Validation économique ESG

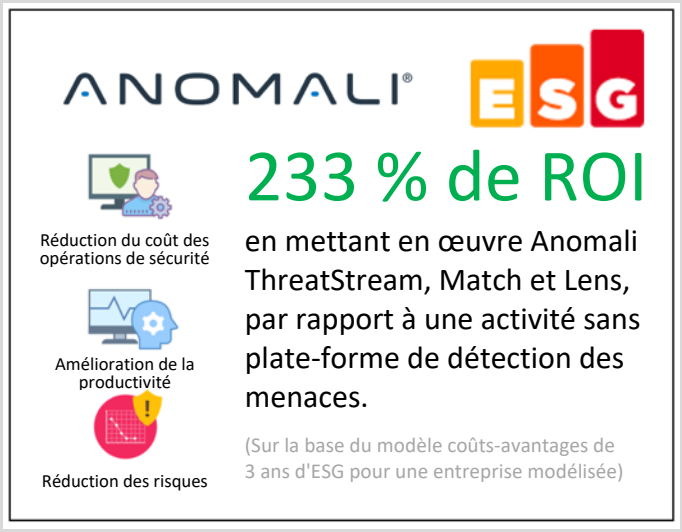
Analyse des avantages économiques de la plate-forme de renseignements sur les menaces

Par Aviv Kaufmann et Alex Arcilla, analystes de validation senior

Juillet 2020

Résumé

Il n'a jamais été aussi important pour les entreprises de donner aux employés de plus en plus éloignés l'accès aux applications et aux ressources dans une variété de régions géographiques et sur divers réseaux et appareils. Les entreprises ont été obligées de mettre en œuvre rapidement des solutions, d'assouplir les restrictions et les politiques et de supprimer les barrières à l'entrée. Il en résulte un alourdissement de la charge de travail de leurs équipes de sécurité pour un fonctionnement efficace permettant de protéger l'organisation et ses ressources. Les équipes de sécurité doivent travailler de manière plus intelligente et plus efficace pour intégrer autant d'informations sur les menaces que possible afin d'identifier les menaces et d'y remédier.



ESG a confirmé que la suite de produits de sécurité basés sur les renseignements d'Anomali a contribué à rationaliser les opérations de sécurité, à automatiser les flux de travail, à réduire les faux positifs, à améliorer la collaboration interne et externe et à réduire les délais de détection et de correction. Au fil d'une série d'entretiens, ESG a validé les avantages dont les clients d'Anomali ont bénéficié. ESG a ensuite utilisé ces informations pour créer un scénario modélisé qui montre comment une entreprise peut économiser 98 000 € par mois grâce à une meilleure productivité, à l'évitement des risques et à la valeur ajoutée des produits inclus. Le modèle d'ESG prévoit un retour sur investissement de 233 % et un délai de rentabilisation de seulement 11 mois pour une entreprise comportant une équipe de sécurité de 10 personnes qui choisit de mettre en œuvre Anomali plutôt que de continuer à fonctionner sans plate-forme de renseignements sur les menaces.

Introduction

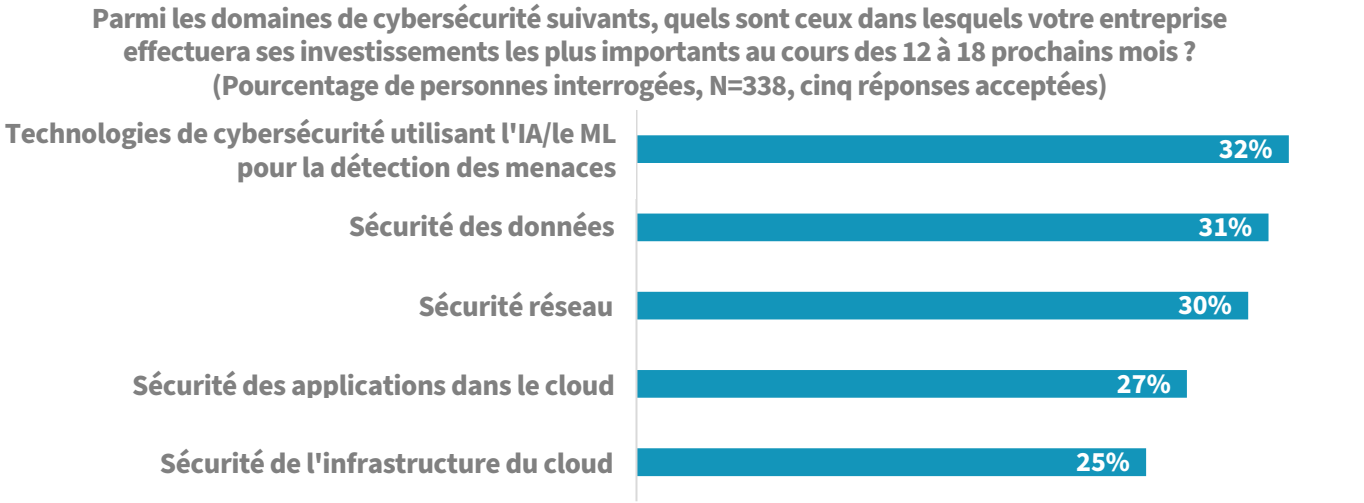
Cette validation économique ESG s'est axée sur les avantages quantitatifs et qualitatifs que les entreprises peuvent attendre en dotant leurs équipes de la suite de produits de sécurité basés sur les renseignements d'Anomali pour analyser, détecter et étudier les menaces potentielles et y répondre plus rapidement et plus efficacement. Ces produits comprennent Anomali ThreatStream (plate-forme de renseignements sur les menaces), Anomali Match (détection des menaces) et Anomali Lens (connaissance des menaces).

Défis

La cybersécurité est une préoccupation majeure pour toute entreprise. Les équipes chargées des opérations de sécurité ont évolué, passant d'une réponse réactive aux alertes et aux failles de sécurité à l'exploitation proactive des volumes toujours plus grands de renseignements sur les menaces, afin de maintenir une meilleure protection. Une étude ESG montre que 62 % des entreprises prévoient d'augmenter leurs dépenses en matière de services de cybersécurité au cours des 12 à 18 prochains mois.[1] La disponibilité de tant de sources de renseignements sur les menaces pèse sur les professionnels de la sécurité, qui ont du mal à trouver des moyens efficaces d'intégrer, de gérer, d'analyser ces renseignements et de prendre des mesures appropriées en conséquence. Ces entreprises n'auront tout simplement jamais les ressources humaines nécessaires pour utiliser toutes les informations dont elles disposent. L'automatisation et l'analyse sont nécessaires pour hiérarchiser et extraire efficacement les informations exploitables dans la masse sans cesse croissante des renseignements sur les menaces.

Au fil du temps, de nombreuses grandes entreprises ont déployé un large éventail de technologies de sécurité et ont développé leur équipe de professionnels de la sécurité pour prendre en charge ces solutions. La mise en œuvre d'un centre d'opérations de sécurité (SOC) a permis à ces équipes de mettre en commun leurs connaissances et leur expérience afin de mieux gérer la détection et la réponse aux menaces. Les experts en sécurité sont cependant une ressource limitée, difficile et coûteuse à trouver, à former et à conserver. De même, le déploiement de systèmes de gestion des informations et des événements de sécurité (SIEM) promet une détection plus efficace des menaces en consolidant les renseignements et les informations générés par un certain nombre de serveurs et de périphériques. Toutefois, les SIEM sont limités par le volume de données qu'ils peuvent rechercher et gérer efficacement. Ils produisent beaucoup de faux positifs qui nécessitent l'attention de l'équipe, ce qui limite la visibilité de l'entreprise sur les menaces. Il n'est donc pas surprenant que les entreprises cherchent à aider leurs équipes de SOC surchargées à mieux identifier les véritables menaces et à accélérer leur réponse face à ces menaces. L'étude ESG identifie l'utilisation de technologies qui s'appuient sur l'intelligence artificielle (IA) et le Machine Learning (ML, dit « apprentissage automatique ») pour la détection des menaces comme le domaine de cybersécurité le plus souvent cité parmi ceux dans lesquels les entreprises investiront le plus en 2020 (voir Figure 1).

Figure 1. Les 5 priorités en matière de dépenses en cybersécurité en 2020



Source : Enterprise Strategy Group

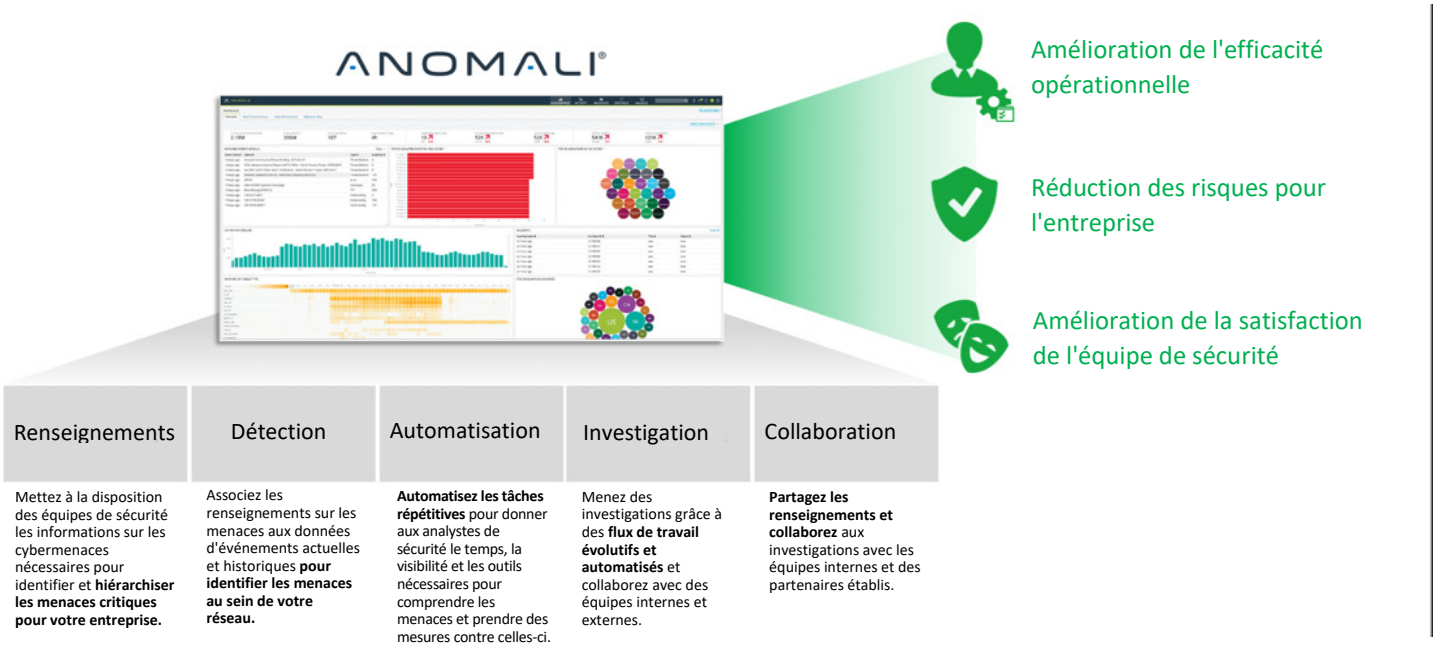
[1] Source : Résultats de l'enquête ESG Master Survey, *Enquête 2020 sur les intentions de dépenses consacrées aux technologies*, janvier 2020. Toutes les références et tous les graphiques de l'étude d'ESG inclus dans cette validation économique sont issus de l'ensemble des résultats obtenus au cours de cette enquête Master Survey.

Bien que la disponibilité d'énormes volumes de renseignements sur les menaces et de systèmes de télémétrie tienne la promesse d'une meilleure sécurité, une protection plus efficace ne peut être obtenue que lorsque les entreprises sont mieux à même de libérer et d'optimiser la communication entre leurs atouts les plus précieux, c'est à dire leur SOC et leurs collaborateurs travaillant sur la cybersécurité.

La solution d'Anomali

Anomali propose une suite de produits de sécurité basés sur les renseignements qui offrent une visibilité inégalée sur les menaces, une détection accélérée, une réponse plus rapide et une productivité accrue. Les produits Anomali aident les entreprises à automatiser la collecte, la gestion et le déploiement de plusieurs flux internes et externes de renseignements sur les menaces, à filtrer les faux positifs, à identifier les menaces dans leurs environnements et à agir plus efficacement pour se concentrer sur les besoins de sécurité les plus importants.

Figure 2. La plate-forme de renseignements sur les menaces d'Anomali



Source : Enterprise Strategy Group

Anomali peut être déployé dans le cloud, sur site ou isolé (sur site, mais déconnecté des données publiques). La plate-forme se compose de trois produits principaux : Anomali ThreatStream, Anomali Match et Anomali Lens.

Anomali ThreatStream – Unifie les données et les informations relatives aux menaces en renseignements haute-fidélité, les diffuse automatiquement vers les contrôles de sécurité et intègre une suite d'outils de recherche permettant d'effectuer des investigations efficaces sur les menaces. ThreatStream automatise la collecte de renseignements sur les menaces provenant de centaines de sources externes et internes, y compris les renseignements Open Source et les flux commerciaux sur les menaces, les renseignements partagés et l'intelligence interne issue des investigations, des alertes de sandbox, etc. Le produit normalise et déduplique ces flux en une taxonomie commune, en utilisant des algorithmes d'apprentissage automatique pour supprimer les faux positifs, enrichir les données et évaluer le niveau de risque de ces renseignements en termes de gravité et de confiance. ThreatStream met ensuite en œuvre les renseignements via la distribution automatisée d'indicateurs de menace lisibles par machine aux contrôles de sécurité (par exemple, SIEM, pare-feu, EDR, IPS, SOAR, etc.). Le produit fournit également aux analystes et aux équipes de SOC des outils permettant d'effectuer des investigations basées sur des modèles à l'aide des frameworks Diamond, Kill Chain, STIX ou MITRE ATT&CK. L'atelier d'investigations comprend un ensemble complet de sources d'enrichissement des données, un puissant outil d'exploration visuelle pour l'expansion et le pivotement des indicateurs, une détonation intégrée des sandbox pour les URL de programmes malveillants et de phishing, ainsi que la collaboration, la rédaction et la publication de bulletins de menace.

Anomali Match – Automatise la détection des menaces sur le réseau en mettant en corrélation tous les renseignements disponibles sur les menaces avec tous les journaux d'activité du réseau. Pour ce faire, Match indexe tous les journaux SIEM et d'autres sources d'événements afin de maintenir un an ou plus de données historiques, analysées en continu par rapport aux renseignements sur les menaces existantes et nouvelles. Il fournit également des alertes automatiques aux systèmes SIEM, SOAR ou de tickets pour répondre et remédier à ces menaces. L'analyse en temps réel permet aux analystes de suivre les preuves de violations passées jusqu'au « patient zéro », de rechercher des menaces en fonction de l'acteur, de la vulnérabilité ou des TTP, ainsi que de hiérarchiser les réponses selon le niveau de risque et la criticité des ressources.

Anomali Lens – Fournit des renseignements sur les menaces à portée de main grâce à l'identification automatique des données de menace dans tout contenu Web par traitement du langage naturel (NLP). Pour ce faire, Lens analyse les pages Web, les plates-formes de médias sociaux, les SIEM et d'autres journaux de sécurité afin d'identifier des indicateurs de compromis (IOC), des acteurs de menaces, des familles de programmes malveillants et des techniques d'attaque. Les renseignements sur les menaces identifiés par Lens sont automatiquement mis en correspondance avec le framework MITRE ATT&CK et peuvent être importés dans Anomali ThreatStream en vue d'une investigation et d'une analyse plus approfondies en cliquant simplement sur un bouton. Lens s'intègre également à Anomali Match pour mettre en évidence les renseignements sur les menaces analysés qui sont présents sur le réseau, ce qui permet d'en comprendre instantanément le niveau de gravité et l'impact sur votre environnement.

Validation économique ESG

ESG a réalisé une validation économique quantitative et modélisé l'analyse de la suite de produits Anomali.

Le processus de validation économique d'ESG est une méthode éprouvée pour comprendre, valider, quantifier et modéliser les propositions de valeur économique d'un produit ou d'une solution. Le processus tire parti des compétences fondamentales d'ESG dans l'analyse du marché et de l'industrie, la recherche prospective et la validation technique et économique. ESG a examiné les résultats d'études de cas et d'investigations auprès des utilisateurs finaux et mené des entretiens approfondis avec ces derniers afin de mieux comprendre et quantifier l'impact d'Anomali sur leur entreprise, en particulier par rapport à la manière dont elle fonctionnait avant de déployer Anomali ou d'autres expériences dans d'autres organisations. Les résultats qualitatifs et quantitatifs ont servi de base à un modèle de retour sur investissement simple comparant les économies et les avantages que peut attendre une entreprise modélisée par rapport au coût attendu du déploiement d'Anomali.

Présentation économique d'Anomali

L'analyse économique d'ESG a révélé que les clients qui avaient déployé Anomali étaient très satisfaits du produit et estimaient qu'ils avaient grandement rationalisé leurs opérations de sécurité, qu'ils étaient plus efficaces et qu'ils protégeaient mieux l'entreprise. ESG a constaté qu'Anomali offrait à ses clients des économies et des avantages significatifs dans les catégories suivantes :

- Réduction du coût d'exploitation des opérations de sécurité – Les entreprises ont considérablement rationalisé leurs opérations de sécurité et amélioré l'utilisation de leurs ressources de sécurité grâce aux capacités d'automatisation et d'orchestration d'Anomali, ainsi qu'à ses outils et fonctionnalités de sécurité, bien conçus et efficaces.

- Amélioration de l'efficacité de la sécurité et réduction des risques pour l'entreprise – Les clients ont signalé qu'Anomali avait contribué à mieux armer l'équipe de sécurité et à opérationnaliser le processus de sécurité, en rendant les équipes plus efficaces et en réduisant le délai d'identification et de résolution des problèmes de sécurité.

- Amélioration de la productivité et de la satisfaction liées aux opérations de sécurité – Anomali contribue à améliorer la productivité et la satisfaction des professionnels de la sécurité en automatisant les tâches répétitives ou chronophages, ce qui leur permet de se concentrer sur des opérations de sécurité à plus forte valeur ajoutée. Les compétences, la collaboration et la visibilité sont rapidement améliorées et la valeur synergique avec d'autres produits de sécurité est amplifiée.

Réduction du coût d'exploitation des opérations de sécurité

ESG a constaté que les équipes de sécurité qui ont déployé les produits Anomali indiquent que leurs opérations de sécurité sont beaucoup plus simples grâce à l'opérationnalisation, à l'automatisation et à l'orchestration. Les utilisateurs ont signalé un gain de temps significatif ou des délais considérablement réduits dans un certain nombre de domaines, notamment le déploiement de nouvelles technologies, la recherche de menaces, l'amélioration des données, la réponse aux faux positifs et la mise en corrélation des informations provenant de plusieurs sources (ainsi que dans de nombreux autres domaines). Cela a permis aux équipes de tirer le meilleur parti de chaque analyste de la sécurité, d'améliorer les capacités des analystes juniors, d'accélérer l'intégration et de réduire le temps passé sur les tâches à faible valeur ajoutée. Ainsi, elles ont pu se concentrer sur les activités à plus forte valeur, telles que la correction.

- **Réduction de la complexité administrative** – Les clients ont signalé que ThreatStream a réduit la complexité administrative liée à la gestion de plusieurs flux de renseignements sur les menaces de sécurité et de produits de sécurité ponctuels : moins d'interfaces à gérer, des essais simples de type boutique d'applications, le déploiement de nouveaux flux premium et la gestion intégrée des IOC. Cela a permis aux entreprises de gagner du temps et d'éviter de devoir déployer, gérer et intégrer de multiples produits avec plusieurs interfaces différentes.
- **Délai de rentabilisation plus court –** Le déploiement de ThreatStream s'est révélé rapide et facile pour les entreprises, tout comme l'intégration avec les IOC et l'ajout ou la suppression de flux premium. Le solide écosystème de partenaires et les kits de développement logiciel (SDK) ont permis aux entreprises d'intégrer rapidement les outils et flux internes et externes de renseignements sur les menaces qui répondent le mieux à leurs besoins. Les options « Freemium » permettent aux clients de s'abonner à des flux de renseignements commerciaux de partenaires afin de mieux optimiser leurs programmes de renseignements sur les menaces. Les achats ont été simplifiés et les entreprises ont estimé qu'elles passaient moins de temps à traiter les questions d'intégration et de support. Cela signifie que les entreprises ont pu tester et intégrer plus rapidement des stratégies et des outils de sécurité. Un client a commenté : « Anomali nous fait gagner du temps et nous facilite la vie pour trouver et installer des flux ; nous savons qu'ils sont déjà configurés et prêts à fonctionner sans intégration nécessaire, ce qui nous fait gagner des heures, voire des jours en fonction de la complexité. »

« Je pouvais passer des heures à chercher et recueillir du contexte. Avec Anomali, je peux simplement saisir l'URL ou utiliser un pivotement Lens et savoir exactement quelles actions de confinement mettre en œuvre. »

- **Flux de travail rationalisé** – Anomali a aidé les entreprises à rationaliser leurs flux de travail de sécurité afin de réduire le temps consacré aux investigations par les équipes SOC, CTI et de réponse aux incidents en les regroupant sur une seule plate-forme. Des flux de travail simplifiés, une intégration étroite avec d'autres flux et solutions de sécurité et l'enrichissement des renseignements et recherches sur les menaces ont permis de réduire le temps passé par les membres de l'équipe de sécurité sur tous les aspects de détection, d'investigation et de réponse aux menaces.
- **Automatisation des tâches** – Les utilisateurs ont signalé une réduction substantielle du nombre tâches manuelles après le déploiement de ThreatStream. Anomali a automatisé un grand nombre des tâches répétitives ou chronophages qui occupent la plus grande partie de la journée des analystes de sécurité, notamment la normalisation des sources, l'enquête et la compréhension du profil de risque, le formatage et l'enrichissement des renseignements sur les menaces, ainsi que la création de rapports. Anomali a également orchestré de nombreuses tâches liées à la configuration, à l'intégration et à la sécurité bidirectionnelle entre des solutions de sécurité comme les SIEM, les pare-feux et les périphériques réseau. Selon des utilisateurs d'Anomali, le traitement des informations de journal d'un client aurait nécessité jusqu'à 2,5 fois plus de personnes sans Anomali Match : « Nous avons quatre personnes pour faire un travail qui aurait autrement occupé peut-être dix personnes. »

« Pour une tâche qui aurait autrement nécessité de restaurer les journaux SIEM à partir de bandes, il faudrait plus de 2 semaines pour répondre à une demande, ce qu'Anomali Match nous a permis de faire en moins d'une heure. »

- **Moins de temps perdu –** Les entreprises qui avaient déployé Anomali ont déclaré qu'elles avaient désormais beaucoup moins de faux positifs à traiter et qu'elles souffraient beaucoup moins de « fatigue d'alerte ». Les utilisateurs ont estimé que cela leur a donné plus de temps pour se concentrer sur des tâches plus importantes. L'automatisation de la recherche et de l'enrichissement des renseignements sur les menaces a permis de réduire le temps passé à essayer de comprendre la situation, le risque d'avoir à répéter des tâches et le dépannage dû à des erreurs humaines. Un utilisateur a expliqué : « Je n'ai pas besoin de partir à la chasse aux menaces ni d'essayer de comprendre ce qu'un indicateur signifie ou pourquoi il est de mauvais augure, ce qui représentait environ 90 % de mon travail auparavant. »

Amélioration de l'efficacité de la sécurité et réduction des risques pour l'entreprise

Anomali travaille en association avec d'autres produits de sécurité pour fournir une solution rationalisée plus efficace pour identifier les IOC, réduire les faux positifs et fournir un contexte et des informations permettant de comprendre et de corriger les menaces. Les clients que nous avons interrogés pensent qu'Anomali a considérablement amélioré l'efficacité globale de leurs opérations de sécurité, certains estimant qu'Anomali les a rendus jusqu'à 90 % plus efficaces pour identifier et corriger les menaces.

- **Délai de connaissance plus court** – Les utilisateurs finaux ont jugé qu'Anomali, lorsqu'il était utilisé conjointement avec leurs autres outils, leur a permis de bénéficier d'un délai de connaissance nettement plus court. Les clients ont indiqué une plus grande agilité des flux, une meilleure visibilité et des données enrichies par les IOC, ce qui a permis d'accélérer le délai de sensibilisation et la détection des menaces, cela se traduisant par une amélioration du temps moyen de réponse (MTTR) et de la résolution des problèmes. Un utilisateur a signalé qu'Anomali Match a contribué à améliorer le MTTR de plus de neuf jours à seulement dix minutes pour valider les IOC. Les clients ont convenu qu'Anomali leur a permis de détecter, d'étudier et de corriger un plus grand nombre et une plus grande variété de menaces et d'IOC en moins de temps.

« Sans Anomali, nous serions passés à côté d'un grand nombre de menaces ou il nous aurait fallu beaucoup plus de temps pour les identifier et les corriger. C'est devenu un élément essentiel de notre surveillance de sécurité. »

- **Intelligence basée sur l'apprentissage automatique** – Anomali utilise des algorithmes d'apprentissage automatique pour enrichir le contexte des menaces, aider à hiérarchiser les menaces et effectuer une évaluation historique des événements. Les entreprises disposent ainsi d'une intelligence plus globale, plus efficace et plus rapide que ce qui pourrait être réalisé après des heures de travail humain. Les équipes ont indiqué que cela les avait aidées à identifier, rechercher et répondre aux menaces beaucoup plus rapidement et que leur équipe chargée des opérations de sécurité était désormais beaucoup plus efficace qu'auparavant. Un utilisateur a commenté : « Avec Anomali, c'est la première fois que nous pouvons accroître et gérer de manière exponentielle notre capacité à recueillir et incorporer des informations à partir d'Internet, au point que l'humain ne constitue plus une limite. »

- **Davantage de traitement des renseignements sur les menaces** – ThreatStream a permis aux équipes de traiter un plus grand volume et une plus grande variété de renseignements sur les menaces qu'auparavant. Elles ont pu tester et gérer davantage de flux externes, ainsi que les associer à des bulletins sur les menaces en temps quasi réel et à des renseignements sur les menaces générés en interne. La possibilité d'effectuer le profilage des acteurs de menaces et de suivre un acteur sur une période plus longue a été extrêmement précieuse. Un client a confié : « D'autres TIP sur le marché permettent de réaliser des tâches comme collecter des flux et effectuer des corrélations, mais Anomali nous apporte vraiment de la valeur en nous donnant également la possibilité d'acquérir nos propres données. »

- **Réponse de sécurité plus efficace** – Tous les utilisateurs que nous avons interrogés ont convenu qu'Anomali les a aidés à réagir beaucoup plus efficacement aux menaces de sécurité. ThreatStream a non seulement permis de traiter un plus grand volume de renseignements et d'identifier les menaces plus rapidement, mais également de réduire considérablement le travail des analystes grâce à l'automatisation de la mise à jour des flux, de la corrélation des indicateurs et de l'analyse des violations afin de comprendre quelles informations sont liées et de suggérer des actions de recherche et de correction en amont. Un client a indiqué : « Plutôt que la simple indication qu'une adresse IP est hostile, je peux voir pourquoi elle l'est, quelle activité elle générait et quelles mesures je dois prendre. »

« Au lieu de devoir vérifier moi-même chacun de ces courriels ou chacune de ces adresses IP, je peux obtenir une vue globale et voir que 90 % d'entre eux proviennent d'une violation, d'un type d'indicateur ou d'une étiquette. »

Pourquoi est-ce important ?

Chaque entreprise a pour objectif d'assurer une sécurité plus efficace de ses activités.

Les clients d'Anomali ont jugé qu'Anomali s'était montré jusqu'à 90 % plus efficace pour identifier et corriger les menaces. Une entreprise a indiqué que grâce à Anomali elle avait évité plus de 400 000 $ de crédits d'utilisateur volés par l'identification et la prise des mesures inter-fonctionnelles de manière proactive pour protéger les comptes des utilisateurs d'une tentative de violation.

- **Prise de décisions plus éclairées en matière de sécurité** – Les utilisateurs ont indiqué qu'Anomali offre un certain nombre de tableaux de bord simples mais efficaces pour aider les équipes à visualiser les menaces, à hiérarchiser la prise de décisions et à partager des informations avec d'autres équipes de manière utile. Les fonctionnalités de sandbox intégrées, la disponibilité des équipes d'experts en renseignements sur les menaces d'Anomali et la possibilité de partager des informations avec des pairs ont contribué à fournir des informations supplémentaires utiles pour prendre des décisions internes. Les utilisateurs ont convenu qu'Anomali permettait de prendre des décisions plus éclairées et plus rapides, contribuant ainsi à réduire les risques pour l'entreprise.

Amélioration de la productivité et de la satisfaction liées aux opérations de sécurité

Toutes les entreprises que nous avons interrogées ont estimé qu'Anomali les avait aidées à transformer leur organisation pour tirer le meilleur parti des ressources dont elles disposaient. Elles ont indiqué que leurs équipes étaient beaucoup plus productives, mais aussi qu'elles étaient plus satisfaites de leurs fonctions et que l'organisation était mieux en mesure de communiquer avec le marché et ses pairs.

- **Des professionnels de la sécurité plus productifs** – ThreatStream permet à chacun d'être plus productif et de se concentrer sur les domaines apportant le plus de valeur ajoutée. Les équipes ont signalé que les membres moins expérimentés s'intégraient et contribuaient à l'activité plus tôt, apprenaient plus vite et gagnaient rapidement plus d'expérience à des postes à plus forte valeur ajoutée. C'est un avantage pour l'entreprise comme pour la carrière de l'individu.

« Avec Anomali, nous affectons deux personnes à un travail auquel [entreprise nommée] consacre une très grande équipe, et nous le faisons mieux. »

- **Équipe de sécurité plus satisfaite** – Les utilisateurs finaux ont indiqué qu'avec l'aide que leur apporte Anomali pour faire un meilleur travail, ils dorment mieux la nuit, progressent plus rapidement dans leur carrière et ont le sentiment d'en avoir fait davantage pour protéger l'entreprise. Dans l'ensemble, ils ont indiqué qu'ils considèrent désormais leur travail comme une expérience plus positive. Les entreprises ont estimé qu'Anomali les a aidées à renforcer leur équipe et à créer un environnement où il est plus facile de retenir les employés, dans un secteur où il est difficile de trouver et conserver les talents.

- **Amélioration des processus métiers –** Les clients ont indiqué que ThreatStream leur a permis de mieux partager les informations entre les organisations de sécurité et a favorisé des discussions beaucoup plus efficaces entre les équipes de sécurité, les unités commerciales et les utilisateurs finaux. Une entreprise a ajouté : « Nous avons pu développer des processus vraiment utiles autour d'Anomali. Nous avons travaillé avec notre équipe de lutte contre la fraude, notre équipe rouge (de test), notre équipe de renseignements sur les menaces et même avec notre équipe en charge de la conformité, et nous leur avons donné un aperçu de ce que nous voyons réellement. » Les clients ont eu l'impression d'avoir mieux informé leurs utilisateurs, car ils étaient mieux à même de montrer facilement quelles menaces étaient observées. Ils considèrent que, sans Anomali, ils n'auraient pas pu communiquer sur leurs activités sans passer des heures à écrire des explications détaillées.

« Anomali améliore certains des processus qui étaient déjà en place, mais nous offre également de nouvelles possibilités parce que nous sommes en mesure de communiquer de manière plus efficace. »

- **Une meilleure collaboration avec les pairs** – Les clients ont estimé qu'Anomali leur avait fourni un moyen fiable de partager les informations sur les menaces collectées en interne et les suggestions de résolution avec des groupes de pairs. Cela permet à l'entreprise de contribuer ou même d'être reconnue comme leader parmi ses pairs tout en rendant le groupe de pairs plus efficace pour identifier et corriger les menaces. Elle gagne également un temps précieux en s'évitant la répétition d'investigations déjà effectuées par d'autres. Un client a confié : « Pouvoir partager des renseignements avec d'autres groupes a été extrêmement utile… Nous n'avons pas besoin de creuser aussi loin ou d'apprendre de nos erreurs parfois car nous sommes capables de partager des renseignements. »

Analyse ESG

ESG a tiré parti des informations recueillies grâce à des documents des fournisseurs, aux connaissances publiques et sectorielles en matière d'économie et de technologies, ainsi que des résultats d'entretiens avec des clients pour créer un modèle de retour sur investissement sur trois ans qui compare les coûts et les avantages de la mise en œuvre d'Anomali ThreatStream, Match et Lens par rapport à une activité sans aucune plate-forme d'analyse et de détection des menaces. Les entretiens d'ESG avec les clients d'Anomali, associés à son expérience et son expertise en modélisation économique et validation technique des produits d'Anomali ont contribué à former la base de notre scénario modélisé.

L'entreprise modélisée par ESG se composait d'une équipe de 10 analystes de renseignements sur les menaces ayant divers degrés d'expérience dans les services de sécurité pour une entreprise de 1 500 employés. ESG a pris en compte le coût prévu d'installation, de mise en œuvre et de formation des employés à l'utilisation de la plate-forme Anomali, ainsi que les coûts d'abonnement annuels, les nœuds matériels, les coûts d'infrastructure, le support et la maintenance sur une période de trois ans.

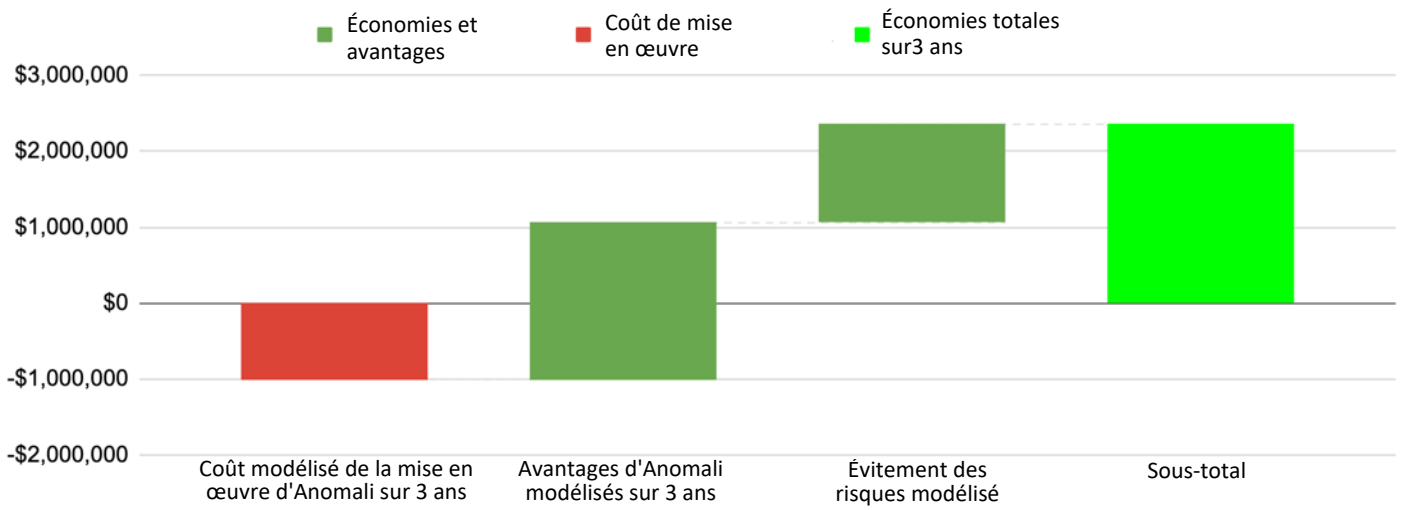
Du côté des avantages, ESG a modélisé le coût évité ou le bénéfice attendu d'une amélioration de la productivité au sein de l'équipe de sécurité, sur la base d'une amélioration prévue de 20 à 70 % sur les tâches liées à la gestion des flux, aux investigations et au reporting de leurs résultats, à l'intégration avec d'autres systèmes de sécurité, au partage des renseignements sur les menaces avec des organisations partenaires ainsi qu'en interne à l'échelle de l'entreprise. D'après les estimations prudentes d'ESG, seulement 35 % du nombre total d'heures de travail de l'équipe de sécurité était consacré à ces tâches. Le modèle d'ESG a permis une amélioration de 58 % de la productivité dans la réalisation de ces tâches et une économie totale de 969 000 $ sur trois ans. Ces économies se manifestent sous la forme d'heures de travail désormais disponibles pour des tâches de sécurité supplémentaires qui n'étaient pas réalisées avant Anomali.

Les modèles d'ESG ont indiqué des économies de coûts attendues grâce à une réduction de 40 % des faux positifs (608 000 $), de la valeur associée aux produits de sécurité fournis par Anomali (sandbox, freemium et flux de renseignements sur les menaces premium, support réactif d'Anomali et formation par Anomali University) pour une valeur totale de 452 000 $, ainsi que d'autres économies réalisées sur des coûts non nécessaires comme des services professionnels, de la formation et de la certification, de même que l'approvisionnement et l'intégration simplifiés (53 000 $).

ESG a également modélisé les risques évités grâce à une probabilité moindre de violation des données découlant d'une plus grande chance de détection précoce, d'une efficacité totale accrue et d'une résolution plus rapide des problèmes, ainsi qu'une réduction des coûts attendus d'une violation de données, grâce à la possibilité de détecter et d'exécuter des actions automatisées plus rapidement et plus efficacement. Les hypothèses de probabilité et de coûts d'une violation de

données formulées par ESG sont basées sur des données publiques publiées par le Ponemon Institute. ESG a calculé qu'Anomali pouvait réduire les risques pour une entreprise, évitant ainsi jusqu'à 1 292 000 dollars sur trois ans en coûts attendus d'une violation de données. Les résultats de l'analyse coûts-avantages modélisée d'ESG sont présentés dans la figure 3.

Figure 3. Résultats de l'analyse coûts-avantages sur trois ans d'ESG sur la plate-forme de renseignements sur les menaces d'Anomali



Source : Enterprise Strategy Group

Signification des chiffres

L'analyse modélisée d'ESG a prédit des économies et des avantages substantiels pour notre entreprise modélisée. Bien qu'aucun scénario modélisé ne puisse jamais représenter précisément l'économie générée par chaque déploiement, ESG encourage les entreprises à effectuer leur propre analyse pour voir combien elles peuvent économiser. ESG suggère aux entreprises de prendre en compte les coûts suivants qui ont été inclus dans notre analyse :

- Coût de mise en œuvre de la solution Anomali – Comprend le coût des abonnements à Anomali, les heures de travail des employés à temps plein et techniciens de service professionnels pour déployer, tester et former les utilisateurs sur la solution, les équipements pour exécuter Anomali, les coûts d'énergie/de refroidissement/d'encombrement, ainsi que le support et la maintenance du matériel.
- Valeur des produits de renseignements sur les menaces inclus – Valeur en dollars attribuée aux solutions équivalentes pour les sandbox, les renseignements TIP, incluant des flux de renseignements sur les menaces freemium et premium, la formation avec Anomali University, une assistance d'experts, etc.
- Coût de traitement des faux positifs évité – ESG a estimé 50 faux positifs par jour par analyste, 2 minutes par faux positif et une réduction de 40 % des faux positifs avec Anomali.
- Amélioration de la productivité des opérations de sécurité – Les modèles conservateurs détaillés d'ESG ont pris en compte le nombre d'heures de travail estimé avant Anomali par rapport à l'amélioration attendue pour la collecte des flux (amélioration de 70 %), leur gestion (amélioration de 70 %), les investigations et les rapports (amélioration de 60 %), l'intégration aux systèmes de sécurité opérationnels (amélioration de 20 %), la collaboration externe (amélioration de 50 %), le partage et les opérations en interne (amélioration de 60 %).
- Quantification de la réduction des risques – ESG a estimé une réduction du risque de violation des données par rapport à la moyenne du secteur, proportionnelle à une amélioration de 70 % de la détection et de la réponse, ainsi qu'une réduction du coût prévu de violation des données pour les systèmes automatisés (ces deux chiffres sont communiqués par le Ponemon Institute).

En conclusion

Depuis plusieurs années, le renforcement de la cybersécurité vient en tête de liste des facteurs économiques qui motivent les dépenses technologiques pour les entreprises interrogées dans le cadre de l'étude d'ESG. Alors que les entreprises continuent à développer leurs équipes, à les organiser et à investir dans de nouvelles solutions, une chose est claire : le problème n'est pas un manque d'outils de sécurité et de renseignements sur les menaces, mais un manque de ressources humaines pour gérer, interpréter et agir efficacement en fonction des renseignements et des alertes. Les entreprises de sécurité modernes ont besoin d'une plate-forme de renseignements sur les menaces capable de rationaliser le processus de sécurité, d'automatiser les tâches répétitives, de fournir des renseignements basés sur l'IA et de permettre aux ressources humaines de devenir plus efficaces sur le plan opérationnel.

ESG a validé qu'Anomali ThreatStream, Match et Lens ont fourni aux clients une plate-forme qui leur permet de tirer le meilleur parti de leurs investissements en matière de sécurité. Les équipes de sécurité sont beaucoup plus autonomes, productives et se concentrent sur les tâches les plus importantes ; leurs investissements dans leur SIEM et d'autres produits de sécurité sont facilement intégrés et améliorés pour offrir encore plus de valeur ; et leurs flux de renseignements sur les menaces sont prêts à être évalués, achetés et intégrés. Les clients ont signalé une visibilité considérablement améliorée et une plus grande capacité à partager les renseignements sur les menaces en interne avec d'autres divisions de l'entreprise et en externe avec leurs pairs et des organisations de sécurité.

L'analyse coûts-avantages modélisée par ESG montre comment une entreprise qui met en œuvre Anomali peut s'attendre à réaliser des économies grâce à une meilleure productivité de l'équipe de sécurité, à la valeur ajoutée des produits de renseignements sur les menaces inclus et à l'évitement des risques. Les hypothèses clés du modèle étaient basées sur la validation d'ESG avec les clients d'Anomali. Le modèle d'ESG a permis de calculer des économies totales attendues jusqu'à 93 000 $ par mois avec un retour sur investissement (ROI) attendu de 233 %.

Anomali n'est pas en concurrence avec les produits de sécurité existants d'une entreprise, et ne cherche pas à modifier de manière fonctionnelle la façon dont les équipes doivent exercer leurs activités. Au lieu de cela, Anomali permet d'opérationnaliser et d'améliorer les renseignements sur les menaces, les outils et les solutions afin de rendre les équipes de sécurité plus efficaces et d'étendre la discussion sur la sécurité à d'autres secteurs de l'entreprise. Toutes les entreprises interrogées par ESG ont estimé qu'elles avaient accompli davantage avec une équipe plus restreinte et qu'elles avaient développé leurs opérations bien au-delà de ce qui était possible de manière réaliste uniquement grâce aux ressources humaines. Certains ont même intégré Anomali dans de nouveaux postes : « J'avais déjà utilisé Anomali dans un rôle précédent et quand je suis arrivé ici, j'ai dit que sans Anomali, nous ne pourrions pas atteindre nos objectifs. » En tant qu'analyste, vous apprenez rapidement qu'une telle affirmation est la marque d'une technologie transformatrice. Si vous souhaitez transformer et rationaliser vos opérations de sécurité et tirer le meilleur parti de vos renseignements sur les menaces, ESG vous recommande de contacter Anomali pour déterminer s'il s'agit de la plate-forme de renseignements sur les menaces adaptée à votre équipe.