riverbed®

Guide de la chasse aux cybermenaces

L'art de détecter les menaces de sécurité avancées de manière proactive

Sommaire

SUNBURST : Quelles leçons en avons-nous tirées ?

S'il ne fallait retenir qu'une chose de l'attaque SUNBURST, c'est que nos stratégies de sécurité doivent être plus proactives pour contrer les menaces avancées modernes. Les équipes responsables de la sécurité ne peuvent plus se reposer exclusivement sur des mesures préventives passives ou se contenter de réagir à des situations d'urgence, en répondant à des alertes laissant entrevoir des indicateurs potentiels de compromission. Les méthodes des cybercriminels d'aujourd'hui sont particulièrement sophistiquées. Ces derniers imaginent constamment de nouvelles attaques qui peuvent rapidement échapper aux défenses classiques. Nombre d'entre eux ne sont même pas des criminels au sens propre, ce sont des agents qui travaillent pour un État-nation. Le temps que votre équipe de sécurité découvre une violation, délai qui se compte souvent en mois, des données confidentielles ont été exfiltrées et déplacées latéralement dans le réseau. Le coût d'une violation se chiffre généralement en millions, sans compter les dégâts causés à votre marque.

La détection de ces menaces capables de traverser vos défenses implique que votre organisation chasse les cybermenaces régulièrement et de manière proactive. Pour que son efficacité soit optimale, la chasse aux menaces ne doit pas être une « campagne » ponctuelle. Elle doit être cohérente et faire partie intégrante de votre stratégie de cybersécurité pour la protection de vos actifs digitaux.

Les violations qui ont fait l'actualité en 2020

- **SUNBURST via SolarWinds** : conséquences toujours en cours d'examen
- **Twitter** : 100 000 USD en bitcoins
- **MGM Resorts** : 10,6 millions de comptes clients
- **Marriott (2020)** : 5,2 millions de comptes clients*
- **Estée Lauder** : 440 millions de dossiers clients
- **Microsoft** : 280 millions de dossiers clients
- **Zoom** : 500 000 comptes clients
- **Magellan Health** : 365 000 dossiers patients

* Marriott subit deux attaques en deux ans.

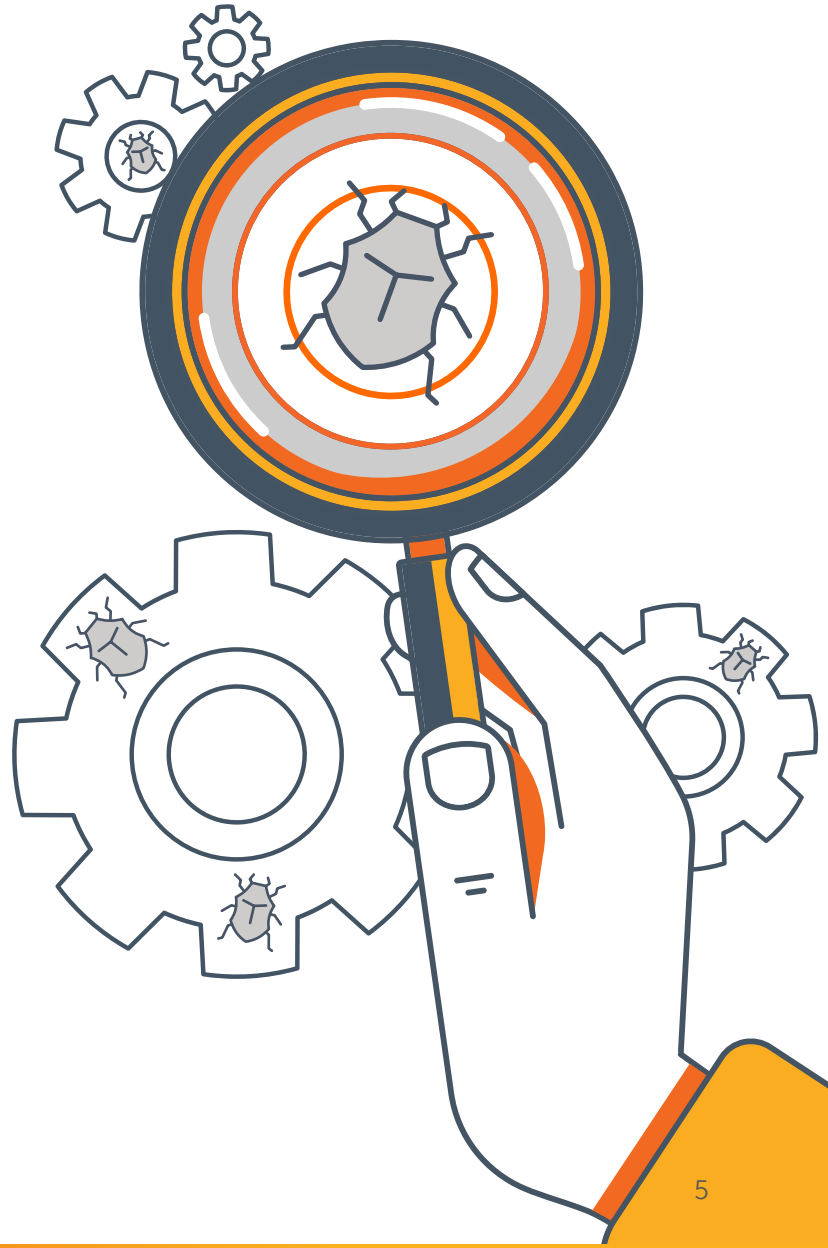
Qu’est-ce que la chasse aux cybermenaces ?

La plupart des menaces auxquelles les analystes de sécurité sont confrontés sont relativement peu sophistiquées et peuvent être facilement détectées et atténuées à l’aide d’outils standard et de bonnes pratiques sécuritaires. Cependant, un pourcentage limité mais en forte croissance d’entre elles sont des menaces avancées capables de traverser vos défenses et se propager au sein de votre réseau. Une fois infiltré dans votre réseau, un pirate peut y rester embusqué pendant des mois et collecter tranquillement des données, rechercher des documents confidentiels ou se procurer les identifiants de connexion qui lui permettront de se déplacer latéralement dans l’environnement.

C’est là qu’intervient le chasseur de cybermenaces.

La chasse aux cybermenaces consiste à rechercher, suivre et neutraliser de manière proactive et itérative les intrus les plus habiles et les plus dangereux sur votre réseau. Ce processus centré sur l’analyste part généralement d’une hypothèse ou d’un élément déclencheur et lance une recherche proactive et itérative sur le réseau, les terminaux et les données afin de détecter et d’isoler les menaces qui ont échappé aux contrôles préventifs classiques.

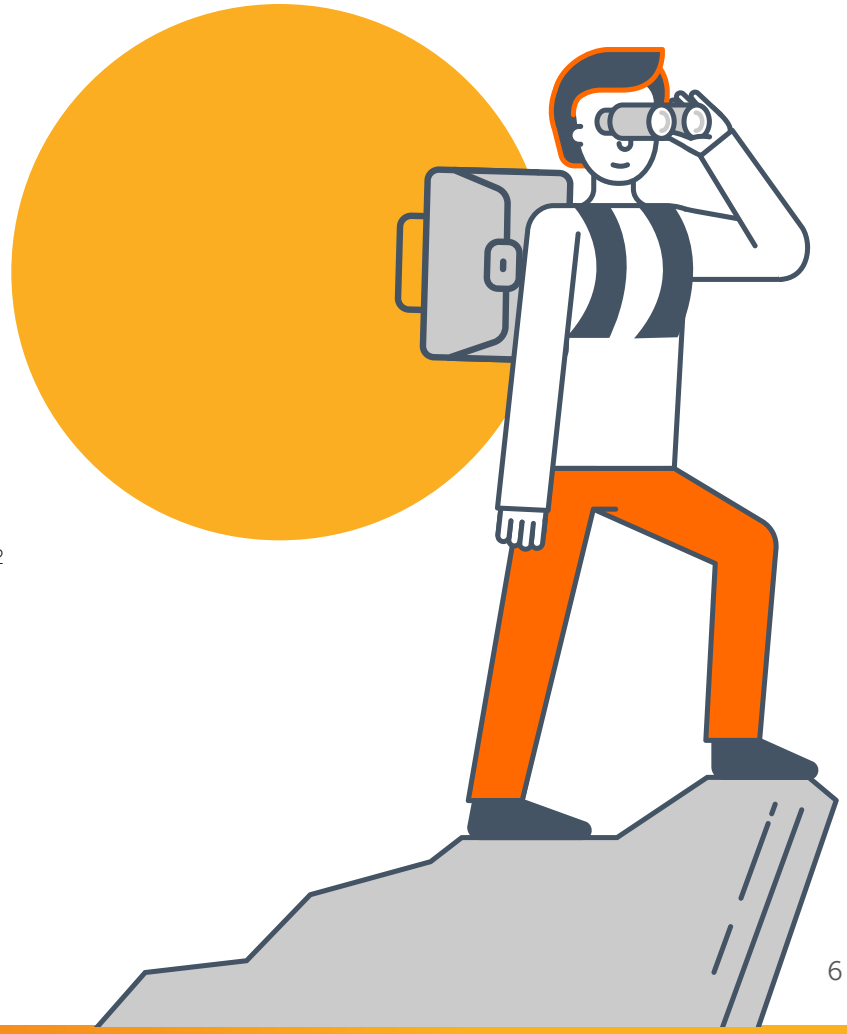
Contrairement aux analystes de sécurité qui attendent que le système de détection des intrusions ou de gestion des informations et des événements de sécurité (SIEM) émette des alertes pour y réagir, la chasse aux menaces leur permet d’être proactifs et d’identifier les menaces plus tôt. Le processus de chasse aux menaces permet également de détecter les vulnérabilités et d’atténuer les risques connexes avant qu’ils n’affectent votre organisation.



Les six bonnes raisons pour votre organisation de faire la chasse aux cybermenaces

Le constat est simple : plus le délai d'identification d'une violation est long, plus le coût est élevé.

1. Temps moyen pour identifier et maîtriser une violation : 280 jours, soit 207 jours pour l'identifier et 73 jours pour la contenir.[1]
2. Coût total moyen d'une violation : 3,86 millions USD.[1]
3. 67 % de l'ensemble de violations résultent de trois types d'attaques : vols d'identifiants de connexion, erreurs et attaques sociales.[2]
4. 70 % des violations sont causées par des personnes extérieures.[2]
5. 86 % des violations sont encore motivées par des raisons financières.[2]
6. Dans 58 % des violations, les données personnelles sont visées, soit près du double par rapport aux chiffres de 2019.[2]



[1] Ponemon, The Cost of a Breach, 2020

[2] Verizon, Data Breach Investigations Report, 2020

Les prérequis de la chasse aux menaces

L'objectif de la chasse aux menaces est d'utiliser le détecteur d'anomalies le plus puissant du monde, c'est-à-dire le cerveau humain, pour débusquer les menaces non découvertes. Cependant, pour réussir, la chasse aux menaces doit être soutenue par un programme de sécurité avancé accompagné d'une visibilité élargie, y compris :

Une visibilité réseau élargie

Une parfaite connaissance de votre réseau et de votre infrastructure est essentielle à la chasse aux menaces. En outre, l'établissement de références de base de l'activité normale du réseau peut aider à identifier toute activité malveillante et fournir un contexte initial pour ouvrir la chasse.

Un personnel qualifié et dédié

Les chasseurs de menaces doivent savoir comment utiliser leurs outils de sécurité et de visibilité réseau et comprendre la façon de penser de leurs adversaires. En bref, pour attraper un pirate, vous devez penser comme un pirate. Les chasseurs de menaces qui effectuent des traques régulières et structurées avec des objectifs clairement définis seront plus efficaces.

Renseignements enrichis sur les menaces

Une connaissance des nouveaux vecteurs de menace permettra aux chasseurs de se tenir au fait des dernières techniques. L'utilisation d'indicateurs publics de compromission tels que les signatures des programmes malveillants, les adresses IP et autres peut contribuer à améliorer la détection de nouvelles menaces.

Analyse scientifique de la sécurité

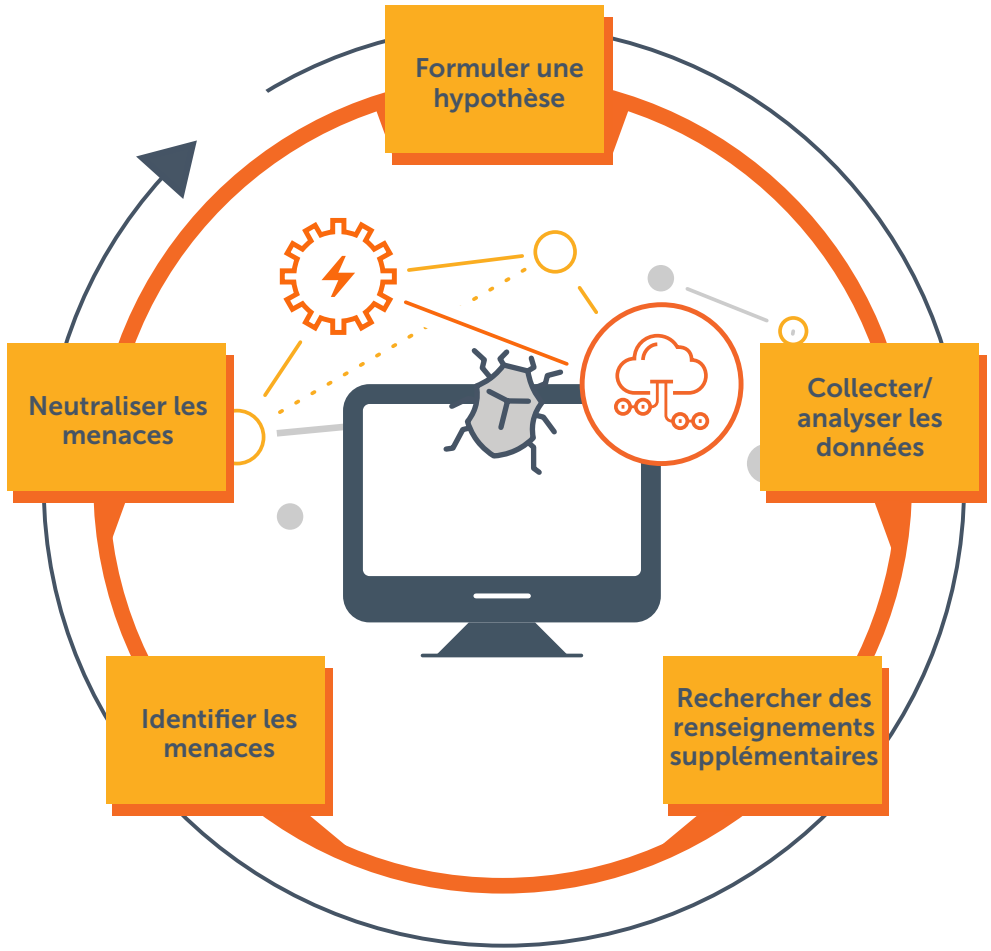
Une fois la menace identifiée, si les circonstances le permettent, vous prenez le temps de capturer la preuve de manière scientifique et précise afin qu'elle soit acceptée dans une procédure judiciaire.

Un chasseur sachant chasser...

Une chasse aux menaces efficace est un processus itératif qu'il faut réexaminer et ajuster régulièrement. Les chasseurs de menaces doivent penser comme leurs adversaires et accumuler des connaissances sur les emplacements où chasser sur le réseau en fonction des tactiques, techniques et procédures reconnues. Ils doivent également anticiper les emplacements où les attaques sont les plus probables et les cibles qui présentent un risque d'attaque plus élevé.

Comprendre ce que font les pirates et où ils sont susceptibles de frapper fournit la structure nécessaire à la chasse aux menaces, qui ne se limite pas à se fier à des intuitions ou à résoudre des problèmes après qu'ils se sont produits.

Le processus de chasse aux menaces



Outils courants de chasse aux menaces

Il existe une variété d'outils qui peuvent être utilisés pour la chasse aux menaces. Utiliser plusieurs outils différents offre des perspectives distinctes sur les données. Cependant, il vous faudra intégrer ces données dans des vues de tableau de bord communes afin d'obtenir des renseignements unifiés pour l'ensemble de vos domaines de sécurité. Voici quelques outils à envisager :

- **La surveillance de flux haute fidélité** pour les rapports sur le trafic réseau avec le mappage des ports et le mappage des dépendances. L'avantage d'une surveillance de flux non échantillonnée est la scrutation omniprésente dans l'ensemble de l'entreprise hybride. Cette large couverture garantit une visibilité dans tous les recoins du réseau. Accompagnée de la conservation des données à long terme, c'est ce que les chasseurs de menaces recherchent dans une solution de sécurité. L'échantillonnage, qui consiste à prendre des instantanés ponctuels du trafic réseau, ne fournit tout simplement pas un ensemble complet de données et ne peut donc pas offrir les mêmes bénéfices. Pour assurer la sécurité en permanence, une visibilité totale et permanente est nécessaire.
- **La capture et l'analyse des paquets** avec inspection des paquets en profondeur (DPI) identifie les détails du protocole et les URL et offre un stockage très important de paquets à l'analyse scientifique. Les paquets fournissent des détails qui permettent d'enquêter avec précision sur ce qui se passe au niveau des données (p. ex., quelles données ont été volées lors d'une attaque avec exfiltration).
- **La surveillance de l'infrastructure** fournit des détails sur la gestion des changements et détecte toute activité inhabituelle sur les équipements réseau, comme la saturation d'une interface par une attaque. Selon le cabinet d'analyse EMA, l'infrastructure réseau est l'origine la plus fréquente des incidents de sécurité.
- **La détection des terminaux** surveille les ordinateurs de bureau, les serveurs, les ordinateurs portables, les tablettes, les smartphones et même les équipements IoT pour détecter et examiner les activités suspectes.
- **L'analyse des journaux** permet d'extraire des données des fichiers journaux pour analyser les tendances et les modèles. Cependant, la première chose qu'un attaquant fait une fois qu'il est entré dans votre réseau est de désactiver la journalisation. C'est donc pour cette raison qu'il est évident que vous devez toujours compléter la journalisation par une ou plusieurs sources alternatives.
- **La détection des anomalies** reconnaît les changements au niveau du volume et de la vitesse du trafic entre les adresses IP. La détection des anomalies peut être intégrée à vos solutions de visibilité ou de sécurité ou constituer une offre distincte pour les équipes d'AIOps.

Conclusion

La chasse aux menaces n'est pas la panacée, et les équipes de sécurité doivent continuer à appliquer les principes fondamentaux de la sécurité. Les organisations qui détiennent de précieuses données continueront à être confrontées à des menaces sophistiquées. Il y aura toujours des individus dont le seul but est d'infiltrer votre réseau sans déclencher d'alertes. La chasse aux menaces est le seul moyen de détecter systématiquement ces menaces avancées.

Grâce à une capture permanente de haute fidélité, la solution de surveillance des performances réseau unifiée de Riverbed vous permet de détecter et de résoudre les problèmes de performances et les menaces de sécurité jusqu'à 90 % plus rapidement. L'identification et la résolution des problèmes réseau commencent toujours par la visibilité. L'adage est plus vrai aujourd'hui que jamais : ce qui ne se mesure pas ne peut être géré. Son corollaire est également vrai : ce que l'on ne peut pas voir ne peut être sécurisé. Tout angle mort ne demande qu'à être exploité.

En matière de visibilité réseau, la lutte contre les menaces de sécurité doit s'appuyer sur une stratégie incluant tous les points ci-dessus. Cela inclut la capacité de capturer chaque paquet, chaque flux et chaque metric des équipements, partout.

Le troisième élément est la capacité de compiler et d'appliquer des analyses pour en tirer des renseignements significatifs et exploitables. Comprendre ce qui constitue des modèles de trafic normaux, détecter les anomalies, identifier avec précision les corrélations par rapport aux causes, pouvoir répondre rapidement aux problèmes de performance et aux menaces de cybersécurité et en atténuer les effets : tout dépend de votre capacité à voir et à analyser ce qui se passe sur votre réseau distribué, que ce soit sur site, d'une manière virtuelle ou dans le cloud.

Pour en savoir plus sur l'utilisation de la solution de gestion des performances réseau unifiée de Riverbed pour la chasse aux menaces, **cliquez ici.**