SOPHOS
Cybersecurity delivered.

Guide d'introduction à la chasse aux menaces

Conseils pratiques pour se préparer à rechercher et neutraliser les cybermenaces furtives

Les cyberattaques évoluent. Les adversaires se tournent de plus en plus vers des méthodes sophistiquées et très évasives pour faciliter et exécuter leurs attaques. La pratique de la chasse et de la neutralisation des activités malveillantes est donc devenue essentielle dans la lutte contre ces menaces avancées — mais cette tâche n'est pas aisée.

Dans ce rapport, nous fournissons des conseils pour vous aider à vous lancer dans la chasse aux menaces, ainsi qu'un résumé des outils et des cadres de travail que les équipes de sécurité utilisent pour garder une longueur d'avance sur les dernières cybermenaces et répondre rapidement à toute attaque potentielle. Nous vous proposons également 5 étapes que les professionnels de l'IT doivent suivre pour se préparer à la chasse aux menaces.

Un livre blanc Sophos. Août 2022

L'état des cybermenaces en 2022

Les attaques ont augmenté en volume, en complexité et en impact

Le défi de cybersécurité auquel sont confrontées les organisations ne cesse de croître. En 2021, 57 % des organisations ont connu une augmentation du volume des cyberattaques, 59 % ont vu la complexité des attaques augmenter et 53 % ont déclaré que l'impact des attaques avait augmenté. Près de trois organisations sur quatre (72 %) ont constaté une augmentation dans au moins un de ces domaines.

Une tendance croissante est l'augmentation des attaques de la supply chain, comme l'incident impliquant SolarWinds révélé en mars 2021. Les attaquants avaient inséré des instructions modifiées dans le code source de la solution Orion, utilisée pour gérer à distance des réseaux complexes. Cette porte dérobée (backdoor) a permis aux adversaires d'accéder aux réseaux des clients de SolarWinds, dont plusieurs agences gouvernementales.

Les ransomwares sont une menace réelle pour toutes les organisations

66 % des organisations ont été touchées par un ransomware en 2021, une hausse de 37 % par rapport à 2020. C'est une augmentation de 78 % en un an. Ce résultat montre que les adversaires sont devenus bien plus capables d'exécuter des attaques à grande échelle.

L'utilisation croissante d'outils légitimes dans les cyberattaques

Les adversaires tirent de plus en plus profit de copies illégales ou piratées de logiciels commerciaux standards et d'outils open source gratuits. En général, ces outils sont conçus pour simuler des cyberattaques afin d'améliorer la sécurité, mais ils peuvent être exploités par des criminels pour faire exactement le contraire.

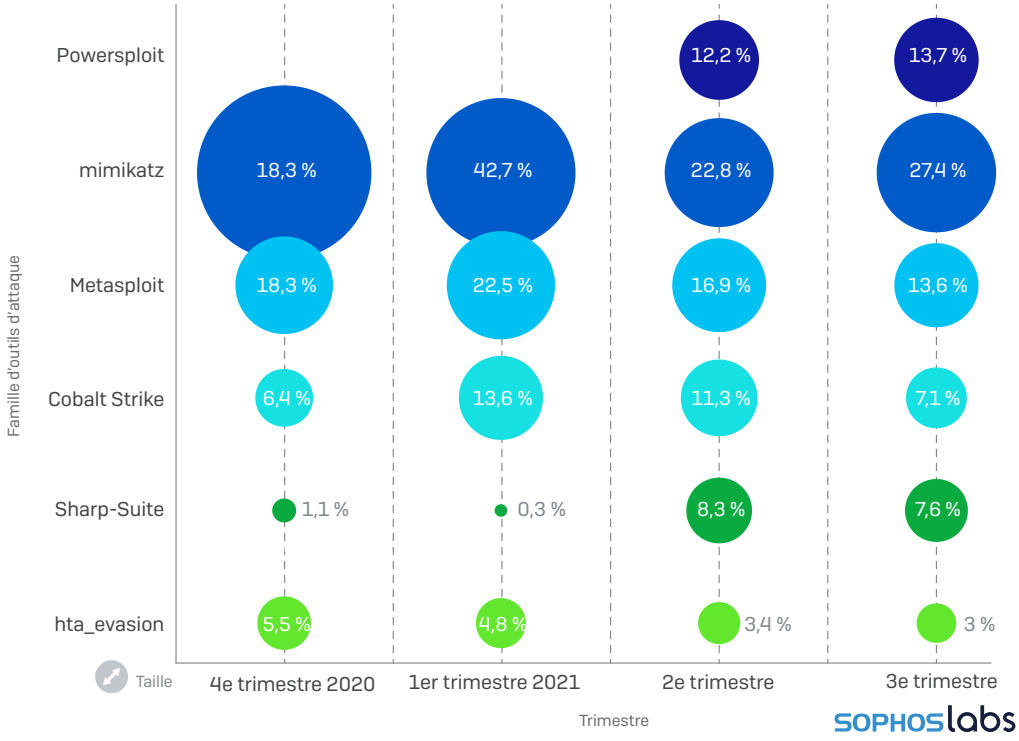
Les outils tels que Mimikatz (utilisé aussi bien par les pentesters que les auteurs de malwares), bien que n'étant pas des offres strictement commerciales, ont été largement utilisés, apparaissant dans presque tous les incidents, pilotés manuellement, que Sophos a investigués en 2021.

En outre, les copies piratées de Cobalt Strike (un logiciel de simulation d'adversaire), utilisées non seulement lors d'attaques de ransomware, mais également distribuées sous la forme de charge virale initiale permettant de déclencher d'autres malwares, étaient également bien présentes (grâce à la fuite de leur code source en 2020).

[1] *L'état des ransomwares 2022 - Sophos*
[2] *L'état des ransomwares 2022 - Sophos*

Prévalence des meilleurs outils d'attaque

Sur une base 'par machine', les outils d'attaque les plus fréquemment rencontrés, observés en 2020-2021



Rapport Sophos 2022 sur les menaces

La fonction « Beacons » de Cobalt Strike, qui permet d'ouvrir une porte dérobée sur les machines Windows, a fait de ce logiciel l'outil préféré des cybercriminels. Ainsi, la plupart des cas de ransomwares que nous avons pu observer en 2021 impliquaient l'utilisation de balises Cobalt Strike.

Pour un aperçu plus détaillé de l'état actuel des cybermenaces, consultez le dernier rapport Sophos sur les menaces.

Des pratiques proactives en matière de cybersécurité sont indispensables

Attaques de la supply chain. Exploits de logiciel. Outils légitimes. Le thème commun est la nature de ces approches. Elles sont pilotées par des personnes, et non par des machines. Elles sont hautement ciblées et calculées. Elles sont évasives et indétectables par les moyens traditionnels.

Les organisations doivent adopter des approches plus proactives en matière de cybersécurité pour garder une longueur d'avance sur les criminels. Répondre à des adversaires humains nécessite une approche menée par des experts humains.

C'est là que la chasse aux menaces entre en scène.

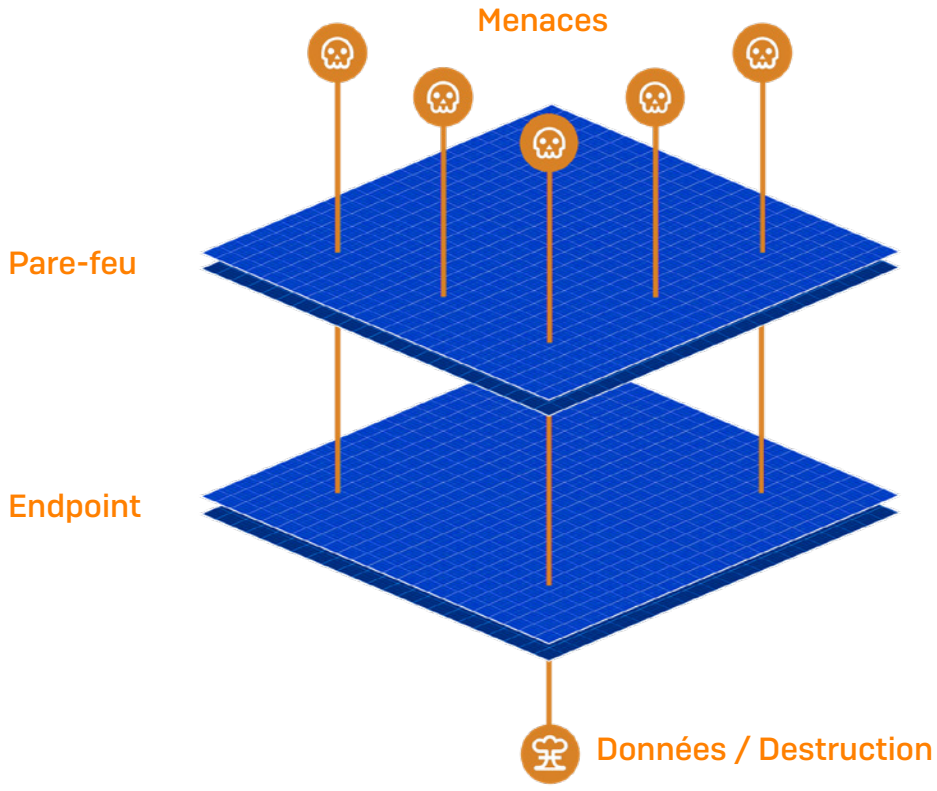
Qu'est-ce que la chasse aux menaces ?

La chasse aux menaces est le processus itératif et proactif de recherche dans les données de télémétrie des postes et des réseaux pour identifier les activités malveillantes. Ce processus doit être effectué avec en tête l'idée que les adversaires ont déjà contourné les défenses. Nous la qualifions d'itérative, car la pratique doit s'adapter en permanence pour rester une méthode efficace pour rechercher et neutraliser les cybermenaces actuelles, qui évoluent tout autant.

Au cours d'une chasse aux menaces, les équipes analysent les tactiques, techniques et procédures (TTP) utilisées par les auteurs de la menace pour déterminer le stade de l'attaque et obtenir des informations. Une fois que le stade sera établi, les équipes prendront une mesure appropriée pour neutraliser la menace si nécessaire.

Pourquoi avons-nous besoin de chasser les menaces ?

Les raisons sont multiples, mais une raison prévaut sur toutes les autres : contrairement à ce que l'on peut parfois entendre, la technologie seule ne peut pas arrêter 100 % des menaces. Malgré de multiples couches de défenses, certaines menaces se faufilent toujours dans les parcs informatiques et les compromettent.



Comme nous l'avons déjà mentionné, les auteurs modernes des menaces se tournent de plus en plus vers des approches adaptatives et évasives qui sont littéralement pilotées manuellement au lieu des attaques automatisées et à grande échelle d'avant.

Cela se reflète dans les observations de nos équipes de réponse aux menaces, qui signalent une augmentation significative du nombre d'adversaires humains contrôlant et dirigeant les attaques. Cela signifie que les équipes de sécurité doivent partir à la chasse à l'inconnu pour rester en première ligne, tout en adoptant l'état d'esprit selon lequel une violation a déjà eu lieu.

La mentalité de la chasse aux menaces

Les chasseurs de menaces expérimentés partent souvent du principe qu'une menace est déjà parvenue à échapper aux défenses, quel que soit l'endroit où elle se trouve dans la chaîne d'attaque. Ils adoptent cette mentalité, car elle les oblige à faire deux choses.

Limiter le temps de présence des auteurs de la menace

Adopter cet état d'esprit oblige les équipes à limiter le temps de présence de l'auteur de la menace. Plus un cybercriminel reste longtemps à l'intérieur de votre réseau, plus il a de temps pour exécuter des activités néfastes. Par conséquent, moins on laisse de temps à un adversaire à l'intérieur d'un réseau, moins il peut faire de dégâts. Les équipes de sécurité sont obligées de rechercher les menaces avant que leur impact ne se fasse sentir en présupposant que les défenses ont déjà été contournées.

Réduire le temps de détection

Adopter cette mentalité oblige également les équipes à réduire le temps moyen de détection. Vous pouvez avoir mis en place plusieurs couches de défense, mais la menace évasive peut déclencher votre défense plus loin dans sa chaîne d'attaque. Le problème, c'est qu'à ce stade, il est déjà trop tard — le mal est fait, car la menace est déjà allée trop loin. En chassant la menace, nous pouvons être en mesure d'identifier les failles dans notre sécurité. Celles-ci peuvent alors être corrigées, réduisant le temps nécessaire pour détecter la même menace ou des menaces similaires à l'avenir.

Qui pratique la chasse aux menaces ?

Profil d'un chasseur de menaces

Avant de savoir qui pratique la chasse aux menaces, il est essentiel de comprendre le rôle d'un chasseur de menaces. La chasse aux menaces est une opération très complexe. Les personnes qui travaillent dans ce domaine doivent posséder un ensemble de compétences spécifiques et spécialisées. Cela dit, les qualités requises d'un chasseur de menaces sont les suivantes :

- **Créatif et curieux** : la recherche de menaces peut s'apparenter à la recherche d'une aiguille dans une botte de foin. Les chasseurs de menaces peuvent souvent passer des jours à chercher des menaces, en utilisant de nombreuses méthodes pour les dénicher.
- **Expérience en cybersécurité** : la chasse aux menaces est l'une des opérations les plus avancées en matière de cybersécurité. Une expérience préalable dans ce domaine et des connaissances de base sont donc indispensables.
- **Connaissance du paysage des menaces** : il est indispensable de comprendre les dernières tendances en matière de menaces pour rechercher et neutraliser des entités inconnues.
- **Capacité à se mettre dans la peau des adversaires** : la capacité de penser comme un cybercriminel est essentielle pour lutter contre les approches humaines actuelles.
- **Capacité de rédaction technique** : les chasseurs de menaces sont tenus de consigner toutes leurs découvertes dans le cadre du processus d'investigation. Par conséquent, la capacité à communiquer des informations complexes est essentielle pour mener la chasse à son terme.
- **Connaissance du système d'exploitation (OS) et des réseaux** : une connaissance pratique avancée des deux est essentielle.
- **Expérience du codage et de l'écriture de scripts** : nécessaire pour aider les chasseurs de menaces à créer des programmes, à automatiser des tâches, à analyser les journaux et à effectuer des tâches d'analyse de données pour faciliter et faire progresser leurs investigations.

Malheureusement, à cette rare combinaison de compétences s'ajoute une pénurie notable de compétences dans le secteur informatique. 54 % des administrateurs informatiques estiment que, même avec tous les outils à leur disposition, les cyberattaques sont désormais trop avancées pour que leur équipe IT puisse y faire face seule. Dans les organisations où ces rôles sont pourvus, nous constatons que la chasse aux menaces est menée par l'une des deux équipes suivantes.

Centre d'opérations de sécurité (SOC) interne

Lorsque les organisations choisissent de pratiquer elles-mêmes la chasse aux menaces, vous trouverez les chasseurs employés au sein du SOC. Un SOC est une fonction interne centralisée qui se concentre sur la surveillance, la détection, l'investigation et la réponse aux cybermenaces tout en améliorant la posture de sécurité globale de l'organisation mère. Il s'agit de l'équipe à contacter au sein de l'organisation pour toute question de cybersécurité.

Fournisseurs tiers d'opérations de sécurité

De nombreuses organisations confient de plus en plus leurs opérations de sécurité à des fournisseurs tiers. Cela peut être dû à un manque de capacités internes (les équipes informatiques ont vu leur charge de travail en matière de cybersécurité augmenter de 69 % en 2021), à un manque de compétences ou à une préférence pour des experts externes pour cette tâche critique assurée 24 h/24 et 7 j/7.

Fournisseurs de services de détection et de réponse managés (MDR)

Le MDR (Managed Detection and Response), fourni sous forme de service entièrement géré, permet aux organisations de disposer d'une équipe dédiée d'analystes de sécurité qui chassent les menaces 24 h/24, 7 j/7 et 365 j/an. Selon ESG Research : « 51 % utilisent un fournisseur de services de détection et de réponse managées (MDR) pour aider à intégrer les données de télémétrie pour la détection et la réponse aux menaces ».

Les fournisseurs de services MDR présentent de nombreux avantages par rapport à un programme d'opérations de sécurité uniquement interne. Le plus grand avantage de ces fournisseurs est l'expérience.

L'équipe Sophos MDR a des milliers d'heures d'expérience, ayant déjà observé et traité les très nombreux défis lancés par les attaquants. Ils peuvent également tirer des leçons d'une attaque ciblant une organisation et les appliquer à tous leurs clients. Un autre avantage est l'échelle : l'équipe Sophos MDR peut fournir un support 24 h/24, 7 j/7 assuré par trois équipes internationales.

Fournisseurs de services de sécurité managés (MSSP)

Les MSSP sont employés pour gérer une partie ou la totalité des opérations de sécurité informatique de l'organisation, ce qui permet aux équipes internes de se concentrer davantage sur les tâches quotidiennes. Les MSSP offrent des capacités de chasse aux menaces dans le cadre d'un service géré. Il peut s'agir de services MDR tels que décrits ci-dessus.

Éléments facilitant la chasse aux menaces

EDR/XDR (Endpoint/Extended Detection and Response)

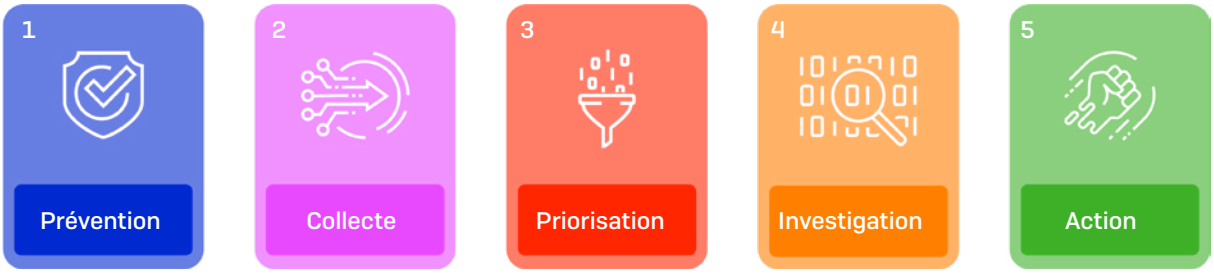
Pour que les chasseurs de menaces puissent identifier et enquêter sur des activités potentiellement malveillantes, ils ont besoin de données et d'outils d'investigation. C'est là qu'interviennent les technologies EDR et XDR. Elles permettent aux chasseurs de voir rapidement les détections suspectes et de les examiner en profondeur.

Comme son nom l'indique, l'EDR (Endpoint Detection and Response) fournit des données provenant de la solution Endpoint. En revanche, le XDR corrèle les signaux provenant de l'environnement informatique au sens large, notamment des solutions de pare-feu, de sécurité mobile, de messagerie et sécurité du Cloud. Étant donné que les adversaires exploitent toutes les opportunités d'attaque, plus vous élargissez votre réseau de signaux, mieux vous pouvez les détecter rapidement.

L'un des plus grands défis pratiques des solutions EDR/XDR est le bruit de fond : les chasseurs de menaces reçoivent tellement de signaux qu'ils peuvent ne voir que l'arbre qui cache la forêt. C'est pourquoi il est essentiel de combiner votre solution EDR/XDR avec une protection Endpoint puissante, qui bloque davantage de menaces en amont, permettant aux défenseurs de se concentrer sur des détections moins nombreuses et plus précises.

L'anatomie de la détection et de la réponse aux menaces

La chasse aux menaces est une composante d'une opération plus vaste : la détection et la réponse aux menaces. Chez Sophos, nous appliquons à nos chasses un cadre conceptuel de détection et de réponse aux menaces. Ce cadre se compose de 5 éléments fondamentaux.



1. Prévention

La mise en place de technologies de prévention robustes et correctement configurées (telles qu'une solution de protection Endpoint) empêche les attaquants de pénétrer dans votre réseau. Plus important encore, cela réduit également le nombre d'alertes de sécurité générées au quotidien. Avec moins d'alertes à traiter, l'équipe de sécurité peut mieux repérer et se concentrer sur les signaux qui comptent — en l'occurrence, les adversaires évasifs pilotant manuellement leurs attaques.

2. Collecte d'événements, d'alertes et de détections de sécurité

Les données sont le carburant qui alimente la chasse et l'analyse des menaces. Sans le bon type, le bon volume et la bonne qualité de signaux, il est difficile pour les équipes de sécurité d'identifier avec précision les indicateurs d'attaque potentiels. Les données sans contexte compliquent la prise de décision de l'analyste. Sans métadonnées significatives associées au signal, l'analyste aura du mal à déterminer si les signaux sont malveillants ou bénins.

3. Priorisation des signaux qui comptent

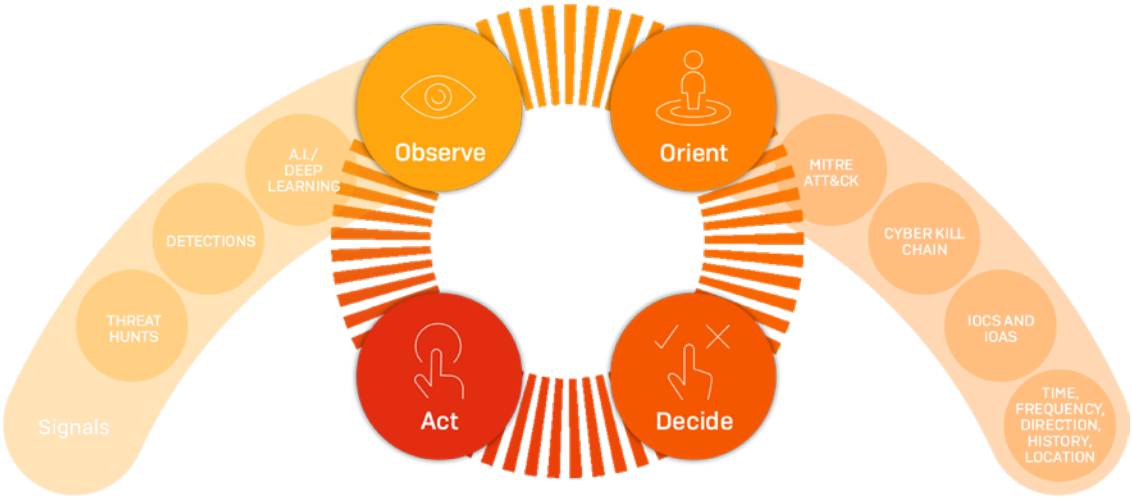
Pour éviter d'être submergé par les données et de ne pas repérer les éléments qui méritent d'être examinés, vous devez être capable d'identifier les alertes qui comptent. Et cela est plus difficile qu'il n'y paraît. Plus vous pouvez améliorer les ratios signal/bruit en utilisant une combinaison de contextes que seuls les producteurs d'événements peuvent fournir et l'intelligence artificielle automatisée, mieux c'est. Même avec l'automatisation, le processus n'est pas simple.

4. Investigation

Une fois que vous avez isolé les signaux clés, il est temps d'ajouter de la connaissance et de mesurer ce que vous avez découvert par rapport aux cadres et modèles de l'industrie pour établir un seuil de confiance dans la conviction d'un comportement malveillant ou bénin.

Cadre d'investigation OODA

Les analystes de sécurité expérimentés utilisent souvent un cadre pour guider leurs investigations. Par exemple, l'équipe Sophos MDR utilise une méthodologie d'investigation connue sous le nom de « boucle OODA ». Cela leur permet de s'engager dans le cycle mentionné ci-dessus pour s'assurer que toutes les conclusions sont testées et prouvées :



La boucle OODA est un concept militaire qui permet à notre équipe de passer par un cycle de raisonnement pour comprendre pleinement l'événement et le comportement qui l'entoure. L'équipe peut ensuite s'appuyer sur ces informations et faire appel à leur capacité de décision et à leur intuition pour déterminer si une activité malveillante est présente dans l'environnement d'un client et, sur cette base, décider comment agir.

Lorsqu'ils appliquent le cadre OODA, les analystes de sécurité de Sophos effectuent souvent les étapes suivantes :

- **Observer** : que voyons-nous dans cette détection ?
  - Observation des connexions externes et internes potentielles liées à la détection.
  - Détermination de l'endroit où la détection a lieu et si des utilisateurs finaux y sont associés.
- **Orienter** : que comprenons-nous de cette détection ?
  - Collecte des données fondées sur des preuves.
  - Compréhension des TTP communs ou spécifiques à cette attaque ou aux auteurs de la menace. L'une des ressources utilisées pour identifier les TTP est le cadre ATT&CK de MITRE, sur lequel nous reviendrons plus loin dans ce rapport.
  - Collecte de renseignements sur les indicateurs d'attaque (IOA) et les indicateurs de compromission (IOC).
- **Décider** : cette détection est-elle malveillante, suspecte ou bénigne ? Une action est-elle nécessaire ?
- **Agir** : sur la base des étapes précédentes, que ferez-vous ?
  - Atténuer – neutraliser – recommencer – améliorer.

5. Action

C'est un point très important. Une fois que vous avez déterminé que vous avez affaire à une menace, vous devez faire deux choses, et elles sont toutes deux aussi importantes l'une que l'autre.

La première consiste à atténuer le problème immédiat, tandis que la seconde consiste à se rappeler que vous ne traitez probablement qu'un symptôme de l'attaque et qu'il vous faut encore traquer et neutraliser la cause profonde. La première étape doit être réalisée sans nuire à votre capacité à réaliser la seconde.

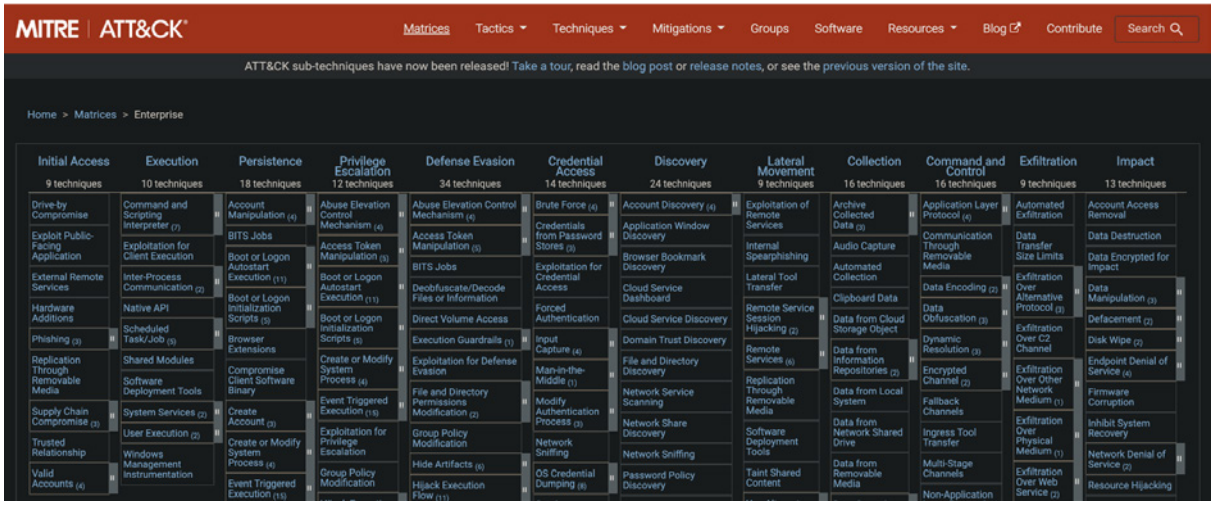
Parfois, il suffira de mettre une machine en quarantaine ou de la déconnecter du réseau, alors qu'à d'autres moments, l'équipe de sécurité devra creuser profondément dans le réseau pour extraire les ramifications d'un attaquant.

Par exemple, ce n'est pas parce que vous avez réussi à bloquer et à supprimer les logiciels malveillants de votre système et à ne plus voir l'alerte qui vous a mis sur la piste que l'attaquant a été éliminé de votre environnement.

Les chasseurs de menaces professionnels, qui voient des milliers d'attaques, savent quand et où il faut regarder plus loin. Ils analysent tout ce que les attaquants font, ont fait ou prévoient de faire dans le réseau, et les neutralisent.

Classification des menaces : le cadre ATT&CK de MITRE

Une ressource souvent utilisée par les chasseurs de menaces est le cadre ATT&CK de MITRE. Si vous avez passé un peu de temps dans le domaine de la cybersécurité, il est fort probable que vous en ayez entendu parler. Parmi de nombreux cadres, MITRE est une base de connaissances accessible au niveau mondial sur les TTP des adversaires, basée sur des observations du monde réel, et est utilisée comme base pour développer des modèles et des méthodologies de menaces spécifiques. Ce cadre permet aux chasseurs de menaces de faire correspondre les comportements des attaquants à une pléthore de TTP préalablement identifiés. Cela permet ensuite aux chasseurs de déterminer à quel stade se trouve l'attaque en cours. Elle est essentielle à l'étape « Orienter » du cadre OODA.



Vous pouvez obtenir des informations plus détaillées sur le cadre ATT&CK de MITRE ici.

Méthodes de chasse aux menaces

Cette section examine certaines méthodes de chasse aux menaces couramment utilisées. Chez Sophos, nous lançons souvent des chasses de deux manières différentes.

Chasse aux menaces à partir d'indices

Dans notre organisation, toute détection nécessitant un examen plus approfondi est analysée par un expert en menaces qui peut appliquer le contexte professionnel et un raisonnement humain à toute situation. Il observe le comportement, tient compte du contexte professionnel précédemment établi, élabore une hypothèse, puis agit en conséquence. L'hypothèse peut consister à s'engager activement dans l'incident potentiel ou à effectuer un travail d'investigation supplémentaire pour consolider ses connaissances sur le problème en question.

Pour boucler la boucle, l'analyste attendra et examinera les résultats de cette hypothèse et de ces tests. Si une investigation plus approfondie est nécessaire, il peut répéter ce cycle jusqu'à ce qu'il prenne une décision. Si l'événement s'est transformé en un incident actif, l'analyste passe en mode de réponse complet pour combattre activement la menace.

Chasse aux menaces sans indices de départ

Alors que les chasses aux menaces avec indices de départ nécessitent qu'un de nos capteurs détecte ou génère un « signal » d'intérêt, une chasse aux menaces sans indices de départ est beaucoup plus organique. Bien que nous puissions toujours utiliser nos algorithmes d'intelligence artificielle pour traiter la grande quantité de données que nous ingérons, les chasses aux menaces sans indices de départ sont presque toujours menées par un expert en menace.

Plutôt que de compter sur le signal systématique initial pour nous avertir que quelque chose doit être examiné, nous effectuons de manière proactive des requêtes sur le parc informatique d'un client, ou de plusieurs clients. Cela peut se produire pour plusieurs raisons, notamment :

- Un client dans le même secteur d'activité a été ciblé d'une manière particulière, et nous voulons nous assurer que les mêmes auteurs de la menace ne tentent pas d'attaquer d'autres clients.
- Les SophosLabs ont informé l'équipe Sophos MDR d'une attaque importante visant des clients, soit dans le même secteur, soit avec des propriétés similaires.
- Un événement important s'est produit dans le paysage de la sécurité, et nous voulons vérifier si l'un de nos clients est affecté.

Étude de cas : La chasse au ransomware qui a mis au jour un trojan bancaire historique

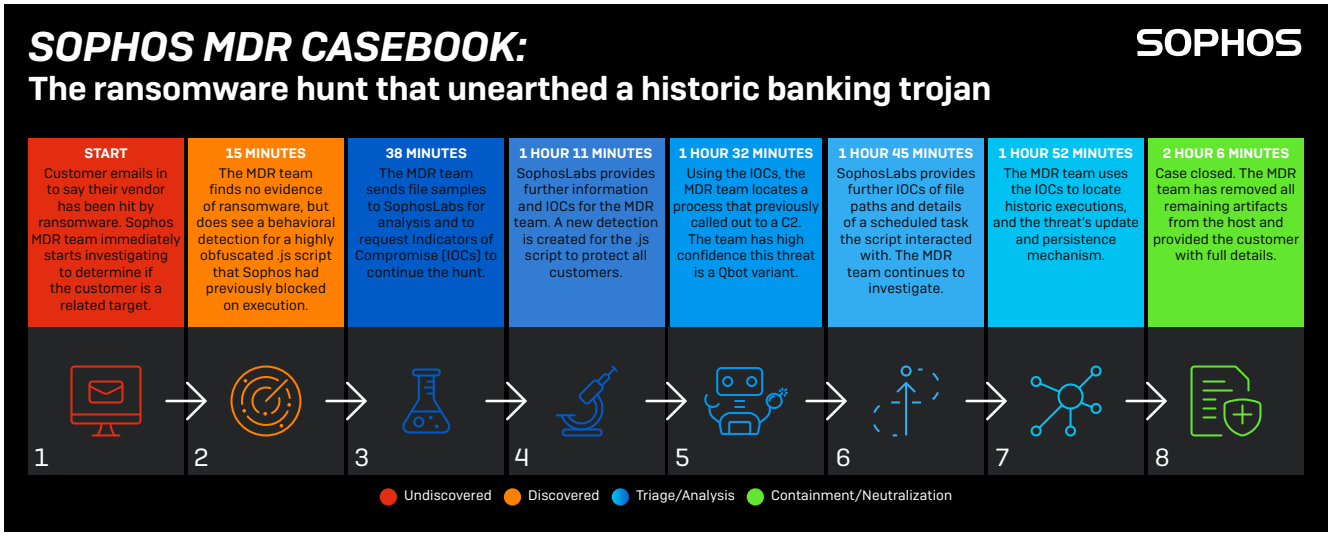
Maintenant que nous avons décrit les subtilités de la chasse aux menaces, passons en revue une chasse aux menaces en action. Ce cas, étudié par l'équipe Sophos MDR, est un excellent exemple qui illustre la manière avec laquelle une chasse aux menaces peut découvrir l'inattendu. Ici, un client nous a contactés pour nous dire qu'un fournisseur avec lequel il travaillait avait été touché par un ransomware et qu'il craignait d'avoir été lui aussi infecté.

L'équipe Sophos MDR a immédiatement commencé à investiguer, en collaboration avec nos experts des SophosLabs. Ils ont rapidement réalisé qu'il n'y avait pas d'indices concordants avec une attaque de ransomware. À ce stade, certaines équipes auraient pu clore le dossier et passer à autre chose. Cependant, l'équipe Sophos MDR a continué son investigation et découvert un trojan bancaire historique.

Le client a pu souffler de soulagement en sachant qu'il n'avait pas été affecté par un ransomware et qu'un malware bancaire historique avait été entièrement supprimé ; un résultat qui n'aurait pas été obtenu sans une intervention experte.

Et comme le montre ce témoignage, si les ransomwares sont souvent la menace la plus visible, il est essentiel d'être également attentif aux attaques qui préfèrent se cacher dans l'ombre.

En 2 heures et 6 minutes, l'incident a été analysé et nettoyé.



Pour plus de détails sur cette histoire, consultez notre article Sophos News ici (en anglais).

Se préparer à la chasse aux menaces : 5 étapes pour un résultat fructueux

Vous avez maintenant, je l'espère, une bonne connaissance de tout ce qui concerne la chasse aux menaces. Cependant, avant de commencer, il est essentiel de s'assurer que votre organisation est équipée pour la mener à bien.

1. Identifiez la maturité de vos opérations de cybersécurité actuelles

Avant de pouvoir commencer à comprendre les adversaires potentiels, vous devez connaître l'état de vos opérations de cybersécurité actuelles. La mise en correspondance de vos processus avec un modèle de maturité de la cybersécurité (tel que le CMMC, Cybersecurity Maturity Model Certification) est un excellent moyen d'établir dans quelle mesure vous êtes bien équipé (ou non) pour commencer la chasse aux menaces. Il est également judicieux d'auditer votre posture de sécurité afin de déterminer votre niveau de vulnérabilités aux menaces.

2. Décidez comment vous voulez procéder à la chasse aux menaces

Une fois que vous avez établi votre cybermaturité, vous pouvez décider si la chasse aux menaces est une activité que vous souhaitez réaliser en interne, externaliser entièrement ou combiner les deux.

3. Identifiez les failles technologiques

Passez en revue vos outils existants et identifiez ce dont vous avez besoin pour effectuer une chasse aux menaces efficace. Quelle est l'efficacité de votre technologie de prévention ? Possède-t-elle ou prend-elle en charge les capacités de chasse aux menaces apportées par l'EDR/XDR ?

4. Identifiez les lacunes en matière de compétences

La chasse aux menaces est complexe et nécessite des compétences spécialisées. Si vous ne disposez pas de l'expérience nécessaire en interne, envisagez de suivre des formations pour vous aider à développer les compétences requises. Envisagez également de travailler avec un prestataire externe pour compléter votre équipe.

5. Élaborez et mettez en œuvre un plan de réponse aux incidents

Avant de vous lancer dans la chasse aux menaces, il est essentiel de mettre en place un plan de réponse aux incidents complet afin de garantir que toute réponse soit mesurée et contrôlée. Un plan de réponse bien préparé et bien compris, que toutes les parties clés peuvent immédiatement mettre en œuvre, réduira considérablement l'impact d'une attaque sur votre organisation.

Un bon plan de réponse aux incidents doit définir les protocoles de préparation, de détection et de reporting, de triage et d'analyse, de confinement et de neutralisation, ainsi que les activités post-incident. Pour obtenir des conseils sur l'élaboration d'un plan de réponse aux incidents efficace, consultez notre guide de réponse aux incidents.

Pour plus de conseils pratiques sur la préparation et la conduite de la chasse aux menaces, visionnez notre événement Sophos Threat Hunting Academy.

Comment Sophos peut vous aider

Comme nous l'avons déjà mentionné, une chasse aux menaces efficace est incroyablement complexe et nécessite des technologies de nouvelle génération associées à une expertise humaine étendue. Heureusement, Sophos peut vous aider à atteindre vos objectifs de chasse aux menaces, quelle que soit votre maturité en matière de cybersécurité.

Empêchez les menaces de pénétrer votre réseau avec Sophos Intercept X Endpoint

Les chasseurs de menaces ne peuvent remplir leur rôle efficacement que s'ils ne sont pas inondés d'alertes de sécurité. Une façon d'y parvenir est d'introduire les meilleures technologies de prévention afin que les défenseurs puissent se concentrer sur des détections moins nombreuses et plus précises, et rationaliser le processus d'investigation et de réponse qui s'ensuivent. C'est là qu'intervient Sophos Intercept X Endpoint.

Sophos Intercept X est la solution de sécurité Endpoint leader sur le marché qui réduit la surface d'attaque et empêche les attaques de se produire. En combinant des capacités anti-exploit et anti-ransomware, le Deep Learning de l'IA et des technologies de contrôle, la solution bloque les menaces avant qu'elles n'aient un impact sur vos systèmes. Intercept X utilise une approche globale de défense en profondeur plutôt que de s'appuyer sur une seule technique de sécurité.

Les capacités de prévention de la protection Endpoint Sophos Intercept X bloquent 99,98 % des menaces (score moyen AV-TEST de janvier à novembre 2021). Les défenseurs peuvent alors mieux se concentrer sur les signaux suspects qui nécessitent une intervention manuelle.

Vous pouvez en savoir plus ou faire un essai d'Intercept X Endpoint ici.

Réalisez la chasse aux menaces vous-mêmes – Sophos XDR

Conçu pour les analystes de sécurité travaillant dans des équipes SOC dédiées et les administrateurs informatiques couvrant la sécurité et d'autres responsabilités informatiques, Sophos XDR permet à votre équipe de détecter, d'enquêter et de répondre aux incidents sur les postes de travail, les serveurs, les pare-feux, les charges de travail du Cloud, la messagerie, les mobiles, etc.

Accédez immédiatement aux informations qui vous intéressent en choisissant parmi une bibliothèque de requêtes pré-écrites et personnalisables couvrant de nombreux scénarios différents de chasse aux menaces et d'opérations informatiques — ou rédigez les vôtres. Vous avez accès aux données en temps réel des appareils, jusqu'à 90 jours de données sur disque, 30 jours de données stockées dans le référentiel Cloud Sophos Data Lake, et une liste d'éléments suspects générée automatiquement pour que vous sachiez exactement par où commencer.

Si vous souhaitez essayer Sophos XDR pour chasser vous-même les menaces, Sophos vous donne les outils dont vous avez besoin pour pratiquer des chasses avancées et maintenir l'hygiène de vos opérations de sécurité. Vous pouvez soit démarrer une évaluation du produit directement dans Sophos Central (si vous avez un compte Sophos Central) ou soit faire une évaluation d'Intercept X, qui inclut Sophos XDR.

Chasse aux menaces en tant que service entièrement géré ou pour compléter votre équipe – Sophos MDR

Sophos MDR est une solution MDR à multiples facettes, complète et primée, qui met l'expertise et les compétences de l'équipe d'analystes de sécurité de Sophos et leur vaste ensemble de capacités au service de votre réseau et de vos environnements Cloud. Sophos devient une extension de vos opérations de sécurité, ajoutant ses vastes capacités aux vôtres.

L'équipe Sophos MDR, composée de chasseurs de menaces et d'experts en réponse, va :

- Chasser de manière proactive et confirmer les menaces et incidents potentiels
- Utiliser toutes les informations disponibles pour déterminer l'ampleur et la criticité des menaces
- Prendre en compte le contexte professionnel approprié pour valider les menaces
- Lancer des actions pour intercepter, contenir et neutraliser les menaces
- Fournir des conseils pratiques pour remédier aux causes profondes des incidents récurrents

Même si votre organisation est dotée d'un SOC expérimenté, vous pourriez avoir besoin d'une deuxième paire d'yeux pour surveiller votre environnement et vous assurer que rien ne vous échappe. Sophos MDR réunit la chasse aux menaces et la protection Endpoint tout en fournissant une supervision et une expertise au quotidien. Vos ressources réseau et Cloud sont une priorité absolue pour les analystes réseau et les chasseurs de menaces Sophos qui surveillent, corrigent et neutralisent activement les menaces en votre nom.

Avec un excellent service MDR, vous et votre organisation pouvez dormir sur vos deux oreilles en sachant qu'une équipe d'experts qualifiés surveille constamment votre organisation, chasse les menaces, analyse les activités suspectes et répond aux incidents potentiels. Avec le panorama des menaces de cybersécurité qui ne cesse de s'étendre, vous pouvez travailler en toute tranquillité avec une équipe dont l'unique objectif est la cybersécurité.

Pour discuter de la façon dont Sophos MDR peut aider votre organisation, contactez votre représentant Sophos ou demandez à être rappelé. Dans l'intervalle, consultez les dernières recherches et les dernières études de cas de Sophos MDR.

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

22-08-08 WP-FR (PC)