OPTIMISATION DES OPÉRATIONS DE SÉCURITÉ GRÂCE AU RETOUR SUR INVESTISSEMENT DE THREATQ™

Ryan W. Trost, ThreatQuotient

THREATQUOTIENT™

LIVRE BLANC

OPTIMISATION DES OPÉRATIONS DE SÉCURITÉ GRÂCE AU RETOUR SUR INVESTISSEMENT DE THREATQ

INTRODUCTION

À l'heure où les équipes de sécurité occupent une place de plus en plus importante au sein de l'entreprise, elles doivent faire de la gestion des informations de cybersécurité un enjeu prioritaire pour assurer sa survie. Elles commencent cependant à trouver leurs marques, en tirant le meilleur parti de la Threat Intelligence, ou renseignement sur les menaces, à l'aide de ThreatQ™, outil essentiel pour gagner en efficacité. ThreatQ permet à ces équipes de réaliser des progrès considérables, non seulement dans la gestion de ces connaissances, mais aussi dans l'automatisation des processus et dans l'identification et le tri des éléments à investiguer. Elles peuvent en outre accomplir ces tâches beaucoup plus rapidement. Ce livre blanc examine le retour sur investissement offert par ThreatQ, en se concentrant spécifiquement sur trois composantes :

- Attribution de scores et priorisation des renseignements sur les menaces
- Automatisation et renforcement du sensor grid
- Réduction des délais de détection et d'intervention

Le déploiement de ThreatQ afin de structurer la Threat Intelligence et d'exécuter des workflows de base permet aux entreprises de réaliser un gain de productivité analytique équivalant à celle de six à neuf analystes de SOC (Security Operations Center) employés à temps plein.

ATTRIBUTION DE SCORES AUX RENSEIGNEMENTS : DANS LA PRATIQUE

Le volume d'indicateurs publiés quotidiennement continue d'augmenter à un rythme alarmant, au point que la masse de renseignements à valider manuellement devient ingérable[1]. En 2016, la Carnegie Mellon University a publié un livre blanc[2] qui analysait l'écosystème de listes noires open source, composé de plus de 180 millions d'indicateurs de compromission (IOC), même si ces listes ne concernent que des adresses IP et des noms de domaine complets. Les indicateurs de compromission déclenchent des alertes qui, à leur tour, donnent lieu à des investigations de la part des analystes. Cependant, les alertes n'ont pas toutes la même importance, de sorte que du personnel est parfois inutilement affecté à la traque de menaces fictives (faux positifs). Une méthodologie d'attribution de scores définie par le client permet aux équipes de définir leur propre positionnement en matière de risques, en fonction des ressources et outils de détection dont elles disposent, ainsi que des autres priorités des équipes.

La fonctionnalité d'attribution de scores et de priorisation de ThreatQ automatise un processus qui nécessite actuellement toute une équipe d'analystes, à savoir la gestion du cycle de vie des données de Threat Intelligence : leur collecte, leur assainissement, leur analyse et leur déploiement. Par ailleurs, l'attribution de scores étant propre au client et définie par ses soins, elle permet à l'équipe d'analystes de déterminer ses propres niveaux de risque et d'appliquer cette configuration à tous les renseignements reçus. Le résultat ? Une optimisation des processus et un retour sur investissement représentant deux à trois équivalents temps plein.

THREATQ™

ATOUTS DE LA MÉTHODOLOGIE D'ATTRIBUTION DE SCORES DE THREATQ :

1) Possibilité pour les clients de maîtriser leur destin en déterminant de façon précise leurs niveaux de risque acceptables
2) Possibilité de personnaliser l'algorithme d'attribution de scores, *parce que personne ne connaît votre environnement mieux que vous*
3) Plage de scores exploitable : une plage de 1 à 5 n'est pas suffisamment nuancée tandis qu'une plage de 1 à 1 000 est trop difficile à conceptualiser et s'écarte considérablement des meilleures pratiques du secteur
4) Juste milieu dans l'attribution de scores : un nombre insuffisant d'éléments ne reflète pas le risque avec précision, tandis que des éléments trop nombreux submergent les équipes et sont par conséquent ignorés
5) Transparence PERMANENTE des scores grâce à l'affichage de leur mode de calcul
6) Scores reflétant les variables d'environnement locales (résultats d'analyse en solution sandbox, résultats issus de la gestion des tickets, dates d'observation, etc.)
7) Mise à niveau du score de l'indicateur à chaque ajout d'une nouvelle information

1 Souvent, les équipes choisissent de « faire confiance sous réserve de vérification » à la Threat Intelligence issue de sources externes pour réduire l'impact opérationnel que pourrait avoir un mauvais renseignement. Certains adversaires sont connus pour dissimuler des fichiers malveillants dans les services d'hébergement légitimes pour augmenter leurs chances de passer outre les mécanismes de filtrage.

2 resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_466029.pdf

L'octroi de scores aux renseignements sur les menaces a pour principal objectif d'assurer un contrôle optimal sur l'ensemble des données et leur extrême précision. En d'autres termes, vous n'avez pas à dépendre uniquement de communautés, d'évaluations ou de flux externes pour décider que telle ou telle menace est plus ou moins dangereuse pour votre environnement.

L'ALGORITHME OPÉRATIONNEL D'ATTRIBUTION DE SCORES EN ACTION

La collecte des indicateurs de compromission sur plusieurs flux pendant quatre mois en a généré près d'un million. Lorsqu'un client applique le cadre personnalisé d'attribution de scores de ThreatQ en fonction de ses niveaux de risque, les renseignements recueillis sont filtrés en un sous-ensemble facile à gérer. ThreatQ offre diverses approches d'attribution de scores qui évoluent en fonction du niveau d'expérience de l'équipe. Cette évolution s'effectue comme suit :

Approche de base — Les équipes débutantes exploiteront tous les indicateurs de compromission de façon équivalente. Un aperçu rapide montre que le nombre total d'indicateurs collectés au sein d'un ensemble de données unique est de **910 321**.

Approche intermédiaire — Les équipes plus expérimentées prendront en compte la gravité des alertes issues de sources commerciales. Le volume d'indicateurs répartis en fonction du score de certitude propre au fournisseur (niveau élevé/moyen/faible) affiché ci-dessous montre qu'il est encore très important.

Niveau de certitude du caractère malveillant = ÉLEVÉ = **319 754**
Niveau de certitude du caractère malveillant = MOYEN = 497 969
Niveau de certitude du caractère malveillant = FAIBLE = 80

Approche avancée — La fonctionnalité la plus puissante calcule un score personnalisé pour l'entreprise en tenant compte de ses ressources, des menaces auxquelles elle est confrontée et des outils dont elle dispose. Dans ce scénario, nous adoptons le point de vue d'un responsable de SOC dans le secteur de la défense et appliquons des scores personnalisés plus élevés aux attributs les plus pertinents pour « notre » entreprise. La figure 1 montre que nous choisissons d'« augmenter » les scores de risque pertinents plutôt que d'allouer des valeurs négatives aux attributs situés à l'autre bout du spectre qui représentent un risque faible ou nul pour l'entreprise.

Avec l'application de l'algorithme d'attribution de scores personnalisé, l'ensemble des indicateurs de compromission, près d'un million, sont répartis en catégories de risque, comme suit :

Catégorie de risque	Nombre d'indicateurs	Pourcentage
Très élevé	27 358	~ 3 %
Élevé	45 651	~ 5 %
Moyen	312 623	~ 34 %
Faible	248 211	~ 27 %
Très faible	276 478	~ 30 %

Figure 1. Ventilation des scores des indicateurs après application de l'algorithme ThreatQ d'attribution de scores personnalisé défini par l'utilisateur.

ThreatQ est capable de recalculer automatiquement les scores d'environ un million d'indicateurs pour n'en conserver que moins de 10 % (soit approximativement 72 500) sans nécessiter l'intervention constante des analystes. Résultat : inutile de mobiliser toute une équipe sur les tâches usuelles du cycle de gestion des données de Threat Intelligence. De plus, l'entreprise adopte ainsi une approche uniforme de gestion des menaces, dont le processus d'évaluation serait autrement déséquilibré du fait que chaque analyste a un seuil de risque légèrement différent.

ThreatQ permet aux clients de déterminer de façon plus stratégique QUELLES connaissances doivent être déployées immédiatement et LESQUELLES nécessitent d'autres recherches. La configuration de l'attribution de scores définie par l'utilisateur est très simple et néanmoins puissante, et offre une grande granularité, comme l'illustre la figure 2. Les renseignements sur les menaces ayant un niveau de certitude plus élevé peuvent être transmis aux technologies de blocage en fonction du risque que celles-ci représentent pour l'entreprise. Ainsi, ceux dotés de scores de menace élevés, qui sont donc plus fiables, seront déployés vers les technologies de blocage (pare-feux, systèmes IPS, proxys web, endpoints, etc.). En revanche, ceux ayant des scores de menace plus faibles et qui sont par conséquent moins fiables seront distribués aux technologies de détection (systèmes IDS, NetFlow, etc.) pour réduire l'impact opérationnel dû aux faux positifs. Le retour sur investissement ainsi obtenu est crucial pour les entreprises aux outils d'infrastructure limités dont les sondes peinent déjà à suivre.

RENFORCEMENT DU SENSOR GRID : CANALISER DE FAÇON PRÉCISE L'AFFLUX DE DONNÉES

ThreatQ est capable de renforcer immédiatement et automatiquement la protection assurée par votre sensor grid en fonction des scores des indicateurs de compromission, de l'exportation personnalisée et de la recherche rétrospective bidirectionnelle, ce qui réduit considérablement le nombre de tâches manuelles et fragmentées actuellement nécessaires. De plus, ThreatQ automatise le processus pour assurer une mise à jour des sondes dans les quelques minutes qui suivent l'importation, offrant ainsi un retour sur investissement qui représente un à deux équivalents temps plein. Auparavant, mon équipe collectait les renseignements de cybersécurité auprès de différentes sources. Toutefois, comme nous n'étions pas administrateurs réseau, nous n'avions pas l'autorisation de déployer ces connaissances. Pour les transmettre aux différentes sondes (pare-feux, proxy web, défenses SMTP, etc.), nous devions nous en remettre entièrement aux administrateurs système et réseau. Malheureusement, nos priorités ne coïncidaient pas avec les leurs, si bien qu'il s'écoulait souvent entre 24 et 48 heures, voire davantage, avant que les renseignements collectés soient déployés. Cet obstacle opérationnel causait des tracas considérables à mon équipe comme nous ne savions jamais exactement « quand » les informations les plus récentes seraient déployées.

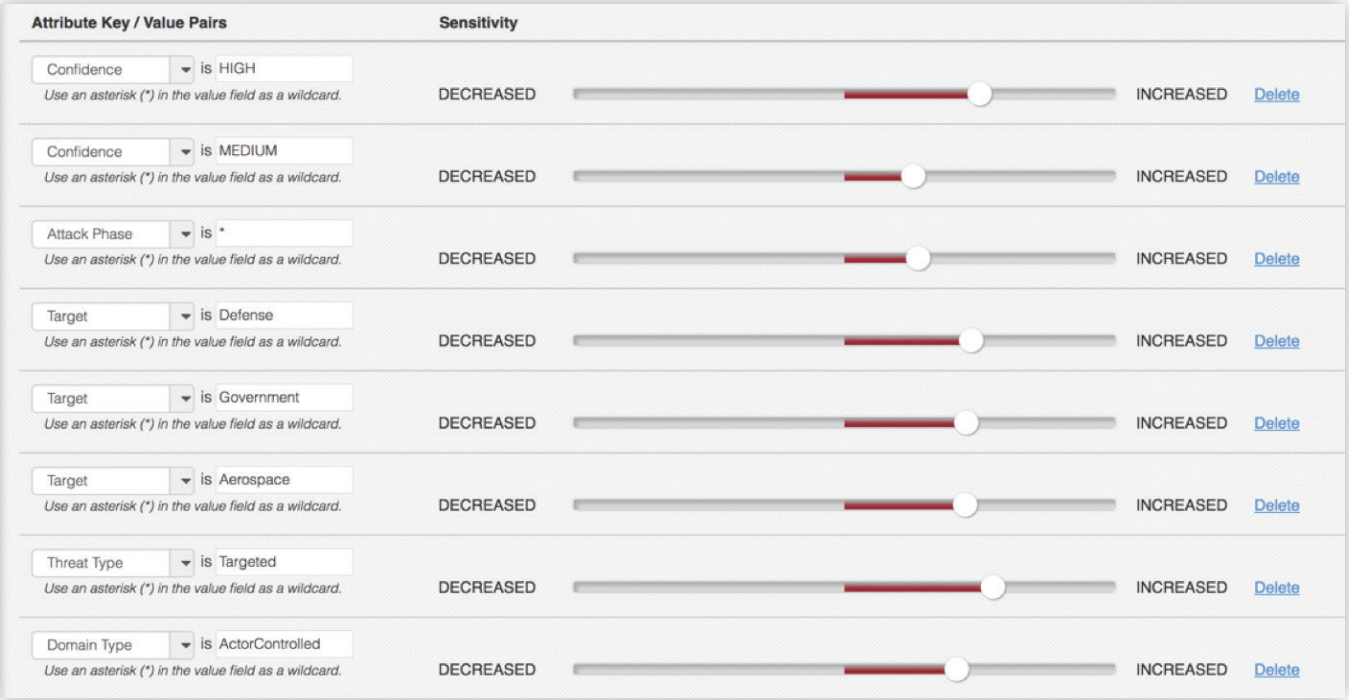


Figure 2. Exemple de conditions définies par le client pour l'attribution de scores.

Afin d'assurer une protection optimale contre les menaces, les équipes déploient les renseignements pertinents toutes les heures, pour être en phase avec la plupart des fournisseurs de Threat Intelligence. Le retour sur investissement en équivalents temps plein lié au sensor grid ne dépend pas du volume de renseignements, mais plutôt de la perturbation régulière du workflow des ingénieurs. Habituellement, celle-ci survient toutes les heures : un ou plusieurs ingénieurs réseau doivent interrompre leurs activités, se connecter à CHAQUE technologie basée sur des sondes (pare-feu, routeur, messagerie électronique, proxy web, DNS, endpoint, etc.), charger les dernières informations reçues et contrôler leur qualité, puis retourner à son travail. L'automatisation du déploiement des renseignements sur les menaces pour qu'ils puissent être exploités par les sondes renforce les défenses de manière impressionnante, tout en allégeant la charge de travail de l'équipe responsable du réseau/de l'infrastructure, qui peut ainsi se concentrer sur ses priorités.

Comme mentionné précédemment, la capacité de ThreatQ à appliquer l'algorithme d'attribution de scores défini par le client joue un rôle décisif dans la sélection des données de Threat Intelligence exportées. SMARTY, le puissant langage de requête d'exportation de ThreatQ, offre des possibilités pratiquement illimitées, qui permettent aux clients d'exporter exactement les données dont ils ont besoin. Les utilisateurs peuvent non seulement définir QUELLES informations ils souhaitent exporter vers le sensor grid, mais également préciser le format de sortie de leur choix. Vous trouverez ci-dessous deux exemples d'exportations illustrant le niveau de complexité que ThreatQ permettra à votre équipe de traiter.

Exemple 1 : Export IOCs associated with *kit_d'exploit* OR *famille_de_logiciels_malveillants* OR *nom_d'adversaire* AND with a ThreatScore >= 65 to ALL BLOCKING TECHNOLOGIES

Cet exemple est une exportation client standard qui déploie les renseignements dont le niveau de risque est élevé et associés à un kit d'exploit, une famille de logiciels malveillants ou un adversaire précis. L'exportation est exécutée toutes les heures afin de garantir que les dernières connaissances recueillies en interne et issues de sources externes sont distribuées aux technologies de blocage de l'infrastructure de sécurité.

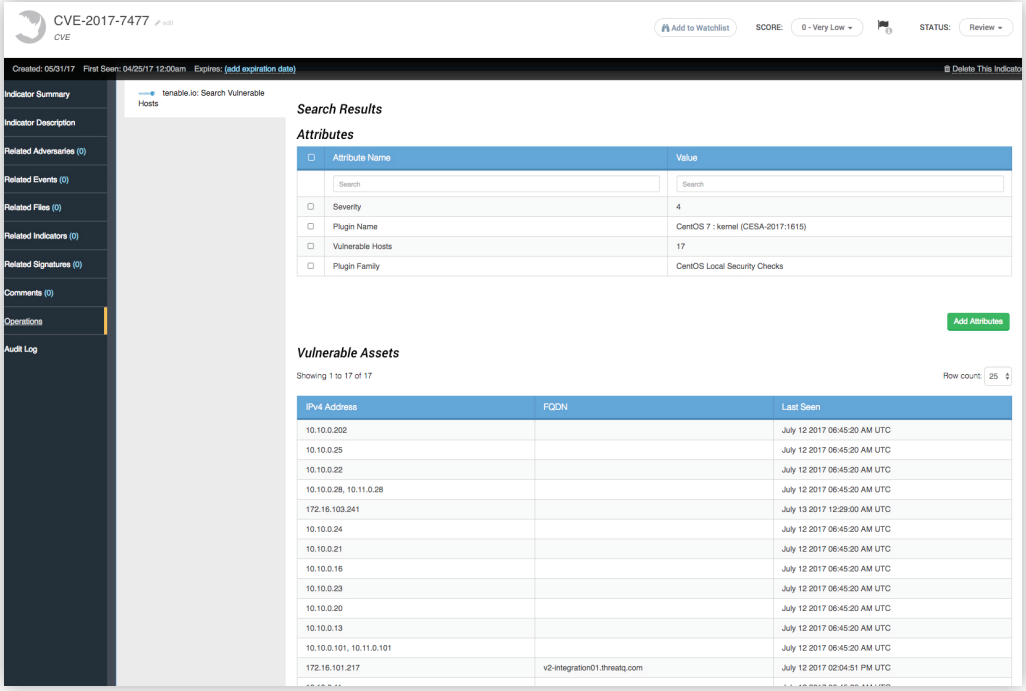
Exemple 2 : Export IOCs associated with CVE-2017-7477 AND where vulnerable_host_systems > 1 to ALL BLOCKING TECHNOLOGIES

Cet exemple démontre la capacité de ThreatQ à recouper la Threat Intelligence avec les données internes d'une entreprise relatives aux vulnérabilités afin de déterminer les niveaux de risque. Cette exportation regroupe uniquement les indicateurs de compromission associés à CVE-2017-7477 si, et seulement si, au moins un des hôtes de l'entreprise est vulnérable. Cette alliance de la gestion des vulnérabilités et du renseignement sur les menaces, telle qu'illustrée à la figure 3, représente la voie d'avenir pour aider les entreprises à harmoniser les défenses entre leurs différents départements.

DÉLAI DE DÉTECTION OU DÉLAI D'INTERVENTION : DÉCOUVREZ CE QUE VOUS IGNOREZ... PLUS RAPIDEMENT

ThreatQ offre des fonctions de personnalisation de l'attribution de scores et de priorisation, d'optimisation automatique de sa bibliothèque Threat Library™ et de déploiement automatique des renseignements pertinents sur les technologies de protection de l'entreprise. Il permet ainsi aux analystes de récupérer du temps de travail. En outre, la plate-forme est capable de limiter la durée d'implantation des adversaires, offrant ainsi un retour sur investissement qui représente trois à quatre équivalents temps plein. Le secteur est désormais conscient que les intrusions sont inéluctables.

Figure 3. Capture d'écran de CVE-2017-7477 avec attributs associés et liste des hôtes vulnérables.



L'objectif est dès lors de réduire les délais d'intervention. Selon un récent rapport du SANS Institute rédigé par Matt Bromiley et intitulé « The 2016 SANS Incident Response Survey[3] » (Enquête 2016 du SANS Institute sur la réponse à incidents), 21 % des participants à l'enquête ont indiqué que la durée d'implantation des adversaires dans l'environnement d'entreprise était de 2 à 7 jours avant la détection et qu'il fallait encore 2 à 7 jours avant la mise en œuvre de mesures correctives. En d'autres termes, les intrus peuvent vaquer à leurs activités pendant près de deux semaines : déplacement latéral dans l'environnement, escalade de privilèges, exfiltration de données et d'informations d'identification, préparation de la prise en otage de données contre rançon ou tout simplement déploiement de portes dérobées dormantes à exploiter par la suite.

Le retour sur investissement lié aux délais de détection et d'intervention provient essentiellement du temps nécessaire aux analystes pour effectuer des recherches dans les référentiels de journaux afin d'y trouver les données de Threat Intelligence auxquels l'algorithme d'attribution de scores a affecté un niveau de menace/de risque élevé. Les référentiels de journaux sont d'immenses lacs de données (data lakes), et il arrive souvent que les recherches rétrospectives allant au-delà des fonctionnalités de corrélation tactique à court terme nécessitent un temps considérable, d'autant que plus il faut remonter loin, plus les recherches sont longues. Les meilleures pratiques du secteur en matière de recherche rétrospective préconisent un délai de précaution raisonnable d'au moins 30 à 45 jours afin de pouvoir identifier les éventuelles tentatives d'attaque antérieures, qu'elles aient abouti ou aient été contrées. L'estimation du retour sur investissement repose sur l'exécution de requêtes de recherche approfondie sur 50 alertes, soit un taux de réussite de 10 % sur les 500 indicateurs avec niveau de risque élevé identifiés chaque jour.

Les fonctions de réduction des délais de détection et d'intervention qui permettent à ThreatQ d'offrir un retour sur investissement substantiel procurent également les avantages suivants :

- Compréhension optimale de la situation
- Intégration bidirectionnelle maximale avec les outils de base
- Exploitation des fonctions d'opérationnalisation de ThreatQ pour renforcer l'automatisation

COMPRÉHENSION DE LA SITUATION

La connaissance de la situation représente l'ensemble du contexte d'un indicateur ou d'un renseignement. Les indicateurs étant des informations essentiellement arbitraires, c'est leur contexte qui permet à l'analyste ou à l'équipe de réponse à incidents de déterminer la conduite à tenir. Plus le contexte d'un élément de renseignement donné est complet, plus la décision peut être prise rapidement. Auparavant, lorsque l'alerte était déclenchée dans la solution SIEM, l'analyste ouvrait immédiatement plusieurs navigateurs web et entamait des recherches sur l'indicateur. Cela prenait beaucoup de temps du fait qu'il devait cliquer sur les différents écrans pour résumer intuitivement les données sur la menace. Avec ThreatQ, c'est de l'histoire ancienne. En effet, la plate-forme centralise le contexte et l'intègre dans la solution SIEM pour offrir aux analystes une compréhension immédiate de la situation. Au moment où l'alerte est déclenchée, ceux-ci ont déjà à disposition toutes les informations contextuelles supplémentaires ou même des rapports de Threat Intelligence spécifiques. Ils gagnent ainsi de 5 à 10 minutes de recherche par indicateur/événement.

INTÉGRATION BIDIRECTIONNELLE

En général, les renseignements sur les menaces sont distribués « après les faits ». Autrement dit, c'est après l'intrusion que les équipes mettent en œuvre les mesures de blocage. Pour réduire les risques à ce stade, vous devez être à même de revenir sur vos données de journaux antérieures et d'y appliquer également les renseignements récents. Pourquoi ? Parce qu'une fois infiltrés dans l'entreprise, les adversaires se tournent vers la « nouvelle » infrastructure de commande et de contrôle

3 https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047

ou se déplacent latéralement au sein de l'environnement pour limiter la probabilité d'être détectés. Cela complique encore davantage l'identification du patient zéro. Conscients du fait que les recherches rétrospectives trop longues peuvent avoir un impact opérationnel négatif sur les technologies des clients, plusieurs fournisseurs commerciaux de flux de données Threat Intelligence incluent pour chaque indicateur un attribut de type « Observé pour la dernière fois ». C'est extrêmement utile pour les entreprises qui collectent de gros volumes de renseignements internes et externes dans la mesure où elles peuvent désormais effectuer des recherches très ciblées dans leurs référentiels de journaux. Dans l'exemple ci-dessous, nous allons utiliser la date « Observé pour la dernière fois » (attribut last_seen) d'un flux et créer une opération qui tient compte de cette date et effectue une recherche sur « +/- 5 jours ». Le critère « + et - 5 jours » est arbitraire et peut être défini par l'utilisateur, mais il est censé offrir une marge de manœuvre pour identifier la campagne d'attaque tout en réduisant la charge imposée à des technologies déjà lourdement sollicitées. Cette opération de recherche s'avère encore plus cruciale si la date « Observé pour la dernière fois » se trouve en dehors de la plage conservée en mémoire par la solution SIEM/le référentiel de journaux.

```
Function search(indicator)
    if indicator.last_seen:
        last_seen = indicator.last_seen
        last_seen_range = last seen - 5 + " - " + last_seen + 5
    else:
        last_seen_range = now() - "30d"
    results = search_siem(indicator,last_seen_range)
    return results
```

FONCTIONS D'OPÉRATIONNALISATION DE THREATQ

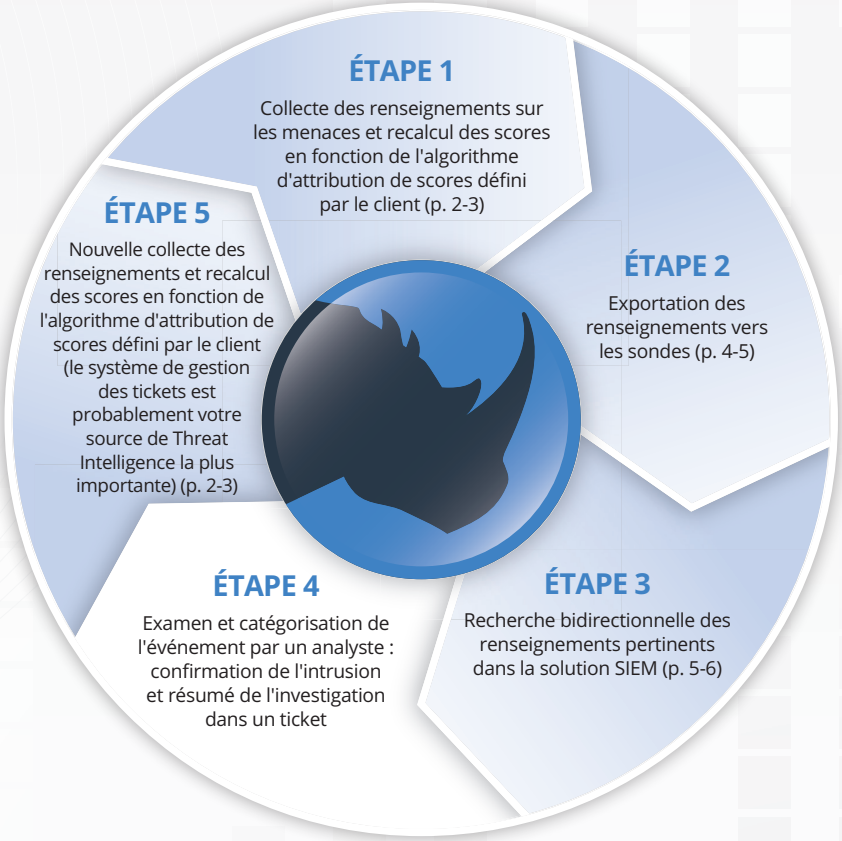
L'utilisation du module d'opérationnalisation (Operations) de ThreatQ via la fonctionnalité de SDK/d'API permet de bénéficier d'un retour sur investissement appréciable. Les meilleures pratiques préconisent que les entreprises traitent les renseignements provenant d'un environnement sandbox et/ou d'un système de gestion des tickets différemment de ceux collectés auprès d'entités externes. Ce traitement distinct tient principalement au fait que les connaissances liées à une attaque active ou directe nécessitent une recherche rétrospective plus longue pour identifier les infections ou tentatives d'infection antérieures. Pourquoi n'est-il pas possible d'appliquer un tel traitement à tous les renseignements sur les menaces ? Bien souvent, leur volume et la durée de la recherche sont

CE QU'IL FAUT RETENIR

Tout au long de ce livre blanc, nous avons exploré plusieurs scénarios de gestion avancée et de base des données de Threat Intelligence à l'aide de ThreatQ. Cette vue d'ensemble démontre les avantages incontestables de la plate-forme en termes de retour sur investissement.

Deux éléments essentiels doivent être soulignés dans ces exemples :

1) D'une part, ThreatQ exécute quatre des cinq étapes automatiquement, sans intervention des analystes, ce qui procure un gain de temps et d'énergie considérable.
2) D'autre part, ces étapes sont cycliques et itératives, quels que soient les compétences, les ressources, le budget ou les capacités de l'équipe. Cela prouve que ThreatQ offre également une valeur ajoutée au niveau des procédures opérationnelles récurrentes, qu'il renforce en ajustant automatiquement sa bibliothèque à optimisation automatique. Si, par exemple, lors de l'examen d'un événement, l'analyste l'a considéré comme un faux positif, ThreatQ peut appliquer un score négatif au renseignement correspondant, de sorte qu'à l'avenir, ce dernier soit automatiquement classé dans une catégorie de risque moindre pour l'entreprise.



tels que cette approche mettrait probablement à genoux votre solution SIEM ou référentiel de journaux, ou entraînerait une perte de paquets. En automatisant toute une série de tâches habituellement manuelles, chronophages et répétitives via l'accès à l'API RESTful de ThreatQ, les clients peuvent gagner un temps considérable et augmenter davantage leur retour sur investissement.

CONCLUSION

ThreatQ offre de nombreux avantages aux équipes de Threat Intelligence de toutes tailles : configuration définie par le client pour l'attribution de scores aux renseignements sur les menaces, déploiement rapide des données pertinentes vers le sensor grid existant et workflows dédiés à la réduction des délais de détection et d'intervention. En déployant ThreatQ pour structurer la Threat Intelligence et exécuter les workflows de base, les entreprises peuvent enregistrer un gain de productivité analytique qui équivaut à celle de six à neuf analystes de SOC employés à temps plein. Automatisation du cycle de gestion des indicateurs, exportation des renseignements sur les menaces à haut risque vers les technologies de blocage et de détection, et accélération notable de la réponse à incidents : grâce à ces atouts, la plate-forme permet de mieux gérer les risques et de faire évoluer les workflows des équipes, tout en fournissant des indicateurs clés de performances (KPI) très prisés des équipes de direction.

Vous cherchez à optimiser vos processus actuels et à mieux gérer les données sur les menaces, sans être submergé par leur volume, tout en écartant les données parasites et faux positifs ? Vous voulez constituer une équipe mais ne disposez pas des ressources nécessaires ? Grâce à ThreatQ, vous pouvez en faire plus avec moins. Ses fonctions d'automatisation et de priorisation permettront aux membres de votre équipe d'être bien plus efficaces et performants. Faites le choix de ThreatQ pour votre entreprise : le retour sur investissement sera immédiat !

À PROPOS DE THREATQUOTIENT™

ThreatQuotient sait parfaitement qu'une sécurité axée sur les renseignements repose essentiellement sur les ressources humaines. Grâce à ThreatQ™, sa plate-forme de Threat Intelligence ouverte et extensible, les acteurs de la cybersécurité ont l'assurance que les renseignements sur les menaces pertinents sont utilisés par les bons outils, au moment opportun. Adoptée par de nombreuses entreprises de premier plan à travers le monde, elle est au cœur même de leur système de gestion et d'opérationnalisation du renseignement sur les menaces. L'ensemble de leur dispositif de sécurité gagne ainsi en performances et en efficacité.

Pour plus d'informations, consultez le site threatq.com.

TQ_ThreatQ-ROI-Whitepaper_Rev1

THREATQUOTIENT™
11400 Commerce Park Drive, Suite 200, Reston, VA 20191, États-Unis • ThreatQ.com
Sales@ThreatQ.com • Demandes de renseignements généraux et commerciaux : +1 703 574-9885