THREATQUOTIENT™

Une société de services financiers fait appel à ThreatQ™ pour accélérer les opérations de sécurité

Une société de services financiers internationale établie aux États-Unis s'est fixé pour mission d'aider ses clients à gérer les risques afin qu'ils puissent réaliser pleinement leur potentiel. Dans ce contexte, elle avait besoin d'un moyen d'exploiter ses ressources existantes de manière optimale pour mieux gérer ses propres risques.

DÉFI

Cette société de services financiers est abonnée à de nombreux flux de données sur les menaces issus de diverses sources. De plus, elle reçoit continuellement un volume croissant de données de journaux et d'événements en provenance de ses dispositifs de protection internes et de sa solution SIEM. Stockées à différents endroits, ces informations disparates étaient devenues difficiles à gérer. Comme leurs outils ne collaboraient pas, les analystes devaient basculer entre plusieurs portails pour visualiser les données, extraire manuellement celles qui semblaient pertinentes en fonction du groupe d'acteurs malveillants étudié, puis déterminer les mesures à prendre et la façon de les mettre en œuvre.

L'approche tactique adoptée consistait à mettre à jour les contrôles de sécurité internes en accord avec les données sur les indicateurs de compromission (IOC) et les informations contextualisées sur les menaces. Très fastidieuse, cette méthodologie était compliquée par le fait que l'équipe chargée des opérations de sécurité était en sous-effectif et que les équipes de Threat Intelligence et de réponse à incidents travaillaient de façon isolée. « Les analyses ad hoc et les actions étaient chronophages, désorganisées et inefficaces », explique l'ingénieur en sécurité de l'entreprise. « Quand nous ne gérions pas une situation de crise, nous réagissions à la nouvelle grande attaque à la une des journaux et nous répondions aux appels urgents de la direction. »

> *« Les données des indicateurs de compromission issues de sources fiables sont désormais envoyées de manière proactive aux listes de surveillance de détection qu'utilisent divers contrôles de sécurité internes, sans que le personnel de l'équipe ne doive assurer une surveillance quotidienne. « Qui plus est, comme nous exportons de façon sélective les données vers l'outil spécifiquement conçu pour les utiliser, nous ne transmettons pas de gros volumes de données sur le réseau et nous ne ralentissons donc pas les opérations. »*
>
> *— Directeur de l'équipe Réponse aux menaces*

EN BREF

SECTEUR D'ACTIVITÉ

Services financiers

DÉFI

Les données sur les menaces étaient disparates et stockées à des endroits différents. Les analyses ad hoc et les actions effectuées par des équipes isolées étaient chronophages, désorganisées et inefficaces.

SOLUTION

La plate-forme de Threat Intelligence ThreatQ permet aux équipes et aux technologies de collaborer efficacement pour détecter les menaces pertinentes et prioritaires et réduire les délais d'intervention, notamment la mise à jour automatique des contrôles de sécurité.

RÉSULTAT

- Détection proactive des menaces et intervention dans les quelques heures ou jours suivants
- Utilisation plus efficace des ressources existantes sans refonte nécessaire
- Démonstration de l'impact métier et du retour sur investissement des opérations de sécurité

SOLUTION

La société s'est mise en quête d'une plate-forme de Threat Intelligence qui lui permettrait de regrouper en un seul endroit à la fois tous les événements et toutes les données externes et internes sur les menaces, afin de mieux évaluer les risques et prendre les mesures nécessaires. En fait, elle avait besoin d'un moyen d'utiliser les données de Threat Intelligence pour les opérations de sécurité par le biais d'un point de contrôle unique.

L'équipe chargée des opérations de sécurité avait défini le cahier des charges suivant :

- La plate-forme de Threat Intelligence devait être installée sur site pour que l'équipe puisse exercer un contrôle complet sur ses données et leur sécurité.
- Elle devait prendre en charge les flux de données existants et futurs, et permettre la personnalisation. Au cours de ses recherches, l'équipe d'évaluation a constaté que certains fournisseurs intégraient des flux de données impossibles à désactiver, qui ne font que créer du bruit supplémentaire s'ils ne sont pas pertinents pour votre environnement.
- La plate-forme de Threat Intelligence devait permettre d'appliquer automatiquement le contexte métier aux données externes entrantes et pouvoir générer des données pertinentes pour les problèmes urgents auxquels l'équipe était confrontée, afin qu'elle puisse les prioriser et concentrer ses efforts sur les problèmes les plus importants.
- Elle devait également offrir une gestion centralisée et un contrôle sur la distribution automatisée des données aux contrôles de sécurité internes.

Après avoir déterminé qu'elle répondait à toutes ces exigences, l'entreprise a opté pour la plate-forme de Threat Intelligence ThreatQ. ThreatQ est mis à jour en permanence avec des données mondiales sur les menaces issues des flux déjà utilisés par l'entreprise, et enrichi avec les données internes sur les menaces, les événements et les incidents pour permettre la contextualisation. Grâce à la possibilité d'évaluer et de filtrer les données sur les menaces en fonction des paramètres définis par l'entreprise, les données de Threat Intelligence sont priorisées et repriorisées en permanence. Tous les membres de l'équipe de sécurité, même sans compétences techniques pointues, peuvent accéder aux données de Threat Intelligence pertinentes nécessaires pour leur travail et continuer d'utiliser les outils de sécurité qu'ils connaissent déjà et dans lesquels ils ont confiance. ThreatQ prend également en charge l'intégration bidirectionnelle pour permettre l'importation des données sur les menaces et les événements dans la plate-forme de Threat Intelligence à partir de la solution SIEM, du système de gestion des tickets et d'autres outils de sécurité. Objectif : ajouter du contexte et améliorer la pertinence des données mondiales sur les menaces. Les données de Threat Intelligence peuvent également être exportées vers la solution SIEM et les différents niveaux de défense dans le cadre des workflows et processus existants afin de renforcer la protection.

« Les données des indicateurs de compromission issues de sources fiables sont désormais envoyées de manière proactive aux listes de surveillance de détection qu'utilisent divers contrôles de sécurité internes, sans que le personnel de l'équipe ne doive assurer une surveillance quotidienne », explique le Directeur de l'équipe Réponse aux menaces de l'entreprise. « Qui plus est, comme nous exportons les données de façon sélective vers l'outil spécifiquement conçu pour les utiliser, nous ne transmettons pas de gros volumes de données sur le réseau et nous ne ralentissons donc pas les opérations. »

RÉSULTAT

Selon le *2017 Verizon Data Breach Investigations Report*, les délais de découverte et de confinement continuent d'atteindre plusieurs mois. Grâce à la plate-forme ThreatQ, les équipes de sécurité de cette société de services financiers, mais aussi leurs outils, peuvent collaborer afin de détecter les incidents spécifiques et de prendre les mesures nécessaires en seulement quelques heures ou quelques jours. « ThreatQ offre une meilleure visibilité sur la nature des activités susceptibles d'affecter les réseaux ou les ressources de l'entreprise. La solution intègre les données des indicateurs de compromission fiables dans les contrôles de sécurité internes en temps quasi réel. Cela nous permet d'être plus proactifs et d'agir en toute confiance », explique le Directeur de l'équipe Réponse aux menaces.

ThreatQ répond aux besoins de contrôle et de personnalisation de l'équipe de sécurité, lui permettant ainsi d'optimiser l'utilisation des ressources dont elle dispose déjà et d'accélérer ses opérations de sécurité. L'installation sur site lui permet de conserver la propriété de ses données et de contrôler le partage des données. Extrêmement flexible et configurable grâce à des connecteurs personnalisés, cette plate-forme ouverte permet en outre à l'équipe de sécurité de travailler avec tous les processus, données et outils disponibles au sein de l'entreprise sans réorganisation de l'architecture.

Par ailleurs, l'équipe a constaté que ThreatQ devenait naturellement de plus en plus robuste au fil du temps. Les équipes de Threat Intelligence et de réponse à incidents utilisent ce référentiel centralisé pour conserver et partager leurs données et leur travail, ce qui permet à chacun de travailler plus efficacement. Comme ThreatQ peut appliquer des modèles de données personnalisés et que les outils ne sont plus isolés, les équipes disposent d'une traçabilité complète, depuis les indicateurs à l'impact métier jusqu'aux attributions. Cette caractéristique leur permet de démontrer un retour sur investissement accru de leurs opérations de sécurité. Tout comme elles le font pour leurs propres clients, elles gèrent mieux les risques et peuvent ainsi exploiter pleinement le potentiel de leur entreprise.

À PROPOS DE THREATQUOTIENT™

ThreatQuotient™ sait parfaitement qu'une sécurité axée sur les renseignements repose essentiellement sur les ressources humaines. ThreatQ™, notre plate-forme de Threat Intelligence ouverte et extensible, et ThreatQ Investigations, notre solution de gestion des situations de crise, fournissent aux équipes de sécurité le contexte, la personnalisation et la priorisation dont elles ont besoin pour prendre des décisions éclairées, accélérer la détection et la réponse à incidents, et favoriser la collaboration entre équipes. Adoptées par de nombreuses entreprises de premier plan à travers le monde, les solutions de ThreatQuotient sont au cœur même de leur système de gestion des menaces et de leurs opérations de sécurité.

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

Copyright © 2018, ThreatQuotient, Inc. Tous droits réservés.

TQ_ThreatQ-Financial-Services-Case-Study_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