Livre blanc réalisé par WithSecure™

Démystifier **le threat hunting**

WITH secure

Sommaire

Pourquoi lire ce livre blanc

Dans le secteur de la cyber sécurité, le terme Threat Hunting a le vent en poupe. Et, comme toute expression à la mode, celui-ci est souvent malmené. Il n'est pas rare de voir des fournisseurs rebaptiser leurs services de sécurité « Threat Hunting » sans pour autant apporter à leur offre la moindre amélioration.

Nous souhaitons ici éclaircir la situation. Ce livre blanc vous expliquera :

- Ce qu'est - et ce que n'est pas - le Threat Hunting
- Ce qu'est la réponse continue et pourquoi celle-ci est essentielle
- Pourquoi la réponse continue et le Threat Hunting sont indispensables pour vous défendre efficacement contre les attaques ciblées
- Comment fonctionne un Threat Hunting efficace
- Quel sera l'avenir du Threat Hunting

Nous avons également réalisé une séquence vidéo, dans laquelle nos « Threat Hunters » vous parlent de leur métier, avec leurs propres mots. Un lien vers cette vidéo vous sera proposé dans ce livre blanc.

1. Confusion sur le marché

Chez WithSecure™ Countercept, nous nous sommes donnés une mission avec ce livre blanc. Nous souhaitons vous aider à comprendre ce qu'est réellement le Threat Hunting. Nous entendons vous en démontrer l'importance et vous expliquer comment mener des opérations de Threat Hunting efficaces. Cependant, avant toute chose, il convient de faire le point sur certaines idées reçues, pour séparer la réalité de la fiction.

Mythes et idées reçues sur le Threat Hunting

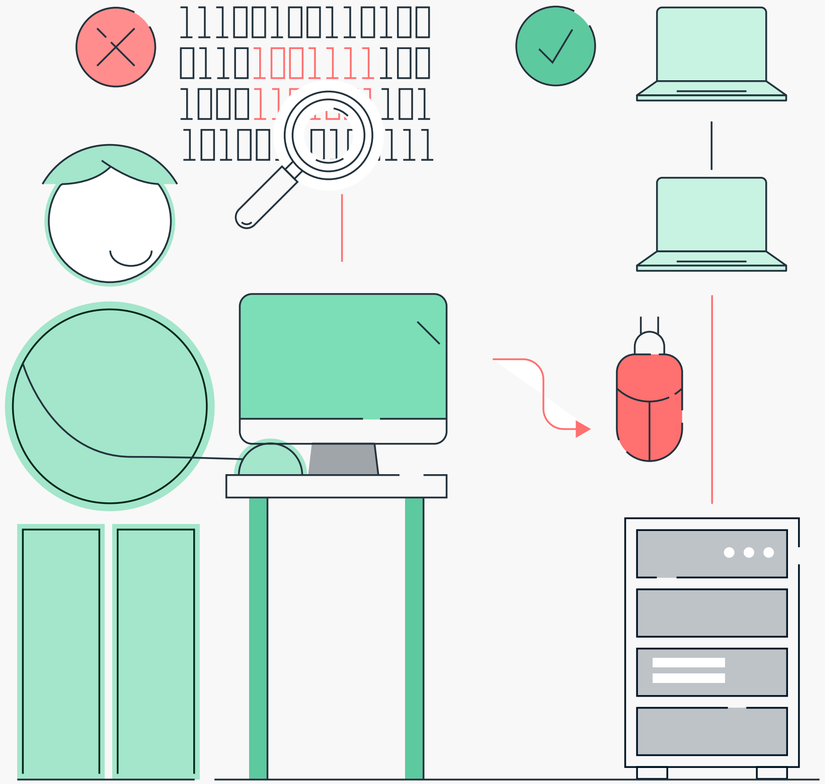
1

Mythe

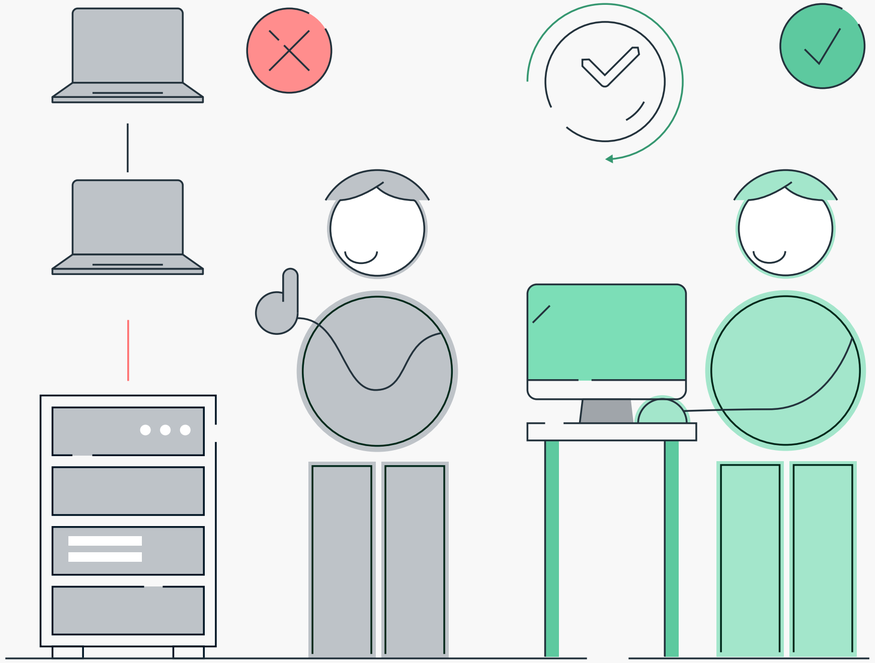
Le Threat Hunting est une recherche manuelle menée sur des données brutes, pour débusquer un pirate informatique.

Réalité

En une seule journée, un seul hôte génère plus d'un million d'événements. Il serait vain de parcourir manuellement de tels volumes de données à la recherche de signes d'attaque potentiels. Plutôt qu'une recherche manuelle laborieuse et inefficace, le Threat Hunting consiste à identifier les lacunes de vos outils de détection et à combler ces lacunes avant qu'un hacker ne cherche à en tirer profit.



2



Mythe

Le Threat Hunting peut être pratiqué de manière sporadique, sous la forme d'opérations ponctuelles menées au sein de l'entreprise (« hunt sprints »).

Réalité

Les hackers sont toujours à la recherche de nouvelles techniques de piratage moins chères et plus efficaces. Ils innovent constamment. Les entreprises doivent, par conséquence, disposer d'une défense continue, sans cesse renouvelée. Il ne peut s'agir seulement d'une activité ponctuelle.

3

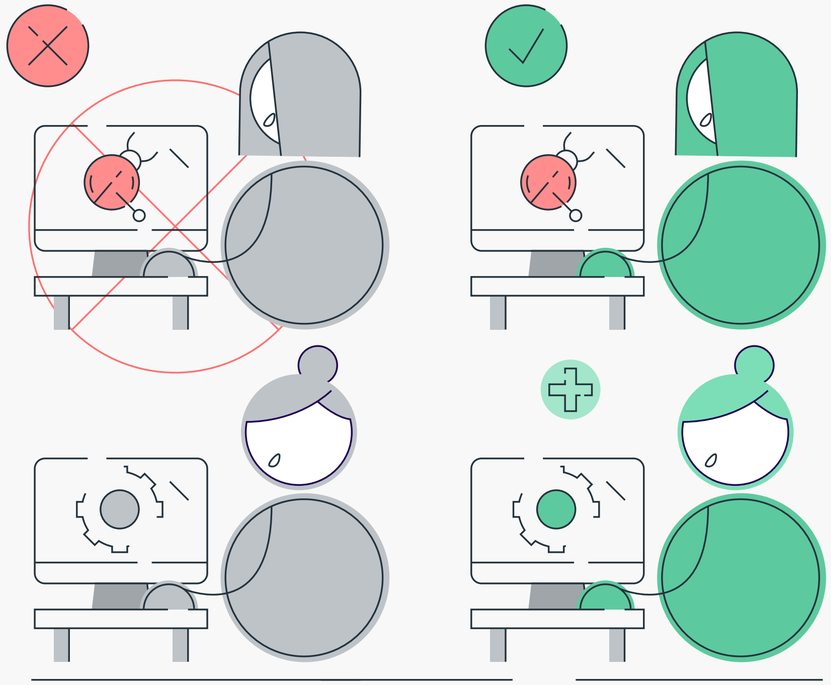
Mythe

Le Threat Hunting est LA nouvelle approche des centres d'opérations de sécurité (SOC).

Réalité

Le Threat Hunting n'est pas une nouvelle méthode destinée à révolutionner les process actuels des centres de cyber sécurité (SOC)… même si certains messages marketing laissent penser le contraire ! Le Threat Hunting est complémentaire des opérations de détection et de réponse. Il ne les remplace pas. Pour une défense efficace, les deux sont nécessaires.

4



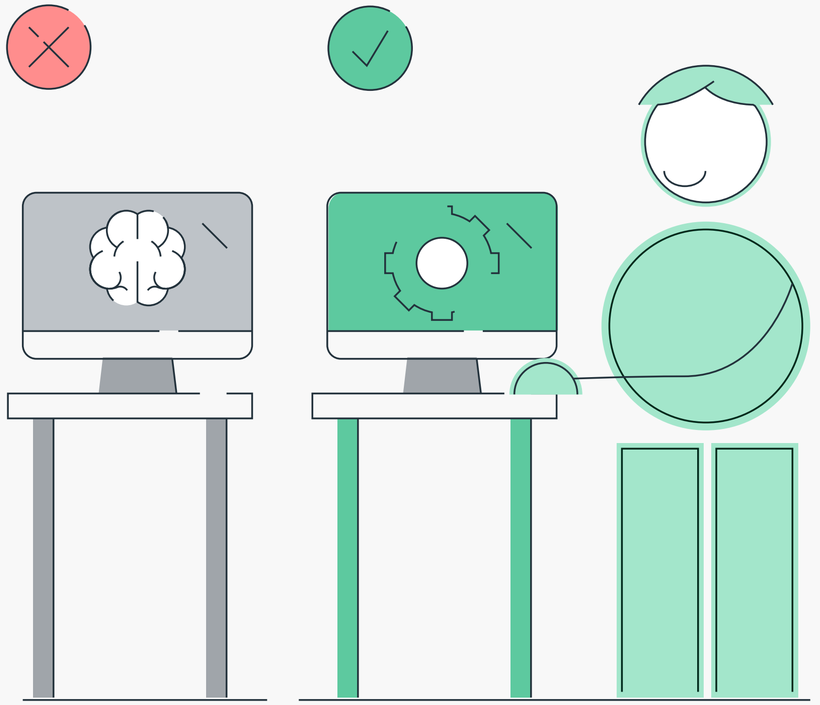
Mythe

Le Threat Hunting managé remplace la détection et la réponse gérées.

Réalité

Le MDR consiste à minimiser l'impact d'une cyber attaque en procurant à l'entreprise les outils de détection et de réponse qu'elle ne possède pas en interne. Le simple fait d'intégrer des "Threat Hunters" à un processus de détection et de réponse ne suffit pas à transformer le MDR en Threat Hunting managé. Tout fournisseur de services MDR fiable utilisera le Threat Hunting en parallèle des opérations de base pour s'assurer que ses outils de détection restent efficaces.

5



Mythe

Le Threat Hunting peut être automatisé grâce à l'intelligence artificielle.

Réalité

Les Threat Hunters les plus efficaces sont entraînés à penser comme les pirates informatiques, c'est-à-dire de manière offensive. Ils identifient les lacunes exploitables dans les systèmes de détection. Ce processus de réflexion exige une certaine créativité dont l'intelligence artificielle n'est pas capable. Certains problèmes de sécurité peuvent être résolus par la seule analyse des données mais le Threat Hunting n'en fait pas partie.

2. Ce qu'est réellement le threat hunting

Le Threat Hunting est né d'un besoin : se défendre contre toute une série d'attaques ciblées capables de contourner les outils de sécurité les plus innovants. Pour obtenir le meilleur des outils et des méthodologies à notre portée, il faut en connaître les limites et chercher à les améliorer constamment. Le Threat Hunting consiste à identifier les menaces échappant à vos outils de détection, pour ensuite définir des cas d'utilisation comblant ces lacunes. Le Threat Hunting complète vos capacités de détection, pour que toutes ces failles soient comblées avant qu'un hacker ne cherche à les exploiter.

Le Threat Hunting permet d'identifier des données complémentaires essentielles à la détection de futures attaques avancées. En développant des hypothèses et en simulant des attaques, cette approche permet d'élaborer une stratégie de détection basée sur les attaques identifiées par l'équipe de détection et réponse.

L'expression « cyber menaces en constante évolution » est également un peu galvaudée, mais elle correspond à une réalité : les pirates informatiques développent sans cesse de nouvelles techniques, plus efficaces et moins coûteuses. Les entreprises ne peuvent pas rivaliser si elles n'utilisent pas une méthodologie adaptée, permettant de lutter contre des stratégies d'attaques en évolution constante.

Le Threat Hunting n'est pas le seul composant dont vous avez besoin pour vous défendre efficacement contre les attaques ciblées. Il ne remplace pas l'approche de détection-réponse. Celle-ci est indispensable et doit reposer sur une équipe d'experts disposant des meilleurs outils disponibles.

Une équipe de détection et réponse doit comprendre comment procèdent les pirates informatiques, posséder le savoir-faire nécessaire en matière d'enquête et être capable de mener des mesures de réponse efficaces. Nous avons développé une méthodologie baptisée « Réponse continue » : il s'agit de procéder au Threat Hunting tout en assurant une réponse continue contre les attaques ciblées. Cette méthodologie vous est expliquée dans le chapitre 3.

Qu'est-ce que le threat hunting?

- Un processus d'amélioration continue pour élaborer des cas d'utilisation pour la détection.
- Une recherche continue sur les techniques d'attaque menée en adoptant le point de vue du pirate informatique.
- Une approche partant du postulat que le réseau informatique est déjà piraté.
- Une activité dont le succès tient à la qualité des cas d'utilisation implémentés pour la détection.
- Un composant nécessaire dans la défense contre les attaques ciblées.

3. Réponse continue

À quoi sert la détection sans réponse ?

Les attaques ciblées - de par leur nature intrinsèque - contourneront tous vos contrôles préventifs.

Il existe désormais beaucoup plus d'outils de détection qu'auparavant. L'EDR en est le principal exemple. Toutefois, la plupart des organisations souffrent encore de deux problèmes majeurs :

- **Ils manquent de professionnels compétents chargés d'enquêter sur les alertes pour déceler les activités réellement malveillantes.**
- **Ils n'ont ni la compréhension, ni le savoir-faire nécessaire pour répondre efficacement si une activité malveillante est détectée.**

Ces problèmes apparaissent clairement lorsque l'on examine les données relatives au temps de réponse aux intrusions informatiques. Le délai entre le début d'une intrusion et son confinement (également appelé cycle de vie de l'intrusion) a sensiblement augmenté entre 2018 et 2019[1].

Pourquoi existe-t-il un tel délai entre le début d'une intrusion et son confinement ?

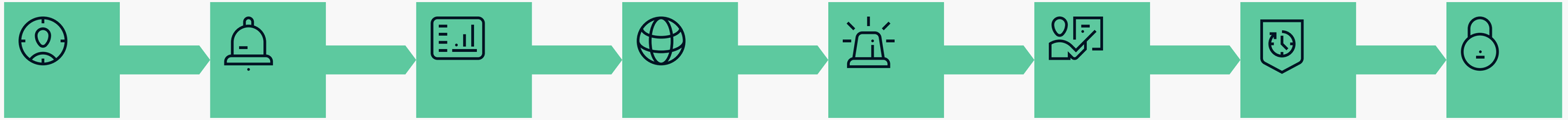
87% des attaques ciblées sont exécutées en quelques minutes[2]	« Généralement, il ne faut au hacker que quelques minutes après sa première action pour compromettre un actif. » [2]
Mais toutes ne sont pas découvertes avec la même rapidité : certaines ne sont détectées qu'après « plusieurs mois, voire davantage »[4]	« Le délai moyen pour identifier une infraction en 2019 était de 206 jours »[5]
Après la découverte d'une intrusion, la lenteur de la réponse donne aux pirates informatiques encore plus de temps pour atteindre leur objectif.	« Le délai moyen pour contenir une intrusion est de 73 jours. »[6]

Le temps nécessaire pour contenir une intrusion informatique est parfois appelé « intervalle de réponse ». Plus cet intervalle est long, plus l'impact de l'attaque est généralement important. Ce délai est, en moyenne, de 73 jours : le pirate informatique dispose donc d'un laps de temps important pour atteindre son objectif.

1. Ponemon "Cost of a Data Breach 2019"
2. Rapport 2018 de Verizon : "Data Breach Investigations Report"
3. Ibid
4. Ibid
5. Ibid
6. Ponemon "Cost of a Data Breach 2019"

Pourquoi existe-t-il un tel intervalle ?

Imaginez le scénario suivant :



Un piratage a lieu.

Peut-être parviendrez-vous à le détecter grâce à vos outils de surveillance traditionnelle... Une détection sera toutefois nettement moins probable si votre SOC n'utilise pas d'EDR.

Vous devez ensuite déterminer s'il s'agit d'une menace réelle. Comment mener l'enquête ? Disposez-vous des bonnes données ? Est-il facile et rapide de recueillir les bons indices ?

Le pirate est-il seulement là où vous l'avez détecté ou bien est-il parvenu à infecter d'autres périphérique ? Y a-t-il plus d'un pirate informatique sur le réseau ? Vous devez répondre à toutes ces questions sans que les individus malveillants ne se rendent compte qu'ils ont été détectés.

Après avoir confirmé au mieux l'existence d'une menace, vous devez faire intervenir l'équipe externe chargée de la réponse aux incidents, tout en veillant à une bonne coordination avec les équipes internes. Tout ce travail sera particulièrement difficile si aucune préparation n'est menée à l'avance.

Vous devez également rassembler toutes les informations à présenter aux membres du conseil d'administration. Il vous faudra décider qui sera chargé de les informer de la situation et de communiquer avec eux.

Une intrusion peut se produire au milieu de la nuit. Vous devez déterminer qui devra se réveiller !

Une fois déterminé l'ampleur du piratage, il faudra vous concentrer sur les mesures de confinement et sur les mesures correctives. Ces tâches seront du ressort de l'Incident Response mais il faudra à ces professionnels suffisamment de renseignements sur votre entreprise pour définir le plan de confinement et de remédiation approprié.

Tout cela prend du temps et l'impact potentiel d'une intrusion peut augmenter considérablement. Un pirate informatique motivé n'attendra pas sagement que vous prépariez votre réponse.

De quoi avez-vous besoin pour garder une longueur d'avance ? Comment mener des opérations de détection - et de réponse - assez efficaces pour minimiser l'impact des attaques ciblées ? En recourant à la réponse continue.

Les trois C de la réponse continue

La réponse continue est le terme que nous avons adopté pour définir une approche associant - au sein d'une même méthodologie - la détection et la réponse. Lorsqu'une attaque est confirmée, la réponse continue permet d'agir immédiatement pour contenir les pirates informatiques et entraver leur progression, avant même qu'un plan de remédiation ait été mis en place. Se défendre contre les cyber attaques sophistiquées exige de trouver un équilibre entre la détection et la réponse. La réponse continue consiste alors à :

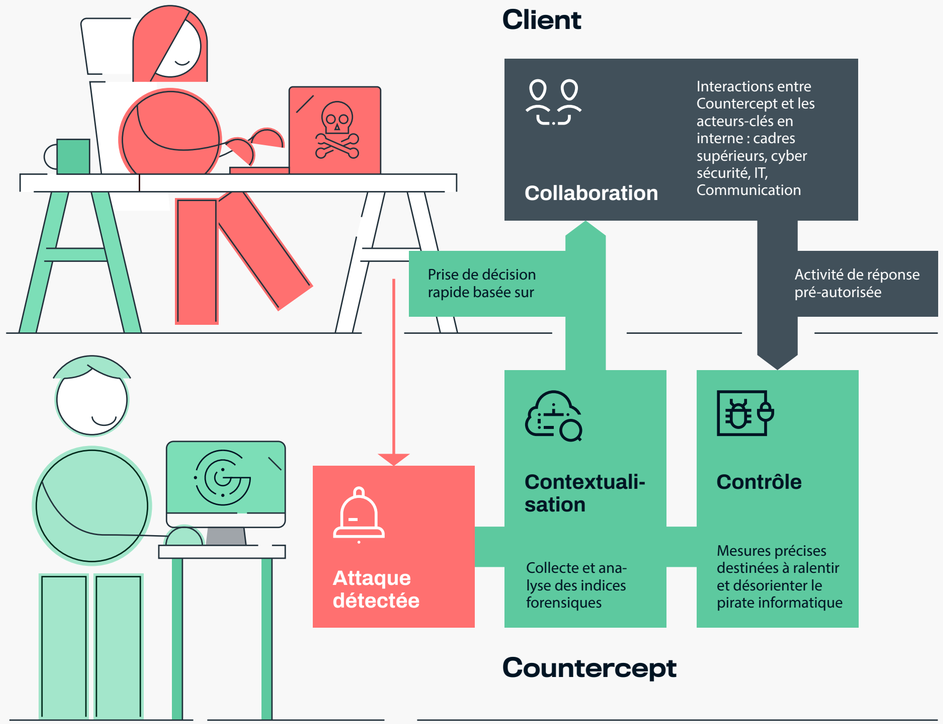
Disposer d'experts capables d'enquêter sur les activités suspectes pour déterminer s'il s'agit réellement de comportements malveillants. Ces spécialistes doivent procéder en recueillant les indices nécessaires et en les analysant. Il est essentiel de se faire une idée de l'attaque pendant que l'intrusion a lieu, et non pas après.

Contenir le pirate informatique une fois l'intrusion confirmée, jusqu'à ce qu'un plan de remédiation complet ait été élaboré et approuvé. Confiner le hacker et entraver sa progression est essentiel pour minimiser l'impact sur l'entreprise.

Exclure le pirate informatique des systèmes en supprimant ses canaux C2, en supprimant les mécanismes de persistance utilisés et en l'empêchant de s'implanter à nouveau sur le réseau.

Exclure le pirate informatique des systèmes en supprimant ses canaux C2, en supprimant les mécanismes de persistance utilisés et en l'empêchant de s'implanter à nouveau sur le réseau.

Comment la réponse continue fonctionne-t-elle ?



4. Les secrets d'un threat hunting efficace

Un Threat Hunting efficace repose sur plusieurs principes-clés : adopter le point de vue du pirate informatique, donner aux équipes le temps de réfléchir, leur donner accès aux outils et aux données dont elles ont besoin, et enfin, collaborer avec les Red Teams et les équipes de réponse aux incidents.

Adopter le point de vue du pirate informatique

Il faut penser comme un hacker. Les Blue Teams ne doivent pas seulement réagir à des techniques d'attaque déjà observées. Il leur faut anticiper. Elles doivent déterminer les opérations que le pirate est susceptible d'entreprendre et développer des capacités défensives en conséquence.

Pour penser comme un pirate informatique, il est nécessaire de disposer des éléments suivants :

Une compréhension détaillée et une bonne connaissance des techniques et des stratégies d'attaques employées par les pirates informatiques pour contourner les outils de sécurité. Les membres de notre équipe acquièrent des certifications de piratage éthique telles que l'OSCP. Ils veillent également à observer nos équipes de simulation d'attaques ciblées.

Une compréhension détaillée des mécanismes sous-jacents : il s'agit, par exemple, des rouages internes des systèmes d'exploitation. L'objectif est de savoir quelles failles peuvent être exploitées et ce qui peut être camouflé par les hackers en activité normale.

Une connaissance générale des comportements des pirates informatiques. Les techniques d'attaques sont nombreuses, variées et complexes. Il est nécessaire de développer et d'entretenir une connaissance étendue des modes opératoires utilisés par les pirates informatiques. Les modèles open source comme MITRE ATT&CK™ sont d'excellents points de départ. Il s'agit ensuite de développer ces connaissances sur la base de recherches et d'expériences propres à chaque entreprise.

Donner aux équipes le temps de réfléchir

Le Threat Hunting a créé un mode d'organisation offrant aux équipes le temps nécessaire pour réfléchir. Les opérations de détection et réponse de base et le Threat Hunting doivent être assurés par la même équipe, mais pas en même temps.

Le fait qu'une seule et même équipe mène les opérations et veille à l'amélioration des capacités de détection crée une culture de responsabilité. Si l'équipe élabore une règle de détection provoquant de nombreux faux positifs, elle devra elle-même gérer ce bruit et y remédier. L'efficacité opérationnelle des membres de l'équipe s'en trouve de facto améliorée, car ils ont une connaissance approfondie des mécanismes sous-jacents des détections.

“Le fait qu'une seule et même équipe mène les opérations et veille à l'amélioration des capacités de détection crée une culture de responsabilité.”

Le Threat Hunting consiste à rechercher des activités malveillantes qui échappent à vos contrôles de détection. Vous devez donc déterminer ce que vous pouvez déjà détecter. C'est ensuite que vous pourrez établir des priorités dans vos activités de Threat Hunting, en fonction de vos faiblesses. En fonctionnant ainsi, vous pourrez démontrer l'amélioration de vos capacités et l'efficacité de vos activités de Threat Hunting. Si votre entreprise définit la réussite sur la base des détections des menaces actives, alors il sera difficile de justifier le temps investi dans la recherche. Ce temps est pourtant essentiel. La réussite doit donc être mesurée sur la base de l'amélioration des capacités de détection et de réponse.

Le fait de consacrer du temps à la recherche et au Threat Hunting permet également de veiller à ce que les membres de l'équipe restent stimulés et donc motivés, du fait de la diversité des missions. Il est difficile de conserver le personnel chargé des opérations de sécurité. Il est donc essentiel de veiller à ce que leurs missions restent variées et intéressantes. Le seul inconvénient devient alors de trouver des professionnels possédant toutes ces compétences. Ces dernières prennent du temps à être développées. Cependant, en offrant davantage de flexibilité aux employés et en leur permettant de se former à un large éventail de compétences spécialisées, il devient possible de maintenir un niveau d'engagement élevé et d'attirer/retenir les bons candidats.

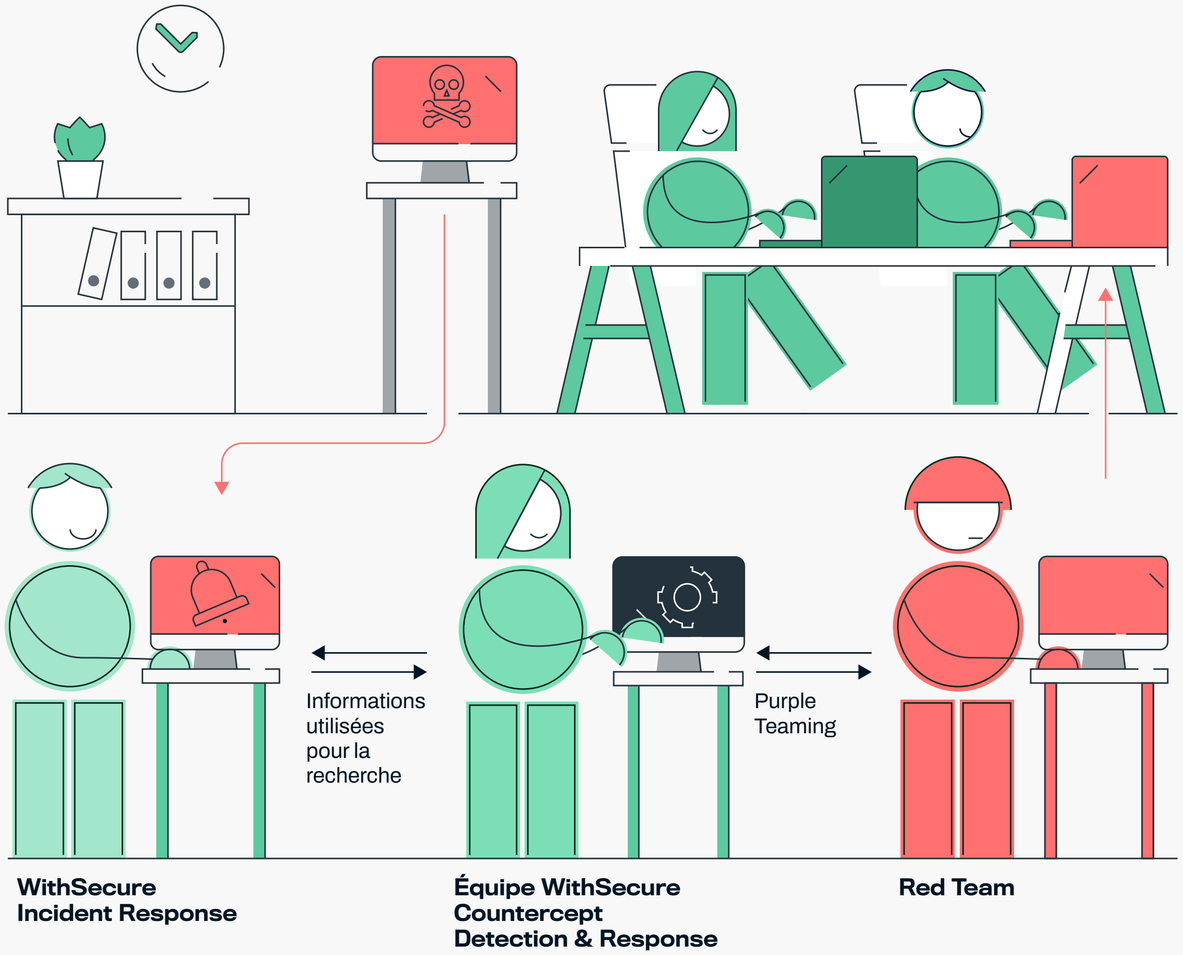
Le travail de recherche exige de larges plages horaires ininterrompues, et non des heures isolées. Chez WithSecure™ Countercept, nous structurons les emplois du temps de manière à ce que chaque membre de l'équipe dispose de temps dédié exclusivement au Threat Hunting. En dédiant 25 % du temps de l'équipe à cette activité, nous veillons à ce que nos employés puissent accorder du temps à la recherche, sans être interrompus. Pour protéger et maintenir ce temps dédié, des renforts sont disponibles pour les journées les plus chargées.

“Le fait de consacrer du temps à la recherche et au Threat Hunting permet également de veiller à ce que les membres de l'équipe restent stimulés et donc motivés, du fait de la diversité des missions.”

Collaboration avec les Red Teams et réponse aux cyber incidents

Le but du jeu : se défendre contre des attaques menées par les Red Teams. La recherche théorique ne remplacera jamais la pratique : la compétition contre les Red Teams est un excellent moyen d'apprendre et de faire des recherches. Bien que votre équipe de Threat Hunters soit déjà formée à adopter le point de vue offensif du pirate informatique, avoir le regard neuf d'une autre équipe offensive peut être d'une aide précieuse. Cela permet de couvrir les angles morts de votre approche et de tester votre équipe en dehors des conditions de laboratoire. Les Red Teams consciencieuses font, elles aussi, leurs propres recherches sur les stratégies de piratage : les Blue Teams ont donc la garantie d'être testées au regard des techniques d'attaques les plus récentes. Les exercices de Purple Team peuvent aussi s'avérer utiles.

Chaque fois qu'elles interviennent sur un cyber incident, les équipes Incident Response acquièrent des informations vitales sur les techniques des hackers. Ces informations peuvent être utilisée pour développer de nouvelles capacités de détection, y compris pendant un cyber incident. De nouvelles règles peuvent être élaborées durant le piratage, afin d'automatiser la détection des postes de travail infectés, plutôt que de devoir les trouver les uns après les autres, via l'enquête. Cette approche a déjà fait ses preuves à maintes reprises.



5. L'avenir du threat hunting

Personne ne sait vraiment ce que l'avenir nous réserve, mais les tendances et technologies émergentes nous donnent une idée de la direction que prendra le Threat Hunting et des besoins auxquels il répondra.

Que l'avenir nous réserve-t-il ?

Un changement de focus

C'est sur les endpoints que se concentrent encore aujourd'hui les attaques. Les Threat Hunters y consacrent donc la plupart de leurs efforts. Toutefois, les environnements informatiques évoluent : les entreprises délaissent les services hébergés au profit du cloud, travaillent à partir de leur navigateur et utilisent des systèmes d'exploitation modernes. Les Threat Hunters devraient tenir compte de ces évolutions dans leurs recherches car les hackers pourraient bien cibler des lacunes de détection présentes à ces niveaux.

Standardisation du terme

Dans le secteur de la cyber sécurité, la définition du terme « Threat Hunting » reste floue. Ce livre blanc détaille ce que nous entendons par ce terme, mais d'autres acteurs lui donnent une toute autre interprétation. Nous espérons qu'à l'avenir, la définition de Threat Hunting deviendra plus standard, pour mieux définir les bonnes pratiques, concevoir les meilleurs outils, et favoriser l'échange d'expériences. Une fois ce terme clarifié, les acheteurs pourront, eux aussi, mieux le comprendre et l'interpréter.

Généralisation du Threat Hunting

Pour les entreprises ayant la volonté affirmée et le budget nécessaire pour développer des capacités en interne, le Threat Hunting, tel que décrit ici, deviendra l'approche de facto destinée à améliorer les mécanismes de détection des attaques.

Cela apportera plusieurs avantages. Tout d'abord, le poste actuel d'analyste - relativement peu populaire - deviendra moins nécessaire : en effet, les Threat Hunters seront nettement plus engagés dans les opérations et les capacités globales. Le fait d'exposer les analystes actuels au Threat Hunting devrait permettre une montée en compétences (via l'exposition concrète aux menaces) et de fidéliser vos collaborateurs.recherches car les hackers pourraient bien cibler des lacunes de détection présentes à ces niveaux.

Ensuite, le Threat Hunting sera évalué du point de vue de l'amélioration des capacités de détection et non plus en se basant sur le nombre effectif de détection. Ainsi, les entreprises pourront plus facilement justifier les investissements en temps liés à cette approche. Et comme il s'agit d'un processus mieux défini, le temps sera également mieux rentabilisé.

Le Threat Hunting tel que nous le connaissons deviendra l'approche de facto par laquelle les entreprises développeront leurs capacités de détection. Elles pourront ainsi attirer et fidéliser des professionnels, ce qui contribuera à faire évoluer encore plus rapidement le domaine de la détection. Le Threat Hunting pourrait ainsi devenir l'une des disciplines les plus passionnantes et les plus efficaces de la cyber sécurité. De plus en plus de professionnels reconnaissent déjà que cette approche conduit à des améliorations tangibles du niveau de sécurité des entreprises.

Amélioration des techniques et outils, au grand dam des pirates informatiques

Les Blue Teams deviendront aussi collaboratives et réactives que les Red Teams. Ce faisant, le Threat Hunting gagnera en popularité. Les Threat Hunters deviendront plus nombreux, plus efficaces. En s'appuyant sur le processus d'amélioration continue propre à cette approche, ils développeront des techniques et des outils spécifiquement conçus pour le Threat Hunting. Les pirates informatiques seront alors contraints de battre en retraite.

Partage de la logique des règles

Aujourd'hui, les entreprises sont confrontées à un défi : recruter du personnel compétent, capable de concevoir une logique de détection sur mesure. En cyber sécurité, le partage des connaissances est courant... mais encore faut-il traduire ces échanges verbaux en règles d'automatisation cohérentes. Des projets comme Sigma cherchent à créer un cadre permettant de partager les logiques des règles, afin d'éviter que plusieurs entreprises ne créent les mêmes logiques de règles pour les mêmes attaques. Le fait d'en finir avec la redondance des règles pour les attaques génériques (attaques sur les appareils Windows, Active Directory, etc.) permettra aux équipes de Threat Hunting de se concentrer plus en aval sur la chaîne de piratage, c'est-à-dire sur des risques plus spécifiques à chaque entreprise. À une heure où les technologies endpoints se standardisent, ce type de partage de règles devraient s'imposer comme le prolongement naturel de projets de partage de connaissances déjà populaires, comme ATT&CK.

6. Conclusion

De nombreux fournisseurs ont fait du « Threat Hunting » une expression marketing à la mode. Il n'est donc pas étonnant qu'une certaine confusion règne désormais autour de ce terme. Dans Démystifier le Threat Hunting, nous avons abordé les principaux mythes et idées erronées qui entourent le Threat Hunting. Nous avons également expliqué ce qu'est réellement cette approche. Nous en avons fourni une définition claire : le Threat Hunting est le processus consistant à identifier les lacunes de vos méthodes de détection, pour ensuite développer des cas d'utilisation capables de combler ces lacunes, avant qu'un pirate informatique ne puisse les exploiter.

Nous avons également étudié la réponse continue, terme que nous avons choisi pour définir notre approche associant détection et réponse au sein d'une seule méthodologie, pour contenir et contrecarrer les attaques dès qu'elles se produisent. Nous avons expliqué que la réponse continue est une discipline en constante évolution et en constante amélioration, et que le Threat Hunting est un élément-clé de ce processus : il garantit que nos capacités de détection et de réponse restent optimales, pour détecter et répondre aux attaques ciblées.

Nous avons passé en revue les éléments d'un Threat Hunting efficace, notamment la nécessité de cultiver un état d'esprit offensif, et de collaborer avec les Red Teams et les équipes Incident Response. Nous avons également insisté sur la nécessité de donner aux Threat Hunters du temps à consacrer à la recherche, tout en leur fournissant les bons outils et les bonnes données, sur le modèle de l'approche de WithSecure™.

Enfin, nous avons partagé nos réflexions, observations et prévisions sur l'avenir du Threat Hunting, et nous vous avons donné un aperçu des tendances qui se dessinent en la matière.

Pour un point de vue nouveau sur notre secteur : suivez-nous sur Twitter

Retrouvez plus d'informations sur notre solution WithSecure™ Countercept sur cette page dédiée.

À Propos de WithSecure™

WithSecure™ est le partenaire européen de reference en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnements cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

WITH secure