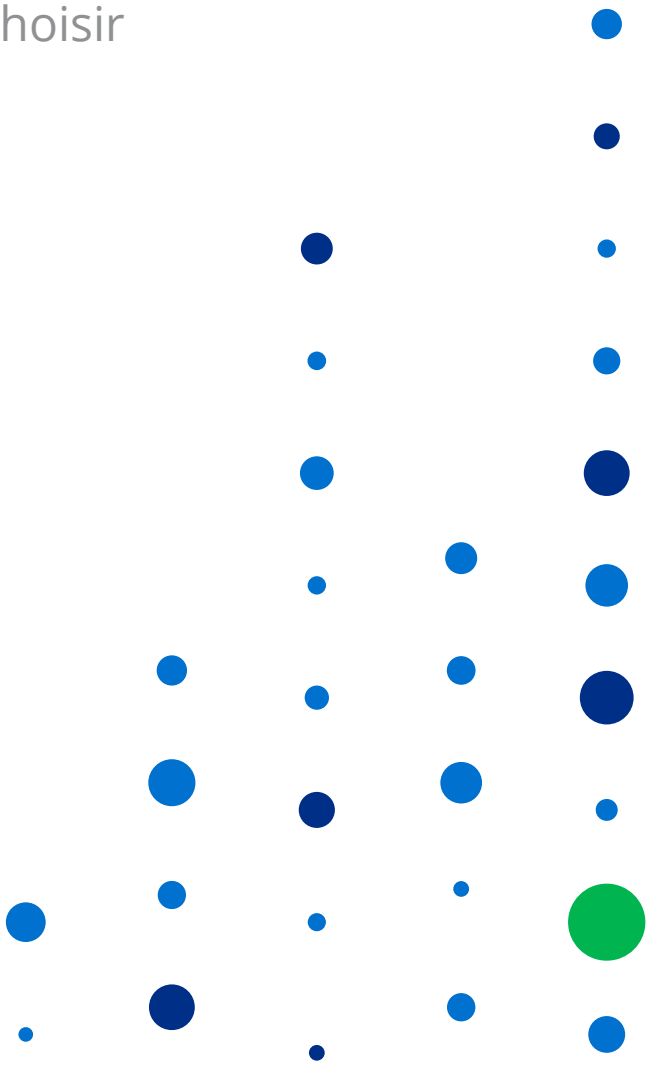
Recorded Future

Livre Blanc

Guide d'Achat pour le Renseignement sur les Menaces

11 questions à vous poser avant de choisir



Introduction

Le paysage des menaces est vaste, complexe et en constante évolution. L'idée que les entreprises peuvent être pleinement protégées contre toute menace potentielle est devenue illusoire.

Un bon système de renseignement sur les menaces est une fenêtre sur le monde de votre adversaire: Les éditeurs, les fabricants et les fournisseurs de services visent à donner plus de moyens aux organisations en les avertissant des vecteurs de menaces spécifiques et des attaques auxquelles ils sont confrontés, ainsi que comment ils devraient être classés par ordre de priorité pour la protection et la prévention.

Gartner définit les renseignements sur les menaces comme des «connaissances fondées sur des preuves, y compris le contexte, les mécanismes, les indicateurs, les implications et les conseils, à propos d'une menace existante ou émergente ou d'un danger pour les actifs qui peuvent être utilisées et aider aux décisions concernant la réponse à donner à cette menace ou danger. "

Cette définition met en évidence les trois facteurs qui distinguent les renseignements sur les menaces des simples données et informations. Intrinsèquement, les renseignements sur les menaces:

Doivent être basés sur des preuves.
Doivent correspondre à une menace existante ou émergente.
Doivent informer la prise de décision.

Si l'une de ces exigences est manquante, un traitement supplémentaire est nécessaire avant que l'information puisse être considérée un renseignement sur les menaces.

Lorsque vous commencez le processus de sélection d'une solution de renseignement sur les menaces, vous devez vous assurer que vous avez clairement défini vos besoins et que vous avez une bonne compréhension des fonctionnalités du fournisseur. Ce petit guide pose 11 questions clés et leurs implications pour vous aider à prendre votre décision sur la sélection d'une solution qui offre une sécurité axée sur le renseignement.

[1] "Market Guide for Security Threat Intelligence Products and Services," Gartner, (July 20, 2017).

1. Quelles catégories de renseignements sur les menaces vous sont les plus utiles?

Les renseignements sur les menaces se présentent sous différentes catégories, et le choix de ce qui convient le mieux à votre organisation dépend en grande partie de vos cas d'utilisation prévus.

Pour vous aider à identifier votre zone de besoin, nous divisons l'information sur les menaces en quatre catégories et leurs cas d'utilisation ciblés:

Threat Intelligence opérationnelle - Liée à des attaques spécifiques et imminentes, et est souvent utilisée par les experts en sécurité. C'est ce qui vient le plus souvent à l'esprit lorsque les gens pensent au renseignement sur les menaces; la capacité d'identifier quand et où les attaques viendront à l'avance.

Threat Intelligence stratégique - Ce type de renseignement donne une vue d'ensemble, conçu pour informer les décisions des conseils d'administration et des responsables de l'entreprise. Ce type de renseignement est rarement technique et est susceptible de couvrir des sujets tels que l'impact financier de la cybersécurité ou des changements réglementaires majeurs, tels que le règlement général sur la protection des données (GDPR).

Threat Intelligence tactique - Souvent désigné sous le nom de tactiques, techniques et procédures (TTP), les renseignements tactiques sur les menaces se rapportent aux vecteurs d'attaque spécifiques favorisés par les acteurs de la menace dans votre secteur ou emplacement géographique. Cette forme de renseignement est très exploitable et est utilisée par le personnel opérationnel, comme les intervenants en cas d'incident, pour s'assurer que les contrôles et les processus techniques sont bien préparés. Par exemple, si le harponnage est identifié comme un vecteur d'attaque important dans votre secteur, vous pouvez investir dans une formation supplémentaire sur la sécurité pour les utilisateurs à privilèges.

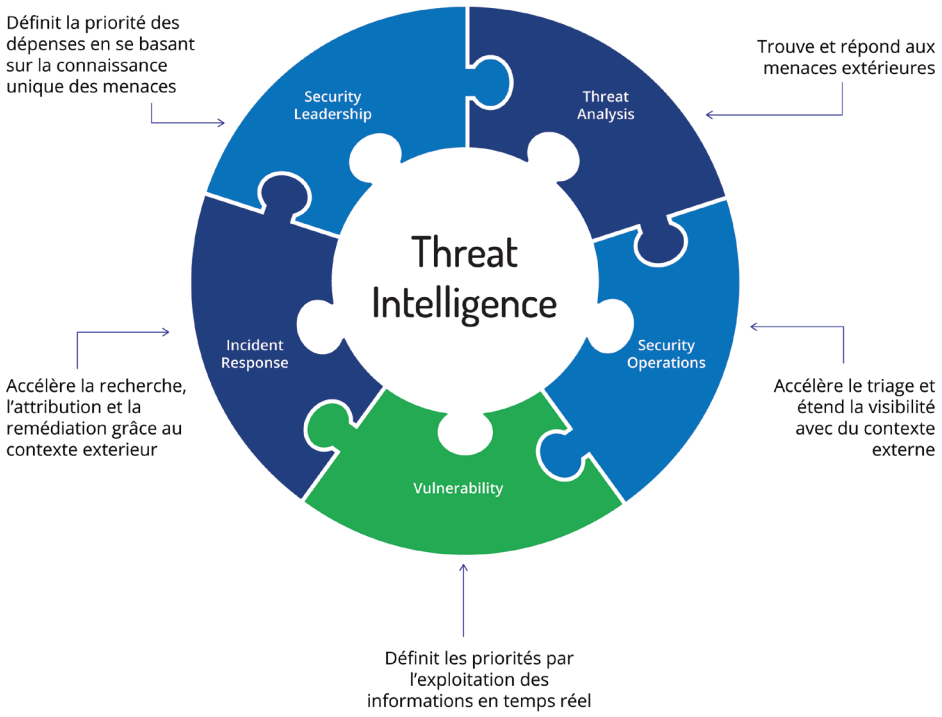
Threat Intelligence technique - Habituellement consommée automatiquement, l'intelligence technique des menaces comprend un flot d'indicateurs qui peuvent être utilisés pour identifier et bloquer automatiquement les communications malveillantes suspectées. Un bon exemple pourrait être un flux d'adresses IP suspectées d'être malveillantes, à partir de laquelle toutes les communications seraient automatiquement bloquées. Ce type de renseignements est généralement transitoire et disponible dans des volumes extrêmement élevés, d'où la nécessité de le traiter automatiquement plutôt que d'impliquer des analystes humains.

Aucune de ces catégories n'est intrinsèquement «meilleure» que d'autres. Au lieu de cela, elles peuvent être utilisées côte à côte pour former une capacité de renseignement cohérente. Les entreprises peuvent décider de ne consommer initialement que des informations techniques sur les menaces, car elles sont les plus facilement disponibles. Mais au fur et à mesure que les besoins évoluent, la plupart des organisations étendent les types de renseignements sur les menaces qu'elles ingèrent, ce qui rend essentiel la sélection d'un fournisseur offrant plusieurs catégories et une solution pouvant s'étendre au fil du temps.

2. Qui utilisera les renseignements sur les menaces?

Les décideurs en matière de sécurité ont traditionnellement quantifié le risque lié aux menaces auxquelles ils font face en se fondant uniquement sur des facteurs internes ou sur ce qu'ils lisent dans les nouvelles. Maintenant, il y a la possibilité d'utiliser des renseignements uniquement liés à votre activité.

En outre, les équipes de votre organisation de sécurité peuvent bénéficier d'une prise de décision plus éclairée et de perspectives uniques. Les renseignements qui peuvent être facilement consommés et compris ont le potentiel de révolutionner la façon dont les différents rôles de votre organisation fonctionnent au jour le jour, il y a des avantages de sécurité importants à cela. Le diagramme ci-dessous montre des exemples de la manière dont différentes équipes au sein des organisations utilisent les renseignements sur les menaces:



Lors de la sélection d'une solution de renseignement sur les menaces, il est important d'identifier tous les utilisateurs potentiels dans votre organisation et de savoir répondre à leurs cas d'utilisation uniques afin d'en tirer le meilleur parti possible.

3. Les renseignements seront-ils intégrés à vos processus de sécurité et à votre infrastructure?

La manière dont les renseignements seront exploités est étroitement liée aux personnes qui dans votre organisation utiliseront ces renseignements. Vaut-il mieux s'intégrer à des systèmes existants, ou les utilisateurs souhaiterons ils apprendre une nouvelle solution et une nouvelle interface pour accéder aux renseignements dont ils ont besoin? L'intégration dans les systèmes existants est un moyen efficace de rendre l'information accessible et utilisable sans surcharger les équipes de nouvelles technologies ou de trop de données.

En combinant des points de données internes et externes, un véritable système de renseignement peut être produit - une intelligence à la fois pertinente pour votre entreprise et placée dans le contexte plus large des menaces. Les objectifs opérationnels clés comme donner plus de moyens aux équipes de gestion des vulnérabilités à celles des réponses aux incidents qui bénéficieront de renseignements spécifiques, pertinents et contextualisés au bon endroit au bon moment. C'est la principale raison pour laquelle tant de solutions de renseignement sur les menaces sont conçues pour s'intégrer aux SIEM et à d'autres outils de sécurité, que ce soit par le biais d'intégrations clés en main avec des partenaires ou des API établis.

En fin de compte, la combinaison de sources internes et externes peut aider à réduire le bruit et à identifier les problèmes les plus urgents. Lors de l'évaluation des solutions de détection des menaces, il est important de comprendre si la solution est capable de s'intégrer à vos solutions existantes et de prendre en charge les cas d'utilisation de vos équipes de sécurité.

4. Comment les rapports de renseignement finis font-ilspartie de votre stratégie de renseignement sur les menaces?

Les rapports finis sont produits et utilisés pour informer les décisions stratégiques de haut niveau. Les rapports sur les menaces, qu'ils soient produits en interne ou par un fournisseur de sécurité, peuvent vous donner une bonne idée des grandes tendances de l'industrie, des vecteurs d'attaque couramment utilisés et des menaces émergentes. Ce type de renseignement est très utile pour prendre des décisions d'investissement ou pour élaborer des documents de politique de sécurité.

Lors de l'évaluation des solutions de renseignement sur les menaces, en plus des exigences de vos différentes équipes de sécurité, tenez compte des besoins de l'équipe de direction. De nos jours, il est inévitable que les responsables de votre organisation posent des questions sur les derniers titres de presse concernant la sécurité. Vous devez donc vous assurer que vous êtes en partenariat avec un fournisseur de renseignements sur les menaces capable de répondre à ces besoins. Particulièrement si vous avez une équipe de sécurité restreinte.

5. De quelle expertise aurez-vous besoin pour commencer?

Le niveau de valeur que vous obtenez des renseignements sur les menaces que vous ingérez est directement lié à votre capacité de les rendre pertinents pour votre organisation et de les appliquer efficacement aux processus de sécurité existants ou nouveaux. Il existe de nombreux produits et services conçus pour vous aider à mettre en œuvre des renseignements sur les menaces. Tout ce que votre équipe exige, ce sont des objectifs clairs sur les avantages que vous attendez d'elle.

Le fournisseur qui peut vous aider à atteindre ces objectifs fournit presque certainement une combinaison de capacités techniques et d'expertise pour permettre aux entreprises de tirer le meilleur parti des renseignements sur les menaces.

Le support technique et les services professionnels d'un fournisseur doivent être là pour vous aider à utiliser n'importe quel logiciel, résoudre les problèmes potentiels et travailler à l'intégration des renseignements avec les systèmes de sécurité existants dont vous avez besoin. Et bien sûr, ce support devrait être disponible quand vous en avez besoin, à travers les canaux de communication qui conviennent le mieux à votre entreprise.

Le fournisseur que vous choisissez doit également être une société pleine d'experts en renseignement sur les menaces. Ces spécialistes sont formés pour comprendre vos besoins et peuvent vous aider à tirer le meilleur parti de votre investissement en vous permettant de produire vos propres renseignements sur les menaces. Vous voudrez être en mesure de faire appel à ces services quand cela vous conviendra, et ils devraient continuer à travailler avec vous pour identifier de nouveaux avantages potentiels à tirer des renseignements sur les menaces dans votre organisation.

6. De quelles sources de données sur les menaces avez-vous besoin?

Pour être vraiment utile, votre programme de renseignement sur les menaces doit tenir compte de la gamme la plus large possible de sources de données sur les menaces dans le cadre des objectifs que vous avez définis. Vous devez également garder à l'esprit que sans traitement, ces sources ne sont que des données, et non du renseignement.

Tout fournisseur de renseignements sur les menaces que vous choisissez devrait avoir accès à plusieurs ou à l'ensemble des sources suivantes:

Technique

(par exemple, listes de menaces, spam, logiciels malveillants, infrastructure malveillante)
Ce type de données est disponible en grande quantité, souvent gratuitement. En raison de sa nature binaire, il est facile de l'intégrer aux technologies de sécurité existantes, même si de nombreuses analyses supplémentaires seront nécessaires pour en dégager le contexte réel.

Forums

Parce que ces canaux sont spécifiquement conçus pour héberger des discussions pertinentes, ils constituent une source potentiellement précieuse d'informations sur les menaces. Cela dit, vous aurez encore besoin de passer du temps sur la collecte et l'analyse pour identifier ce qui est vraiment précieux.

Médias sociaux

Il existe indubitablement des masses de données potentiellement utiles sur les réseaux sociaux, mais il est difficile de déterminer les faux positifs et la désinformation. En règle générale, vous trouverez de nombreuses références aux mêmes menaces et tactiques qui peuvent imposer un gros travail de tri aux analystes humains.

Médias

(par exemple, actualités, sites de sécurité de l'information, recherche de fournisseurs, blogs, divulgations de vulnérabilités)
Ces sources fournissent souvent des indicateurs utiles sur les menaces nouvelles et émergentes, mais il sera difficile de les relier à des indicateurs techniques pertinents pour mesurer le risque réel.

Dark Web

(plusieurs niveaux de communautés souterraines)
Souvent, il s'agit d'une source d'informations très spécifiques, tactiques et techniques sur les menaces, mais il est incroyablement difficile d'y accéder, en particulier aux communautés criminelles de niveau supérieur. De plus, comme plusieurs de ces communautés ne parlent pas anglais, la langue est souvent un défi.

Vous pouvez également trouver certains fournisseurs spécialisés dans la production de renseignements provenant d'un type de sources particulières, comme les médias sociaux ou le dark web.

Pour la plupart des organisations, c'est la combinaison de toutes ou de la plupart des sources ci-dessus qui est la plus puissante. L'intégration et l'analyse de données provenant de sources multiples peuvent vous donner des perspectives uniques, un contexte profond et une vue équilibrée qui ne peut être atteinte autrement. Dépendant trop d'une ou de deux sources de données, il y aura des occasions manquées et, finalement, des perspectives faussées.

Par exemple, si vous ne traitez que des flux de menaces open source, vous ne disposerez pas du contexte nécessaire pour prendre des décisions éclairées. Comment pourriez-vous savoir parmi les milliers de vulnérabilités découvertes chaque année lesquelles devraient être corrigées en premier? Ou si vous devez agir immédiatement, plutôt que d'attendre la prochaine période de maintenance planifiée? Recherchez des solutions qui peuvent ajouter ce type de contexte pour vous donner des indications claires sur les risques pouvant être appliqués à votre stratégie de sécurité plus large.

Lors de l'évaluation de la solution qui vous aidera le mieux à atteindre vos objectifs, il est essentiel de prendre en compte l'équilibre entre les sources de données et les points de vue que chacune d'elles fournira. Vous avez besoin d'une solution qui consomme des données provenant d'un large éventail de sources (y compris celles auxquelles vous avez déjà accès), mais vous avez également besoin d'une solution qui peut contextualiser et hiérarchiser les alertes pertinentes tout en supprimant le bruit.

7. Comment votre capacité de renseignement sur les menaces évoluera-t-elle?

Peut-être votre investissement financier et humain initial dans les renseignements sur les menaces sera-t-il relativement petit, mais avec le temps et plus vous chercherez à utiliser les renseignements sur les menaces dans différents domaines, et plus ils deviendront exponentiellement exigeants en ressources si vos processus sont manuels. En réalité, le volume des données disponibles sur les menaces rend la collecte et le traitement impossibles pour des seuls humains. Même avec des alertes agrégées et normalisées en un seul endroit (comme c'est le cas avec de simples plates-formes de renseignement sur les menaces, ou TIPs), votre équipe sera rapidement dépassée.
Les fournisseurs de renseignements sur les menaces utilisant uniquement des analystes humains sont confrontés au même défi. Les humains sont lents et coûteux si on additionne les ressources. Une solution efficace est celle où les tâches simples - agrégation de données, comparaison, étiquetage et contextualisation - sont complétées par des machines, laissant les humains faire ce qu'ils font le mieux: prendre des décisions efficaces et éclairées. L'utilisation de l'automatisation de cette manière vous donnera l'assurance que, lorsque vos besoins changent, votre solution de renseignement sur les menaces peut évoluer efficacement pour les atteindre.

Examinez jusqu'à quel niveau les fournisseurs emploient l'automatisation, non seulement pour croiser ou regrouper des données, mais aussi pour ajouter un contexte qui permet à vos équipes de prendre des décisions basées sur les risques en toute confiance. Gardez à l'esprit qu'avec les renseignements sur les menaces, plus de données donnent de meilleurs résultats - à condition qu'elles soient correctement analysées, structurées et livrées dans un format facile à utiliser.

8. Avez-vous besoin de renseignement surles menaces en temps réel?

Nous avons déjà établi qu'il existe d'énormes volumes de données sur les menaces. Ces données sont facilement disponibles en temps réel, mais une grande partie de celles-ci n'aura aucune valeur réelle pour identifier les menaces qui concernent votre organisation, votre secteur d'activité ou votre infrastructure. C'est pourquoi l'équilibre entre la vitesse et le contexte est peut-être le facteur le plus important dans la production de renseignements sur les menaces exploitables.

Sans contexte, il est très difficile de déterminer une réponse appropriée aux alertes. Cependant, en même temps, le contexte ne peut pas toujours être trouvé instantanément, et de nombreux événements de sécurité sont sensibles au temps. Pris à l'extrême, cela peut vous amener à prendre la bonne décision très lentement, ou la mauvaise décision très rapidement.

C'est pourquoi il est si important de trouver un équilibre. Pour obtenir le maximum d'avantages, vous avez besoin d'une solution capable d'équilibrer la vitesse des nouvelles données avec le contexte dont vous aurez besoin pour prendre une décision rapide en fonction du risque réel.

9. Avez-vous besoin d'une solution tout-en-un ou d'outils logiciels distincts?

Il existe une idée fausse commune depuis un certain temps que pour «faire» des renseignements sur les menaces, une organisation doit simplement acheter une plateforme et s'abonner à quelques flux.

En réalité, cette approche peut créer une somme de travail encore plus grande. S'abonner à même un petit nombre de flux risque de générer un afflux massif d'alertes, dont chacune doit être triée rapidement par un analyste humain pour s'assurer que rien n'est manqué. Étant donné que de nombreuses alertes sont soit des faux positifs, soit simplement non pertinentes, les analystes finissent par passer un temps excessif à obtenir très peu de résultats.

Pour faire la lumière sur ces questions, voici les quatre principaux types de services et technologies de renseignement sur les menaces disponibles pour les organisations:

1. Rapports d'analyse humains

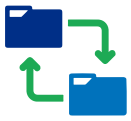
Externaliser votre production d'informations sur les menaces en vous abonnant à un service d'analyse humaine. Au lieu de recevoir des alertes directement, un fournisseur de sécurité consommera des quantités massives d'informations en votre nom. S'il estime que quelque chose d'important pour votre organisation apparait, vous serez informé via un service de reporting - généralement, un portail en ligne.

Avantages:
- **Minimise la pression sur les ressources internes.**
- **Fournit un accès à une grande variété de sources.**
- **Aucune dépense en capital requise.**

Inconvénients:
- **Distance entre les analystes internes et le processus de collecte de renseignements.**
- **Par conception plus lent que les solutions internes.**
- **S'appuie sur des analystes moins familiers avec votre entreprise.**

2. Flux de données sur les menaces

Flux en temps réel d'indicateurs de menaces ou d'artefacts fournis par des tiers, dont c'est le métier de vous fournir ce type de renseignements. Les flux sont invariablement livrés en ligne et se concentrent généralement sur un type spécifique de données, comme les adresses IP suspectées d'être liées à une activité malveillante. Un grand nombre de flux gratuits et payants sont disponibles, couvrant tous les domaines imaginables de la cybersécurité.



Avantages:
- **De nombreux flux contiennent des alertes très utiles.**
- **Les données en temps réel peuvent déclencher une réponse automatique quasi instantanée.**
- **Facilement disponible et facile à utiliser.**

Inconvénients:
- **Le manque de contexte rend les alertes difficiles à traiter (données, pas renseignement).**
- **Le volume de faux positifs est énorme.**
- **Très consommateur de temps pour les analystes humains.**

3 Threat Intelligence Platforms

Les flux de données sur les menaces sont rarement utilisés isolément. Les plates-formes de renseignement sur les menaces sont utilisées pour combiner les flux en un seul flux en utilisant une technologie standardisée, généralement STIX / TAXII. Alors que la plupart des plates-formes de base s'arrêtent ici, des produits plus complets offrent des fonctionnalités supplémentaires telles que des flux normalisés, l'intégration SIEM, ainsi que l'automatisation et l'orchestration.

Avantages:
- **Combine les entrées dans un seul flux.**
- **L'intégration avec les SIEM permet un certain degré d'automatisation.**

Inconvénients:
- **Les alertes vitales peuvent être ignorées car les analystes ne peuvent pas gérer le volume entrant.**
- **Le manque de contexte peut rendre le traitement des alertes lent et lourd.**
- **Les analystes finissent par arrêter de trier les alertes et deviennent désillusionnés.**

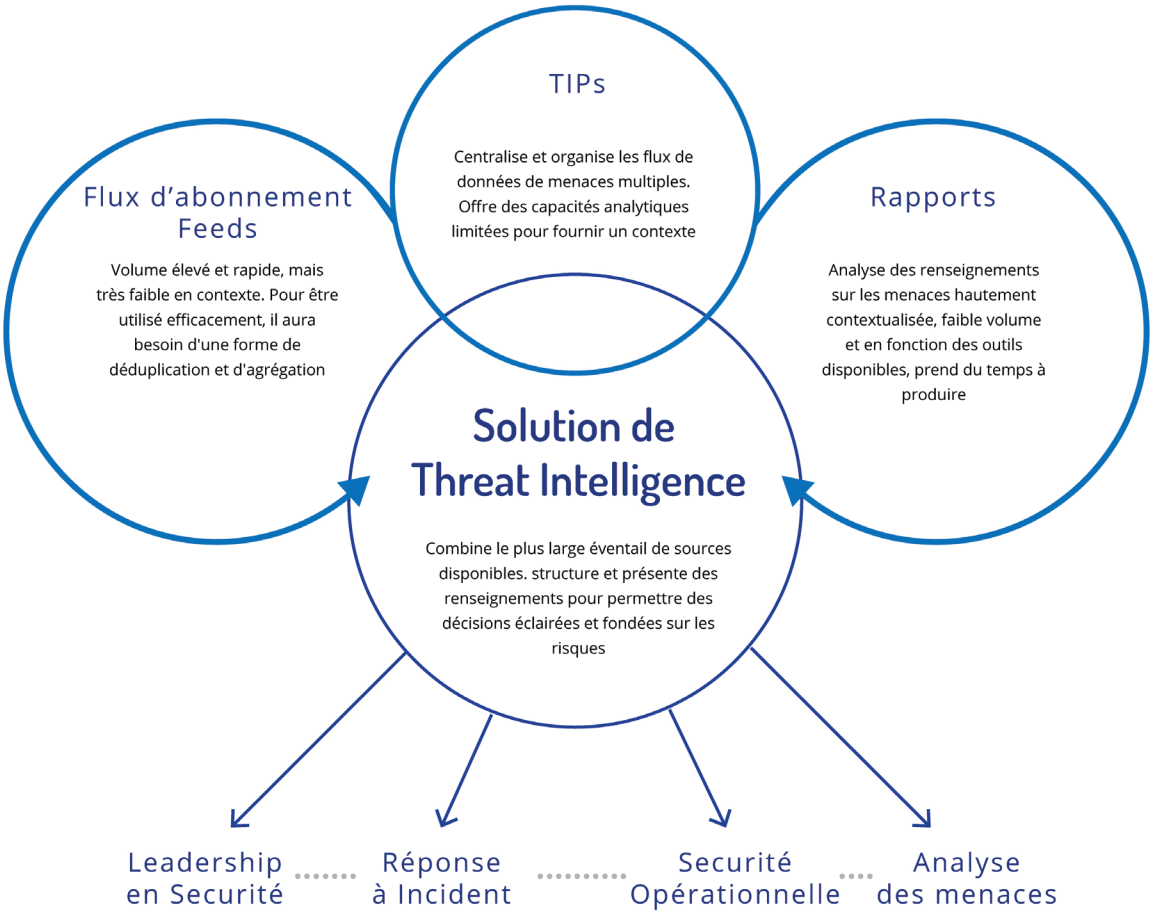
4 Solution Complète de Threat Intelligence

Combine les capacités des offres définies ci-dessus. Présente des données sur les menaces (y compris tous les types de flux) et des informations provenant du Web et du Dark Web, en combinant des techniques d'apprentissage automatique, y compris le traitement du langage naturel (PNL) pour produire des informations contextualisées pertinentes. Les solutions phares offriront également des services de renseignement humain alimentés par leur technologie.

Avantages:
- **Facilement actionnable par des machines et des humains.**
- **Les alertes sont entièrement contextualisées.**
- **Permet à plus de défenseurs de travailler avec plus de renseignements.**
- **Extrait les données de tout le Web public et caché, quelle que soit la langue source.**

Les inconvénients:
- **Peut nécessiter un investissement initial plus important.**

Lorsque vous évaluez ce qui est disponible auprès des fournisseurs de renseignements sur les menaces, assurez-vous d'avoir déterminé quels types d'offres sont les plus susceptibles de répondre à vos besoins. Essayez de classer leurs capacités par importance et évitez rapidement les fournisseurs qui n'ont pas ces capacités. La plupart des organisations exigent une combinaison de tout ou partie de ce qui précède - soit au début ou au fur et à mesure que votre programme se développe. Par conséquent, il est important de réfléchir aux besoins à long terme lors de l'évaluation de ces options. De plus, si vous avez déjà investi dans d'autres systèmes de sécurité, recherchez des solutions qui s'intégreront à ces derniers via des partenariats ou une API flexible.



A true threat intelligence solution combines key features from threat data feeds, threat intelligence platforms, and reports created by analysts.

10. Quel est le meilleur endroit pour déployer la solution?

La plupart des solutions de détection des menaces apportent des données externes à votre organisation pour analyse ou intégration avec des logiciels de sécurité déjà installés sur site. Ce flux de données provenant de l'extérieur est parfaitement adapté au déploiement basé sur le cloud, ce qui réduit les efforts de mise en œuvre et supprime le besoin de correctifs ou de mises à niveau.

Comme il est peu probable que la solution contienne des données d'entreprise confidentielles ou précieuses, il y a moins de problèmes de sécurité. Cela dit, vous devez veiller à ce que tout produit SaaS prenne en compte la sécurité en rendant anonymes toutes les données qui s'y trouvent et en fournissant une authentification à deux facteurs, ainsi que des intégrations avec tous les services d'annuaire utilisés par votre entreprise.

Le plus grand avantage d'une implémentation basée sur le cloud est l'immédiateté. Des renseignements nouvellement collectés et analysés devraient être disponibles immédiatement avec le nuage - ne pas utiliser les informations disponibles en temps réel n'est pas la meilleure façon de tirer le meilleur parti des renseignements sur les menaces. De nouvelles fonctionnalités ou techniques d'analyse devraient également être disponibles immédiatement dans le cloud, évitant ainsi des mises à niveau matérielles sur site potentiellement longues.

11. Comment allez-vous pérenniser votre investissement dans le renseignement sur les menaces?

Le moyen le plus simple de maximiser votre investissement dans les renseignements sur les menaces consiste à vous assurer que vous avez sélectionné un fournisseur capable de répondre à vos besoins. Si vous en êtes aux premiers stades et décidez de mettre en œuvre uniquement une solution capable de fournir des sources de données sur les menaces ou des rapports d'analystes, lorsque vous devrez intégrer les renseignements à d'autres produits de sécurité ou employer vos propres experts, vous risquez de devoir recommencer à zéro. Étudiez toutes les capacités d'un fournisseur potentiel afin de vous assurer qu'il ne vous permet pas seulement d'atteindre vos objectifs à court terme, mais qu'il peut répondre à vos critères selon l'évolution de vos besoins.

Nous avons également déjà mentionné que votre fournisseur choisi devrait avoir suffisamment d'experts en renseignement sur les menaces - cela signifie également qu'il est le plus susceptible de fournir une formation continue ou même une certification pour permettre à vos équipes et valider leur efficacité.

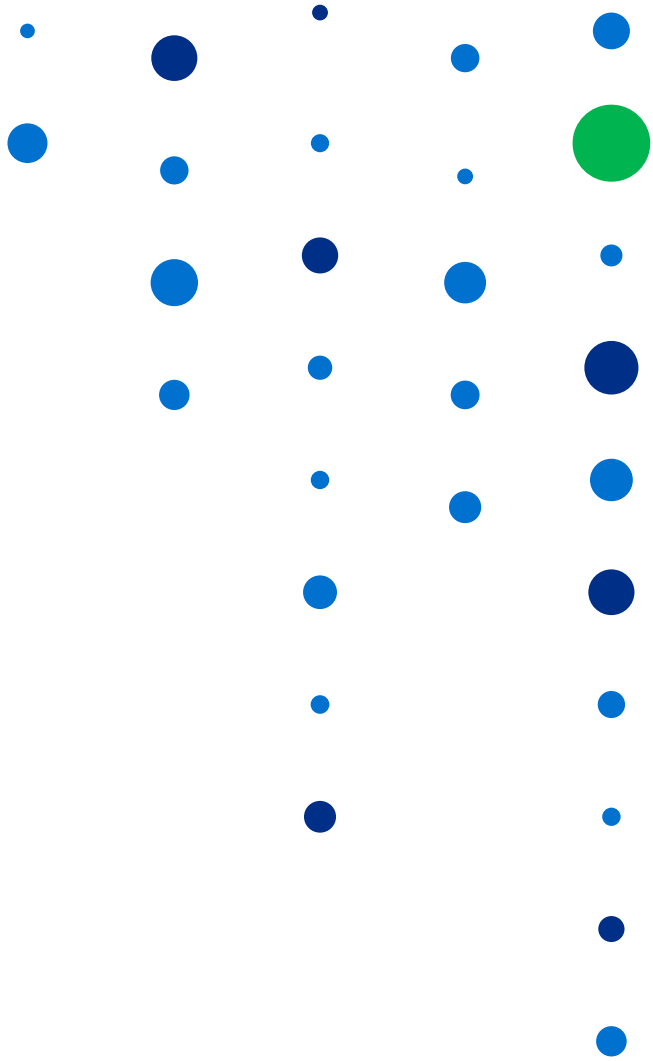
Modèle de demande de renseignements sur les menaces

Pour lancer le processus de sélection d'une solution de renseignement sur les menaces, nous avons fourni un modèle que vous pouvez utiliser pour créer une demande de proposition, ce qui vous aide à évaluer les capacités des fournisseurs que vous évaluez. Vous pouvez le télécharger ici .

Informez-vous et soyez proactif

Une fois que vous êtes satisfait de la façon dont vous avez répondu à ces questions, vous devriez être en mesure de prendre une décision éclairée quant à la meilleure façon d'investir dans les renseignements sur les menaces. Au cours de votre processus de sélection, gardez vos cas d'utilisation (actuels et futurs) à l'esprit et suivez ce mantra:

Décidez de ce pour quoi vous avez besoin de renseignements sur les menaces et choisissez la solution qui non seulement vous fournit ce dont vous avez besoin aujourd'hui, mais qui ajoute également la possibilité de devenir un partenaire capable de vous accompagner tout au long de votre évolution.



Recorded Future

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.