THREATQUOTIENT

PRÉSENTATION PRODUIT

ThreatQ Investigations

Prendre les bonnes mesures, plus rapidement

Véritable salle de crise virtuelle de cybersécurité, ThreatQ™ Investigations est conçu pour une analyse collaborative des menaces, permettant une compréhension commune et une réaction coordonnée. Cette solution intègre la visualisation et la documentation dans un environnement unique partagé pour améliorer la compréhension et la hiérarchisation tout au long du processus d'analyse.

Elle offre une fenêtre unique sur le paysage chaotique des menaces, des incidents et des opérations où de multiples collaborateurs et équipes exécutent des tâches liées mais néanmoins séparées.

ThreatQ Investigations s'appuie sur la plate-forme ThreatQ et permet la collecte, l'apprentissage et le partage des connaissances. En résulte une représentation visuelle unique de l'investigation complète en cours (auteur, nature et chronologie) sur la base d'une compréhension commune de l'ensemble des composants de l'investigation (renseignements sur les menaces, preuves et utilisateurs).

Compte tenu de la dispersion des équipes de sécurité à travers le monde, il est de plus en plus difficile de collaborer et de coordonner les activités entre équipes et au sein des équipes d'une entreprise. ThreatQ Investigations optimise la collaboration tout en offrant aux membres des équipes la possibilité de mettre leur théorie à l'épreuve avant de la partager avec le groupe, afin de s'assurer de son exactitude et de sa pertinence. Les responsables d'équipes peuvent orienter les mesures, affecter des tâches et observer les résultats des actions menées en temps quasi réel.

ACCÉLÉRER LA COMPRÉHENSION

AMÉLIORER LA COLLABORATION

COORDONNER LES ACTIONS

Accélérer la compréhension

- Transfert instantané des connaissances
- Réduction des délais moyens de détection et d'intervention
- Investigation simultanée de plusieurs hypothèses

Améliorer la collaboration

- Renforcement de la sensibilisation entre les équipes et au sein de chacune d'elles
- Optimisation de la communication entre analystes, équipes de réponse à incident et direction
- Mise à l'épreuve des théories avant le partage avec le groupe pour s'assurer de leur exactitude et de leur pertinence

Coordonner les actions

- Identification de l'identité du collaborateur, de la tâche exécutée et de la chronologie
- Amélioration de la compréhension des mesures prises pendant une investigation
- Rationalisation des opérations de sécurité et amélioration de l'efficacité du processus

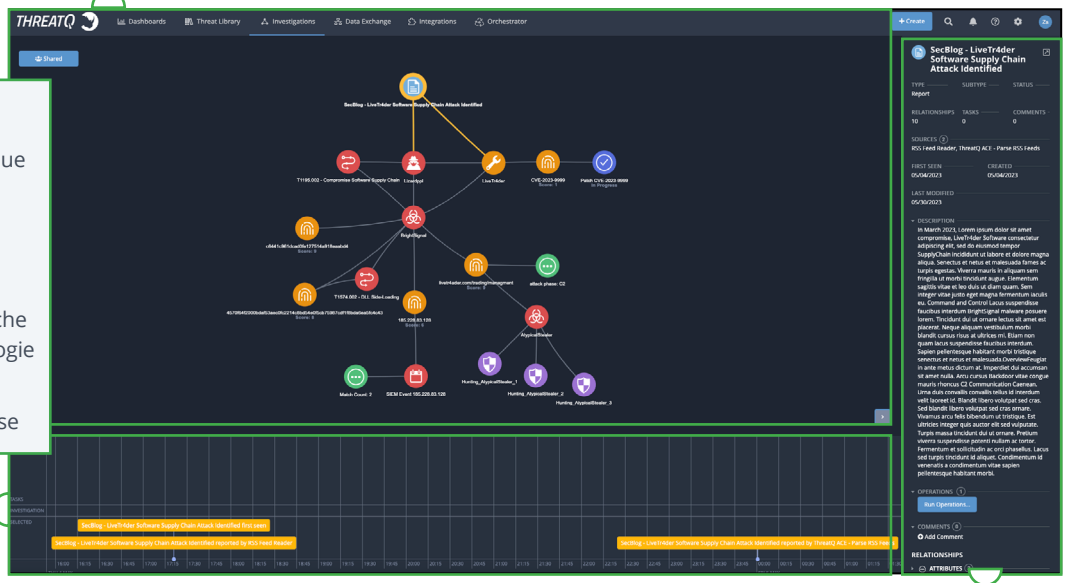
Fonctionnalités de ThreatQ Investigations

Tableau des preuves

- Regroupement des données sur les menaces, des éléments de preuve obtenus et des utilisateurs
- Investigation, analyse et compréhension plus rapides des menaces pour une mise à jour proactive du dispositif de sécurité
- Réduction des délais moyens de détection et d'intervention

Chronologie

- Présentation chronologique des activités liées aux incidents, cybercriminels et campagnes d'attaques
- Identification de l'identité du collaborateur, de la tâche exécutée et de la chronologie
- Compréhension du déroulement de la réponse



Fenêtre d'action

- Rationalisation de la réponse à incident et de l'investigation
- Identification de l'impact du travail d'autres collaborateurs sur le vôtre
- Contrôle accru des équipes chargées du traitement des incidents, de la recherche sur les malwares, des analystes du SOC et des responsables des investigations leur permettant de prendre les bonnes mesures au moment opportun

Scénarios d'utilisation de ThreatQ Investigations

Tri des alertes

Automatisation

Réponse à incident

Lutte contre le spear phishing

Threat Hunting

Gestion de la Threat Intelligence

Gestion des vulnérabilités

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 d'opérations de sécurité 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 dans 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 Sales@ThreatQ.com • + 1 703.574.9885