THREATQUOTIENT™

THREATQ™ — POUR LES ÉQUIPES DE RÉPONSE À INCIDENTS

L'équipe de réponse à incidents constitue le pilier sur lequel reposent les capacités de résolution des cyberincidents de l'équipe de sécurité informatique. Elle est aussi la dernière ligne de défense de l'entreprise. ThreatQ™ offre à ces experts un référentiel central qui combine les données sur les menaces issues de sources externes avec les événements et données générés au sein de l'entreprise, pour leur assurer à la fois contexte et pertinence. De plus, ThreatQ automatise la priorisation des données sur les menaces en fonction de paramètres définis par le client, éliminant ainsi les éléments parasites et la traque de menaces fictives. Avec ThreatQ, les menaces importantes, présentant un risque élevé, s'affichent dans une vue unique : votre équipe de réponse à incidents peut identifier l'origine des attaques et prendre les mesures qui s'imposent plus rapidement.

ThreatQ a été conçu pour doter vos équipes de réponse à incidents d'une plate-forme aux multiples fonctions et avantages :

- **Détection des menaces et interventions plus rapides**
- **Contextualisation et priorisation des menaces**
- **Optimisation de l'efficacité grâce aux recoupements entre investigations simultanées**
- **Interventions immédiates basées sur des outils, techniques et procédures définis**
- **Recoupement avec des investigations antérieures pour accélérer et éclairer la prise de décisions**
- **Automatisation de tâches exécutées manuellement auparavant**

Ces fonctions de base de la réponse à incidents sont indispensables pour détecter et désarmer les acteurs malveillants avant qu'ils n'occasionnent davantage de dommages à votre entreprise et à son infrastructure de sécurité.

THREATQ™

AVANTAGES DE THREATQ POUR LES ÉQUIPES DE RÉPONSE À INCIDENTS

AUTOMATISER LA PRIORISATION DES MENACES ET DES INCIDENTS DE SÉCURITÉ

DÉMARRER RAPIDEMENT LES INVESTIGATIONS POUR NEUTRALISER LES ACTEURS MALVEILLANTS

DIFFUSER AUTOMATIQUEMENT LES RENSEIGNEMENTS PERTINENTS VERS LES OUTILS DE DÉTECTION ET DE RÉPONSE À INCIDENTS

COMMENT LES ÉQUIPES DE RÉPONSE À INCIDENTS UTILISENT-ELLES THREATQ ?

Le contexte, la priorisation et l'automatisation offerts par ThreatQ permettent aux équipes de réponse à incidents d'améliorer leur compréhension de la situation, de prendre des décisions plus avisées et d'intervenir plus rapidement. ThreatQ simplifie la réponse à incidents de plusieurs façons :

- Bibliothèque sur les menaces qui s'optimise automatiquement pour déterminer leur pertinence et leur niveau de priorité
- Données contextuelles et pertinentes qui accélèrent l'analyse et l'intervention
- Centralisation du stockage des données sur les menaces et de l'historique des indicateurs, pour un traitement et des recherches rapides
- Création et gestion de dossiers sur les hackers
- Collecte et gestion de signatures pour une mise en œuvre simplifiée des actions
- Application simplifiée de délais d'expiration pour écarter les indicateurs obsolètes, de façon à améliorer la priorisation des menaces et mieux cibler les priorités
- Diffusion automatique des renseignements basés sur des données internes et externes vers les outils de détection et de réponse à incidents
- Application des enseignements tirés pour redéfinir continuellement les priorités des données sur les menaces et accélérer les futures opérations de réponse à incidents

COMMENT THREATQ RATIONALISE-T-IL LES TÂCHES DE L'ÉQUIPE DE RÉPONSE À INCIDENTS ?

ThreatQ a été conçu pour automatiser les tâches courantes liées à la priorisation, l'enrichissement et la recherche des données de Threat Intelligence et des indicateurs de compromission. La solution allège la charge opérationnelle et permet aux équipes de réponse à incidents de réagir de manière plus rapide et efficace. Avec ThreatQ :

- Une source unique et fiable centralise toutes les informations.
- Les données sur les menaces et leur contexte sont rapidement accessibles.
- Les menaces et les incidents de sécurité sont priorisés automatiquement.
- L'analyse porte uniquement sur les incidents importants ; plus besoin de passer au crible les faux positifs.
- Les données de Threat Intelligence sont pertinentes, contextualisées et validées, pour être utilisées en toute confiance lors des réponses à incidents.

THREATQ™

GESTION ET OPÉRATION-NALISATION DES RENSEIGNEMENTS SUR LES MENACES

ThreatQ est une plate-forme de Threat Intelligence conçue pour assurer la gestion et l'opérationnalisation des renseignements sur les menaces. Intégrant Threat Library™, Adaptive Workbench™ et Open Exchange™, ThreatQ vous permet de concentrer vos interventions sur les menaces les plus importantes pour votre entreprise et de tirer le meilleur parti de votre infrastructure de sécurité existante.

COMPRÉHENSION PLUS FINE DE LA SITUATION

DÉTECTION ET RÉPONSE À INCIDENTS PLUS RAPIDES

RENTABILISATION OPTIMALE DES INVESTISSEMENTS EN SÉCURITÉ

MEILLEURE COLLABORATION ENTRE ÉQUIPES

PRATIQUES EFFICACES ET RATIONALISÉES DE RÉPONSE À INCIDENTS

Gérez les données de Threat Intelligence pour répondre de façon proactive aux besoins de votre équipe.

- Profitez d'une mise en contexte et d'une connaissance de la situation.
- Bénéficiez d'une vue centralisée, puisqu'il est inutile d'utiliser plusieurs navigateurs pour consolider manuellement les données de Threat Intelligence.
- Intégrez la solution à vos outils de sécurité existants pour créer un dispositif de défense unifié.
- Ciblez très précisément les données et incidents pertinents.
- Limitez la durée d'implantation des hackers dans l'entreprise.

GAIN DE TEMPS ET D'ARGENT

Aidez votre équipe de cybersécurité à se concentrer sur les priorités et réduisez les délais d'intervention.

- Éliminez les tâches manuelles des workflows quotidiens.
- Limitez les problèmes de surabondance de données, d'éléments parasites et de faux positifs.
- Menez une traque active des menaces pour identifier leur origine.
- Analysez de façon approfondie uniquement les événements malveillants avérés.
- Assurez à votre équipe une efficacité et une productivité accrues en lui confiant les tâches les plus prioritaires.

TM

CONNAISSANCES AU SERVICE DE LA PROTECTION DE L'ENTREPRISE

Corrélez tous les types de données de Threat Intelligence et interprétez-les pour déterminer les mesures à prendre afin de protéger votre entreprise.

- Cernez les menaces en vous appuyant sur des données contextuelles et des profils de hackers.
- Mettez automatiquement en relation les événements de sécurité, les vulnérabilités et les attaques détectées avec les données agrégées pertinentes.
- Transformez votre connaissance de la situation en compréhension de la situation approfondie.

OPÉRATIONS DE SÉCURITÉ ET D'INTERVENTION ADAPTATIVES

Mettez en place des processus de sécurité efficaces et ramenez vos délais d'intervention de plusieurs semaines à quelques heures à peine.

- Enrichissez, organisez et contextualisez les données dans les meilleurs délais.
- Affinez vos données en fonction des besoins de votre équipe de réponse à incidents.
- Offrez à vos analystes le contexte nécessaire pour prendre des décisions plus avisées.
- Déterminez facilement les données à utiliser en fonction des priorités pour assurer une intervention efficace.
- Automatisez les tâches de façon à intervenir plus rapidement sur les menaces.

FONCTIONNALITÉS ET AVANTAGES

BIBLIOTHÈQUE SUR LES MENACES À OPTIMISATION AUTOMATIQUE	Simplifiez la recherche d'indicateurs grâce à Threat Library, une bibliothèque personnalisable sur les menaces.
PRIORISATION DÉFINIE PAR LE CLIENT	Automatisez l'attribution de scores et de niveaux de priorité aux données de Threat Intelligence en fonction de paramètres *définis par vos soins*, pour garantir l'efficacité de la réponse à incidents.
AUTOMATISATION DES MESURES À PRENDRE	Bloquez automatiquement les menaces au niveau de vos équipements de sécurité pour que seuls les incidents à caractère malveillant soient transmis à l'équipe de réponse à incidents.
OPTIMISATION DE LA COLLABORATION ENTRE ÉQUIPES	Centralisez le partage, l'analyse et l'investigation des informations de Threat Intelligence à l'aide d'Adaptive Workbench, une console adaptative à laquelle toutes les équipes peuvent accéder.
OUVERTURE ET TRANSPARENCE	Cernez le contexte, le degré de pertinence et la priorité de l'ensemble des données collectées, de façon à améliorer l'intervention.

VOUS SOUHAITEZ EN SAVOIR PLUS ?

Inscrivez-vous sur threatq.com/demo pour bénéficier d'une démonstration de ThreatQ.

À PROPOS DE THREATQUOTIENT™

ThreatQuotient sait parfaitement qu'une sécurité axée sur les renseignements repose essentiellement sur les ressources humaines. Grâce à ThreatQ™, sa plate-forme de Threat Intelligence ouverte et extensible, les acteurs de la cybersécurité ont l'assurance que les renseignements sur les menaces pertinents sont utilisés par les bons outils, au moment opportun. Adoptée par de nombreuses entreprises de premier plan à travers le monde, elle est au cœur même de leur système de gestion et d'opérationnalisation des renseignements sur les menaces. L'ensemble de leur dispositif de sécurité gagne ainsi en performances et en efficacité.

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

Copyright © 2017, ThreatQuotient, Inc. Tous droits réservés.

TQ_ThreatQ-for-IR Teams-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