PARTAGE DE LA THREAT INTELLIGENCE

LES DÉFIS À RELEVER PAR LES ENTREPRISES

La gestion de la Threat Intelligence expose les entreprises à des difficultés pour protéger les opérations internes sensibles tout en mettant en place la collaboration requise avec les partenaires externes. Les entreprises doivent conserver la souveraineté sur leurs données en veillant à ce qu'elles soient possédées, contrôlées et hébergées dans une instance privée dont le fonctionnement est autonome et confidentiel. Mais elles ont également besoin d'une plate-forme assurant un accès contrôlé à ces renseignements par des entités externes, comme les opérations fédérées et les réseaux de distributeurs, afin que cette collaboration ne compromette pas la sécurité.

La complexité de la cybersécurité moderne nécessite la prise en charge de différents modèles de partage, allant des échanges entre machines supportant plusieurs langages et formats, notamment STIX, à la distribution de données lisibles par l'utilisateur. L'accès à des tableaux de bord personnalisés, à des rapports complets et à des outils analytiques sophistiqués est indispensable à l'exploitation de ces renseignements.

La plate-forme doit également s'adapter aux niveaux de maturité variables des équipes externes pour leur permettre d'utiliser ces renseignements et d'y accéder quelle que soit leur expertise. Elle doit également s'intégrer harmonieusement aux différentes infrastructures et architectures afin de favoriser une approche polyvalente et inclusive du partage de la Threat Intelligence au sein de l'écosystème de cybersécurité.

Protection fiable, flexible et collaborative avec ThreatQ

La plate-forme de Threat Intelligence ThreatQ est une solution de pointe pour permettre et gérer le partage d'informations au sein d'une entreprise ou entre plusieurs entreprises de taille et de complexité variées. Combinant un modèle de données flexible et la prise en charge de normes ouvertes de partage de Threat Intelligence, la plate-forme a été élaborée pour garantir une personnalisation et une coopération harmonieuse. Elle permet non seulement d'appliquer mais aussi d'améliorer les mesures de cybersécurité de diverses entreprises, facilitant ainsi une collaboration interne et externe fiable et efficace.

ThreatQ est indépendant de tout fournisseur et assure ainsi une intégration bidirectionnelle avec un large éventail de technologies et de niveaux de maturité opérationnelle, ce qui permet aux équipes de partager largement des renseignements sur les menaces sans risque d'exposition de données sensibles. ThreatQ assure l'autonomie des équipes tout en mettant en place un large réseau de sécurité collaborative.

Principaux atouts du partage avec ThreatQ

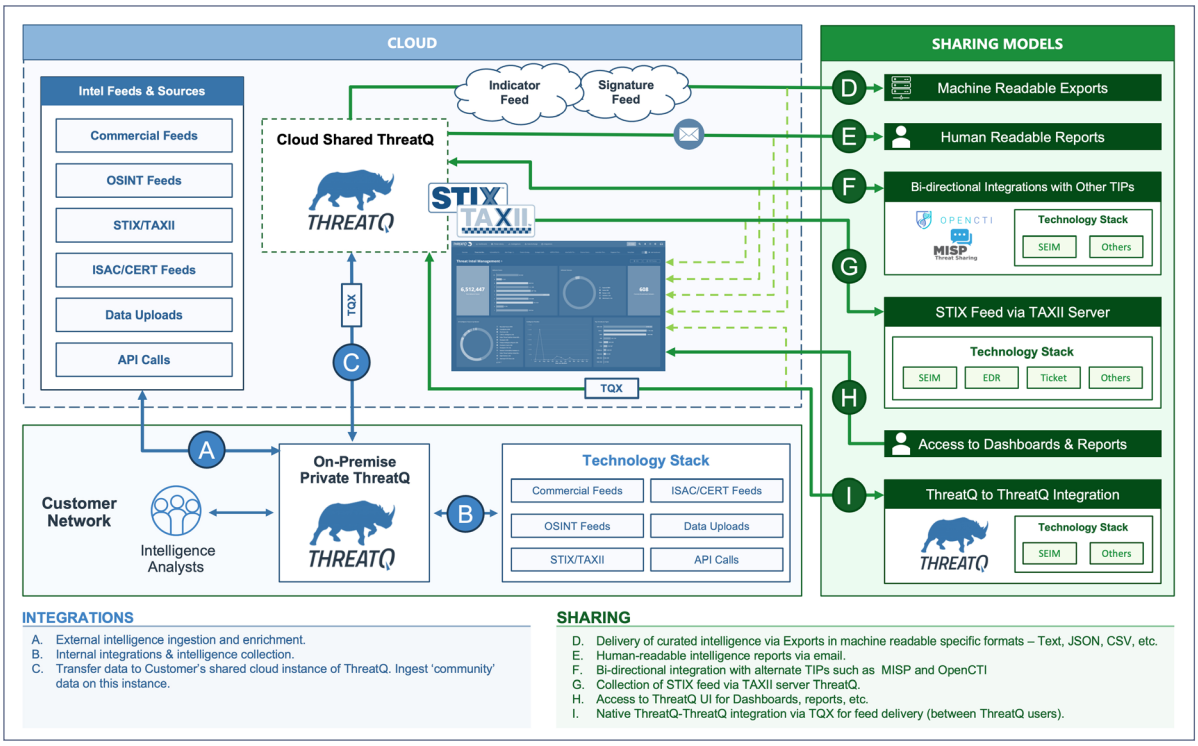
1. Plate-forme agnostique : la plate-forme d'échange ouvert ThreatQ prend en charge l'intégration avec un large éventail de technologies, favorisant la collaboration sans restriction.

2. Environnements isolés : ThreatQ assure la séparation physique du partage de Threat Intelligence interne et externe, garantissant une confidentialité et une intégrité des données équivalentes au sein d'instances distinctes.

3. Flexibilité de déploiement : les clients peuvent adopter des solutions sur site, hébergées dans le cloud d'AWS ou d'un autre fournisseur cloud et garder la main sur leur stratégie de déploiement.

Exemple de déploiement

Une entreprise de premier plan du secteur des services financiers a utilisé l'architecture collaborative de ThreatQ pour conserver une plate-forme sur site pour ses opérations internes et utiliser une plate-forme hébergée dans le cloud pour la collaboration avec des établissements financiers externes. Comme illustré sur le schéma ci-dessous, la plate-forme sur site s'intègre directement à l'infrastructure de sécurité de l'entreprise, permettant la collecte de flux de Threat Intelligence sans manipulation intermédiaire. L'instance cloud, hébergée éventuellement sur AWS, sert de plate-forme de communauté et permet à l'entreprise de partager en toute sécurité avec ses pairs les renseignements sur les menaces. Cette flexibilité de déploiement est la preuve de l'engagement de ThreatQ en matière de sécurité, d'indépendance opérationnelle et de stratégies de défense collaborative.



Avantages pour les clients ThreatQ :

- Grandes entreprises ayant des filiales : la plate-forme ThreatQ permet un contrôle centralisé de la Threat Intelligence tout en prenant en charge des opérations autonomes dans différentes entités ou emplacements géographiques.
- MSSP : les fournisseurs de services peuvent gérer la Threat Intelligence de plusieurs clients tout en maintenant une séparation stricte des données et en fournissant une Threat Intelligence personnalisée sous forme de service à valeur ajoutée.
- ISAC : les ISAC (Information Sharing and Analysis Centers) peuvent utiliser la technologie d'échange sécurisé de ThreatQ pour distribuer les renseignements sur les menaces au sein de leur réseau afin de renforcer la défense collective.

ThreatQuotient améliore les opérations de sécurité en regroupant des sources de données, des outils et des équipes hétérogènes afin d'accélérer la détection des menaces et la réponse à incident. La plate-forme de Threat Intelligence orientée sur les données de ThreatQuotient permet aux équipes de prioriser les menaces, d'automatiser les tâches et de collaborer pour résoudre les incidents de sécurité. Elle permet une prise de décision plus ciblée et optimise les ressources limitées en intégrant les processus et technologies existants à un espace de travail unifié. Résultat : une réduction des informations parasites, des menaces prioritaires claires et la possibilité d'automatiser les processus avec des données extrêmement fiables. Les fonctionnalités de pointe en matière de gestion, orchestration et automatisation des données de ThreatQuotient prennent en charge de nombreux scénarios d'utilisation, notamment la réponse à incident, le Threat Hunting, la lutte contre le spear phishing, le tri des alertes et la priorisation des vulnérabilités. Par ailleurs, elles peuvent également servir de plate-forme de Threat Intelligence. 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, Inc.
Sales@ThreatQ.com • + 1 703.574.9885