Guide de l'orchestration, de l'automatisation et de la réponse de sécurité pour le RSSI visionnaire

Donner aux équipes de sécurité le temps d'être proactives et stratégiques pour aider les entreprises à innover et à se développer

splunk>

Sommaire

Les chefs d’entreprise ont besoin d’équipes de sécurité qui soient des moteurs de transformation

Le rôle du responsable sécurité des systèmes d’information (RSSI) évolue.

Comme les DSI et les directeurs de la technologie avant eux, les RSSI ne sont plus de simples contributeurs au portefeuille de responsabilités limité : ce sont des moteurs hautement intégrés et stratégiques de la transformation de l’entreprise. Les entreprises les plus performantes reconnaissent qu’une véritable transformation numérique et commerciale dépend de la modernisation de la sécurité.

Les experts de PwC ont découvert que 40 % des dirigeants recherchaient des RSSI capables de diriger des équipes polyvalentes et agiles, non seulement pour suivre le rythme de la transformation numérique, mais aussi, dans de nombreux cas, pour montrer la voie à suivre.[1]

Une étude menée pour l’Information Security Systems Association a révélé que les professionnels de la sécurité du monde entier considéraient les compétences en communication et en leadership comme les meilleurs atouts d’un excellent RSSI.[2]

Les quatre qualités les plus appréciées des dirigeants :

1. Réflexion stratégique
2. Capacité de prendre des risques intelligents
3. Compétences en leadership
4. Capacité à identifier et favoriser l’innovation

L’étude de l’ISSA a également révélé qu’une majorité d’analystes de la sécurité souhaitent assumer des rôles plus stratégiques et reconnaissent qu’ils devront développer des compétences en leadership, en communication et en gestion des affaires pour devenir des leaders de la croissance et de la transformation.

« La sécurité de l’information ne se limite plus à la prévention des attaques : elle est un moyen de soutenir et d’accélérer les activités. »

– Yassir Abousselham, RSSI, Splunk

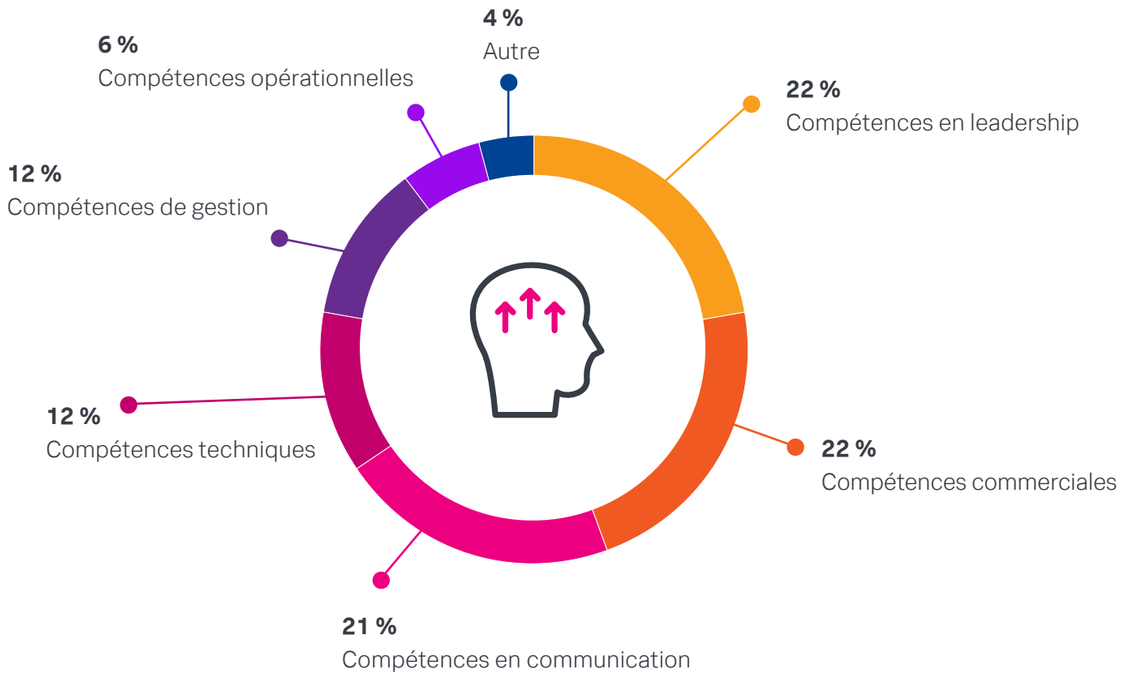
[1]https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-digital-trust-insights/cyber-strategy.html

[2]https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf

Les analystes de sécurité savent qu'il leur faut plus que des compétences techniques pour devenir des leaders organisationnels

Enterprise Strategy Group a demandé aux analystes de sécurité quelles compétences ils devaient développer pour devenir CSO ou RSSI.

Source : Enterprise Strategy Group



Mais dans de trop nombreux cas, les aspirations stratégiques des chefs de la sécurité et des analystes sont contrecarrées par la réalité du quotidien : **il y a trop d'alertes et pas assez de personnes pour y répondre**.

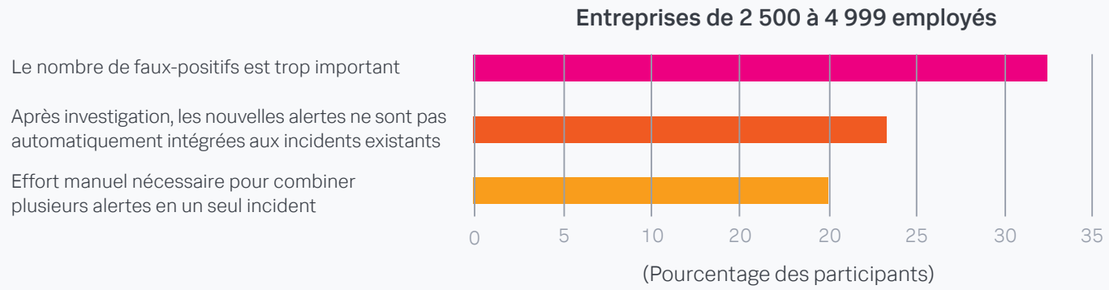
Reprenez le contrôle sur le désordre

Près d'un tiers des professionnels de la cybersécurité ont déclaré à l'ISSA que la « charge de travail écrasante » était la principale source de stress de leur rôle. Cette charge de travail écrasante prend la forme de centaines voire de milliers d'alertes quotidiennes qui doivent être hiérarchisées, analysées et traitées.

Les trois principales causes des alertes non étudiées

Qu'est-ce qui empêche votre organisation d'analyser et de traiter TOUTES les alertes suspectes chaque jour ?

Source : IDC



Le défi du déluge d'alertes est aggravé par une pénurie de talents en cybersécurité. Il n'y a tout simplement pas assez de professionnels de la cybersécurité qualifiés pour doter adéquatement les SOC dans le monde.
Ce manque de talents bien documenté, associé au volume considérable d'alertes quotidiennes, explique pourquoi 64 % des tickets de sécurité générés chaque jour ne sont pas traités.[3]
Les analystes n'ont pas les moyens de traiter toutes les alertes tous les jours, laissant leurs entreprises vulnérables aux attaques.

64 %
des alertes de sécurité quotidiennes ne sont pas traitées[4]

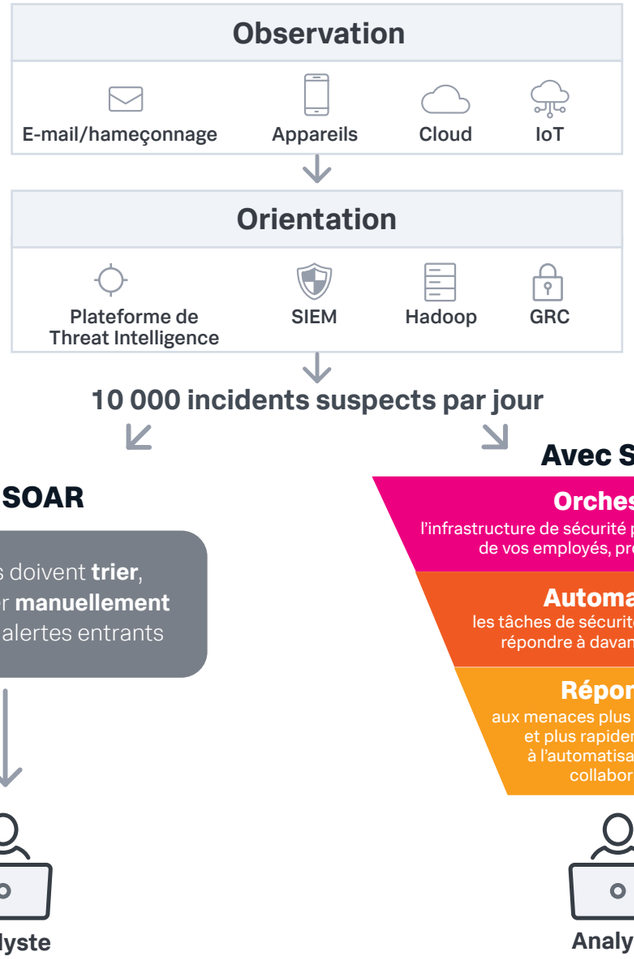
Comme les équipes de sécurité ont du mal à assurer le suivi des alertes, les RSSI ne peuvent pas fournir de conseils stratégiques et les analystes n'ont pas le temps d'effectuer des tâches essentielles d'ingénierie et d'optimisation, d'affiner les réponses automatisées et de traquer les menaces de manière proactive.

La réponse à ces défis réside dans l'orchestration, l'automatisation et la réponse de la sécurité (SOAR). Les plateformes comme Splunk SOAR modifient les rapports de force en matière de sécurité. En supprimant les tâches banales et routinières de la mission de l'analyste et en orchestrant les outils de sécurité pour qu'ils fonctionnent en coordination, les équipes de sécurité peuvent passer plus de temps à améliorer la posture de sécurité de l'entreprise et à la faire progresser.

[3]https://www.splunk.com/en_us/form/an-enterprise-management-associates-research-report.html
[4]https://www.splunk.com/pdfs/analyst-reports/an-enterprise-management-associates-research-report.pdf

Une journée dans la vie d'un analyste

Avant et après le SOAR



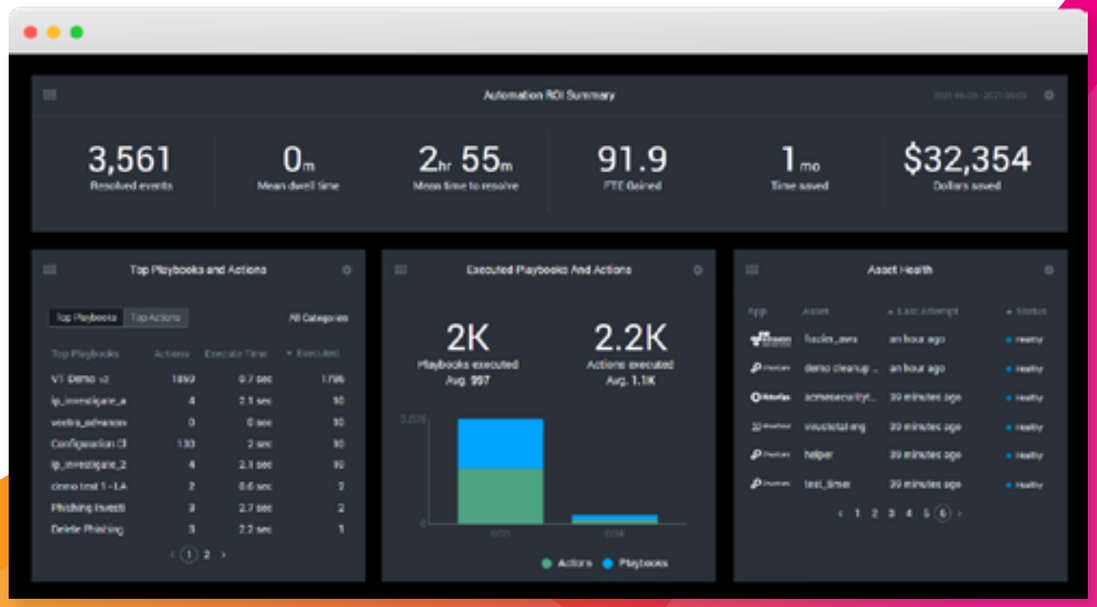
Le retour sur investissement du SOAR

Selon une estimation, le coût annuel de la lutte contre les attaques d'hameçonnage s'élève à près de 700 000 $. Le coût des ransomwares peut également être élevé et causer des dommages durables à la réputation. Le SOAR permet d'économiser du temps et de l'argent.[5] Le gain de temps se mesure en équivalent de charge de travail manuel d'un salarié à temps plein. Par exemple, avec une plateforme SOAR, un SOC de trois analystes peut avoir l'impact d'une équipe de 10 à 15 professionnels effectuant toutes les tâches manuellement.

> **« Viendra un moment où vous serez submergé par la quantité de travail et où vous ne pourrez plus embaucher davantage de personnes. L'automatisation est la seule solution. »**
>
> – Jason Mihalow, Architecte senior en Cybersécurité cloud, McGraw Hill

Voir l'étude de cas (en anglais)

Le tableau de bord principal de Splunk SOAR fournit aux équipes de sécurité un aperçu de l'activité du SOC, des événements notables et des playbooks, ainsi qu'un résumé du retour sur investissement des actions automatisées. Le résumé du ROI de l'automatisation montre en temps réel l'impact de l'automatisation : temps gagné, économies réalisées, ETP (équivalents temps plein) économisés et le temps de séjour moyen.



[5]https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

ÉTUDE DE CAS

Norlys : Réussir avec le SOAR

Avec 1,5 million de clients, Norlys est la plus grande entreprise de services publics et de télécommunications du Danemark. Après avoir créé ses propres systèmes d'analyse des logs et de réponse aux incidents, l'équipe de sécurité de Norlys s'est trouvée freinée par des tâches répétitives, des outils trop nombreux, des interfaces web lentes et des processus lourds. Avec Splunk, Norlys a automatisé les tâches répétitives et centralisé les investigations.

Voir l'étude de cas (en anglais)

Le résultat :

- 35 heures de travail économisées par semaine
- 30 secondes pour achever des processus qui prenaient 30 minutes auparavant
- 98 % de réduction du délai d'ouverture des tickets

Top cinq des tâches fastidieuses automatisées par Norlys :

1 Transfert des notables de Splunk ES vers SOAR
De **3 minutes** à **2 secondes**

2 Automatisation des investigations sur les alertes AV
De **40 minutes** à **10 minutes**

3 Automatisation des investigations sur les identifications IOC à partir du flux de menaces
De **15 minutes** à **10 secondes**

4 Automatisation du processus d'obtention de l'historique du navigateur
De **30 minutes** à **20 secondes**

5 Automatisation de l'ouverture des tickets dans des systèmes externes
De **10 minutes** à **10 secondes**

Modernisez la sécurité pour transformer votre entreprise

Pour que le RSSI devienne le partenaire stratégique dont l'entreprise a besoin, et pour que les analystes de sécurité trouvent des opportunités de développement professionnel, l'orchestration et l'automatisation sont indispensables. Splunk SOAR permet aux équipes de sécurité de réaliser tout le potentiel de leurs investissements dans les outils et les talents de sécurité.

Essayez Splunk SOAR dès aujourd'hui

splunk>