THREATQUOTIENT

TÉMOIGNAGE CLIENT

Un éditeur de logiciels international se concentre sur 5 scénarios d'utilisation avec ThreatQ

Un éditeur de logiciels international basé aux États-Unis qui fournit des logiciels de sécurité, de virtualisation et d'infrastructure cloud avait besoin d'une plate-forme centralisée pour améliorer la surveillance de la sécurité et accélérer la détection et la réponse à incident.

Difficulté

Cet éditeur de logiciels international recherchait un moyen plus efficace d'exploiter ses multiples sources de Threat Intelligence pour comprendre et limiter les risques d'attaques. Lors de l'analyse des renseignements, l'équipe de sécurité passait énormément de temps à tenter de mettre en corrélation les menaces en circulation dans le monde avec les menaces qui nécessitaient d'être traquées et neutralisées dans l'environnement spécifique de l'entreprise. L'éditeur avait besoin d'un moyen simple et efficace d'identifier les groupes qui le visaient, les vulnérabilités à corriger en priorité en fonction de ces risques, et dans quelle mesure les attaques visant son écosystème de partenaires pouvaient mettre en danger ses clients, ses employés et son infrastructure.

- Collecte de données provenant de flux internes, open source et commerciaux
- Focalisation sur les menaces actives à rechercher dans l'environnement de l'entreprise
- Priorisation et gestion des vulnérabilités

« Nous avions besoin d'une plate-forme robuste qui permette à nos analystes en Threat Intelligence d'évaluer plus rapidement les menaces de cybersécurité visant l'entreprise et d'y répondre immédiatement, explique l'analyste en TI en chef. Comme notre équipe est réduite et dispersée à travers le monde afin d'assurer un suivi 24 h/24, l'automatisation et la collaboration étaient d'une importance cruciale. »

Solution

Le client avait besoin d'une plate-forme qui servirait de référentiel central pour toutes les données de Threat Intelligence et permettrait à l'équipe de travailler de façon efficace tout au long des cinq phases du cycle de gestion des renseignements : planification, collecte, traitement, enrichissement et diffusion.
Il avait défini le cahier des charges suivant :

- Agrégation des flux de leurs services de renseignements open source et commerciaux avec inclusion des rapports et des flux d'indicateurs
- Enrichissement des données avec possibilité d'établir des relations entre les indicateurs, et ajout des informations contextuelles provenant des systèmes internes
- Priorisation du traitement des menaces en fonction des tactiques, techniques et procédures (TTP) des cybercriminels, en corrélation avec les vulnérabilités et le profil de risque de l'entreprise
- Fonctionnalités de génération de rapports permettant aux analystes de générer rapidement des rapports finis et détaillés et ainsi de mieux faire comprendre aux dirigeants l'impact potentiel des menaces sur l'environnement de l'entreprise
- Bibliothèque regroupant l'ensemble des données externes et internes sur les menaces et les événements, rapports, résumés et notes d'information en un seul et même endroit, pour une source d'informations unique, fiable et consultable
- Fonctionnalités de collaboration pour travailler avec les équipes internes, et fonctionnalités de suivi et de coordination des activités pour faciliter les investigations et la génération de rapports
- Possibilité de partager les indicateurs et leur contexte avec des groupes externes en fonction des besoins

Après une évaluation approfondie de trois éditeurs de solutions, l'entreprise a choisi ThreatQ, estimant qu'il remplissait

PRÉSENTATION

SECTEUR : Entreprise technologique internationale

CLIENT DEPUIS : 2018

EFFECTIF : > 24 000

CHIFFRE D'AFFAIRES : > 8 milliards de dollars

LIEU : Siège social aux États-Unis

DIFFICULTÉ

Collecte et priorisation des données de Threat Intelligence utilisées pour le Threat Hunting, la gestion des menaces, l'investigation des attaques de spear phishing, la réponse à incident et la gestion des vulnérabilités.

SOLUTION

Grâce à l'automatisation et à la collaboration, la plate-forme ThreatQ permet aux analystes d'évaluer rapidement les menaces et d'y répondre immédiatement en collectant, corrélant, évaluant et diffusant les renseignements sur un éventail complet de sources et de technologies.

RÉSULTAT

- ✔ Efficacité accrue des équipes et des technologies
- ✔ Réduction des délais dans cinq scénarios d'utilisation prioritaires
- ✔ Rapports détaillés offrant aux dirigeants un suivi des mesures clés
- ✔ Retour sur investissement accru sur l'infrastructure de sécurité en place

www.threatquotient.com

parfaitement le cahier des charges. ThreatQ est actuellement utilisé pour répondre aux principaux scénarios d'utilisation de l'entreprise : gestion des menaces, Threat Hunting, investigation des attaques de spear phishing, réponse à incident et gestion des vulnérabilités. Grâce à la possibilité d'évaluer et de filtrer les données sur les menaces en fonction des paramètres définis par l'équipe d'analystes, celle-ci est en mesure de cerner les menaces qui ciblent l'environnement et peut ainsi gérer plus efficacement les menaces et prioriser les activités telles que la correction des vulnérabilités en fonction des risques posés. Les données de Threat Intelligence sont automatiquement actualisées à mesure que de nouvelles données et de nouveaux enseignements sont ajoutés à la plate-forme. Le regroupement des données sur les menaces, des preuves et des utilisateurs permet à tous les membres de l'équipe impliqués dans une investigation de travailler de concert, que ce soit pour bloquer les campagnes de spear phishing, traquer les menaces ou accélérer la réponse à incident. L'intégration de la collaboration dans le processus d'investigation garantit la coopération des équipes, qui peuvent alors intervenir plus rapidement et réduire plus efficacement les risques. La passation des tâches entre les analystes, les équipes et les fuseaux horaires est fluide, ce qui est important lorsque les membres d'une même équipe sont répartis dans différentes zones géographiques.

« Grâce à des intégrations prêtes à l'emploi à nos flux entrants et à des outils et contrôles de sécurité complémentaires, ThreatQ a pu prendre en charge nos processus de Threat Intelligence et d'investigation sans que nous soyons obligés de changer nos méthodes. L'ajout de l'automatisation et de la collaboration à des points clés du cycle de Threat Intelligence a fait passer nos capacités de surveillance, de détection et de réponse à incident au niveau supérieur. »

- Analyste en Threat Intelligence en chef

Résultat

Réduction des délais

L'automatisation de l'agrégation des données, de la corrélation, de la priorisation et de la diffusion des données de Threat Intelligence sur tous les systèmes et à toutes les équipes, alliée à la collaboration tout au long du processus d'investigation, permet à l'équipe d'accélérer la détection et la réponse à incident.

Modèles de rapports normalisés

ThreatQ permet de simplifier les rapports destinés aux dirigeants grâce à des modèles conçus pour mettre l'accent sur les mesures et les résultats dans des termes qui leur parlent.

Source d'informations unique et fiable

Toutes les données sont regroupées dans un référentiel central auquel les analystes peuvent intégrer les observations, les enseignements et la documentation relatifs aux investigations. Cela leur permet non seulement de préserver l'actualité et la pertinence des renseignements, mais aussi d'améliorer leur productivité et leur efficacité.

Prise en charge de cinq scénarios d'utilisation

L'équipe de sécurité utilise ThreatQ pour améliorer les opérations de sécurité dans cinq scénarios d'utilisation : gestion des menaces, investigation des attaques de spear phishing, Threat Hunting, réponse à incident et gestion des vulnérabilités.

Intégration de la technologie dans l'infrastructure pour un retour sur investissement accru

Grâce à un kit de développement logiciel (SDK) et des interfaces de programmation d'applications (API) faciles à utiliser, ThreatQ s'intègre entièrement aux technologies et outils existants du client pour augmenter et optimiser la valeur de ses investissements en matière de sécurité.

Adaptation de la plate-forme aux processus existants (et non l'inverse)

Les analystes peuvent accéder, au moyen de leurs outils habituels, aux renseignements dont ils ont besoin dans le cadre de leur workflow, et collaborer dans un environnement transparent qui leur permet de voir le travail des autres et d'accélérer leurs investigations.

À mesure que le client utilise ThreatQ, il renforce l'intégration avec des outils d'enrichissement et d'analyse supplémentaires au sein de son infrastructure de sécurité existante. Il augmente également ses capacités de Threat Hunting grâce à des fonctionnalités de Threat Hunting proactif, qui l'informent de l'existence d'une menace sur la base d'un rapport externe et lui permettent de rechercher les indicateurs associés dans son environnement. ThreatQ fournit au client le contexte dont il a besoin pour ne pas perdre de temps à traquer des menaces inexistantes. En outre, il lui offre des options de collaboration pour explorer tous les recoins de l'entreprise afin d'identifier les TTP des adversaires et les activités malveillantes et de mettre en œuvre des mesures correctives appropriées.

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, Inc.