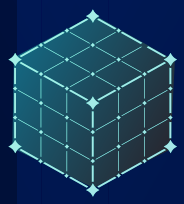
THREATQUOTIENT

FICHE TECHNIQUE

La sécurité dans un environnement Air-Gap



Les réseaux hors ligne ou classifiés, non connectés à Internet, occupent une place essentielle dans la sécurité nationale et la défense des gouvernements. Le but de tels environnements classifiés est de pouvoir utiliser et traiter des informations sensibles qui doivent rester inaccessibles au reste de la communauté Internet. Cela dit, pour fonctionner, les environnements classifiés doivent généralement avoir accès à une fraction des informations accessibles aux réseaux connectés à Internet. Une telle pratique engendre une série de défis, dont les suivants :

- L'existence de réseaux déconnectés donne lieu au cloisonnement des informations pertinentes de Threat Intelligence.
- L'accès aux informations contextuelles sur les menaces nécessaires à la prise de décision sur les réseaux tactiques et classifiés est retardé par de laborieux processus de transfert de données entre les différents domaines.
- Il est difficile de tirer parti du travail réalisé par les équipes SecOps à la fois dans des réseaux non classifiés et classifiés.
- La détection et la réponse étendues (eXtended Detection and Response, XDR) sont limitées à l'infrastructure connectée au sein d'un même réseau et peuvent être difficilement transférées vers d'autres réseaux.

Dans le domaine de la cybersécurité, qu'elle soit offensive ou défensive, le contexte est primordial. Offrir un accès à ces données contextuelles constitue un défi pour la plupart des plates-formes et flux de Threat Intelligence, car ces fonctionnalités exigent généralement une connexion Internet pour fonctionner correctement ou pour qu'il soit possible d'exploiter tout leur potentiel. Les analystes et opérateurs de sécurité sont contraints de compiler et d'extraire manuellement les informations pertinentes avant de pouvoir les réintégrer et les utiliser dans leur environnement classifié. Dès qu'ils terminent ces tâches manuelles et fastidieuses, les informations sont souvent dépassées et il leur faut évaluer et analyser de nouvelles données.

La plate-forme ThreatQ

La plate-forme ThreatQ accélère les opérations de sécurité par une optimisation de la gestion et des contre-mesures défensives. La Threat Library, dont l'optimisation est automatique, l'interface Adaptive Workbench et les API Open Exchange permettent aux organisations d'agréger les données, de comprendre et prioriser rapidement les menaces, de prendre de meilleures décisions et d'automatiser l'ingestion des renseignements appropriés sur les menaces dans les bons outils, au bon moment, afin d'accélérer la détection et la réponse à incident. ThreatQ Data Exchange facilite l'implémentation 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 sites. 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.

AVANTAGES DE LA SOLUTION THREATQ AIR-GAP DATA SYNC (AGDS)

L'intégrité du réseau est préservée grâce à un déploiement véritablement Air-Gap.

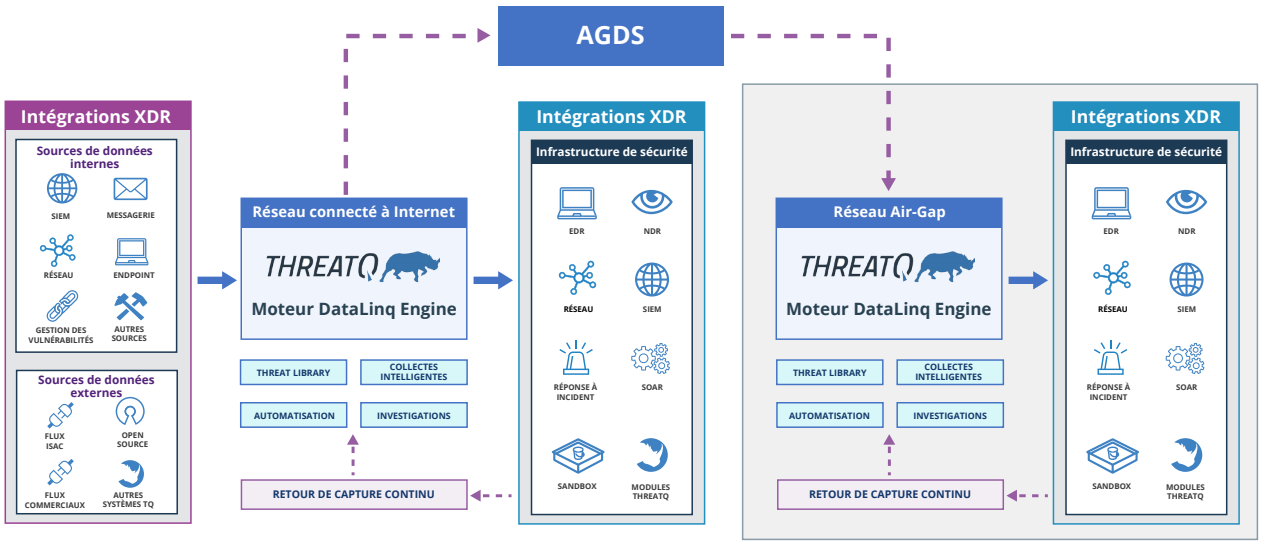
Les fonctionnalités de contrôle et d'intégration nécessaires à l'opérationnalisation des données sur les menaces dans des réseaux non classifiés peuvent être utilisées par l'infrastructure de sécurité dans des réseaux classifiés, de quelque niveau que ce soit.

Il est possible de partager en toute sécurité des données enrichies et non classifiées de Threat Intelligence avec des réseaux classifiés grâce à plusieurs méthodes de transfert.

La plate-forme ThreatQ fonctionne avec des technologies et processus existants et applique une approche orientée données pour gérer les opérations de sécurité. Elle prend en charge divers scénarios d'utilisation, notamment la gestion de la Threat Intelligence, le Threat Hunting, la réponse à incident, la lutte contre le spear phishing, le tri des alertes et la gestion des vulnérabilités. Une autorisation de fonctionnement (Authority to Operate, ATO) a été octroyée par l'agence DISA (Defense Information Systems Agency) au niveau du réseau DoDIN (Department of Defense Information Network) dans le cadre de l'infrastructure de solutions de sécurité des endpoints (ESS). Ce processus approuvé permet un déploiement plus rapide de la plate-forme ThreatQ chez des clients ThreatQuotient dans le monde entier afin de répondre à leurs défis de cybersécurité.

Air-Gap Data Sync (AGDS) transfère efficacement les données entre deux instances ThreatQ, l'instance en ligne connectée à Internet et l'instance hors ligne, ou déconnectée. ThreatQ AGDS est conçu pour prendre en charge des environnements Air-Gap et a été implémenté selon deux approches : les diodes de données (ou passerelles unidirectionnelles) et le transfert manuel.

Comme illustré dans le diagramme, ThreatQ AGDS utilise une architecture qui prend en charge un flux de données unidirectionnel entre l'instance connectée à Internet et l'instance Air-Gap de la plate-forme de Threat Intelligence. L'architecture permet d'exporter les données depuis l'instance 1 vers le mécanisme de transfert. Ce mécanisme de transfert, à savoir une diode unidirectionnelle ou une solution High Speed Guard, permet de transmettre les données vers l'environnement Air-Gap. Une fois les données transférées, ThreatQ AGDS télécharge ensuite les nouvelles données dans la bibliothèque Threat Library de l'instance 2.



Pour une analyse plus approfondie des éléments intervenant dans la conception et l'implémentation d'une plate-forme de Threat Intelligence dans un environnement Air-Gap, téléchargez le livre blanc « Using ThreatQ in Air-Gapped Environments ».

TÉLÉCHARGER

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, consultez le site www.threatquotient.com.

THREATQUOTIENT **Sales@ThreatQ.com • +1 703.574.9885**