THREATQUOTIENT™

DÉVELOPPER OU ACHETER ?

Réponse à l'éternelle interrogation des équipes informatiques

par Ryan W. Trost, cofondateur et Directeur des technologies

En matière de technologies, une question resurgit sans cesse : *« Développer ou acheter ? »*. Elle se pose généralement lorsqu'une solution a atteint une maturité suffisante pour répondre à un besoin du marché défini et être disponible sous une forme open source, mais n'existe pas depuis suffisamment longtemps pour avoir engendré une discipline à part entière dont les pratiques se sont affinées au fil des années et pour laquelle un nombre réduit d'éditeurs proposent une gamme limitée de solutions ayant toutes fait l'objet d'évaluations par les analystes du secteur.

Les plates-formes de Threat Intelligence ont aujourd'hui atteint ce point d'inflexion et les équipes de sécurité s'interrogent : « *Devrions-nous développer ou acheter une plate-forme de Threat Intelligence ?* ». En réalité, elles devraient plutôt se poser la question suivante : *« Devrions-nous développer une plate-forme de Threat Intelligence simplement parce que nous le pouvons ? »*.

PRINCIPALES CARACTÉRISTIQUES D'UNE PLATE-FORME DE THREAT INTELLIGENCE

Une plate-forme de Threat Intelligence a pour but de permettre aux SOC (Security Operations Centers), aux analystes en Threat Intelligence ainsi qu'aux équipes de gestion des vulnérabilités, de gestion des risques et d'intervention sur incidents de répondre aux événements et alertes, mais également d'anticiper les menaces et de devenir plus proactifs. Pour ce faire, elle doit servir de source d'informations unique et fiable pour toutes les données sur les menaces issues de sources internes et externes, favorisant ainsi la collaboration, une prise de décision plus judicieuse, des mesures proactives et une réduction des délais de détection et d'intervention. Qu'elle soit développée en interne ou achetée à un fournisseur tiers, cette plate-forme doit être en mesure de vous aider à comprendre, prioriser et neutraliser les menaces les plus importantes pour votre entreprise. À mesure que le paysage des menaces et votre environnement interne évoluent, la plate-forme de Threat Intelligence peut également vous aider à mieux comprendre et anticiper les menaces potentielles grâce à une évaluation continue, vous permettant ainsi de renforcer vos défenses de façon proactive.

Conçue pour optimiser la gestion et l'opérationnalisation du renseignement sur les menaces, une plate-forme de Threat Intelligence doit vous permettre de réunir rapidement les informations internes sur les menaces, notamment les données sur les événements de sécurité, l'analyse des logiciels malveillants et l'analyse du comportement des hackers, et de les recouper avec les informations externes afin d'obtenir un contexte critique sur l'auteur, la nature, la chronologie, le mode d'action et la motivation d'une menace. Elle doit également assurer la priorisation pour vous permettre de filtrer automatiquement les données parasites et de déterminer quels événements sont importants pour votre entreprise en fonction de paramètres que vous définissez. Elle doit en outre vous permettre de renforcer la configuration et les stratégies de votre infrastructure de sécurité de façon proactive, ainsi que d'accélérer la détection et les interventions sur incidents grâce à l'orchestration, à l'automatisation et à la synchronisation du renseignement sur les menaces. Des mises à jour régulières à l'aide de données contextuelles priorisées et prétraitées ainsi que la possibilité de bénéficier d'un retour d'informations et d'appliquer les enseignements tirés permettent aux équipes de reprioriser et d'anticiper les menaces afin de réduire les risques actuels et à venir.

CONSIDÉRATIONS IMPORTANTES POUR LA PRISE DE DÉCISION

Au cours du processus de prise de décision, vos équipes de sécurité et la direction devront définir un cahier des charges des exigences techniques et des besoins métier. Cependant, quel que soit le nombre de fonctionnalités identifiées comme critiques, vous devez tenir compte des compromis suivants lors de l'examen des arguments en faveur du développement interne ou de l'achat d'une solution.

RESSOURCES

Votre entreprise dispose-t-elle d'une équipe de développement dédiée ?

Trouver une personne possédant les compétences nécessaires pour concevoir un composant logiciel de base pour une équipe SOC, voire constituer une équipe de développement de taille réduite, est un véritable défi. Et il est encore plus difficile de conserver ces ressources à long terme pour assurer la maintenance en continu et développer de nouvelles fonctionnalités et intégrations, surtout lorsque le projet ne génère pas de revenus directs. Méfiez-vous des plans prévoyant d'« emprunter » les ressources ou de « détourner des cycles de développement » d'un autre département, notamment si vous évoluez dans un environnement où les développeurs peuvent être réaffectés selon les besoins. Le développeur remplaçant devra restructurer le code avant de pouvoir continuer à avancer, ce qui retardera inévitablement le projet, si cela n'y met pas fin.

OBSTACLES FINANCIERS

Avez-vous pris en compte tous les coûts initiaux et de maintenance ?

La constitution d'une équipe pour la prise en charge d'une application développée en interne, aussi simple soit-elle, nécessite au minimum quatre collaborateurs à temps plein : deux développeurs, un administrateur de base de données/Big Data dédié et une ressource chargée de l'assurance qualité (QA). D'aucuns contesteront la nécessité d'une ressource dédiée à l'administration des bases de données/Big Data. Cependant, si vous prenez en compte l'agrégation des sources externes, l'analyse interne (notamment des données sur les logiciels malveillants et sur les vulnérabilités et des facteurs de gestion des risques) et toutes les associations connexes reliant chacun de ces objets, l'ampleur de la tâche apparaît instantanément. Si vous faites l'impasse sur une ressource dédiée et renoncez à une partie des fonctionnalités de la plate-forme de Threat Intelligence, son efficacité sera rapidement limitée, vous empêchant ainsi d'atteindre votre objectif final. Si le coût annuel que représente une telle équipe varie selon les régions et peut sembler raisonnable sur papier, dans la plupart des entreprises, il est bien plus difficile d'augmenter les effectifs que d'acquérir un nouvel outil. En particulier si cet outil présente un coût inférieur, répond à 85-90 % des besoins et inclut le support et les mises à niveau.

DÉCALAGES OPÉRATIONNELS

Vos ressources possèdent-elles une expérience suffisante en développement logiciel et en opérationnalisation du renseignement sur les menaces ?

Le développement logiciel et l'opérationnalisation du renseignement sur les menaces sont deux disciplines très différentes. Le développeur doit maîtriser les architectures logicielles, les activités de développement et les opérations et technologies de sécurité, une palette de compétence extrêmement rare. En pratique, il devra probablement faire appel à un collègue spécialisé dans la sécurité et/ou le renseignement sur les menaces, qui devra soutenir la conception, fournir des explications et servir de « partie prenante finale » du processus de développement. Cependant, cela signifie que ce collègue perdra des cycles de productivité dans le cadre de ses propres responsabilités en tant qu'analyste en sécurité, d'expert en intervention sur incidents ou d'analyste en renseignements sur les menaces.

INNOVATION

Êtes-vous disposé à affecter des ressources permanentes aux demandes de fonctionnalités et aux corrections de bugs ?

Plus la plate-forme de Threat Intelligence sera utilisée, plus les analystes demanderont de nouvelles fonctionnalités, surtout si la plate-forme a pour but d'agréger les renseignements sur les menaces provenant de plusieurs équipes ou départements. Serez-vous en mesure de maintenir une équipe de développement sur le long terme afin d'enrichir la plate-forme ? Qu'adviendra-t-il si des demandes de fonctionnalités sont repoussées en raison de priorités concurrentes ? Disposez-vous des ressources nécessaires pour véritablement favoriser l'innovation, ou aurez-vous constamment une longueur de retard sur les solutions offertes par les entreprises spécialisées dans les plates-formes de Threat Intelligence ? En revanche, les fournisseurs, en particulier ceux qui proposent des abonnements annuels, vous offrent un levier d'achat qui vous permet de vous assurer que la feuille de route du produit correspond toujours à vos besoins et à vos attentes. Le paysage des éditeurs de plates-formes de Threat Intelligence est suffisamment dynamique pour que vous puissiez changer de fournisseur, le cas échéant. Bien qu'aucune migration ne soit simple, la perspective de soustraire un client à un concurrent incite généralement les éditeurs à faire tout ce qui est en leur pouvoir pour faciliter autant que possible la transition.

ASSURANCE QUALITÉ

Votre équipe est-elle en mesure d'effectuer tous les tests système, d'intégration et de régression nécessaires ?

Dans un premier temps, une évaluation du code des développeurs par leurs pairs pourra peut-être suffire, mais cette approche n'est pas évolutive. Au fil du temps, votre plate-forme évoluera inévitablement en robustesse et en sophistication pour répondre à vos besoins. Vous devrez alors mettre en place un processus de contrôle de la qualité normalisé, notamment des tests unitaires standard, des tests de type « écran de fumée », des tests de régression et des tests manuels fastidieux. Sans oublier qu'il vous faudra maintenir plusieurs environnements pour le développement, la mise en service et la production. Vous devez vous préparer à la réalité : plus les analystes de l'équipe exploiteront la plate-forme de Threat Intelligence et s'appuieront sur elle, plus le volume de code augmentera et plus les corrections de code ponctuelles finiront par nécessiter des efforts de refactorisation considérables. Cette tâche détournera par ailleurs du temps nécessaire pour traiter la liste déjà longue de nouvelles fonctionnalités en attente, engendrant ainsi des frictions entre les équipes. Une fois arrivé à ce stade, vous devez être conscient du fait que le développeur initial possède désormais des compétences de développement en Threat Intelligence extrêmement prisées qui ne manqueront pas d'attirer la convoitise d'autres entreprises. Il serait judicieux d'envisager le recrutement d'un troisième développeur et d'un deuxième ingénieur QA pour assurer la redondance en cas de débauchage de l'un ou plusieurs d'entre eux.

INTÉGRATION

Votre équipe est-elle qualifiée pour réaliser toutes les intégrations actuelles et à venir dans des délais raisonnables ?

La plupart des entreprises traitent des millions de données sur les menaces issues de sources commerciales, d'open sources et de divers éditeurs de solutions de sécurité. Ajoutons à cela les volumes considérables de données de journaux et d'événements provenant de chaque produit individuel intégré à votre système de protection et/ou à votre SIEM. L'agrégation de ces données dans votre plate-forme et leur conversion en un format uniforme exploitable représentent une tâche gigantesque et extrêmement complexe qui nécessite un administrateur de bases de données à temps plein. Il s'agit également d'appliquer les données de Threat Intelligence pertinentes que vous souhaitez déployer aux technologies appropriées de votre sensor grid, ce qui implique de les intégrer à votre pare-feu, à votre système de prévention d'intrusions (IPS), à votre système de détection d'intrusions (IDS), à votre système NetFlow, à votre solution de protection des terminaux, etc. La gestion des particularités des intégrations représente sans aucun doute une tâche à plein temps.

TEMPS

Disposez-vous d'une estimation réaliste des délais de développement et de déploiement ?

Comparez le temps nécessaire pour concevoir, élaborer et développer correctement une plate-forme au temps que prennent l'évaluation de solutions tierces, ainsi que la sélection, la preuve de concept et le processus de mise en œuvre avec l'aide d'un fournisseur. Pensez également au temps dont votre équipe aura probablement besoin pour reconstruire l'application développée en interne, afin de prendre en compte les obstacles cachés qui émergent plusieurs mois plus tard lorsque les concepts et les calculs théoriques ne se traduisent pas en routines opérationnelles. Toute divergence entraîne des retards supplémentaires pendant lesquels votre programme d'opérationnalisation du renseignement sur les menaces est inefficace, et offre aux hackers une plus grande fenêtre d'opportunité pour lancer des attaques.

RISQUES

Quels risques êtes-vous disposé à accepter pour un développement interne ?

L'objectif final est de réduire les risques de cybersécurité. Il n'est pas toujours facile d'évaluer les performances et la capacité de réduction des risques d'une solution développée en interne par rapport à une plate-forme commerciale. Il n'existe pas de données de référence pour les solutions propriétaires ; ces solutions ne font pas l'objet de tests indépendants permettant de valider les performances, de garantir les meilleures pratiques en matière de programmation et d'évaluer en permanence les outils sous licence open source intégrés. Par ailleurs, elles ne font généralement pas l'objet de contrats de niveau de service. De plus, si un hacker s'attaque à l'application développée en interne, les opérations visant à rétablir la situation sont naturellement plus chronophages que s'il s'agit d'une solution commerciale. En effet, vous devez non seulement intervenir sur l'incident mais également combler les éventuelles failles de la solution susceptibles d'avoir contribué au succès de l'attaque.

GESTION DES FOURNISSEURS

Souhaitez-vous un point de contact unique pour les mises à jour de la plate-forme et les feuilles de route du produit ?

Qu'il s'agisse de travailler en collaboration sur une nouvelle fonctionnalité de pointe ou de résoudre un problème, il est toujours plus facile de traiter avec un fournisseur que de licencier ou de recruter un employé.
Le responsable du SOC est généralement le propriétaire principal de la plate-forme de Threat Intelligence. À ce titre, il passe généralement 60 % de son temps à arbitrer les rapports humains, 20 % à servir de traducteur pour la direction et 20 % à régler les problèmes techniques. Ces 60 % ne feront qu'augmenter si le responsable de votre SOC doit gérer encore plus de problèmes d'effectifs, réduisant ainsi le temps qu'il consacre à d'autres activités plus importantes.

CONCLUSION

Votre capacité à accélérer les opérations de sécurité dans le cadre d'un programme rationalisé de gestion et d'opérationnalisation du renseignement sur les menaces est fonction de l'outil chargé d'unifier les données sur les menaces, l'analyse et les mesures qui en découlent. En parcourant cette liste de considérations, comparez les prévisions de coûts associées à l'affectation de plusieurs employés à temps plein à la gestion continue d'une plate-forme développée en interne par rapport à l'achat d'une solution logicielle. Prenez également en compte les coûts d'opportunité et les risques liés au détournement des ressources de sécurité des premières lignes vers les tâches de développement. Quelle que soit la décision prise par une entreprise, celle-ci doit être guidée par une stratégie de maturation capable de s'adapter à l'évolution de l'entreprise et du paysage des menaces.

À PROPOS DE L'AUTEUR

En tant que cofondateur et Directeur des technologies de ThreatQuotient, Ryan Trost s'appuie sur plus de 15 années d'expérience dans la sécurité consacrées à la détection des intrusions et à la cyberveille de sécurité pour promouvoir la réflexion et des discussions autour de produits innovants. Leader reconnu du secteur de la cybersécurité, Ryan intervient fréquemment lors de conférences sur la sécurité telles que BlackHat, DEFCON, SANS, HTCIA (High Technology Crime Investigation Association) et FIRST. Il est l'auteur de l'ouvrage « Practical Intrusion Analysis » (Analyse pratique des intrusions) et a développé l'un des premiers algorithmes géospatiaux de détection des intrusions utilisés pour identifier les modèles d'attaque par géolocalisation. Avant de cofonder ThreatQuotient, Ryan a dirigé plusieurs SOC commerciaux et rattachés au gouvernement fédéral américain, et a occupé le poste de Directeur de la sécurité et Responsable de la protection de la vie privée pour un établissement de soins de santé de taille moyenne de Virginie du Nord. Il préside également le conseil consultatif en charge du programme du diplôme en cybersécurité du Northern Virginia Community College.

À PROPOS DE THREATQUOTIENT™

ThreatQuotient sait parfaitement qu'une sécurité axée sur les renseignements repose essentiellement sur les ressources humaines. Grâce à ThreatQ™, sa plate-forme de Threat Intelligence ouverte et extensible, les acteurs de la cybersécurité ont l'assurance que les renseignements sur les menaces pertinents sont utilisés par les bons outils, au moment opportun. Adoptée par de nombreuses entreprises de premier plan à travers le monde, elle est au cœur même de leur système de gestion et d'opérationnalisation du renseignement sur les menaces. L'ensemble de leur dispositif de sécurité gagne ainsi en performances et en efficacité.

Pour plus d'informations, consultez le site threatq.com.

TQ_Build-vs-Buy_Rev1