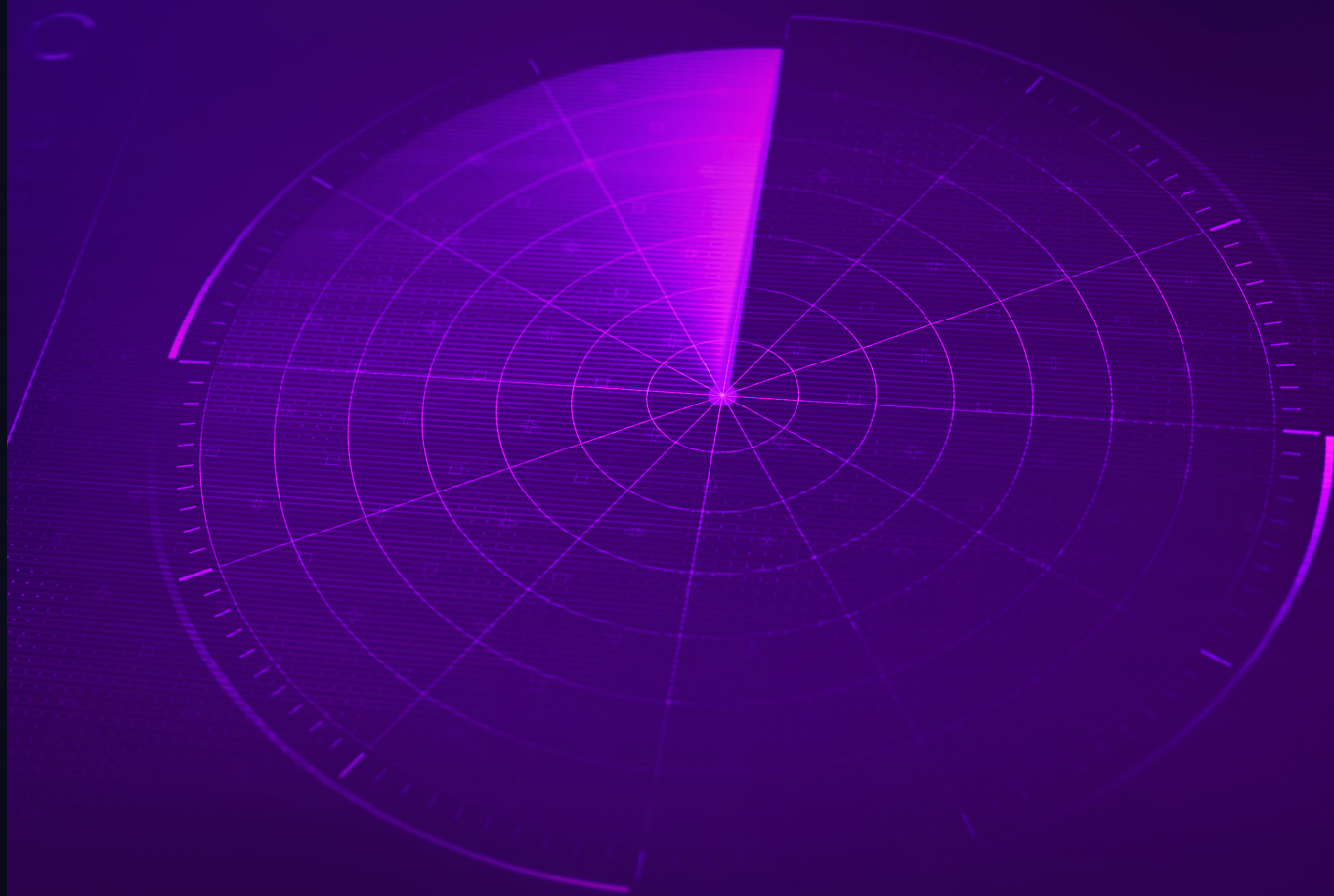




Les six étapes d'une **chasse aux menaces** efficace



Sommaire

Introduction	3
Qu'est-ce que la chasse aux menaces ?	4
Quel est l'intérêt de la chasse aux menaces ?	5
Six étapes pour créer un programme de chasse aux menaces efficace	6
Conclusion	12



38 % de menaces non détectées

Selon un rapport publié par Cybersecurity Insider, 38 % des menaces émergentes avancées échappent aux outils de sécurité traditionnels.

La cybersécurité ressemble souvent au jeu du chat et de la souris. À peine nos solutions améliorent-elles leur capacité de neutralisation d'un type d'attaque que les cybercriminels ont souvent déjà développé et commencé à utiliser de nouvelles tactiques et techniques. Selon le rapport d'enquête sur les compromissions de données de Verizon, les menaces avancées rôdent souvent pendant plusieurs mois dans nos environnements sans être détectées, recherchant discrètement des informations précieuses à voler ou des données à compromettre. Si vous attendez que leurs activités les révèlent ou qu'une alerte soit générée par les outils de surveillance traditionnels du SOC, il est souvent trop tard.

La chasse aux menaces peut aider l'entreprise à relever ces nombreux défis. Au lieu d'attendre une alerte, les chasseurs de menaces partent du principe qu'une menace avancée sévit au sein du réseau et s'efforcent de l'identifier. Ce livre blanc consacré à la chasse aux menaces explique pourquoi elle est indispensable et comment la plateforme SentinelOne permet à votre équipe d'adopter des stratégies de chasse efficaces.

Qu'est-ce que la chasse aux menaces ?

La chasse aux menaces consiste à analyser les réseaux et les endpoints en profondeur pour identifier les menaces qui échappent aux contrôles de sécurité avant qu'elles ne puissent exécuter une attaque ou atteindre leurs objectifs. Plutôt que de s'en remettre simplement aux solutions de sécurité, la chasse aux menaces est une approche proactive permettant de détecter les menaces dissimulées dans votre réseau.



La chasse aux menaces est considérée comme une « intervention sur incident de sécurité informatique avant qu'il ne se déclare » ; d'autres la définissent comme la « détection des menaces à l'aide de solutions d'intervention sur incident » ou encore la « vérification d'hypothèses de sécurité dans un environnement informatique de production ».

Contrairement aux équipes SOC et d'intervention sur incident, les chasseurs de menaces ne se contentent pas de réagir aux menaces identifiées, mais les recherchent activement. Cette approche consiste à formuler des hypothèses sur l'existence de menaces potentielles, qui sont ensuite soit confirmées soit démenties sur la base des données collectées et de leur analyse. La chasse aux menaces est également une démarche très différente de l'intervention sur incident ou de l'investigation numérique. Dans ces deux dernières disciplines, l'objectif est de déterminer ce qui s'est passé après la découverte d'une compromission. Lors de la chasse aux menaces, en revanche, l'équipe a pour objectif de rechercher les attaques susceptibles d'avoir déjà franchi vos différents niveaux de protection. La chasse aux menaces se distingue également des tests d'intrusion et de l'évaluation des vulnérabilités qui tentent de simuler une attaque et de déterminer ce qui pourrait se produire si un individu compromettait la sécurité de l'entreprise. En revanche, les chasseurs de menaces partent du principe qu'un cyberpirate s'est déjà introduit dans le réseau et recherchent ensuite des indicateurs de compromission, de déplacement latéral ou d'autres artefacts révélateurs susceptibles de fournir des preuves de la présence du cyberpirate.

Quel est l'intérêt de la chasse aux menaces ?



191 jours

En moyenne, les cybercriminels passent 191 jours à l'intérieur d'un réseau avant d'être découverts, durée plus que suffisante pour causer des dommages.

En d'autres termes, si aucune recherche proactive n'est menée sur les cybercriminels, vous risquez de ne jamais les découvrir. Que se passerait-il si un hacker bloquait votre accès aux systèmes avant que vous ne vous rendiez compte qu'une attaque est en cours ? Avec un programme de chasse aux menaces efficace, vous n'avez pas à vous inquiéter de cette éventualité.

La chasse aux menaces est une activité itérative, adaptative et systématique pilotée par l'homme. Elle limite efficacement les dommages et diminue le risque global d'une entreprise, car sa nature proactive permet aux professionnels de la sécurité de réagir aux incidents plus rapidement. Elle réduit la probabilité qu'une attaque provoque des dommages dans une entreprise, sur ses systèmes et ses données. La chasse aux menaces limite également votre dépendance vis-à-vis des prestataires extérieurs, généralement moins familiarisés, que votre équipe de sécurité, au comportement habituel de vos collaborateurs et aux spécificités de votre réseau. Enfin, cette approche vous obligera à acquérir une connaissance approfondie de vos réseaux, systèmes, applications et utilisateurs. La compréhension de tous ces composants constitue un élément essentiel d'un dispositif de sécurité robuste.

Six étapes pour créer un programme de chasse aux menaces efficace

Dès lors, comment créer le programme parfait de chasse aux menaces ? En réalité, dans ce domaine, la perfection n'existe pas. Votre programme de chasse aux menaces doit être une combinaison itérative de processus, d'outils et de techniques évoluant constamment pour s'adapter aux besoins de l'entreprise. Voici six étapes qui vous aideront à créer un programme de chasse aux menaces efficace au sein de votre entreprise.

1. Assurez-vous de collecter des données pertinentes.

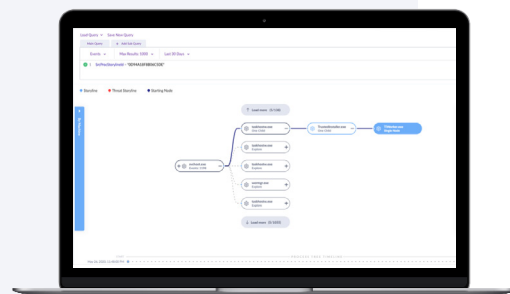
La chasse aux menaces est impossible sans données. C'est aussi simple que cela. Le succès d'une campagne de chasse aux menaces commence obligatoirement par la collecte de données pertinentes permettant de répondre aux bonnes questions. Sans les données appropriées, vous ne serez pas en mesure de mener une chasse aux menaces efficace. Les données télémétriques qui capturent, sur des systèmes d'exploitation multiples, un large éventail d'activités et de comportements, peuvent servir de base au dispositif. Les données collectées doivent notamment inclure les modèles de trafic réseau, les hachages de fichiers, les processus, l'activité des utilisateurs et du réseau, les opérations sur les fichiers, les activités persistantes, les journaux système et d'événements, les connexions refusées ou encore l'activité des équipements périphériques.

Mais les données brutes ne suffisent pas : vous devez également vous assurer que vous disposez du contexte dans lequel elles s'inscrivent. En effet, il est essentiel de savoir quelles données combiner, corrélérer ou étendre. Idéalement, vous utiliserez des outils offrant une vue d'ensemble claire de toutes les données, dotés de fonctionnalités puissantes capables de contextualiser et corrélérer automatiquement les différents événements de façon à unifier la détection et réduire au minimum l'analyse manuel de fichiers journaux bruts.



La technologie Storyline™ brevetée de SentinelOne fournit aux analystes une corrélation et un contexte en temps réel directement exploitables, et permet aux analystes en sécurité de comprendre exactement ce qui s'est passé dans votre environnement.

Chaque agent SentinelOne autonome crée un modèle de l'infrastructure de son endpoint et de son comportement d'exécution en temps réel. Chaque élément d'une histoire d'incident a la même analyse Storyline. Vous bénéficiez ainsi d'une vue complète sur ce qui s'est passé au niveau d'un équipement et de ce qui l'a provoqué. SentinelOne met automatiquement en corrélation les activités connexes dans des alertes unifiées qui fournissent des informations sur la campagne. Cela permet de réduire le tri manuel, le déficit d'attention lié à un nombre d'alertes trop élevé, ainsi que les compétences nécessaires pour répondre aux alertes.



2. **Dressez un profil de référence afin de savoir ce qui est la "norme"**

Les chasseurs de menaces doivent avoir une bonne compréhension du profil de l'entreprise et des activités métier susceptibles d'attirer les cybercriminels, telles que le recrutement de nouveaux collaborateurs, l'acquisition de nouvelles ressources ou entreprises. En résumé, il faut établir un profil de référence "normal" afin de repérer les anomalies. Les cybercriminels tentent souvent de se fondre dans la masse des utilisateurs ordinaires pour obtenir leurs identifiants au travers de campagnes de phishing. Il est donc utile de connaître et comprendre le comportement habituel d'un utilisateur pour repérer des accès anormaux aux fichiers ou connexions. En identifiant les données d'entreprise présentant de la valeur pour les cybercriminels ainsi que leur emplacement, puis en combinant ces informations aux données comportementales, il devient possible de créer des hypothèses telles que : « Un cybercriminel essaie-t-il de voler des données situées à tel endroit ? » Cette hypothèse pourra alors entraîner la collecte de données répondant à des questions comme : « Quels utilisateurs ont accédé à cet emplacement pour la première fois au cours des X derniers jours ? »

3. **Développez une hypothèse.**

De nombreuses chasses aux menaces partent d'une source de renseignements utilisant des indicateurs de compromission (IoC), des valeurs de hachage, des adresses IP, des noms de domaine ou des artefacts de réseau ou d'hôte fournis par des sources de données tierces telles que l'ISAC (Information Sharing and Analysis Center) ou le FBI. La chasse aux menaces peut également être motivée par les incidents : pour chaque incident, vous devez déterminer comment et quand il s'est produit. Cependant, toutes les menaces ne sont pas connues. En fait, un grand nombre sont inconnues ; par conséquent la chasse aux menaces ne peut pas uniquement reposer sur l'utilisation de méthodes connues.

Dans un workflow basé sur les hypothèses, une chasse aux menaces commence par l'élaboration d'une hypothèse, ou d'une supposition éclairée, sur un type d'activité susceptible d'être en cours dans votre environnement. L'utilisation d'outils OSINT (Open Source Intelligence) et de cadres de travail tels que le framework MITRE ATT&CK est efficace si vous savez ce que vous recherchez. Cela nous amène à l'une des phases essentielles de la chasse aux menaces : la formation et la vérification d'hypothèses. Les hypothèses sont généralement formulées par les chasseurs de menaces à l'aide d'outils et de cadres de travail, de données sociales, d'informations de cyberveille sur les menaces et expériences passées. Voici quelques exemples de questions d'ordre général : « Si je voulais attaquer cet environnement, comment m'y prendrais-je ? À quoi est-ce que j'essaierais d'avoir accès ? Quelles seraient mes cibles ? » Il peut également s'agir de questions plus précises : « Pourquoi y a-t-il du trafic HTTPS et FTP chiffré vers les pays de l'Est dans mon environnement » ou « Pourquoi y a-t-il un volume anormal de requêtes DNS provenant d'une seule machine ? » Les sources suivantes peuvent vous servir d'inspiration :

- **Framework MITRE ATT&CK**

Vaste base de connaissances des tactiques, techniques et procédures d'attaque. L'étude des techniques MITRE et leur simulation dans des environnements de test peuvent servir de base à l'élaboration d'hypothèses.

- **Rapports de cyberveille**

Ils contiennent des précieuses informations sur les techniques et procédures d'attaque mises en œuvre dans le cadre d'incidents réels. L'analyse systématique de ces rapports ne manquera pas de susciter la réflexion et faire jaillir de nombreuses idées de chasse aux menaces.

- **Blogs, Twitter et conférences**

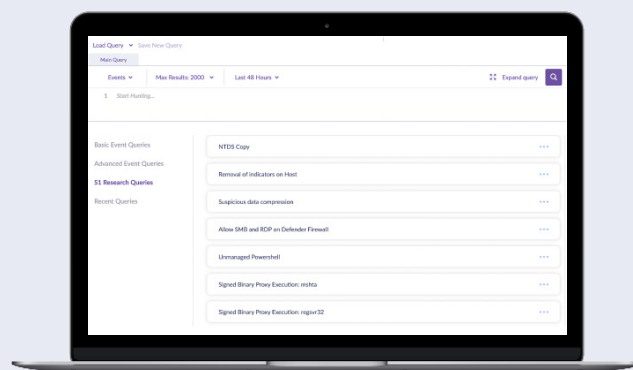
Les informations sur les nouvelles techniques d'attaque apparaissent pour la première fois sur des blogs de recherche et dans le cadre de conférences, parfois même avant que les cybercriminels ne commencent à les utiliser activement. L'étude régulière de ces informations permettra aux chasseurs de menaces de se montrer proactifs et de se préparer avant que la nouvelle technique d'attaque ne se généralise.

- **Tests d'intrusion**

Les cybercriminels ont tendance à utiliser des outils similaires à ceux utilisés par les spécialistes en tests d'intrusion. Par conséquent, l'étude des pratiques de cette discipline livre une mine de connaissances extrêmement utiles pour la formulation d'hypothèses de chasse aux menaces.



Le système Deep Visibility™ breveté de SentinelOne vous permet d'interroger et de faire pivoter rapidement et de manière itérative les données télémétriques capturées sur les différents endpoints afin de valider des hypothèses. SentinelOne met automatiquement en corrélation tous les objets liés à une menace (processus, fichiers, threads, événements et autres). Par exemple, un processus modifie un autre processus en injectant du code. Lorsque vous exécutez une requête, toutes les interactions entre le processus source, le processus cible et le processus parent sont corrélées. Cela vous permet de comprendre rapidement les relations entre les données : la cause première d'une menace ainsi que son contexte, ses relations et ses activités. Les analystes peuvent également s'appuyer sur les données historiques pour cartographier les campagnes de menaces avancées dans le temps afin de favoriser une génération d'hypothèses efficace.

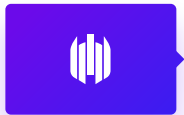


Vous pouvez en outre créer des requêtes de chasse aux menaces puissantes à l'aide de raccourcis. Dans le cadre de vos activités de chasse des menaces, le framework MITRE ATT&CK est probablement devenu l'un de vos outils de prédilection. SentinelOne facilite et accélère la chasse aux tactiques, techniques et procédures MITRE ATT&CK. Il suffit d'entrer l'ID de la technique MITRE et de l'utiliser pour effectuer une chasse.

SentinelOne fournit une bibliothèque de recherche dédiée, alimentée par les données provenant de diverses sources ouvertes, commerciales et personnalisées sélectionnées par les chercheurs de SentinelOne. Ces chasses aux menaces sont le résultat d'hypothèses génériques vérifiées par des données de recherche. Par exemple, l'utilisation d'une instance PowerShell non gérée et non signée est probablement anormale dans la plupart des environnements et nécessitera généralement une investigation supplémentaire. Les deux exemples ci-dessus ne sont pas malveillants en soi, mais s'inscrivent dans un processus de chasse aux menaces dans la mesure où ils décrivent des anomalies.

4. Recherchez et analysez les menaces potentielles.

Une fois une hypothèse formulée, l'étape suivante consiste à faire appel à divers outils et techniques pour découvrir de nouveaux modèles malveillants dans les données et d'identifier les tactiques, techniques et procédures du cybercriminel. Si l'hypothèse est avérée et que des preuves d'une activité malveillante sont trouvées, le chasseur de menaces doit immédiatement déterminer la nature, l'étendue, l'impact et la portée de la découverte.



Bien que la chasse aux menaces commence par une hypothèse générée par un humain, les solutions de protection contre les menaces, tels que SentinelOne, accroissent l'efficacité de l'investigation.

Le système Deep Visibility de SentinelOne accélère la chasse aux menaces grâce à la fonctionnalité Storyline. Chaque agent SentinelOne autonome surveille l'activité du endpoint et le comportement d'exécution en temps réel. Un ID Storyline est un ID attribué à un groupe d'événements connexes dans ce modèle. Lorsque vous constatez un événement anormal qui vous semble pertinent, utilisez l'ID Storyline pour identifier rapidement tous les processus, fichiers, threads, événements et autres données connexes en une seule requête. Associé à Storyline, Deep Visibility renvoie des données contextualisées complètes qui vous permettent de comprendre rapidement la cause d'une menace, en révélant son contexte, ses relations et ses activités en une seule recherche. Storyline permet aux chasseurs de menaces de comprendre exactement ce qui s'est passé sur un endpoint et de voir la chaîne complète des événements, faisant ainsi gagner un temps précieux à vos équipes de sécurité.

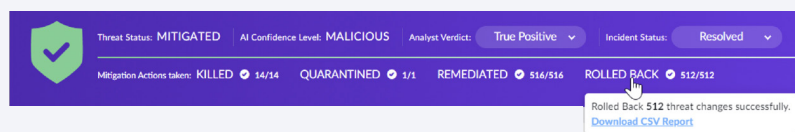
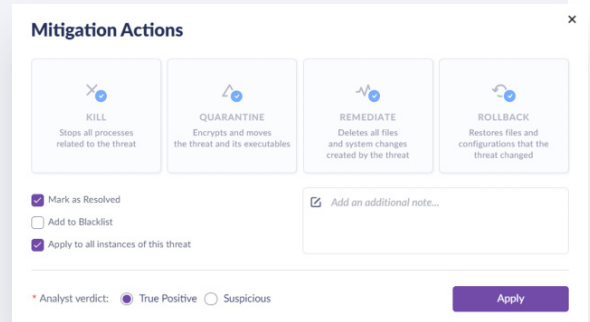
5. Intervenez rapidement pour neutraliser les menaces.

Lorsque vous découvrez un nouveau mode opératoire, vous devez vous assurer que vous pouvez réagir efficacement pour neutraliser la menace. L'intervention doit définir spécifiquement les mesures à court et long terme qui seront mises en œuvre. Le principal objectif est de mettre immédiatement fin à l'attaque en cours afin d'éviter que le système ne soit endommagé. Il est tout aussi essentiel de déterminer la cause essentielle de comprendre la cause de la menace pour améliorer la sécurité et prévenir des attaques similaires à l'avenir.

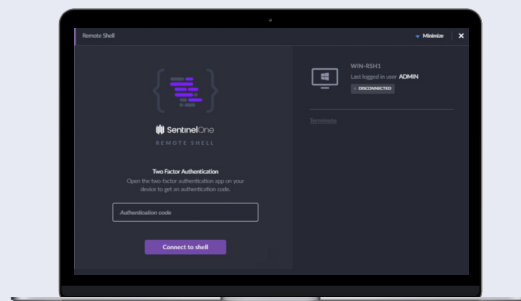


SentinelOne permet aux analystes de prendre toutes les mesures nécessaires pour neutraliser la menace en un clic. Une seule action suffit à l'analyste pour restaurer la machine ou exécuter n'importe quelle autre mesure d'atténuation disponible.

La menace peut être ajoutée aux exclusions et considérée comme résolue, et l'analyste a la possibilité de faire des commentaires pour expliquer le raisonnement et les décisions prises. SentinelOne offre également des fonctionnalités complètes de shell distant



pour donner à votre équipe de sécurité un moyen rapide d'enquêter sur les attaques, de collecter des données analysées et de corriger les failles, quel que soit l'endroit où se trouvent les endpoints compromis. Cela permet d'éliminer l'incertitude et de réduire considérablement les temps d'arrêt qui résultent d'une attaque.



SentinelOne peut également détecter les menaces à l'avance grâce à ses fonctionnalités d'apprentissage automatique et d'automatisation intelligente. Il peut anticiper les menaces et les attaques en scrutant les fichiers, documents, e-mails, identifiants, navigateurs, charges actives et le stockage mémoire. Il peut automatiquement déconnecter un équipement d'un réseau lorsqu'il identifie une menace ou attaque potentielle.

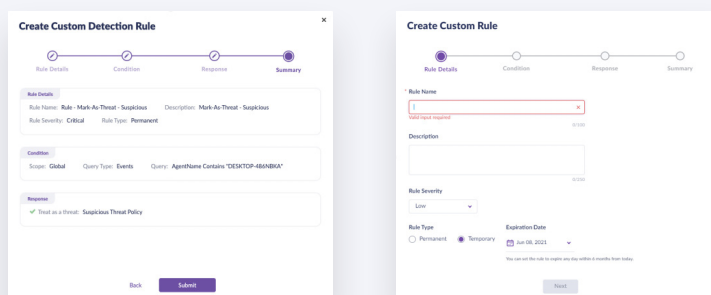
6.

Enrichissez et automatisez vos processus pour faire face aux événements à venir.

Enfin, les chasses aux menaces fructueuses offrent une source précieuse d'informations et d'enrichissement pour les analyses automatisées. La dernière étape de la chasse aux menaces consiste à mettre à profit les connaissances acquises pendant le processus au cours du processus de chasse aux menaces pour enrichir et améliorer les systèmes EDR. Ainsi, la sécurité globale de l'entreprise est renforcée grâce aux découvertes réalisées au cours de l'investigation.

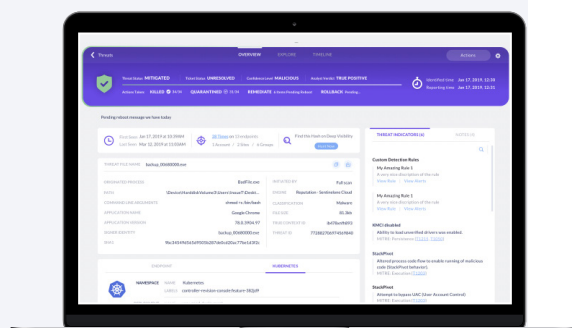


SentinelOne est conçu pour alléger la charge de travail de votre équipe de toutes les façons possibles, y compris en mettant à votre disposition les outils nécessaires pour configurer et exécuter des recherches personnalisées de chasse aux menaces. Grâce aux règles de détection STAR (Storyline Auto-Response) personnalisables, vous pouvez transformer les requêtes Deep Visibility en règles automatisées de chasse aux menaces, qui déclenchent des alertes et interventions en cas de correspondance. STAR vous offre la possibilité de créer des alertes personnalisées propres à votre environnement afin d'améliorer la pertinence des alertes et l'efficacité du tri des événements.



SentinelOne peut également neutraliser automatiquement les menaces détectées en appliquant la stratégie relative aux menaces suspectes ou aux menaces malveillantes, ou mettre les endpoints en quarantaine réseau. Les alertes sont déclenchées en temps quasi réel et sont consignées dans le journal des activités de la console de gestion. Vous pouvez activer dans Syslog des alertes pouvant être utilisées pour le tri et l'intégration SIEM.

Une fois la requête exécutée dans Deep Visibility et l'investigation terminée, vous pouvez sélectionner une réponse automatique pour la règle, afin de neutraliser automatiquement les menaces détectées. Votre solution SentinelOne est configurée ainsi pour protéger automatiquement votre environnement contre toutes les menaces en fonction de vos besoins, à chaque seconde du jour et de la nuit. Les cybercriminels modernes automatisent leurs techniques, tactiques et procédures pour échapper aux défenses préventives. Il semble donc logique que les équipes de sécurité des entreprises automatisent elles aussi leur charge de travail manuelle afin de mieux contrer les attaques.



Conclusion

La mise en place d'un programme de chasse aux menaces peut être très bénéfique à l'entreprise, notamment la découverte proactive des incidents de sécurité, l'accélération des délais d'intervention sur incident et un dispositif de sécurité plus robuste. Une chasse aux menaces efficace doit permettre d'alléger la charge de travail de vos analystes tout en protégeant durablement votre SOC contre tout un éventail de menaces connues et inconnues. SentinelOne vous offre la visibilité, l'ergonomie, la rapidité et le contexte nécessaires à une chasse aux menaces plus efficace que jamais.

Contactez-nous ou **demandez une démonstration** pour découvrir comment SentinelOne peut vous aider à mettre au point un programme de chasse aux menaces efficace.

Ressources supplémentaires

En immersion — **La chasse aux menaces avec MITRE ATT&CK**

Consultez la page de la **plateforme SentinelOne**

Découvrez la **Chasse aux menaces accélérée grâce à Storyline**

Consultez le rapport du Sans Institute sur la chasse aux menaces : **Automating the Hunt for Hidden Threats**

Lisez le rapport de Gartner **Using Threat Hunting for Proactive Threat Detection**

ATT&CK®

MITRE ATT&CK 2020

- Le plus grand nombre de détections
- Le plus grand nombre de corrélations
- Meilleure couverture de l'enrichissement des données

FORRESTER®

**RAPPORT FORRESTER
WAVE™ 2020 POUR
LES SOLUTIONS EDR**

« Acteur de premier plan »

kuppingercoale
ANALYSTS

**MARKET COMPASS 2020
DE KUPPINGERCOLE**

Innovateur sur le
marché EPDR

SentinelOne place ses clients au centre de ses priorités

Nos évaluations et améliorations continues nous poussent à dépasser les attentes de nos clients.



97 %

des évaluateurs du rapport Gartner Peer Insights™ « Voice of the Customer » 2020 recommandent SentinelOne.

97 %

Satisfaction des clients (CSAT)



À propos de SentinelOne

Plus de fonctionnalités, moins de complexité. SentinelOne développe des solutions de cybersécurité de pointe qui s'appuient sur une cyberveille autonome, distribuée sur les endpoints, afin de simplifier la pile de sécurité tout en offrant aux entreprises les fonctionnalités dont elles ont besoin. Notre technologie est conçue pour renforcer les équipes de sécurité grâce à l'automatisation et à une résolution des menaces d'une grande efficacité. Êtes-vous prêt ?

Nous contacter

sales@sentinelone.com

+1-855-868-3733

sentinelone.com