5 attributs d'un programme de sécurité moderne

Insight

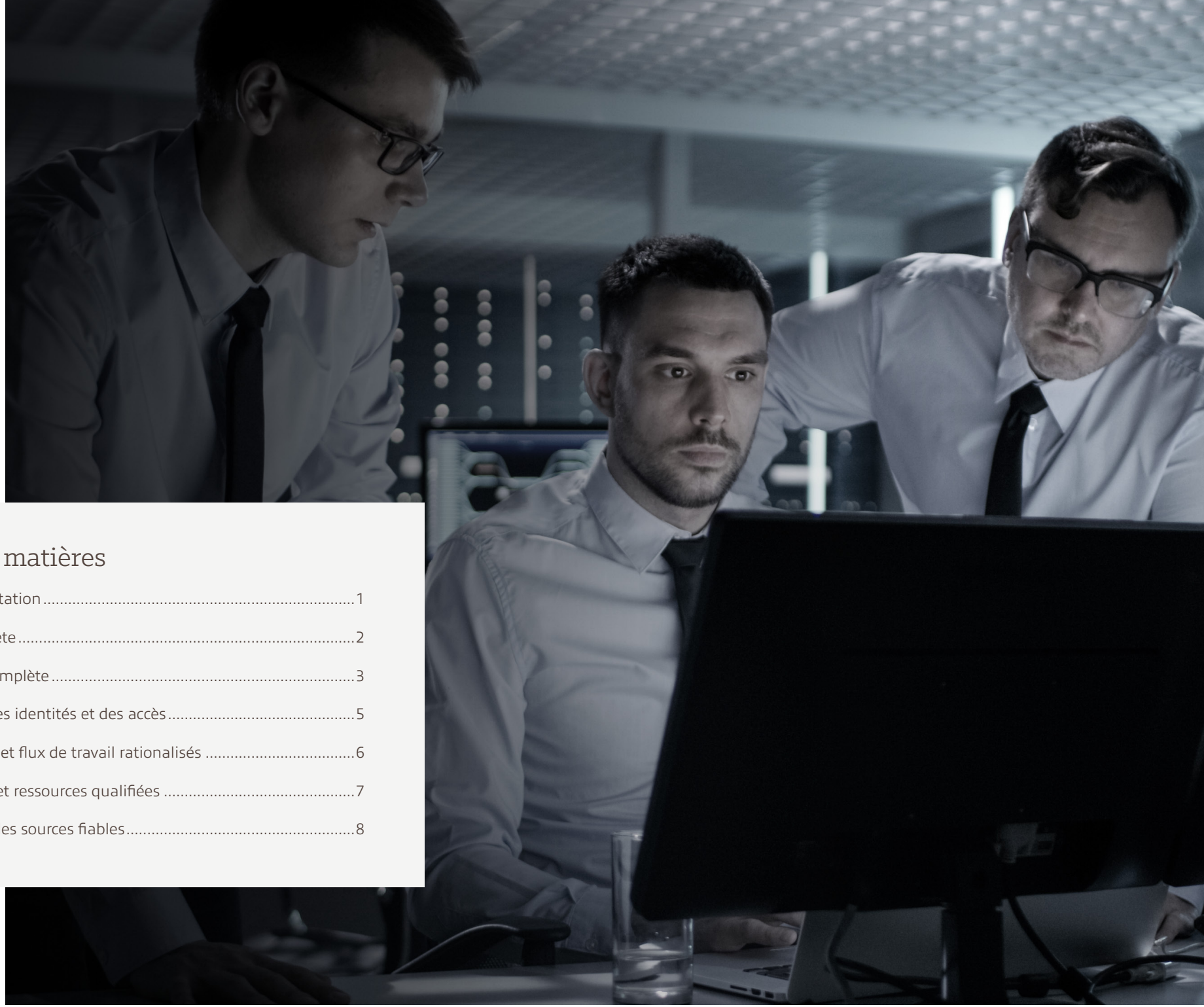


Table des matières

Une brève orientation 1

Visibilité complète 2

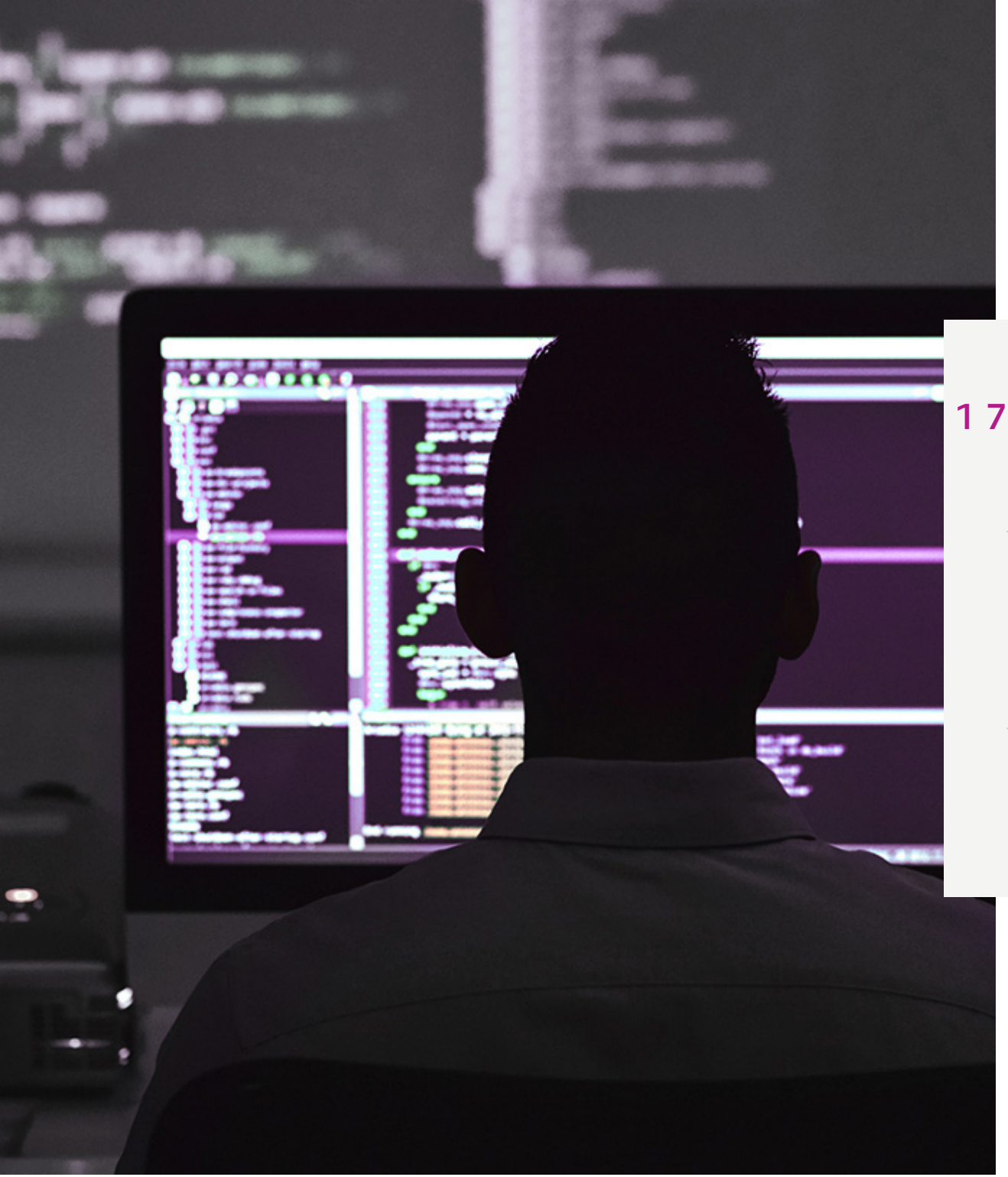
Gouvernance complète 3

Management des identités et des accès 5

Automatisation et flux de travail rationalisés 6

Outils efficaces et ressources qualifiées 7

- Rechercher des sources fiables 8



Une brève orientation

La croissance exponentielle des données s'accompagne d'une augmentation du nombre de personnes qui cherchent à tirer profit des attaques malveillantes. Aujourd'hui plus que jamais, il est essentiel que les organisations évaluent leur stratégie de sécurité.

Au premier semestre 2021,

1 767 infractions ont été signalées,

entraînant une exposition de

plus de 18,8 milliards de données.[1]

Le coût moyen était supérieur à

1,07 million de dollars

en cas de violations où le travail à distance rentrait en ligne de compte dans l'origine de la violation.[2]

Le coût moyen total d'une infraction à la protection des données s'élève à

4,24 millions USD[2]

Dans de tels cas, il est utile de prendre du recul. Quel devrait être l'objectif d'un programme de sécurité ? Quels objectifs sont réalistes et quels objectifs ne le sont pas ? Comment les investissements en sécurité doivent-ils être effectués et mesurés ?

Nous estimons qu'il existe cinq attributs clés à un programme de sécurité réussi et modernisé, pour tout type ou taille d'entreprise.

[1] Risk Based Security. (août 2021). 2021 Mid Year QuickView Data Breach Report.
[2] Ponemon Institute. (2021). 2021 Cost of a Data Breach Report. Sponsorisé par IBM Security.

CHAPITRE 1

Visibilité complète

Les environnements IT se développent. Nous assistons à une croissance des volumes de données, du nombre d'appareils, des plateformes et du trafic. Chaque nouvelle expansion apporte de nouveaux vecteurs de menaces et des défis supplémentaires en termes de visibilité.

Réalité :	Réflexion :
La génération de données à l'échelle mondiale **passera de 64,2 ZB en 2020 à 180 ZB d'ici 2025**.[3]	**Comment toutes ces données seront-elles surveillées et sécurisées,** en particulier lorsqu'elles se déplacent dans les environnements IT ?
Il y aura plus de 41 milliards d'appareils IoT (Internet des objets) d'ici 2027, contre environ 8 milliards en 2019.[4]	**Quel niveau de visibilité pouvons-nous raisonnablement viser,** compte tenu de ce niveau de croissance des appareils connectés ?
87 % des entreprises ont adopté ou commencé à adopter une approche multiCloud (en utilisant plus d'un fournisseur de Cloud public) l'année dernière.[5]	**Comment rendre la visibilité facile, voire possible,** avec plusieurs plateformes de différents types dans le même environnement IT ?

Pourtant, il est essentiel d'avoir une visibilité complète. Les avantages sont nombreux d'un environnement IT qui offre une visibilité de qualité et que les activités sont surveillées.

Tout d'abord, les tentatives d'attaque peuvent être déjouées et les dommages potentiels atténués. Une attaque réussie commence généralement par l'exploitation d'une vulnérabilité, puis pénètre dans plusieurs systèmes, à partir de ce point de départ unique. Si une infraction est détectée plus tôt, l'étendue de la perte peut être mieux contrôlée. En 2019, le délai moyen d'identification d'une infraction était de 206 jours.[2] Imaginez le nombre d'enregistrements, de systèmes et d'utilisateurs qu'une cyberattaque peut affecter durant plus de six mois. Le seul fait d'y penser fait froid dans le dos.

La visibilité, associée à des outils de surveillance et/ou de veille sur les menaces, contribue également largement à l'efficacité des efforts de prévention. Le comportement de l'utilisateur a tendance à être modelé, se déplaçant de manière logique et répétitive. Des activités ou mouvements inhabituels peuvent signaler la présence d'acteurs malveillants, aidant ainsi les responsables de la sécurité IT à prévenir les attaques et à apporter des modifications d'accès ou de politique qui peuvent combler les lacunes de sécurité jusqu'alors inaperçues.

[3] Statista. (Mai 2022). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025.
[4] Newman, P. (mars 2020). The Internet of Things 2020. Business Insider Intelligence.
[5] Marketpulse Research by IDG Research Services. (Février 2020). The State of IT Modernisation 2020. Commissionnée par Insight.

CHAPITRE 2

Gouvernance complète

Nombreux sont ceux qui, lorsqu'ils pensent à la gouvernance, se réfèrent à des structures telles que COBIT ou ITIL. À un niveau élevé, la gouvernance concerne la manière dont les décisions IT sont en phase avec les objectifs ou les besoins de l'entreprise. La gouvernance doit également aborder la question de la propriété et de la responsabilité, qui est responsable et qui sont les parties prenantes.

La gouvernance est essentielle pour la sécurité, car elle aide les organisations à :

- Définir et harmoniser les objectifs de sécurité
- Sélectionner et valider les solutions de sécurité
- Organiser la formation, les directives et autres programmes de sécurité des utilisateurs
- Intégrer la sécurité dans les conversations sur l'adoption de la plateforme, l'architecture réseau et d'autres composants de la stratégie IT
- Améliorer la posture de sécurité grâce à des rôles et des processus définis

Cependant, une gouvernance efficace peut être difficile à atteindre. Dans la dernière enquête IDG commanditée par Insight, les personnes interrogées ont indiqué que le principal défi de modernisation IT consiste à établir de nouvelles stratégies et de nouveaux processus de gouvernance pour soutenir la modernisation IT et le Cloud.[5]

L'un des aspects difficiles de la conception d'une gouvernance efficace est, en fait, l'utilisation accrue du Cloud. Les organisations peuvent avoir mis en place des cadres de gouvernance de travail depuis des années, qui ne concernaient que le datacenter et son périmètre clairement défini.

Selon le rapport « State of the Cloud » de Flexera 2022

89 % des organisations ont adopté une stratégie multiCloud,

et

80 % adoptent une approche de Cloud hybride en combinant l'utilisation de Clouds publics et privés.[6]

L'extension de la gouvernance traditionnelle au Cloud est essentielle, mais n'est pas une formule magique, et nécessite des investissements en temps et en ressources.

Cela a des répercussions sur la sécurité du Cloud, ou la perception de celle-ci, du moins. L'enquête IDG a révélé que la gestion de la sécurité du Cloud public est le défi numéro un lors de l'optimisation de l'expérience et des résultats du Cloud, suivie de près par les difficultés liées à la gouvernance et au processus.[5]

En établissant une gouvernance complète, incluant toutes les plateformes, rôles, parties prenantes, etc., une organisation peut s'assurer que ses opérations de sécurité restent performantes, pertinentes et continues.

[6] Flexera. (2022). 2022 State of the Cloud Report.

CHAPITRE 3

Management des identités et des accès

Tout le monde et tous les systèmes qui n'ont pas d'intention malveillante ont, ou devraient avoir, une identité et des privilèges d'accès spécifiques. À mesure que les environnements IT s'étendent et que les terminaux se multiplient, la gestion des identités et des accès devient un sujet central des conversations de sécurité.

La plupart des organisations disposent d'Active Directory® et ont recours à divers services tiers. Cela se traduit par de multiples identités, systèmes et solutions, et de nombreuses complications, en particulier lorsque tous ces éléments requièrent une gestion manuelle.

Voici plusieurs considérations à prendre en compte pour la gestion des identités et des accès, en ce qui concerne la sécurité :

Pensez aux données.

À quel point sont-elles sensibles ? Qui a vraiment besoin d'y accéder ? Quand et pendant combien de temps ? Quel est le point de contact initial, et est-ce la meilleure option ? Les organisations peuvent avoir besoin de procéder à une démarche de classification des données dans un premier temps.

Pensez à vos utilisateurs.

Avez-vous établi des types d'utilisateurs ? Quand avez-vous contrôlé les autorisations pour la dernière fois ? Comment vérifiez-vous les identités et les points d'accès ? De la défense renforcée à la confiance zéro, il existe de nombreux modèles viables.

Pensez à l'authentification.

Les mots de passe sont en train de tomber en désuétude, rapidement. Quelles alternatives avez-vous envisagées ? Des mécanismes tels que la biométrie fonctionneraient-ils pour votre organisation ? Comment pourriez-vous faire évoluer votre approche actuelle de l'authentification vers une approche plus sécurisée dans un futur proche ?

Pour que la gestion des identités et des accès soit stratégique et réussie, les organisations doivent conserver toutes les identités dans un référentiel unique, envisager la mise en œuvre d'une solution Cloud Access Security Broker (CASB) et mettre en œuvre une approche de sécurité en couches.

CHAPITRE 4

Automatisation et flux de travail rationalisés

La sécurité n'a pas de deuxième chance. Toute vulnérabilité ou faille peut être exploitée à tout moment. On ne peut pardonner les erreurs humaines qui conduisent à des attaques réussies. En matière de sécurité, les erreurs coûtent cher. Paradoxalement, les éviter peut également s'avérer très coûteux, selon l'approche que vous adoptez.

Que voulons-nous dire par là ? Les centres d'opérations de sécurité (SOC) doivent être modernisés, y compris les ensembles d'outils, les technologies, les processus/méthodologies et les ressources. Dans l'enquête « L'état de la modernisation IT 2020 », 57 % des personnes interrogées ont déclaré que la mise à niveau de l'infrastructure et des processus de sécurité était un obstacle majeur à la modernisation de l'environnement d'exploitation IT.[5] Mais, lorsque les ressources internes sont rares, les organisations doivent trouver des partenaires externes capables d'apporter l'automatisation et d'autres compétences essentielles.

L'automatisation au sein du SOC offre :

- Des capacités de détection, de réponse et de remédiation plus rapides
- Moins d'erreurs dues aux efforts manuels
- Des ressources de sécurité libérées pour les priorités stratégiques
- De meilleures expériences utilisateur et satisfaction

Certaines tâches sont particulièrement bien adaptées à l'automatisation. Prenez par exemple la réponse aux alertes. Dans une étude menée par CRITICALSTART, 70 % des personnes interrogées ont déclaré qu'elles enquêtaient sur plus de 10 alertes par jour, chacune prenant plus de 10 minutes (chiffres qui étaient respectivement 45 % et 64 % plus élevés que l'année précédente). La lassitude liée aux alertes est une plainte courante dans de tels environnements, ce qui conduit les professionnels des SOC à ignorer les alertes, à payer pour embaucher plus de collaborateur pour partager la charge, voire à quitter entièrement leur poste.[7]

En réduisant le nombre de tâches répétitives effectuées par les collaborateurst en automatisant les processus de sécurité courants, les organisations peuvent accroître la motivation des équipes, créer un SOC plus stratégique et adopter plus facilement une approche multicouche de la sécurité avec moins de ressources.

[7] CRITICALSTART. (2019). The Impact of Security Alert Overload.

CHAPITRE 5

Outils efficaces et ressources qualifiées

Une organisation ne peut pas faire grand-chose sans les bons outils, les bonnes technologies et les bonnes ressources. Le mot clé de la réussite étant « approprié ». Un rapport du Ponemon Institute a révélé que les entreprises ont déployé en moyenne 47 solutions et technologies de cybersécurité.[8] Le même rapport indique que plus de la moitié (53 %) des experts IT ne savent pas dans quelle mesure les outils de cybersécurité qu'ils ont déployés fonctionnent, et seulement 39 % déclarent qu'ils tirent pleinement parti de leurs investissements en sécurité.

Quel est le problème ? Il en existe plusieurs :

- Disposer du temps ou posséder l'expertise nécessaires pour prendre des décisions judicieuses concernant les produits ou plateformes de sécurité
- Comprendre les compétences requises pour déployer, adopter, intégrer, personnaliser et optimiser les investissements de sécurité
- Environnements IT complexes (en raison de la croissance rapide, de l'activité de fusions et acquisitions, etc.) présentant une multitude de vecteurs d'attaque
- Ajustement des investissements IT aux budgets, ce qui entraîne parfois des compromis contraignants
- Acquérir des solutions ponctuelles qui offrent chacune une portée limitée et contribuent à la fatigue des outils
- Trouver et retenir des talents indispensables en matière de sécurité

Les directeurs IT doivent continuellement réévaluer leur niveau de risque et leurs capacités de réponse aux menaces, tout en tirant parti des dernières offres de sécurité. En coopérant étroitement avec les dirigeants des entreprises et des secteurs d'activité, les organisations informatiques peuvent également s'assurer de l'adhésion nécessaire pour développer une organisation sensibilisée à la sécurité et minimiser l'apparition de l'informatique parallèle et d'autres comportements à risque.

Comment répondez-vous à ces préoccupations et apportez-vous des améliorations significatives à vos opérations de sécurité ?

[8] Ponemon Institute. (2019). The Cybersecurity Illusion: The Emperor Has No Clothes. Sponsorisé par AttackIQ.

Rechercher des sources fiables

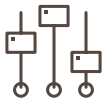
Insight aide les organisations à évaluer leur environnement de sécurité, à développer une feuille de route exploitable, à mettre en œuvre les solutions optimales et à gérer un SOC de premier ordre qui présente les cinq attributs décrits ici. Notre principe est que la sécurité n'est pas seulement un problème technologique, mais une priorité commerciale : nous conjuguons expérience technique et de conseil et intelligence pour renforcer l'ensemble de votre programme de sécurité.

L'une de nos solutions est Microsoft® Sentinel™, une solution Cloud native de gestion des informations et des événements de sécurité (SIEM) et d'orchestration de la sécurité et de réponse automatisée (SOAR) qui collecte les données de sécurité dans toute l'entreprise et utilise la puissance de l'intelligence artificielle (IA) pour identifier et enquêter rapidement sur les menaces.

Pourquoi Insight et Microsoft Sentinel ?

Maximisez les avantages et les capacités de votre investissement dans la sécurité

Mieux aligner les efforts de sécurité sur les objectifs commerciaux



L'objectif : améliorer la sécurité, la visibilité et le contrôle de l'ensemble de votre environnement IT

Accélérer et automatiser la traque et la détection des cybermenaces

Simplifier la tâche de surveillance de votre réseau, de vos systèmes, de vos applications et de vos données

Réduire les risques et rendre les coûts liés à la sécurité plus prévisibles

À propos d'Insight

Plus de 20 ans de prestation de Support services

Conforme à la norme PCI DSS, certifié SOC 2 Type II, certifié ISO 27000 et membre de TSANet et TSIA

Un partenaire Microsoft de premier plan avec **18 compétences Gold et Silver**

Gold Microsoft Partner Microsoft | Azure Expert MSP

Expert Managed Services Provider (MSP) Azure et **plus grand partenaire Azure**

Récemment récompensé par le prix Microsoft Security 20/20 pour la catégorie Partenaire de déploiement Azure Security de l'année

Que dit Microsoft ?

Ann Johnson, vice-présidente des solutions de cybersécurité chez Microsoft, a déclaré : « En associant notre portefeuille de sécurité Microsoft aux services de sécurité d'Insight, nous donnons à nos clients les moyens de moderniser leurs opérations de sécurité. La cybersécurité est complexe, mais elle n'a pas besoin d'être compliquée. Le renforcement de notre relation avec Insight en matière de sécurité aide les organisations à simplifier leurs opérations de sécurité et à accompagner leur croissance. »

À propos de Microsoft Sentinel

- Rapide et relativement facile à déployer, sur site vierge ou via la redirection des journaux
- Flexible et évolutif, permettant des ajustements dynamiques en fonction des charges de travail ou de la conformité
- Rentable, sans coûts initiaux ni exigences matérielles
- Développé et constamment amélioré par les leaders du secteur IT et de la sécurité
- Exploite les avancées de l'IA et de l'apprentissage automatique de pointe

Obtenez les outils et l'expertise dont vous avez besoin pour atteindre les cinq attributs décrits dans cet eBook. Démarrez avec Insight et Microsoft Sentinel dès aujourd'hui.

Nous contacter

fr.insight.com

MKT6270_FR