THREATQUOTIENT

THALES
Construisons ensemble un avenir de confiance

TÉMOIGNAGE CLIENT

Le groupe Thales met en place un service de Threat Intelligence fondé sur la plate-forme ThreatQ

Thales (Euronext Paris : HO) choisit la plate-forme ThreatQ pour créer un service de Threat Intelligence personnalisé permettant à ses clients d'optimiser leurs outils et technologies de cybersécurité ; le groupe met alors en place la plus grande équipe de Threat Intelligence d'Europe.

Défi

En 2016, Ivan Fontarensky, directeur technique cyberdéfense chez Thales, souhaitait déployer un service de Threat Intelligence pour continuer d'apporter de la valeur ajoutée aux produits de cybersécurité du groupe, qui sont utilisés dans le monde entier par les entreprises des secteurs aux infrastructures critiques. En effet, la Threat Intelligence est indispensable pour renforcer la détection et la réponse à incident, et adopter une stratégie de cyberdéfense proactive. Thales avait déjà intégré les données sur les menaces dans ses solutions de détection et réponse à incident, mais M. Fontarensky était conscient que l'explosion de la Threat Intelligence, en termes de volume de données et de variété des sources, allait se poursuivre. De plus, chaque client est confronté à un paysage des menaces qui lui est propre et, de ce fait, doit disposer de renseignements pertinents, organisés et ciblés pour son environnement.

Par ailleurs, face au foisonnement de renseignements sur les menaces provenant de ses recherches internes et de sources commerciales, open source, gouvernementales et sectorielles, Thales avait besoin d'un moyen de mettre à profit toutes ces données à des fins d'analyse et de les proposer sous une forme directement exploitable à ses SOC internes et à ses clients à travers le monde.

Solution

À la recherche d'un partenaire qui partage sa vision et puisse l'aider à développer sa capacité de Threat Intelligence, Thales s'est tourné vers ThreatQuotient et sa plate-forme ThreatQ hautement flexible et évolutive, qui répondait à ses principaux critères, notamment :

Intégration et personnalisation : ThreatQ propose une vaste bibliothèque d'API et de connecteurs personnalisés pouvant être écrits et

« La Threat Intelligence est incontournable et était indispensable à la montée en puissance de notre portefeuille de solutions de cybersécurité. Nous partageons une vision commune avec ThreatQuotient et, comme l'entreprise dispose de la plate-forme la plus mature et robuste du marché, nous savions qu'elle pourrait nous aider à industrialiser notre modèle de Threat Intelligence pour répondre à nos besoins dans le monde entier. »

– Ivan Fontarensky, Directeur technique cyberdéfense, Thales

PRÉSENTATION

SECTEUR : Technologies

CLIENT DEPUIS : 2017

EFFECTIF : > 80 000

CHIFFRE D'AFFAIRES : 17,6 milliards d'euros

LOCALISATION : 68 pays ; siège : France

DÉFI

Créer et lancer un service de Threat Intelligence pour continuer d'ajouter de la valeur aux produits de cybersécurité de Thales, utilisés par les entreprises du secteur des infrastructures critiques, partout dans le monde.

SOLUTION

La plate-forme ThreatQ et la solution ThreatQ Investigations répondaient aux critères essentiels de Thales, notamment l'intégration à des sources de données et outils de cybersécurité toujours plus nombreux aux fins d'une analyse et d'une compréhension plus approfondies, une détection et une réponse à incident renforcées, et une cyberdéfense proactive.

RÉSULTAT

- ✔ Threat Intelligence personnalisée au bénéfice des clients du monde entier
- ✔ Avantage stratégique grâce à une Threat Intelligence plus évoluée
- ✔ Le plus grand fournisseur de Threat Intelligence d'Europe

www.threatquotient.com

déployés rapidement afin de faciliter l'intégration avec les outils et les sources de Threat Intelligence existants. Cela permet à l'équipe de Thales d'agréger et de normaliser d'énormes volumes de données brutes sur les menaces, de corréler et analyser les données pour les transformer en renseignements précis sur les menaces, de prioriser ces renseignements et de créer des règles de détection des menaces spécifiquement adaptées au client. Elle peut ensuite distribuer les renseignements et règles de détection des menaces pertinents à ses SOC internes, ainsi qu'aux capteurs CYBELS de Thales et aux autres outils de sécurité réseau déployés dans l'environnement du client.

Collaboration et visualisation : Lorsque Thales a commencé à travailler avec ThreatQuotient, le concept de Threat Intelligence lui était relativement nouveau. Grâce à la plate-forme ThreatQ, M. Fontarensky a pu montrer aux différentes équipes comment elles pourraient collaborer pour obtenir une visibilité sur les événements en cours partout sur le réseau, et communiquer dans un langage commun, même si elles se trouvent dans des pays différents. Grâce à la mise en commun des données sur les menaces provenant de différentes sources et des informations de détection et alertes générées par différents outils, on obtient une Threat Intelligence collective qui amène à une stratégie de cyberdéfense mature et proactive.

Service et support : Pionnier dans le domaine de la Threat Intelligence, ThreatQuotient disposait des connaissances et compétences nécessaires pour accompagner la stratégie de commercialisation de Thales au moyen d'une plate-forme robuste et fiable. Les deux entreprises ont vite établi un partenariat solide qui a permis à Thales d'obtenir rapidement des réponses à ses questions et de relever les défis auxquels elle a été confrontée lors du lancement de son nouveau service de Threat Intelligence en 2017.

Aujourd'hui, les activités de Threat Intelligence de Thales sont pilotées par l'équipe centrale de Threat Intelligence, composée de 50 analystes – des spécialistes du renseignement sur la menace et des experts en géopolitique. Cette équipe possède la plate-forme ThreatQ principale et est responsable de l'agrégation et de l'analyse des données sur les menaces, de la création et du partage des détections, et de l'élaboration de rapports sur les menaces les plus récentes.

Elle collabore avec les équipes SOC et l'équipe de réponse à incident pour répondre aux principaux scénarios d'utilisation suivants :

Tri des alertes : Thales dispose de huit SOC qui analysent les renseignements reçus et les enrichissent avec d'autres données sur les menaces et informations de contexte provenant du propre environnement de l'entreprise, par exemple en corrélant les renseignements avec des données supplémentaires issues

Résultat

Threat Intelligence personnalisée au bénéfice des clients du monde entier

Comme la plate-forme ThreatQ est ouverte, Thales peut adapter son modèle de Threat Intelligence à chacun de ses clients. Avec le service de Threat Intelligence personnalisé, son équipe peut transmettre les renseignements pertinents au bon moment et aux outils adéquats en fonction de l'environnement et du secteur d'activité du client. Ce dernier peut ainsi mener une stratégie proactive en matière de cyberdéfense.

Avantage stratégique grâce à une Threat Intelligence plus évoluée

La collaboration et la visualisation ont permis à Thales de devenir l'un des leaders de la recherche en Threat Intelligence, ses études aidant les clients à comprendre l'évolution du paysage des menaces et la façon de réduire les risques.

Le plus grand fournisseur de Threat Intelligence d'Europe

Thales a mis en place tout un service de Threat Intelligence fort de 50 experts en la matière, ce département ne comptant à la base qu'une personne. ThreatQuotient fournit la plate-forme et le support nécessaires pour permettre à Thales de faire évoluer son service et d'accélérer la distribution de renseignements exploitables et de détections, tout en maintenant un faible coût total de possession.

de son système SIEM. Ces opérations lui permettent de réduire le nombre de faux positifs, d'améliorer la qualité des alertes, de les prioriser et de déterminer les mesures à prendre.

Investigation et réponse à incident : Afin de comprendre les effets et le cheminement d'une attaque, l'équipe de Threat Intelligence utilise ThreatQ Investigations pour se pencher sur d'autres éléments et ainsi mieux cerner l'attaquant et son mode opératoire. Les visualisations lui permettent de collaborer avec l'équipe de réponse à incident et de lui montrer le comportement exact de l'attaque, afin de déterminer les mesures les mieux indiquées pour parvenir à une réponse globale.

Recherche et rapports : Au fil des ans, Ivan Fontarensky et l'équipe de Threat Intelligence ont étendu leur utilisation de la plate-forme, passant des applications tactiques à d'autres plus stratégiques. Par exemple, leur carte des cybermenaces (Cyberthreat Hitmap), très appréciée des professionnels de la sécurité, fournit des informations sur les régions et secteurs les plus ciblés, les principaux points de départ des attaques et les logiciels malveillants les plus actifs. L'équipe élabore environ 300 rapports par an. Outre les indicateurs et les empreintes numériques, elle étudie la méthodologie et les TTP des attaques pour en connaître les tenants et les aboutissants : l'attaquant, la cible, la localisation, le motif et le procédé. La mise en corrélation des événements géopolitiques et des cyberactivités permet à Thales et à ses clients d'anticiper les attaques. Un exemple d'analyse approfondie offrant un aperçu des connaissances géopolitiques de l'équipe de Threat Intelligence est disponible ici : Cyber Threat Intelligence | Thales Group. Cette analyse sur un an est consacrée au cyberconflit en Ukraine et à ses répercussions sur l'ensemble de la zone géographique européenne.

« Notre partenariat avec ThreatQuotient nous a permis de donner de l'ampleur à notre service, passant d'un responsable à une équipe de 50 personnes en quelques années, et de devenir le plus grand fournisseur de Threat Intelligence d'Europe. »

– Ivan Fontarensky,
Directeur technique cyberdéfense, Thales

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 la réponse à incident. 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**.

Sales@ThreatQ.com • + 1 703.574.9885