PRÉSENTATION

Choisir une plate-forme de Threat Intelligence de qualité professionnelle

Généralités

Si vous décidez de mettre en œuvre une plate-forme de Threat Intelligence, il est important de prendre en compte le profil, la qualité et le potentiel futur du partenaire que vous allez choisir. Il existe aujourd'hui plus de 2 000 sociétés de cybersécurité. Tous ces fournisseurs de technologies ne se valent pas et tous ne tiennent pas leurs promesses.

Investir dans une plate-forme de Threat Intelligence, qui deviendra un élément central de votre infrastructure de sécurité, est une décision importante. Cette plateforme doit être en mesure de regrouper des sources de données, des outils et des équipes hétérogènes afin de prioriser le risque lié aux menaces et d'accélérer la détection des menaces et la réponse à incident.

Le choix d'une plate-forme de Threat Intelligence ne se limite pas à un achat, c'est un parcours à mener. Nous vous encourageons à choisir avec précaution les entreprises avec lesquelles vous vous associerez pour mettre en place cette technologie stratégique.

Pour effectuer un investissement de ce type, plusieurs critères méritent d'être pris en compte :

- **La maturité, l'architecture et les fonctionnalités de la plate-forme**
- **Les services, la mise en œuvre et l'assistance après-vente**
- **Les utilisateurs et la clientèle**
- **L'histoire, l'équipe et la capacité d'exécution de l'entreprise**

Maturité, architecture et fonctionnalités de la plate-forme

Comme pour tout investissement de sécurité, la maturité, l'architecture et les fonctionnalités d'une plate-forme de Threat Intelligence sont des éléments critiques de votre décision. Dans la mesure où elle deviendra un élément central de votre infrastructure de sécurité, cette plate-forme doit être stable et évoluer avec les besoins de votre entreprise tout en unifiant les sources de données et les outils hétérogènes de vos technologies et équipes de sécurité.

Le développement de la plate-forme ThreatQ a débuté en 2013, bien plus tôt que d'autres produits concurrents. Les choix architecturaux judicieux faits par notre équipe ont ainsi permis de concevoir dès le départ une plate-forme de Threat Intelligence de qualité professionnelle. À mesure de l'élargissement du marché et de l'augmentation du nombre de fournisseurs, ces décisions architecturales et la décennie d'apprentissage et d'expérience constituent un différenciateur majeur en faveur de ThreatQ par rapport aux fournisseurs concurrents.

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 de Threat Intelligence 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 à 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.

Une plate-forme de Threat Intelligence de qualité professionnelle se doit d'être évolutive et stable et de proposer un large écosystème d'intégrations prenant en charge une grande variété de scénarios d'utilisation.

L'approche orientée sur les données permet aux équipes d'identifier rapidement les menaces majeures avant d'intervenir. Le moteur DataLinq Engine de ThreatQ alimente la plate-forme de Threat Intelligence pour la rendre plus évolutive et plus facile à gérer et permet d'obtenir plus rapidement de meilleurs résultats. Son modèle de données entièrement personnalisable offre un niveau de flexibilité inégalé dans la gestion des données. L'approche orientée sur les données de ThreatQ permet de bénéficier de fonctionnalités de pointe, comme l'attribution dynamique de scores, la priorisation et l'automatisation no-code.

Le développement de la plate-forme ThreatQ a débuté il y a plus de dix ans. La version 5 actuelle de la plate-forme procure un niveau de stabilité et de maturité bien supérieur à celui des produits concurrents. La meilleure preuve en est qu'elle a été choisie par de nombreuses grandes entreprises et organismes gouvernementaux du monde entier. ThreatQuotient maintient un dialogue ouvert avec des fournisseurs de flux de renseignements afin d'être prévenu rapidement de toute modification pouvant affecter les intégrations et de pouvoir ainsi les tester et les mettre à jour de façon proactive le cas échéant. Les logiciels d'entreprise requièrent en outre une grande résilience de la part de la plate-forme qui ne peut être obtenue qu'avec un solide processus d'assurance qualité et de développement. Ces différents critères ont permis à ThreatQuotient d'obtenir et de conserver des certifications telles que SOC2 : type 2SOC, niveau 2.

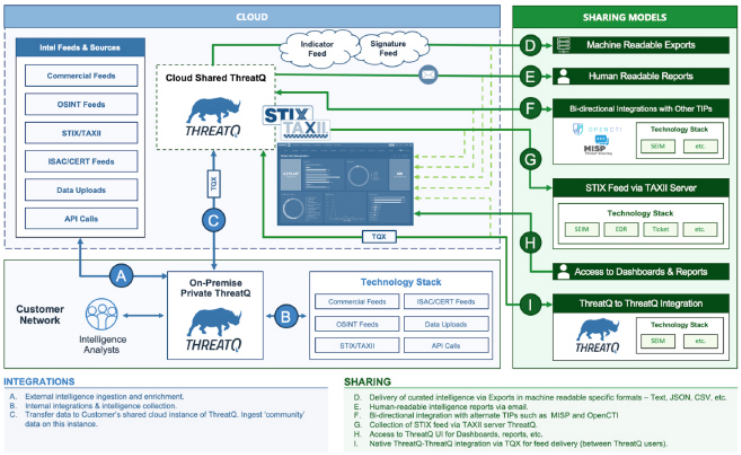
L'élargissement de la couverture de l'infrastructure de sécurité offre aux utilisateurs une visibilité et un contexte améliorés ; le regroupement des données dans une même plate-forme permet de mieux cerner la menace et de la neutraliser rapidement.

La valeur et la diversité des intégrations ThreatQ permettent d'ingérer n'importe quelle source de données et d'effectuer des intégrations bidirectionnelles avec les outils et technologies du SOC. Des flux commerciaux, open source et ISAC, ainsi que des données propriétaires, structurées et non structurées, peuvent être utilisés par la plate-forme et stockés afin d'être en permanence accessibles via la Threat Library, une source unique d'informations fiables en matière de détection des menaces et d'intervention, et autres contenus liés. En conservant et en priorisant les données recueillies lors de détections, d'investigations et d'incidents précédents, la Threat Library est une véritable mémoire organisationnelle capable d'apprendre et de s'améliorer avec le temps. La boutique ThreatQ propose des intégrations avec plus de 400 produits et services de sécurité. Le cas échéant, le développement d'autres intégrations est également possible.

ThreatQ fonctionne avec les technologies et processus existants pour améliorer l'efficacité de vos collaborateurs et technologies. La plate-forme permet aux équipes chargées des opérations de sécurité de traiter les scénarios d'utilisation les plus fréquents, notamment : gestion de la Threat Intelligence, partage de la Threat Intelligence, réponse à incident, tri des alertes, Threat Hunting, analyse antiphishing et priorisation des vulnérabilités.

COLLECTES INTELLIGENTES (SMART COLLECTIONS) DE THREATQ

Les collectes intelligentes de ThreatQ sont au cœur de l'évolutivité de la plate-forme. Les utilisateurs peuvent rapidement créer des ensembles de données très raffinés à l'aide de contrôles de filtres flexibles, puis utiliser ces collectes intelligentes pour effectuer des analyses dans les tableaux de bord, mener des investigations dans ThreatQ Investigations, créer des automatisations dans ThreatQ TDR Orchestrator, partager les informations au sein d'une communauté d'utilisateurs, et bien d'autres choses encore.



ThreatQ prend en charge l'intégration et le partage pour un large éventail de technologies favorisant la collaboration sans restriction.

Services, mise en œuvre et assistance après-vente

La complexité de l'environnement de sécurité d'une entreprise et la diversité des technologies connexes utilisées nécessitent une planification en amont de la mise en œuvre avant le déploiement d'une plate-forme de Threat Intelligence. Certaines entreprises disposent des ressources internes nécessaires pour implémenter et déployer une plate-forme de Threat Intelligence. D'autres confieront ces tâches au fournisseur de la plate-forme. C'est pourquoi il est important de se renseigner sur les services d'assistance et de mise en œuvre proposés par les différents fournisseurs de plates-formes de Threat Intelligence : le fournisseur est-il un partenaire fiable, a-t-il la souplesse nécessaire pour s'adapter à vos processus et a-t-il votre réussite à cœur ?

ThreatQuotient propose plusieurs services de distribution directe ou indirecte par l'intermédiaire d'un réseau croissant de partenaires d'intégration. Le déploiement d'une plate-forme de Threat Intelligence a pour objectif d'accélérer la détection des menaces et la réponse à incident. Notre objectif est de vous aider à planifier et à mener à bien cette mission.

Services professionnels :

ThreatQ propose à ses clients des services professionnels adaptés à tous les niveaux de maturité des opérations de sécurité et de la Threat Intelligence. Notre équipe s'appuie sur des pratiques de pointe et l'expertise de collaborateurs ayant plus de dix ans d'expérience dans les domaines de la Threat Intelligence au niveau public et privé et de la cybersécurité opérationnelle.

Nos services fournissent les fonctionnalités de base nécessaires à l'évaluation, à la conception et à la mise en œuvre d'une Threat Intelligence orientée sur les données. L'équipe des services professionnels identifie les personnes, les processus et les technologies nécessaires pour intégrer efficacement la Threat Intelligence aux opérations de sécurité et aux programmes de gestion des cyberrisques. Ces services permettent aux entreprises de passer d'une surveillance, détection et réponse traditionnelles basées sur les signatures à un programme d'opérations axé sur les menaces externes.

Réussite client :

L'équipe de ThreatQ chargée de la réussite de nos clients adopte une approche proactive pour assurer la pérennité de la valeur ajoutée de leur investissement à mesure du changement et de l'évolution de leurs besoins. Dès le processus d'intégration, un ingénieur dédié (CSE) rencontre régulièrement les clients. Il a pour mission d'identifier les difficultés rencontrées par le client ainsi que ses objectifs futurs, de définir des étapes importantes et d'accompagner le projet de bout en bout. Ce type de relation permet à l'équipe CSE de représenter le client au sein de ThreatQ.

Formation et certification :

La formation est essentielle à la cybersécurité. La ThreatQ Academy a été créée dans l'optique d'encourager l'acquisition de connaissances. Cette plate-forme de formation permet aux professionnels d'approfondir leurs connaissances en matière de Threat Intelligence. ThreatQ Academy, par son offre de cours, de ressources et de certifications, traduit l'engagement de ThreatQuotient d'évoluer avec ses clients et partenaires pour leur offrir une protection de pointe adaptée à leurs ressources informatiques. ThreatQ Academy propose des modules de formation standard, ainsi que des solutions d'apprentissage sur mesure qui peuvent répondre à pratiquement tous les besoins opérationnels et sont accessibles au moment voulu.

Les certifications de ThreatQ Academy constituent un investissement majeur. Dans un paysage des cybermenaces en constante évolution et toujours plus sophistiqué, il est indispensable de pouvoir s'appuyer sur des professionnels certifiés. Les certifications permettent de renforcer l'expertise de vos collaborateurs en matière de Threat Intelligence. Elles leur permettent d'acquérir les connaissances et les compétences requises pour identifier et évaluer les menaces de cybersécurité et y remédier. Cela permet non seulement d'améliorer leurs capacités, mais aussi de renforcer les défenses de l'entreprise.

Elles aident également à identifier les collaborateurs chevronnés et à exploiter ainsi leur expertise pour des tâches et des projets spécifiques. En outre, elles instaurent un climat de confiance avec les clients et partenaires, sachant que l'entreprise s'engage à respecter les normes les plus strictes en matière de cybersécurité grâce à des professionnels certifiés. En substance, les programmes de certification de la ThreatQ Academy constituent un investissement stratégique pour les compétences de l'équipe et le niveau de sécurité de l'entreprise.

Utilisateurs, clients et partenaires

La qualité et le profil de la clientèle d'un fournisseur sont le reflet de la fiabilité de son entreprise. Avant d'effectuer un achat, les clients professionnels aguerris font preuve d'une extrême rigueur à l'égard d'un fournisseur dans de nombreux domaines : examen technique approfondi, sécurité de la plate-forme, viabilité financière, exigences en matière d'assurance et vérification des références des clients actuels.

ThreatQuotient est fier de protéger les entreprises les plus prestigieuses au monde du classement Fortune 500 et les organismes fédéraux les plus renommés.

ThreatQuotient compte parmi ces clients des entreprises de premier plan comme le ministère de la Défense des États-Unis, PWC France/CIX-A, ainsi que la Saudi Investment Bank, mais également des entreprises de renom dans les secteurs de la technologie, de la santé, de la fabrication, de la vente au détail, des services financiers, de l'énergie et du gouvernement fédéral.

Des accords très stricts de non-divulgation et de confidentialité et notre charte de déontologie nous empêchent de publier la liste complète de nos clients. Nous nous ferons cependant un plaisir d'organiser des appels téléphoniques individuels avec des clients de votre secteur, le cas échéant.

Par ailleurs, ThreatQ Community offre une communauté privée de cybersécurité dédiée au partage d'informations de Threat Intelligence à l'échelle mondiale. Cette communauté comprend des membres issus d'un large éventail de secteurs et de régions qui ont à cœur de partager les informations de Threat Intelligence afin d'améliorer les capacités collectives de détection et de réponse du groupe. En intégrant cette communauté, vous bénéficierez d'une instance hébergée de la plate-forme ThreatQ avec plus de 50 flux de Threat Intelligence open source et aurez la possibilité de collaborer avec d'autres membres.

Outre la gestion de la Threat Intelligence et des données pour protéger des entreprises spécifiques, la plate-forme ThreatQ est déployée comme système back-end chez de multiples intégrateurs de systèmes, fournisseurs de services de sécurité managés (MSSP) et entreprises de gestion de la détection et de la réponse à incident (MDR).

Partenariats :

La collaboration est indispensable à une expérience positive pour les utilisateurs et clients. Un partenariat avec des entreprises de premier plan comme Thalès et ATOS nous a permis d'étendre notre rayon d'action, de bénéficier d'une expertise diversifiée et de proposer des solutions améliorées.

> **“Les collectes intelligentes de ThreatQ sont au cœur de l'évolutivité de la plate-forme. Les utilisateurs peuvent rapidement créer des ensembles de données très raffinés à l'aide de contrôles de filtres flexibles, puis utiliser ces collectes intelligentes pour effectuer des analyses dans les tableaux de bord, mener des investigations dans ThreatQ Investigations, créer des automatisations dans ThreatQ TDR Orchestrator, partager les informations au sein d'une communauté d'utilisateurs, et bien d'autres choses encore.”**
>
> **- Tyler Greer, Cyber Threat intelligence Lead, LPL Financial**

Ces partenariats nous permettent de renforcer notre engagement envers nos clients pour leur fournir des technologies de pointe et des solutions de sécurité complètes adaptées à l'évolution de leurs besoins.

Histoire, équipe et capacité d'exécution de l'entreprise

Ces dernières années, le secteur de la cybersécurité a connu un afflux d'entrepreneurs passionnés et bien intentionnés. Poussées par une foule d'investisseurs souhaitant se faire une place sur le marché de la sécurité, de nouvelles entreprises et équipes ont vu le jour presque chaque semaine. Il est important de se renseigner sur la qualité, le profil, les données de référence et la capacité d'exécution de l'entreprise. L'équipe a-t-elle déjà créé et exploité avec succès une entreprise, recruté et fidélisé de brillants professionnels et développé une technologie pouvant être déployée par de grandes entreprises ?

L'équipe ThreatQuotient a collaboré avec certains des noms les plus réputés dans le domaine de la cybersécurité, ce qui témoigne de sa compréhension approfondie du problème de la cybersécurité, de l'importance de l'innovation et de la valeur de relations durables avec ses clients et partenaires. Une équipe performante et expérimentée dispose d'une large expérience pour gagner la confiance des utilisateurs tout en fournissant des solutions d'opérations de sécurité uniques adaptées aux dernières tendances avec une approche mesurée.

La reconnaissance témoigne de la persévérance indéfectible de l'entreprise à atteindre l'excellence. Nous sommes fiers d'avoir remporté récemment plusieurs prix prestigieux, comme le Washington Post Top Workplaces, Cybersecurity Breakthrough for Overall SOAR Platform of the Year et Cyber Defense Magazine Market Leader in Threat Intelligence, en reconnaissance de notre innovation, de notre engagement en matière de sécurité et de nos contributions pour le secteur grâce à notre plate-forme de Threat Intelligence. Ces distinctions récompensent nos efforts constants pour fournir des solutions et des services de pointe visant à mieux protéger nos clients contre les cybermenaces.

Conclusion

Le choix d'une plate-forme de Threat Intelligence de qualité professionnelle est une décision stratégique majeure. Il est essentiel de choisir un partenaire proposant une plate-forme robuste et mature et offrant des fonctionnalités évolutives et une assistance après-vente performante. Une approche orientée sur les données, un traitement des données évolutif et une intégration aux technologies existantes sont autant de qualités indispensables pour une détection des menaces et une réponse efficaces. En s'associant à un fournisseur tel que ThreatQuotient réputé pour ses données de référence fiables, son engagement en matière d'innovation et de sécurité et reconnu par le secteur, votre entreprise a l'assurance de bénéficier d'une puissante plate-forme pour des opérations de sécurité orientées sur les données, efficaces et performantes.

Pour de plus amples informations, y compris des recommandations d'établissements financiers partenaires de ThreatQuotient, contactez-nous à l'adresse **www.threatq.com/demo/**.

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 de Threat Intelligence 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 à 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