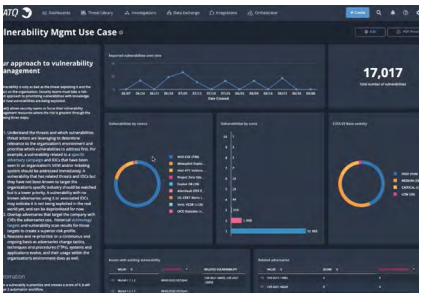
EN BREF

MODULES D'AUTOMATISATION THREATQ TDR ORCHESTRATOR

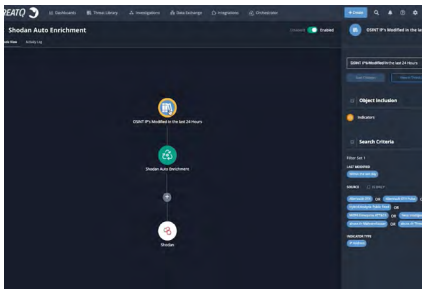
Quelle que soit leur taille, les entreprises se tournent vers l'automatisation de la cybersécurité pour gagner en efficacité, mieux se protéger contre des cyberattaques en progression constante et respecter des obligations de conformité et réglementations de plus en plus strictes. Pour autant, la mise en œuvre pose encore problème à de nombreuses équipes.

Les plates-formes d'automatisation de la cybersécurité permettent la prise en charge d'un large éventail de scénarios d'utilisation. Cette polyvalence, probablement appréciée des équipes chargées de résoudre toutes sortes de problèmes, risque toutefois de créer des difficultés à celles qui ne savent pas par où commencer.

Grâce aux modules d'automatisation de ThreatQ TDR Orchestrator, les équipes trouvent rapidement leurs marques. Ils intègrent tout ce dont elles ont besoin pour traiter les scénarios d'utilisation les plus courants, leur offrant une méthodologie pour définir leur propre positionnement en matière de risques, en fonction des ressources et outils dont elles disposent, ainsi que d'autres priorités internes.



Gestion des vulnérabilités



Enrichissement des indicateurs

XDR

Les modules d'automatisation rassemblent le tableau de bord, les rapports, TQ Smart Collections, les intégrations et bien d'autres éléments nécessaires à la prise en charge des scénarios d'utilisation fréquents, tels que la gestion des vulnérabilités, l'enrichissement automatique et le XDR, mais aussi d'autres scénarios tout prochainement.

ThreatQ TDR Orchestrator est la première solution du secteur à introduire une approche orientée sur les données pour faciliter l'implémentation des plates-formes SOAR, XDR et de Threat Intelligence : elle accélère la détection des menaces et la réponse à incident sur les systèmes disparates, pour des opérations de sécurité plus performantes.

Contactez-nous pour en savoir plus sur les modules d'automatisation ThreatQ TDR Orchestrator.

ThreatQuotient améliore les opérations de sécurité en regroupant des sources de données, des outils et des équipes disparates afin d'accélérer la détection des menaces et les interventions. 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. Pour plus d'informations, consultez le site www.threatquotient.com.

Sales@ThreatQ.com • + 1 703.574.9885

© ThreatQuotient, Inc.