Recorded Future®

Le renseignement sur les menaces Guide de l’acheteur

Tout ce que vous devez savoir concernant le renseignement sur les menaces avant d’acheter

Introduction

Recorded Future®

Protéger votre entreprise des groupes de ransomware, des hacktivistes, des fraudeurs, des courtiers en accès initial et de tout autre type d'acteur de la menace est un défi. Un défi auquel les organisations de toutes tailles et de presque tous les secteurs n'échappent pas en raison d'un paysage de menaces moderne qui est vaste, complexe et en constante évolution.

L'idée que les organisations peuvent être totalement protégées contre toutes les menaces potentielles est devenue intenable et nécessite un changement dans les outils et les approches dont les équipes ont besoin pour garder une longueur d'avance sur une attaque.

L'utilisation et la mise en œuvre de renseignement sur les menaces est un élément essentiel de l'équipe de sécurité moderne d'aujourd'hui et, lorsqu'il est utilisé à son plein potentiel, il fait souvent la différence entre la prévention d'un incident et le fait d'en être la victime.

Un renseignement sur les menaces bien fait est une fenêtre sur le monde de votre adversaire et les cibles qu'il cherche à exploiter. Les fournisseurs et les prestataires de services visent à responsabiliser les organisations en les alertant sur les vecteurs de menace et les attaques spécifiques auxquels elles sont confrontées, ainsi que sur les actions à mener en priorité en matière de protection et de prévention.

Il n'est donc pas étonnant que dans le rapport 2023 State of Threat Intelligence, créé par CyberEdge et sponsorisé par Recorded Future, 98 % des personnes interrogées reconnaissent qu'un renseignement exhaustif sur les menaces est essentiel pour leur programme de cybersécurité.

Lorsque vous commencez le processus de sélection d'une solution de renseignement sur les menaces, vous devez vous assurer d'avoir clairement défini vos besoins et d'avoir une bonne compréhension des capacités d'un fournisseur.

Ce guide complet pose 12 questions clés et leurs implications pour vous aider à prendre une décision éclairée sur le choix d'une solution qui offre une sécurité basée sur le renseignement afin de protéger votre organisation contre les menaces connues et émergentes.

Recorded Future®

Qu’est-ce que le renseignement sur les menaces ?

Avant d’entrer dans le vif du sujet, définissons le terme « renseignement sur les menaces ». Le renseignement sur les menaces est constitué de données collectées et indexées à partir de sources multiples, notamment le dark web, le web ouvert, les sources techniques, la télémétrie des clients et d’autres sources.

Ces données ont été organisées, analysées et fournies pour aider les professionnels de la sécurité et les dirigeants à comprendre leur paysage unique de menaces, y compris les acteurs de la menace, l’infrastructure malveillante qu’ils construisent, leurs tactiques, leurs comportements et leurs cibles.

Le renseignement sur les menaces ne se limite pas à trouver des flux libres et à les consulter. Il consiste à trouver et à acquérir les données les plus pertinentes qui vous donnent un aperçu unique de votre paysage des menaces. Le renseignement sur les menaces organise les informations pertinentes de manière à ce qu’elles soient utiles à l’analyse, puis à la diffusion au sein de l’organisation ou des organisations, afin qu’elles soient exploitables et qu’elles contribuent à la prise de décision.

Le renseignement sur les menaces fournit également aux utilisateurs la même vue extérieure des lacunes et des faiblesses qu’un attaquant voit et peut chercher à exploiter.

La valeur du renseignement sur les menaces réside dans sa capacité à permettre aux organisations de prendre plus rapidement et plus efficacement des décisions de sécurité fondées sur des données, en aidant les équipes à devenir proactives plutôt que réactives dans la défense de leurs actifs critiques contre les attaquants.

QUESTIONS À POSER À UN FOURNISSEUR :

↳ Quelle est votre définition du renseignement sur les menaces, qu’en pense votre entreprise ?

↳ Êtes-vous un créateur ou un agrégateur de renseignement ?

Recorded Future®

Quels défis le renseignement sur les menaces peut-il aider mon équipe à résoudre ?

Il existe de nombreux défis que le renseignement des menaces peut aider les organisations à surmonter. Nous vous recommandons d'évaluer les solutions de renseignement sur les menaces qui peuvent vous aider à relever les cinq défis ci-dessous, qui, d'après les études de marché et les entretiens avec les clients de Recorded Future, empêchent souvent les cadres et les professionnels de la sécurité de dormir la nuit :

- **Atténuation des ransomwares :** en 2023, les entreprises, les particuliers et les autres victimes d'attaques de ransomwares ont payé aux pirates plus de 1,1 milliard de dollars en échange du déverrouillage de leurs données (The Record). Le renseignement sur les menaces peut aider les équipes de sécurité à se concentrer sur les acteurs de la menace qui ciblent leur organisation et à renforcer leurs défenses contre leurs outils, tactiques et procédures (TTP) les plus courants.
- **Automatisation des flux de travail de sécurité :** selon le rapport Tines Voice of the SOC, les professionnels de la sécurité déclarent que « le temps passé à effectuer des tâches manuelles est l'aspect le plus frustrant de leur travail ». L'intelligence sur les menaces automatise la collecte, le traitement et l'analyse des informations, ce qui peut aider les équipes de sécurité à automatiser les flux de travail. Recherchez des solutions qui prennent en charge une gamme d'intégrations.
- **Protection contre les risques numériques :** l'augmentation du patrimoine numérique oblige les entreprises à sécuriser leurs actifs numériques et leurs données contre les menaces externes telles que l'usurpation d'identité de marque ou de dirigeant, la prise de contrôle de comptes et les fuites de données. Évaluez les solutions de renseignement sur les menaces qui fournissent un contexte exploitable sur les risques numériques et automatisent le processus de collecte et d'alerte sur les nouveaux risques numériques.
- **Risque lié à la chaîne d'approvisionnement :** les fournisseurs tiers et les sites physiques représentent des menaces potentielles pour une organisation, mais de nombreuses pratiques de gestion du risque lié à la chaîne d'approvisionnement adoptent une approche statique de l'évaluation du risque. Le renseignement sur les menaces peut vous aider à examiner les risques associés aux fournisseurs tiers que votre organisation envisage d'intégrer, et à fournir des alertes en temps réel sur les menaces qui pèsent sur les tiers et les quatrième parties de votre chaîne d'approvisionnement.
- **Gestion de l'exposition :** à mesure que votre organisation adopte sa stratégie de croissance numérique et tire parti des ressources basées sur le cloud, votre surface d'attaque externe est probablement en constante évolution. Sans visibilité sur les actifs externes, les organisations peuvent compter sur des centaines d'actifs inconnus ou mal gérés, ce qui accroît considérablement le risque de cyberattaque. Certaines solutions de renseignement sur les menaces aident les organisations à identifier et à inventorier les actifs en contact avec Internet, à hiérarchiser les efforts de remédiation tels que la correction des vulnérabilités, et à accélérer la remédiation des expositions à haut risque.

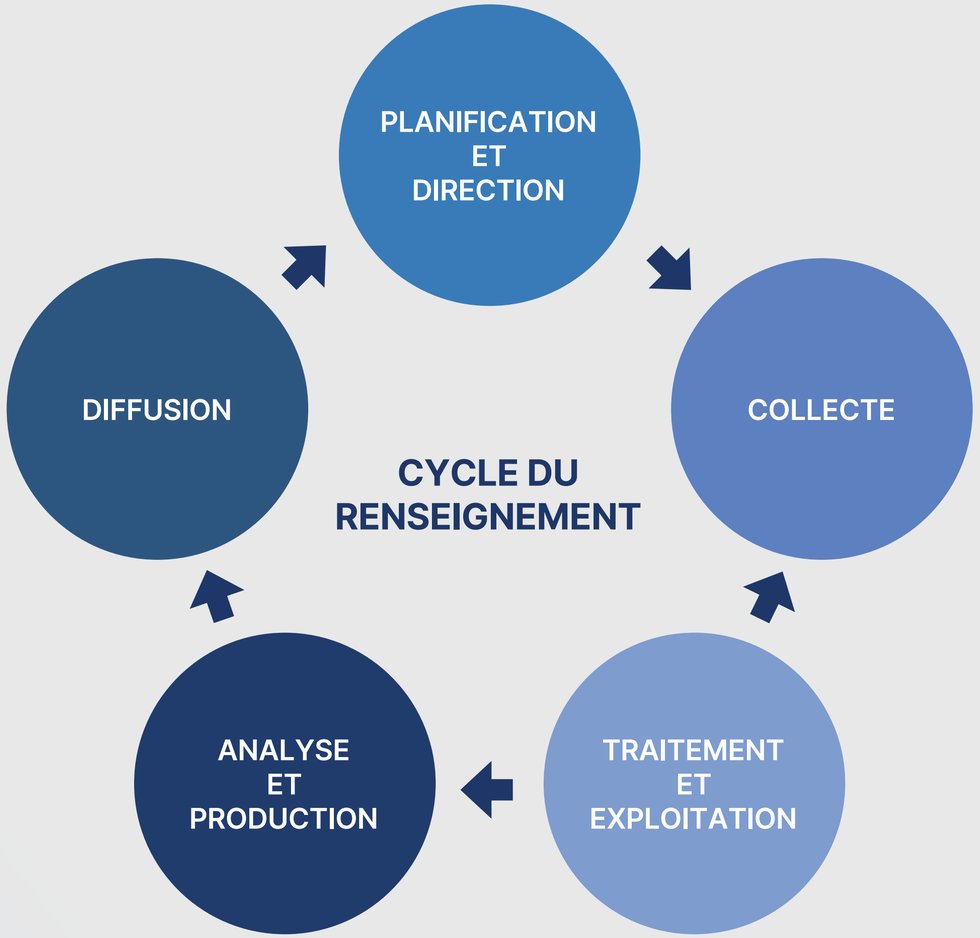
QUESTIONS À POSER À UN FOURNISSEUR :

↳ Quels sont les défis courants que vos clients résolvent avec votre produit ?

Recorded Future®

Quel est le cycle du renseignement et pourquoi est-ce important ?

Pour approfondir ce concept, il est utile de comprendre le cycle du renseignement, qui est le processus de création et d'utilisation du renseignement. Le cycle du renseignement est un processus développé à l'origine par la CIA, qui comporte cinq étapes : la direction, la collecte, le traitement, l'analyse et la production, et la diffusion. Au terme d'un cycle, un retour d'information et une évaluation de la réussite ou de l'échec du cycle précédent sont effectués, ce qui est
ensuite répété.



Recorded Future®

Mais comment cela s’applique-t-il au renseignement sur les menaces utilisés au sein de votre organisation ?

DIRECTION

Tout comme dans la communauté du renseignement au sens large, les directives viennent d’en haut : le RSSI d’une organisation, par exemple, ou le responsable du centre des opérations de sécurité (SOC) d’une organisation. Les éléments essentiels du renseignement sur les menaces fournissent les informations nécessaires pour orienter correctement les analystes des domaines physique et numérique : alors qu’une agence gouvernementale peut se concentrer sur une certaine zone géographique, un SOC peut choisir de se concentrer sur les menaces directes qui pèsent sur son réseau et sur l’identification des indicateurs de compromission.

COLLECTE

Les données sont recueillies auprès de sources techniques et humaines. Aujourd’hui, alors qu’il faut des millions, voire des milliards de points de données individuels pour constituer un échantillon suffisamment important pour identifier des modèles fiables, l’automatisation offerte par le renseignement sur les menaces permet de réduire considérablement le temps nécessaire à l’étape de la collecte. Les données collectées uniquement à partir de sources publiques sont souvent insuffisantes. Coopérer avec d’autres organisations pour partager des données privées provenant de sources fermées, voire avoir une présence active sur le dark web, permet d’obtenir des ensembles de données plus complets.

TRAITEMENT

Comme les grands ensembles de données rendent l’automatisation nécessaire dans la phase de collecte, elle est également nécessaire pour traiter ces données de manière compréhensible. Et de nombreux produits de renseignement sur les menaces offrent des outils automatisés efficaces pour produire des rapports et d’autres ressources. Mais une collaboration étroite entre les humains et les machines est essentielle : l’œil d’un expert peut fournir le contexte supplémentaire et l’intuition nécessaires pour éliminer toute ambiguïté. Dans un secteur où les secondes, voire les jours, peuvent faire toute la différence dans la réponse à une menace, la bonne direction donnée par un expert humain peut aider même le processus automatisé le plus rapide à effectuer une recherche intelligente et efficace plutôt que de s’en remettre uniquement à la force brute.

Recorded Future®

ANALYSE ET PRODUCTION

Comme indiqué précédemment, les données traitées doivent être rendues cohérentes et triées efficacement, et là encore, aucune automatisation ne peut réellement remplacer l'analyse humaine. Comme défini ci-dessus, le renseignement comprend une analyse des motivations et des prédictions sur le comportement futur, et ce type d'analyse ne peut être bien fait que par du personnel armé de la bonne technologie.

DIFFUSION

Le produit fini remonte vers le haut, recommençant le cycle. Il peut s'agir de rapports d'information finaux, de briefings de l'équipe, d'alertes ou de tout autre moyen choisi par les parties prenantes pour consommer du renseignement.

RETOUR D'INFORMATION

L'efficacité d'un cycle de renseignement sur les menaces déterminera les éléments d'information essentiels nécessaires pour le cycle suivant, y compris les domaines sur lesquels il faut se concentrer lors de la collecte des données et la rapidité avec laquelle des mesures doivent être prises à l'avenir.

Le renseignement sur les menaces influence l'action

« Au fond, la valeur du renseignement sur les menaces réside dans l'influence : vous utilisez vos
résultats pour convaincre l'entreprise de faire quelque chose, qu'il s'agisse d'investir dans une capacité, de changer la façon de faire quelque chose ou d'accorder plus d'attention à un risque identifié »

Jasmina Zito, Spécialiste principale du renseignement sur les cybermenaces chez Canva

QUESTIONS À POSER À UN FOURNISSEUR :

- ↳ Comment votre produit prend-il en charge/s'applique-t-il à l'ensemble du cycle de renseignement ?
- ↳ Comment le cycle de renseignement informe-t-il la façon dont votre produit est développé

Recorded Future®

Quels sont les différents types de renseignement sur les menaces et qui les consomme ?

Le renseignement sur les menaces est multiple et appartient à des catégories différentes, et le choix de la meilleure solution pour votre organisation dépend en grande partie des cas d'utilisation prévus. Pour vous aider à identifier les types de renseignement qui peuvent le mieux soutenir votre organisation, examinez les trois catégories de renseignement suivantes et leurs cas d'utilisation ciblés :

RENSEIGNEMENT STRATÉGIQUE SUR LES MENACES

Ce type de renseignement donne une vue d'ensemble, conçue pour éclairer les décisions des cadres et des dirigeants sur les risques que représentent les cybermenaces ou les menaces physiques pour leur organisation. Il est rarement technique et couvre généralement des sujets tels que les tendances des menaces dans le secteur, les tendances géopolitiques, les technologies et menaces émergentes, les normes de conformité et de réglementation, et l'impact financier des événements liés à la sécurité. Les dirigeants qui disposent de ce niveau de renseignement peuvent l'utiliser pour créer une stratégie de sécurité fondée sur le renseignement, maximiser les investissements en matière de sécurité ou informer d'autres parties prenantes.

PARTIES PRENANTES/CONSOMMATEURS

- Membres de la direction (RSSI, CIO, CSO, CTO)
- Membres du conseil d'administration
- Vice-présidents principaux
- Leaders du renseignement (cyber et physique)

Recorded Future®

RENSEIGNEMENT SUR LES MENACES OPÉRATIONNELLES

Bien plus approfondie que le renseignement stratégique sur les menaces, le renseignement opérationnel sur les menaces est utilisé pour comprendre le « qui, quoi, pourquoi, quand et comment » des menaces ciblant l'organisation. Les analystes peuvent effectuer des analyses approfondies sur les acteurs de la menace et leurs tactiques en créant des rapports qui informent les autres équipes de sécurité pour leur permettre de prendre des mesures. Il s'agit généralement d'attaques spécifiques et imminentes, qui sont souvent le fait du personnel de sécurité de haut niveau ou des équipes de renseignement sur les cybermenaces.

PARTIES PRENANTES/CONSOMMATEURS

- Responsables de la sécurité
- Responsable SOC
- Responsable SOC
- Équipe de renseignement sur les cybermenaces
- Intervenants en cas d'incident

RENSEIGNEMENT SUR LES MENACES TACTIQUES

Généralement consommée automatiquement, le renseignement tactique sur les menaces comprend un flux d'indicateurs qui peuvent être utilisés pour identifier et bloquer automatiquement les communications soupçonnées d'être malveillantes. Par exemple, un flux d'adresses IP suspectées d'être malveillantes, à partir desquelles toute communication serait automatiquement approuvée ou bloquée. Ce type de renseignement est généralement éphémère et disponible en très grand nombre, d'où la nécessité de le traiter automatiquement plutôt que de le soumettre à une analyse humaine. En règle générale, cette forme de renseignement est hautement exploitable et est utilisée par le personnel opérationnel, tel que les intervenants en cas d'incident, pour s'assurer que les contrôles et les processus techniques sont préparés et mis en place.

PARTIES PRENANTES/CONSOMMATEURS

- Analyste SOC
- Analyste informatique
- Gestion des vulnérabilités
- Architectes de sécurité (pour les intégrations)

Recorded Future®

Aucune de ces catégories n’est intrinsèquement « meilleure » que les autres. Au lieu de cela, elles peuvent être utilisées côte à côte pour former une capacité cohérente de renseignement sur les menaces. En fonction de ses besoins et de ses capacités, une organisation peut décider de ne consommer dans un premier temps que du renseignement technique
ou tactique sur les menaces, car c’est celui qui est le plus facilement disponible. Toutefois, les besoins évoluant
au fil du temps, la plupart des organisations élargiront les types de renseignement sur les menaces qu’elles ingèrent, d’où l’importance de choisir un fournisseur qui propose plusieurs catégories et qui peut les accompagner dans
leur démarche de renseignement sur les menaces.

QUESTIONS À POSER À UN FOURNISSEUR :

- ↳ Fournissez-vous du renseignement dans ces trois catégories ? Pouvez-vous me montrer des exemples ?
- ↳ Dans quel type de renseignement investissez-vous le plus ?

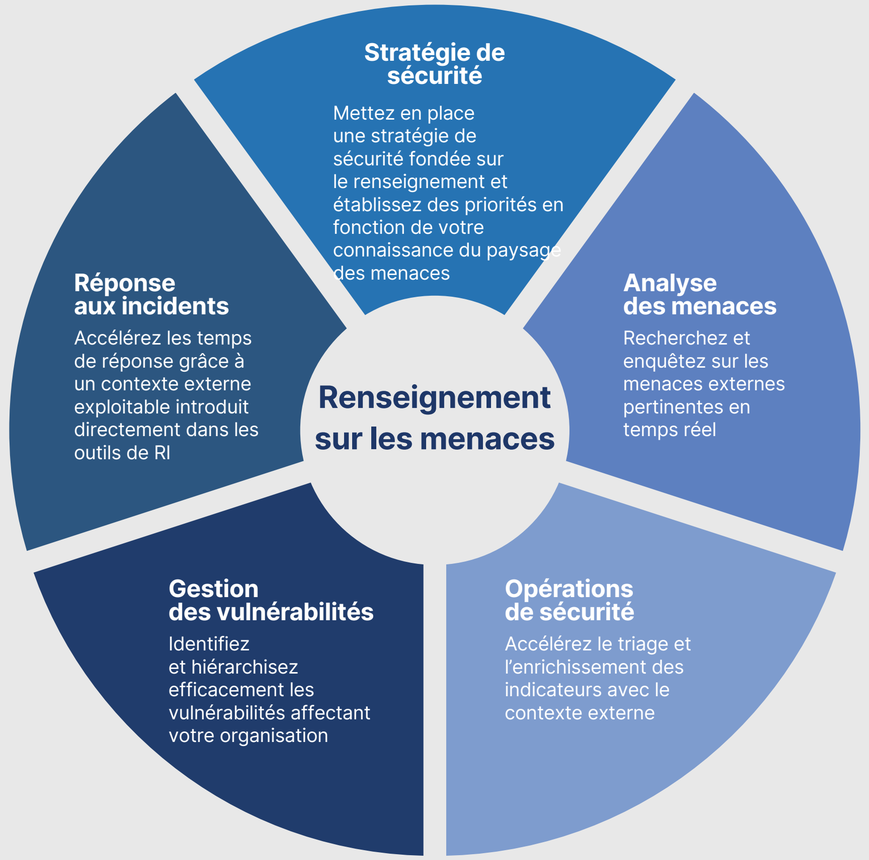
Recorded Future®

Qui devrait utiliser le renseignement sur les menaces ?

Au plus haut niveau, les décideurs en matière de sécurité ont traditionnellement évalué et quantifié le risque lié aux menaces auxquelles ils sont confrontés en se basant uniquement sur des facteurs internes, les tendances du secteur ou ce qu'ils lisent dans les journaux. Le renseignement sur les menaces permet de comprendre les menaces actuelles et émergentes qui concernent exclusivement votre organisation ou votre secteur d'activité, et la manière dont elles affectent votre stratégie de sécurité globale et votre prise de décision.

Par ailleurs, les équipes de votre organisation de sécurité peuvent bénéficier d'une prise de décision plus éclairée et de perspectives uniques. Le renseignement qui peut être facilement consommé et compris a le potentiel de révolutionner la façon dont les différents rôles au sein de votre organisation fonctionnent au quotidien.

Le diagramme de droite montre des exemples de la façon dont différentes équipes au sein d'une organisation utilisent le renseignement sur les menaces. Ce diagramme est conçu pour vous donner une idée des équipes et des utilisations les plus courantes du renseignement, mais ce ne sont pas les seules équipes qui pourraient bénéficier du renseignement :



QUESTIONS À POSER À UN FOURNISSEUR :

- ↳ Comment votre renseignement et votre produit peuvent-ils soutenir les différentes équipes de mon organisation, tant les décideurs que le groupe de sécurité ?
- ↳ Qui sont les consommateurs typiques du renseignement de votre produit ?

Avec qui le renseignement sur les menaces doit-il être partagé ?

Ce qui n'est pas assez évoqué dans le cadre du renseignement sur les menaces, c'est la collaboration
entre les équipes autres que celles chargées de la cybernétique et de la sécurité. Il existe de nombreuses équipes différentes au sein d'une organisation qui peuvent bénéficier du renseignement sur les menaces. Certaines des équipes avec lesquelles j'aime travailler sont celles des communications marketing pour la surveillance de la marque, notre équipe de gestion des risques des tiers en ce qui concerne les violations des tiers, ainsi que votre équipe BCPDR en cas de catastrophe
et de nombreuses autres équipes non techniques avec lesquelles le renseignement sur les menaces doit interagir.

– Christopher Martinkus, Responsable du renseignement sur les menaces, Banque commerciale de taille moyenne

Recorded Future®

Quels sont les types de sources à partir desquelles un fournisseur de renseignements sur les menaces doit collecter des informations ?

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

Tout fournisseur de renseignement sur les menaces que vous choisissez doit avoir accès à plusieurs ou à toutes les sources suivantes :

- Forums
- Flux de menaces
- Paste Sites
- Dark Web
- Actualités
- Réseaux sociaux et blogs traditionnels et alternatifs
- Dépôts de codes
- Données techniques, notamment télémétrie du réseau, DNS passif, flux net, données sur les points d'extrémité, etc.
- Sources de langues étrangères
- Renseignement fini créé par le fournisseur

Vous constaterez peut-être aussi que certains fournisseurs se spécialisent dans la production de renseignements à partir de sources particulières, comme les réseaux sociaux ou le dark web. C'est une bonne chose, mais cela ne fournit pas nécessairement le contexte ou une vue d'ensemble permettant d'enquêter efficacement sur une menace ou d'y faire face.

Pour la plupart des organisations, c'est la combinaison de toutes ou de la plupart des sources susmentionnées qui se révèle la plus efficace. L'intégration et l'analyse de données provenant de sources multiples peuvent vous fournir des informations uniques, un contexte approfondi et une vision équilibrée qui ne peuvent être obtenus d'aucune autre manière. Si vous dépendez trop d'une ou deux sources de données, vous risquez de rater des occasions et, en fin de compte, de fausser les perspectives.

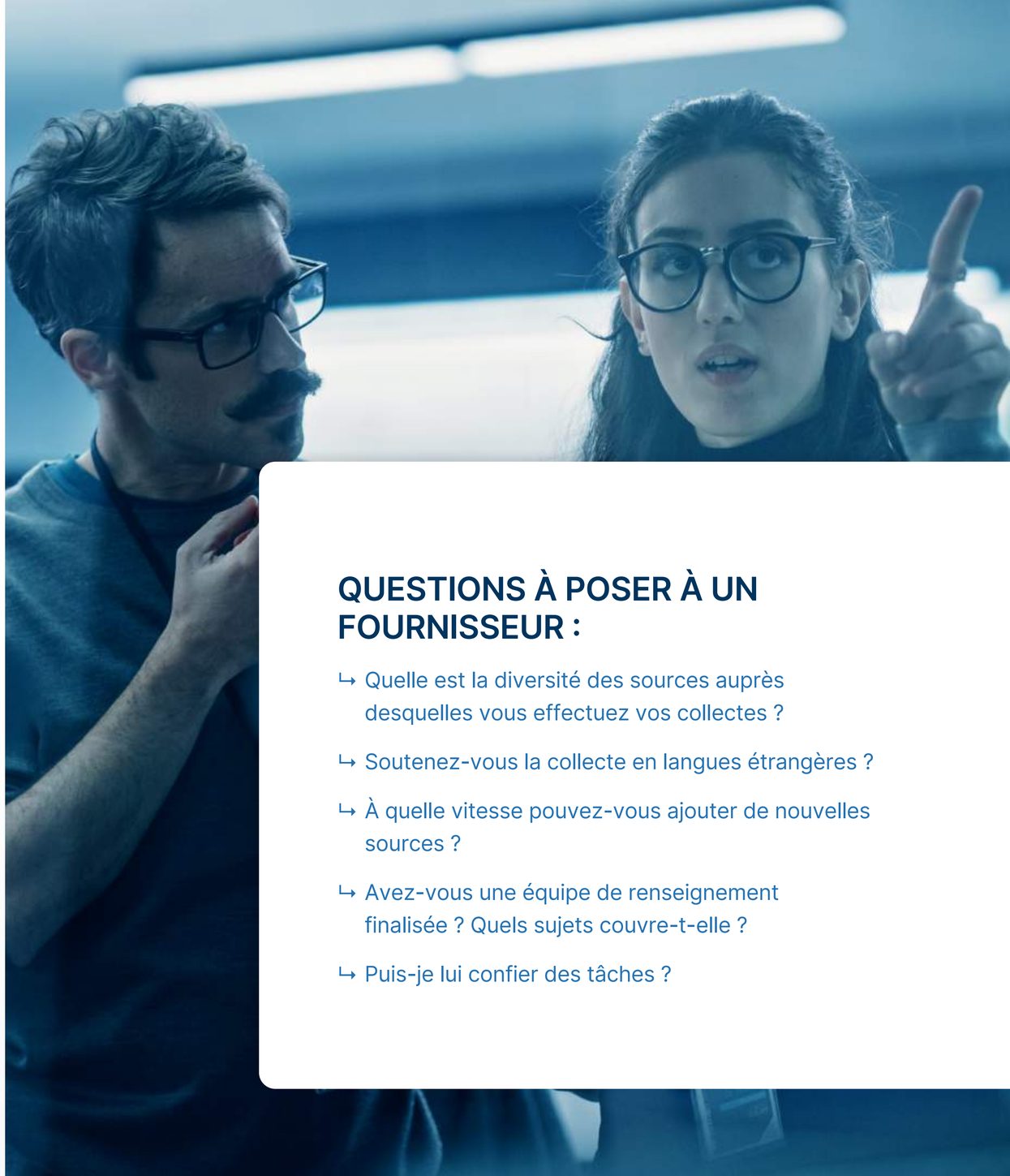
Recorded Future®

Par exemple, si vous n'ingérez que des flux de menaces open source, vous n'aurez pas le contexte nécessaire pour prendre des décisions éclairées. Les questions qui se posent à la suite de l'utilisation ou de la limitation de sources dépourvues de contexte sont les suivantes :

- Comment déterminer, parmi les milliers de vulnérabilités découvertes chaque année, celles qui doivent être corrigées en priorité ?
- Devez-vous agir immédiatement, plutôt que d'attendre la prochaine période de maintenance planifiée ?
- Comment pouvez-vous justifier auprès du propriétaire de l'entreprise que son actif doit être mis hors ligne pour y remédier ?

Recherchez des solutions qui ajoutent ce type de contexte pour vous donner des indications claires sur les risques qui peuvent être appliquées à votre stratégie de sécurité plus large.

Lorsque vous évaluez la solution qui vous permettra le mieux d'atteindre vos objectifs, il est essentiel de prendre en compte l'équilibre entre les sources de données et les informations fournies par chacune d'entre elles. 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 aussi d'une solution qui contextualise et hiérarchise les alertes pertinentes tout en éliminant le bruit.



QUESTIONS À POSER À UN FOURNISSEUR :

↳ Quelle est la diversité des sources auprès desquelles vous effectuez vos collectes ?

↳ Soutenez-vous la collecte en langues étrangères ?

↳ À quelle vitesse pouvez-vous ajouter de nouvelles sources ?

↳ Avez-vous une équipe de renseignement finalisée ? Quels sujets couvre-t-elle ?

↳ Puis-je lui confier des tâches ?

Recorded Future®

Comment dois-je mesurer la valeur d'une solution de renseignement sur les menaces ?

Dans une étude réalisée par l'université Johns-Hopkins pour le compte de CISA, les chercheurs ont cherché à répondre à la question suivante : « Comment une organisation peut-elle évaluer un produit, un service ou un flux et les coûts associés pour déterminer quelle solution correspond le mieux aux exigences de l'organisation ? »

Ils ont découvert que le meilleur indicateur de la valeur d'un fournisseur de renseignements sur les menaces est la pertinence et l'utilité de ce renseignement.

> « Il y a deux domaines à considérer pour évaluer la valeur potentielle d'un flux CTI : la pertinence et la facilité d'utilisation. Cependant, la plupart des organisations se concentrent uniquement sur la pertinence. Bien qu'il soit important de déterminer si une offre est pertinente, cela ne suffit pas. L'organisation / le client / le consommateur doit également s'assurer que l'information est utilisable et applicable dans son environnement ; qu'elle est exploitable et peut être utilisée pour conduire les processus opérationnels et les décisions en temps opportun avec un impact minimal sur les ressources locales. »[2]

Son renseignement sur les menaces est-il pertinent ?

- **Applicable :** le renseignement du fournisseur contient des informations directement liées aux menaces et aux risques pertinents pour l'organisation et le secteur.
- **Précis :** une organisation doit s'assurer que le renseignement qu'elle obtient est suffisamment précis pour la façon dont elle a l'intention de l'utiliser.
- **Rapide :** les informations fournissent un aperçu des menaces à temps pour que l'organisation puisse prendre des décisions pertinentes en matière de risques.

Le renseignement sur les menaces est-il utilisable ?

- **Lisible par machine :** les données sont fournies dans un format structuré qui peut être traité de manière automatisée.
- **Consommable :** les données peuvent être consultées et converties en informations utilisées par les processus opérationnels en temps voulu.
- **Exploitable :** les données peuvent être converties en informations qui sont utilisées directement par les processus de prise de décision dans le délai où la prise de décision a de la valeur.

[2] CISA. Évaluation de la valeur potentielle des flux de renseignement sur les cybermenaces (CTI)

Recorded Future®

EST-CE PERTINENT ?

APPLICABLE

Menaces d'intérêt ?

Quelles/qui sont les sources de menace pour le prestataire ?

PRÉCIS

Quel est le degré de bruit de l'information ?

Quel est leur degré de confiance ?

Savez-vous comment ils obtiennent certains contenus ?

RAPIDE

Combien de temps faut-il pour générer les informations ?

À quelle vitesse sont-elles partagées ?

EST-IL UTILISABLE ?

LISIBLE SUR MACHINE

Qu'est-ce que l'infrastructure de partage ?

Pouvez-vous y accéder de manière automatisée ?

CONSOMMABLE

Pouvez-vous accéder et injecter dans les processus opérationnels de manière automatisée ?

Les informations sont-elles cohérentes dans leur utilisation et leur existence ?

EXPLOITABLE

Pouvez-vous utiliser les informations pour prendre des décisions opérationnelles en temps utile ?

Recorded Future®

Dois-je créer des besoins prioritaires en renseignement (PIR) avant d'acheter une nouvelle solution de renseignement sur les menaces ?

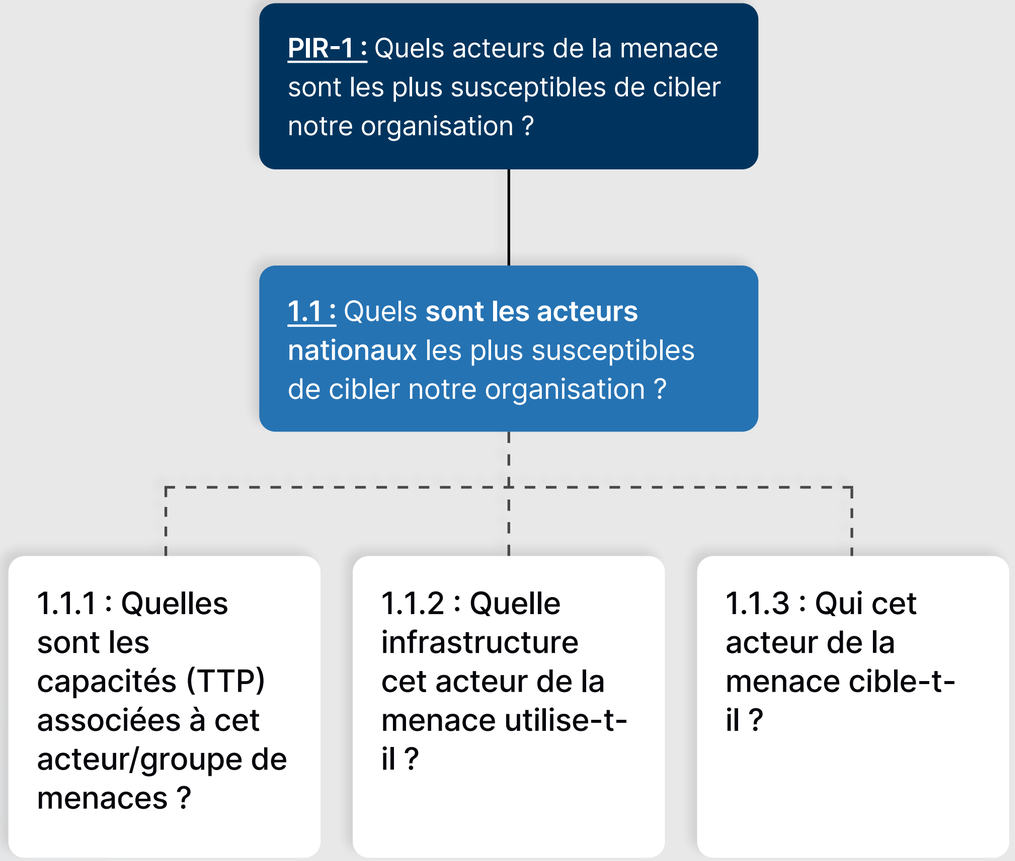
La réponse courte est oui, mais laissez-nous approfondir ce sujet : les besoins prioritaires en renseignement (PIR) aident les organisations à déterminer les questions auxquelles il est essentiel de répondre pour assurer le succès global de l'organisation. Au lieu d'examiner chaque risque avec la même intensité, ils aident les organisations à concentrer leurs efforts de renseignement sur les menaces et les risques les plus critiques et les plus pertinents.

Ces exigences permettent à votre public de savoir ce qu'il doit savoir pour agir et, plus important encore, elles permettent à vos analystes de savoir à quelles questions il faut répondre.

Ces besoins vous facilitent également la vie, car ils vous permettent de savoir ce qui est important pour les responsables. Ainsi, lorsque vous ne savez plus où donner de la tête, vous savez ce qui doit être priorisé par rapport à autre chose.

- Voici quelques exemples de besoins prioritaires en renseignement :
  - Quels acteurs de la menace sont les plus susceptibles de cibler notre organisation ?
  - Quelles menaces pèsent sur la marque de mon organisation ?
  - Comment l'infrastructure numérique de mon organisation est-elle vulnérable à l'exploitation ?
  - À quels risques sommes-nous confrontés en raison de notre chaîne d'approvisionnement ou de nos partenariats avec des fournisseurs tiers ?
  - À quelles menaces de sécurité majeures notre industrie/nos industries est-elle (sont-elles) confrontée(s) ?

L'élaboration de vos PIR avant l'intégration d'une nouvelle solution de renseignement sur les menaces peut vous aider à identifier les moyens par lesquels un fournisseur peut répondre à vos besoins et à évaluer les fournisseurs qui apportent le plus de valeur à votre équipe.



Recorded Future®

Comment puis-je consommer du renseignement sur les menaces ?

- **Plateforme de renseignement complète :** contrairement aux agrégateurs de flux, les fournisseurs de renseignements fournissent des données sur les menaces (y compris tous les types de flux) et des informations collectées à partir de sources ouvertes, techniques et du dark web, en utilisant une combinaison de techniques d'apprentissage automatique, y compris le traitement automatique du langage naturel (NLP). Les informations collectées sont utilisées pour produire un renseignement pertinent et exploitable à grande échelle, qui est généralement diffusé aux utilisateurs via un portail basé sur SaaS qui permet d'effectuer des requêtes et des analyses approfondies, ou via des alertes personnalisées. Des solutions de pointe offriront également des services de renseignement humain alimentés par leur technologie.

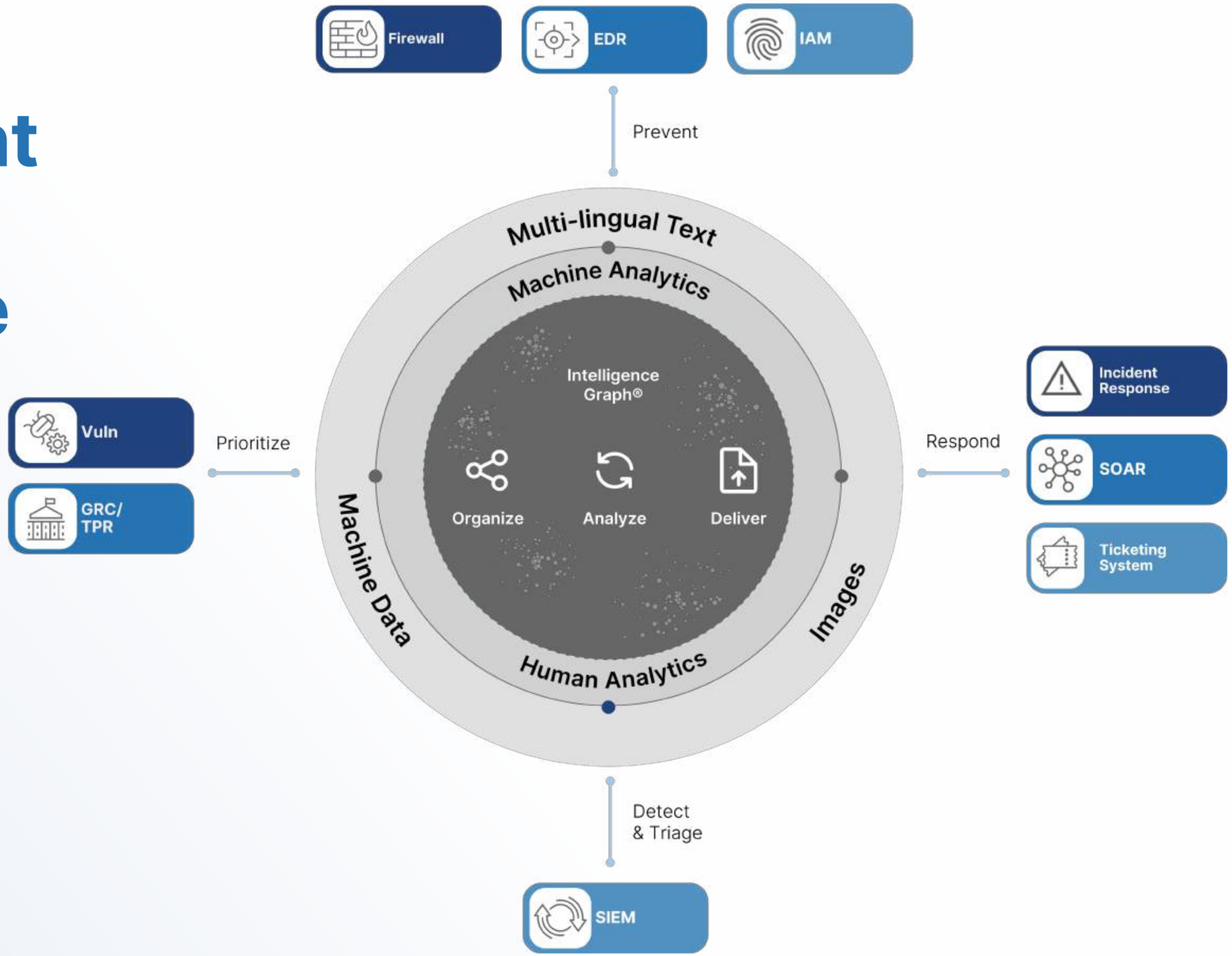
- **Intégrations directes avec les outils de sécurité et les API :** les équipes de sécurité doivent pouvoir obtenir du renseignement directement dans les outils qu'elles utilisent grâce à des intégrations prêtes à l'emploi avec les SIEM, les plateformes SOAR, la gestion des vulnérabilités, les points d'extrémité, les tickets, l'analyse des liens, et bien plus encore. Les équipes de sécurité avancées pourraient également tirer parti d'une API pour développer les intégrations existantes ou pour créer des intégrations spécialisées dans le renseignement sur les menaces avec leurs produits de sécurité et leurs flux de travail personnalisés ou propriétaires.

- **Renseignement finalisé :** la rédaction de rapports est l'une des fonctions les plus chronophages d'une équipe de sécurité. Avec le renseignement sur les menaces, vous pouvez externaliser la production de rapports de renseignement en utilisant des rapports de renseignement finalisés et rédigés par un fournisseur de renseignement.

- **Services gérés :** au lieu de recevoir des alertes directement, un fournisseur de sécurité consommera des quantités considérables d'informations pour vous. S'il estime que votre organisation est concernée, vous en serez informé par l'intermédiaire d'un service de signalement, généralement via un portail en ligne, et il vous aidera à prendre les mesures qui s'imposent. Par ailleurs, si le fournisseur identifie des sites web frauduleux, des noms de domaine de réseaux sociaux ou des domaines de typosquattage, il les fera supprimer en votre nom.

Recorded Future®

Le renseignement rend vos outils de sécurité plus intelligents



Recorded Future®

Par où commencer ?

Obtenez le soutien de l'équipe de direction

Les dirigeants et autres responsables doivent évaluer et gérer les risques en équilibrant les ressources disponibles limitées et la nécessité de protéger leur organisation contre des menaces en constante évolution. Pour obtenir le soutien de la direction, il faut qu'elle comprenne que le renseignement sur les menaces permet de cartographier le paysage des menaces, de calculer les risques et de donner au personnel de sécurité le contexte nécessaire pour prendre de meilleures décisions, plus rapidement.

Aujourd'hui, les responsables de la sécurité sont chargés des tâches suivantes :

- Évaluer les risques commerciaux et techniques, y compris les menaces émergentes et les « inconnues connues » susceptibles d'avoir un impact sur l'entreprise
- Identifier les bonnes stratégies et technologies pour atténuer les risques
- Communiquer la nature des risques à direction et justifier les investissements dans des mesures défensives

Le renseignement sur les menaces aide les leaders dans toutes ces activités et constitue une ressource essentielle, fournissant des informations sur les tendances générales, telles que :

- Quels types d'attaques deviennent plus (ou moins) fréquentes ?
- Quels types d'attaques coûtent le plus cher aux victimes ?
- Quels nouveaux types d'acteurs de la menace se manifestent et quels actifs et entreprises ciblent-ils ?
- Quelles pratiques et technologies de sécurité se sont avérées les plus (ou les moins) efficaces pour arrêter ou atténuer ces attaques ?

Recorded Future®

Obtenir le soutien de la direction en matière de sécurité

Le renseignement sur les menaces permet également aux équipes de sécurité d'évaluer si une menace émergente
est susceptible d'affecter leur entreprise spécifique sur la base de facteurs tels que :

- **Industrie :** la menace affecte-t-elle d'autres organisations de notre secteur ?
- **Technologie :** la menace implique-t-elle de compromettre les logiciels, le matériel ou d'autres technologies utilisées dans notre entreprise ?
- **Géographie :** la menace cible-t-elle les installations dans les régions où nous ou nos fournisseurs exerçons des activités ?
- **Méthode d'attaque :** les méthodes utilisées dans l'attaque, y compris l'ingénierie sociale et les méthodes techniques, ont-elles été utilisées avec succès contre notre entreprise ou des entreprises similaires ?

Grâce à ce niveau de renseignement, recueilli à partir d'un large éventail de sources de données externes, les décideurs en matière de sécurité sont en mesure d'obtenir une vision holistique du paysage global des risques et de hiérarchiser les risques les plus importants pour leur entreprise.

Voici cinq domaines clés que vous pouvez présenter aux responsables de la sécurité pour les aider à comprendre la valeur qu'apporte le renseignement car il leur permet d'être mieux informés et sensibilisés aux risques qui pèsent sur leur organisation :

- **Évaluer les risques :** face à la multiplicité des menaces cybernétiques, physiques, d'influence et même de la chaîne d'approvisionnement, il est difficile de savoir quelles sont celles dont vous devez vous préoccuper et ce que vous devez faire pour les contrer. Le renseignement sur les menaces aide les dirigeants à évaluer les menaces dans le contexte du risque pour leur entreprise, afin qu'ils puissent donner la priorité aux vecteurs de menace et aux acteurs qui peuvent réellement nuire à leur personnel et à leurs actifs, et cesser de perdre du temps et des ressources sur des menaces qui n'ont pas d'importance.
- **Atténuation des menaces :** le renseignement sur les menaces aide les responsables de la sécurité à classer par ordre de priorité les vulnérabilités et les faiblesses que les acteurs de la menace sont le plus susceptibles de cibler, en fournissant un contexte sur les TTP que ces acteurs utilisent, et donc les faiblesses qu'ils ont tendance à exploiter.
- **Communication :** les RSSI sont souvent contraints de décrire les menaces et de justifier les contre-mesures en des termes qui motiveront les chefs d'entreprise non techniques, tels que le coût, l'impact sur les clients et les nouvelles technologies à mettre en œuvre. Le renseignement sur les menaces offre de puissantes munitions pour ces discussions, telles que l'impact d'attaques similaires sur des entreprises de même taille dans d'autres secteurs ou des tendances et du renseignement provenant du dark web indiquant que l'entreprise est susceptible d'être ciblée, ou que des fournisseurs de la chaîne d'approvisionnement ont été mentionnés sur des sites d'extorsion de ransomwares.
- **Soutenir le leadership :** le renseignement sur les menaces peut fournir aux responsables de la sécurité une image en temps réel des dernières menaces, tendances et événements, ce qui les aide à répondre à une menace ou à communiquer l'impact potentiel d'un nouveau type de menace aux chefs d'entreprise et aux membres du conseil d'administration de manière opportune et efficace.
- **Réduire le déficit de compétences en matière de sécurité :** les RSSI doivent s'assurer que l'organisation informatique dispose du capital humain nécessaire pour mener à bien sa mission. Mais en raison de la pénurie de compétences dans le domaine de la cybersécurité, le personnel de sécurité existant est souvent soumis à une charge de travail ingérable. Le renseignement sur les menaces automatise certaines des tâches les plus gourmandes en main-d'œuvre, en collectant rapidement des données et en mettant en corrélation le contexte de plusieurs sources de renseignement, en hiérarchisant les risques et en réduisant le nombre d'alertes inutiles. Un renseignement puissant sur les menaces permet également au personnel débutant de se perfectionner rapidement et de réaliser des performances supérieures à son niveau d'expérience.

Recorded Future®

Conclusion

Que vous soyez novice en matière de renseignement sur les menaces et que vous envisagiez d'ajouter une solution de renseignement sur les menaces à votre pile technologique de cybersécurité, ou que vous soyez à la recherche de nouvelles stratégies à envisager pour votre programme, nous espérons que ce guide de l'acheteur vous a été utile.

Chez Recorded Future, nous sommes convaincus que le renseignement sur les menaces est le multiplicateur de force essentiel pour la pile de sécurité moderne, qui permet aux organisations d'atténuer les attaques rapides d'aujourd'hui en fournissant des informations précieuses sur lesquelles agir rapidement.

Si vous souhaitez en savoir plus sur Recorded Future, la plateforme cloud de renseignement sur les menaces la plus complète et la plus indépendante du marché, réservez une démonstration ou parlez-en à votre gestionnaire de compte.

Recorded Future®

Les avantages de Recorded Future pour les équipes de sécurité

- **Évaluation des risques :** les client de Recorded Future indiquent une **augmentation de 61 %** de la visibilité sur les menaces potentielles
- **Atténuation des menaces :** les clients déclarent être **48 % plus rapides** dans l'identification d'une nouvelle menace
- **Communication :** les clients indiquent avoir économisé **9,2 heures** par utilisateur et par semaine sur les recherches et la chasse aux menaces
- **Assistance à la direction : 90 % des clients** déclarent mieux comprendre le paysage des menaces
- **Réduction de l'écart de compétences en matière de sécurité :** les clients indiquent que **21 % du travail** qui, avant l'utilisation de Recorded Future, ne pouvait être effectué que par des analystes seniors, peut désormais être confié à des analystes juniors.

La hyérarchisation donne à l'équipe un pouvoir « prophétique »

« le renseignement sur les menaces de Recorded Future donne à notre équipe un pouvoir prophétique.
Nous sommes en mesure de dire : « Il y a quelque chose dont nous devons nous préoccuper, alors sensibilisons-nous à
ce sujet », et bien sûr, cette chose que nous avons identifié ne tarde pas à se produire un mois ou deux plus tard. Le fait que Recorded Future nous donne un coup de pouce dès le début nous permet de prendre les devants lorsque quelque chose se prépare. »

– Alex Minster, Ingénieur en sécurité chez Kyriba

Recorded Future®

À propos de Recorded Future

Recorded Future est la plus grande entreprise de renseignement sur les menaces au monde. L'Intelligence Cloud de Recorded Future fournit des renseignements de bout en bout sur les adversaires, l'infrastructure et les cibles. En indexant Internet à travers l'open web, le dark web et les sources techniques, Recorded Future fournit une visibilité en temps réel sur une surface d'attaque et un paysage de menaces en expansion, permettant aux clients d'agir rapidement et en toute confiance afin de réduire les risques et de poursuivre leurs activités. Avec son siège à Boston et des bureaux et des employés dans le monde entier, Recorded Future travaille avec plus de 1 800 entreprises et organisations gouvernementales dans plus de 75 pays pour fournir un renseignement en temps réel, impartial et exploitable

Pour en savoir plus, visitez recordedfuture.com