THREATQUOTIENT

ÉTUDE DE CAS

Le ministère de la Défense américain renforce l'efficacité de ses cybercombattants grâce au partage de Threat Intelligence de la plate-forme ThreatQ

Présentation

Les acteurs de la défense sont sans cesse confrontés à de nouveaux obstacles, qui semblent émerger au quotidien et dont le seul objectif est de les empêcher d'accomplir leur mission. Dans le domaine cyber, ces obstacles ne se contentent pas de se multiplier, ils mutent à toute vitesse. De fait, les adversaires renouvellent et affinent constamment leurs méthodes, même si leurs objectifs restent inchangés. Les acteurs de la cybersécurité doivent par exemple se montrer particulièrement attentifs face à des attaquants qui se connectent à des ressources via Internet, compromettent les chaînes logistiques et exploitent des ransomwares pour lancer des cyberattaques contre des infrastructures critiques essentielles aux missions des organes fédéraux américains.

Les cybercombattants ont un arsenal d'outils à leur disposition, depuis la détection des endpoints et le Threat Hunting jusqu'à la surveillance réseau ou la réponse à incident. Pourtant, ils se retrouvent souvent en position de désavantage et :

- Confrontés à une surabondance de données et d'alertes
- Dépassés par la complexité de la gestion de la multitude d'outils nécessaires pour collecter les informations requises
- Obligés de déterminer la validité d'une menace sans disposer du contexte complet ou d'une vue d'ensemble de la situation
- Incapables de partager facilement des données sur les menaces et des informations contextuelles pour accélérer la détection des incidents et la réponse
- Et en sous-effectifs dans certains cas

La plate-forme ThreatQ

La plate-forme ThreatQ accélère les opérations de sécurité en optimisant la gestion et l'opérationnalisation du renseignement sur les menaces. La Threat Library à optimisation automatique, la console Adaptative Workbench et la série d'API Open Exchange permettent d'agréger les données, de comprendre et prioriser rapidement les menaces, de prendre de meilleures décisions et d'automatiser le traitement de la Threat Intelligence à l'aide des bons outils et au moment opportun, pour accélérer la détection et la réponse à incident. ThreatQ Data Exchange facilite la configuration du partage bidirectionnel d'une partie ou de la totalité de vos données de Threat Intelligence au sein de la plate-forme ThreatQ, et vous permet de l'étendre à de nombreuses équipes et de multiples emplacements. ThreatQ Investigations est une solution de gestion des situations de crise permettant une analyse collaborative des menaces, une compréhension commune et une réaction coordonnée.

ACCÉLÉREZ LES OPÉRATIONS DE SÉCURITÉ PAR L'AUTOMATISATION DU PARTAGE DE THREAT INTELLIGENCE EN TEMPS RÉEL :

Partagez immédiatement des renseignements sur les menaces connues

Exécutez des actions sans intervention humaine dans le cas de menaces connues

Priorisez automatiquement les informations provenant de sources internes et externes de Threat Intelligence et de sources d'enrichissement

Intégrez la solution à des technologies de mise en œuvre déjà en place dans l'infrastructure

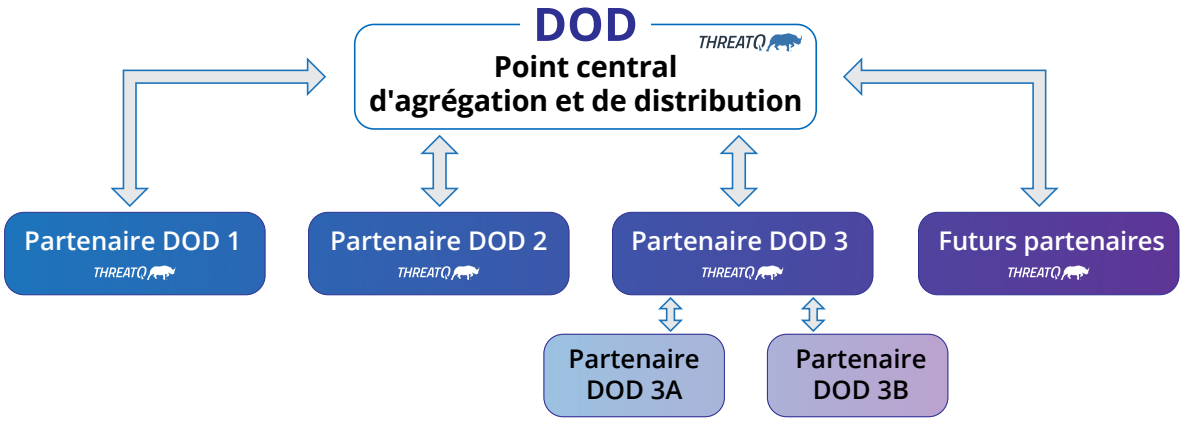
La plate-forme ThreatQ s'intègre aux technologies et processus existants et applique une approche des opérations de sécurité axée sur les menaces pour prendre en charge une grande variété de scénarios d'utilisation au-delà de la gestion des renseignements sur les menaces. Citons par exemple le Threat Hunting, la réponse à incidents, le spear phishing, le tri des alertes et la gestion des vulnérabilités.

La plate-forme ThreatQ a reçu l'autorisation ATO (Authority to Operate) de l'agence DISA (Defense Information Systems Agency) au niveau du DoDIN (Department of Defense Information Network) dans le cadre de l'infrastructure HBSS (Host Based Security System), ce qui permet au ministère de la Défense américain de déployer la plate-forme ThreatQ plus rapidement pour répondre à ses défis de cybersécurité.

Plate-forme ThreatQ et ministère de la Défense américain

Aujourd'hui, le ministère de la Défense américain (DOD, Department of Defense) utilise la plate-forme ThreatQ pour aider les cybercombattants à gérer l'énorme volume d'informations auxquelles ils ont accès, et à comprendre leur pertinence et leurs priorités respectives, pour ensuite passer à l'action de manière efficace. Non seulement cette plate-forme est employée par diverses équipes responsables des opérations de sécurité au sein de plusieurs branches distinctes de la Défense, mais grâce à ThreatQ Data Exchange, ces divers services peuvent partager une Threat Intelligence organisée et validée avec leurs homologues du ministère. Étant donné que l'échange est bidirectionnel et point à point, chaque partenaire participant peut identifier et partager des renseignements sous la forme d'indicateurs de compromission et d'indicateurs connexes connus avec le point de centralisation des données, pour qu'ils soient distribués aux autres partenaires.

La capacité à partager une Threat Intelligence correctement organisée avec des homologues de la sécurité constitue un multiplicateur de force pour tous les participants. Chaque équipe peut ainsi tirer parti des connaissances et des compétences de toutes les parties en présence. Collectivement, elles sont mieux à même de comprendre le dispositif de sécurité contre les menaces spécifiques dont elles assurent le suivi, tout comme elles peuvent identifier les tendances et déterminer les domaines où la protection en place est insuffisante.



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**.

Sales@ThreatQ.com • + 1 703.574.9885