Threat Hunting : quoi, comment et pourquoi ?

kaspersky

Contenu de cette présentation

Introduction

Bien que de nombreuses organisations utilisent les solutions de cybersécurité comme des plates-formes de protection des terminaux (EPP), environ 10 % des cybermenaces (incluant les menaces nouvelles, inconnues et difficilement détectables, telles que de nombreux types de ransomwares) sont capables de contourner ces défenses.

Le Threat Hunting fonctionne en partant du principe suivant : bien que les contrôles de sécurité existants d'une organisation n'aient rien détecté ou signalé, l'organisation a été en fait été compromise et une menace est déjà présente dans le système.

Le Threat Hunting utilise alors des outils qui incluent l'EDR (Endpoint Detection and Response) et des processus clairement définis et structurés pour repérer les signes avant-coureurs qu'une violation a eu lieu et pour l'identifier. Cette approche proactive, en amont, peut non seulement minimiser les dommages que peuvent infliger des attaques d'origine humaine potentiellement extrêmement dévastatrices, mais également contribuer à renforcer et à valider les contrôles de sécurité pour mieux défendre l'organisation à l'avenir.

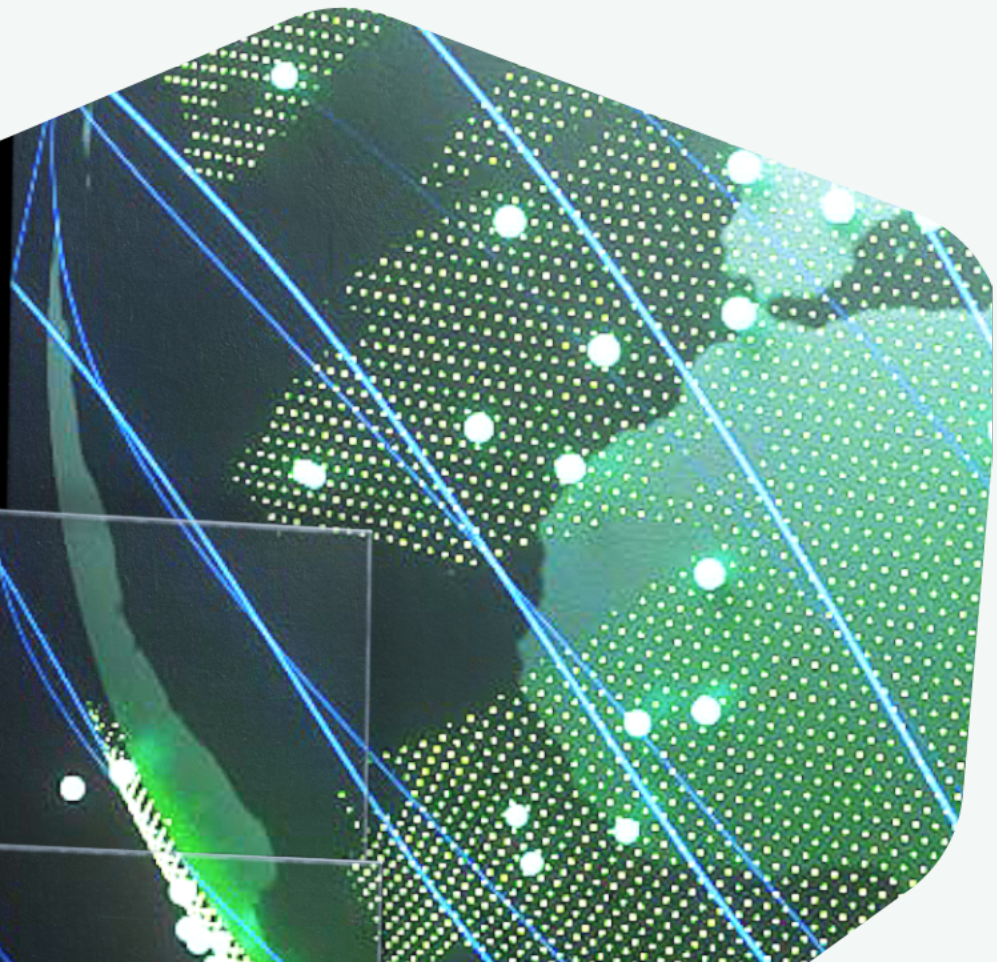
Des loups, des ours et une forêt obscure

Si le terme « Threat Hunting » évoque pour vous des images de loups, d'ours et de forêt obscure, cette présentation est faite pour vous.

Dans celle-ci, nous présentons succinctement ce qu'est le Threat Hunting et les raisons pour lesquelles vous devriez l'utiliser. Nous allons évoquer également une partie de son histoire, ainsi que les trois acronymes (IoC, IoA et TTP) que vous devez vraiment connaître.

Pour éviter toute confusion, nous allons examiner quelques idées reçues les plus courantes relatives à au Threat Hunting (en particulier ce qu'elle n'est pas), avant d'aller à l'essentiel des détails pratiques du processus, en incluant différents types de recherche de menaces, ainsi que les étapes que cela implique.

Pour terminer, nous nous intéresserons rapidement à ce dont vous avez besoin pour réussir le Threat Hunting, avec une checklist pratique. Soyez donc prêts à commencer à rechercher des brindilles brisées, de la végétation piétinée, des empreintes de pas, des traces et d'autres signes avant-coureurs que les loups et ours affamés cachent quelque part dans la forêt.



À quoi correspond exactement le Threat Hunting ?

Vous pourriez penser que la chose la plus facile pour une présentation comme celle-ci serait de commencer par une simple définition. Cependant, si vous fouillez dans le Web, vous constaterez que presque tous les secteurs, journalistes ou fournisseurs dans le domaine des outils ou des services de recherche de menaces possèdent leur propre version légèrement différente.

Par exemple :

- SANS Institute indique que « la pratique formelle du Threat Hunting vise à révéler la présence des tactiques, techniques et procédures (TTP) non encore découvertes d'un attaquant dans un environnement, en employant des technologies de détection existantes ».

- Selon IBM, « le Threat Hunting, également appelée recherche des cybermenaces, est une approche proactive permettant d'identifier des menaces jusque là inconnues ou des menaces en cours, mais qui n'ont pas été résolues, dans le réseau d'une organisation ».

- En outre, la définition de Kaspersky est la suivante : « Le Threat Hunting désigne le processus mis en œuvre pour la détection proactive d'une activité malveillante dans des réseaux d'ordinateurs. »

Bien que ces définitions soient différentes dans leur formulation et leur mise en avant, le point essentiel à retenir de toutes les trois est que le Threat Hunting est à la fois proactive et préventive. Son postulat de base est que, même si vos contrôles de sécurité existants n'ont rien détecté ou signalé, votre organisation a été en fait été compromise et une menace est déjà présente dans le système.

Alors, pourquoi auriez-vous besoin d'effectuer ce type d'approche ?

Quelles sont les raisons pour lesquelles vous devriez effectuer cela ?

Étant donné que vous lisez ce guide, vous disposez presque certainement d'une forme d'EPP (Endpoint Protection Platform) et vraisemblablement d'une solution EDR (Endpoint Detection and Response).

Pour commencer avec l'EPP, il s'agit essentiellement d'une solution réactive. Une menace entre dans votre réseau et/ou tente d'attaquer un ou plusieurs de vos terminaux et, dans la mesure où il reconnaît cette menace, l'EPP la neutralise automatiquement pour protéger votre entreprise et les utilisateurs.

Bien que cela fonctionne pour environ 90 % des menaces (souvent appelées « traditionnelles » ou « basiques »), il existe de nombreuses menaces nouvelles, inconnues et furtives qui correspondent aux 10 % capables de contourner une protection des terminaux automatisée.

Quelques-unes de celles-ci sont les menaces d'origine humaine sur mesure ciblant des domaines de l'industrie spécifiques, voire des entreprises individuelles. Elles partagent en général deux caractéristiques importantes :

- Lorsqu'une attaque est d'origine humaine, le pirate s'implique activement et participe de manière interactive pendant toute la durée de l'attaque. C'est la raison pour laquelle ces attaques sont en mesure d'échapper à la détection de solutions entièrement automatisées telles que l'EPP et les systèmes de prévention contre les intrusions (IPS), et ne sont identifiées qu'après l'apparition d'une compromission ou d'une violation.
- Étant donné que le pirate peut modifier son approche au cours de l'attaque, les détections basées sur l'utilisation d'outils ou d'indicateurs de compromission (IoC) sont également inefficaces, la seule manière de détecter s'effectue via les tactiques, techniques et procédures (TTP) utilisées par la personne ou le groupe de cybercriminels (pour obtenir l'accès, acquérir un contrôle permanent, élever des privilèges, se déplacer latéralement, etc.), même si l'attaque en cours de déploiement n'a encore jamais été vue auparavant.

Toutes ces caractéristiques signifient qu'une approche plus proactive (plutôt que réactive) est nécessaire. Et c'est précisément la capacité permise et fournie par le Threat Hunting. Plutôt que d'attendre que quelque chose se produise, les membres de votre équipe de sécurité informatique entreprennent une approche proactive, préventive, qui implique une vision large pour regarder les signes avant-coureurs que votre entreprise a déjà fait l'objet d'une intrusion par un acteur de menace, qui s'emploie actuellement à éviter de se faire découvrir ou détecter.

Comment en sommes-nous arrivés à cette situation ?

Comme il le remarquer dans son blog, Richard Bejtlich, ancien directeur de la réponse aux incidents de GE-CIRT (GE Cyber Incident Response Team), semble avoir été la première personne à écrire un article décrivant le Threat Hunting de manière judicieuse. Cet article, intitulé « Devenez chasseur » a été publié dans le numéro de juillet/août 2011 du magazine Information Security.

Comme il l'explique, « pour mieux contrer les attaques ciblées, il est nécessaire de mener des opérations de contre-menace (CTOps). En d'autres termes, les défenseurs doivent « chasser » (rechercher) activement les intrus dans leur entreprise. Ceux-ci peuvent prendre la forme de menaces externes, qui persistent, ou de menaces internes, qui abusent de leurs privilèges. Plutôt que d'espérer que les défenses vont repousser les envahisseurs, ou que les violations seront repérées par des mécanismes d'alerte passive, les professionnels des CTOps reconnaissent que, pour vaincre les intrus, il est nécessaire de les détecter de manière active et de leur répondre. Les experts CTOps ont ensuite tiré des enseignements de ce qu'ils ont appris en recherchant et en supprimant les attaquants, pour les appliquer au cycle de vie de développement des logiciels (SDL), ainsi qu'à la configuration et aux processus de gestion informatique, afin de réduire la probabilité d'incidents ultérieurs...

« En plus d'effectuer le travail du SOC, les CTOps nécessitent des idées et des approches plus actives, non structurées et créatives. Une manière de caractériser cette approche plus dynamique pour détecter et répondre aux menaces est l'emploi du terme « hunting » (chasse). Dans le milieu des années 2000, l'Air Force a popularisé le terme « hunter-killer » (chasseur-tueur) pour désigner les missions dans lesquelles des équipes d'experts en sécurité effectuaient une « projection de forces amicales » sur leurs réseaux. Ils ont passé au peigne fin les données des systèmes et, dans certains cas, ont occupé les systèmes eux-mêmes dans le but de rechercher des menaces avancées. Le concept de « chasse » (sans le terme sensiblement plus agressif « killing ») gagne actuellement du terrain dans le monde civil.

« Si le SOC est caractérisé par un groupe qui examine les alertes en recherchant des signes de l'action d'un intrus, le CIRT est reconnu par la possibilité que des analystes confirmés emmènent des analystes débutants dans des « expéditions de chasse ». Un enquêteur confirmé qui a découvert une manière nouvelle ou plus astucieuse de détecter éventuellement des intrus va alors guider un ou plusieurs analystes novices à travers les données les systèmes pour rechercher des signes de l'ennemi. Lors de la validation de la technique (et de la réponse aux actions de l'ennemi), l'équipe de chasse doit travailler pour incorporer la nouvelle méthode de détection dans les processus reproductibles utilisés par les analystes de type SOC. Cette idée de développer de nouvelles méthodes, de les tester dans la nature, puis de les rendre opérationnelles, est l'élément essentiel pour combattre les adversaires modernes. »

Ainsi, bien que l'acronyme CTOps de Richard ne s'est pas avéré avoir le succès qu'il aurait peut-être espéré, sa description des aspects pratiques du Threat Hunting a certainement passé l'épreuve du temps.

Trois autres définitions importantes

Il existe beaucoup de jargon associé au Threat Hunting, et les trois termes les plus importants qui doivent être clarifiés, que nous avons déjà mentionnés pour quelques-uns, sont les indicateurs de compromission (IoC), les indicateurs d'attaque (IoA) et les tactiques, techniques et procédures (TTP).

Indicateurs de compromission (IoCs)

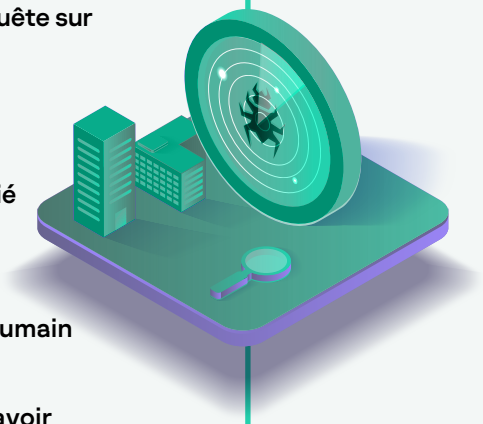
Un indicateur de compromission (IoC) est un indicateur ou un objet statique qui, lorsqu'il est observé sur un réseau ou un périphérique, indique une probabilité élevée d'un accès non autorisé au système : en d'autres termes, que **le système est compromis**. Ces indicateurs sont utilisés pour détecter une activité malveillante à ses stades précoces, ainsi que pour empêcher des menaces connues.

Exemples courants d'IoC :

- Recherches DNS inhabituelles
- Fichiers, applications et processus suspects
- Adresses IP et domaines appartenant à des botnets ou des serveurs de commande et de contrôle (C&C ou C2) de programmes malveillants
- La signature d'une attaque ou le hachage de fichiers d'une partie connue de programmes malveillants
- Une taille inhabituelle de réponses HTML
- Une modification non autorisée de fichiers de configuration, de registres ou de paramètres de périphériques

Indicateurs d'attaque (IoA)

Contrairement aux IoC, les indicateurs d'attaque (IoA) sont des motifs de comportement qui démontrent les intentions qui se cachent derrière une cyberattaque, ainsi que les techniques utilisées par l'acteur de la menace pour accomplir ses objectifs. Ces éléments incluent des bases de données propriétaires d'IoA alimentées et maintenues par des chercheurs de menaces experts, qui contribuent à fournir un contexte supplémentaire lors d'une enquête sur des activités cybercriminelles.



Exemples d'IoA :

- Un nombre important d'accès à un fichier unique
- Une activité suspecte sur les comptes d'administrateurs ou d'utilisateur privilégié
- Une mise à jour inattendue de logiciels
- Un transfert de données sur des ports rarement utilisés
- Un comportement sur un site Web atypique par rapport à ce que ferait un être humain
- Un grand nombre de tentatives de connexion infructueuses
- La communication d'hôtes internes avec des ressources Internet connues pour avoir une mauvaise réputation, ou avec des pays situés en dehors de la plage d'activité de l'entreprise

Pour accélérer l'analyse d'incidents complexes, les IoA seront idéalement mappées à la base de connaissances MITRE ATT&CK® à des fins d'analyse approfondie des tactiques, techniques et procédures de l'adversaire.

Tactiques, techniques et procédures (TTP)

Selon MITRE ATT&CK :

- **Les tactiques** illustrent le « pourquoi » d'une technique ou d'une sous-technique d'ATT&CK. Il s'agit de l'objectif tactique de l'adversaire : la raison pour laquelle il effectue une action, par exemple, l'accès à des identifiants.
- **Les techniques** représentent le « comment » un adversaire atteint un objectif tactique en réalisant une action, par exemple en extrayant des identifiants pour y obtenir un accès.
- **Les procédures** sont la mise en œuvre que l'adversaire utilise pour appliquer des techniques ou des sous-techniques, par exemple, l'utilisation de PowerShell pour injecter du code dans le processus lsass.exe afin d'extraire les identifiants en récupérant des informations dans la mémoire du processus LSASS d'une victime.

Ce que le Threat Hunting n'est pas

Comme nous l'avons déjà vu, il existe différentes interprétations de ce qu'est exactement le Threat Hunting. C'est pourquoi, avant de poursuivre sur les aspects pratiques du Threat Hunting, il est intéressant de passer quelques instants à examiner certains éléments qu'elle n'est pas.

Ce n'est pas la Threat Intelligence

La Threat Intelligence est une source d'informations extrêmement puissante concernant les intrusions tentées et réussies, collectées et analysées par des systèmes de sécurité automatisés faisant appel à l'IA et au Machine Learning, et parfois à des experts humains.

Le Threat Hunting utilise toujours ces renseignements, y compris les indicateurs de menaces, tels que IoC, IoA et TTP, comme point de démarrage pour une recherche. Cela implique ensuite une recherche minutieuse dans tout le système de la présence d'acteurs malintentionnés. Ensuite, si une recherche identifie de manière fructueuse des menaces qui n'ont pas encore été signalées dans la nature, les résultats sont engrangés dans la base de connaissances de la surveillance des menaces (incluant éventuellement MITRE ATT&CK) pour aider les futures recherches.

Davantage d'idées reçues

D'autres idées reçues ou informations erronées concernant le Threat Hunting que vous pouvez trouver en ligne incluent les éléments suivants :

- Il s'agit essentiellement d'un processus manuel
- Elle est seulement destinée à une utilisation précise
- Vous pouvez l'automatiser avec l'IA
- Vous pouvez l'utiliser pour remplacer des pare-feu, des IDS ou SIEM
- C'est une tâche ponctuelle
- Vous avez besoin d'une visibilité totale de vos terminaux
- Vous ne pouvez trouver que des menaces actives
- Cela ne vaut pas la peine d'y consacrer du temps et des efforts
- Vous avez besoin d'années d'expérience pour l'exploiter

Pour éviter toute confusion supplémentaire, aucune de ces déclarations n'est correcte.

Ce n'est pas (nécessairement) une attribution

Des cybercriminels particuliers et des groupes ont leurs TTP favorites, qui peuvent agir comme une sorte de « signature » de leur approche spécifique pour commettre une attaque.

Lorsqu'un centre d'opérations de sécurité (SOC) ou une équipe de sécurité informatique commence à suivre des types d'adversaires ou des groupes particuliers en se basant sur la Threat Intelligence, et en associant cela aux TTP que ceux-ci utilisent, il peut être très séduisant d'attribuer une attaque découverte à un adversaire particulier en se basant sur ces TTP.

Cependant, en réalité, l'attribution nécessite généralement le niveau le plus élevé de preuves et une analyse extrêmement poussée fournie par certains fournisseurs de cybersécurité, dont Kaspersky, qui peut être ensuite utilisée par une organisation disposant du niveau d'expertise requis pour travailler avec ces solutions.

S'il est possible d'attribuer un fichier particulier à un groupe de menaces spécifiques, l'étape suivante consiste à déterminer quelles informations sont disponibles sur les TTP de ce groupe, ce qui peut ensuite être utilisé comme source pour le Threat Hunting, une investigation et une réponse ultérieures.

Un autre avantage du suivi des adversaires réside dans son rôle essentiel pour l'affinage des pratiques de sécurité, par exemple en validant des contrôles de sécurité existants, en s'assurant que les outils de détection du SOC sont efficaces, en permettant aux équipes rouges (jouant le rôle de cyber-adversaires) de reproduire des types d'acteurs de menaces particuliers, etc.

La chasse (recherche) est ouverte

Comment le Threat Hunting fonctionne-t-il ?

Maintenant que nous avons réfuté quelques-unes des idées reçues les plus courantes, il est temps de s'intéresser à la manière de repérer les signes avant-coureurs de ces loups et ours avides.

Tous les exercices de Threat Hunting doivent se baser sur une combinaison de Threat Intelligence et d'une connaissance de la situation. Pour le dire en termes simples, le processus implique une recherche manuelle ou assistée par ordinateur pour effectuer une analyse des IoC, IoA et TTP (voir ci-dessus), basée sur le cycle suivant :

- Création d'une hypothèse
- Examen de l'hypothèse
- Découverte de nouveaux motifs de comportement
- Utilisation de ces éléments pour informer et enrichir les analyses existantes

Le processus doit être considéré comme un ajout aux systèmes de productions existants, plutôt qu'un remplacement de ceux-ci, permettant une détection précoce de menaces nouvelles et sophistiquées dans le réseau. De plus, comme la pénétration du système peut se produire à tout moment, le Threat Hunting doit également être un processus constant, se composant des étapes suivantes :

- **Formulation d'une hypothèse.** Les experts en sécurité informatique suggèrent des domaines de Threat Hunting en fonction de données qui peuvent être internes (par exemple, information de la société concernant l'état de l'infrastructure informatique, résultats de tests de pénétration, etc.) ou externes (par exemple, matrices MITRE ATT&CK matrices, rapports de veille stratégique des cybermenaces, actualités en matière de sécurité, etc.). À titre d'exemple, si un nouveau rapport met en évidence un élément inconnu de logiciel malveillant, on peut émettre l'hypothèse que ce logiciel malveillant a infiltré l'infrastructure de la société.
- **Test de l'hypothèse.** Une fois que l'hypothèse a été formulée, elle est alors testée. Ainsi, dans le cas de l'hypothèse ci-dessus, les données provenant des terminaux sont analysées pour rechercher des IoC associés avec le nouveau logiciel malveillant mis en évidence dans le rapport.

Si l'hypothèse se confirme, l'organisation peut alors prendre les mesures de réponse à l'incident nécessaires. Les informations obtenues au cours du processus de Threat Hunting peuvent également être utilisées pour formuler de nouvelles hypothèses et améliorer les systèmes de protection, en mettant par rapport à jour les règles de filtrage du trafic.

Modèle de maturité de la recherche

Le modèle de maturité de la recherche (HMM) est un système utilisé pour évaluer le degré de préparation d'une organisation en vue d'effectuer une recherche proactive des menaces. Le niveau de « maturité » dépend des outils et des méthodes disponibles et utilisées par l'entreprise :

- **Initial (HMM0)** : l'organisation s'appuie principalement sur des systèmes de sécurité traditionnels. Dans le même temps, des informations minimales sont recueillies à partir d'éléments clés de l'infrastructure informatique.
- **Minimal (HMM1)** : les analystes collectent régulièrement des informations à partir de l'infrastructure informatique et utilisent des données de cyber-intelligence.
- **Procédural (HMM2)** : l'organisation utilise des scénarios de Threat Hunting standards. À ce niveau, les experts en sécurité informatique collectent et analysent une grande quantité de données, mais ne développent pas leurs propres procédures de Threat Hunting.
- **Innovant (HMM3)** : les experts en sécurité informatique collectent et analysent une grande quantité de données, développent et mettent en œuvre leurs propres méthodes de Threat Hunting, et les utilisent régulièrement.
- **De pointe (HMM4)** : les experts en sécurité informatique ne se contentent pas de développer le Threat Hunting et des méthodes d'analyse, mais automatisent également ces éléments. Cela aide à révéler davantage de menaces et permet aux analystes de se concentrer sur l'amélioration des systèmes de détection et sur la protection globale de la société.

De quoi avez-vous besoin pour réussir votre Threat Hunting ?

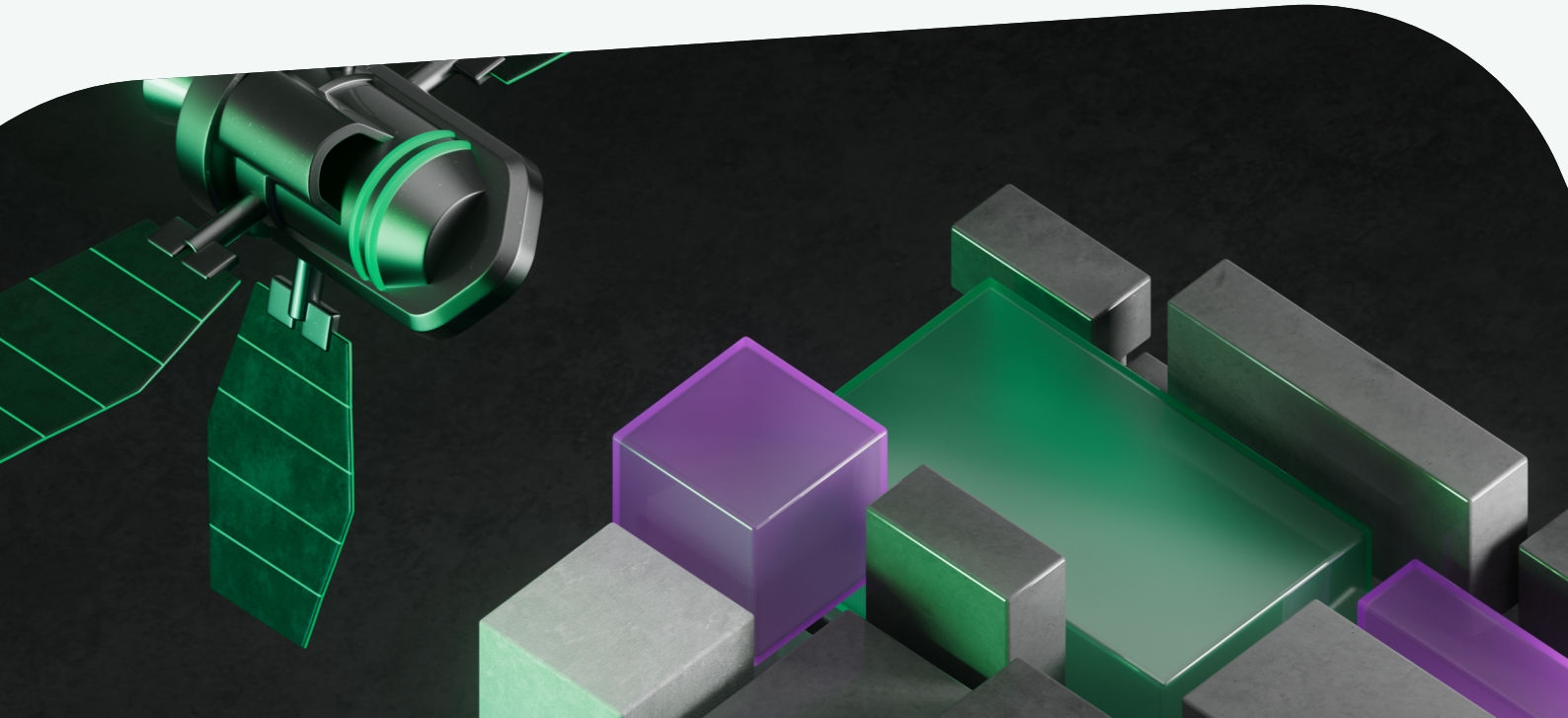
Pour fournir les bases d'une recherche, les « chasseurs » de menaces utilisent généralement les données de solutions incluant l'EDR (Endpoint Detection and Response) et les analyses de sécurité. Dans l'idéal, ces outils doivent être intégrés pour permettre aux IoA et aux IoC de fournir une assistance maximale pour guider la recherche.

- L' EDR offre une visibilité complète sur tous les terminaux du réseau de l'entreprise et procure des systèmes de défense avancés, automatisant les tâches de routine EDR et permettant aux analystes de rapidement chercher, hiérarchiser, examiner et neutraliser les menaces les plus sophistiquées et les attaques de type APT.
- Les analyses de la sécurité offrent des informations plus approfondies sur les données de sécurité. En combinant le Big Data recueilli par la technologie de sécurité à l'IA et au Machine Learning, les analyses de la sécurité peuvent accélérer l'examen des menaces en fournissant des données d'observation détaillées pour le Threat Hunting.

Le Threat Hunting avec Kaspersky EDR Expert ou Kaspersky MDR

Une impossibilité à rendre opérationnel le Threat Hunting, ou le fait de ne pas avoir une vision claire des TTP d'un adversaire, peut entraver la hiérarchisation des alertes et une analyse et une réponse plus poussées. Cependant, grâce à Kaspersky Endpoint Detection and Response (EDR) Expert, les données brutes et les diagnostics sont agrégés de manière centralisée, et les possibilités d'examen sont renforcées grâce à nos IoA propriétaires, à l'enrichissement MITRE ATT&CK, à un outil flexible de création de recherche et à l'accès à notre portail de Threat Intelligence. Toutes ces capacités améliorent la recherche efficace des menaces et accélèrent la réponse aux incidents, afin de limiter et d'empêcher les dommages.

Kaspersky Managed Detection and Response (MDR) peut être utilisé pour fournir des capacités de Threat Hunting en sous-traitant cette expertise difficile à trouver aux experts de Kaspersky. Le MDR applique la Threat Intelligence et le Threat Hunting proactif pour identifier et supprimer les menaces avancées. Le MDR peut également contribuer à réduire les temps d'arrêt dus aux attaques, et proposer des réponses rapides et décisives aux attaques dans le réseau.



Votre checklist du Threat Hunting

Maintenant que vous avez terminé cette courte présentation, vous devriez avoir une compréhension plus claire de ce qu'est ou n'est pas le Threat Hunting, et savoir pourquoi et à quel moment vous devez l'effectuer. Aussi, pour vous aider à préparer votre premier exercice de Threat Hunting, voici une checklist rapide.

Avez-vous bien conscience que 90 % des menaces sont interceptées par des outils comme l'EPP, et que le Threat Hunting peut vous aider à découvrir les 10 % restants, et savez-vous pourquoi il est important de faire cela régulièrement ?

Comprenez-vous la différence entre les termes IoC, IoA et TTP ? Avez-vous consulté les éléments les plus récents de la Threat Intelligence et des ressources essentielles telles que MITRE ATT&CK, qui peuvent vous aider en vous fournissant les informations détaillées dont vous avez besoin ?

Pouvez-vous expliquer à vos collègues ce qu'est le Threat Hunting et ce qu'il n'est pas, afin de faciliter la définition d'attentes réalistes pour votre équipe de sécurité informatique ? En particulier, savez-vous clairement pourquoi un Threat Hunting qui ne délivre aucun résultat concret est aussi important qu'une autre recherche révélant une menace n'ayant encore jamais été vue dans la nature ?

Êtes-vous prêt à utiliser des outils comme l'EDR, le MDR et les analyses de sécurité pour obtenir les données dont vous avez besoin pour savoir ce qui se passe dans votre système, et analyser cela en recherchant des signes d'une attaque ?

Répondez « oui » à toutes ces questionset vous serez opérationnel. Voici venu le moment de commencer à repérer tous ces loups et ours.

En savoir plus

www.kaspersky.fr