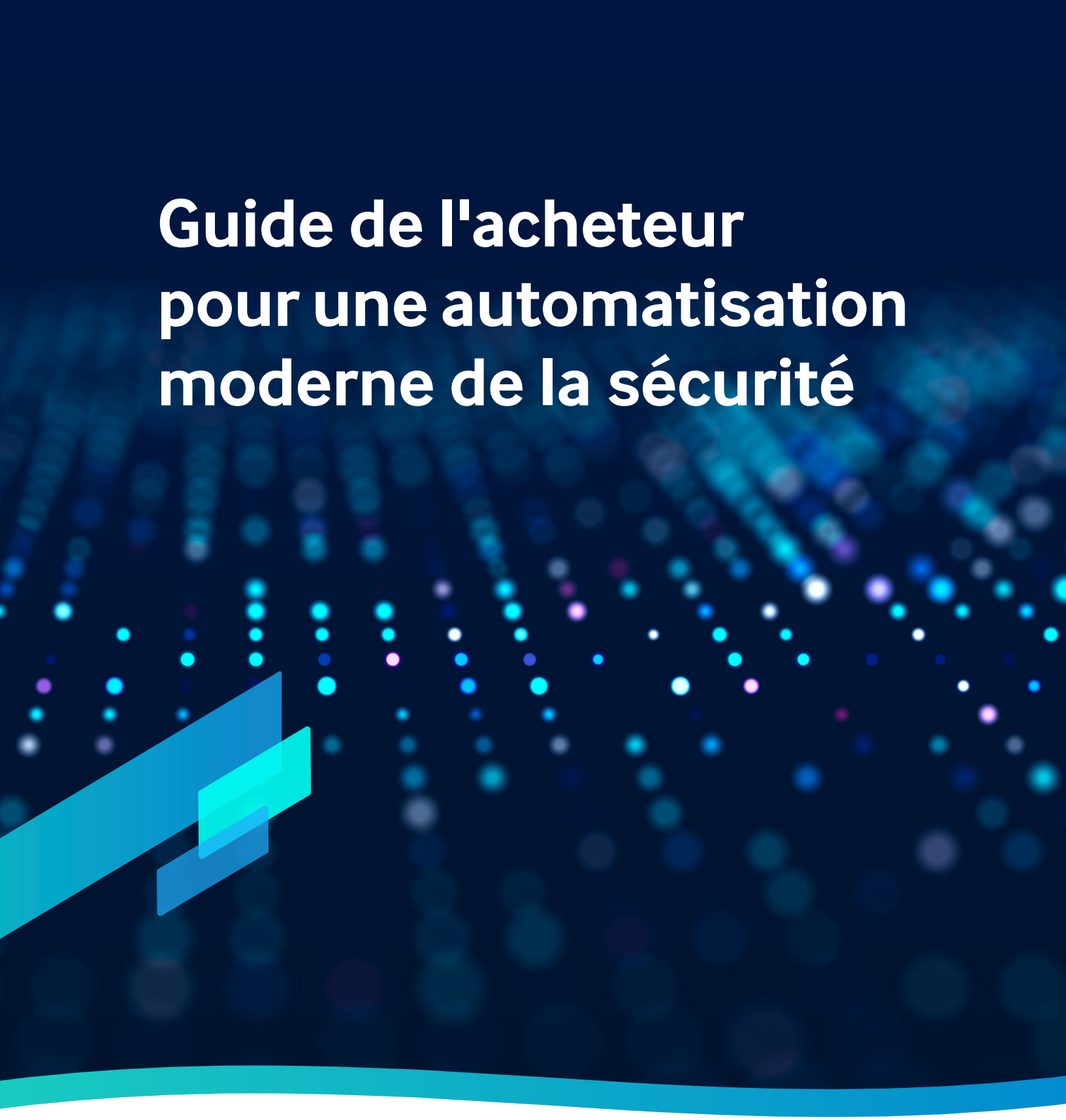
Guide de l'acheteur pour une automatisation moderne de la sécurité



SWIMLANE

Introduction

La plupart des grandes entreprises reconnaissent la nécessité de l'automatisation, car elles s'efforcent de suivre le rythme et l'ampleur de leurs opérations de sécurité (SecOps). Mais malheureusement, les équipes de sécurité ont souvent du mal avec les solutions d'automatisation elles-mêmes - entravées par des plateformes qui sont soit trop compliquées, soit trop simplistes pour faire le travail efficacement.

En particulier à l'échelle d'une grande entreprise, l'automatisation de la sécurité devrait transférer la charge de travail à la technologie, et non aux personnes de l'organisation. Mais cela n'est pas possible lorsque les équipes sont accablées par la complexité de solutions d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR), qui nécessitent l'utilisation de nombreux scripts, ou par les lacunes en matière de capacités qui apparaissent lorsque le pendule va trop loin vers des solutions simplistes - limitées - sans code.

Les RSSI, les responsables de SOC, les architectes de sécurité, les développeurs et les analystes sont trop souvent contraints de choisir entre une complexité SOAR excessive et une visibilité, une capacité d'action, une gestion des cas, des rapports, des tableaux de bord et un contrôle limité qu'ils devraient accepter dans le cadre d'une solution sans code. La bonne nouvelle, c'est qu'une solution bien conçue qui s'appuie sur de nouvelles méthodologies innovantes à faible code (Low Code) peut faire la part des choses entre ces deux extrêmes - pour finalement tirer plus d'efficacité, de fiabilité et de valeur d'un investissement dans l'automatisation de la sécurité.

Ce guide de l'acheteur est conçu pour apporter clarté et confiance dans la navigation parmi les nombreuses options et approches du marché de l'automatisation de la sécurité. À l'aide de cas d'utilisation réels, des meilleures pratiques de l'industrie, d'exemples de questions à poser aux fournisseurs et de listes de contrôle spécifiques à ce marché, nous examinerons comment la clé du succès réside dans les méthodologies low-code comme base de solutions d'automatisation de la sécurité puissantes et flexibles pour le SOC et au-delà.

SWIMLANE

L'AUTOMATISATION DE LA SÉCURITÉ ET POURQUOI ELLE EST NÉCESSAIRE

Le mandat organisationnel pour l'automatisation de la sécurité est motivé par la liste croissante de défis auxquels toute grande entreprise opérant aujourd'hui doit faire face dans sa pile technologique. Les processus SecOps au niveau d'une société Fortune 500, d'une grande multinationale ou d'une autre grande entreprise constituent un environnement intimidant défini par des pressions multiples et simultanées. Les principales d'entre elles sont les suivantes:

- *Surface d'attaque élargie* – Qu'il s'agisse d'attaques par hameçonnage, de vulnérabilités des points d'accès ou d'incidents au-delà du SOC comme la fraude et les menaces internes, la fréquence et la sophistication des attaques ne cessent d'augmenter. Les analystes de sécurité sont submergés par ce qui peut représenter jusqu'à 10 000 alertes par jour pour une grande entreprise, avec une marge d'erreur nulle. L'automatisation de la sécurité est donc indispensable pour aider les équipes à trier le déluge croissant d'alertes afin qu'elles puissent établir des priorités et répondre de manière proactive aux menaces et aux incidents..
- *Pénurie mondiale de personnel de sécurité* – La grande démission touche tous les travailleurs, mais plus particulièrement le personnel de sécurité, qui reste particulièrement rare, alors que les prévisions font état de 3,5 millions de postes de cybersécurité non pourvus dans le monde d'ici 2025.[1] Cette pénurie est particulièrement ressentie par les entreprises dont les piles technologiques sont de plus en plus volumineuses et distribuées dans des environnements multi-clouds. La capacité humaine à sécuriser de tels environnements numériques n'a pas rattrapé la demande écrasante, ce qui signifie que l'automatisation de la sécurité est le seul moyen de combler ce fossé.
- *Des architectures et des processus de sécurité de plus en plus complexes et cloisonnés* – Les équipes SecOps doivent assurer la sécurité et le fonctionnement de l'ensemble de la pile technologique. En particulier dans le cas de scénarios complexes et multi-clouds, cela peut nécessiter de naviguer dans des environnements technologiques avec 75 outils ou plus.[2] Sans automatisation pour orchestrer les opérations dans cet enchevêtrement de domaines d'entreprise, d'outils, d'équipes et de protocoles commerciaux uniques, les équipes de sécurité se noient dans la complexité et ne parviennent pas à combler toutes les failles de sécurité.

Pour diverses raisons que nous allons explorer plus en détail ci-dessous, les solutions d'automatisation de la sécurité qui répondent le mieux à ces défis reposent sur une approche low-code. En effet, l'approche low-code offre un équilibre optimal entre puissance et simplicité pour les équipes de sécurité qui ont besoin de plus de visibilité et possibilités d'action. Il s'agit d'un équilibre que de nombreuses approches d'automatisation ne parviennent pas à atteindre de manière adéquate.

[1] swimlane.com/blog/10-hard-hitting-cyber-security-statistics

[2] panaseer.com/wp-content/uploads/2021/11/Panaseer-2022-Security-Leaders-Peer-Report.pdf

TOUTES LES SOLUTIONS N'ONT PAS LA MÊME EFFICACITÉ

Les plateformes d'automatisation de la sécurité sont conçues pour s'adapter aux processus opérationnels uniques d'une organisation et automatiser des tâches qui, autrement, prendraient beaucoup de temps et nécessiteraient une surveillance constante de systèmes tiers. Pour comprendre l'attrait de cette proposition de valeur, il suffit de consulter un récent rapport de Gartner[3] sur les tendances en matière d'automatisation de la sécurité, qui fait état du rythme rapide d'adoption et d'innovation de ces solutions.

Le plus grand défi à relever lors de la mise en œuvre ou de la mise à niveau de l'automatisation de la sécurité est de trouver le juste équilibre entre complexité et simplicité. Cela tient en grande partie à la quantité de connaissances en codage que les équipes de sécurité et les experts du domaine doivent posséder pour obtenir une visibilité et une capacité d'action adéquates sur la pile technologique qu'ils sont chargés de protéger.

L'automatisation de la sécurité peut être divisée en trois catégories principales : SOAR (full-code), no-code et solutions mixtes basées sur le low-code.

Commençons par le **SOAR**. Il offre une certaine flexibilité pour personnaliser les options, mais s'accompagne souvent d'une expérience utilisateur rigide qui nécessite des développeurs dédiés pour gérer les intégrations, les flux de travail et les processus. La coût d'acquisition et d'utilisation est élevé et nécessite beaucoup plus de temps et d'expertise pour fonctionner pleinement. La complexité du SOAR laisse les équipes de sécurité mal équipées pour changer et s'adapter à l'évolution des besoins de l'entreprise au fil du temps.

En revanche, l'automatisation no-code offre un accès sans code aux bases de l'automatisation de la sécurité. Cependant, vous êtes limité à des intégrations, des cas d'utilisation et des flux de travail préfabriqués qui permettent une personnalisation minimale et laissent des angles morts dans les fonctionnalités de rapport, de gestion des cas et de tableau de bord. Une plateforme d'automatisation de la sécurité sans code peut suffire pour les tâches les moins importantes de l'équipe SOC dans un environnement de petite entreprise, mais à mesure que les petites organisations grandissent et se développent, leurs besoins en matière d'automatisation de la sécurité évoluent également. Les implémentations sans code sont rapidement dépassées lorsqu'elles sont utilisées dans des organisations plus grandes ou plus matures qui traitent généralement des ensembles de données plus larges et des intégrations plus diverses provenant d'endroits plus difficiles à atteindre dans leur pile technologique.

Ceci nous amène à l'approche low-code. Une solution d'automatisation de la sécurité low-code bien conçue supprime la dépendance des développeurs à l'égard des intégrations et de l'automatisation, ce qui permet de surmonter les pénuries de compétences et de réduire les silos en permettant aux experts du domaine de devenir des créateurs d'automatisation.

[3] https://www.swimlane.com/resources/gartner-soar-market-guide-2022

ÉVALUER LE MARCHÉ :

5 CRITÈRES CLÉS POUR ÉVALUER LES SOLUTIONS D'AUTOMATISATION DE LA SÉCURITÉ

Compte tenu de la grande diversité des solutions d'automatisation de la sécurité disponibles sur le marché, c'est à l'acheteur de sécurité de faire ses recherches et de faire les bons choix en matière de capacités et de configuration pour une approche d'automatisation de la sécurité qui réponde à plus d'incidents, en moins de temps, sans ajouter de frais généraux inutiles. Voici une poignée de critères clés, ainsi que les questions correspondantes que vous devriez poser aux fournisseurs pour clarifier leurs qualifications par rapport à chacun de ces critères:

1

Assurez-vous que la solution d'automatisation de la sécurité peut ingérer des ensembles de données plus importants et plus larges provenant d'endroits difficiles à atteindre

Vérifiez que votre solution peut améliorer les indicateurs clés de performance (ICP) tels que l'accélération du temps moyen de résolution (MTTR) et la réduction du temps d'attente. Cela nécessite un débit et une puissance de traitement supérieurs à ce que la plupart des solutions d'automatisation de la sécurité sont conçues pour gérer. Les solutions les plus performantes seront capables d'ingérer des volumes plus importants et des types d'ensembles de données plus variés. Recherchez les caractéristiques de la solution qui vous aideront dans ce domaine, comme l'ingestion distribuée de big data, l'enrichissement en ligne, le prétraitement et les fonctionnalités connexes.

- Question clé pour les fournisseurs: "Est-il facile de faire évoluer votre solution, et sera-t-elle capable de répondre aux mêmes indicateurs clés de performance si nous faisons évoluer l'environnement de production ?"

2

Vérifiez que la solution d'automatisation de la sécurité peut s'intégrer à un large éventail de formats et de sources

La solution d'automatisation de la sécurité doit pouvoir s'intégrer à des éléments qui ne font pas forcément partie des équipements typiques des SecOps. Assurez-vous que la solution peut aller au-delà des simples alertes provenant d'outils SOC standard tels que la gestion des informations et des événements de sécurité (SIEM), la détection et la réponse aux points de terminaison (EDR) et le renseignement sur les menaces, pour inclure également la télémétrie provenant des appareils du cloud ou de l'internet des objets (IoT), des centres de données et des sources d'informatique périphérique. Dans tous les cas, la solution doit rester indépendante des écosystèmes.

- Question clé pour les fournisseurs : "Votre solution est-elle capable de s'intégrer à n'importe quelle API sans dépendre des ressources des développeurs ?"

SWIMLANE

ÉVALUER LE MARCHÉ :

5 CRITÈRES CLÉS POUR ÉVALUER LES SOLUTIONS D'AUTOMATISATION DE LA SÉCURITÉ

3

Adapter la facilité d'utilisation aux besoins de l'analyste et de l'expert du domaine

Historiquement, de nombreuses ressources de développeurs d'automatisation de la sécurité sont restées compliquées, rigides et difficiles à travailler. Pour construire un Playbook, par exemple, un analyste doit être capable d'écrire du code Python. Votre solution Low-Code doit être suffisamment simple sur le plan technique pour être accessible à un analyste SOC de niveau 1 ou à un expert du domaine de la sécurité, tout en fournissant les flux de données, les connecteurs, les outils d'analyse et de visualisation appropriés pour que les architectes et les analystes de sécurité puissent exercer leur métier.

- **Question clé pour les fournisseurs:** "Mes analystes de domaine n'auront pas nécessairement des compétences de développeur. Quelle quantité de code est nécessaire pour qu'ils puissent faire leur travail ?"

4

S'efforcer d'obtenir un "système d'enregistrement" sur l'ensemble de la pile technologique

S'assurer que la solution peut fournir une visibilité et des rapports transparents sur l'ensemble des écosystèmes afin que les groupes de parties prenantes obtiennent des renseignements exploitables grâce à un système d'enregistrement définitif pour toute la sécurité. À l'instar de Salesforce pour les ventes, de Workday pour les professionnels des RH ou de ServiceNow pour l'informatique, votre solution d'automatisation de la sécurité doit fonctionner comme un hub de gestion central, qui saisit non seulement les données des machines et les fonctions automatisées, mais aussi les décisions et les interventions humaines effectuées au cours des processus de réponse, qui restent une partie essentielle des opérations de sécurité.

- **Question clé pour les fournisseurs:** "Quelles sont les entrées que votre solution utilise pour capturer et documenter les fonctions automatisées ; quelles sont les entrées qui le font avec les actions des analystes ; et comment votre solution intègre et visualise ces données ?"

5

Recherchez la simplicité clé en main de la documentation et des rapports de conformité

Ce critère est étroitement lié au précédent dans la mesure où les grandes entreprises sont aux prises avec une liste toujours plus longue de règles sectorielles et de règlements de conformité. La bonne solution d'automatisation de la sécurité peut automatiser non seulement les contrôles et les procédures de sécurité, mais aussi la documentation et le reporting de ces activités afin de garantir la conformité et d'éviter les violations de la réglementation qui peuvent entraîner des amendes et éroder la réputation d'une entreprise.

- **Question clé pour les fournisseurs:** "Comment les rapports d'activité sont-ils générés, et comment votre solution les aligne-t-elle avec les lois réglementaires spécifiques au secteur et les normes industrielles qui sont les plus pertinentes pour mon organisation ?"

SWIMLANE

CAS D'UTILISATION

Un grand prestataire de soins de santé utilise l'automatisation de la sécurité pour lutter contre les menaces internes.

Défi

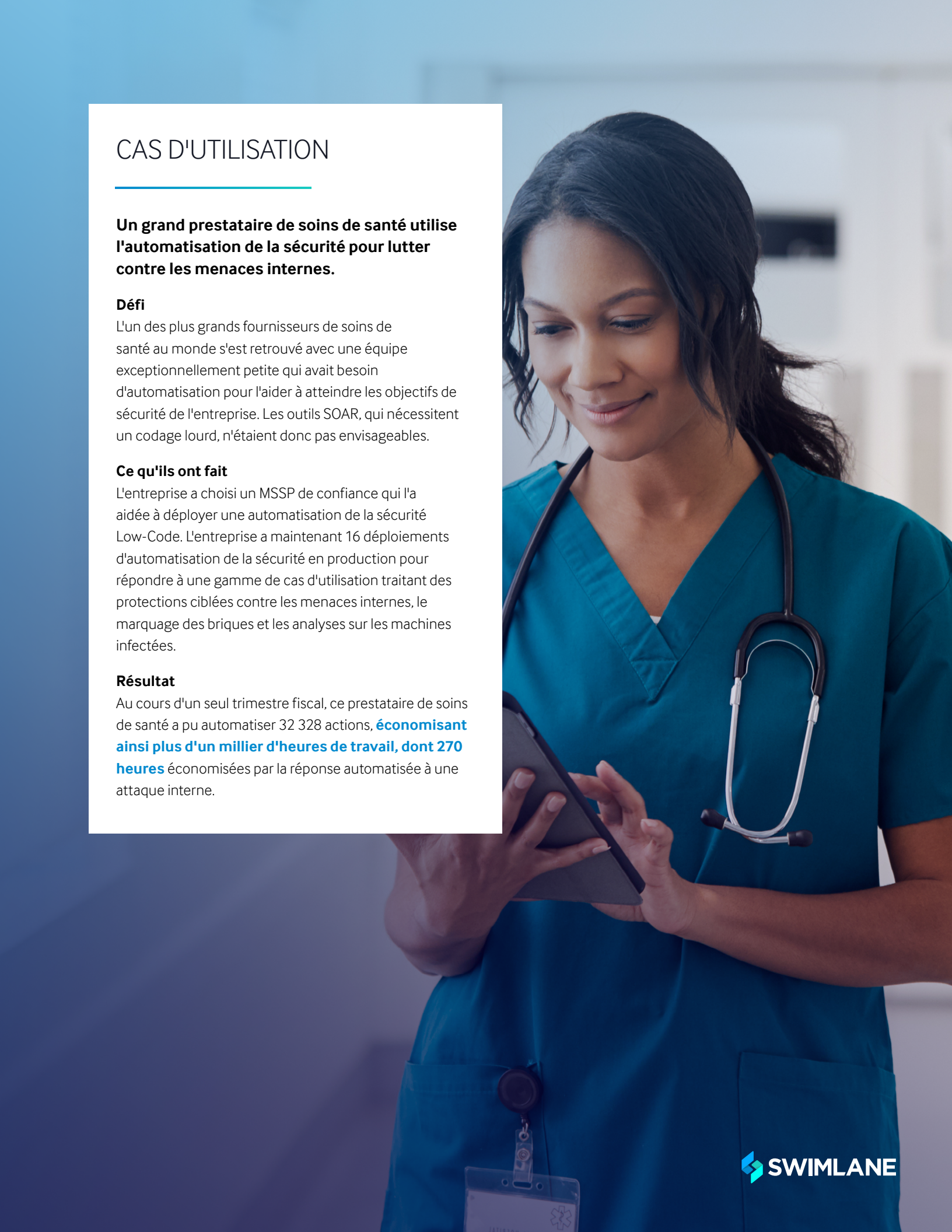
L'un des plus grands fournisseurs de soins de santé au monde s'est retrouvé avec une équipe exceptionnellement petite qui avait besoin d'automatisation pour l'aider à atteindre les objectifs de sécurité de l'entreprise. Les outils SOAR, qui nécessitent un codage lourd, n'étaient donc pas envisageables.

Ce qu'ils ont fait

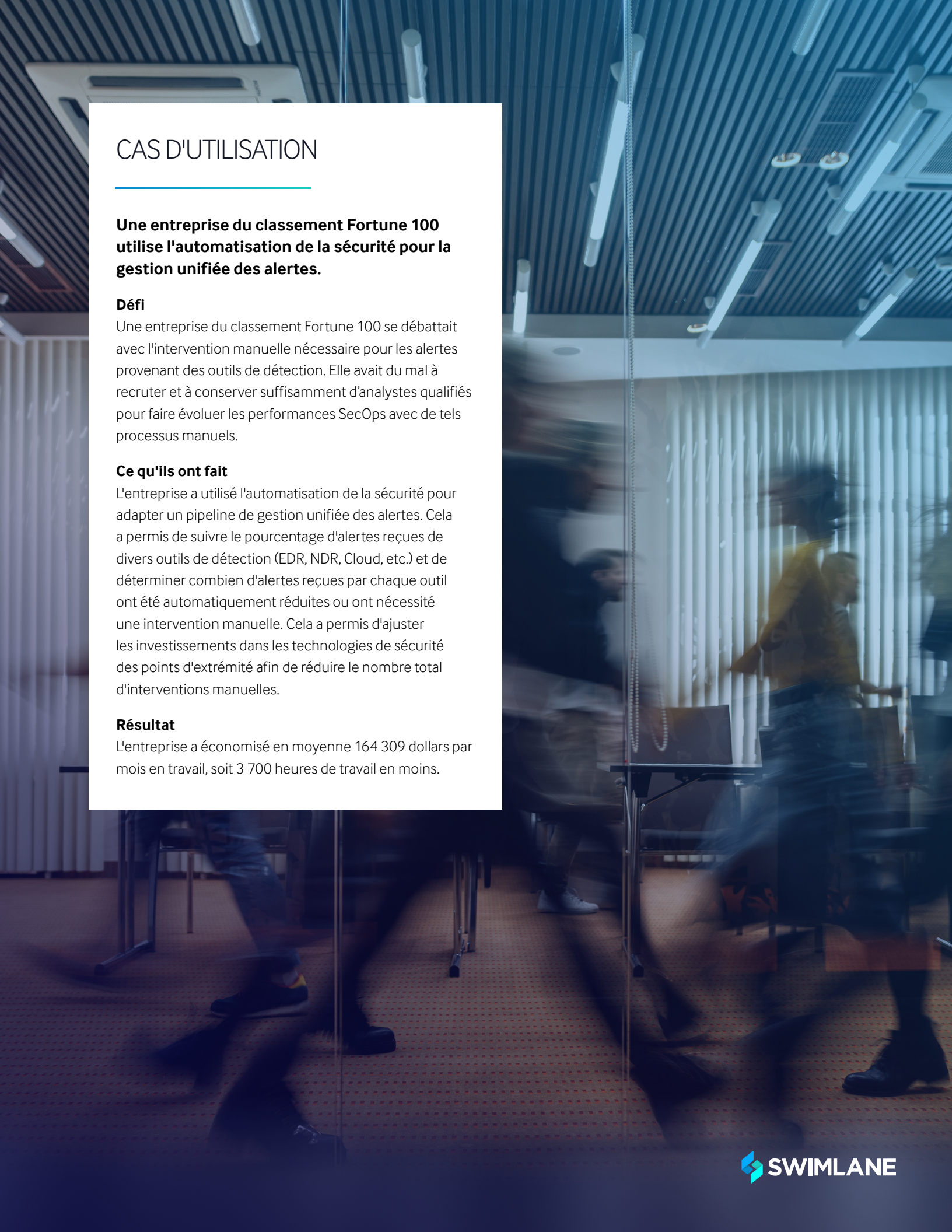
L'entreprise a choisi un MSSP de confiance qui l'a aidée à déployer une automatisation de la sécurité Low-Code. L'entreprise a maintenant 16 déploiements d'automatisation de la sécurité en production pour répondre à une gamme de cas d'utilisation traitant des protections ciblées contre les menaces internes, le marquage des briques et les analyses sur les machines infectées.

Résultat

Au cours d'un seul trimestre fiscal, ce prestataire de soins de santé a pu automatiser 32 328 actions, **économisant ainsi plus d'un millier d'heures de travail, dont 270 heures** économisées par la réponse automatisée à une attaque interne.



SWIMLANE



CAS D'UTILISATION

Une entreprise du classement Fortune 100 utilise l'automatisation de la sécurité pour la gestion unifiée des alertes.

Défi

Une entreprise du classement Fortune 100 se débattait avec l'intervention manuelle nécessaire pour les alertes provenant des outils de détection. Elle avait du mal à recruter et à conserver suffisamment d'analystes qualifiés pour faire évoluer les performances SecOps avec de tels processus manuels.

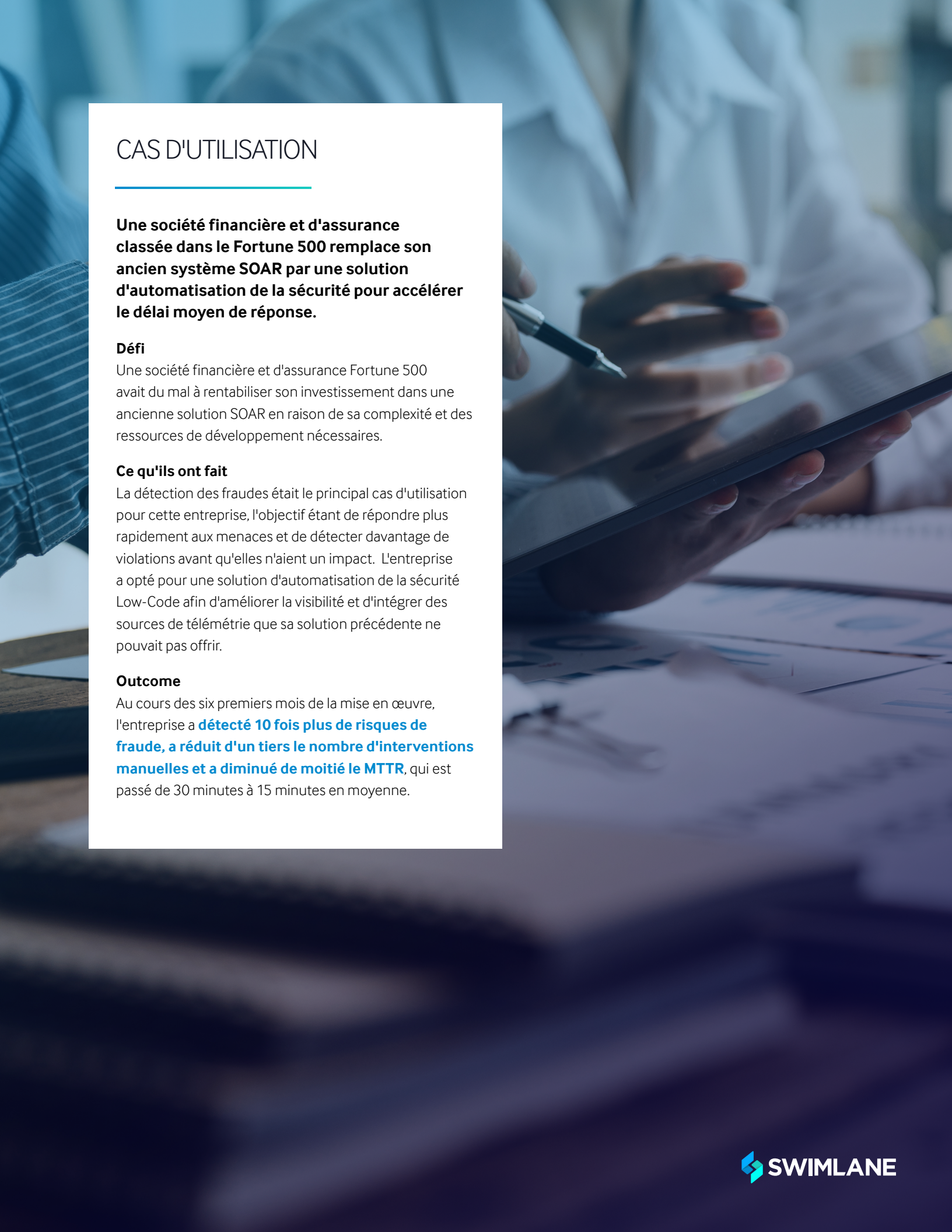
Ce qu'ils ont fait

L'entreprise a utilisé l'automatisation de la sécurité pour adapter un pipeline de gestion unifiée des alertes. Cela a permis de suivre le pourcentage d'alertes reçues de divers outils de détection (EDR, NDR, Cloud, etc.) et de déterminer combien d'alertes reçues par chaque outil ont été automatiquement réduites ou ont nécessité une intervention manuelle. Cela a permis d'ajuster les investissements dans les technologies de sécurité des points d'extrémité afin de réduire le nombre total d'interventions manuelles.

Résultat

L'entreprise a économisé en moyenne 164 309 dollars par mois en travail, soit 3 700 heures de travail en moins.

SWIMLANE



CAS D'UTILISATION

Une société financière et d'assurance classée dans le Fortune 500 remplace son ancien système SOAR par une solution d'automatisation de la sécurité pour accélérer le délai moyen de réponse.

Défi

Une société financière et d'assurance Fortune 500 avait du mal à rentabiliser son investissement dans une ancienne solution SOAR en raison de sa complexité et des ressources de développement nécessaires.

Ce qu'ils ont fait

La détection des fraudes était le principal cas d'utilisation pour cette entreprise, l'objectif étant de répondre plus rapidement aux menaces et de détecter davantage de violations avant qu'elles n'aient un impact. L'entreprise a opté pour une solution d'automatisation de la sécurité Low-Code afin d'améliorer la visibilité et d'intégrer des sources de télémétrie que sa solution précédente ne pouvait pas offrir.

Outcome

Au cours des six premiers mois de la mise en œuvre, l'entreprise a **détecté 10 fois plus de risques de fraude, a réduit d'un tiers le nombre d'interventions manuelles et a diminué de moitié le MTTR**, qui est passé de 30 minutes à 15 minutes en moyenne.

SWIMLANE

CAS D'UTILISATION

Une agence du gouvernement fédéral utilise l'automatisation de la sécurité pour maintenir un SOC 24x7.

Défi

Une grande agence gouvernementale fédérale avait du mal à attirer et à retenir les talents possédant des habilitations de sécurité et des compétences en sécurité spécifiques au cloud. Malgré ces difficultés, l'agence devait maintenir un SOC 24x7 et des processus d'escalade de réponse aux incidents.

Ce qu'ils ont fait

L'agence a mis en œuvre une solution de sécurité à faible code qui a automatisé plus de 100 activités de niveau 1, y compris des listes de contrôle discrètes pour le triage, l'analyse, les notifications, la remontée des alertes de sécurité et d'autres activités.

Résultat

L'agence a pu réorienter son nombre limité d'analystes de niveau 1 vers des rôles plus avancés, comme la réponse aux incidents et la criminalistique. Ce faisant, l'agence a considérablement réduit le taux de rotation du personnel - **ce qui a permis d'économiser les connaissances institutionnelles et les coûts de recrutement** - car les travailleurs ont exprimé le désir de continuer à travailler avec des outils d'automatisation de la sécurité qui réduisent la pénibilité de leur travail.

SWIMLANE

REGARDEZ BIEN SOUS LE CAPOT:

LA CHECK-LIST DE L'ACHETEUR POUR L'AUTOMATISATION DE LA SÉCURITÉ

Même après avoir défini les critères clés et clarifié les cas d'utilisation qui ont le plus grand impact positif sur l'organisation, une série de choix plus granulaires attend le décideur en matière de sécurité. C'est là que le travail de l'acheteur avisé porte vraiment ses fruits. Afin de définir et d'affiner l'approche optimale pour s'engager sur le marché, voici une liste des principales considérations et exigences auxquelles il faut réfléchir et se préparer à discuter avec les fournisseurs potentiels:

Comprendre votre environnement informatique et votre pile technologique

Vous devez avoir une solide connaissance des technologies et des produits que vous utilisez actuellement dans le cadre de votre dispositif de sécurité existant. Vous devez également savoir à quelle fréquence votre pile de sécurité change et clarifier tous les processus internes, les procédures opérationnelles standard et les accords de niveau de service qui s'appliquent à cette pile.

Mettez en correspondance les processus opérationnels actuels et les cas d'utilisation que vous souhaitez automatiser

Dressez une liste des technologies qui génèrent des alertes ou des événements auxquels il faut donner suite. Vous devez spécifiquement cartographier les produits et processus de renseignement utilisés dans les systèmes de gestion des incidents et des événements de sécurité (SIEM) et de réponse à la détection des points finaux (EDR). Tout au long du processus, veillez à identifier toutes les API pertinentes.

Obtenez un alignement interne sur les objectifs, les priorités et les indicateurs clés de performance

Définissez ce qu'est le succès pour l'automatisation de la sécurité, y compris l'image souhaitée dans 6 mois, 1 an et 3 ans. Pour chaque point dans le temps, essayez d'être aussi précis que possible en fixant des objectifs pour le temps moyen de détection (MTTD) et le temps moyen de résolution (MTTR) et d'autres indicateurs clés de performance. Veillez à ce que les buts et les objectifs soient formulés en des termes que les RSSI, les gestionnaires de risques et les autres parties prenantes clés comprendront et apprécieront.

Priorisez les lacunes et les silos dans votre pile de sécurité que l'automatisation aidera à combler

Choisir où commencer à mettre en œuvre l'automatisation de la sécurité ne devrait pas être un tirage au sort. Essayez d'identifier les processus manuels qui prennent le plus de temps, les domaines qui génèrent le plus d'alertes ou les parties de la pile de sécurité où vous constatez un grand nombre de fausses alarmes et les rapports signal/bruit les plus faibles.

Pensez aux membres de votre équipe

Un autre facteur important pour donner la priorité à l'automatisation est de savoir où vos équipes sont actuellement le plus en difficulté. L'épuisement professionnel des responsables de la sécurité est une tendance réelle qui est en hausse.[4] Pour cette raison, choisissez des domaines où l'automatisation peut être un multiplicateur de force pour les départements surchargés, en particulier ceux qui comprennent du personnel avec des compétences uniques que vous ne voulez pas perdre.

[4] https://www.cnbc.com/2022/09/08/cisos-say-stress-and-burnout-are-their-top-personal-risks.html

REGARDEZ BIEN SOUS LE CAPOT:

LA CHECK-LIST DE L'ACHETEUR POUR L'AUTOMATISATION DE LA SÉCURITÉ

Considérez votre approche de l'automatisation dans le contexte de votre stratégie SecOps plus large

Réfléchissez à la proportion de SecOps actuellement réalisée en interne par rapport à celle externalisée, et si vous souhaitez que cette proportion change au fil du temps. Si vous externalisez actuellement des composants d'automatisation SecOps, évaluez si votre nouvel investissement dans l'automatisation remplacera ou complétera ce travail.

Engagez un ensemble plus large de parties prenantes de la sécurité

Réfléchissez au-delà du SOC pour voir si l'automatisation peut apporter une valeur ajoutée aux équipes chargées de la criminalistique numérique, de la gestion des vulnérabilités, de la gestion des fraudes, des menaces internes ou de spécialités de sécurité connexes. Si l'élargissement des cas d'utilisation apporte une valeur ajoutée, assurez-vous de sélectionner un outil qui s'aligne sur les capacités de ces parties prenantes en matière de codage, d'expertise en automatisation ou d'autres ensembles de compétences.

Évaluez les avantages et les inconvénients des différents modèles de déploiement sur site ou dans le Cloud pour déterminer lequel convient le mieux à votre entreprise

Dressez une liste des technologies qui seront au cœur de votre pile de sécurité à l'avenir, notamment les pare-feu, la sécurité d'Active Directory (AD), la réponse à la détection des points d'extrémité (EDR) et d'autres composants de sécurité. Pour chacune d'entre elles, évaluez et comparez les fonctionnalités, le coût et les implications en termes de licences pour un déploiement sur site ou dans le cloud.

Comprendre vos besoins en matière de rapports et vos obligations de conformité

Clarifiez vos besoins spécifiques en matière de rapports et de conformité, y compris la documentation spécifique du processus de réponse aux incidents, comme Playbooks et les flux de procédures, qui sont exigés de votre organisation. Votre évaluation doit inclure les outils existants, le cas échéant, pour documenter les indicateurs de compromission (IOC) et préciser s'ils sont manuels ou automatisés.

Quantifiez le retour sur investissement pour justifier les dépenses

Essayez de quantifier les indicateurs clés de performance en termes d'économies de coûts pour l'organisation grâce à la réduction des risques et des temps d'arrêt, et n'oubliez pas de prendre en compte les économies de coûts de main-d'œuvre également. Cela comprend les heures d'analyse économisées et l'augmentation du taux de rétention des employés hautement qualifiés pour lesquels vous réduisez le labeur grâce à l'automatisation qui remplace les processus pénibles ou banals.

Passez à l'étape suivante

Pour en savoir plus sur Swimlane et sur la puissance de l'automatisation de la sécurité en low-code, consultez notre site Web. Si vous avez un projet d'automatisation de la sécurité à venir, si vous êtes confronté à des problèmes de SecOps tels que la fatigue des alertes ou si vous ne voyez pas les résultats que vous attendiez de votre plateforme d'automatisation de la sécurité existante, nous vous invitons à programmer une démonstration personnalisée avec l'un de nos experts.

Demandez une démo ici
https://swimlane.com/request-a-demo-french

SWIMLANE