et intuitive qui s'intègre sans effort dans les flux de travail quotidiens. S'appuyant sur les vingt années d'expertise d'ESET dans **la protection des endpoints grâce à l'IA**, cet outil fournit non seulement **des informations granulaires sur les incidents** mais également **des conseils stratégiques** adaptés aux équipes des SOC. Cet atout est transformateur pour les entreprises, en particulier celles dont les moyens humains et/ou techniques sont limités et qui souhaitent maximiser l'utilité d'une threat intelligence pertinente.

> **« Le module ESET AI Advisor représente une avancée significative dans notre mission de combler le déficit de compétences en cybersécurité et de permettre aux organisations de protéger efficacement leurs infrastructures numériques. »**
>
> Juraj Malcho, directeur de la technologie chez ESET.

Que votre organisation dispose de professionnels de la sécurité moins expérimentés ou d'experts compétents et fiables, ESET AI Advisor est un **moyen simple de repérer**, **analyser** et **résoudre les risques pour la sécurité**. Tout est présenté de manière à ce que vous puissiez passer directement à l'action.

L'interface est facile d'emploi et permet de transformer des informations complexes sur les menaces en connaissances que vous pouvez **immédiatement utiliser** quel que soit votre niveau d'expertise.

Les organisations utilisant l'IA pour leur sécurité informatique ont maîtrisé les menaces en

108

jours de moins

que les organisations qui n'utilisent pas l'IA.

Source : *Rapport d'IBM sur le coût d'une atteinte à la sécurité des données en 2023*.

ESET AI Advisor joue un rôle crucial pour accélérer les décisions lors d'incidents critiques. Les analystes de sécurité peuvent consulter sans effort ESET AI Advisor afin d'obtenir des informations sur les menaces ciblant spécifiquement leur environnement.

ESET AI Advisor est disponible dans la console ESET Threat Intelligence avec les rapports sur les APT.

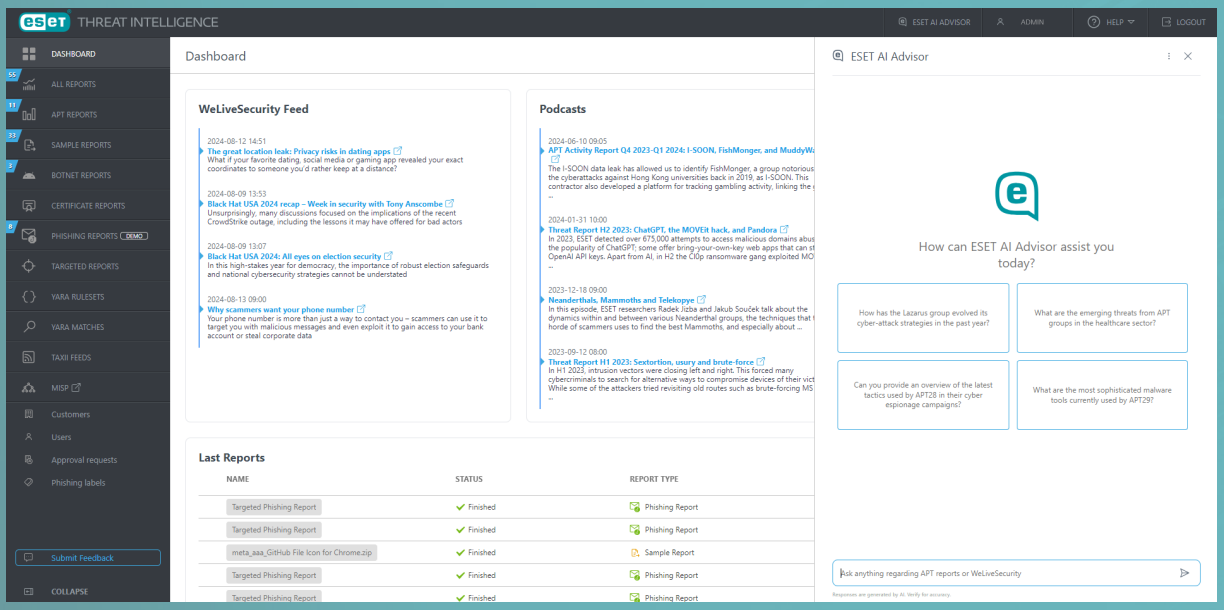

Image 1 : *Intégration d'ESET AI Advisor dans la console ESET Threat Intelligence.*

Conclusion

Dans le paysage actuel de la cybersécurité, il est essentiel d'utiliser la cyber threat intelligence (CTI) pour assurer une prévention efficace. Il est préférable pour les organisations de toutes tailles d'**accorder la priorité aux mesures préventives** car cela permet d'économiser des ressources, d'assurer la continuité des activités et de préserver l'entreprise des répercussions juridiques potentielles dues à la non-conformité.

Les adversaires, ainsi que leurs outils et pratiques, sont tout simplement trop sophistiqués pour se contenter de rester réactifs aujourd'hui. Les organisations peuvent être confrontées à des défis importants dans l'adoption de mesures préventives, notamment des contraintes de ressources et la complexité de l'intégration de la CTI. Nos experts affirment que **comprendre la CTI** ainsi que les données précieuses qu'elle fournit et la manière dont elle peut

être utilisée dans le cadre de la prévention, constituent l'une des étapes clés pour surmonter ces obstacles et devenir résilient.

ESET offre une threat intelligence avancée, basée sur des **flux de données robustes** et des **rapports détaillés**, et accompagnée par **ESET AI Advisor** qui aide à traiter et évaluer de grandes quantités de données. Des intégrations transparentes sont également incluses dans le service. Même s'il n'existe pas de solution miracle pour adopter une approche préventive, l'exhaustivité de la CTI et d'autres mesures de défense peut à coup sûr booster la résilience opérationnelle des organisations.

Déterminez votre cas d'utilisation d'ETI et accédez aux rapports d'ESET sur les APT, aux flux de données d'ETI et à un ensemble complet d'outils pour une approche centrée sur la prévention grâce à ESET.

EN SAVOIR PLUS

À propos d'ESET

Défense proactive. Notre activité consiste à minimiser la surface d'attaque.

Prenez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre **approche préventive reposant sur l'IA et l'expertise humaine**.

Bénéficiez d'une protection de haut niveau grâce à notre **cyber threat intelligence** interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par **des chercheurs reconnus**. ESET protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie.

Prévention multicouche

IA de pointe associée à une expertise humaine

Threat intelligence de renommée mondiale

Support hyperlocal et personnalisé

eset®
Digital Security
Progress. Protected.