Liste de questions aux fournisseurs de plates-formes de Threat Intelligence

Une plate-forme de Threat Intelligence a pour but de permettre aux SOC (Security Operations Centers), aux analystes en Threat Intelligence ainsi qu'aux équipes de gestion des vulnérabilités, de gestion des risques et de réponse à incidents de réagir aux événements et alertes, mais également d'anticiper les menaces et de devenir plus proactifs. Pour ce faire, elle doit servir de référentiel central pour toutes les données sur les menaces issues de sources internes et externes, favorisant ainsi la collaboration, une prise de décision plus judicieuse, des mesures proactives et une réduction des délais de détection et d'intervention. Cette plate-forme doit être en mesure de vous aider à comprendre, prioriser et neutraliser les menaces les plus importantes pour votre entreprise.

La présente liste rassemble les questions les plus importantes à poser à tout fournisseur de plate-forme de Threat Intelligence avant de prendre une décision. Utilisez-la comme outil de référence rapide et téléchargez le guide de l'acheteur relatif aux plates-formes de Threat Intelligence pour obtenir des informations complémentaires.

Acquisition de données

De combien de feeds open source et commerciaux prêts à l'emploi disposez-vous ?

Les clients ont-ils la possibilité d'activer / de désactiver les feeds individuellement ?

Les clients ont-ils la possibilité d'activer / de désactiver les composants d'un feed (par ex., pour importer uniquement les renseignements d'un secteur d'activité donné) ?

Contexte

Les indicateurs de compromission générés ou définis par un client sont-ils partagés avec vos autres clients ?

Si un indicateur ressort plusieurs fois, chaque nouvelle apparition vient-elle annuler les précédentes ?

Puis-je définir des attributs personnalisés adaptés aux besoins de mon entreprise (adresses de comptes bitcoin, identifiants Twitter, code SWIFT, etc.) ?

Attribution de scores

Un client peut-il personnaliser l'attribution de scores en fonction de son entreprise, mais aussi de ses équipes, ressources et capacités sans que ces personnalisations soient partagées avec vos autres clients ?

Puis-je créer moi-même l'algorithme d'attribution de scores et ainsi choisir les informations sur lesquelles il sera basé ?

Prenez-vous en charge des scores négatifs ?

Puis-je contrôler les scores associés aux feeds ?

Expiration

Quelle est votre approche concernant les renseignements arrivant à expiration ?

Puis-je adapter la méthode d'expiration afin que celle-ci soit en accord avec mes attributions de scores personnalisées ainsi qu'avec les technologies de mon sensor grid ?

La plate-forme de Threat Intelligence peut-elle adapter automatiquement les dates d'expiration en fonction des paramètres que je définis ?

LISTE DE QUESTIONS AUX FOURNISSEURS DE PLATES-FORMES DE THREAT INTELLIGENCE

Mise en corrélation des données internes et externes

L'utilisation d'API pour l'intégration de données internes et externes engendre-t-elle un surcoût ?

En cas d'activation des données bidirectionnelles, jouissez-vous de droits de propriété sur les données de mon entreprise que vous stockez au sein de votre environnement ?

Dois-je ouvrir des ports supplémentaires sur mon pare-feu en vue des intégrations ?

Intégrations

L'utilisation d'API pour les intégrations engendre-t-elle un surcoût ?

Proposez-vous une intégration bidirectionnelle de toutes les solutions SIEM et de gestion des vulnérabilités, ainsi que de tous les systèmes de gestion des tickets ?

Quels autres outils avec intégration bidirectionnelle prenez-vous en charge ?

Dois-je recourir à des services professionnels pour la gestion de ces intégrations ?

Les informations issues des solutions SIEM sont-elles partagées avec des tiers ?

Notifications

Un analyste peut-il créer une liste d'alertes au sein de votre tableau de bord pour un objet quelconque du système ?

Les notifications d'alerte sont-elles envoyées via l'interface utilisateur, par e-mail ou via un autre client tiers (par ex., Slack, HipChat, flux RSS, etc.) ?

Exportation

La fonctionnalité d'exportation prend-elle en charge les formats de fichier prêts à l'emploi les plus courants (CSV, JSON, CIF, etc.) ?

Un analyste peut-il exporter tous les objets et données contextuelles souhaités ?

La fonction d'exportation utilise-t-elle un langage de script qui offre un contrôle complet sur le type et le format des données exportées ? Par exemple, est-il possible pour un analyste de définir les renseignements à exporter et de les extraire dans un format spécifique, le tout au sein d'une seule et unique interface utilisateur ?

Est-il possible pour un analyste de configurer plusieurs feeds d'exportation (par ex., pour chaque technologie de sonde ou emplacement géographique, ou encore à des fins de recherches exploratoires quotidiennes) ?

Partage et collaboration

La plate-forme de Threat Intelligence peut-elle faire office de console partagée pour l'ensemble des membres de l'équipe de sécurité ?

Puis-je intégrer la fonctionnalité collaborative dans mon workflow existant ? Si oui, comment ? Et cette intégration entraîne-t-elle un surcoût ?

Suis-je libre d'accepter ou de refuser le partage de mes données avec un fournisseur ou une communauté ?

Les données partagées sont-elles anonymisées ? Si oui, de quelle manière ?

En cas de partage des données, de quelle manière les utilisez-vous ?

En tant que fournisseur de la plate-forme de Threat Intelligence, jouissez-vous de droits de propriété sur les données qu'elle stocke ?

LISTE DE QUESTIONS AUX FOURNISSEURS DE PLATES-FORMES DE THREAT INTELLIGENCE

Options de déploiement

- Suis-je le seul et unique propriétaire de mes données ?
- Mes données sont-elles mélangées à celles d'autres clients au sein d'un environnement multilocataire ?
- À quelles fonctionnalités n'aurai-je pas accès si je ne déploie pas de serveur d'intégration sur site ?
- Si l'infrastructure du fournisseur de services de cloud bascule en mode hors ligne, quelles fonctionnalités deviennent inaccessibles ?
- Partagez-vous les rapports des tests d'intrusion trimestriels que vous faites faire par des tiers ?

Tarification

- Des frais s'appliquent-ils pour chaque API ou intégration au sein d'un système de défense ? Si oui, à combien s'élèvent-ils ?
- L'intégration de données ou d'indicateurs de compromission personnalisés est-elle payante ?
- À combien s'élève le coût total de possession compte tenu de mes exigences métier ?
- Le déploiement d'une instance de cloud privée entraîne-t-il un surcoût ?
- Le nombre de licences utilisateur est-il adaptable sans frais ?
- Existe-t-il une licence utilisateur illimitée ?
- Les services de sécurité managés (MSSP) sont-ils soumis à une tarification spéciale ?

Assistance

- L'assistance peut-elle être contactée par différents biais ?
- Quels sont les contrats de niveau de service proposés en ce qui concerne les tickets de support ?
- Comment puis-je mettre à jour les tickets de support ?
- Comment puis-je faire remonter un incident ?
- Comment les demandes de fonctionnalités sont-elles gérées et quel est leur délai de traitement ?
- Comment les rapports de bug sont-ils gérés et quel est le délai habituel de résolution des bugs ?
- Quelle est votre politique en matière d'autorisation de retour de marchandise (le cas échéant) ?

À PROPOS DE THREATQUOTIENT™

ThreatQuotient s'est donné pour mission d'améliorer l'efficacité des opérations de sécurité à l'aide d'une plate-forme entièrement axée sur les menaces. En intégrant les processus et technologies existants d'une entreprise dans une architecture de sécurité unique, ThreatQuotient accélère et simplifie les investigations et la collaboration, non seulement au sein des équipes mais également entre les outils. Grâce à l'automatisation, la priorisation et la visualisation, les solutions ThreatQuotient réduisent le bruit et mettent en évidence les menaces prioritaires afin de permettre aux ressources souvent limitées de se concentrer sur les événements à haut risque et de prendre des décisions avisées. ThreatQuotient est basé en Virginie du Nord, et possède des filiales chargées des opérations internationales en Europe et en Asie-Pacifique. Pour plus d'informations, consultez le site https://threatquotient.com.

TQ_Vendor-Question-List-for-TIPs_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