LE

MANUEL DU RENSEIGNEMENT SUR LA SÉCURITÉ

TROISIÈME ÉDITION

Comment perturber vos adversaires et diminuer les risques grâce au renseignement sur la sécurité

Préface de Dr Christopher Ahlberg

À propos de Recorded Future

Recorded Future fournit le renseignement sur la sécurité le plus perfectionné du monde, sur le plan technique, pour perturber vos adversaires, armer vos défenseurs et protéger votre entreprise. La plate-forme proactive et prédictive de Recorded Future transmet en temps réel un renseignement d'élite exploitable, intuitif, riche en contexte et prêt à être intégré dans l'ensemble de votre écosystème de sécurité.

recordedfuture.com

Le manuel du renseignement sur la sécurité

Troisième édition

Comment perturber vos adversaires et diminuer les risques avec le renseignement sur la sécurité

Revu par Jeff May
Couverture et dessins de Lucas Clauser
Préface de Dr Christopher Ahlberg

CYBEREDGE
PRESS

Le manuel du renseignement sur la sécurité, troisième édition

Publié par:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
+1 (800) 327-8711
www.cyber-edge.com

ISBN : 978-1-948939-15-7 (livre de poche)
ISBN : 978-1-948939-16-4 (livre électronique)

Imprimé aux États-Unis d'Amérique

10 9 8 7 6 5 4 3 2 1

Remerciements de l'éditeur

Le CyberEdge Group remercie les personnes suivantes pour leurs contributions respectives :

Rédactrice en chef : Susan Shuttleworth
Conception graphique : Debbi Stocco
Coordinatrice de la production : Jon Friedman

Remerciements

Ce livre a pu être publié grâce au personnel de Recorded Future qui a fait part de ses idées et de son expertise pour cette troisième édition, ainsi que pour les éditions précédentes, notamment, **Lucas Clauser** (concepteur), **Brendan Gibson** (collaborateur), **Levi Gundert** (collaborateur), **Allan Liska** (collaborateur), **Jeff May** (rédacteur), **Maggie McDaniel** (collaboratrice), **Zane Pokorny** (ancien rédacteur et collaborateur), **John Wetzel** (collaborateur) et **Ellen Wilson** (collboratrice).

Avant-propos de Dr Christopher Ahlberg, cofondateur et PDG de Recorded Future.

Table des matières

Préface de la troisième édition

À la fin de 2019, je me suis rendu compte de deux choses.

La première : Il n'y a jamais eu de meilleur moment pour être un cybercriminel.

La seconde : Seules les équipes de défenseurs qui se concentrent sur la perturbation proactive de leurs adversaires gagneront la partie.

Dans les mois qui ont suivi, ces deux théories se sont avérées correctes.

Toute personne souhaitant faire du tort à une entreprise peut mettre en danger ses données les plus sensibles en achetant des outils standard et en accédant facilement à des marchés clandestins.

Les vulnérabilités héritées, l'absence de processus de développement de code sécurisé, la croissance explosive des appareils connectés et la décimation complète des périmètres organisationnels ont poussé à bout, et parfois totalement submergé, les équipes de sécurité.

En mars 2020, la pandémie COVID-19 a forcé les entreprises à renvoyer leur main-d'œuvre chez elle pendant des mois avec peu voire aucune possibilité d'implémenter des contrôles de sécurité à distance. Pour compliquer les choses, il n'y a pas d'organismes gouvernementaux, pas de front unifié, qui protègent les intérêts des organisations contre les auteurs de menaces, que ceux-ci soient de simples malfaiteurs ou des États-nations.

Alors, comment vos équipes de sécurité survivent-elles et continuent-elles à défendre votre entreprise lors de périodes comme celles-ci ?

Le renseignement sur la sécurité est une approche axée sur les résultats visant à diminuer les risques, qui combine les informations internes et externes sur les menaces, la sécurité et les perspectives commerciales pour l'ensemble de l'entreprise. Il est facile de l'adapter à la taille, à la maturité et aux besoins spécifiques de l'entreprise. Depuis ses débuts, la capacité de recueil, de structure, d'analyse et de transmission de toutes les informations de sécurité pertinentes figurant sur Internet est ce qui distingue Recorded Future. Désormais, nous segmentons cette capacité pour répondre aux besoins spécifiques de chaque solution de sécurité.

En septembre 2020, Recorded Future a annoncé l'adaptation de sa plate-forme de renseignement sur la sécurité pour relever les défis de chaque fonction de sécurité. Les six modules individuels que nous proposons constituent une source unique de renseignement fiable et personnalisé, qui permet aux utilisateurs de maintenir souplesse et précision dans leurs décisions en matière de sécurité. Selon leur rôle, les utilisations cibles et les résultats ciblés, ces solutions incluent le module Renseignement sur la marque, le module Renseignement pour les SecOps, le module Renseignement sur les menaces, le module Renseignement sur la vulnérabilité, le module Renseignement sur les tiers et le module Renseignement géopolitique.

Le renseignement géopolitique est la dernière innovation ajoutée à la plate-forme de renseignement Recorded Future. Cette solution accélère la prise de décision critique grâce au renseignement contextuel Open Source (OSINT) sur les menaces et les tendances géopolitiques, permettant aux utilisateurs de protéger leurs actifs et de comprendre l'évolution de la dynamique des zones géographiques pertinentes pour leur entreprise. L'élimination des recherches manuelles et l'émergence de renseignement en temps réel permet aux utilisateurs de défendre leurs actifs partout dans le monde grâce à une vue complète du panorama des menaces physiques et cybernétiques pesant sur leur entreprise.

À la fin de 2019, nous avons présenté les trois principes d'un renseignement sur la sécurité efficace. En 2020, nous en avons ajouté un quatrième. Il est rapidement passé au numéro un de notre liste :

1. Vous devez vous concentrer sur la perturbation des adversaires les plus susceptibles de vous cibler et leur rendre la vie la plus difficile possible. Le renseignement sur la sécurité est la façon la plus efficace d'y parvenir.

2. Le renseignement sur la sécurité doit fournir le contexte à point nommé, clair et exploitable, nécessaire pour prendre des décisions rapides et éclairées, ainsi que les mesures efficaces appropriées pour relever chaque défi de sécurité. Le renseignement doit vous parvenir au moment opportun et sous forme compréhensible, et amplifier l'impact des solutions existantes. Il doit enrichir vos connaissances, ne pas compliquer le processus de prise de décision et faire en sorte que tout le personnel de votre entreprise soit sur la même longueur d'onde.

3. Les gens et les machines travaillent mieux quand ils collaborent. Les machines sont capables de traiter et de classer les données brutes de façon exponentiellement plus rapide que les êtres humains. En revanche, les êtres humains sont nettement plus aptes à effectuer une analyse intuitive et globale que toute intelligence artificielle, tant qu'ils ne sont pas submergés par le tri d'énormes ensembles de données et par des recherches fastidieuses. Quand êtres humains et machines sont appariés, chacun fonctionne plus intelligemment, ce qui permet d'économiser du temps et de l'argent, de diminuer l'épuisement du personnel et d'améliorer la sécurité dans son ensemble.

4. Le renseignement sur la sécurité est pour tout le monde. Quel que soit le rôle que vous jouiez en matière de sécurité, le renseignement vous permet de prendre de meilleures décisions plus rapidement. Il ne s'agit pas d'un domaine de sécurité distinct. C'est le contexte qui vous permet de travailler plus intelligemment, que vous soyez chargé d'affecter du personnel à un centre d'opérations de sécurité (SOC), de gérer des vulnérabilités ou de prendre des décisions de sécurité

de haut niveau. Toutefois, pour vous faciliter la tâche, pas la rendre plus complexe, le renseignement sur la sécurité devrait s'intégrer aux solutions et aux flux de travail que vous utilisez déjà et devrait être facile à mettre en œuvre.

Chez Recorded Future, nous croyons de tout cœur en ces principes fondamentaux, et notre approche a fait ses preuves au cours de l'année qui a suivi la parution de la première édition du présent manuel. Notre renseignement arrête les menaces dans les services de sécurité de 99 des 100 plus grandes entreprises de *Fortune* aux États-Unis, sans parler d'innombrables organisations de toutes tailles et d'institutions gouvernementales du monde entier. Et nous avons grandi : nous sommes passés à plus de 500 employés dans 40 pays.

Nous espérons que ce manuel jouera son rôle en offrant des informations pratiques et des conseils que vous pourrez appliquer dès aujourd'hui pour perturber les adversaires de votre organisation.

Je suis reconnaissant à tous ceux qui ont contribué au contenu de ce manuel : nos utilisateurs et nos clients, des experts du secteur et l'équipe de Recorded Future. Nous espérons que vous considérerez cette troisième édition de notre manuel comme un bon complément d'information lorsque vous intégrerez le renseignement pour la sécurité à votre écosystème de sécurité.

Dr Christopher Ahlberg
Cofondateur et PDG
Recorded Future

Introduction

Une image complète du renseignement sur la sécurité

Comme dans la parabole des aveugles et de l'éléphant, la plupart des gens n'ont qu'une compréhension limitée du renseignement sur la sécurité parce qu'ils ne connaissent qu'un aspect particulier de celui-ci.

Vous avez peut-être entendu dire que le renseignement sur la sécurité impliquait la collecte de données à partir d'une grande variété de sources, y compris de l'Internet clandestin. Vous savez peut-être aussi qu'il combine ces données aux perspectives des experts en cybersécurité et en distille du renseignement pour les professionnels de la sécurité informatique. Vous travaillez peut-être avec des flux de menaces ou des rapports hebdomadaires sur les attaques sur le réseau, ou même avec une analyse experte des cyber-risques. Cependant, il est peu probable que vous perceviez l'ensemble du large éventail de rôles et de fonctions pris en charge par le renseignement sur la sécurité, toutes les façons dont il protège les organisations et leurs actifs, ou l'intégralité de son potentiel de réduction des risques.

Ce manuel vous donnera une image complète de l'éléphant. Le début vous donnera un tour d'horizon du renseignement sur la sécurité et des phases de son cycle de vie. Au milieu, le livre examine les façons spécifiques dont le renseignement sur la sécurité renforce six fonctions de sécurité critiques et leurs flux de travail. Les derniers chapitres traitent de questions de gestion et de mise en œuvre, comme l'utilisation du renseignement sur la sécurité pour évaluer les risques et justifier les investissements. Ils abordent aussi les manières de mettre sur pied une équipe de renseignement sur la sécurité.

À la fin du livre, vous comprendrez comment le renseignement sur la sécurité renforce l'efficacité des équipes et des responsables de la sécurité en exposant les menaces

inconnues, en clarifiant les priorités, en fournissant des données pour prendre plus rapidement de meilleures décisions et en permettant une compréhension commune de la diminution des risques dans l'ensemble de l'entreprise.

Du renseignement sur les menaces au renseignement sur la sécurité

Jusqu'à il y a peu, les sujets abordés dans ce livre étaient habituellement appelés « renseignement sur les menaces ». En fait, la version précédente était intitulée *Le manuel du renseignement sur les menaces, deuxième édition*.

Toutefois, le terme « renseignement sur les menaces » est généralement associé à des informations sur les menaces pesant sur les systèmes informatiques traditionnels contrôlés par l'organisation elle-même. Cette conception du domaine est beaucoup trop étroite.

Les auteurs de menaces novateurs cherchent constamment à découvrir les points faibles et conçoivent de nouveaux moyens de pénétrer ou de contourner les défenses informatiques traditionnelles. Ils dérobent les informations d'identification de tiers de confiance et les utilisent pour pénétrer dans les systèmes de l'entreprise. Ils recueillent des informations personnelles à partir de plates-formes de réseaux sociaux pour lancer des campagnes de hameçonnage convaincantes et créer des sites Web de typosquatting afin d'usurper l'identité des marques et d'escroquer les clients. Ils planifient des cyberattaques et tirent parti d'événements physiques contre des sites éloignés du monde entier. Ils planifient des attaques qui, sans avertissement préalable, sont indétectables par les solutions de sécurité informatique traditionnelles.

Des experts en cybersécurité et des groupes informatiques visionnaires ont compris qu'ils devaient affronter les auteurs de menaces en découvrant leurs méthodes et en perturbant leurs activités avant les attaques. Cette prise de conscience les a poussés à étendre leurs programmes de renseignement en y incluant des domaines tels que les risques posés par les tiers (exposition par le biais de fournisseurs, de vendeurs et de partenaires commerciaux), la protection de la marque

(capacité de détecter et de résoudre les problèmes de sécurité qui menacent la réputation d'une entreprise), les risques géopolitiques (les menaces associées à l'emplacement des actifs physiques et des événements), et bien plus encore.

Aujourd'hui, les experts et les fournisseurs utilisent le terme « renseignement sur la sécurité » pour englober tout ce qui était auparavant appelé « renseignement sur les menaces », ainsi que les ajouts les plus récents au domaine. C'est pourquoi le livre que vous lisez actuellement est intitulé *Le manuel du renseignement sur la sécurité*.

Vous remarquerez peut-être également que nous avons révisé et réorganisé les informations des éditions précédentes afin de les aligner sur le concept du renseignement sur la sécurité. Voici quelques exemples de cette réorganisation.

- Nous avons prêté plus d'attention au fait que le renseignement sur la sécurité tire sa force de six fonctions de sécurité essentielles.
- Nous avons examiné de nouveaux cas d'utilisation et de moyens de recourir au renseignement sur la sécurité pour des activités telles que la réponse aux incidents et la chasse aux menaces proactive.
- Nous avons approfondi la description de la protection de marques
- Nous avons ajouté un nouveau chapitre sur les risques géopolitiques
- Nous avons inclus une description de l'utilisation d'un cadre de risques par catégorie de menaces (TCR) pour quantifier les menaces en fonction de leur impact monétaire sur une entreprise.

Nous espérons que ce manuel vous permettra de perturber vos adversaires et de diminuer les risques posés à votre organisation, ou, tout au moins, qu'il vous poussera à réfléchir à la signification du rôle de défenseur dans le panorama actuel.

— L'équipe de Recorded Future

Bref aperçu des chapitres

Section 1 : Que signifie « renseignement sur la sécurité » ?

Le chapitre 1, « Qu'est-ce que le renseignement sur la sécurité ? », décrit la valeur du renseignement sur la sécurité et les caractéristiques des programmes de renseignement sur la sécurité réussis.

Le chapitre 2, « Types et sources », traite des différences entre le renseignement opérationnel et le renseignement stratégique sur la sécurité, ainsi que des rôles des sources de données et de l'Internet clandestin.

Le chapitre 3, « Le cycle de vie du renseignement sur la sécurité », examine les phases du cycle de vie du renseignement sur la sécurité et la relation entre outils et analystes humains.

Section 2 : Applications du renseignement sur la sécurité

Le chapitre 4, « Le renseignement pour les opérations de sécurité, 1re partie : le triage », examine comment le renseignement fournit un contexte pour le triage et permet aux équipes chargées des opérations de sécurité de prendre plus rapidement de meilleures décisions.

Le chapitre 5, « Le renseignement pour les opérations de sécurité, 2e partie : la réponse », décrit comment le renseignement minimise la réactivité des réponses aux incidents et présente quatre exemple.

Le chapitre 6, « Le renseignement sur les vulnérabilités », examine comment le renseignement permet de hiérarchiser les vulnérabilités en fonction du risque véritable pour l'entreprise.

Le chapitre 7, « Le renseignement sur les menaces, 1re partie : comprendre les attaquants », explique la valeur de la recherche sur les tactiques, techniques et procédures des attaquants (TTP).

Le chapitre 8, « Le renseignement sur les menaces, 2e partie : l'analyse des risques »,analyse la valeur des modèles de risques et la manière dont le renseignement fournit des données fiables sur les probabilités d'attaque et leurs coûts.

Le chapitre 9, « Le renseignement sur les tiers », examine comment le renseignement est utilisé pour évaluer les partenaires de chaîne d'approvisionnement et diminuer les risques posés par les tiers.

Le chapitre 10, « Le renseignement sur la marque », passe en revue les différents types de risques numériques pour les marques et la manière comment le renseignement sur la sécurité permet aux équipes de sécurité de défendre la réputation de leur entreprise.

Le chapitre 11, « Le renseignement géopolitique », décrit comment le renseignement sur la sécurité émet des avertissements anticipés sur les menaces pesant sur les installations et les biens physiques, partout dans le monde.

Le chapitre 12, « Le renseignement sur la sécurité pour les responsables de la sécurité », examine comment le renseignement sur la sécurité permet aux responsables de la sécurité informatique (CISO), aux directeurs informatiques (CIO) et aux autres dirigeants d'obtenir une vue globale du panorama des cyber-risques et de prendre de meilleures décisions pour l'entreprise.

Section 3 : Création et mise à l'échelle de votre programme de renseignement sur la sécurité

Le chapitre 8, "Analyse des matrices de renseignement" **explique comment trois principales matrices de menaces fournissent des structures de réflexions sur les attaques.**

Le chapitre 14, « Votre parcours du renseignement sur la sécurité » fournit des suggestions sur la manière de mettre sur pied et d'agrandir un simple programme de renseignement sur la sécurité.

Le chapitre 15, « Le développement de l'équipe principale de renseignement sur la sécurité », décrit comment la création d'une équipe dévolue à cette tâche peut permettre au renseignement sur la sécurité d'atteindre un nouveau sommet.

Icônes utiles

Suggestions fournissant des conseils pratiques qui pourraient être utiles à votre entreprise.

Lorsque vous voyez cette icône, prenez-en bonne note car le contenu associé contient des informations essentielles à ne pas oublier.

Soyez prudent, sinon cela pourrait vous coûter très cher, ainsi qu'à votre entreprise.

Le contenu associé à cette icône est de nature plus technique et destinée aux informaticiens.

Vous souhaitez en savoir plus ? Rechercher du contenu apparenté en ligne.

Section 1 : Que signifie « renseignement sur la sécurité » ?

Chapitre 1

Que signifie « renseignement sur la sécurité » ?

Dans ce chapitre

- Comprenez l'importance du renseignement sur la sécurité
- Examinez les caractéristiques des programmes de renseignements de sécurité efficaces
- Découvrez qui sont les bénéficiaires du renseignement sur la sécurité

"Chaque bataille est gagnée avant d'être livrée"

— Sun Tzu

Visibilité des menaces avant qu'elles ne sévissent 3

Les cybermenaces revêtent de nombreuses formes. Dans certains cas, il s'agit certainement de cyber-criminels qui attaquent votre réseau au niveau du pare-feu. Cependant, elles incluent également des auteurs de menace opérant sur l'Internet ouvert et clandestin, qui vous attaquent par l'intermédiaire de vos employés et de vos partenaires commerciaux. Certaines ravagent votre marque par le biais de réseaux sociaux et de sites Web externes, sans jamais toucher votre réseau. Des initiés malveillants ou simplement négligents peuvent également ravager vos données et votre réputation.

Lorsque des indicateurs de ces menaces apparaissent sur votre réseau, il est probablement trop tard. Pour éviter les dommages, vous devez recevoir des avertissements anticipés des menaces, accompagnés de faits concrets exploitables afin de :

- ☑ Éliminer vos vulnérabilités les plus graves avant qu'elles ne soient exploitées
- ☑ Détecter les sondes et les attaques dès que possible, et réagir efficacement immédiatement
- ☑ Comprendre les tactiques, techniques et procédures (TTP) des attaquants probables et mettre en place des défenses efficaces
- ☑ Identifier et corriger les faiblesses de vos partenaires commerciaux en matière de sécurité, en particulier pour ceux qui ont accès à votre réseau
- ☑ Détectez les fuites de données et les usurpations de la marque de votre entreprise
- ☑ Effectuez des investissements judicieux dans la sécurité afin d'optimiser le retour sur investissement et de minimiser les risques

De nombreux services informatiques ont créé des programmes de renseignement pour obtenir les avertissements anticipés et les faits exploitables qu'il leur faut pour protéger leurs données et leurs marques. La figure 1-1 répertorie des mesures qui montrent les améliorations spectaculaires de la sécurité et de l'efficacité qu'un programme de renseignement sur la sécurité peut apporter.

Figure 1-1 : Un programme de renseignement sur la sécurité peut apporter des améliorations considérables à la sécurité et à l'efficacité opérationnelle. Source des données : IDC

Faits et analyses exploitables

Lorsque les gens parlent du renseignement sur la sécurité, ils font parfois référence à certains types de faits et de renseignements, et d'autres fois au processus qui les produit. Examinons le premier cas.

Plus que des données ou des informations

Même les professionnels de la sécurité utilisent parfois les mots « données », « informations » et « renseignement » de manière interchangeable, mais les distinctions sont importantes. La figure 1-2 illustre ces différences.

Les données consistent en faits et statistiques distincts recueillis pour une analyse plus approfondie.

Les informations sont des points de données multiples, combinés pour répondre à des questions spécifiques.

Le renseignement est le résultat d'une analyse des données et des informations qui présente des modèles et fournit un contexte vital pour éclairer la prise de décision.

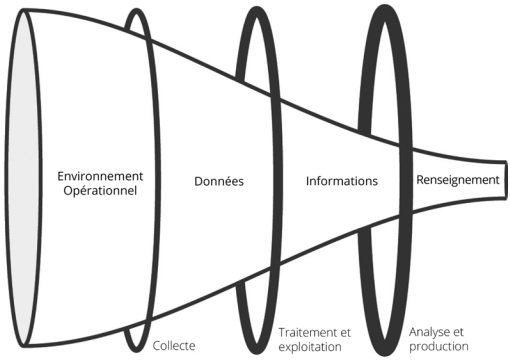


Figure 1-2 : La relation entre données, informations et renseignement

Bien sûr, les détails des données, des informations et du renseignement diffèrent selon qu'il s'agit de programmes politiques, militaires, économiques, commerciaux ou autres. Pour le renseignements sur la sécurité :

- ☑ Les données ne sont généralement que des indicateurs tels que des adresses IP, des URL ou des hachages. Les données ne nous disent pas grand-chose sans analyse.
- ☑ Les informations répondent à des questions comme : « Combien de fois mon entreprise a-t-elle été mentionnée sur les réseaux sociaux ce mois-ci ? » Bien qu'il s'agisse d'une sortie bien plus utile que les données brutes, elle ne permet pas, en elle-même, de prendre une décision éclairée sur des mesures spécifiques.

> ☑ Le renseignement consiste en perspectives factuelles fondées sur des analyses qui mettent en corrélation des données et des informations provenant de différentes sources afin de découvrir des modèles et d'ajouter des points de vue. Il permet aux personnes et aux systèmes de prendre des décisions éclairées et des mesures efficaces pour prévenir les violations, corriger les vulnérabilités, améliorer la sécurité de l'entreprise et réduire les risques.

L'idée que chaque instance de renseignement sur la sécurité est *exploitable* par un *public spécifique* est implicite dans la présente définition de « renseignement ». Autrement dit, le renseignement doit accomplir deux choses :

1. Indiquer des décisions ou des interventions spécifiques
2. S'adapter à une utilisation facile sur mesure par une personne, un groupe ou un système spécifique qui l'utilisera pour prendre une décision ou une mesure

Les sources de données qui ne sont jamais utilisées et les rapports qui ne sont jamais lus ne constituent pas du renseignement. Les informations, aussi précises qu'elles soient, ne le sont pas non plus si elles sont transmises à une personne qui ne peut pas les interpréter correctement ou qui n'est pas en mesure d'y donner suite.

Le renseignement sur la sécurité : le processus

Le renseignement sur la sécurité concerne aussi le processus selon lequel les données et les informations sont recueillies, analysées et diffusées dans l'ensemble de l'organisation. Les étapes de ce processus seront abordées dans le Chapitre 3, où nous décrivons le cycle de vie du renseignement sur la sécurité. Toutefois, il est important de souligner dès le début que les processus de renseignement sur la sécurité efficaces présentent quatre caractéristiques.

1. Un processus et un cadre collaboratifs

Dans de nombreuses entreprises, les activités de renseignement sur la sécurité sont cloisonnées. Par exemple, les équipes chargées des opérations de sécurité (SecOps), de la prévention de la fraude et de la gestion des risques posés par les tiers peuvent chacune disposer de leurs propres analystes et outils pour recueillir et analyser le renseignement. Cela mène à du gaspillage, à des doublons et à l'incapacité de partager les analyses et le renseignement. Les silos empêchent également l'évaluation des risques pour de l'entreprise et l'affectation de ressources de sécurité là où elles auront le plus grand impact. Les programmes de renseignement sur la sécurité doivent partager un processus et un cadre communs, permettre un grand accès aux informations et aux flux de travail opérationnels, encourager une vision globale des risques et prendre en compte l'affectation des ressources.

2. Une visibilité sous tous les angles

Les cyber-menaces pouvant provenir de n'importe où, les programmes de renseignement sur la sécurité nécessitent une visibilité omniprésente, notamment :

- ☑ Des événements de sécurité sur le réseau de l'entreprise
- ☑ Des flux de données sur les menaces traditionnels
- ☑ Ouvrez les forums Web sur lesquels des attaquants échangent des informations et des outils pour exploiter les vulnérabilités
- ☑ Des communautés de l'Internet clandestin où les pirates et les auteurs parrainés par des États partagent des techniques et planifient des attaques.
- ☑ Des marchés en ligne où les cybercriminels achètent et vendent des informations confidentielles
- ☑ Des comptes de réseaux sociaux où les auteurs de menaces usurpent l'identité de vos employés et contrefont vos produits

Désormais, de nombreuses entreprises se concentrent sur les sources de données de menaces classiques et sont désormais conscientes de la nécessité de scruter régulièrement une plus grande variété de sources et un plus grand nombre de sources.

3. Une Automatisation et une intégration de grande envergure

Vu la quantité de données et d'informations à capter, à corréler et à traiter, un programme de renseignement sur la sécurité nécessite un haut niveau d'automatisation pour réduire les efforts manuels et produire rapidement des résultats significatifs. Pour ajouter un contexte aux constatations initiales et diffuser efficacement le renseignement, les programmes réussis de renseignement sur la sécurité doivent également s'intégrer à de nombreux types de solutions de sécurité, comme les tableaux de bord de sécurité, les solutions de gestion des informations sur la sécurité et des événements (SIEM), les systèmes de gestion des vulnérabilités, les pare-feu et les outils d'orchestration, d'automatisation et de réponse (SOAR).

4. Un alignement sur l'entreprise et sur les cas d'utilisation de la sécurité

Les entreprises gaspillent parfois d'énormes ressources pour capter et analyser des informations hors de propos. Un programme réussi de renseignement sur la sécurité doit déterminer et documenter ses besoins en matière de renseignement pour s’assurer que les activités de collecte et de traitement s’harmonisent avec les priorités réelles de l’organisation. L'alignement implique également l'adaptation du contenu et du format du renseignement pour faciliter son utilisation par des employés et des systèmes.

Quels sont les bénéficiaires du renseignement sur la sécurité ?

Le renseignement sur la sécurité est parfois perçu comme un simple service de recherche pour les équipes de réponse aux incidents et des opérations de sécurité, ou comme le domaine d'analystes d'élite. En réalité, il ajoute de la valeur à chaque fonction de sécurité et à plusieurs autres équipes de l'entreprise.

La section centrale de ce manuel examine les principaux cas d'utilisation :

- ☑ **Les opérations de sécurité et les équipes de réponse aux incidents** sont régulièrement submergées par des alertes. Le renseignement sur la sécurité accélère le triage des alertes, diminue les faux positifs, fournit un contexte pour une meilleure prise de décision et permet de réagir plus rapidement.
- ☑ **Les équipes de gestion des vulnérabilités** ont souvent du mal à faire la différence entre les vulnérabilités cruciales et pertinentes et celles qui ne sont pas importantes pour leur entreprise. Le renseignement sur la sécurité fournit un contexte et une cote de risque qui leur permettent de réduire les temps d'arrêt tout en corrigeant les vulnérabilités qui comptent le plus.
- ☑ **Les analystes de menaces** doivent comprendre les motivations et les TTP des auteurs de menaces et suivre les tendances en matière de sécurité pour les différents secteurs, technologies et régions. Le renseignement sur la sécurité leur fournit des connaissances plus approfondies et plus étendues pour générer des points de vue plus perspicaces.

- ☑ **Les programmes de gestion des risques posés par les tiers** ont besoin d'informations à jour sur les systèmes de sécurité des fournisseurs, vendeurs et autres tiers qui ont accès aux systèmes de l'entreprise. Le renseignement sur la sécurité leur procure un flux continu d'informations objectives et détaillées sur les partenaires commerciaux que les questionnaires statiques des fournisseurs et les méthodes d'approvisionnement traditionnelles ne peuvent leur fournir.
- ☑ **Les équipes chargées de la protection de la marque** ont besoin d'une visibilité continue des mentions non autorisées sur le Web et les réseaux sociaux, des fuites de données, des usurpations d'identité d'employés, des produits contrefaits, des sites Web de typosquatting, des attaques de hameçonnage, etc. Les outils de renseignement sur la sécurité surveillent ces problèmes à grande échelle sur Internet et rationalisent les processus d'élimination et de correction.
- ☑ **Les équipes chargées de la gestion des risques géopolitiques et de la sécurité physique** se fient aux avertissements anticipés d'attentats, de manifestations et d'autres menaces pesant sur les actifs partout dans le monde. Les programmes de renseignement sur la sécurité captent des données et des « bavardages » provenant de sources multiples et les filtrent pour fournir des renseignements précis sur ce qui se passe dans les villes, les pays et les régions pertinents.
- ☑ **Les responsables de la sécurité** utilisent le renseignement sur les menaces probables et leur impact commercial potentiel pour évaluer les exigences en matière de sécurité, quantifier les risques (idéalement en termes monétaires), élaborer des stratégies d'atténuation et justifier les investissements en cybersécurité auprès des PDG, des directeurs financiers et des membres de leur conseil d'administration.

Pour une présentation concise du renseignement sur la sécurité et des six domaines de solutions critiques, lisez le livre blanc « Security Intelligence: Driving Security From Analytics to Action » (Le renseignement sur la sécurité : la sécurisation, des analyses aux interventions).

Chapitre 2

Types et sources

Dans ce chapitre

- Apprenez quelle est la différence entre renseignement sur la sécurité opérationnel et stratégique
- Appréhendez le rôle des flux de données, des canaux privés et de l'Internet clandestin

« Il est très triste de constater qu'il y a aujourd'hui si peu d'informations inutiles. »

— Oscar Wilde

Deux types de renseignements sur la sécurité

Le renseignement sur la sécurité est un vaste concept constitué de deux sortes de renseignements : **le renseignement opérationnel** et **le renseignement stratégique**. Ces deux types de renseignements ont des sources, des publics et des formats différents.

Le but de cette distinction est de reconnaître que les diverses fonctions de sécurité ont des objectifs et des degrés de connaissances techniques différents. Comme mentionné précédemment, le renseignement doit être exploitable, mais étant donné que les responsabilités d'une équipe de gestion des vulnérabilités diffèrent considérablement de celles d'un CISO, l'« exploitabilité »a des implications différentes pour chacun, et la forme et le contenu du renseignement le plus utile à chacun diffère aussi.

Le renseignement opérationnel sur la sécurité

Le renseignement opérationnel sur la sécurité consiste en connaissances sur les cyberattaques, les événements et les campagnes en cours. Il fournit des informations spécialisées qui aident à comprendre la nature, l'intention et le moment d'attaques spécifiques au fur et à mesure qu'elles se produisent. Il provient généralement de machines.

Le renseignement opérationnel est parfois appelé **renseignement technique sur la sécurité** ou **renseignement technique sur les menaces**, car il comprend habituellement des informations techniques sur les attaques, telles que les vecteurs d'attaque utilisés, les vulnérabilités exploitées et les domaines de commandement et de contrôle utilisés par les attaquants. Ce genre de renseignement est souvent le plus utile pour le personnel directement impliqué dans la défense d'une organisation, comme les architectes de systèmes, les administrateurs et le personnel de sécurité.

Les flux de données sur les menaces sont souvent utilisées pour obtenir des informations techniques. Ils se concentrent généralement sur un seul type d'indicateur de menace, comme les hachages de programmes malveillants ou les domaines suspects. Comme nous le décrirons ci-après, les flux de données sur les menaces fournissent des données pour le renseignement sur la sécurité mais ne constituent pas en elles-mêmes du renseignement sur la sécurité.

L'une des utilisations du renseignement opérationnel sur la sécurité est l'orientation des améliorations des contrôles et des processus de sécurité existants, et l'accélération de la réponse aux incidents. Une solution de renseignement opérationnel intégrée aux données de votre réseau est cruciale car elle peut répondre à des questions urgentes spécifiques à votre organisation comme « Cette vulnérabilité critique, exploitée en ce moment dans mon secteur, est-elle présente dans mes systèmes ? »,

Le renseignement stratégique sur la sécurité

Le renseignement stratégique sur la sécurité procure un aperçu général du panorama de menaces contre une entreprise. Il est avant tout utile pour éclairer les décisions de haut niveau des cadres supérieurs. Le contenu est généralement orienté vers les entreprises et présenté sous forme de rapports ou de briefings. Les machines ne sont pas capables de produire cette documentation — elle doit être créée par des experts humains.

Ce genre de renseignement nécessite une interaction humaine, car l'évaluation et l'essai de TTP de l'adversaire contre des contrôles de sécurité existants exige mûre réflexion et analyse. Des parties de ce processus peuvent être automatisées, mais un cerveau humain est nécessaire pour mener à bien cet effort.

Du bon renseignement stratégique doit fournir un aperçu des risques liés à certaines actions, des schémas généraux des tactiques et des cibles des auteurs de menaces, des événements et tendances géopolitiques et d'autres sujets semblables.

Les sources de renseignements stratégiques de sécurité courantes sont les suivantes :

- ☑ Des documents sur les politiques d'États-nations ou d'organisations non gouvernementales
- ☑ Des actualités de médias locaux et nationaux, des articles de publications relatives à des secteurs et sujets spécifiques et des contributions d'experts dans des domaines spécifiques
- ☑ Des livres blancs, des rapports sur des recherches et autre contenu produit par des organismes de sécurité

Les entreprises doivent établir des exigences en matière de renseignement sur la sécurité stratégique en posant des questions précises et ciblées. Il faut des analystes possédant une expertise dépassant les compétences typiques en matière de cybersécurité, plus spécifiquement avec une bonne

compréhension des concepts sociopolitiques et commerciaux, pour recueillir et interpréter le renseignement stratégique sur la sécurité.

Certains aspects de la production de renseignement stratégique sur la sécurité devraient être automatisés. Bien que le produit final ne soit pas technique, la production de renseignement stratégique sur la sécurité efficace nécessite des recherches approfondies et des volumes massifs de données, souvent dans plusieurs langues. Ces défis rendent la collecte et le traitement initiaux de données trop difficiles à effectuer manuellement, même pour les rares analystes qui possèdent les compétences linguistiques, le contexte technique et le savoir-faire professionnel appropriés. Une solution de renseignement sur la sécurité qui automatise la collecte et le traitement des données diminue cette charge de travail et permet aux analystes disposant de moins d'expertise de travailler plus efficacement.

Le rôle des flux de données sur les menaces

Nous avons mentionné précédemment que les données ne sont pas du renseignement et que les flux de données sur les menaces peuvent submerger les analystes déjà accablés par d'innombrables alertes et notifications quotidiennes. Cependant, lorsqu'ils sont utilisés correctement, les flux de données sur les menaces peuvent constituer des matières premières précieuses pour le renseignement sur la sécurité.

Les flux de données sur les menaces sont des flux de données en temps réel qui fournissent des informations sur les cybermenaces et les risques potentiels. Il s'agit généralement de listes d'indicateurs simples ou d'artefacts axés sur un seul centre d'intérêt, comme les domaines suspects, les hachages, les mauvais IP ou les codes malveillants. Ils fournissent un aperçu rapide et en temps réel du panorama de menaces.

Toutefois, de nombreux flux sont remplis d'erreurs, de répétitions et de faux positifs. Cela occasionne de la confusion et du travail supplémentaire. Il est donc essentiel de sélectionner des flux de données de haute qualité.

L'évaluation des flux de données sur les menaces

Utilisez ces critères pour évaluer les flux de données sur les menaces pour votre entreprise :

Sources de données : Les flux de renseignement obtiennent leurs données de toutes sortes de sources dont bon nombre ne sont pas pertinentes pour votre entreprise. Vous tirerez par exemple le meilleur parti de données recueillies auprès d'entreprises de votre secteur.

La transparence des sources : Connaître la provenance de vos données vous permet d'évaluer leur pertinence et leur utilité

Pourcentage de données uniques: Certains flux payants sont simplement des ensembles de données provenant d'autres flux et mentionnent les mêmes éléments plusieurs fois.

Périodicité des données : Les données doivent être recueillies fréquemment et couvrir la période pertinente pour votre organisation. Elles devraient également couvrir une période suffisamment longue pour soutenir le renseignement stratégique sur les tendances à long terme.

Les résultats mesurables : Il est indispensable de pouvoir suivre le taux de corrélation — le pourcentage d'alertes correspondant à votre télémétrie interne au cours d'une semaine, d'un mois ou d'un trimestre donné — pour calculer les résultats mesurables d'un flux particulier.

Au lieu d'afficher des dizaines de flux séparément, utilisez une plate-forme de renseignement sur la sécurité qui les combine tous en un seul flux, supprime les répétitions et les faux positifs, les compare à la télémétrie interne et génère des alertes hiérarchisées. Les plates-formes les plus puissantes de renseignement sur la sécurité permettent même aux entreprises de créer des flux personnalisés de renseignement sur la sécurité ou d'organiser et de mettre en œuvre des alertes automatisées.

Le rôle des canaux privés et de l'Internet clandestin

Les flux de données sur les menaces et les informations accessibles au public ne sont pas les seules sources de données externes du renseignement sur la sécurité. Du renseignements opérationnel et stratégique vital sur des attaques spécifiques,

des TTP d'attaquants, des objectifs politiques d'hacktivistes et des États auteurs de menaces, ainsi que d'autres sujets cruciaux peuvent être rassemblés en s'insinuant ou en s'immisçant dans des canaux privés de communication utilisés par les groupes d'auteurs de menaces. Ceux-ci comprennent des applications de messagerie chiffrées et des forums exclusifs de l'Internet clandestin.

Toutefois, il existe des obstacles à la collecte de ce genre de renseignement :

- ☑ **Accès** : Les groupes d'auteurs de menaces peuvent communiquer sur des canaux privés et cryptés ou exiger une preuve d'identification ou une invitation d'un administrateur.
- ☑ **Langue** : Les activités des forums se déroulent en russe, en chinois, en indonésien, en arabe et dans de nombreuses autres langues, et de l'argot ainsi que du jargon spécialisé sont régulièrement utilisés.
- ☑ **Bruit** : Les volumes de conversation sont si importants qu'il peut être difficile ou impossible de collecter manuellement de bonnes informations à partir de sources telles que les salles de discussion et les réseaux sociaux.
- ☑ **Obscurcissement** : Pour éviter d'être détectés, de nombreux groupes d'auteurs de menaces utilisent des tactiques d'obscurcissement, comme des noms de code.

Pour surmonter ces obstacles, il faut de grands investissements en outils et en expertise afin de surveiller ces canaux privés, ou un recours à des fournisseurs de renseignement sur la sécurité qui ont déjà effectué cet investissement.

Cherchez des solutions et des services de renseignement sur la sécurité qui recourent à des algorithmes et à des processus analytiques pour une automatisation à grande échelle de la collecte de données. Une solution qui utilise un traitement de langage naturel, par exemple, peut recueillir des informations de sources en langue étrangère sans nécessiter d'expertise humaine pour les déchiffrer.

Chapitre 3

Le cycle de vie du renseignement sur la sécurité

Dans ce chapitre

- Étudiez les phases du cycle de vie du renseignement sur la sécurité
- Passez en revue les sources du renseignement sur la sur la sécurité
- Examinez le rôle des outils de renseignement sur la sécurité et des analystes humains

« Vous devez faire confiance à votre processus »

— Tom Brady

Les six phases du cycle de vie du renseignement sur la sécurité

Le renseignement sur les menaces se fonde sur des techniques d'analyse affinées depuis des dizaines d'années par les instances gouvernementales et militaires. Il existe six phases distinctes qui forment ce que l'on appelle le «cycle du renseignement » :

1. La direction
2. Collecte

3. Le traitement
4. L'analyse
5. La diffusion
6. Le retour d'information

La figure 3-1 montre comment ces 6 phases s'alignent sur le renseignement sur la sécurité.

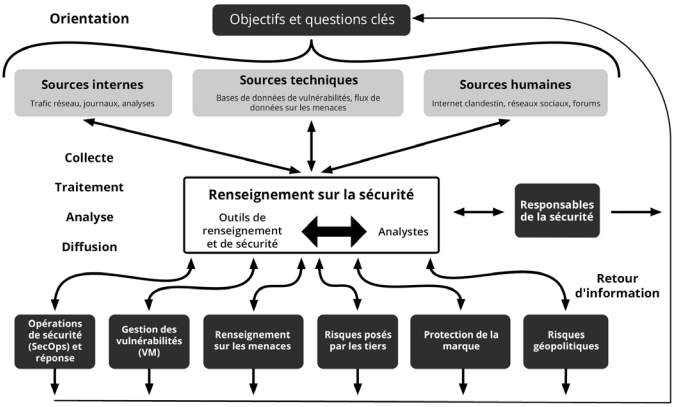


Figure 3-1 : le renseignement sur la sécurité et les six phases du cycle du renseignement.

La direction

La phase « orientation » du cycle de vie du renseignement sur la sécurité est celle durant laquelle vous établissez des objectifs pour votre programme de renseignement sur la sécurité Cela signifie comprendre et articuler les éléments suivants :

- ☑ Les actifs informationnels et les processus opérationnels qui doivent être protégés.
- ☑ Les répercussions éventuelles de la perte de ces actifs ou de l'interruption de ces processus.
- ☑ Les types de renseignements sur les menaces que le service de sécurité exige pour protéger les actifs et répondre aux menaces.

- ☑ Les priorités concernant ce que vous devez protéger

Une fois que les besoins de renseignement de haut niveau sont déterminés, une organisation peut formuler des questions qui convertissent le besoin d'informations en exigences distinctes. Par exemple, si l'objectif est de comprendre qui sont les adversaires probables, une question logique serait : "quels acteurs, sur les forums clandestins, demandent activement des données concernant notre organisation ?"

Une bibliothèque d'objectifs

Recorded Future a créé une liste d'objectifs de renseignement préconfigurés qui comprend la plupart des exigences en termes de renseignement des sociétés Global 500. Cette liste permet aux entreprises novices en renseignement sur la sécurité de réfléchir à leurs problèmes et à leurs priorités, et de déterminer comment intégrer le renseignement sur la sécurité à leurs processus existants. Pour en savoir plus sur la Bibliothèque des objectifs de renseignement, consultez https://www.recordedfuture.com/intelligence-goals-library-overview/.

Des modèles fondés sur les adversaires comme la Cyber Kill Chain de Lockheed - Martin et la matrice MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) (décrite au chapitre 13) peuvent aussi aider les sociétés à se concentrer sur les types de renseignement sur la sécurité dont elles ont besoin pour empêcher les violations et diminuer les risques.

Collecte

La collecte est le processus de rassemblement d'informations pour répondre aux principales exigences en matière de renseignement Elle peut se faire en interne par des moyens divers, notamment :

- ☑ L'extraction de métadonnées et de journaux des réseaux internes et des dispositifs de sécurité
- ☑ Les abonnements aux flux de données sur les menaces d'entreprises du secteur et de fournisseurs de cybersécurité
- ☑ Les conversations et les entrevues ciblées avec des sources bien informées

- ☑ L'analyse de sites Web d'actualités et de blogs
- ☑ L'analyse des plates-formes de réseaux sociaux
- ☑ La fouille et les récoltes sur les sites Web et les forums
- ☑ L'infiltration de sources fermées telles que les forums de l'Internet clandestin

Les données recueillies sont généralement un mélange de données sous forme de produits finis, comme les rapports d'experts et de fournisseurs de cybersécurité, et de données brutes, comme les signatures de logiciels malveillants ou les informations d'identification ayant fait l'objet d'une fuite qui figurent dans un site de stockage de textes.

Les sources du renseignement sur la sécurité

Les sources techniques Les sources techniques sont faciles à intégrer aux technologies de sécurité existantes mais contiennent souvent une grande proportion de faux positifs et des résultats obsolètes.

Les médias (p. ex., les sites Web sur la sécurité, les recherches de fournisseurs) - Ces sources fournissent souvent des renseignements utiles sur les nouvelles menaces, mais il est difficile de se connecter aux indicateurs techniques pour mesurer le risque.

Les réseaux sociaux Les faux positifs et la désinformation sont monnaie courante, de sorte que déterminer quelles connaissances sont utilisables nécessite une quantité énorme de recoupements avec d'autres sources.

Les forums d'auteurs de menaces : ces forums spécialement conçus pour héberger des discussions sur les cyberattaques présentent certaines des idées les plus exploitables disponibles où que ce soit. Mais encore une fois, une analyse et des recoupements sont indispensables pour déterminer ce qui est réellement précieux.

l'Internet clandestin (y compris ses marchés et forums) — Bien qu'elles soient souvent à l'origine de renseignements incroyablement précieux, les sources de l'Internet clandestin sont d'un accès extrêmement difficile, surtout celles qui hébergent des communautés criminelles importantes.

Vous avez besoin de plusieurs sources de renseignement pour obtenir une image complète des menaces potentielles et réelles. Comme le montre la figure 3-1, ces sources sont les suivantes :

- ☑ **Des sources internes** telles que les journaux de pare-feu et de routeur, les outils de capture de paquets réseau et les analyses de vulnérabilités
- ☑ **Des sources techniques** telles que les bases de données sur les vulnérabilités et les flux de données sur les menaces
- ☑ **Des sources humaines**, notamment les médias traditionnels et les réseaux sociaux, les forums et blogs sur la cybersécurité et les forums de l'Internet clandestin

Toute absence de l'un de ces éléments peut ralentir les enquêtes et provoquer des lacunes dans les corrections.

Automatisez ! Les analystes devraient consacrer le moins de temps possible à la collecte des données et le plus de temps possible à l'évaluation et à la communication des informations sur les menaces.

Le traitement

Le traitement est la transformation des informations recueillies en format utilisable par l'organisation. Presque toutes les données brutes collectées doivent être traitée d'une manière ou d'une autre, que ce soit par des êtres humains ou des machines.

Différentes méthodes de collecte exigent souvent des modes de traitement différents. Il se peut que les rapports d'êtres humains doivent être corrélés et hiérarchisés, conciliés et vérifiés. Par exemple, des adresses IP peuvent être extraites du rapport d'un fournisseur de sécurité et ajoutées à un fichier CSV pour être importées dans un produit de gestion d'informations et d'événements de sécurité (SIEM). Sur un plan plus technique, le traitement peut comprendre l'extraction d'indicateurs provenant d'un e-mail, leur enrichissement avec d'autres informations, puis la communication avec des outils de protection de terminal pour un blocage automatique.

Automatisez davantage ! Les bons outils vous permettront d'automatiser la plupart des processus de traitement de flux de données et de collecte. Par exemple, un outil d'automatisation de sécurité pourrait reconnaître un IOC suspect, puis effectuer une séquence de contrôles afin d'établir un contexte pour cet IOC. Cela permet à l'analyste de gagner un temps précieux qui, autrement, devrait être consacré à des vérifications manuelles.

Pour en savoir plus sur la manière dont l'automatisation améliore le renseignement sur la sécurité, lisez le court livre électronique de Recorded Future, «Beyond SOAR: 5 Ways to Automate Security With Intelligence » (Au-delà de SOAR : 5 façons d'automatiser la sécurité grâce au renseignement).

L'analyse

L'analyse est le processus de transformation d'informations en renseignement pouvant éclairer des décisions. Selon les circonstances, les décisions peuvent comprendre enquêter ou non sur une menace potentielle, déterminer les mesures à prendre immédiatement pour bloquer une attaque, préciser comment renforcer les contrôles de sécurité ou justifier le montant d'investissements en ressources de sécurité supplémentaires. L'analyse est généralement effectuée soit par un être humain, soit par un algorithme très sophistiqué.

Les analystes doivent comprendre clairement qui utilisera leur renseignement et quelles décisions ces personnes prendront. Le renseignement que vous fournissez doit être perçu comme étant exploitable, pas uniquement théorique. La plus grande partie de ce livre vise à vous donner une image claire de la façon dont le renseignement sur les menaces peut améliorer l'adoption de décisions et les interventions dans différents domaines de la cybersécurité.

La forme sous laquelle les informations sont présentées revêt une importance particulière. La collecte et le traitement d'informations qui seront transmises sous une forme incompréhensible et inutilisable par le décideur sont un gaspillage inutile.

Par exemple, si vous souhaitez communiquer avec des responsables non techniques, votre rapport doit :

- ☑ Être concis (une note d'une page ou quelques diapositives)
- ☑ Éviter les termes et le jargon déroutants et trop techniques
- ☑ Décrire les problèmes en termes commerciaux (tels que les coûts directs et indirects et l'impact sur la réputation)
- ☑ Comprendre des recommandations sur la marche à suivre

Il peut être nécessaire de transmettre certains renseignements dans différents formats pour différents publics, comme, par exemple, par flux vidéo et dossier écrit. Tous les renseignements ne doivent pas être assimilés au moyen d'un rapport officiel. Les équipes dont le travail de renseignement sur les menaces est couronné de succès fournissent des rapports techniques continus aux autres équipes de sécurité en établissant un contexte extérieur pour les IOC, les logiciels malveillants, les auteurs de menaces, les vulnérabilités et les tendances des menaces.

La diffusion

La diffusion consiste à faire parvenir les renseignements sous forme de produit fini aux endroits qu'ils doivent atteindre.

Comme le montre la figure 3-1, la plupart des organisations de cybersécurité ont au moins six équipes qui peuvent bénéficier du renseignement sur la sécurité. Pour chacun de ces publics, vous devez vous demander :

- Quels renseignements sur la sécurité leur faut-il, et comment des informations externes peuvent-elles les aider dans leurs activités ?
- Comment le renseignement doit-il être présenté pour être facile à comprendre et exploitable par ce public ?

- À quelle fréquence devons-nous transmettre des mises à jour et d'autres informations ?
- Sur quels supports (e-mails, bulletins, forums Web, documents, diapositives, présentations orales) le renseignement devrait-il être diffusé?
- S'ils ont des questions, comment y donner suite ?

Le retour d'information

Des informations régulières sont nécessaires pour veiller à bien comprendre les exigences de chaque groupe et à effectuer des ajustements au fur et à mesure de l'évolution de leurs exigences et de leurs priorités. Ces informations sont recueillies lors de la phase de retour d'information. Il est extrêmement important de comprendre vos priorités globales en matière de renseignement, ainsi que les exigences de vos « clients », les équipes de sécurité qui utilisent le renseignement sur la sécurité. Leurs besoins orientent toutes les phases du cycle de vie du renseignement et vous disent :

- ☑ Quels types de données recueillir
- ☑ Comment traiter et enrichir les données pour les convertir en informations utiles
- ☑ Comment analyser les informations et les présenter sous forme de renseignement exploitable
- ☑ À qui adresser chaque type de renseignement à diffuser, à quelle allure il doit être diffusé et à quelle vitesse il faut répondre aux questions

Pour chaque équipe "cliente", mettez en place un canal pour un retour d'information rapide et informel (comme une adresse e-mail, un forum interne ou un outil de collaboration d'équipe), et un processus de sondage officiel et structuré (comme un sondage en ligne ou des réunions trimestrielles en face-à-face). Le canal informel vous aide à réagir et à effectuer des ajustements immédiats, tandis que le processus structuré garantit que vous obtenez la contribution de chacun et que vous pouvez suivre vos progrès au fil du temps.

Les outils et les personnes

Les outils sont indispensables pour l'automatisation des étapes de collecte, de traitement et de diffusion du cycle de vie du renseignement, ainsi que pour soutenir et accélérer l'analyse. Sans les bons outils, les analystes consacrent tout leur temps aux aspects mécaniques de ces tâches et n'ont jamais le temps d'effectuer une véritable analyse.

La plupart des groupes bien établis de renseignement sur les menaces utilisent deux types d'outils :

- ☑ Les solutions de renseignement sur les menaces qui visent à recueillir, traiter et analyser tous les types de données sur les menaces de sources internes, techniques et humaines.
- ☑ Les outils de sécurité actuels tels que les outils SIEM et les outils d'analyse de la sécurité qui recueillent et mettent en corrélation les événements de sécurité et les données de journaux

Les analystes humains sont tout aussi importants, voire davantage. Vous ne pouvez pas compter sur des outils pour des entrevues avec des experts en sécurité ni pour sonder des forums fermés de l'Internet clandestin. En outre, vous avez besoin de personnes pour analyser et synthétiser le renseignement pour les équipes de sécurité et les responsables qui l'utilisent.

Il n'est pas nécessaire que les analystes fassent partie d'un service d'élite centralisé du renseignement sur les menaces. Quelqu'un doit envisager la fonction du renseignement sur les menaces au niveau de l'ensemble de l'organisation, prendre des décisions concernant les ressources et les priorités et faire le suivi des progrès, mais différentes structures organisationnelles peuvent y parvenir. Vous pourriez avoir un groupe central, avec des analystes qui se consacrent entièrement au renseignement sur la sécurité, ou un petit groupe au sein des opérations de sécurité ou de l'équipe de réponse aux incidents. Sinon, les membres des différents groupes de cybersécurité peuvent être responsables de l'analyse du renseignement sur les menaces pour leurs collègues.

Au chapitre 14, nous discutons de l'évolution fréquente de la structure organisationnelle au fur et à mesure de la maturation de la fonction de renseignement sur la sécurité, et le chapitre 15 fournit des conseils sur la façon d'organiser une équipe centrale de renseignement sur la sécurité.

Section 2 : Applications du renseignement sur la sécurité

Chapitre 4

Le renseignement sur les opérations de sécurité, 1re partie : le triage

Dans ce chapitre

- Voyez comment « la lassitude face aux alertes » risque de détruire le bon travail des équipes des SecOps
- Comprenez la valeur du contexte pour l'amélioration du triage
- Découvrez comment le renseignement sur la sécurité évite les pertes de temps et améliore le triage

"Les pires états passent les premiers"

— Panneau de salle d'urgence d'un hôpital

Le triage est un travail essentiel mais épuisant pour les équipes des opérations de sécurité. Elles sont prises en otage par les énormes volumes d'alertes générées par les réseaux qu'elles surveillent. D'après le rapport de Ponemon intitulé "Coût du confinement des logiciels malveillants", les équipes de sécurité peuvent s'attendre à enregistrer près de 17 000 alertes de logiciels malveillants lors d'une semaine typique. Cela veut dire plus de 100 alertes par heure pour une équipe qui fonctionne 24 heures sur 24, 7 jours sur 7. Et il ne s'agit que des alertes de logiciels malveillants. Pour mettre ces chiffres en perspective, toutes ces alertes peuvent amener les équipes de sécurité à consacrer plus de 21 000 heures-personnes chaque année à la chasse aux faux positifs. Autrement dit, il faut 2 625 postes de huit heures simplement pour distinguer les mauvaises alertes des bonnes.

Examinons comment le renseignement sur la sécurité atténue cette surcharge en filtrant les fausses alarmes, en accélérant l'analyse des alertes et en fournissant un contexte pour prendre de meilleures décisions de triage.

Responsabilités de l'équipe des SecOps

Sur papier, les responsabilités de l'équipe COS paraissent simples :

- ☑ Surveiller les menaces potentielles
- ☑ Détecter les activités réseau suspectes
- ☑ Contenir les menaces actives
- ☑ Y remédier à l'aide de la technologie disponible

Lorsqu'un événement suspect est détecté, l'équipe COS fait une enquête et collabore ensuite avec d'autres équipes de sécurité pour atténuer les répercussions et la gravité de l'attaque. Considérez que les rôles et les responsabilités des SecOps sont comparables à ceux des équipes de services d'urgence répondant aux appels d'urgence, comme le montre la figure 4-1.

Niveau	Rôle	Responsabilités
Triage	Opérateur (Centre 911) Analyste de sécurité (SOC)	Détermine la pertinence et l'urgence de chaque alerte entrante. Détermine si l'alerte est légitime et doit être transmise aux échelons supérieurs.
Première réponse	Premier Répondeur (911) Intervenant en cas d'incident (SOC)	Détermine la portée de l'incident. Identifie les systèmes touchés et vulnérables. Recommande des mesures pour contenir les répercussions.
Enquête	Détective (911) Chasseur de menaces (SOC)	Détermine les causes profondes et les faiblesses des défenses. Recommande des mesures pour empêcher que cela ne se reproduise.

Figure 4-1 : Les rôles et les responsabilités des équipes de services d'urgence et des équipes COS sont comparables.

Le volume d'alertes ahurissant

Au cours des dernières années, la plupart des entreprises ont ajouté de nouveaux types de technologies de détection des menaces à leurs réseaux. Chaque outil sonne l'alarme lorsqu'il détecte un comportement suspect ou anormal. Ensemble, ces outils peuvent créer une cacophonie d'alertes de sécurité. Les analystes de sécurité ne peuvent tout simplement pas, à eux seuls, examiner et hiérarchiser toutes ces alertes, et faire une enquête à leur sujet. La lassitude face aux alertes les amène souvent à ne pas en tenir compte, à faire une chasse aux faux positifs et à commettre des erreurs.

Les recherches confirment l'ampleur de ce problème. Dans son rapport intitulé « 2020 State of the SOC », (État des centres d'opérations de sécurité en 2020), le fournisseur SIEM Exabeam a révélé que 39 pour cent des professionnels qui en font partie estiment qu'ils manquent de personnel, et 50 pour cent pensent qu'ils pourraient employer au moins six collaborateurs supplémentaires. L'étude « Security Capabilities Benchmark » (Point de référence sur les capacités de sécurité) de Cisco 2020 a conclu que les entreprises ne peuvent enquêter que sur 48 pour cent des alertes de sécurité qu'elles reçoivent en un jour et que 26 pour cent seulement

des alertes faisant l'objet d'enquêtes sont considérées comme étant légitimes (Figure 4-2).

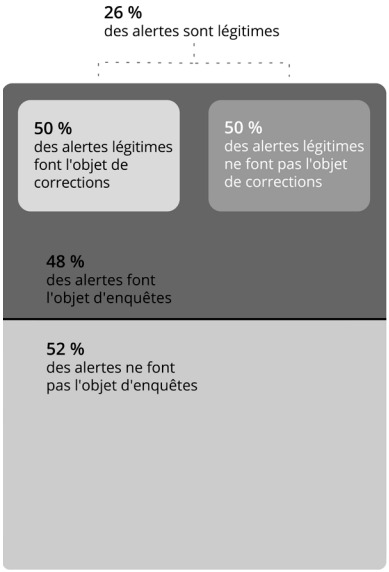


Figure 4-2 : De nombreuses alertes ne font l'objet ni d'enquête ni de corrections. (Source : Cisco)

Le contexte est roi

Le renseignement pour les SecOps vise spécifiquement à les aider à effectuer un triage en enrichissant les alertes internes grâce aux informations externes et au contexte nécessaires pour prendre des décisions fondées sur les risques. Le contexte est crucial pour le triage rapide et très important aussi pour évaluer la portée des incidents et les contenir.

Le triage exige beaucoup de contexte

L'analyste de COS consacre une très grande partie de sa journée aux réponses aux alertes générées par les systèmes de sécurité internes tels que les technologies SIEM ou EDR. Ces sources de données internes sont vitales pour l'identification d'activités réseau susceptibles d'être malveillantes ou les violations de données.

Malheureusement, ces données sont souvent difficiles à interpréter de façon isolée. Déterminer si une alerte est pertinente et urgente nécessite une collecte d'informations connexes (contexte) d'une grande variété de journaux internes du système, de périphériques réseau et d'outils de sécurité (Figure 2-3), *et* de bases de données externes sur les menaces. Effectuer des recherches dans toutes ces sources de données pour établir le contexte de chaque alerte prend un temps énorme.

Figure 4-3 : Principaux aspects de la surveillance de la sécurité et des sources de contexte internes. (Source : UK NCSC)

Cas d'utilisation : La corrélation entre les alertes et leur enrichissement

Un analyste qui tente de trier une alerte sans accès à un contexte suffisant peut être comparé à une personne qui essaie de comprendre un reportage en ne lisant que la manchette. Même lorsque l'analyste a accès à des informations externes sous forme de flux de données sur les menaces (Figure 2-4), ces informations sont très difficiles à assimiler et à corréler avec d'autres données relatives à l'alerte.

2020-09-13 02:46:26	E	63.153.27.53	Hors ligne
2020-09-12 21:41:44	E	75.130.100.165	En ligne
2020-09-12 18:54:45	E	71.172.252.50	En ligne
2020-09-12 15:51:16	E	118.189.9.243	Hors ligne
2020-09-12 14:11:41	E	31.167.248.50	Hors ligne
2020-09-12 08:32:01	E	78.134.74.39	En ligne
2020-09-12 05:03:02	E	42.114.73.81	Hors ligne
2020-09-12 04:56:53	E	216.59.200.206	Hors ligne
2020-09-11 11:35:10	E	183.82.97.20	Hors ligne
2020-09-11 08:59:59	E	128.2.98.139	Hors ligne
2020-09-11 08:12:12	E	47.38.231.174	Hors ligne
2020-09-11 08:01:28	E	217.36.122.251	Hors ligne
2020-09-11 07:45:59	E	107.184.160.132	Hors ligne
2020-09-11 06:45:54	E	71.75.206.192	En ligne
2020-09-11 06:43:49	E	123.231.21.141	Hors ligne
2020-09-11 05:54:51	E	189.222.75.8	Hors ligne
2020-09-11 05:54:51	E	189.211.177.113	Hors ligne
2020-09-11 05:54:51	E	92.27.115.15	Hors ligne
2020-09-11 05:54:51	E	207.107.101.210	Hors ligne
2020-09-11 05:31:45	E	185.97.32.6	En ligne

Figure 4-4 : Il est très difficile de trouver l'information pertinente dans des flux de données brutes sur les menaces et de les corréler avec d'autres données relatives à une alerte.

Le renseignement pour les SecOps transforme complètement cette situation. Une telle solution peut enrichir automatiquement les données sur les menaces, les transformant en renseignement sur les menaces et établissant une corrélation avec les alertes, comme illustré à la Figure 2-5. Le contexte fourni peut inclure les premières et les toutes dernières mentions de logiciels malveillants ou d'adresses IP suspectes, le nombre de fois où elles ont été observées, leur association à des types d'attaques et à des auteurs de menaces spécifiques, et des descriptions du comportement du logiciel malveillant ou des utilisations de l'adresse IP (par exemple dans le cadre d'un botnet).

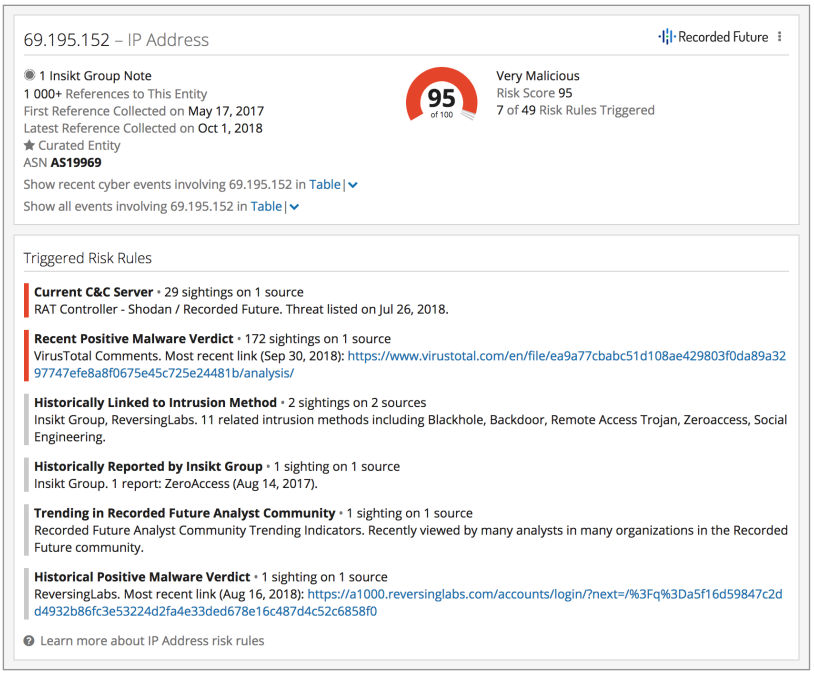


Figure 4-5 : Une solution de renseignement sur les menaces peut automatiquement enrichir les alertes avec un contexte comme des observations antérieures, des associations à des types d'attaques et à des auteurs de menaces, et des cotes de risque. (Source : Recorded Future)

Cet enrichissement permet aux analystes COS d'identifier rapidement les menaces les plus importantes et de prendre immédiatement des mesures en connaissance de cause pour les résoudre.

L'enrichissement permet même à des analystes moins chevronnés des SecOps de « jouer dans la cour des grands » en établissant des corrélations qui, sinon, auraient exigé plus d'expérience. Il permet aussi une sorte d'apprentissage accéléré au travail en fournissant des informations approfondies sur les menaces les plus récentes.

Comme exemple de développement d'analystes moins chevronnés, supposons qu'une alerte est générée quand une adresse IP externe tente de se connecter au port TCP 445. Des analystes expérimentés sauraient probablement qu'un récent logiciel d'exploitation malveillant pour SMB a été utilisé par du

ransomware pour se propager et identifieraient l'IP comme étant sans doute compromis en fonction du propriétaire, de l'emplacement, et des données open source. Les analystes moins expérimentés ne sont pas toujours capables d'établir ces rapports sans assistance, mais le renseignement contextuel sur les menaces peut leur montrer que d'autres appareils du réseau utilisent SMB sur le port 445 pour transférer des fichiers et des données entre différents serveurs. Il pourrait aussi les informer du fait que le nouveau logiciel d'exploitation malveillant et le ransomware ont été associés à cette adresse IP.

Amélioration du délai d'élimination des fausses alarmes

Malgré l'importance que revêt l'accélération et l'amélioration de la précision de la collecte des menaces réelles pour les analystes de COS, on peut faire valoir que la capacité d'éliminer rapidement les fausses alarmes est encore plus importante.

Le renseignement sur la sécurité fournit au personnel des SecOps le contexte nécessaire pour trier rapidement les alertes et avec beaucoup moins d'efforts. Il permet aux analystes d'éviter de gaspiller des heures à poursuivre des alertes fondées sur :

- ☑ Les actions plus susceptibles d'être inoffensives que malveillantes
- ☑ Les attaques qui ne concernent pas leur entreprise
- ☑ Les attaques pour lesquelles des contrôles et des mécanismes de défense sont déjà en place

Certaines solutions du renseignement sur les menaces effectuent automatiquement une grande partie de ce filtrage en personnalisant des flux de données de risque de manière à ignorer ou déclasser les alertes qui ne correspondent pas aux critères spécifiques au secteur et à l'entreprise.

Chapitre 5

Le renseignement pour les SecOps 2e partie : la réponse

Dans ce chapitre

- Découvrez comment le renseignement sur la sécurité minimise la réactivité
- Examinez les caractéristiques des solutions du renseignement sur les menaces qui leur permettent de relever efficacement les défis que pose l'intervention en cas d'incident
- Examinez les exemples d'utilisation du renseignement sur la sécurité des équipes de réponse aux incidents

"Les soins ne devraient pas commencer en salle d'urgence."

— James Douglas

Une fois les attaques réelles identifiées, les processus de réponse aux incidents sont mis en œuvre. Toutefois, ces deux flux de travail sont devenus plus stressants pour les équipes de sécurité. Voici certaines raisons :

- ☑ Le volume de ceux-ci a constamment augmenter ces vingt dernières années.
- ☑ Les menaces sont devenues plus complexes et difficiles à analyser ; suivre les tendances du contexte des cybermenaces en constante évolution est devenu une tâche ardue en elle-même.

- ☑ Lors de la réponse aux incidents de sécurité, les analystes sont forcés de passer beaucoup de temps à vérifier manuellement et diffuser des données provenant de sources disparates.
- ☑ Le confinement des attaques et la suppression des vulnérabilités devient de plus en plus difficile.

Du fait de leur fonction, les équipes de réponse aux incidents fonctionnent en général sous d'immenses contraintes de temps et sont souvent incapables de contenir rapidement les cyberincidents.

Des défis continuels

Bien qu'il soit difficile d'être précis sur le nombre d'incidents rencontrés par une organisation typique, il n'y a aucun doute que le volume des cyberattaques augmente rapidement. Selon « 2020 State of Malware Report » (Rapport sur l'état des logiciels malveillants 2020) des Malwarebytes Labs, le volume des attaques détectées sur les entreprises a augmenté de 13 pour cent en 2019. Bien qu'une partie de cette pression croissante soit atténué par les technologies de prévention, les équipes de réponse aux incidents subissent d'énormes pressions supplémentaire en raison des facteurs suivants.

La pénurie de compétences

La réponse à l'incident n'est pas une fonction de sécurité du premier échelon. Elle englobe une vaste gamme de compétences, y compris l'analyse statique et dynamique des logiciels malveillants, l'ingénierie à rebours, les enquêtes juridico-informatiques et bien davantage. Elle exige des analystes qui ont une expérience du secteur et sur lesquels on peut compter pour effectuer des opérations complexes sous pression.

Le déficit très médiatisé en matière de compétences en cybersécurité a fortement augmenté au cours de la dernière décennie. Cyber seek calcule qu'il existe actuellement plus d'un demi-million d'emplois disponibles dans le domaine de la cybersécurité rien qu'aux États-Unis. Selon le rapport

ISSA-ESG intitulé « The Life and Times of Cybersecurity Professionals 2020 » (La vie et l'époque des professionnels de la cybersécurité 2020) , 70 % des entreprises sont touchées par la pénurie de professionnels de la cybersécurité.

Des délais de réponse croissants

Avec trop peu de personnel qualifié et trop d'alertes, un résultat est possible : le délai de résolution des véritables incidents de sécurité augmente. Selon le « 2020 Cost of a Data Breach Report » (Coût d'un signalement de violation de données 2020) du Ponemon Institute et d'IBM Security, le temps nécessaire pour détecter et contenir une violation des données est passé de 257 jours en 2017 à 280 jours en 2020.

Bien sûr, les cybercriminels n'ont pas de telles contraintes de temps. Une fois qu'ils s'implantent à l'intérieur d'un réseau cible, le délai de compromission est généralement mesuré en minutes. Nous aborderons cela de façon plus détaillée au chapitre suivant.

Une approche décousue

La plupart des services de sécurité des entreprises ont connu une croissance organisme parallèlement à l'augmentation des cyber-risques. Par conséquent, beaucoup se bornent à ajouter des technologies et des processus de sécurité, mais ensuite, quand ils doivent répondre à des besoins spécifiques, ils le font sans conception stratégique.

Bien que cette approche ad hoc soit parfaitement normale, elle force les équipes de réponse aux incidents à consacrer beaucoup de temps à regrouper les données et le contexte de différentes technologies de sécurité (p. ex., SIEM, EDR et les journaux de pare-feu) et de flux de données de menaces. Ces efforts augmentent considérablement les délais d'intervention et augmentent la probabilité d'erreurs.

Le problème de la réactivité

Une fois que l'alerte est signalée, elle doit faire l'objet d'un triage, être corrigée et être suivie dès que possible pour minimiser les risques. Examinons le processus typique de réponse aux incidents :

1. **Détection de l'incident** — une alerte est reçue d'un SIEM, EDR, ou d'un produit similaire.
2. **Investigation informatique** — détermination de ce qu'il s'est passé et comment y réagir.
3. **Triage et confinement** — adoption de mesures immédiates pour atténuer la menace et minimiser les dommages.
4. **Correction** — réparation des dommages et suppression des infections.
5. **Transfert aux équipes chargées des actions routinières** — transfert de l'incident aux équipes chargées des routines pour les interventions finales.

Notez la nature réactive de ce processus. Pour la plupart des organisations, presque tous le travail nécessaire pour remédier à un incident est concentré en fin de période, ce qui signifie qu'il ne peut être achevé qu'après qu'une alerte est signalée. Bien que cela soit inévitable dans une certaine mesure, c'est loin d'être idéal lorsque les équipes de réponse aux incidents éprouvent déjà des difficultés à résoudre les incidents assez rapidement.

Minimiser la réactivité dans les réponses aux incidents

Pour diminuer les délais d'intervention, les équipes de réponse aux incidents doivent devenir moins réactives. Deux domaines dans lesquels la préparation anticipée peut s'avérer particulièrement utile sont l'identification des menaces probables et la hiérarchisation.

Identification des menaces probables

Si une équipe de réponse aux incidents identifie les menaces les plus courantes à l'avance, elle peut mettre au point de solides processus cohérents pour y faire face. Cette préparation réduit considérablement le temps dont l'équipe a besoin pour contenir les incidents individuels, évite les erreurs et libère des analystes pour faire face aux nouvelles menaces inattendues lorsqu'elles surviennent.

Hiérarchisation

Toutes les menaces ne sont pas égales. Si les équipes de réponse aux incidents peuvent comprendre quels vecteurs de menaces posent les plus grands risques à leur organisation, elles peuvent leur affecter leur temps et leurs ressources en conséquence.

Pour savoir comment les experts en sécurité utilisent le renseignement sur les menaces pour réduire la réactivité lors des réponses aux incidents, regardez le webinaire conjoint de Recorded Future et de LIFARS "Fuel Incident Response With Threat Intelligence to Lower Breach Impact" (Alimentez la réponse à l'incident avec du renseignement sur les menaces pour diminuer l'impact).

Le renforcement de la réponse aux incident avec le renseignement sur la sécurité

D'après ce que nous avons décrit jusqu'à présent, il devrait être clair que *les technologies de sécurité à elles seules ne suffisent pas pour diminuer les pressions sur les analystes humains*.

Le renseignement sur la sécurité diminue sur les demandes auxquelles font face les équipes de réponse aux incidents et résout un grand nombre de problèmes que nous avons mentionnés grâce aux interventions suivantes :

- ☑ Identification automatique et rejet des fausses alertes
- ☑ L'enrichissement des alertes avec un contexte en temps réel provenant de l'Internet ouvert et de l'Internet clandestin
- ☑ L'assemblage et la comparaison des informations provenant de sources de données internes et externes afin d'identifier les menaces réelles
- ☑ La notation des menaces en fonction des besoins et de l'infrastructure spécifiques de l'organisation.

En d'autres termes, le renseignement sur les menaces fournit aux équipes de réponse aux incidents les idées réalisables dont elles ont besoin pour prendre plus rapidement de meilleures décisions, tout en contenant la marée d'alertes hors de propos et peu fiables qui rendent leur travail si difficile.

Le renseignement pour les SecOps en pleine action

Examinons trois exemples d'utilisation et un exemple d'abus qui montrent comment le renseignement sur les menaces affecte les équipes de réponse aux incidents dans le monde réel.

Cas d'utilisation : Préparer à l'avance les processus

Comme nous l'avons mentionné auparavant, les processus de réponse aux incidents sont hautement réactifs, la plupart de l'activité ayant lieu seulement après l'incident. Cela prolonge le temps nécessaire à l'évaluation et à la correction des incidents.

Les renseignements pour les SecOPs permettent aux équipes de réponse aux incidents de se préparer aux menaces en fournissant :

- ☑ Une image complète et à jour du paysage des menaces
- ☑ Des informations sur les TTP prisés par les auteurs de menaces
- ☑ Les faits marquants des tendances des attaques spécifiques aux secteurs et aux régions

Avec le renseignement pour les SecOps, les équipes de réponse aux incidents peuvent élaborer et tenir à jour de solides processus pour les incidents et les menaces les plus courants. Avoir ces processus à sa disposition accélère les investigations informatiques, le triage et le confinement. Cela permet aussi de fortement améliorer la cohérence et la fiabilité des interventions de l'ensemble des fonctions de réponse.

Cas d'utilisation : Évaluer et contenir les incidents

Lorsqu'un incident se produit, les analystes de réponse aux incidents doivent prendre des décisions rapides sur trois facteurs :

1. Ce qui s'est produit
2. Ce que l'incident peut signifier pour l'organisation
3. Les mesures à adopter

Ces trois facteurs doivent tous être analysés dès que possible avec un haut degré de précision. Le renseignement pour les SecOPs a un impact mesurable :

- ☑ En rejetant automatiquement les faux positifs, ce qui permet aux équipes de se concentrer sur les véritables incidents de sécurité
- ☑ En enrichissant les incidents d'informations connexes provenant de l'Internet ouvert et de l'Internet clandestin, facilitant ainsi la détermination de la gravité de la menace et de son effet éventuel sur l'organisation.

- ☑ En fournissant des détails sur la menace et des perspectives sur les TTP de l'attaquant, ce qui aide l'équipe à prendre rapidement des décisions de confinement et de correction

Le temps joue-t-il en votre faveur ou contre vous ?

Vous êtes-vous jamais demandé comment l'équilibre de puissance entre attaquants et défenseurs fluctue au fil du temps ? Pour le découvrir, lisez le billet de blog de Recorded Future intitulé « The 4th in the 5th: Temporal Aspects of Cyber Operations » (Le 4e dans le 5e : aspects temporels des cyberopérations).

Cas d'utilisation : Détection anticipée des violations de données

Il est fréquent que les organisations prennent beaucoup de temps à se rendre compte qu'une violation s'est produite. Selon le rapport d'IBM intitulé « Cost of a Data Breach Report 2020 » (Rapport 2020 sur le coût d'une violation de données), le délai moyen pour identifier une violation de données est de 207 jours.

Il n'est donc guère surprenant que les données volées et les actifs confidentiels soient vendus sur l'Internet clandestin avant que leurs propriétaires légitimes ne sachent ce qui s'est passé.

Une puissante fonctionnalité de renseignements pour les SecOps offre un avantage considérable en vous alertant d'une violation et en vous avertissant rapidement que vos ressources sont exposées en ligne ou que quelqu'un met ces ressources en vente.

Obtenir ce renseignement en temps réel est essentiel car cela vous permettra de contenir l'incident le plus rapidement possible et vous aidera à déterminer quand et comment votre réseau a été violé.

Cas d'utilisation à mauvais escient : Les demi-mesures sont pires que de ne rien faire

Nous souhaitons vous mettre en garde à propos d'un "exemple d'utilisation à mauvais escient" où le renseignement sur les menaces peut en fait nuire à la réponse à l'incident.

Au début de leur parcours du renseignement sur les menaces, certaines organisations optent pour une solution minimaliste, comme une solution de renseignement sur les menaces jumelée avec à divers flux gratuits de données sur les menaces. Ils croient peut-être que cette approche superficielle permettra de minimiser les coûts initiaux.

Bien que ce type d'implémentation permette aux équipes de réponses aux incidents d'obtenir quelques renseignements utilisables, il ne fait habituellement qu'aggraver les choses en forçant les analystes à patauger dans d'énormes quantités de faux positifs et d'alertes hors de propos. Pour pleinement aborder les principaux points douloureux de l'incident, les capacités de renseignement sur les menaces doivent être globales, pertinente, contextualisées et intégrées.

Caractéristiques essentielles du renseignement sur les menaces pour la réponse aux incidents

Il est temps à présent que nous examinions les caractéristiques des capacités puissantes de renseignement sur les menaces et leur façon d'aborder les points les plus douloureux pour les équipes de réponse aux incidents.

Global

Pour être utile aux équipes de réponse aux incidents, le renseignement sur les menaces doit être capté automatiquement sur la plus grande gamme d'emplacements possible dans des sources ouvertes, des flux techniques et l'Internet clandestin. Sinon, les analystes sont forcés d'effectuer leurs propres recherches manuelles pour veiller à ce que rien d'important ne manque.

Imaginez qu'une analyste doive savoir si une adresse IP a été associée à des activités malveillantes. Si elle est sûre que son renseignement sur les menaces proviennent d'une gamme complète de sources de menaces, elle peut interroger les données instantanément et être certaine d'obtenir un résultat précis. Si elle n'en est pas sûre, elle devra consacrer du temps à comparer manuellement l'adresse IP à plusieurs sources de données sur les menaces. La figure 3-1 montre comment le renseignement sur les menaces peut connecter une adresse IP au logiciel malveillant Trickbot. Ce type de renseignement peut être corrélé avec des journaux de réseau interne pour révéler des indicateurs de compromission.

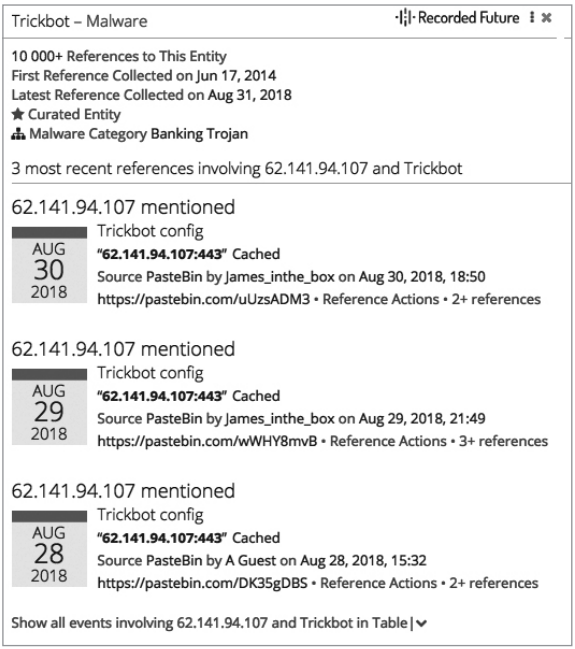


Figure 5-1 : Le renseignement sur la sécurité connecte une adresse IP au logiciel malveillant Trickbot. (Source : Recorded Future)

Pour une description de la façon de distiller des quantités massives de données pour produire un flux restreint mais régulier de renseignement sur la sécurité exploitable, lisez le billet de blog de Recorded Future, « Security Intelligence, Information, and Data: What Is the Difference? » (Sécurité, renseignement, informations et données : quelle est la différence ?).

Pertinent

Il est impossible d'éviter tous les faux positifs lors du travail d'identification et de confinement des incidents. Toutefois, le renseignement sur les menaces devrait aider les équipes de réponse aux incidents à identifier et purger rapidement les faux positifs générés par les technologies de sécurité tels que les produits SIEM et EDR.

Deux catégories de faux positifs sont à envisager :

1. Les alertes pertinentes pour une organisation mais inexactes ou inutiles
2. Les alertes qui sont exactes et/ou intéressantes mais ne sont pas pertinentes pour l'organisation

Les deux types peuvent, potentiellement, faire gaspiller un temps énorme aux analystes de réponse aux incidents.

Les produits sophistiqués de renseignement sur la sécurité utilisent désormais des algorithmes et des processus d'analyse puissants pour identifier et éliminer automatiquement les faux positifs et attirer l'attention des analystes sur le renseignement le plus important (autrement dit le plus pertinent).

La négligence dans le choix de votre technologie de renseignement sur les menaces peut faire perdre un temps énorme à votre équipe avec des renseignements inexacts, périmés ou hors de propos pour votre organisation.

Contextualisé

Toutes les menaces ne sont pas égales. Même parmi les alertes de menace pertinentes, certaines sont inévitablement plus urgentes et plus importantes que le reste. Une alerte provenant d'une source unique peut être à la fois exacte et pertinente mais ne pas constituer une priorité très élevée. C'est pour cette raison que le contexte est si important : il fournit des indices critiques sur les alertes les plus susceptibles d'être importantes pour votre organisation.

Le renseignement contextuel relatif à une alerte peut inclure :

- ☑ La corroboration par plusieurs sources que le même type d'alerte a été lié à des attaques récentes
- ☑ La confirmation qu'elle a été liée à des auteurs de menaces reconnus comme étant actifs dans votre secteur
- ☑ Une chronologie montrant que l'alerte a eu lieu un peu avant ou après d'autres événements liés à des attaques

Des analyses et algorithmes modernes qui permettent à une solution de renseignement sur la sécurité d'envisager plusieurs sources simultanément et de déterminer quelles alertes sont les plus importantes pour une organisation spécifique.

Intégré

L'une des fonctions cruciales d'un système de renseignement sur la sécurité est sa capacité de s'intégrer dans une vaste gamme d'outils de sécurité, notamment SIEM et les solutions de réponse aux incidents. Grâce à l'intégration, le produit peut examiner les alertes qu'il génère et :

- ☑ Déterminer si chaque alerte doit être rejetée comme faux positif
- ☑ Noter l'alerte en fonction de son importance
- ☑ Enrichir l'alerte avec un contexte précieux

Une intégration efficace élimine le besoin pour les analystes de comparer manuellement chaque alerte aux informations figurant sur leur écosystème de sécurité et leurs outils de renseignement sur la sécurité. Plus important encore, les processus d'intégration et d'automatisation peuvent éliminer un grand nombre de faux positifs sans vérification d'analyste humain. Gagner du temps et éviter les frustrations sont peut-être les plus grands avantages du renseignement sur la sécurité pour les équipes de réponse aux incidents.

Chapitre 6

Le renseignement sur les vulnérabilités

Dans ce chapitre

- Examinez les défis actuels pour la lutte contre les vulnérabilités basées sur les risques réels
- Découvrez comment le renseignement sur les vulnérabilités offre des aperçus des comportements des auteurs de menaces
- Voyez comment le renseignement fondé sur les risques rationalise la gestion des éléments opérationnels des vulnérabilités

"Reconnaître notre faiblesse est la première étape de la réparation de notre perte."

— Thomas à Kempis

La gestion des vulnérabilités n'est pas une activité prestigieuse, mais c'est un des rares moyens d'être proactif dans la sécurisation de votre organisation. Son importance ne saurait être surestimée.

La clé du succès dans la gestion des vulnérabilités est de modifier la façon de penser de vos équipes de sécurité de manière à passer du rafistolage aux décisions fondées sur les risques. C'est essentiel parce que le vaste océan de vulnérabilités déclarées chaque année tend jusqu'à se rompre les équipes chargées d'identifier les actifs vulnérables et de déployer des correctifs. Pour prendre de bonnes décisions fondées sur les risques, il est crucial de tirer parti de plus de sources de renseignement sur la sécurité.

Les chiffres sur le problème de la vulnérabilité

Selon le Gartner Market Guide for Security Threat Intelligence Products and Services, environ 8,000 vulnérabilités par an ont été divulguées au cours de la dernière décennie. Le nombre n'a augmenté que légèrement d'une année à l'autre, et seulement une sur huit environ a été exploitée. Cependant, au cours de la même période, la quantité de nouveaux logiciels utilisés a considérablement augmenté, et le nombre de menaces a augmenté de façon exponentielle.

En d'autres termes, bien que le nombre de violations et de menaces ait augmenté au cours des 10 dernières années, seul un petit pourcentage était fondé sur de nouvelles vulnérabilités. Comme le dit Gartner : "plus de menaces exploitent le même petit ensemble de vulnérabilités."

Zero-day ne signifie pas priorité absolue

Les menaces zero-day attirent régulièrement beaucoup trop d'attention. Toutefois, la grande majorité des "nouvelles" menaces appelées zero-day sont en fait des variations sur un thème, qui exploitent les vulnérabilités de toujours de manières un peu différentes. Ce que cela signifie, c'est que l'approche la plus efficace pour la gestion des vulnérabilités n'est pas de se concentrer sur les menaces zero-day mais plutôt d'identifier et de corriger les vulnérabilités spécifiques des logiciels utilisés par votre organisation.

Le temps est un facteur clé

Les auteurs de menaces sont devenus plus rapides dans l'exploitation des vulnérabilités. Selon Gartner, le temps moyen nécessaire entre l'identification d'une vulnérabilité et l'apparition d'un logiciel d'exploitation malveillant dans le milieu naturel est passé de 45 jours à 15 ces dix dernières années.

Cette tendance a deux implications pour les équipes de gestion des vulnérabilités :

1. Vous avez environ deux semaines pour corriger ou protéger vos systèmes contre une nouvelle attaque.
2. Si vous ne pouvez pas corriger cela durant ce délai, il vous faut un plan pour atténuer les dommages.

Des recherches d'IBM X-Force montrent que si une vulnérabilité n'est pas exploitée dans un délai de deux semaines à trois mois après qu'elle est annoncée, il est statistiquement peu probable qu'elle le sera jamais. La correction des "anciennes" vulnérabilités n'est donc habituellement pas une priorité.

Pour en savoir plus sur les vulnérabilités récentes, lisez l'analyse des menaces de Recorded Future, « The Top 10 Vulnerabilities Used by Cybercriminals in 2019 » (Les 10 principales vulnérabilités utilisées par les cybercriminels en 2019). Les logiciels d'exploitation malveillants visent en général les technologies les plus souvent utilisées. Un épisode de podcast de Recorded future intitulé « 7 of the Top 10 Vulnerabilities Target Microsoft » (7 des 10 principales vulnérabilités ciblent Microsoft) explique pourquoi.

Toutes ces statistiques indiquent une conclusion : votre but ne doit pas être de corriger la plupart des vulnérabilités ni même la plupart des menaces zero-day, mais plutôt d'identifier et d'aborder les menaces les plus susceptibles d'être exploitées contre votre organisation.

Évaluer les risques en se fondant sur l'exploitabilité

Utilisons une métaphore : si l'application de correctifs aux vulnérabilités pour protéger votre réseau est comme vacciner pour vous protéger d'une maladie, vous devez décider des vaccins prioritaires et de ceux qui ne sont pas nécessaires. Vous avez peut-être besoin chaque année d'un vaccin contre la grippe pour rester en bonne santé, mais vous ne devez être vacciné contre la fièvre jaune ou la malaria que si vous allez y être exposé.

Les deux contributions les plus précieuses d'une solution de renseignement sur les vulnérabilités sont l'identification de vulnérabilités spécifiques qui présentent un risque réel pour votre organisation et la visibilité de leur probabilité d'exploitation.

La Figure 4-1 illustre cet argument. Des milliers de vulnérabilités ont été révélées. Des centaines sont exploitées et un certain nombre de vulnérabilités existent dans votre environnement. Vous n'avez vraiment qu'à vous préoccuper de celles qui se trouvent au croisement de ces deux dernières catégories : les vulnérabilités se trouvant dans votre environnement qui sont activement exploitées.

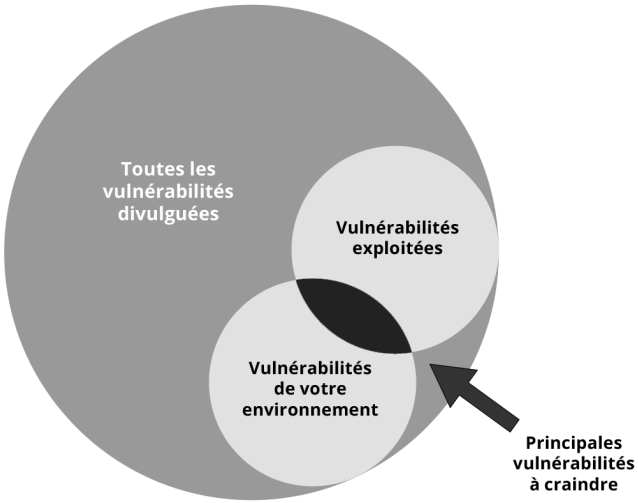


Figure 6-1 : Les plus grands risques sont les vulnérabilités présentes dans votre organisation et exploitées actuellement. (Source : Gartner)

Les indices de gravité sont souvent trompeurs

Classer les menaces en termes de gravité est une erreur que les gestionnaires de vulnérabilité commettent régulièrement. Les systèmes de classification et de classement comme les désignations CVE (Common Vulnerabilities and Exposures, les vulnérabilités et expositions courantes) et de CVSS

(Common Vulnerability Scoring Systems, les systèmes de notation des vulnérabilités courantes) ne tiennent pas compte du fait que les auteurs de menaces exploitent ou non ces vulnérabilités dans votre secteur ou dans les régions où vous êtes implanté actuellement. Compter uniquement sur la gravité de la vulnérabilité est comme obtenir un vaccin contre la peste bubonique avant un vaccin contre la grippe parce que la peste a tué plus de gens à un certain moment dans l'histoire.

La genèse du renseignement sur la sécurité : Les bases de données de vulnérabilités

Les bases de données sur les vulnérabilités groupent les informations sur les vulnérabilités révélées et leur attribuent une cote d'exploitabilité.

En fait l'une des premières formes de renseignement sur les menaces a été NVD (National Vulnerability Database, la base de données nationale sur les vulnérabilités) de NIST. Elle centralisait les informations sur les vulnérabilités révélées pour permettre aux organisations de voir plus facilement s'il était probable qu'elles soient touchées. Pendant plus de 20 ans, la NVD a recueilli des informations sur plus de 100 000 vulnérabilités, devenant une source d'une valeur inestimable pour les professionnels de la sécurité de l'information. D'autres pays, notamment la Chine et la Russie, ont emboîté le pas à NIST en établissant leurs propres bases de données de vulnérabilités.

Vous trouverez la NVD de NIST sur le site https://nvd.nist.gov/. Un catalogue des bases de données de vulnérabilité est publié ici par l'organisation FIRST du secteur : https://www.first.org/global/sigs/vrdx/vdb-catalog.

Cependant, deux limitations importantes affectent la plupart des bases de données de vulnérabilités :

1. Elles se concentrent sur l'exploitabilité technique plutôt que sur l'exploitation active.
2. Elles ne sont pas mises à jour assez rapidement pour avertir de certaines menaces qui se propagent rapidement.

L'exploitabilité par rapport à l'exploitation

Les informations des bases de données sur les vulnérabilités sont presque toujours axées sur l'exploitabilité technique, une évaluation de la probabilité que l'exploitation d'une certaine vulnérabilité aboutisse à des dommages plus ou moins graves pour les systèmes ou les réseaux. Dans la NVD, ceci est mesuré par le système de notation CVSS.

Cependant, exploitabilité technique n'est pas synonyme d'exploitation active. Les cotes CVSS de base de données fournissent une mesure raisonnable, suffisamment précise et facile à comprendre, à condition de savoir ce qu'elle signifie. Toutefois, à moins qu'une cote de base de données ne soit modifiée par une cote temporelle ou environnementale, elle ne vous indique que la gravité hypothétique de la vulnérabilité, sans mentionner si elle est réellement exploitée dans la pratique.

La figure 6-2 illustre le type de renseignement sur la sécurité fournis par un outil de renseignement sur les vulnérabilités. Dans ce cas, le risque posé par une vulnérabilité est déterminé en fonction de rapports impliquant l'apparition de la CVE avant que la NVD ne lui ait attribué une cote CVSS.

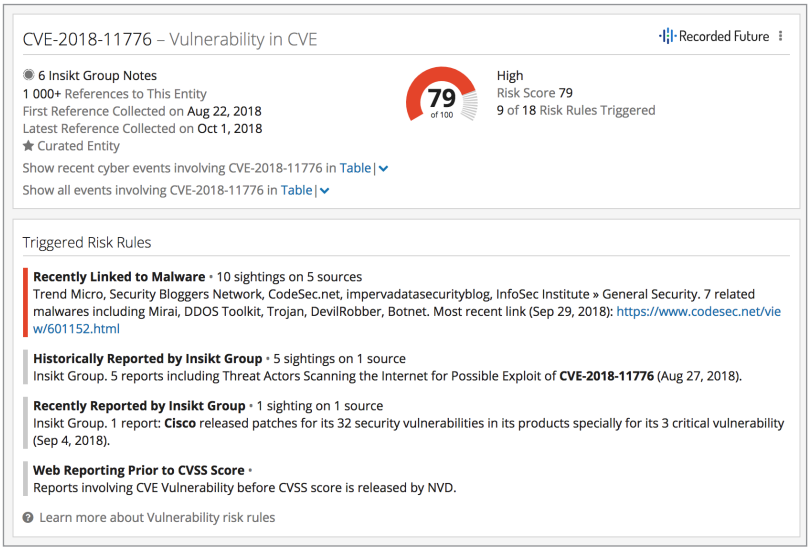


Figure 6-2 : Le renseignement sur la sécurité lié à une vulnérabilité (Source : Recorded Future)

Une leçon de choses sur la différence entre le "risque officiel" selon la NVD et le "risque réel" posé par une vulnérabilité en pratique est la référence CVE-2017-0022. Malgré sa cote de gravité CVSS de 4,3 seulement (moyenne), Recorded Future a considéré cette vulnérabilité comme l'une des 10 principales vulnérabilités utilisées en 2017. Le vrai risque est très élevé parce que les auteurs de menaces ont ajouté cette vulnérabilité au Neutrino Exploit Kit où il joue un rôle essentiel en vérifiant si un logiciel de sécurité est installé sur un système cible.

La semaine prochaine par rapport à maintenant

Un autre défaut de nombreuses bases de données sur les vulnérabilités est leur lenteur. Par exemple, 75 % des vulnérabilités déclarées apparaissent sur d'autres sources en ligne avant de figurer dans la NVD, et il faut en moyenne une semaine à ces vulnérabilités pour y apparaître. C'est un problème très grave, parce qu'il entrave les équipes de sécurité dans la course aux correctifs avant que des adversaires ne puissent exploiter la vulnérabilité, comme illustré à la Figure 4-3.

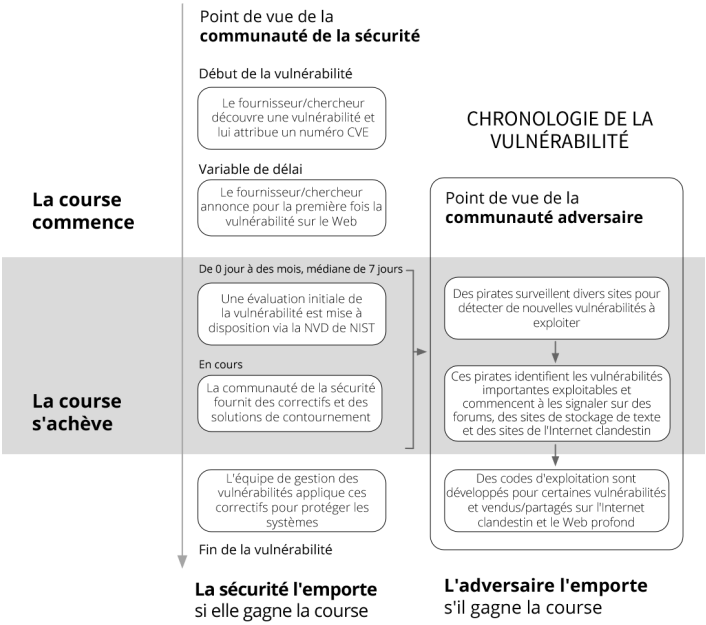


Figure 6-3 : La course entre les professionnels de la sécurité et leurs adversaires.

La manière informelle de divulguer et d'annoncer les vulnérabilités contribue à retarder leur reconnaissance dans les bases de données de vulnérabilités. Généralement, un fournisseur ou un chercheur révèle la vulnérabilité à la NVD, qui attribue un CVE et commence une analyse. Dans l'intervalle, le fournisseur ou le chercheur publie plus d'informations sur son propre blog ou un compte de réseau social. Bonne chance pour recueillir des données de ces sources disparates et difficiles à trouver avant que des criminels ne développent une validation technique de logiciel et ne l'ajoutent aux kits de code d'exploitation malveillant !

Pour plus de détails sur les processus que les auteurs de menaces utilisent pour exploiter les vulnérabilités, consultez le billet de blog de Recorded Future « Behind the Scenes of the Adversary Exploit Process » (Vue en coulisse du processus d'exploitation de l'adversaire).

Le renseignement sur les vulnérabilités et les risques réels

Le moyen le plus efficace pour évaluer le risque réel d'une vulnérabilité de votre organisation est de combiner :

- ☑ Les données d'analyse des vulnérabilités internes
- ☑ Le renseignement externe provenant de nombreuses sources différentes
- ☑ La compréhension des raisons pour lesquelles les auteurs de menaces ciblent certaines vulnérabilités sans s'intéresser à d'autres.

Analyse interne des vulnérabilités

Presque toutes les équipes de gestion des vulnérabilités analysent leurs systèmes internes pour détecter les vulnérabilités, établissent des corrélations des résultats avec les informations signalées dans les bases de données de vulnérabilités et utilisent le résultat obtenu pour déterminer ce qui doit être corrigé. Il s'agit d'une utilisation élémentaire du renseignement sur les menaces opérationnelles, même si nous ne voyons généralement pas cela de cette façon.

L'analyse classique est un excellent moyen de déclasser les vulnérabilités qui n'apparaissent pas sur vos systèmes. En soi, cependant, l'analyse n'est pas une manière adéquate de hiérarchiser avec précision les vulnérabilités détectées.

Jalons pour les risques posés par les vulnérabilités

Une puissante façon d'évaluer le risque d'une vulnérabilité est d'examiner dans quelle mesure elle a progressé entre sa première identification et sa mise à disposition, sa conversion en arme et sa marchandisation dans des kits de code d'exploitation malveillant.

Le niveau de risque réel augmente considérablement au fur et à mesure qu'elle passe par les jalons illustrés à la Figure 6-4. Des renseignements généraux sur les vulnérabilités révèlent la progression d'une vulnérabilité sur cette voie.

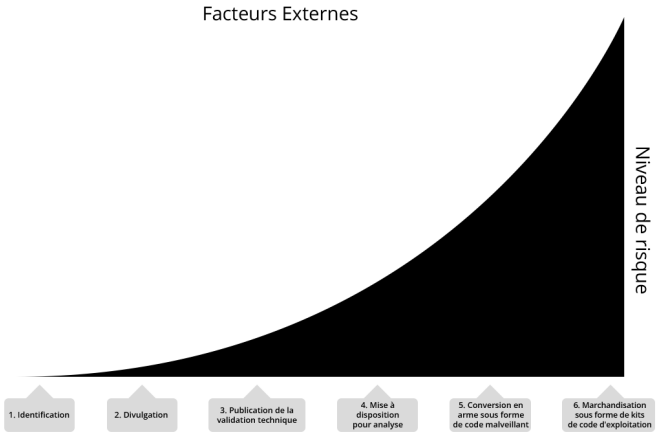


Figure 6-4 : Le risque réel augmente considérablement quand les vulnérabilités arrivent au niveau de conversion en arme et de marchandisation.

Comprendre l'adversaire

Comme nous l'avons vu ailleurs dans ce livre, le bon renseignement sur la sécurité ne doit pas se borner à fournir des informations sous forme de cotes et de statistiques. C'est pour cette raison que le renseignement sur les vulnérabilités permet de mieux comprendre comment et pourquoi les auteurs de menaces ciblent certaines vulnérabilités et en ignorent d'autres. Nous décrivons ci-dessous les sources de renseignement qui peuvent contribuer à faire comprendre cela.

Comment créer des cotes de risque qui ont un sens

Outre les caractéristiques techniques, quels sont les facteurs qui peuvent être utilisés pour calculer les cotes de risque des vulnérabilités ? Le système natif de notation de risque de Recorded Future incorpore des données sur l'adoption criminelle, des modèles de partage de code d'exploitation malveillant et le nombre de liens vers les logiciels malveillants. Ces informations proviennent souvent de sources à accès difficile, comme des forums de l'Internet clandestin.

Sources de renseignement

Les données d'analyses d'actifs et de bases de données externes sur les vulnérabilités ne sont que les points de départ de la production de renseignement qui vous permette d'évaluer les risques posés par les vulnérabilités. Le renseignement sur les vulnérabilités doit comprendre des données d'un grand éventail de sources variées, sinon les analystes risquent de ne pas détecter des vulnérabilités émergentes avant qu'il ne soit trop tard.

Citons parmi les sources d'information précieuses pour l'évaluation des risques véritables pour votre entreprise :

- ☑ **Les sites relatifs à la sécurité de l'information**, y compris les blogs de fournisseurs, la divulgation officielle d'informations sur les vulnérabilités et les sites d'actualités sur la sécurité
- ☑ **Les réseaux sociaux** où le partage de liens fournit des points de départ pour découvrir des renseignements utiles
- ☑ **Les dépositaires de codes** tels que GitHub, qui donne des aperçus du développement de code de validation technique pour les vulnérabilités
- ☑ **Les sites de stockage de texte,** comme Pastebin et Ghostbin (définis parfois, incorrectement, comme des sites de l'Internet clandestin), qui hébergent souvent des listes de vulnérabilités exploitables

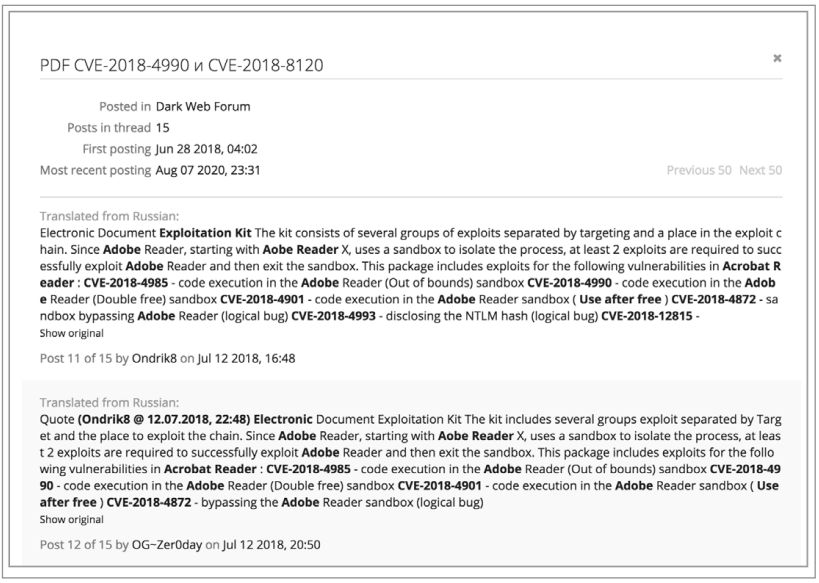
- ☑ **l'Internet clandestin**, composé de communautés et de marchés à accès interdit où les codes d'exploitation malveillants sont développés, partagés et vendus
- ☑ **Les forums** auxquels l'accès n'est pas interdit et sans exigence d'utilisation de logiciel spécifique où les auteurs de menaces échangent des informations sur les vulnérabilités et sur les codes d'exploitation malveillants
- ☑ **Les flux techniques**, qui transmettent des flux de données sur des indicateurs susceptibles d'être malveillants qui ajoutent un contexte utile aux activités des logiciels malveillants et des kits de code d'exploitation malveillant

Bavardage sur les vulnérabilités sur l'Internet clandestin

Pour différentes raisons, il est difficile (et potentiellement dangereux) d'intercepter les conversations sur les canaux où les auteurs de menaces communiquent et exercent leurs activités :

- Les forums souterrains sont difficiles à trouver (après tout, il n'existe pas de Google de l'Internet clandestin)
- Les auteurs de menaces changent d'endroit chaque fois qu'ils estiment que leur anonymat est menacé.
- Il faut effectuer beaucoup de recherches pour trouver des miettes d'informations qui sont pertinentes pour votre sécurité.
- Ces forums peuvent exiger des droits d'entrée ou l'endossement de membres existants de la communauté pour vous y donner accès.
- Beaucoup de ces forums ne fonctionnent qu'en langue locale.

C'est ici qu'entrent en jeu les fournisseurs de renseignement sur les menaces experts en collecte et analyse du renseignement de l'Internet clandestin. Ils offrent des informations contextualisées provenant de forums de l'Internet clandestin sur des vulnérabilités directement pertinentes pour votre réseau, sans vous mettre en danger ni menacer votre entreprise.


PDF CVE-2018-4990 и CVE-2018-8120

Posted in Dark Web Forum
Posts in thread 15
First posting Jun 28 2018, 04:02
Most recent posting Aug 07 2020, 23:31
Previous 50 Next 50

Translated from Russian:
Electronic Document **Exploitation Kit** The kit consists of several groups of exploits separated by targeting and a place in the exploit c hain. Since **Adobe** Reader, starting with **Aobe Reader** X, uses a sandbox to isolate the process, at least 2 exploits are required to succ essfully exploit **Adobe** Reader and then exit the sandbox. This package includes exploits for the following vulnerabilities in **Acrobat R eader** : **CVE-2018-4985** - code execution in the **Adobe** Reader (Out of bounds) sandbox **CVE-2018-4990** - code execution in the **Adob e** Reader (Double free) sandbox **CVE-2018-4901** - code execution in the **Adobe** Reader sandbox (**Use after free**) **CVE-2018-4872** - sa ndbox bypassing **Adobe** Reader (logical bug) **CVE-2018-4993** - disclosing the NTLM hash (logical bug) **CVE-2018-12815** -
Show original

Post 11 of 15 by Ondrik8 on Jul 12 2018, 16:48

Translated from Russian:
Quote **(Ondrik8 @ 12.07.2018, 22:48) Electronic** Document Exploitation Kit The kit includes several groups exploit separated by Targ et and the place to exploit the chain. Since **Adobe** Reader, starting with **Aobe Reader** X, uses a sandbox to isolate the process, at leas t 2 exploits are required to successfully exploit **Adobe** Reader and then exit the sandbox. This package includes exploits for the follo wing vulnerabilities in **Acrobat Reader** : **CVE-2018-4985** - code execution in the **Adobe** Reader (Out of bounds) sandbox **CVE-2018-49 90** - code execution in the **Adobe** Reader (Double free) sandbox **CVE-2018-4901** - code execution in the **Adobe** Reader sandbox (**Use after free**) **CVE-2018-4872** - bypassing the **Adobe** Reader sandbox (logical bug)
Show original

Post 12 of 15 by OG~Zer0day on Jul 12 2018, 20:50

Figure 6-5 : Un échange d'informations entre des auteurs de menaces sur un forum de l'Internet clandestin traduit du russe. (Source : Recorded Future)

Cas d'utilisation de recoupement des renseignements

Pour évaluer avec précision le risque réel, vous devez être capable de corréler les informations de plusieurs sources de renseignements sur les menaces. Une fois que vous commencez à comprendre la façon dont les références individuelles se combinent pour raconter toute l'histoire, vous serez en mesure d'organiser les renseignements que vous possédez selon les jalons de risque par lesquels une vulnérabilité passe habituellement.

Vous pouvez, par exemple, remarquer qu'une nouvelle vulnérabilité est révélée sur le site Web d'un fournisseur. Puis, vous découvrez un tweet avec un lien vers un code de validation technique sur GitHub. Ensuite, vous voyez qu'un code de logiciel d'exploitation malveillant est en vente sur un forum de l'Internet clandestin. Et enfin, il est possible que vous voyiez des bulletins d'actualités sur l'exploitation de la vulnérabilité dans le milieu naturel.

Voici un autre exemple. Le site Web d'un centre d'analyse et de partage d'informations (ISAC) pour votre secteur d'activité montre qu'une organisation comme la vôtre a été victime d'un kit de code d'exploitation qui attaque une vulnérabilité d'une application logicielle spécialisée spécifique au secteur. Vous constatez qu'il existe quatre copies de ce logiciel dans des recoins de votre organisation qui n'ont pas reçu de correctif depuis trois ans.

Les recoupements de ce genre de renseignement vous permettent de vous retirer de la « course aux correctifs pour absolument tout » et de vous concentrer sur les vulnérabilités qui présentent le plus grand risque réel.

Combler les lacunes en matière de risques entre les services de sécurité, l'exploitation et la direction de l'entreprise

Dans la plupart des organisations, la responsabilité de la protection contre les vulnérabilités incombe à deux équipes :

1. L'équipe en charge de la gestion des vulnérabilités effectue des analyses et hiérarchise les vulnérabilités en fonction du risque potentiel.
2. L'équipe des opérations informatiques déploie des correctifs et remédie aux problèmes des systèmes affectés.

Cette dynamique crée une tendance à aborder la gestion de la vulnérabilité "en fonction du nombre." Par exemple, l'équipe de gestion des vulnérabilités du service de sécurité peut déterminer que plusieurs vulnérabilités des serveurs Web Apache présentent un risque très élevé pour l'entreprise et devraient être prioritaires. Toutefois, il est possible que l'équipe des opérations informatiques soutienne beaucoup plus de systèmes Windows que de serveurs Apache. Si les membres de l'équipe sont évalués strictement d'après le nombre de systèmes corrigés, ils ont intérêt à se concentrer sur les vulnérabilités Windows moins prioritaires.

Le renseignement sur l'exploitabilité prépare également votre entreprise à trouver le bon équilibre entre l'application de correctifs aux systèmes vulnérables et l'interruption des activités d'exploitation. La plupart des entreprises détestent perturber la continuité de l'exploitation. Toutefois, si vous savez qu'un correctif va la protéger contre un risque réel imminent, une courte interruption est complètement justifiée.

La matrice des jalons de risque décrits ci-dessus facilite fortement la communication du danger présenté par une vulnérabilité à vos équipes de sécurité et d'exploitation, et même à la direction, voire au conseil d'administration. Ce niveau de visibilité dans la justification de décisions adoptées en fonction des vulnérabilités augmente la confiance dans l'équipe de sécurité de l'ensemble de l'entreprise.

Pour combler le fossé entre les équipes de gestion des vulnérabilités et celles des opérations informatiques, présentez les risques d'exploitabilité comme l'un des principaux moteurs de la hiérarchisation des correctifs. Dotez l'équipe de gestion des vulnérabilités de données plus contextualisées sur le risque d'exploitabilité pour qu'elle puisse identifier un nombre plus limité de CVE à haut risque, exigeant ainsi moins de l'équipe des opérations informatiques. L'équipe des opérations informatiques pourra alors accorder la plus haute priorité à un petit nombre de correctifs cruciaux tout en disposant du temps nécessaire pour s'attaquer à d'autres objectifs.

Chapitre 7

Le renseignement sur les menaces, 1re partie : connaître les attaquants

Dans ce chapitre

- Examiner le rôle des analystes de menaces
- Voyez comment les conversations au sein des communautés clandestines offrent des possibilités de recueillir de précieux renseignements sur la sécurité
- Examinez les cas d'utilisation pour appliquer les connaissances sur les attaquants à la sécurité

"Le problème pour le capitalisme, c'est que les choses qui donnent confiance engendrent aussi l'environnement de la fraude."

— James Surowiecki

Le renseignement sur les menaces dans le cadre du renseignement sur la sécurité

Jusqu'à récemment, de nombreux sujets abordés dans ce manuel étaient appelés dans la communauté de la sécurité « renseignement sur les menaces ». Cependant, comme le terme « renseignements sur les menaces » est devenu si étroitement lié aux informations sur les menaces directes contre les systèmes informatiques traditionnels,

les experts informés utilisent maintenant « renseignement sur la sécurité », qui englobe ces informations et des détails supplémentaires sur les risques liés à des aspects tels que les tiers, la présence de marques sur des sites Web et des plateformes de réseaux sociaux n'appartenant pas au réseau d'entreprise, les risques menaçant les ressources physiques du monde entier, et davantage encore.

Ce changement n'a pas éliminé le besoin de renseignement sur les menaces. Il est toujours essentiel de permettre aux analystes de menaces d'exécuter leurs fonctions les plus importantes, notamment :

- ☑ Identifier les auteurs qui menacent le plus activement l'organisation
- ☑ Comprendre les motivations et les cibles des attaquants
- ☑ Enquêter sur leurs TTP et les documenter
- ☑ Suivre des tendances macro qui affectent l'entreprise, y compris les tendances pertinentes à son secteur et aux régions où elle exerce ses activités.

Une solution de renseignement sur la sécurité est essentielle au succès des analystes de menaces, car elle identifie les menaces les plus pertinentes, diminue le temps passé à les rechercher et produit davantage d'informations à leur sujet, souvent en provenance de sources auxquelles les analystes ne pourraient pas ou pourraient difficilement accéder eux-mêmes.

Dans ce chapitre et dans le prochain, nous examinerons plusieurs des principales responsabilités des analystes de menaces.

Comprendre votre ennemi

Les analystes de menaces ne peuvent pas se concentrer uniquement sur la détection et la réponse aux menaces déjà présentes dans leur environnement. Ils doivent anticiper les attaques en recueillant du renseignement sur la sécurité relatif aux gangs de cyber-criminels, aux groupes de pirates soutenus

par des États, aux « hacktivistes » idéologiques et aux autres personnes qui ciblent leurs organisations.

Examinons par exemple le genre de renseignement que vous pourriez trouver sur les gangs de cybercriminels motivés par le profit. Il s'agit d'une cible de renseignement importante, car le « Verizon 2020 Data Breach Investigations Report » (Rapport 2020 sur les enquêtes de violation de données de Verizon) attribue 55 % des violations confirmées au crime organisé (figure 7-1).

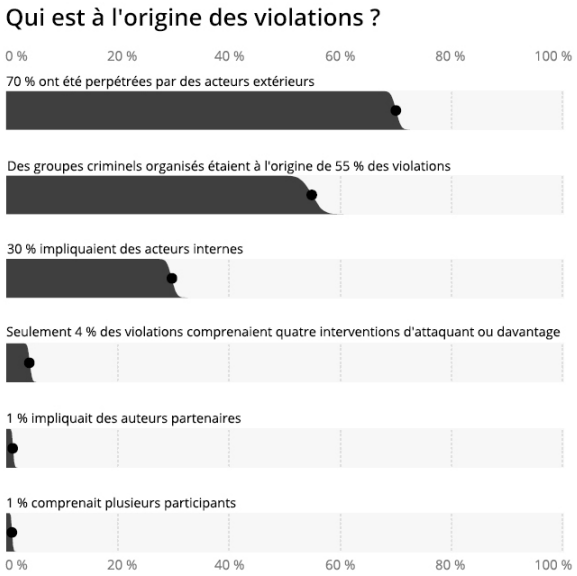


Figure 7-1 : Auteur externe principal de différentes violations de données (Source : rapport de Verizon sur la violation de données de 2020)

Ces données correspondent aux renseignements recueillis par Recorded Future sur l'Internet clandestin, qui montrent que les groupes criminels organisés (OCG) emploient des pirates indépendants pour escroquer les entreprises et les particuliers. Ces groupes fonctionnent comme des entreprises légitimes de bien des façons, avec une hiérarchie de membres qui travaillent en équipe pour créer, exploiter et tenir à jour des arnaques.

Un OCG typique est contrôlé par un seul cerveau. Il peut inclure des spécialistes possédant l'expertise requise pour les crimes qu'ils commettent. Par exemple, des banquiers avec nombreuses relations dans le secteur financier peuvent prendre des dispositions de blanchiment d'argent, des faussaires peuvent être chargés de faux documents et de formalités administratives, des chefs de projets professionnels peuvent superviser les aspects techniques des opérations, des ingénieurs logiciels écrivent du code et d'autres pirates très compétents peuvent être impliqués dans des tâches spécifiques. Certains groupes comprennent même d'anciens membres des forces de l'ordre qui recueillent des renseignements et se livrent à des activités de contre-espionnage.

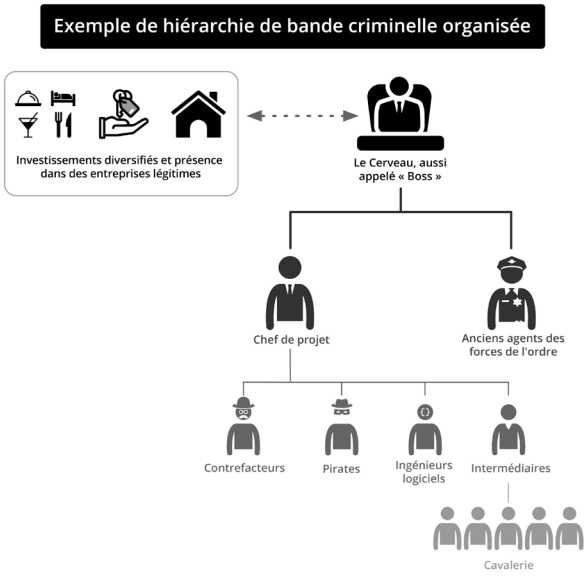


Figure 7-2 : Organigramme typique d'un syndicat du cybercrime. (Source : Recorded Future)

Les membres de ces syndicats du cybercrime ont tendance à avoir des liens solides dans la vie réelle et sont souvent des membres respectés de leurs groupes sociaux. Ils ne se considèrent certainement pas comme pas comme des criminels de gangs de rue. Ils croisent rarement ce que la plupart des gens considèrent des gangsters ordinaires,

préférant rester dans l'ombre pour ne pas attirer l'attention des forces de l'ordre et des branches locales de la mafia. Cependant, les arnaques qui nécessitent un grand nombre de personnes, comme celles qui exigent que l'on prenne l'argent comptant à plusieurs distributeurs automatiques simultanément, peuvent inclure une chaîne d'intermédiaires qui recrutent et gèrent la "cavalerie" qui fait le travail sur le terrain.

Les communautés criminelles et l'Internet clandestin

Il est très rare que des analystes de menaces puisse imputer une cyberattaque à une seule personne travaillant seule. Les attaques sophistiquées exigent en général un large éventail de compétences et d'outils, ainsi qu'une infrastructure capable de lancer et de prendre en charge des campagnes qui utilisent le ransomware, le hameçonnage et d'autres dispositifs techniques ainsi que des techniques d'ingénierie sociale.

De nos jours, tous ces produits et services sont en vente ou en location au sein d'une économie souterraine perfectionnée. Les cybercriminels, les pirates et leurs complices échangent des informations et effectuent des opérations liées à des activités illicites sur la toile profonde (les domaines de l'Internet que ne peuvent atteindre les moteurs de recherche) et l'Internet clandestin (les zones qui ne sont accessibles qu'avec des logiciels et des outils qui masquent l'identité des visiteurs).

Des quartiers privés

Tous les cybercriminels n'opèrent pas exclusivement dans ce que l'on appellerait techniquement l'Internet clandestin. Certains édifient des communautés basées sur un forum de discussion assez ordinaire, chiffré derrière des informations de connexion, et utilisent des technologies comme Jabber et Telegram pour se livrer à leurs activités.

Les membres potentiels de ce réseau souterrain sont approuvés par des participants actifs dans des salles de chat et des forums avant d'être acceptés. Il est possible qu'ils doivent payer un droit d'entrée allant de 50 USD à 2 000 USD ou

davantage. En fait, on sait qu'un forum au moins exige un dépôt de plus de 100 000 USD de ses membres potentiels.

Un atout et une faiblesse

l'Internet clandestin et les communautés criminelles donnent aux auteurs de menace accès à des informations, des outils, une infrastructure et des services contractuels qui multiplient leur puissance et leur portée. Cependant, ces communautés posent également des risques pour les auteurs de menaces, car ils sont susceptibles d'être surveillés et de procurer ainsi du renseignement sur la sécurité qui permet aux équipes de sécurité d'anticiper les attaques et d'en sortir victorieuses.

Familiarisez-vous avec vos réseaux de l'Internet clandestin

Nous avons constaté que l'Internet clandestin était organisé en trois communautés distinctes : les forums clandestins de niveau inférieur, les forums clandestins de niveau supérieur et les marchés de l'Internet clandestin. Une analyse a révélé qu'un groupe important d'auteurs publiaient sur des forums de niveaux inférieurs et supérieurs, ce qui indique une relation entre ces deux communautés. Toutefois, les marchés de l'Internet clandestin sont en grande partie déconnecté de ces forums. Pour acquérir une meilleure compréhension de la façon dont la criminalité clandestine maintient une hiérarchie parmi ses utilisateurs, lisez les recherches suivantes de Recorded Future : « Dark Networks: Social Network Analysis of Dark Web Communities » (Réseaux clandestins : analyse des réseaux sociaux des communautés de l'Internet clandestin).

Tirer les conclusions

Le renseignement sur les menaces recueilli auprès des communautés criminelles souterraines donne un aperçu des motivations, des méthodes et des tactiques des auteurs de menaces quand il est corrélé avec des informations du Web en surface, y compris des flux et des indicateurs techniques.

La puissance du renseignement sur la sécurité véritablement contextualisé est clairement prouvée dans la façon dont il

rassemble des données de différentes sources et établit des liens entre des informations disparates.

Les informations contextuelles suivantes peuvent par exemple être utilisées pour convertir en renseignement des actualités sur une nouvelle variante de logiciel malveillant :

- ☑ Des preuves que des auteurs de menace utilisent ce logiciel malveillant dans un milieu naturel
- ☑ Des rapports selon lesquels des kits de code d'exploitation utilisant le logiciel malveillant sont en vente sur l'Internet clandestin
- ☑ La confirmation que les vulnérabilités ciblées par les kits de code d'exploitation malveillant existent dans votre entreprise

Surveillez l'Internet clandestin et les communautés criminelles pour voir s'il y a des mentions directes de votre organisation et de ses actifs. Ces mentions indiquent souvent des cibles ou des violations potentielles. Surveillez aussi les mentions de votre secteur et d'autres termes moins spécifiques susceptibles de se rapporter à vos activités. Utiliser le renseignement sur la sécurité pour évaluer les risques de cette manière renforce votre confiance en vos défenses et vous permet de prendre de meilleures décisions.

Cas d'utilisation : Une réponse aux incidents plus complète

Lorsque des indicateurs d'une menace sont détectés, les équipes des SecOps prennent des mesures immédiates pour protéger les actifs ciblés. Cependant, elles comptent sur les analystes de menaces pour rechercher l'attaque et fournir des informations supplémentaires pour mieux mettre fin à l'attaque, corriger ses effets et empêcher qu'elle se reproduise à l'avenir.

Par exemple, les analystes de menaces sont souvent en mesure d'attribuer une attaque à un groupe spécifique de piratage informatique cybercriminel ou parrainé par un État et d'effectuer des recherches sur les TTP du groupe. Les

équipes de sécurité pourraient alors utiliser ce renseignement pour prendre des mesures comme trouver d'autres cas de programmes malveillants et d'e-mails d'hameçonnage utilisés dans l'attaque, nettoyer les systèmes affectés, mettre les e-mails en quarantaine, obliger les comptes compromis à modifier leur mot de passe et prendre d'autres mesures pour perturber la chaîne de destruction de l'attaquant.

La recherche d'une réponse complète aux incidents et de mesures correctives prend beaucoup de temps. Pour obtenir une réponse rapide, il est essentiel d'utiliser une solution de renseignement sur la sécurité dotée de fonctionnalités d'automatisation et d'intégration pour recueillir et traiter de grands volumes de données provenant de nombreuses sources et trouver un contexte et des informations pertinents. La solution de renseignement sur la sécurité doit également être capable d'automatiser les flux de travail pour analyser le renseignement et le transmettre rapidement aux équipes de sécurité et à la direction appropriées, en utilisant leurs outils de sécurité existants et dans leurs formats préférés.

Cas d'utilisation : Recherche de menaces proactive

La plupart des programmes de sécurité sont réactifs, ce qui signifie qu'ils s'appuient sur des alertes avant de prendre des mesures. Cependant, de nombreuses entreprises créent des équipes de chasseurs de menaces pour rechercher proactivement des indicateurs de menaces avant qu'une alerte ne soit générée et, dans l'idéal, avant que l'attaque n'ait réalisé de grands progrès.

Il existe des centaines d'indices que les chasseurs de menaces peuvent rechercher sur les réseaux et les terminaux. Ceux-ci comprennent : les fichiers de programmes malveillants, les modifications suspectes de clés de registre, de configurations système et les autorisations d'applications, les DLL, scripts et pilotes inhabituels, l'utilisation à mauvais escient d'utilitaires comme PowerShell et PsExec, les comportements anormaux de fichiers de tâche, les binaires qui initient des connexions en dehors du réseau d'entreprise, les séquences d'événements inhabituelles (par exemple, les applications qui téléchargent et

exécutent des scripts au démarrage) et les techniques utilisées pour dérober des informations d'identification.

Les solutions de renseignement sur la sécurité fournissent du renseignement sur les auteurs de menaces qui attaquent actuellement des entreprises semblables, ainsi que sur les techniques et les outils qu'ils utilisent. Ces informations permettent aux chasseurs de menaces d'éviter de tenter l'impossible en essayant de capter et d'analyser d'énormes quantités de données. Au lieu de cela, ils sont en mesure de hiérarchiser les recherches pour trouver les menaces les plus dangereuses pour leur entreprise et de se concentrer sur la recherche d'indicateurs et d'artefacts spécifiques liés à ces attaques.

Cas d'utilisation : Avertissement anticipé de fraude sur les paiements

Depuis la naissance du commerce, des criminels ont cherché des moyens de profiter facilement de ceux qui possèdent des biens et de tirer le meilleur parti de la technologie disponible à leur époque. Au 17e siècle en Angleterre, par exemple, l'augmentation des voyages en diligence au sein de la classe des riches marchands, combinée à l'invention du pistolet à silex, a donné naissance au bandit de grand chemin.

À l'époque du numérique, les entreprises qui effectuent des opérations en ligne remarquent que leurs données sont ciblées par différentes formes de cyberfraude.

Le terme "fraude sur les paiements" comprend une grande variété de techniques qui permettent aux cybercriminels de profiter de données de paiement compromises. Par exemple, ils peuvent recourir à l'hameçonnage pour collecter les informations de la carte de paiement. Des attaques plus complexes peuvent compromettre des sites de commerce électronique ou des terminaux de point de vente pour atteindre le même but. Une fois qu'ils ont obtenu des données de carte bancaire, les criminels peuvent les revendre (souvent sous forme de paquets de nombres) et s'en aller après avoir obtenu leur portion des bénéfices.

Un exemple de l'utilisation efficace du renseignement sur les menaces est de fournir aux analystes de menaces un avertissement anticipé des attaques futures liées à la fraude sur les paiements. La surveillance de sources comme les communautés clandestines, les sites de stockage de texte et d'autres forums pour trouver des numéros de cartes bancaires pertinents, des numéros d'identification bancaire ou des références spécifiques à des institutions financières peut vous permettre de détecter des opérations criminelles susceptibles d'affecter votre entreprise. Les analystes peuvent ensuite collaborer avec d'autres équipes de sécurité pour prévenir les attaques planifiées en corrigeant les vulnérabilités pertinentes, en augmentant la surveillance des systèmes ciblés et en renforçant les contrôles de sécurité.

Chapitre 8

Le renseignements sur les menaces, 2e partie : analyser les risques

Dans ce chapitre

- Examinez la valeur des modèles de risques tels que la matrice FAIR
- Voyez quelles sont les manières adéquates et inadéquates de recueillir des données sur les risques
- Découvrez comment le renseignement sur la sécurité vous permet de prévoir les probabilités d'attaque et les coûts financiers des attaques

"Établir et promouvoir les meilleures pratiques de gestion des risques liés à l'information qui ... [atteignent] le bon équilibre entre la protection de l'organisation et la gestion de l'entreprise."

- Énoncé de mission du FAIR Institute

Une fonction clé des analystes de menaces est de modéliser les risques et de donner aux gestionnaires les moyens de prendre des décisions éclairées sur la diminution des risques. La modélisation des risques propose un moyen d'évaluer objectivement les risques actuels et d'estimer des résultats clairs et quantifiables des investissements en cybersécurité.

Toutefois, de nombreux modèles de cyber-risques présentent les défaillances suivantes :

- ☑ Des sorties vagues, non quantifiées, souvent sous forme de graphiques de type "feux de circulation" affichant des niveaux de menace en vert, jaune et rouge.
- ☑ Des estimations de probabilités de menace et de coûts rassemblées à la hâte, basées sur des informations partielles, et pleines d'hypothèses sans fondement

Des sorties non quantifiées sont peu susceptibles de produire des résultats pratiques, et les modèles fondés sur des entrées erronées aboutissent à des scénarios GIGO ("foutaises en entrée, foutaises en sortie") dont les sorties semblent précises mais sont en fait trompeuses. Pour éviter ces problèmes, les entreprises ont besoin d'un modèle de risque bien conçu et de beaucoup d'informations actuelles valides, notamment de renseignement sur la sécurité.

L'évaluation des risques de cybersécurité ne devrait pas se fonder uniquement sur des critères définis pour prouver que l'on se conforme aux règlements. Si l'on applique de tels critères, l'évaluation des risques se borne souvent à cocher des cases de contrôles de cybersécurité comme les pare-feu et le chiffrement. Compter le nombre de cases cochées vous donne souvent une image très trompeuse du risque réel.

Le modèle de risque FAIR

Le type d'équation au cœur de tout modèle de risque est simple :

« probabilité d'occurrence multiplié par impact = coût attendu »

Mais il est clair que les difficultés surgissent dans les menus détails. Heureusement, des personnes intelligentes ont développé de très bons modèles de risque et des méthodes que vous pouvez utiliser ou adapter à vos propres besoins. Une méthode qui nous plaît est le modèle FAIR (analyse des facteurs de risque informatique) du FAIR institute. La figure 6-1 montre la matrice de ce modèle.

La matrice FAIR vous aide à créer un modèle d'évaluation quantitative des risques comprenant des probabilités spécifiques de pertes causées par des types de menaces spécifiques.

SUR LE WEB

Pour en savoir plus sur FAIR, consultez le site Web du FAIR Institute. Ce modèle quantitatif pour la sécurité de l'information et les risques d'exploitation est axé sur la compréhension, l'analyse et la quantification du risque informatique réel en termes financiers.

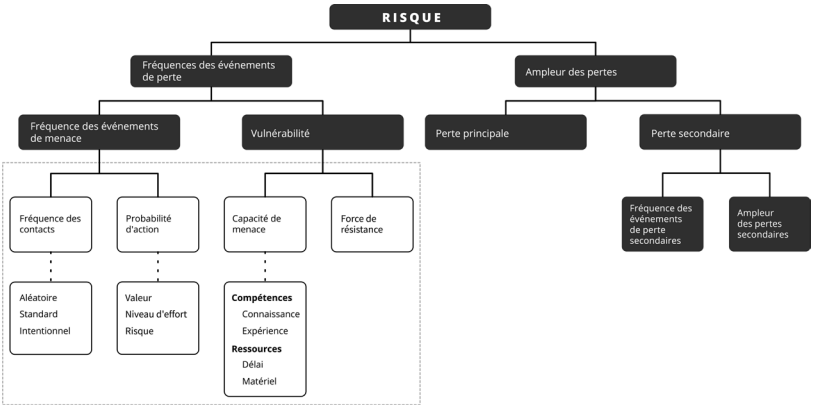


Figure 8-1 : La matrice FAIR, où les éléments obtenus par du renseignement sont mis en évidence. (Source : le FAIR Institute)

Les mesures et la transparence sont cruciales

La matrice FAIR (et les autres cadres semblables) vous permettent de créer des modèles de risques qui :

- ☑ Prennent des mesures définies du risque
- ☑ Sont transparents en ce qui concerne les hypothèses, les variables et les résultats
- ☑ Montrent les probabilités spécifiques de pertes en termes financiers

Les mesures, les formules, les hypothèses, les variables et les résultats doivent être rendus transparents pour être décrits, défendus, et modifiés. Étant donné qu'une grande partie du modèle FAIR est défini en termes commerciaux et financiers, les cadres, les responsables de secteur d'activité et d'autres intervenants peuvent apprendre à parler le même langage et à classer les actifs, les menaces et les vulnérabilités et de la même façon.

Essayez autant que possible d'incorporer des probabilités spécifiques sur les pertes futures dans votre modèle de risque. Les probabilités spécifiques permettent aux gestionnaires de risques et aux cadres supérieurs de discuter du modèle et des améliorations éventuelles à y apporter. Ils feront alors plus confiance au modèle et à ses recommandations.

Quel est l'énoncé le plus utile ?

" La menace d'attaques DDoS contre notre entreprises est passée d'élevée à moyenne (du rouge au jaune)."

Ou

"Il existe une probabilité de 20 pour cent que notre entreprise subisse une perte de plus de 300 000 dollars dans les 12 mois à venir parce qu'une attaque de déni de service distribué (DDoS) perturbera la disponibilité de nos sites Web orientés clients."

Le renseignement sur la sécurité et les probabilités de menaces

Comme indiqué du côté gauche de la Figure 6-1, une grande partie de la création d'un modèle de menaces consiste à estimer la probabilité de réussite des attaques (ou de "fréquence d'événements de perte" pour utiliser le langage de la matrice FAIR).

La première étape consiste à créer une liste de catégories de menaces qui pourraient toucher l'entreprise. Cette liste comprend généralement les logiciels malveillants, les attaques de hameçonnage, les kits de code d'exploitation malveillant

d'applications Web, les attaques par déni de service distribué (DDoS), le ransomware et beaucoup d'autres menaces.

L'étape suivante est beaucoup plus difficile : estimer les probabilités que les attaques surviennent et qu'elles réussissent (autrement dit, les chances que l'entreprise ait des vulnérabilités liées aux attaques et que les contrôles existants ne soient pas suffisants pour les arrêter).

Un membre de l'équipe GRC (gouvernance, risque et conformité) demande à un analyste de la sécurité : "Quelle est la probabilité que nous devions faire face à cette attaque spécifique" ? L'analyste de la sécurité (qui ne peut réellement pas répondre à cela) réfléchit pendant 30 secondes aux expériences antérieures et aux contrôles de sécurité actuels et se lance dans de la pure spéculation :

Pour éviter d'avoir l'air de ne rien y connaître, votre équipe de sécurité a besoin de réponses mieux éclairées que celle-là. Le renseignement sur la sécurité, et plus particulièrement le renseignement sur les menaces, permettent de répondre à des questions telles que :

- ☑ Quels sont les auteurs de menaces qui utilisent cette attaque et ciblent-ils notre secteur ?
- ☑ À quelle fréquence cette attaque spécifique a-t-elle récemment été observée par des entreprises comme la nôtre ?
- ☑ La tendance est-elle à la hausse ou à la baisse ?
- ☑ Quelles vulnérabilités cette attaque exploite-t-elle (et ces vulnérabilités sont-elles présentes dans notre entreprise) ?
- ☑ Quel genre de dommages techniques et financiers cette attaque a-t-elle causé dans des entreprises comme la nôtre ?

Les analystes doivent encore très bien connaître l'entreprise et ses défenses, mais le renseignement sur les menaces enrichit leur connaissance des attaques, de leurs auteurs et de leurs cibles. Il fournit également des données sur la fréquence des attaques.

Les figures 6-2 et 6-3 montrent certaines des formes que pourrait prendre le renseignement. La figure 6-2 indique les types de questions sur un logiciel malveillant auxquelles une solution de renseignement sur les menaces peut répondre pour les analystes.

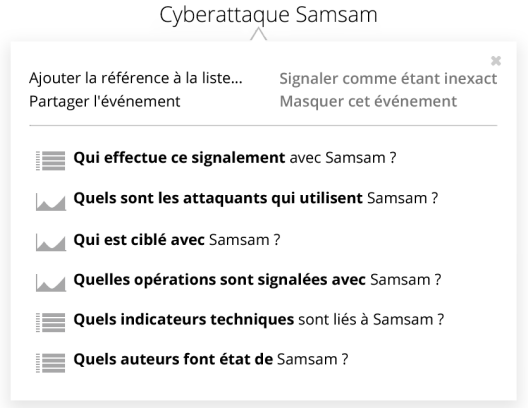


Figure 8-2 : Questions sur un logiciel malveillant auxquelles une solution de renseignement sur la sécurité peut répondre. (Source : Recorded Future)

La figure 6-3 montre l'évolution de la prolifération des familles de ransomware.

La ligne de tendance à la droite de chaque famille de ransomware indique l'augmentation ou la diminution des références dans un énorme éventail de sources de données sur les menaces comme les référentiels de code, les sites de stockage de texte, les blogs à propos des recherches sur la sécurité, les forums criminels et les forums .onion (accessibles via Tor). Des informations supplémentaires sont peut-être disponibles sur la façon de connecter les familles de ransomware aux auteurs de menaces, aux cibles et aux kits de code d'exploitation malveillant.

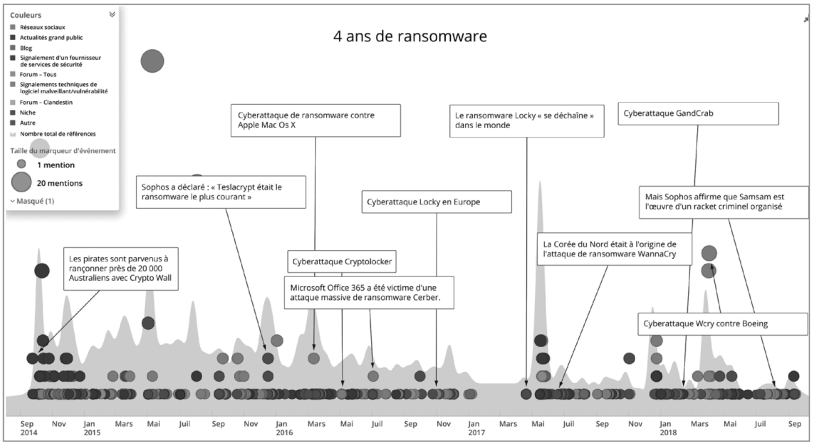


Figure 8-3 :Chronologie décrivant la prolifération de nouvelles familles de ransomware. (Source : Recorded Future)

Le renseignement sur la sécurité et le coût financier des attaques

L'autre composant essentiel des formules de notre modèle est le coût probable des attaques réussies. La plupart des données d'estimation de coût sont susceptibles de provenir de l'intérieur de l'organisation. Cependant, le renseignement sur la sécurité peut fournir des points de référence utiles sur des sujets comme :

- ☑ Le coût d'attaques semblables sur des entreprises de la même taille dans le même secteur
- ☑ Les systèmes qui doivent être corrigés après une attaque et le type de correctif dont ils ont besoin

Nous décrirons de façon plus approfondie la gestion des risques au chapitre 12, notamment le cadre de risque de catégorie de menace (TCR) développé par Levi Gundert de Recorded Future, et expliqué en détail dans son livre, « The Risk Business, What CISOs Need to Know About Risk-Based Cybersecurity » (Le secteur du risque, ce que les CISO doivent savoir sur la cybersécurité basée sur les risques).

Chapitre 9

Le renseignement sur les tiers

Dans ce chapitre

- Examinez l'impact de l'augmentation des risques posés par les tiers
- Comprenez pourquoi les évaluations statiques des risques posés par les tiers sont inadéquates
- Découvrez pourquoi l'utilisation du renseignement sur la sécurité automatisé, en temps réel, est le meilleur moyen d'atténuer les risques posés par les tiers

« Une chaîne n'est pas plus forte que son maillon le plus faible. »

— Proverbe

Les risques posés par les tiers sont considérables

Étant donné que les chaînes logistiques actuelles sont si étroitement intégrées, il est crucial de tenir compte de la sécurité chez nos partenaires, fournisseurs et autres tiers lors de l'évaluation du profil de risque de notre propre entreprise.

Une étude récente du Ponemon Institute, « Digital transformation & Cyber Risk: What You Need to Know to Stay Safe » (Transformation numérique et cyber-risque : ce que vous devez savoir pour maintenir la sécurité), a constaté que 55 % des entreprises ont subi une violation de données provenant d'un tiers, et 53 % affirment que leurs outils

de gestion des risques posés par les tiers ne sont que peu efficaces ou inefficaces. Ces statistiques et d'autres statistiques connexes sont présentées à la figure 9-1.

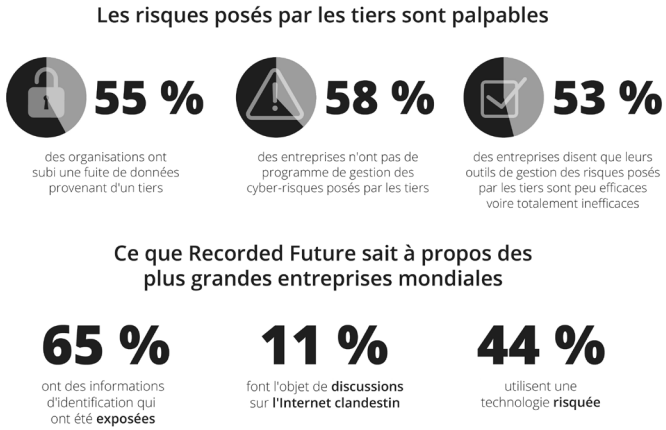


Figure 9-1 : La plupart des entreprise sont exposées à des risques importants posés par leurs relations avec des tiers. (Sources : Ponemon Institute et Recorded Future)

Il faut se rendre à l'evidence : Les attaques contre les tiers vont continuer à augmenter et à empirer, et vont compliquer davantage la gestion des cyberrisques.

Les méthodes d'évaluation traditionnelles des risques posés par les tiers reposent sur des résultats statiques tels que des auto-évaluations, des audits financiers, des rapports mensuels sur les nouvelles vulnérabilités découvertes dans les systèmes utilisés par une entreprise et des rapports occasionnels sur l'état de conformité de son contrôle de sécurité. Tous ces éléments deviennent rapidement obsolètes et ne fournissent pas les renseignements complets dont vous avez besoin pour prendre des décisions éclairées sur la gestion des risques posés par les tiers pour votre entreprise.

En revanche, le renseignement sur la sécurité en temps réel, particulièrement le renseignement sur les tiers, vous permet d'évaluer avec précision les risques posés par les tiers et de tenir à jour les évaluations au fur et à mesure que les conditions évoluent et que de nouvelles menaces apparaissent.

Les approches traditionnelles d'évaluation des risques sont inadéquates

Bon nombre des pratiques les plus courantes de gestion des risques posés par les tiers utilisées aujourd'hui sont à la traîne par rapport aux exigences de sécurité. Les évaluations statiques des risques, comme les audits financiers et les vérifications des certificats de sécurité sont toujours importantes, mais, souvent, elles ne présentent pas de contexte et ne sont pas adaptées aux circonstances du moment.

Les entreprises qui suivent des approches traditionnelles de gestion des risques posés par les tiers utilisent souvent les trois étapes suivantes :

1. Elles tentent de comprendre leur relation d'affaires avec un tiers et comment celle-ci expose l'entreprise à des menaces.
2. Fortes de cette compréhension, elles identifient des cadres d'évaluation de la santé financière, des contrôles d'entreprise, et de l'hygiène et de la sécurité informatiques du tiers, ainsi que des liens entre ces facteurs et l'approche de leur propre entreprise en matière de sécurité.
3. À l'aide de ces cadres d'évaluation, elles évaluent le tiers, en déterminant s'il respecte des normes de sécurité telles que SOC 2 ou FISMA. Parfois, elles effectuent un audit financier du tiers.

Ces étapes sont essentielles pour évaluer les risques posés par les tiers, mais elles ne donnent pas une image complète de la situation. Ces données sont statiques et ne peuvent pas refléter les conditions en évolution rapide ni les menaces émergentes. Souvent, l'analyse est trop simpliste pour produire des recommandations exploitables. Parfois, le rapport final est opaque, ce qui empêche tout examen approfondi des méthodes d'analyse. Tous ces facteurs créent des angles morts qui empêchent les décideurs de savoir avec certitude s'il est possible que des informations cruciales aient été négligées.

Lors de l'évaluation des risques posés par des tiers, ne vous limitez pas aux questionnaires d'auto-déclaration ni aux points de vue axés uniquement sur les propres défenses de sécurité de vos fournisseurs. Complétez cela en obtenant un point de vue externe et impartial sur le paysage de menaces de ces derniers.

Exercice mental

Imaginez que vous êtes passé par les étapes traditionnelles d'une évaluation de risques statique, comme décrit ci-dessus. Vous en avez conclu qu'un fournisseur de votre chaîne logistique est un collaborateur sûr.

À présent, ce fournisseur subit une violation de données qui a peut-être (ou n'a peut-être pas) exposé les données internes de votre entreprise. Pouvez-vous déterminer avec précision les mesures de sécurité proactives que vous devez adopter, le cas échéant, et la rapidité avec laquelle vous devez agir ?

Trois aspects qui doivent figurer dans le renseignement sur la sécurité

Pour évaluer avec précision les risques posés par les tiers en temps réel, vous avez besoin d'une solution qui offre un contexte immédiat sur le paysage de menaces actuel. Le renseignement sur la sécurité, transmis sous forme de renseignement sur les tiers, fournit un contexte indispensable, qui vous permet de déterminer quelles sont les lacunes des défenses de vos partenaires de chaîne d'approvisionnement qui présentent des risques significatifs pour votre entreprise. Ceux-ci comprennent non seulement les risques présents au moment de l'évaluation mais aussi les risques actuels et une perspective historique qui peut fournir des contextes additionnels pour détecter, prévenir et résoudre les risques.

Pour évaluer efficacement les risques posés par les tiers, une solution de renseignement sur les tiers doit :

1. Être automatisée et offrir des analyses pour trier rapidement et exhaustivement des quantités massives de données
2. Offrir des alertes en temps réel sur les menaces et la modification des risques
3. Procurer une visibilité continue des environnements de menaces en constante évolution de vos partenaires

L'automatisation et les analyses

Pour gérer les risques pour votre entreprise, vous devez avoir accès à des quantités massives de données sur les menaces provenant d'un grand éventail de sources diverses de l'Internet ouvert, de l'Internet clandestin, de sources techniques, d'actualités et de forums de discussion. Il en va de même pour l'évaluation des risques introduits par les tiers dans votre chaîne d'approvisionnement.

Toutefois, compte tenu de l'ampleur du contenu lié à la cybersécurité provenant de ces sources, présentant des milliards de faits, il vous faut une solution de renseignement sur les tiers qui recoure à l'automatisation et aux algorithmes pour recueillir et analyser et analyser ces informations. Elle doit être capable de :

- ☑ Analyser, classer, fusionner et indexer les points de données à l'aide de capacités de traitement des langues naturelles et de différents modèles d'analyse.
- ☑ Générer des cotes de risque objectives, basées sur des données, à l'aide d'une formule simple
- ☑ Fournir des preuves claires et accessibles pour étayer les cotes de risque attribuées

Mise à jour en temps réel des cotes de risque

Les évaluations statiques deviennent rapidement obsolètes. Les rapports de renseignement hebdomadaires ou mensuels produits par les analystes humains fournissent des aperçus essentiels mais arrivent souvent trop tard pour permettre une intervention efficace. La notation des risques est beaucoup plus efficace lorsqu'elle est mise à jour en temps réel et s'appuie sur un grand réservoir de sources. Ces capacités rendent les cotes de risque beaucoup plus fiables pour les évaluations immédiates et la prise de décisions de sécurité.

Par exemple, un partenaire commercial peut généralement être considéré comme à faible risque selon des rapports standard. Toutefois, imaginons qu'il subisse une violation de données susceptible ou non d'affecter votre entreprise. Si vous n'effectuez que des évaluations statiques des risques, vous ne saurez probablement pas que cette violation s'est produite, ou vous ne l'apprendrez que trop tard. Il est également possible que vous deviez attendre trop longtemps pour obtenir les renseignements nécessaire pour évaluer le risque avec précision. Quelle est la cause de la violation ? S'agit-il d'une vulnérabilité d'un système utilisé par votre partenaire qui a été exploitée ? Est-ce une attaque d'ingénierie sociale ? Les évaluations statiques ne fournissent pas, à elles seules, les preuves justifiant l'exigence qu'un tiers mette en place des contrôles de sécurité supplémentaires.

Si vous souhaitez améliorer l'efficacité de votre programme de gestion des risques posés par les tiers, commencez par réfléchir de manière critique à cinq questions clés :

1. Qui sont mes fournisseurs les plus importants ?
2. De quoi suis-je légalement responsable ?
3. Quel est mon processus actuel d'évaluation des risques posés par mes fournisseurs ?
4. Qui d'autre dans mon entreprise a besoin de ces informations ?
5. Comment le panorama mondial des menaces affecte-t-il mes partenaires ?

Pour en savoir plus sur ces questions et sur la manière d'y répondre, lisez le livre électronique de Recorded Future intitulé « Closing the Visibility Gap: 5 Questions to Ask Yourself About Your Third-Party Risk » (Combler les lacunes en matière de visibilité ; 5 questions que vous devez vous poser sur les risques posés par les tiers)

Évaluations transparentes des risques

Pourquoi évaluer les risques si vous ne pouvez pas convaincre les tiers avec lesquels vous traitez de prendre des mesures ?

Les informations sans contexte nous placent dans la situation de Cassandre dans la mythologie grecque. Pour obtenir son amour, le dieu Apollon en fit une prophétesse, mais elle refusa malgré tout ses avances romantiques. En colère, Apollon lui permit de conserver ce don mais la maudit en faisant en sorte que personne ne croie jamais ses avertissements sur l'avenir.

De nombreuses évaluations de risques actuelles subissent le même sort que les prophéties de Cassandre. Quand nous nous appuyons sur des méthodes de notation vagues ou des sources opaques, notre avis est difficile à accepter, même s'il est exact. Trop souvent, les entreprises n'interviennent pas après avoir obtenu le renseignement, car leurs directeurs ne le comprennent pas ou ne connaissent pas sa source.

Une solution de renseignement sur la sécurité doit afficher les règles de risque déclenchées par une alerte et être transparente quant à ses sources (figure 9-2). Cela permet aux professionnels de la sécurité de voir eux-mêmes pourquoi une alerte sur une adresse IP particulière peut présenter un risque réel. Ces détails supplémentaires éliminent également tout soupçon que des informations auraient pu être ignorées. Ce contexte permet d'accélérer les contrôles préalables et la vérification des références, notamment lors de l'examen des évaluations statiques.

Figure 9-2 : Le renseignement sur les tiers fournit un contexte et aide à identifier les lacunes dans les défenses des partenaires de chaîne d'approvisionnement.

Réagir face aux cotes de risque élevées de tiers

Que faire quand vous êtes confronté à des cotes de risque élevées chez un tiers ? Toutes les violations de données ne justifient pas la cessation d'affaires avec ce partenaire. À peu près toutes les entreprises font face à des cyberattaques et à des temps d'arrêt imprévus, et les partenaires ne font pas exception. La question la plus importante est de savoir comment ils gèrent les incidents et prennent des mesures pour réduire les risques futurs (et comment vous le faites).

Un changement de cotes de risque peut vous donner l'occasion de discuter avec vos partenaires commerciaux de leur approche de la sécurité. De votre côté, il est important d'examiner de plus près si les règles de risque déclenchées auront un impact sur le réseau de votre entreprise. Par exemple, la cote de risque d'un partenaire pourrait augmenter parce que des sites Web typosquattants ressemblant étroitement à des sites Web légitimes exploités par le partenaire ont été découverts. Placer ces sites sur la liste noire de votre propre réseau est une manière de contrecarrer les campagnes d'hameçonnage pendant que vous examinez les mesures que le partenaire envisage de prendre pour protéger l'identité de sa marque.

Pour prendre des décisions intelligentes impliquant vos partenaires tiers, il vous faut un contexte constamment actualisé et des preuves fournies par le renseignement sur les tiers.

Étude de cas : Bénéfices de compagnie d'assurance Visualisation en temps réel des risques posés par un tiers

Depuis des années, une compagnie d'assurance *Fortune 100* avait du mal à maintenir une vision claire et actualisée des profils de risque de ses partenaires. La solution de cette entreprise reposait sur des données souvent obsolètes et rarement mises à jour. La société ne pouvait voir ni les tendances de la cote de risque de ses partenaires au fil du temps ni les événements spécifiques influençant cette cote.

Cette compagnie d'assurance a adopté une solution de renseignement sur la sécurité de Recorded Future qui comprend le renseignement sur les tiers. Ce renseignement permet à son équipe de sécurité de mieux comprendre, analyser et traiter rapidement les risques posés par les tiers, notamment :

- Les e-mails d'entreprise, les informations d'identification et les mentions de la société sur l'Internet clandestin
- Les discussions négatives sur les réseaux sociaux
- Les utilisations de domaine à mauvais escient (indiquant souvent des attaques de hameçonnage)
- L'utilisation de technologies vulnérables
- L'utilisation impropre ou à mauvais escient de son infrastructure informatique

Selon le directeur de l'équipe de gestion des risques posés par les informations détenues par des tiers, « [le renseignement sur les tiers] donne des aperçus précieux des niveaux de risque des fournisseurs essentiels avec lesquels nous traitons en affaires, allant de cotes de risque en temps réel à des alertes personnalisées que nous établissons, et nous permet d'approfondir nos analyses au besoin. » La hiérarchisation du renseignement sur la sécurité de la solution de Recorded Future permet à l'entreprise de pouvoir rapidement :

- Exclure les alertes à faible risque et les faux positifs
- Se concentrer sur les menaces les plus importantes
- Prendre des mesures immédiates pour les résoudre

Cette solution a permis à la société de diminuer de 50 % le temps consacré aux contrôles préalables et à la vérification de références, et de remplacer une approche statique et ponctuelle par une surveillance continue.

Lisez cette cette étude de cas dans son intégralité sur https://go.recordedfuture.com/hubfs/insurance-case-study.pdf.

Chapitre 10

Le renseignement sur les marques

Dans ce chapitre

- Examinez les nombreux types de risques numériques menaçant les marques
- Découvrez comment le renseignement sur la sécurité identifie les attaques contre les marques en ligne et y remédie

« Chaque contact laisse une trace »

— Principe d'échange de Locard en criminalistique

La protection de la marque consiste à protéger l'image, la réputation et les clients d'une entreprise contre les attaques qui ne touchent jamais principalement son réseau ou ses systèmes. Ces menaces comprennent :

- ☑ Les faux sites Web et comptes de réseaux sociaux utilisés pour usurper l'identité de l'entreprise ou de ses employés pour se livrer à de la fraude et à des attaques d'hameçonnage.
- ☑ Le contenu malveillant et les fausses informations sur l'entreprise et ses produits, publiés sur des sites Web et des plates-formes de réseaux sociaux
- ☑ Les produits et les logiciels contrefaits offerts sur les marchés numériques et les boutiques d'applications
- ☑ Les fuites de données et les fuites d'informations d'identification d'employés et de cadres

La plupart de ces menaces émanent de criminels motivés par des gains financiers, mais elles peuvent également impliquer des hacktivistes, des clients insatisfaits, des concurrents et des employés négligents ou mécontents qui divulguent des informations en ligne.

Protéger votre marque et vos clients

Pour vraiment protéger votre marque, vous devez vous préoccuper des menaces qui l'exploitent pour nuire à vos clients ou les influencer. Les clients qui se laissent séduire par une imitation de votre site Web et sont victimes d'escroquerie et de fraude peuvent en attribuer la responsabilité à votre entreprise. Ceux qui achètent une version contrefaite, de mauvaise qualité, de votre produit sur un marché en ligne peuvent perdre confiance en votre marque. Ceux qui pensent que l'un de vos cadres a publié du contenu offensant sur Internet peuvent boycotter vos produits, même si ce n'est pas votre cadre qui l'a publié. Plaider « ce n'était pas de notre faute » ne restaurera leur confiance ou votre réputation dans aucun de ces scénarios.

Un autre type de détection

La plupart des activités que nous avons décrites dans ce manuel impliquent la création de renseignement sur les attaquants et sur leurs outils. Le renseignement sur la marque comprend certaines de ces informations, mais l'accent est plutôt mis sur la détection du nom et de la marque de votre organisation partout où ils surviennent sur Internet.

Vous devez vous montrer rigoureux dans l'énumération et la recherche des mentions de toutes vos marques et noms de produits, et des mots-clés qui leur sont associés. Il s'agit notamment des noms :

- ☑ De votre société mère
- ☑ De vos filiales et unités opérationnelles

- ☑ De vos produits
- ☑ De vos cadres dirigeants
- ☑ Des responsables et des employés qui communiquent avec le public sur des forums du Web et sur des réseaux sociaux

Ceci comprend également les marques commerciales, les marques de service et les slogans publicitaires qui apparaissent sur les sites Web autorisés de votre organisation, car ils sont fréquemment utilisés sur des sites Web frauduleux.

Détection de preuves d'usurpation et d'usage à mauvais escient de votre marque

Savoir ce qu'il faut rechercher vous permet de trouver des preuves d'usurpation et d'usage à mauvais escient de votre marque dans des endroits où de nombreuses entreprises ne font jamais de recherches. Par exemple, une solution de renseignement sur la sécurité vous permet de :

- ☑ Faire des recherches dans des registres de domaines qui incluent le nom de votre organisation ou de votre produit, ou des variantes de ceux-ci
- ☑ Parcourir le Web pour trouver des domaines typosquattants
- ☑ Surveiller les réseaux sociaux pour vous avertir des mots-dièses qui incluent le nom de votre entreprise ou de vos produits, ou de variations de ceux-ci
- ☑ Analyser les réseaux sociaux pour détecter les comptes qui prétendent appartenir à votre entreprise, à vos cadres ou à vos employés
- ☑ Consulter les boutiques d'applications pour découvrir les applications mobiles non autorisées qui utilisent votre marque
- ☑ Passer au crible les forums pour repérer les auteurs de menaces qui envisagent d'usurper votre marque

Le typosquattage et les domaines frauduleux

Le typosquatting comprend la manipulation des caractères du nom de domaine d'une société pour créer des domaines presque identiques. Par exemple, exemple.com peut devenir exenple.com. Ainsi, les auteurs de menaces visant exemple.com pourraient créer L'URL typosquattante exenple.com. Les attaquants enregistrent souvent des milliers de domaines différant par un seul caractère des URL de leurs organisations cibles. Ils le font pour des raisons allant de suspectes à totalement malveillantes.

Les sites Web voyous utilisant ces noms de domaines sont conçus de manière à ressembler à des sites Web légitimes. Les domaines et les sites Web voyous peuvent être utilisés dans des campagnes de spear phishing contre les collaborateurs ou les clients de l'entreprise, des attaques de point d'eau et les attaques de "drive-by download" (infections par téléchargement).

Être averti en temps réel des domaines de typosquatting et de hameçonnage qui viennent d'être enregistrés diminue le temps dont les auteurs de menaces disposent pour usurper votre marque ou escroquer des utilisateurs qui ne se méfient pas. Une fois cette infrastructure repérée, vous pouvez recourir à un service de démantèlement pour annuler la menace.

Détection de preuves de violations de données sur Internet

En surveillant le Web, y compris les forums privés de l'Internet clandestin, les solutions de renseignement sur la sécurité vous permettent de découvrir des preuves de violations de données au sein de votre entreprise et de votre écosystème de partenaires. Vous pourriez y trouver :

- ☑ Les noms et les données de vos clients
- ☑ Des données de comptes financiers et des numéros de sécurité sociale

- ☑ La divulgation ou le vol d'informations d'identification de membres de votre personnel
- ☑ Des sites de stockage de texte contenant votre code de logiciel propriétaire
- ☑ Des forums mentionnant votre entreprise et annonçant des intentions de l'attaquer
- ☑ Des forums vendant des outils et discutant de techniques pour attaquer des entreprises comme la vôtre

La découverte en temps opportun de ces indicateurs peut vous permettre de :

- ☑ Sécuriser les sources des données
- ☑ Détecter et corriger les vulnérabilités et les erreurs de configuration de votre infrastructure
- ☑ Atténuer les risques futurs en améliorant les contrôles de sécurité
- ☑ Identifier les moyens d'améliorer les formations de votre personnel et vos pratiques de codage
- ☑ Donner la possibilité à vos équipes des SecOps et de réponse aux incidents de reconnaître les attaques plus rapidement

Il est souvent possible de limiter les possibilités d'origine d'une fuite en examinant exactement les informations et les artefacts figurant sur le Web, l'endroit où ils se trouvent et les autres choses qui se trouvent au même endroit. Si, par exemple, vous trouvez des conceptions de produits ou des codes logiciels sur un site de l'Internet clandestin et que vous savez qu'ils ont été partagés avec quelques fournisseurs seulement, vous saurez que vous devrez faire une enquête sur les contrôles de sécurité de ces fournisseurs dans le cadre de votre programme de gestion des risques posés par les tiers. Si le nom de votre organisation a été mentionné sur un forum de pirates dont on sait que les membres attaquent certaines applications, vous pourriez renforcer la protection des applications visées en appliquant des correctifs sur les systèmes où elles sont exécutées, en les surveillant plus étroitement et en ajoutant des contrôles de sécurité.

Cas d'utilisation : Les données compromises

Les auteurs de menaces se remplissent les poches avec de nombreux types d'informations personnelles compromises et de propriété intellectuelle d'entreprise. Des exemples de données compromises en vente sur l'Internet clandestin comprennent des dossiers médicaux, des cartes-cadeaux clonées et compromises, et des informations d'identification volées pour « le paiement » de services comme Netflix, Uber et des articles payés via PayPal, comme illustré à la figure 10-1.

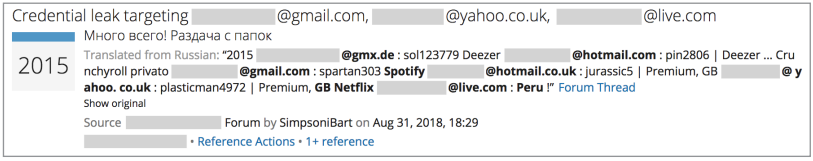


Figure 10-1 : Les données compromises - des informations d'identification pour Spotify divulguées sur l'Internet clandestin. (Source : Recorded Future)

Un grand pourcentage de violations liées au piratage ont recours à des mots de passe faibles ou volés. Les cybercriminels téléchargent régulièrement des mémoires-tampons énormes de noms d'utilisateurs et de mots de passe sur des sites de stockage de texte et sur l'Internet clandestin ou les mettent en vente sur des marchés souterrains. Ces vidages de données peuvent comprendre des adresses électroniques et mots de passe professionnels, ainsi que des informations de connexion à d'autres sites.

Surveiller les sources externes pour trouver ce type de renseignement augmente fortement ce que vous pouvez observer, non seulement en termes de fuites d'informations d'identification mais aussi de violation de données d'entreprise ou de code propriétaire

Fait alarmant : la désinformation est simple et peu coûteuse

La diffusion de mensonges sur une entreprise est facile et bon marché sur Internet. Comme exercice d'apprentissage, le Groupe Insikt® de Recorded Future a utilisé un fournisseur de services de désinformation pour lancer une campagne négative contre une société fictive pour 4,200 USD seulement.

L'exercice

Insikt Group a créé une société fictive. Elle a ensuite trouvé deux fournisseurs de services de désinformation sur des forums russophones de l'Internet clandestin et les a chargés de générer des récits intentionnellement faux sur le Web. On a demandé à l'un d'eux de créer de la propagande positive pour que l'entreprise semble attrayante. L'autre a été chargé de diffuser du matériel malveillant accusant la même société de pratiques commerciales immorales.

Les résultats

Insikt Group a découvert que le lancement de campagnes de désinformation est bon marché et d'une simplicité alarmante. Les deux campagnes de désinformation ont produit des résultats en moins d'un mois pour seulement quelques milliers de dollars : 1,850 USD pour l'effort de propagande positive et 4,200 USD pour la campagne de désinformation négative. Les fournisseurs de services ont diffusé leurs messages avec succès en plaçant des articles sur des sites Web réputés et en créant des comptes de réseaux sociaux de personnes semblant réelles.

Les conclusions

- Les services de désinformation sont accessibles au public sur des forums souterrains.
- Pour quelques milliers de dollars, les fournisseurs de services de désinformation publieront des articles dans des sources de médias allant de sites Web douteux à des organes de presse réputés.
- Ces fournisseurs de services utilisent une combinaison de comptes de réseaux sociaux établis et neufs pour propager du contenu sans déclencher de contrôles de modération de contenu.

Pour en savoir plus sur les méthodes utilisées par les fournisseurs de services de désinformation, consultez le rapport d'analyse des cyber-menaces du groupe Insikt : « The Price of Influence : Disinformation in the Private Sector » (Le prix de l'influence : la désinformation dans le secteur privé).

Qualités essentielles des solutions de renseignement sur la sécurité

Il est évident qu'atténuer les risques numériques menaçant votre marque ne se limitent pas à découvrir par hasard un domaine typosquattant ou des données volées isolées. Quelqu'un, ou quelque chose, doit réaliser les travaux de plus large envergure suivants : recueillir des masses de données, passer au crible de milliers de points de données, déterminer les priorités et, enfin, prendre des mesures.

La meilleure approche est d'utiliser une solution de renseignement sur la marque capable de :

- ☑ **Recueillir et analyser des données à partir de l'éventail le plus étendu de sources les plus diverses** : L'automatisation de l'étape de collecte des données permet aux analystes de gagner un temps précieux. Les meilleures solutions collectent des données non seulement à partir de sources Web ouvertes, mais aussi à partir de l'Internet clandestin et de sources techniques.
- ☑ **Mapper, surveiller et coter les risques pour la marque** : Grâce à de l'automatisation, à de la science des données avancée et à des techniques analytiques telles que le traitement des langues naturelles, les outils efficaces du renseignement sur la marque permettent aux analystes de lier des attributs commerciaux à des ressources numériques associées et de détecter, d'évaluer et de hiérarchiser les événements liés aux risques pour la marque.
- ☑ **Coordonner les corrections** : De solides solutions de renseignement sur la marque génèrent des alertes et des rapports qui fournissent des informations sur la manière de corriger les problèmes. Elles s'intègrent également à des outils qui effectuent immédiatement la correction et à des fournisseurs de services qui démantèlent les domaines utilisés à mauvais escient.

Étude de cas : Défaite du typosquatting chez un grand fournisseur de solutions RH

Un grand fournisseur de services de ressources humaines et de prestations de santé et financières permet à d'autres entreprises de gérer leurs ressources humaines. Cette société manipule de nombreuses données personnelles, notamment des données sensibles sur la santé et financières. Pour protéger ces données, elle dispose d'un vaste centre d'opérations de sécurité, avec surveillance 24/7/365, réponse aux incidents, enquêtes et criminalistique, etc.

Selon son vice-président des opérations de sécurité, elle avait besoin, à un moment donné, d'une équipe d'environ 100 personnes pour gérer ces fonctions. Avec Recorded Future, il ne lui en faut plus que dix. « L'obtention d'une liste de toutes les mentions de notre entreprise sur Internet d'ici la fin de la journée était totalement irréalisable, même si j'avais 10 ou 20 personnes qui y travaillaient », a déclaré ce vice-président.

« Bien sûr, nous aurions pu dépenser beaucoup d'argent pour créer des comptes bidons et accéder à ces espaces privés, mais quel gaspillage ! Tout ce qui exige plus de deux personne n'a aucun sens comparé à l'utilisation de Recorded Future. Son coût est inférieur à celui de deux employés, comparé aux 10 ou 20 qu'il me faudrait pour essayer de faire quelque chose de semblable. »

Par exemple, un matin, une alerte au sujet d'un domaine typosquattant potentiel a été déclenchée. Cette alerte a été lancée par une règle de surveillance établie chez Recorded Future pour un contrôle des domaines frauduleux ressemblant à ceux de l'entreprise. L'enregistrement de ces domaines est souvent la première étape d'une attaque d'hameçonnage.

Dès que l'équipe a reçu l'alerte, elle a enquêté et trouvé des tentatives d'hameçonnage visant à la fois son entreprise et certains de ses clients. Elle a immédiatement envoyé un rapport instantané à toute son organisation et à tous ses clients et partenaires. Le rapport a fourni des recommandations concrètes sur la manière de contrer l'attaque : bloquez le domaine au niveau de votre proxy et utilisez les journaux d'événements pour rechercher la menace avec votre SIEM. Bon nombre de leurs partenaires ont signalé des visites du site, mais ils ont pu bloquer l'accès avant tout dommage.

Grâce au renseignement sur la marque en temps réel, l'entreprise a pu atténuer la menace en quelques heures plutôt qu'en quelques semaines (voire jamais).

Chapitre 11

Le renseignement géopolitique

Dans ce chapitre

- Comprenez quels sont les facteurs qui provoquent des risques géopolitiques
- Découvrez tous les groupes qui utilisent le renseignement géopolitique
- Examinez les types d'événements de gardiennage virtuel et de risque géopolitique

« Une ville vous donne des cadeaux, une autre vous vole... Les villes et les pays sont aussi vivants, aussi sensibles, aussi capricieux et aussi incertains que les gens. »

— Roman Payne

Qu'est-ce que le risque géopolitique ?

Le risque géopolitique est l'exposition à des événements spécifiques à un endroit.

Pensez à un pays ou à une ville où votre organisation a un bureau ou une installation comme une usine, un bureau, un entrepôt, ou peut-être une clinique ou un consulat. Les activités de cette installation pourraient être affectées par :

- ☑ Des décisions et des actions d'organes et d'organismes gouvernementaux, de l'adoption de lois et de l'introduction de règlements, à la mobilisation de forces de police ou militaires lors d'un état d'urgence
- ☑ Les actions des partis politiques, des syndicats, des groupes d'activistes et d'autres organisations, y compris les grèves, les manifestations, les boycotts, les campagnes sur les réseaux sociaux, et même les émeutes et les attaques ciblées contre des lieux et des biens
- ☑ Les catastrophes naturelles et causées par l'homme, comme les épidémies, les ouragans et les tremblements de terre, les interventions militaires et les attentats terroristes

Les effets de ces événements vont de perturbations temporaires à des millions de dollars en coûts directs et indirects, et à la perte de vies humaines.

Un grand d'impact

Dans une récente enquête menée auprès d'entreprises internationales ayant un chiffre d'affaires de 250 millions USD ou davantage, environ 90 % des cadres d'entreprises des Amériques affirment que les risques géopolitiques et nationaux ont un impact assez élevé ou très élevé. Dans le monde entier, 70 % des cadres affirment que leur entreprise comprend une personne ou une fonction responsable de la gestion des risques politiques.

Les auteurs de l'étude ont mis en évidence quatre types de risques politiques :

- Les risques découlant de conflits entre pays et des modifications des systèmes internationaux
- Les risques liés aux environnements politiques nationaux, à la stabilité des gouvernements et des institutions, et à la législation
- Les risques qui apparaissent lorsque les gouvernements modifient les réglementations concernant l'environnement, la santé et la sécurité, le marché financier et autres
- Les risques créés par l'activisme de groupes tels que des syndicats et des organisations de consommateurs

Source : EY, « GeoStrategy in Practice 2020 » (Géostratégie en pratique 2020), mai 2020.

Le renseignement géopolitique

Songez aux avantages d'être averti des jours avant que ces types d'événements n'affectent votre organisation, ou d'être alerté en temps réel quand ils se produisent. Ces connaissances peuvent vous permettre d'éviter que les événements n'affectent votre organisation ou vous donner l'occasion de réagir plus rapidement pour atténuer leur effet.

En outre, le renseignement sur les attitudes locales et les tendances à long terme vous fournit les points de vue dont vous avez besoin pour prendre des décisions plus intelligentes sur l'expansion d'activités dans des pays et des villes spécifiques.

Le plus important, c'est l'endroit

Le renseignement géopolitique utilise le cycle de vie du renseignement sur la sécurité décrit au chapitre 3. La principale différence entre le renseignement géopolitique et les autres types de renseignements sur la sécurité est le point de départ.

Les activités de renseignement sur la sécurité pour les opérations de sécurité, la réponse aux incidents, la gestion des vulnérabilités, l'analyse des menaces et les équipes de gestion des risques posés par les tiers sont organisées principalement en fonction des menaces et des auteurs de menaces. Le renseignement sur la marque se concentre sur les noms et mots-clés liés aux marques et aux produits de l'entreprise.

En revanche, le renseignement géopolitique se fonde, pour commencer, sur les emplacements géographiques, généralement les villes, les pays et les régions où votre organisation possède des ressources et des installations physiques. Ses résultats sont des faits et des aperçus sur des événements spécifiques aux emplacements qui ont un impact potentiel sur les activités de ces installations et leur personnel local.

Chaînes d'approvisionnement, clients et risque géopolitique

Le risque géopolitique ne concerne pas seulement les bureaux et les installations de votre organisation. Comme l'illustre la situation en 2020, au cours des premières phases de la pandémie COVID-19, les perturbations qui affectent les partenaires de chaîne d'approvisionnement et les réseaux de transport ont également un effet spectaculaire sur les activités d'une organisation. C'est vrai même dans les régions où l'organisation n'a pas de biens matériels ou de personnel. Lorsque des événements spécifiques à un endroit affectent un grand nombre de ses clients, une entreprise peut donc avoir des difficultés.

Qui utilise le renseignement géopolitique ?

Le renseignement géopolitique est précieux pour de nombreux groupes au sein d'organisations mondiales ou qui aspirent à une expansion à l'échelle mondiale. Les noms des groupes diffèrent souvent d'une organisation à l'autre mais peuvent inclure les équipes suivantes :

- ☑ Sécurité physique
- ☑ Opérations de sécurité
- ☑ Continuité des activités
- ☑ Gestion de la chaîne d'approvisionnement
- ☑ La gestion des risques
- ☑ Relations avec les gouvernements
- ☑ Politique publique ou affaires publiques
- ☑ Direction juridique
- ☑ Gestion régionale et nationale

Ces groupes ont diverses responsabilités liées aux risques géopolitiques, notamment :

- ☑ Anticiper et prévenir les dommages (p. ex., fermer une installation avant une énorme manifestation)
- ☑ Réagir rapidement pour atténuer les effets des événements (p. ex., fournir de l'aide aux employés ou trouver d'autres sources d'approvisionnement après une catastrophe naturelle)
- ☑ Communiquer les faits essentiels aux employés, aux clients, aux partenaires commerciaux et aux organismes gouvernementaux
- ☑ Évaluer les risques liés à l'emplacement pour l'avenir, pour orienter les investissements et décisions d'expansion

Pour tirer le meilleur parti du renseignement géopolitique, consultez ces groupes pour vous enquérir de leurs besoins en informations et utilisez leur contribution pour établir des priorités en matière de collecte et d'analyse de renseignement. Personnalisez votre production pour qu'elle soit facilement comprise et exploitable par ces publics. Reportez-vous aux sections « Orientation » et « Diffusion » de la description du cycle de vie des renseignements sur la sécurité au chapitre 3.

Collecte de données à gardiennage virtuel

Pour permettre à votre entreprise d'anticiper et d'affronter des événements spécifiques à un emplacement, vous devez commencer par sélectionner les lieux et les types d'événements qui sont importants pour votre entreprise. La solution de renseignement géopolitique surveille et filtre les données par emplacement, ce que l'on appelle « gardiennage virtuel ».

Si votre entreprise dispose d'un service de sécurité physique ou de continuité des activités, cette équipe tient probablement à jour une liste de tous vos bureaux et installations, partout dans le monde.

Ne vous limitez pas à votre liste de bureaux et d'installations, et posez à différents groupes de votre entreprise des questions sur vos partenaires de chaîne d'approvisionnement, les réseaux de transport, vos clients, et d'autres entités susceptibles d'affecter vos activités. Documentez les lieux où ceux-ci pourraient ressentir l'effet d'événements géopolitiques et surveillez-les.

Vous devez également préciser les types d'événements à surveiller. La figure 11-1 est un exemple de catégories d'événements géopolitiques de haut niveau et de certains des éléments spécifiques qui pourraient être proposés au sein d'une catégorie.

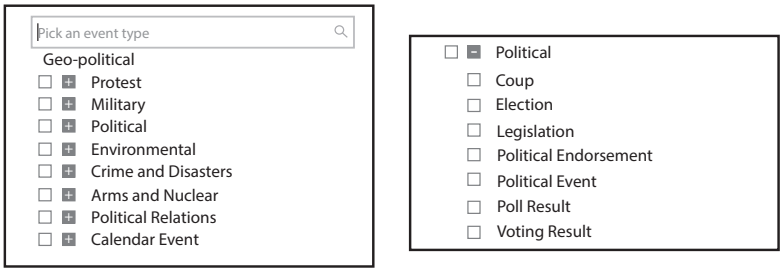


Figure 11-1 : Exemples de catégories d'événements géopolitiques et d'éléments spécifiques au sein d'une catégorie. (Source : Recorded Future)

Sources de données et d'informations

Les sources de données et d'informations utilisées pour produire du renseignement géopolitique et celles qui sont utilisées pour d'autres types de renseignement de sécurité se recoupent. Les sources techniques telles que les sources de menaces jouent généralement un rôle moins important dans le renseignement géopolitique, car la plupart des cyber-menaces ne sont pas spécifiques aux emplacements. Les sources de renseignement géopolitiques les plus précieuses ont tendance à être spécifiques à un pays ou à une ville, par exemple :

- ☑ Les sites Web d'actualités et de médias publics

- ☑ Les publications de réseaux sociaux
- ☑ Les blogs
- ☑ Les forums et les marchés sur Internet, ouvert et clandestin.

La plupart de ces sources comprennent des données et des renseignements provenant de gouvernements nationaux et d'administrations locales, d'organismes de réglementation, d'organes de presse, de syndicats, de groupes de consommateurs et de particuliers. Cependant, les activistes et les criminels utilisent également l'Internet clandestin pour planifier des activités dangereuses et illégales ciblant des endroits spécifiques, ce qui rend les sources de l'Internet clandestin précieuses pour le renseignement géopolitique.

Automatisation, analyse et expertise

Il faut énormément de travail pour déterminer quels sites, et quels articles, vidéos, messages et publications spécifiques, concernent un emplacement et un type de menace particuliers. C'est pourquoi les entreprises qui prennent au sérieux la gestion des risques géopolitiques doivent utiliser une plate-forme de renseignement sur la sécurité qui combine analyse, automatisation et expertise humaine pour traiter et analyser les données et les informations.

L'automatisation réduit, et élimine souvent, les recherches manuelles fastidieuses et gourmandes en ressources. Elle accélère également les processus de calcul et de mise à jour des cotes de risque, la diffusion des alertes, la création de représentations visuelles des données et de nombreuses tâches supplémentaires.

Les analyses permettent à une solution de renseignement sur la sécurité de collecter des millions d'informations provenant de sources de l'Internet ouvert et clandestin, et de sources techniques, de les lier dynamiquement et de les classer afin de générer du renseignement sur des emplacements spécifiques

et des types d'événements géopolitiques. Grâce aux analyses, les analystes ne doivent pas manuellement passer au crible des volumes massifs de contenu, découvrir des modèles et établir des corrélations entre les faits et les informations concernant des lieux et des types de menaces spécifiques.

Des outils d'analyse spécialisés les aident également dans d'autres domaines. Alors que la plupart des communications entre les auteurs de menaces se font en anglais ou en russe, les annonces gouvernementales, les reportages et les publications sur les réseaux sociaux et les blogs sont, naturellement, écrits dans une variété de langues locales. Le traitement du langage naturel (TANL) est un outil analytique qui identifie des éléments de contenu contenant des mots clés et des expressions dans chaque langue. Par exemple, le TANL permet à une solution de renseignement sur la sécurité de trouver des articles d'actualité pertinents, des publications de blog et des bavardages sur l'Internet clandestin liés à un message d'un forum en russe qui mentionne « В Киеве будет протестный марш » (une marche de protestation à Kiev).

Il va de soi que le renseignement sur la sécurité ne se limite pas à l'automatisation et à l'analyse. Souvent, il n'existe pas de remplacement de l'expertise humaine. C'est particulièrement vrai pour les questions liées à des régions et des pays spécifiques, pour lesquelles les compétences linguistiques (y compris la connaissance de l'argot local) et la connaissance de l'histoire et de la politique sont indispensables. C'est pour cette raison que vous devez également évaluer les solutions de renseignement sur la sécurité en fonction de leur capacité à fournir des renseignements qui sont des produits finis, en particulier pour les renseignements géopolitiques.

Le renseignement sous forme de produit fini peut inclure des comptes-rendus de recherches personnalisés évaluant les risques dans des régions spécifiques, des informations personnalisées sur les dernières menaces qui affectent ces régions et des « forfaits de chasse aux informations » qui accélèrent les recherches de vos équipes de réponse aux incidents, de recherche de menaces et de gestion des risques géopolitiques.

Pour une discussion technique sur la façon dont une plate-forme de renseignement sur la sécurité combine les analyses avec l'expertise humaine et l'automatisation pour classer et connecter d'énormes volumes de données de sécurité, lisez le livre blanc de Recorded Future, « The Security Intelligence Graph: Inside Recorded Future's Methodology and Patented Technology » (Le graphique du renseignement sur la sécurité : pénétrer dans la méthodologie et dans la technologie brevetée de Recorded Future).

Interactions avec le renseignement géopolitique

Les solutions de renseignement sur la sécurité vous permettent d'accéder au renseignement géopolitique et d'interagir avec lui sous différents formats, tels que :

- ☑ Des tableaux de bord et des cartes montrant les niveaux de risque par pays et par ville
- ☑ Des alertes déclenchées par des événements ou des modifications des cotes de risque
- ☑ Des rapports détaillant des événements et des problèmes liés à des endroits spécifiés
- ☑ Des documents sur le contexte et des aperçus résumant les principales conclusions sur les pays et les villes

En outre, certaines solutions de renseignement sur la sécurité s'intègrent à des outils de sécurité tels que les SIEM et les systèmes de tickets, et utilisent des balises géographiques pour garantir que les personnes concernées par des villes, des pays et des régions spécifiques reçoivent immédiatement des alertes d'événements qui y ont lieu.

La figure 11-2 est un exemple de tableau de bord de renseignement géopolitique qui met en évidence les zones à haut risque sur une carte du monde.

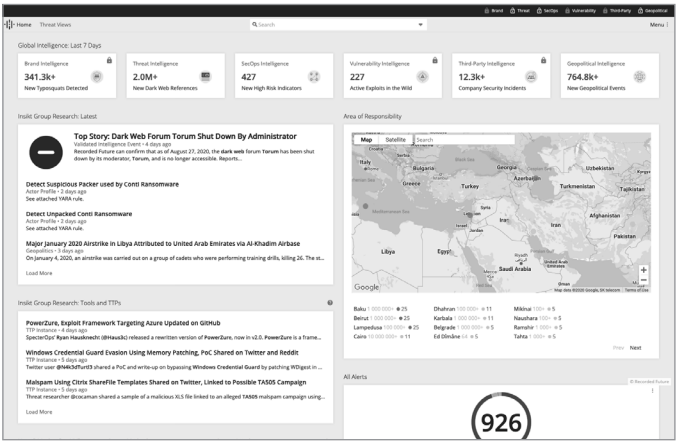


Figure 11-2 : Exemple de tableau de bord qui met en évidence les zones à haut risque. (Source : Recorded Future)

Géopolitique et cybermenaces

Ce chapitre portait sur les menaces et les événements survenant dans les pays des installations que vous voulez protéger. Cependant, le risque géopolitique implique également, naturellement, la géopolitique : les conflits politiques, économiques et idéologiques entre les nations et les alliances mondiales.

Au cours des dernières années, le monde a subi des cyber-attaques contre des infrastructures d'Internet, ainsi que des infrastructures financières et physiques. Parmi celles-ci, on compte des tentatives de surcharge ou de désactivation de sites Web d'agences gouvernementales, d'organisations non gouvernementales (ONG) et d'organes de presse indépendants, ainsi que des campagnes de désinformation ciblant des gouvernements, des élections et des entreprises.

La plupart de ces attaques ont été attribuées à des groupes de pirates mystérieux, parfois liés à des gouvernements, et parfois même à des ministères d'un gouvernement ou d'un service de l'armée. De nombreux organismes gouvernementaux, entreprises commerciales et ONG sont pris entre deux feux, même lorsqu'ils n'ont que peu voire rien à voir avec le conflit entre les nations qui l'ont déclenché.

La défense de votre entreprise contre ces types de menaces nécessite un programme de renseignement sur la sécurité complet qui couvre tous les sujets abordés dans ce manuel, des opérations de sécurité et du renseignement sur les menaces à la protection de la marque, et de la gestion des risques posés par les vulnérabilités et les tiers au renseignement géopolitique.

Pour en savoir plus sur le lien entre les conflits géopolitiques et les cybermenaces, lisez le billet de blog de Recorded Future, « Geopolitics: An Overlooked Influencer in Cyber Operations » (La géopolitique : une influence oubliée sur les cyberactivités). Pour en savoir plus sur le lien entre les rivalités nationales et l'hacktivisme, lisez « Return to normalcy: False Flags and the Decline of International Hacktivism » (Retour à la normale : les faux pavillons et le déclin de l'hacktivisme international)

Chapitre 12

Le renseignement sur la sécurité pour les responsables de la sécurité

Dans ce chapitre

- Voyez comment le renseignement sur la sécurité prend en charge la gestion des risques et les investissements dans des programmes de cybersécurité
- Examinez les types de renseignements sur les menaces que les responsables de la sécurité informatique considèrent comme les plus précieux
- Observez comment le renseignement sur la sécurité permet d'atténuer la pénurie de compétences en cybersécurité

"Un investissement dans le savoir paie l'intérêt le plus élevé."

— Benjamin Franklin

Le travail du responsable de la sécurité informatique (CISO) a connu des changements spectaculaires au cours des dernières années. Auparavant, il était axé sur les prises de décision concernant l'achat et la mise en œuvre de technologies de sécurité. À présent, les CISO sont beaucoup plus susceptibles d'interagir avec le PDG et le conseil d'administration et de

s'efforcer de maintenir un équilibre délicat entre la prévention des risques et la continuité des activités. Les responsables de la sécurité doivent être en mesure de :

- ☑ Évaluer les risques commerciaux et techniques, y compris les nouvelles menaces et les "inconnues connues" qui pourraient avoir des répercussions sur l'entreprise
- ☑ Identifier les bonnes stratégies et technologies d'atténuation des risques
- ☑ Communiquer la nature des risques aux cadres supérieurs et justifier les investissements en sécurité en fonction de leur valeur financière pour l'entreprise

Le renseignement sur la sécurité peut constituer une ressource cruciale pour toutes ces activités.

La gestion des risques

La plus grande responsabilité du CISO moderne est peut-être la gestion des risques. Celle-ci comprend l'affectation des ressources et du budget nécessaires pour minimiser l'impact probable des menaces sur l'entreprise. La figure 5-1 présente les étapes par lesquelles passent les responsables de la sécurité pour faire face à ce défi.

Évaluez les exigences en matière de sécurité	Appréhendez les objectifs commerciaux et informatiques et définissez les responsabilités de la fonction sécurité.
Évaluez les protocoles de sécurité actuels	Analysez le personnel, les processus et les technologies de sécurité actuels pour mettre en place une image exacte de la fonction sécurité.
Élaborez des initiatives	En recourant à une approche fondée sur les risques, identifiez les lacunes les plus importantes en matière de sécurité, puis mettez sur pied et hiérarchisez des initiatives pour y remédier.
Suivi des progrès	Surveillez continuellement les progrès et assurez-vous que la fonction sécurité s'améliore conformément aux exigences. Élaborez des mesures pour évaluer constamment l'efficacité

Figure 12-1 : L'approche habituelle est l'évaluation et l'élaboration d'une stratégie de sécurité

Les données internes ne suffisent pas

L'approche de la sécurité décrite dans la figure 5-1 dépend de bonnes informations sur les facteurs de risque pertinents et et les faiblesses éventuelles des programmes de sécurité existants. Le problème est que, trop souvent, ce type de renseignement ne se fonde que sur des audits internes, des problèmes connus et des incidents de sécurité antérieurs. Cette approche produit une liste de défis qui ont déjà affecté votre organisation mais omet des problèmes qui ne vous ont pas encore atteint.

Un contexte extérieur est nécessaire pour :

- ☑ Vérifier les risques liés aux problèmes connus
- ☑ Vous avertir de menaces émergentes et imprévues

Il est évident que les données de trafic du réseau interne, les journaux d'événements et les alertes contribuent à la gestion des risques, mais ils ne fournissent pas de contexte suffisant pour élaborer un profil de risque complet, et certainement pas suffisant pour définir l'intégralité d'une stratégie. Les professionnels de la sécurité doivent être proactifs envers la découverte de risques inconnus. Le contexte est ce qui permet aux responsables de la sécurité de déterminer quelles menaces potentielles sont les plus susceptibles de devenir des menaces réelles pour leur entreprise.

Cibler les efforts

Le renseignement sur la sécurité fournit des informations sur les tendances générales telles que :

- ☑ Les types d'attaques qui sont de plus en plus (ou de moins en moins) fréquents
- ☑ Les types d'attaques qui sont les plus coûteux pour les victimes
- ☑ Les TTP des nouveaux auteurs de menaces qui émergent, ainsi que les biens et les entreprises qu'ils ciblent

- ☑ Les pratiques et technologies de sécurité qui ont indubitablement eu le plus (ou le moins) de succès dans l'arrêt ou l'atténuation de ces attaques.

Les données sur ces tendances peuvent aider les services de sécurité à prévoir les menaces qui seront les sujets brûlants de l'actualité de demain. Cependant, le renseignement externe contextualisé sur la sécurité externes est beaucoup plus puissant. Il permet, par exemple, aux groupes chargés de la sécurité d'évaluer s'il est *probable* qu'une menace émergente touche leur entreprise en fonction de facteurs comme :

- ☑ **Secteur** : La menace touche-t-elle d'autres activités en amont et en aval ?
- ☑ **Technologie** : la menace compromet-elle des logiciels, du matériel, ou d'autres technologies utilisées dans notre organisation ?
- ☑ **Régions géographiques** : la menace cible-t-elle des installations dans des régions où nous exerçons nos activités ?
- ☑ **Mode d'attaque** : Les techniques utilisées dans l'attaque, y compris l'ingénierie sociale et les méthodes techniques, ont-elles été employées avec succès contre notre société ou d'autres sociétés semblables ?

Sans renseignement approfondi recueilli auprès d'un éventail immense de sources de données externes, il est impossible pour les décideurs des questions de sécurité d'obtenir un aperçu global du panorama des cyber-risques et d'identifier les plus grands dangers pour leur organisation.

La figure 12-2 illustre la façon dont un tableau de bord personnalisé de renseignement sur la sécurité peut mettre en évidence les renseignements les plus pertinents pour une organisation particulière.

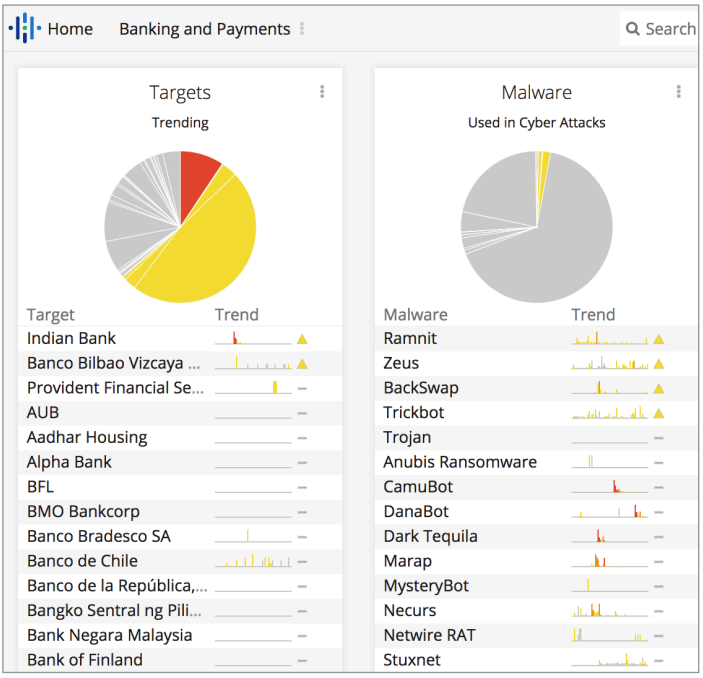


Figure 12-2 : Un tableau de bord de renseignement sur la sécurité repère les menaces les plus pertinentes pour notre secteur ou notre technologie. (Source : Recorded Future)

L'atténuation : les gens, les processus et les outils

Les analyses de vulnérabilités et les techniques telles que les tests de pénétration et les simulations contribuent à la capacité de l'équipe de sécurité à repérer les lacunes de ses mécanismes de défense. Cependant, de nombreuses organisations ont nettement plus de vulnérabilités techniques, de faiblesses dans leurs processus et leurs règles de sécurité, et de collaborateurs vulnérables aux techniques d'ingénierie sociale qu'elles ne pourraient corriger, renforcer et former dans l'immédiat.

Le renseignement sur la sécurité permet aux responsables de la sécurité d'identifier les défis à relever en premier lieu en leur montrant :

- ☑ Les auteurs de menaces les plus susceptibles de cibler l'entreprise
- ☑ Les TTP utilisés par les auteurs de menace, et donc les faiblesses qu'ils ont tendance à exploiter

Les alertes rapides

Les analystes trouvent sur l'Internet clandestin des auteurs de menaces qui annoncent leur intention d'attaquer des secteurs spécifiques, et même des entreprises spécifiques. Parfois, ces auteurs de menaces utilisent ces plates-formes pour recruter des pirates qui ont les mêmes idées, pour les aider. Les analystes qui surveillent les marchés de l'Internet clandestin peuvent aussi suivre le développement et la vente d'outils de pirates et de kits de code d'exploitation malveillant qui ciblent des vulnérabilités spécifiques.

Le renseignement sur la sécurité établit les rapports entre toutes ces entités pour fournir un contexte sur ce qu'elles signifient pour votre entreprise. Et, comme décrit auparavant dans ce livre, il est indispensable de corriger les vulnérabilités et d'atténuer les faiblesses qui risquent encore d'être exploitées avant de s'attaquer à d'autres dont l'exploitation n'est encore que purement théorique.

Utilisez des solutions de renseignement sur la sécurité pour analyser l'Internet clandestin et d'autres sources afin de repérer les mentions de votre organisation, de votre secteur et des technologies particulières installées dans votre organisation.

Les investissements

Décider de la façon d'investir dans la cybersécurité est devenue un formidable défi ces derniers temps. Les conseillers en investissements financiers Momentum Partners ont identifié en 2017 plus de 1 700 entreprises qui se spécialisaient en technologies et services de cybersécurité. Avec un si grand choix, comment les CISO peuvent-ils identifier les solutions les plus efficaces à mettre en œuvre dans le cadre d'une stratégie de sécurité proactive ?

La seule façon logique est de prendre des décisions d'investissement fondées sur les risques. Chaque organisation a son propre profil de risque particulier, façonné par son secteur, sa localisation et son infrastructure interne. Le renseignement sur la sécurité permet aux responsables de la sécurité de comprendre quelles sont les menaces les plus pressantes pour leur organisation, ce qui simplifie fortement leur tâche d'identification et de justification des domaines dans lesquels investir. L'objectif final est d'être en mesure d'évaluer ce risque et d'investir en se fondant sur de solides connaissances du vrai paysage de menaces.

Les communications

Il est souvent difficile pour les CISO de devoir décrire des menaces et justifier des contre-mesures en utilisant des termes qui motivent les chefs d'entreprise non techniques, comme le coût, le retour sur investissement, l'impact sur la clientèle et les avantages concurrentiels.

Bombarder les principaux intervenants de nouvelles sur chaque menace n'est pas conseillé. En revanche, le renseignement sur la sécurité fourni de puissantes perspectives pour éclairer ces types de discussions, telles que :

- ☑ L'impact d'attaques semblables sur des entreprises du même secteur et de la même taille dans d'autres secteurs
- ☑ Les cybertendances et le renseignement de l'Internet clandestin qui indiquent qu'il est probable que l'entreprise soit ciblée

Étude de cas : Le renseignement sur la sécurité et l'automatisation chez un détaillant mondial

Avec près de 3 600 magasins et plus de 135 000 collaborateurs dans le monde, une chaîne de magasins mondiale est confrontée à des problèmes qui vont de la prévention de pertes et de fraude, à la sécurité de l'entreprise et à la protection des données personnelles de ses clients.

Ce détaillant a automatisé la centralisation et la personnalisation du renseignement sur la sécurité pour toutes les fonctions de sécurité. L'automatisation garantit que le renseignement sur la sécurité en temps réel transmis à ses SIEM est exact et très contextuel, et que les données qui en sortent sont présentées dans des formats souples et conviviaux.

Son meilleur retour sur investissement — et le plus grand avantage de la gestion de son renseignement sur les menaces au moyen d'une plate-forme tout-en-un — est l'amélioration des relations aussi bien entre les équipes de cybersécurité et qu'avec ses autres services.

Un cadre supérieur du centre de cyberdéfense de la société a déclaré : « Aucun de nous n'opère dans un silo. Pouvoir utiliser le renseignement sur les menaces pour nous protéger mais augmenter également la visibilité de notre programme nous aide à présenter nos arguments pour augmenter nos capacités. Avoir des champions dans les autres équipes pour confirmer les avantages du renseignement sur les menaces nous aide réellement à prouver que c'est rentable."

Pour une analyse complète des économies et des avantages commerciaux de la chaîne de distribution, lisez le rapport de Forrester : « The Total Economic Impact™ Of Recorded Future ».

L'aide aux responsables de la sécurité

Nous avons déjà mentionné plusieurs fois que le renseignement sur les menaces doit être global, pertinent et contextualisé pour être utile aux membres des services de sécurité. Quand il s'agit de CISO et autres responsables de la sécurité, il doit aussi d'être concis et opportun.

Le renseignement sur les menaces peut, par exemple, fournir aux responsables de la sécurité une image en temps réel des menaces, tendances et événements les plus récents. Un tableau de bord convivial de renseignement sur la sécurité ou un autre format succinct permet aux responsables de la sécurité de répondre à une menace ou de communiquer l'impact potentiel d'un nouveau type de menace à des dirigeants d'entreprise ou à des membres d'un conseil d'administration..

Le renseignement sur la sécurité n'est pas seulement destiné aux équipes des SecOps et aux analystes de menaces. Les responsables de la sécurité figurent aussi parmi ses principaux consommateurs. Réfléchissez aux types de renseignement dont les responsables de la sécurité ont besoin au quotidien (comme, disons, un tableau de bord et une liste des nouvelles conclusions clés du renseignement de la veille), à intervalles réguliers (comme des récapitulatifs et des tendances pour un rapport trimestriel sur les risques) et en cas de crise (du renseignement sur des attaques qui viennent d'être détectées), et veillez à mettre en place des processus et des outils de renseignement sur les menaces pour répondre à ces besoins.

Le déficit en compétences en matière de sécurité

L'une des responsabilités d'un CISO est de veiller à ce que son service de sécurité et son service informatique soient dotés du personnel approprié pour exécuter leurs missions. Malheureusement, le domaine de la cybersécurité souffre d'un déficit en compétences bien connu, et le personnel de sécurité existant est fréquemment pressé de faire face à des charges de travail insurmontables.

Le renseignement sur la sécurité fournit une réponse partielle en automatisant les tâches de cybersécurité les plus laborieuses mais critiques, ce qui libère du temps pour les tâches les plus expertes qui font appel aux compétences du personnel. Il peut, par exemple, diminuer l'énorme quantité d'alertes générées par des SIEM et d'autres outils de sécurité,

rassembler et corréler rapidement du contexte de différentes sources de renseignement et fournir des données permettant de hiérarchiser les risques.

Mettre le renseignement sur la sécurité à la disposition de toutes les fonctions de sécurité peut faire gagner un temps énorme, car les équipes des opérations de sécurité et de réponse aux incidents, les spécialistes en gestion des vulnérabilités et d'autres membres du personnel de sécurité reçoivent les informations et le contexte dont ils ont besoin pour prendre en toute confiance des décisions rapides.

Un renseignement sur la sécurité puissant permet aussi aux collaborateurs inexpérimentés de se perfectionner rapidement et d'être plus performants que d'ordinaire pour leur niveau d'expérience, de sorte que le CISO ne doit pas recruter autant de collaborateurs chevronnés.

La cybersécurité basée sur les risques : mieux gérer

De nombreuses équipes de cybersécurité sont axées soit sur les menaces, soit sur la conformité. Les équipes axées sur les menaces se concentrent sur la réaction aux dernières menaces de grande notoriété, qu'elles représentent ou non un risque réel pour l'entreprise. De leur côté, les équipes axées sur la conformité font de leur mieux pour répondre à toutes les normes et à tous les cadres de conformité.

Aucune de ces équipes n'optimise la sécurité, et elles compliquent l'organisation de discussions constructives avec les responsables et les cadres qui s'intéressent beaucoup plus aux profits et pertes qu'aux menaces et à la conformité.

Dans son livre, « The Risk Business, What CISOs Need to Know about Risk-based Cybersecurity » (Le secteur du risque, ce que les CISO doivent savoir sur la cybersécurité basée sur les risques), Levi Gundert propose une meilleure solution. Son concept, appelé « cybersécurité basée sur le risque », postule que :

1. Risque signifie possibilité qu'un événement entraîne, en fin de compte, une baisse de la rentabilité.
2. Le risque posé par une cyber-menace est quantifiable sans grand effort en termes monétaires.
3. L'impact net des activités d'atténuation peut être calculé en comparant le coût de l'atténuation aux économies attendues de l'atténuation du risque.
4. Ces calculs permettent aux programmes de sécurité de sélectionner les activités qui maximisent l'impact positif sur la rentabilité de l'entreprise.

Un voyant d'alerte clignotant orange s'est-il éteint dans votre esprit en voyant les mots « sans grand effort » au point numéro 2 ? En se fondant sur les travaux de Douglas W. Hubbard et Richard Seiersen, Gundert illustre comment utiliser l'estimation, la simulation et un cadre de risque de catégorie de menace (TCR) pour quantifier facilement les menaces pesant sur une entreprise en termes monétaires.

Outre guider les équipes de sécurité vers la répartition la plus efficace possible des ressources et du personnel, la sécurité basée sur les risques permet aux responsables de la sécurité de communiquer avec les cadres dans une langue qu'ils comprennent et apprécient : la langue de l'argent.

Pour télécharger « The Risk Business, What CISOs Need to Know About Risk-Based Cybersecurity » (Le secteur du risque, ce que les CISO doivent savoir sur la cybersécurité basée sur les risques), rendez-vous sur https://go.recordedfuture.com/the-risk-business. Pour plus d'informations sur la manière de quantifier les risques de cybersécurité, lisez l'ouvrage de Hubbard et de Seiersen intitulé « How to Measure Anything in CyberSecurity Risk » (Comment mesurer quoi que soit en matière de risques pour la cybersécurité).

Section 3 : Création et mise à l'échelle de votre programme de renseignement sur la sécurité

Chapitre 13

Matrices analytiques du renseignement sur la sécurité

Dans ce chapitre

- Apprenez quels sont les avantages de l'utilisation des matrices de renseignement sur les menaces
- Comprenez quels sont les points forts et faibles des trois matrices les plus connues
- Voyez comment les trois matrices peuvent se compléter

"Une structure est nécessaire à la créativité".

— Twyla Tharp

Les matrices de renseignement sur les menaces fournissent des structures permettant de réfléchir aux attaques et aux adversaires. Elles encouragent une vaste compréhension de la façon de penser des attaquants, des méthodes qu'ils utilisent et des moments où des événements spécifiques se produisent au cours du cycle de vie d'une attaque. Ces connaissances permettent aux défenseurs de prendre plus rapidement des mesures décisives et d'arrêter plus tôt les attaquants.

Les matrices attirent également l'attention sur les détails qui nécessitent une enquête plus approfondie. Cette minutie garantit ce que les menaces ont été entièrement supprimées et que des mesures ont été mises sur pied pour empêcher des intrusions futures du même type.

Enfin, les matrices sont utiles pour le partage d'informations au sein d'une organisation et entre organisations. Elles fournissent une grammaire et une syntaxe commune pour l'explication des détails des attaques et leur corrélation. Une matrice partagée facilite l'absorption du renseignement sur la sécurité provenant de sources comme des fournisseurs de renseignement sur la sécurité, des forums open source et des centres de partage et d'analyse d'informations (ISAC).

Les matrices décrites ci-dessous sont complémentaires. Elles ne se font pas concurrence. Vous pouvez décider d'en utiliser une ou deux, ou toutes les trois.

La Cyber Kill Chain® de Lockheed Martin

La Cyber Kill Chain®, élaborée en premier lieu par Lockheed Martin en 2011, est la matrice de renseignement sur les cybermenaces la plus connue. La Cyber Kill Chain se fonde sur le concept militaire de la chaîne de frappe qui divise la structure d'une attaque en étapes. En divisant une attaque de cette manière, les défendeurs peuvent déterminer à quelle étape elle en est et déployer des contre-mesures appropriées.

La Cyber Kill Chain décrit sept étapes d'une attaque :

1. La reconnaissance
2. La conversion en arme
3. La transmission
4. L'exploitation
5. L'installation
6. Commande et contrôle
7. Les actions et les objectifs (parfois appelés exfiltration)

Ces étapes sont souvent présentées dans un diagramme semblable à la Figure 8-1.

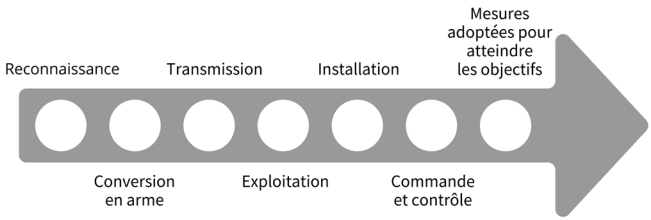


Figure 13-1 : Diagramme de la matrice Cyber Kill Chain® de Lockheed Martin

Les équipes de sécurité peuvent élaborer des réponses standard pour chaque étape. Par exemple, si vous parvenez à arrêter une attaque lors de la phase d'exploitation, vous pouvez être pratiquement sûr que rien n'a été installé sur les systèmes ciblés et qu'une intervention complète pour répondre à l'incident n'est peut-être pas nécessaire.

La Cyber Kill Chain permet également aux organisations de construire un modèle de défense en profondeur qui cible des parties spécifiques de la chaîne de frappe. Vous pouvez, par exemple, acquérir du renseignement sur les menaces auprès de tiers pour surveiller :

- ☑ Les mentions de votre entreprise sur le Web qui pourraient signaler des activités de reconnaissance
- ☑ Des informations sur une conversion en armes contre des vulnérabilités récemment signalées d'applications de votre réseau

Les limitations de la Cyber Kill Chain

La Cyber Kill Cahin est un bon moyen de commencer à réfléchir à la défense contre les attaques, mais elle a certaines limitations. L'une des grandes critiques de ce modèle est le fait qu'il ne tient pas compte de la manière dont de nombreuses attaques modernes fonctionnent. Par exemple, beaucoup d'attaques de hameçonnage sautent entièrement la phase d'exploitation et, au lieu de cela, dépendent de l'ouverture par la victime d'un document Microsoft Office avec macro incorporée ou d'un double-clic sur un script joint.

Toutefois, malgré ses limitations, la Cyber Kill Chain crée une base solide de discussion des attaques et du moment où les arrêter. Elle facilite aussi le partage d'informations sur des attaques au sein des organisations et à l'extérieur à l'aide de points d'attaque standard bien définis.

Pour en savoir plus sur la Cyber Kill Chain, lisez le livre blanc précurseur et visitez le site Web de Cyber Kill Chain.

Le modèle en diamant (Diamond Model)

Le modèle en diamant a été créé en 2013 par le Center for Cyber Intelligence Analysis and Threat Research (CCIATR, le centre d'analyse de cyber-renseignement et de recherche sur les menaces) désormais dissout. Il est utilisé pour le suivi des groupes d'attaque au fil du temps plutôt que pour la progression d'attaques individuelles.

Sous sa forme la plus simple, le modèle en diamant est semblable à la Figure 8-2. Il est utilisé pour classer les différents éléments d'une attaque. Le diamant d'un attaquant ou d'un groupe d'attaque n'est pas statique. Il évolue au fur et à mesure que l'attaquant modifie l'infrastructure et les cibles, et modifie les TTP.

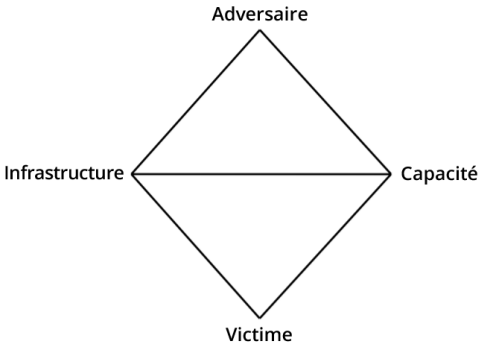


Figure 13-2 : Une conception simple du modèle en diamant

Le modèle en diamant aide les défenseurs à suivre un attaquant, ses victimes, ses capacités et l'infrastructure qu'il utilise. Chaque point du diamant est un point de pivot que les défenseurs peuvent utiliser pendant une enquête pour lier un aspect d'une attaque aux autres.

Pivotement

Disons que vous découvrez du trafic de commande et contrôle vers une adresse IP suspecte. Le modèle en diamant pourrait vous aider à "pivoter" de cet indicateur initial pour découvrir des informations sur l'attaquant lié à cette adresse IP, puis faire des recherches sur les capacités connues de cet attaquant. Connaître ces capacités vous aidera à réagir plus rapidement et plus efficacement à l'incident. Ou imaginez que votre renseignement sur les menaces utilise le modèle en diamants. Si le conseil d'administration demande qui lance des attaques semblables contre d'autres entreprises de votre secteur (attribution), vous pourriez peut-être trouver facilement une liste de victimes, l'attaquant probable et une description des TTP de l'attaquant. Cela vous aidera à déterminer les défenses à mettre en place.

La souplesse

L'un des plus grands avantages du modèle en diamant est sa souplesse et son extensibilité. Vous pouvez ajouter différents aspects d'une attaque sous le point approprié du diamant pour créer des profils complexes de différents groupes d'attaque. Les autres caractéristiques d'une attaque qu'il est possible de suivre comprennent :

1. La phase
2. Le résultat
3. La direction
4. La méthodologie
5. Les ressources

Inconvénients du modèle diamant

L'inconvénient est que les modèles en diamant nécessitent beaucoup d'entretien. Certains aspects du modèle, en particulier l'infrastructure, changent rapidement. Si vous ne mettez pas constamment à jour le diamant d'un attaquant, vous courez le risque de travailler avec des informations obsolètes. Malgré ces problèmes, le modèle en diamant peut faciliter le travail de beaucoup de membres du personnel de sécurité en présentant des réponses rapides aux menaces en évolution.

Horodatez chaque mise à jour d'un diamant pour permettre à tout le monde de savoir de quand date l'information.

Si vous ne disposez pas du temps et des ressources pour gérer ce type de modèle vous-même, vous pourriez peut-être obtenir des renseignements à jour auprès d'un fournisseur tiers de renseignement sur les menaces.

Pour en savoir plus sur le modèle en diamant, lisez le blog de Recorded Future intitulé "Applying Threat Intelligence to the Diamond Model of Intrusion Analysis" (l'application du renseignement sur les menaces au modèle en diamant de l'analyse d'intrusion), ou téléchargez le livre blanc original, "The Diamond Model of Intrusion Analysis" (le modèle en diamant d'analyse d'intrusion).”

La matrice MITRE ATT&CK™

MITRE est une organisation unique aux États-Unis : il s'agit d'une entreprise responsable de la gestion du financement fédéral de projets de recherche de plusieurs organismes fédéraux. Elle a eu un impact énorme sur le secteur de la sécurité, notamment en développant et tenant à jour les bases de données CVE (vulnérabilités et expositions courantes) et CWE (énumération des faiblesses courantes).

MITRE a mis sur pied plusieurs autres matrices très importantes pour le renseignement sur les menaces, notamment :

- ☑ AXII™ (Trusted Automated Exchange of Intelligence Information), un protocole de transport qui permet aux entreprises de partager des informations sur les menaces via HTTPS et d'utiliser des commandes d'interfaces de programmation d'application (API)) pour extraire ce renseignement sur les menaces
- ☑ STIX™ (Structured Threat Information eXpression), un format normalisé de présentation d'informations du renseignement sur les menaces
- ☑ La matrice CybOX™ (Cyber Observable eXpression), une méthode de suivi des aspects observables des incidents de cybersécurité

Catégories de comportements d'attaquant

La matrice ATT&CK™ (MITRE Adversarial Tactics, Techniques, and Common Knowledge) a été créée comme moyen de suivi du comportement des adversaires au fil du temps. ATT&CK s'appuie sur la Cyber Kill Chain, mais au lieu de décrire une seule attaque, elle se concentre sur les indicateurs et les tactiques liés à des adversaires spécifiques.

ATT&CK utilise 11 catégories de tactiques différentes pour décrire le comportement des adversaires :

1. Accès initial
2. Exécution
3. Persistance
4. Escalade de privilèges
5. Évitement des défenses
6. Accès aux informations d'identification
7. Découverte
8. Mouvement latéral

9. Collecte
10. Commande et contrôle
11. Exfiltration
12. Impact

Chacune de ces catégories tactiques comprend des techniques individuelles qui peuvent être utilisées pour décrire le comportement de l'adversaire. Par exemple, dans la catégorie Accès initial, les comportements comprennent Spearphishing Attachment (pièce jointe de spear phishing), Spearphishing Link (lien de spear phishing, Trusted Relationship (relation de confiance) et Valid Accounts (comptes valides).

Vous pouvez consulter la matrice MITRE Enterprise ATT&CK sur https://attack.mitre.org/wiki/Main_Page.

Cette classification des comportements permet aux équipes de sécurité d'être très précises dans la description et le suivi du comportement de l'adversaire et facilite le partage d'informations entre les équipes.

ATT&CK™ est utile à un large éventail de fonctions de sécurité, des opérations de sécurité et de l'analyse des menaces à la réponse aux incidents. Le suivi du comportement de l'adversaire d'une manière structurée et reproductible permet aux équipes de :

- ☑ Hiérarchiser les réponses aux incidents
- ☑ Mapper des indicateurs vers les attaquants
- ☑ Identifier les lacunes de la sécurisation d'une organisation

Les matrices de renseignement peuvent être utilisées pour normaliser la façon dont vos équipes de sécurité examinent les menaces, les indicateurs, les vulnérabilités et les auteurs. Si vous n'êtes pas prêt à élaborer votre propre matrice d'analyse, envisagez de vous associer à des entreprises de sécurité qui ont conçu des solutions fondées sur ces matrices. Cette approche vous permet de bénéficier rapidement des avantages de la matrice et d'augmenter rapidement l'efficacité de vos activités de sécurisation.

Chapitre 14

Votre parcours du renseignement sur la sécurité

Dans ce chapitre

- Examinez les moyens de clarifier vos besoins et vos objectifs en matière de renseignement sur la sécurité
- Examinez les principaux facteurs de succès qui contribuent à l'efficacité des programmes
- Découvrez comment commencer par de simples solutions et les étendre

« Personne ne s'est jamais perdu sur une route droite. »

— Proverbe

Dans ce chapitre, nous vous recommandons quelques bonnes pratiques pour mapper votre parcours du renseignement et pour créer petit à petit un programme complet de renseignement sur la sécurité.

Ne commencez pas par les flux de données sur les menaces

En fait, de nombreuses organisations entament leurs programmes de renseignement sur les menaces en s'abonnant à des flux de données sur les menaces et en les connectant à une solution SIEM. Cela peut sembler être une bonne façon de commencer parce que beaucoup de flux de données sur les menaces sont open source (donc gratuits) et que les

indicateurs techniques qu'ils transmettent semblent utiles et faciles à interpréter. Donc, puisque tous les logiciels malveillants son malveillants et que toute URL suspecte pourrait être utilisée par un attaquant, plus vous avez d'indices à leur sujet, mieux cela vaut, n'est-ce pas ?

En réalité, la grande majorité des échantillons de logiciels malveillants et des URL suspectes ne concernent pas des menaces actuelles contre votre entreprise. C'est pourquoi transmettre de grands volumes de données non filtrées à votre SIEM donnera presque certainement lieu au genre de lassitude face aux alertes que nous avons examinée au Chapitre 3.

Clarifiez vos besoins et vos objectifs en matière de renseignement sur la sécurité

Comme le renseignement sur la sécurité est utile à un grand nombre d'équipes de votre entreprise, il est important de développer des priorités qui reflètent précisément les besoins et les objectifs globaux de l'entreprise.

Répondez aux questions suivantes

Définissez un ensemble clair d'objectifs en déterminant les besoins de chaque groupe chargé de la sécurité de votre organisation et les avantages que le renseignement sur la sécurité leur fournira.

Commencez par envisager les questions suivantes :

- ☑ Quels sont vos plus grands risques ?
- ☑ Comment faut-il que le renseignement sur la sécurité aborde chacun de ces risques pour vous ?
- ☑ Quel est l'impact potentiel du traitement de chaque risque ?
- ☑ Quelles sont les lacunes devant être comblées par des technologies de l'information ou des ressources humaines pour assurer l'efficacité du renseignement sur la sécurité dans ces domaines ?

Pour un aperçu complet de la puissance du renseignement sur la sécurité, téléchargez « The Ultimate Security Intelligence Kit » (Le kit suprême du renseignement sur la sécurité). Cette collection de livres blancs, de rapports, de vidéos, de podcasts et bien plus encore décrit en détail le fonctionnement du renseignement sur la sécurité et tous les avantages qu'il procure à votre organisation.

Identifiez les équipes qui bénéficieront du renseignement sur la sécurité

Les équipes de l'ensemble de votre service de sécurité bénéficieront de renseignement permettant des prises de décisions éclairées et offrant des points de vue uniques. Le renseignement qui est global, pertinent et facile à absorber peut, potentiellement, révolutionner le fonctionnement de certains rôles de votre organisation. Lors de la détermination de la manière de faire progresser votre stratégie de renseignement sur les menaces, il est important d'identifier tous les utilisateurs potentiels de votre organisation et d'aligner le renseignement sur leurs utilisations spécifiques.

Découvrez les résultats du renseignement sur la sécurité que chaque groupe utilisera et comment ces groupes en bénéficieront en termes de délais de réponse, d'économies, d'efficacité du personnel, de décisions d'investissement, etc. Les besoins et les avantages ne sont pas toujours clairs. Documenter ces détails vous permettra d'établir des priorités, de justifier des investissements et de découvrir de nouvelles utilisations du renseignement sur la sécurité.

Facteurs de réussite clés

Plusieurs facteurs contribuent souvent à l'efficacité des programmes de renseignement sur la sécurité. Plus tôt vous les implémenterez, plus vite vous tirerez le meilleur parti possible du renseignement sur la sécurité.

Obtenir des avantages rapidement grâce à la surveillance

La surveillance du renseignement sur la sécurité fournit souvent des avantages rapidement avec des investissements assez modestes. Pour ce faire, il est essentiel d'examiner quels sont les quelques types de données qui sont particulièrement importantes pour votre entreprise et quelle stratégie de sécurité de l'information vous aidera à prévoir les menaces émergentes ou à obtenir des alertes rapides lors d'attaques véritables. Ces activités peuvent inclure :

- ☑ Examiner les nouvelles vulnérabilités affectant vos logiciels, vos serveurs et vos terminaux les plus importants
- ☑ Suivre les tendances des menaces qui posent le plus de risques potentiels à vos activités
- ☑ Être à l'affût de toute fuite d'informations d'identification, de données ou de codes d'entreprise, ou d'apparition de code sur des sites publics ou de l'Internet clandestin
- ☑ Analyser le Web et les réseaux sociaux pour rechercher les noms de votre organisation et de ses marques, divisions et produits

Il existe probablement certains types de données d'importance vitale pour votre entreprise que vous pouvez surveiller sans investissement dans de nouvelles infrastructures ou du personnel. Il est probable que cette surveillance vous procure des bénéfices rapides, prouve les avantages du renseignement sur la sécurité et suscite de plus en plus d'enthousiasme envers le programme.

S'assurer que les rapports sont utiles

De nombreuses entreprises se retrouvent piégées par la production de rapports quotidiens qui sont peu ou ne sont pas utilisés. Souvent, ceux-ci prennent la forme de listes à puces des menaces détectées avec une simple note d'impact faible/moyenne/élevée. Bien que ces rapports montrent que les analystes sont occupés et sensibilisent l'entreprise aux cybermenaces, ils n'ont généralement aucun impact sur les résultats opérationnels.

Ne vous inquiétez pas de la production de rapports selon un calendrier. Assurez-vous plutôt que chaque rapport et communication que vous produisez contient du renseignement et des perspectives qui permettent aux parties concernées de prendre des décisions et d'adopter les mesures appropriées. Dans l'idéal, ceux-ci comprennent, minimum, les informations élémentaires suivantes.

- ☑ Le ou les auteurs de menace(s) probable(s)
- ☑ Des techniques et outils utilisés par les auteurs de menaces
- ☑ Les cibles probables dans l'organisation
- ☑ Si la menace représente un réel danger pour l'organisation
- ☑ La probabilité que les contrôles de sécurité existants soient en mesure d'atténuer la menace
- ☑ Les mesures recommandées pour y répondre

Automatiser autant que possible

Les programmes de renseignement sur les menaces efficaces mettent généralement l'accent sur l'automatisation dès le départ. Ils commencent par automatiser les tâches fondamentales telles que l'agrégation, la comparaison, l'étiquetage et la contextualisation des données. Quand ces tâches sont effectuées automatiquement, les êtres humains ont plus de temps à consacrer à la prise de décisions éclairées et efficaces.

Au fur et à mesure que votre programme de renseignement sur les menaces se perfectionne, vous découvrirez encore plus d'occasions d'automatiser. Vous serez en mesure d'automatiser le partage d'informations au sein d'un plus grand groupe de solutions de sécurité et d'automatiser davantage de flux de travail qui fournissent du renseignement aux équipes chargées des opérations de sécurité et de la réponse aux incidents, aux analystes de menaces, aux équipes de prévention de fraude, aux spécialistes en gestion des vulnérabilités, aux gestionnaires des risques posés par les tiers et aux défenseurs de la marque. Vous pourrez

vous débarrasser d'énormes quantités de travail grâce à vos solutions de renseignement sur la sécurité, car vous disposerez de logiciels qui établissent automatiquement des corrélations entre les données sur les menaces, produisent des cotes de risque, identifient les faux positifs et bien davantage.

Lorsque vous évaluez des solutions de renseignement sur les menaces, examinez la mesure dans laquelle ils automatisent. L'automatisation se limite-t-elle à l'agrégation et au recoupement des données ou la solution ajoute-t-elle du contexte qui permet à vos équipes de prendre des décisions fondées sur les risques en toute confiance ? N'oubliez pas qu'entrer davantage de données brutes dans votre logiciel de renseignement sur la sécurité n'ajoute de la valeur que si elles sont analysées, organisées et transmises automatiquement dans un format facile à comprendre et à utiliser.

L'intégration du renseignement sur les menaces à l'infrastructure et aux processus

L'intégration d'outils de renseignement sur les menaces à des systèmes existants est une manière efficace de le rendre accessible et utilisable sans submerger vos équipes avec de nouvelles technologies.

Un aspect essentiel de cette intégration consiste à garantir la visibilité, pour vos logiciels de renseignement sur la sécurité, des événements et des activités de sécurité captés par vos outils de sécurité et de réseau existants . La combinaison et la corrélation de points de données internes et externes peuvent produire un véritable renseignement qui est à la fois pertinent pour votre entreprise et placé dans le contexte du paysage plus vaste des menaces.

L'autre aspect critique de l'intégration est la transmission du renseignement le plus important, spécifique, pertinent et contextualisé au bon groupe, au bon moment. Pour ce faire, intégrez votre solution de renseignement sur la sécurité à vos SIEM et à d'autres outils de sécurité via des API ou des interfaces développées conjointement avec des fournisseurs d'outils de sécurité.

Lorsque vous évaluez les solutions de renseignement sur les menaces, il est important de comprendre quelles sont celles qui peuvent s'intégrer à vos logiciels existants et être utiles aux utilisations de vos équipes de sécurité.

Obtenir l'aide d'experts aide à cultiver des experts internes

La valeur que vous obtenez du renseignement sur les menaces est directement liée à votre capacité à le rendre pertinent pour votre organisation et à l'appliquer à ses processus de sécurité neufs et existants.

Pour atteindre plus rapidement ces objectifs, travaillez avec un fournisseur ou un expert-conseil qui fournit à la fois une expertise et des capacités techniques pour permettre à votre organisation de tirer le meilleur parti possible du renseignement sur les menaces. Au fil du temps, travailler avec un tel partenaire permettra aux membres de votre équipe de devenir eux-mêmes experts en renseignement sur la sécurité.

Cherchez des partenaires qui disposent d'un éventail d'experts en renseignement sur la sécurité à connaissances variées et approfondies. Ces spécialistes devraient avoir les connaissances et l'expérience nécessaires pour comprendre vos besoins afin de vous aider à tirer le meilleur parti de votre investissement. Assurez-vous qu'ils sont disponibles quand vous faites appel à leur expertise et qu'ils collaborent avec vous pour identifier de nouveaux avantages à tirer du renseignement sur la sécurité dans votre entreprise. Les partenaires que vous choisissez doivent être dévoués à votre réussite actuelle et soutenir vos équipes de sécurité au fur et à mesure de vos progrès.

Pour plus d'informations sur le choix de la bonne solution de renseignement sur la sécurité, téléchargez « The Buyer's Guide to Intelligence » (Guide de l'acheteur de renseignement) de Recorded Future. Il comprend un modèle d'appel d'offres pratique à utiliser lors de l'évaluation des capacités de différents fournisseurs.

Commencez par de simples solutions et étendez-les

Le renseignement sur la sécurité n'est pas un monolithe qui tombe en un coup sur le service de sécurité. Au contraire, vous pouvez choisir comment collecter, traiter, analyser et diffuser le renseignement de sécurité à différents groupes et intervenants.

Vous pouvez décider commencer simplement avec votre personnel actuel (au lieu de constituer une équipe dédiée au renseignement sur la sécurité), quelques sources de données et l'intégration à des outils de sécurité existants, comme les solutions SIEM et les systèmes de gestion des vulnérabilités. Bientôt, il est possible que vous bénéficiez du passage à du personnel dédié, à davantage de sources de données, d'outils et d'intégrations et à des flux de travail plus automatisés, comme illustré à la figure 14-1.

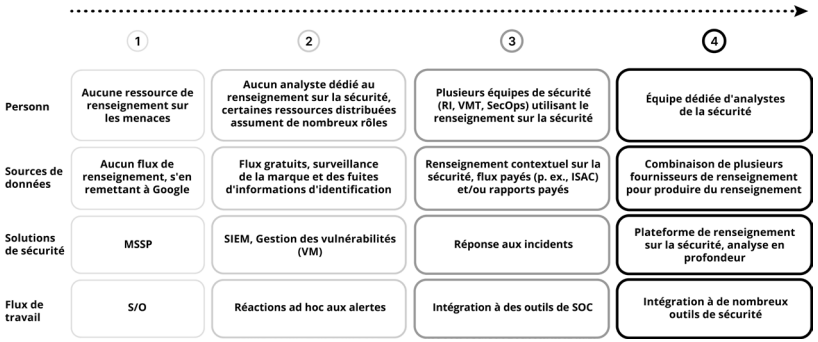


Figure 14-1 : Quatre étapes de maturité du programme de renseignement sur la sécurité, de l'absence de ressources internes à un programme doté de personnel et fortement automatisé.

Entamez ce parcours en examinant les besoins de tous les groupes de votre service de cybersécurité et voyez comment le renseignement sur la sécurité leur permettra d'atteindre leurs objectifs.

Au fil du temps, vous serez en mesure d'élaborer un programme complet de renseignement sur la sécurité capable d'accomplir les fonctions suivantes :

- ☑ Scrute le plus grand éventail possible de sources techniques, ouvertes et de l'Internet clandestin
- ☑ A recours à l'automatisation pour fournir des renseignements faciles à utiliser
- ☑ Fournit des alertes pleinement contextualisées, en temps réel, avec peu de faux positifs
- ☑ S'intègre aux technologies et processus de sécurité existants et les améliore
- ☑ Améliore constamment l'efficacité et l'efficience de l'ensemble de votre service de sécurité

Chapitre 15

Mettre sur pied votre équipe de renseignement sur la sécurité

Dans ce chapitre

- Comprenez quels sont les processus, les personnes et la technologie dont est composée une capacité dédiée de renseignement sur les menaces
- Découvrez comment ces équipes utilisent le renseignement sur la sécurité pour évaluer les risques et pour assurer la continuité des activités
- Examinez les moyens de collaborer avec les communautés du renseignement sur les menaces

"Les talents permettent de gagner des matchs, mais le travail en équipe et le renseignement permettent de gagner des championnats."

— Michael Jordan

Nous avons vu les avantages du renseignement sur la sécurité pour vos équipes de sécurité. Voici quelques suggestions sur la façon d'organiser votre équipe centrale dédiée au renseignement sur la sécurité.

Dédiée, mais pas nécessairement séparée

Comme nous l'avons mentionné dans le chapitre précédent, il est possible que vous souhaitiez entamer votre parcours du renseignement sur la sécurité avec des collaborateurs qui continuent aussi à jouer d'autres rôles dans différentes équipes de l'organisation.

Finalement, deux questions se poseront probablement :

1. Devrait-il y avoir une équipe dédiée au renseignement sur la sécurité ?
2. Devrait-elle être indépendante ou exister au sein d'un groupe de sécurité existant ?

Les réponses sont : oui et cela dépend.

Il vaut mieux avoir une équipe dédiée

Au fur et à mesure de la constitution d'un programme complet de renseignement sur les menaces, vous devriez constituer une équipe qui se consacre uniquement à la collecte et à l'analyse des données sur les menaces et à leur conversion en renseignement. Le seul objectif de cette équipe devrait être de fournir des renseignements pertinents et exploitables à des intervenants clés, y compris des membres de la direction et du conseil d'administration.

Du dévouement et une vision globale large sont nécessaires pour s'assurer que les membres de votre équipe consacrent suffisamment de temps à la collecte, au traitement, à l'analyse et à la diffusion du renseignement le plus précieux pour l'ensemble de l'organisation. Il est essentiel d'éviter la tentation de se concentrer sur les besoins en renseignement d'un seul groupe plutôt que les autres.

Votre entreprise détermine la position de l'équipe

Avoir une équipe de renseignement sur la sécurité jouissant d'indépendance organisationnelle présente des avantages, comme l'illustre la figure 15-1, tels que plus d'autonomie et de prestige.

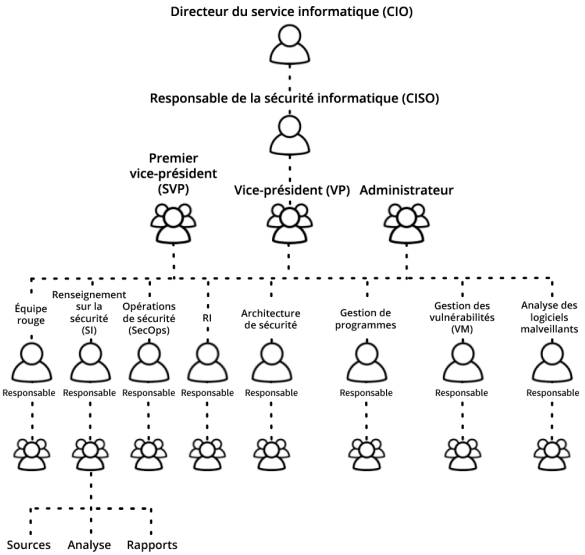


Figure 15-1 : Le renseignement sur la sécurité en tant que groupe indépendant au sein de la structure organisationnelle de sécurité.

Toutefois, ces avantages peuvent être totalement contrecarrés par des questions politiques liées à la création d'une équipe avec un nouveau responsable de haut niveau et un budget qui lui est propre, et qui retire des analystes compétents de leurs groupes existants.

Une équipe dédiée de renseignement sur les menaces ne doit pas nécessairement être une fonction séparée qui rend directement compte à un vice-président ou au CISO. Elle peut, au contraire, appartenir à un groupe qui s'occupe déjà du renseignement sur la sécurité. Très souvent, il s'agit d'un groupe de réponse aux incidents. Cette approche est souvent une option viable pour éviter les conflits avec les équipes de sécurité bien établies.

Choisir les collaborateurs

Si vous adoptez une approche graduelle pour la mise sur pied de votre équipe principale de renseignement sur les menaces, commencez par des personnes qui font déjà partie du service de cybersécurité et qui appliquent le renseignement sur les menaces à leurs domaines de sécurité particuliers. Ils ne possèdent peut-être pas le titre d'« analyste du renseignement sur la sécurité » ou ne se considèrent peut-être pas comme tels au début, mais ils sont probablement les collaborateurs disponibles les plus capables de constituer l'épine dorsale de votre capacité émergente de renseignement sur la sécurité.

Compétences essentielles

Le but de la fonction de renseignement sur la sécurité est de renforcer toutes les autres équipes de sécurité, ce qui permet à chacun de mieux protéger l'ensemble de l'entreprise. Il est crucial que le renseignement sur la sécurité inclue des collaborateurs qui comprennent l'activité principale, les flux de travail opérationnels, l'infrastructure de réseau, les profils de risque et la chaine d'approvisionnement, ainsi que l'infrastructure technique et les applications logicielles de l'ensemble de l'organisation.

Au fur et à mesure de la maturation de l'équipe de renseignement sur la sécurité , vous souhaiterez lui ajouter des membres compétents en :

- ☑ Corrélation entre données externes et télémétrie interne
- ☑ Ingénierie inverse de logiciels malveillants et reconstruction d'attaque (enquête juridico-informatique)
- ☑ Sensibilisation aux situations de menaces et recommandations de contrôles de sécurité
- ☑ Chasse proactive aux menaces internes, y compris aux menaces d'initiés

- ☑ Formation des collaborateurs et des clients aux cybermenaces
- ☑ Collaboration avec la communauté du renseignement sur la sécurité au sens plus large
- ☑ Identification et gestion de sources d'information

Vous pouvez également ajouter du personnel de domaines divers, y compris avec de l'expérience en dehors des technologies de l'information. En particulier :

- ☑ **Les analystes qui ont des antécédents militaires et de renseignement** comprennent généralement comment structurer les processus de collecte, d'analyse et de compte-rendu de données, comment contrecarrer le parti pris des sources et comment présenter le renseignement et les conclusions de manière claire, concise et adaptée à leur public.
- ☑ **Les membres du personnel expérimentés en application de la loi** s'y connaissent en tactiques et méthodes criminelles et sont aptes à distinguer les faits des opinions.

Collecte et enrichissement des données sur les menaces

Nous avons parlé des données des différentes sources de données au chapitre 2. Ici, nous examinons comment travailler avec tout un éventail de sources pour garantir leur exactitude et leur pertinence.

La supériorité humaine

Les fournisseurs de renseignement sur la sécurité fournissent souvent certains types de renseignement stratégique, mais vous pouvez aussi constituer des capacités internes pour recueillir des informations sur les sujets et les événements les plus pertinents pour votre organisation.

Vous pouvez, par exemple, élaborer un robot d'indexation qui analyse le code des pages Web des 5 000 destinations Web les plus souvent consultées par vos collaborateurs. Cette analyse peut vous donner une idée du potentiel d'attaques par infection de téléchargement. Vous pouvez faire part de ces perspectives à l'équipe chargée de l'architecture de sécurité pour les aider à proposer des contrôles pour vous défendre contre ces attaques. Ce genre de renseignement génère des données concrètes beaucoup plus utiles que des anecdotes, des conjectures et des statistiques génériques sur des attaques.

Sources supplémentaires

Des sources exclusives qui peuvent renforcer vos ressources en matière de renseignement sur la sécurité comprennent :

- ☑ Des flux de fournisseurs ou d'ISAC
- ☑ Autoriser les listes
- ☑ Refuser les listes
- ☑ Les recherches d'équipes de renseignement sur la sécurité

Combiner les sources

Une solution automatisée de renseignement sur les menaces permet à l'équipe qui en est chargée de centraliser, de combiner et d'enrichir les données de différentes sources avant que les données ne soient ingurgitées par d'autres systèmes de sécurité ou visualisées par des analystes humains d'équipes d'opérations de sécurité.

La figure 1--3 affiche les éléments d'une solution automatisée de ce type. Dans ce processus, les informations d'un fournisseur de renseignement sur la sécurité sont filtrées pour trouver les données importantes pour l'organisation et pour des équipes de cybersécurité spécifiques. Elles sont alors enrichies de données de sources externes de renseignement sur la sécurité et converties en formats appropriés pour des outils, notamment les systèmes SIEM, de tickets et autres. Cette traduction automatisée des données en aperçus pertinents est l'essence même du renseignement sur les menaces.

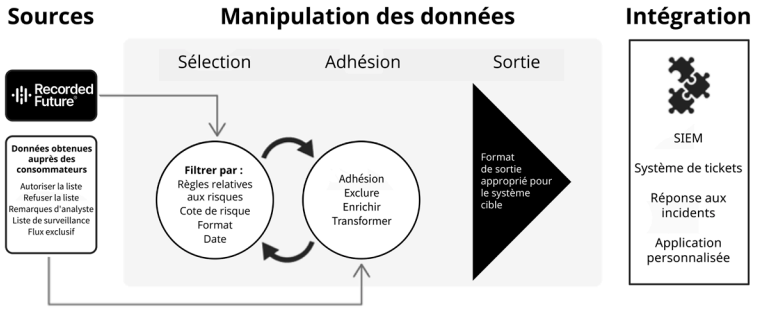


Figure 15-2 : Une plate-forme de renseignement sur la sécurité peut centraliser, combiner et enrichir les données, puis les formater pour différents systèmes cibles. (Source : Recorded Future)

Le rôle des machines intelligentes

Nous en sommes au point où les composants IA ont réussi à dominer le langage des menaces et peuvent identifier avec précision les termes "malveillants".

Les progrès des analyses et du traitement automatique des langues naturelles (TALN) peuvent conférer des avantages supplémentaires à l'équipe de renseignement sur la sécurité. Avec la bonne technologie, les mentions de menaces provenant de toutes sources peuvent être comprises quelle que soit leur langue. Cela permet aux êtres humains et aux machines de les analyser sans égard à leur langue d'origine.

La combinaison des analyses et du TALN offre aux organisations d'excellentes occasions de tirer parti du renseignement sur la sécurité. Ces technologies peuvent non seulement supprimer les barrières linguistiques mais aussi réduire les charges de travail des analystes en se chargeant de nombreuses tâches liées à la collecte de données et à la corrélation. Combinées au pouvoir d'envisager simultanément plusieurs sources de données et d'informations pour produire du véritable renseignement sur les menaces, ces capacités facilitent l'élaboration d'un plan compréhensible du paysage de menaces.

Collaborer avec les communautés du renseignement sur la sécurité

Le renseignement sur la sécurité ne peut pas se développer dans le vide. Les relations externes sont indispensables à la réussite des équipes du renseignement sur la sécurité. Aussi avancée que soit votre équipe, aucun groupe n'est, à lui seul, aussi intelligent que l'ensemble du monde du renseignement sur la sécurité.

De nombreuses communautés du renseignement sur la sécurité permettent aux organisations individuelles de partager des données pertinentes et opportunes sur des attaques, permettant à d'autres membres de protéger leurs organisations avant d'en être victimes. Collaborer avec des communautés dignes de confiance comme les ISAC (centres de partage et d'analyse d'informations) est crucial pour diminuer les risques non seulement pour vos entreprises individuelles mais aussi pour l'ensemble de votre secteur et pour le monde de la cybersécurité au sens large. La participation nécessite du temps et des ressources, comme la communication par e-mail avec des pairs et la participation à des congrès sur la sécurité. Toutefois, l'établissement de relations doit être une priorité pour la réussite du renseignement sur la sécurité.

Conclusion

Utiliser le renseignement d'élite pour perturber vos adversaires

« Aucun opposant prudent ne prend à la légère ses adversaires. »

— Johann Wolfgang von Goethe

Deux points essentiels à retenir de ce livre

L'idée, au début de ce livre, était que le renseignement est précieux pour tous ceux qui occupent des fonctions de sécurité sans se limiter à celles-ci. Le renseignement permet aux équipes d'anticiper les menaces, de réagir plus rapidement aux attaques et de prendre de meilleures décisions pour diminuer les risques. Tout au long du livre, nous avons examiné comment adopter une approche proactive et complète de la sécurité en utilisant le renseignement pour différentes facettes de la stratégie de sécurité de votre organisation.

C'est en cela que consiste le renseignement sur la sécurité : une approche qui amplifie l'efficacité des équipes et des outils de sécurité en exposant les menaces inconnues, en éclairant mieux les décisions et en permettant une compréhension commune pour aboutir à l'accélération de la réduction des risques dans l'ensemble de l'organisation. Les six piliers : le renseignement pour les opérations de sécurité, le renseignement sur les vulnérabilités, le renseignement sur les menaces, le renseignement sur les tiers, le renseignement sur la marque et le renseignement géopolitique offrent aux

organisations un puissant tour d'horizon sur les risques qu'elles courent, tout en rationalisant les modes de travail de leurs équipes.

Revenons aux quatre principes du renseignement sur la sécurité décrits dans la préface. Quels résultats atteindrez-vous lorsque vous adopterez ces principes ?

1. Vous perturberez les adversaires qui ciblent votre organisation.

En identifiant les adversaires les plus dangereux pour votre organisation et en comprenant comment ils opèrent, vous mettrez en place les défenses appropriées et rendrez la vie si difficile à vos attaquants qu'ils renonceront à leurs efforts pour vous cibler.

2. Vous obtiendrez le contexte nécessaire pour prendre des décisions éclairées et adopter des mesures.

En générant des informations contextuelles opportunes, claires et exploitables, vous enrichirez vos connaissances, simplifierez vos processus de prise de décision et amplifierez l'impact de toutes vos solutions de sécurité.

3. Vos employés et vos machines travailleront de concert pour améliorer l'efficacité globale.

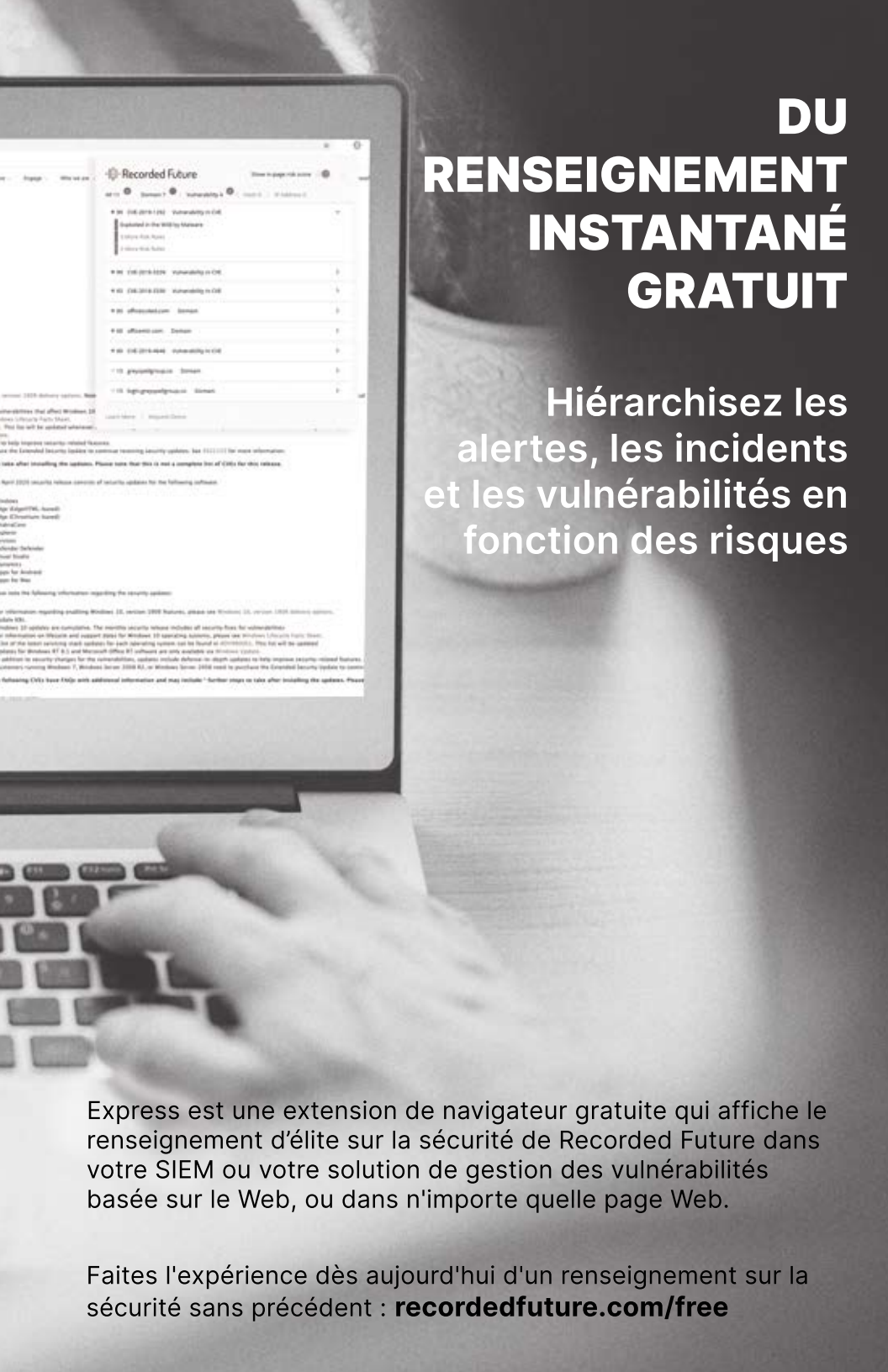
Les machines traitent et classent les données brutes à une vitesse et sur une échelle extraordinaires, ce qui donne aux êtres humains le temps et le contexte nécessaires pour effectuer une analyse intuitive et globale. En améliorant les flux de travail humains et automatisés, le renseignement sur la sécurité permet de gagner du temps et de l'argent, de diminuer l'épuisement professionnel et d'améliorer la sécurité globale.

4. Vos équipes de sécurité et de nombreux autres membres de votre entreprise travailleront plus intelligemment.

Toutes les équipes de sécurité, ainsi que les cadres de votre organisation et l'ensemble de vos collègues, de la gestion des risques et de la prévention de fraude, à la gestion de la marque et des risques posés par les tiers, et à d'autres encore, recevront du renseignement plus pertinent et moins

de données brutes inadéquates. Ils pourront interagir avec le renseignement approprié au moment opportun, dans des formats faciles à comprendre, grâce aux outils de collaboration et de sécurité existants. Ils seront en mesure de prendre de meilleures décisions plus rapidement.

L'un des grands avantages du renseignement sur la sécurité est qu'il vous permet de développer votre programme par étapes. Commencez par améliorer l'efficacité des activités essentielles dans les opérations de sécurité, la réponse aux incidents, la gestion des vulnérabilités et le renseignement sur les menaces, ou en établissant de nouvelles bases pour des programmes de plus en plus importants liés aux risques posés par les tiers, à la protection de la marque et à la sécurité géopolitique. Quoi qu'il en soit, vous obtiendrez des avantages mesurables pour votre organisation à chaque étape. Nous espérons que ce manuel vous a fourni une vue d'ensemble du vaste potentiel du renseignement sur la sécurité et de la façon de le réaliser.



DU RENSEIGNEMENT INSTANTANÉ GRATUIT

Hiérarchisez les alertes, les incidents et les vulnérabilités en fonction des risques

Express est une extension de navigateur gratuite qui affiche le renseignement d'élite sur la sécurité de Recorded Future dans votre SIEM ou votre solution de gestion des vulnérabilités basée sur le Web, ou dans n'importe quelle page Web.

Faites l'expérience dès aujourd'hui d'un renseignement sur la sécurité sans précédent : **recordedfuture.com/free**

LE MANUEL DU RENSEIGNEMENT SUR LA SÉCURITÉ

Troisième édition

Comment perturber vos adversaires et diminuer les risques grâce au renseignement sur la sécurité

Le renseignement sur la sécurité est une approche visant à diminuer les risques axée sur les résultats, qui amalgame les perspectives internes et externes sur les menaces, la sécurité et les activités. Ce livre explique comment utiliser le renseignement sur la sécurité pour exposer les menaces inconnues, clarifier les priorités en matière de sécurité, prendre des décisions rapides et éclairées, et favoriser une compréhension commune de la diminution des risques dans l'ensemble de votre entreprise.

Découvrez comment le renseignement sur la sécurité apporte une aide précieuse à toutes les équipes de sécurité sans se limiter à celles-ci :

- **Renseignement des opérations de sécurité (SecOps) :** accélérez le triage et favorisez une intervention proactive en cas d'incident.
- **Renseignement sur les vulnérabilités :** hiérarchisez les correctifs en fonction de la pertinence et de l'exploitabilité réelles des vulnérabilités.
- **Renseignement sur les menaces :** utilisez la connaissance des tactiques, techniques et procédures des attaquants pour renforcer vos défenses de sécurité et évaluer les risques.
- **Renseignement tiers :** identifiez et atténuez les sources de risque de votre chaîne d'approvisionnement avant qu'elles n'affectent vos systèmes.
- **Renseignement sur la marque :** mettez fin à l'usurpation de marque pour protéger la réputation de votre entreprise sur le Web et sur les réseaux sociaux.
- **Renseignement géopolitique :** défendez-les les sites et les installations physiques essentiels à votre entreprise, partout dans le monde.
- **Renseignement pour les responsables de la sécurité :** améliorez la visibilité sur le vaste panorama des menaces afin d'évaluer les risques et de prendre des décisions intelligentes qui amélioreront vos résultats financiers.

À propos de Recorded Future

Recorded Future fournit le renseignement sur la sécurité le plus perfectionné du monde, sur le plan technique, pour perturber vos adversaires, armer vos défenseurs et protéger votre entreprise. La plate-forme proactive et prédictive de Recorded Future transmet en temps réel un renseignement d'élite exploitable, intuitif, riche en contexte et prêt à être intégré dans l'ensemble de votre écosystème de sécurité.

recordedfuture.com

ISBN 978-1-948939-16-4

Recorded Future®