THREATQUOTIENT

FICHE TECHNIQUE

THREATQ DATA EXCHANGE

Comment la plate-forme ThreatQ et ThreatQ Data Exchange peuvent aider les entreprises à partager efficacement des données de Threat Intelligence ciblées et organisées

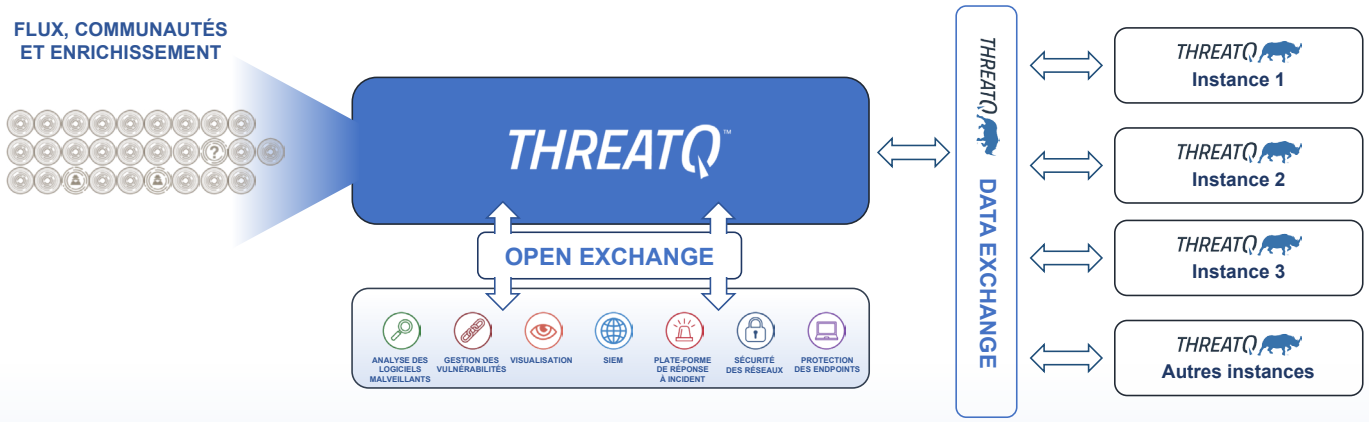
ThreatQ Data Exchange constitue le meilleur moyen de permettre et de gérer le partage de Threat Intelligence au sein d'une entreprise ou entre plusieurs entreprises de taille et de complexité variées. Cette solution facilite la configuration du partage bidirectionnel d'une partie ou de la totalité de vos données de Threat Intelligence au sein de la plate-forme ThreatQ, et vous permet de l'étendre à de nombreuses équipes et entreprises de toutes tailles.

Fondée sur le modèle de données flexible de ThreatQuotient et sur la prise en charge de normes ouvertes de partage de Threat Intelligence, la solution est conçue pour être personnalisée et favoriser la collaboration. Chaque équipe peut donc l'adapter en fonction de ses exigences et missions spécifiques, et ainsi partager avec ses partenaires les données qu'elle désire tout en préservant la confidentialité des informations de son choix.

Principaux atouts

- Interface utilisateur intuitive permettant d'établir facilement des connexions bidirectionnelles ou unidirectionnelles avec des systèmes externes
- Graphique topologique interactif représentant tous les systèmes connectés et garantissant une administration et une surveillance simples et évolutives
- Workflows d'installation simples avec bundles de configuration de connexions pour permettre l'ajout de plusieurs nœuds connectés de manière aisée et reproductible
- Journal d'activité complet indiquant l'état des connexions et fournissant des détails sur les données échangées à des fins de suivi et de génération de rapports

TRANSFERT DE DONNÉES À L'AIDE DE THREATQ DATA EXCHANGE



Qui peut tirer parti de ThreatQ Data Exchange ?

ThreatQ Data Exchange permet à n'importe quel réseau multiniveau de partage de Threat Intelligence offrant des fonctionnalités de contrôle et de surveillance à un administrateur général d'opérationnaliser la Threat Intelligence plus rapidement et plus facilement. En voici quelques exemples :

- Grands organismes publics avec plusieurs équipes et missions de Threat Intelligence qui collaborent et partagent des informations pertinentes en continu
- Fournisseurs de services de sécurité managés (MSSP) couvrant plusieurs secteurs ou régions géographiques
- Grandes et moyennes entreprises d'envergure mondiale ou divisées en plusieurs entités (multinationales, groupes, entités couvrant plusieurs régions géographiques et soumises à des exigences en matière de ségrégation des données de Threat Intelligence)

SCÉNARIO D'UTILISATION

Une entreprise gère ses opérations de sécurité depuis son siège. Compte tenu de la nature de ses activités, elle possède plusieurs filiales à travers le monde et a besoin de partager des données de Threat Intelligence organisées avec les équipes de sécurité de ces filiales. L'équipe de Threat Intelligence du siège est chargée de collecter, d'analyser et de prioriser les données pertinentes pour le secteur. Un sous-ensemble de ces informations doit être envoyé à chaque filiale afin de permettre une détection cohérente et de garantir une protection contre les risques de sécurité dans le monde entier.

Grâce à ThreatQ Data Exchange, l'équipe du siège peut configurer la plate-forme ThreatQ comme principale source de Threat Intelligence au sein de son environnement. Permettre aux entités de recevoir des données de cette source ne pose aucun problème. Il suffit à l'équipe du siège de générer un bundle de connexion sur la plate-forme ThreatQ principale et de l'exporter vers le nœud de chaque filiale. Une fois ces bundles en place, la communication peut avoir lieu.

Les analystes utilisant la plate-forme ThreatQ principale peuvent organiser les données de Threat Intelligence. Ainsi, lorsque les filiales reçoivent et utilisent les informations collectées, celles-ci sont pertinentes et priorisées pour leur environnement. L'équipe de Threat Intelligence du siège peut enregistrer la recherche afin qu'à chaque fois qu'elle crée un ensemble de données et le partage pour une utilisation locale, celui-ci soit déjà organisé en fonction des paramètres qu'elle a définis. Les ensembles de données ne se limitent pas à des indicateurs techniques. Ils peuvent inclure du contexte ainsi que des informations sur les logiciels malveillants, des campagnes spécifiques, ainsi que les motivations et les tactiques, techniques et procédures employées par les acteurs malveillants. L'activation des flux de transfert de données a permis d'organiser les informations de Threat Intelligence pour chaque filiale.

Un échange bidirectionnel

Il est également important que l'équipe de Threat Intelligence du siège puisse recueillir le feedback des filiales du monde entier concernant les renseignements diffusés. ThreatQ Data Exchange propose une intégration bidirectionnelle permettant de configurer la même couche de transport afin de permettre à chaque filiale de transmettre son feedback à l'équipe de Threat Intelligence du siège. Cette dernière sera ainsi mieux à même de comprendre le dispositif de sécurité de l'entreprise contre les menaces spécifiques dont elle assure le suivi, ainsi que d'identifier les tendances et les vulnérabilités potentielles.

Cette communication bidirectionnelle permet également de créer une mémoire globale et centralisée des menaces. À mesure que chaque filiale gère des incidents de sécurité, identifie de nouvelles menaces ou collecte des informations contextuelles supplémentaires sur des menaces connues, ces données peuvent être regroupées dans un référentiel central. La couche de transport peut être simplement configurée pour transmettre automatiquement toutes les données liées aux incidents ou créées localement à la plate-forme ThreatQ principale de manière à créer une source d'informations unique et fiable pouvant être partagée avec les équipes du monde entier.

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 technologies et les processus 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 dans le nord de la Virginie, et possède des filiales chargées des opérations internationales en Europe, en Asie-Pacifique et dans la région Moyen-Orient/Afrique du Nord. Pour plus d'informations, consultez le site **www.threatquotient.com**.

THREATQUOTIENT

Sales@ThreatQ.com • +1 703.574.9885