THREATQUOTIENT

EN BREF

Une approche orientée données de la gestion des vulnérabilités fondée sur les risques

Établir un cadre robuste de gestion des vulnérabilités pour réduire les risques et renforcer la sécurité

Protéger une entreprise contre l'exposition aux risques numériques par la gestion des vulnérabilités et des correctifs soulève de nombreuses difficultés. La complexité croissante de l'entreprise moderne, à laquelle s'ajoutent des ressources limitées et l'évolution du paysage technologique, rend indispensable l'adoption d'une approche orientée sur les données afin de prioriser efficacement les vulnérabilités.

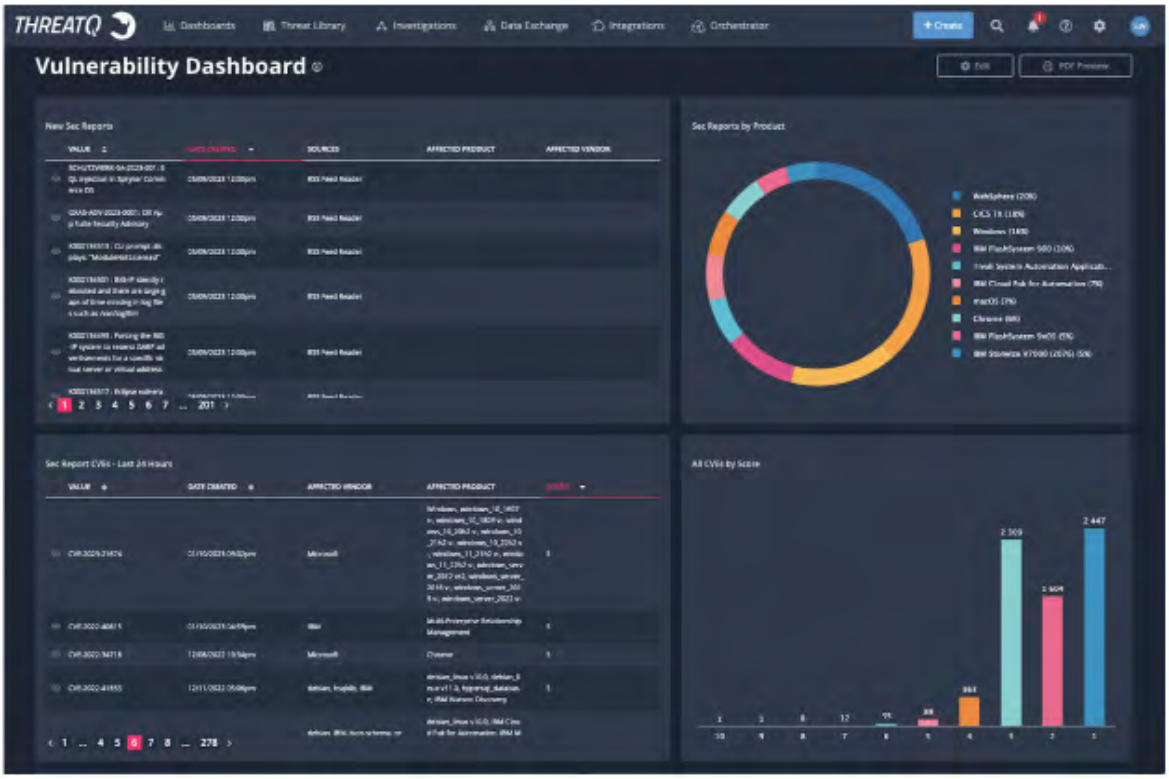
Les processus traditionnels de réduction et de correction des vulnérabilités suivent souvent une approche linéaire, susceptible de donner lieu à une mise en œuvre incomplète des mesures correctives et de rendre difficile la prise en compte de priorités changeantes. Pour relever ces défis, les entreprises doivent exploiter les données pour gagner en agilité. Une sécurité orientée sur les données fournit des informations contextuelles qui permettent aux équipes de se concentrer sur les problèmes prioritaires et de prendre des décisions avisées. La priorisation en temps réel des vulnérabilités et la mise en évidence des interdépendances entre systèmes permet aux entreprises d'améliorer leur gestion des vulnérabilités.

Au fil des années, les grandes mutations technologiques ont influencé les processus d'évaluation des vulnérabilités et de réduction des risques. Cela étant, la plupart des entreprises et des fournisseurs se concentrent généralement sur la gravité et les conséquences des vulnérabilités plutôt que sur la probabilité qu'elles soient exploitées. Cette probabilité, qui est propre à chaque entreprise, est déterminante pour prioriser avec précision les vulnérabilités. Les entreprises doivent prendre en compte la Threat Intelligence externe, qui informe notamment sur la disponibilité des outils d'exploitation, leur concordance avec les techniques et procédures des acteurs malveillants, ainsi que les cas d'exploitation précédemment observés dans leur secteur ou région.

La mise en œuvre efficace d'un cadre de gestion des vulnérabilités orienté sur les données passe par plusieurs étapes : assimilation, standardisation, corrélation, priorisation et conversion des données, documentation, génération de rapports et correction. La plate-forme ThreatQ de ThreatQuotient, optimisée par DataLinq Engine, contribue au bon déroulement de ces étapes grâce à l'intégration de sources de données et d'outils disparates. Elle aide les équipes à prioriser les vulnérabilités, à automatiser les processus, à travailler en étroite collaboration et à tirer le meilleur parti de ressources limitées.

Plusieurs outils et technologies ont une importance capitale dans la gestion des vulnérabilités orientée données : des analyseurs de vulnérabilité aux outils de test d'intrusion en passant par les systèmes de gestion des informations et des événements de sécurité (SIEM), les outils de gestion des configurations, les outils de surveillance de la sécurité des réseaux, les outils d'évaluation des risques et les systèmes de gestion des tickets. Le recours à ces outils permet aux entreprises de collecter, d'analyser et de gérer efficacement les données, ce qui renforce leurs pratiques de gestion des vulnérabilités.

Une approche orientée données de la gestion des vulnérabilités fondée sur les risques est essentielle pour parvenir à réduire les risques numériques. En mettant à profit les données, les entreprises peuvent améliorer leur agilité, prioriser les vulnérabilités avec précision et prendre des décisions avisées. Aidée de son moteur DataLinq Engine, la plate-forme ThreatQ de ThreatQuotient fournit les outils et fonctionnalités nécessaires à la mise en œuvre d'un cadre robuste, orienté données, pour la gestion des vulnérabilités. L'adoption de cette approche permet aux entreprises de réduire le risque de compromissions, de protéger leurs ressources et de renforcer leur sécurité globale.



À PROPOS DE THREATQUOTIENT™

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. 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, visitez **www.threatquotient.com**.

THREATQUOTIENT™
20130 Lakeview Center Plaza Suite 400 Ashburn, VA 20147 • ThreatQuotient.com
Sales@ThreatQuotient.com • +1 703 574-9885