Gros plan sur la sécurité : Le coût des erreurs humaines et les avantages de l'automatisation

Pourquoi les organismes publics remettent en cause la gestion manuelle de la sécurité et comment l'automatisation intelligente aide à prévenir les menaces dues à des failles de sécurité coûteuses

Suivant

Sommaire :

01 Introduction : la cybercriminalité, une menace grandissante

02 La sécurité est l'affaire de tous

03 Défis courants liés à la gestion des risques

04 Renforcer votre posture de sécurité avec l'automatisation

05 Notre rôle dans la cybersécurité

01 Introduction : la cybercriminalité, une menace grandissante

La cybercriminalité est en hausse. L'année 2021 a connu une augmentation du nombre de cyberattaques (+15,5 %) et du nombre de failles significatives (+24,5 %[1]. Pour autant, 34 % des organismes du secteur public affirment ne pas être suffisamment préparés face à l'évolution rapide des menaces[1].

Les organismes publics adoptent de nouvelles technologies et s'adaptent aux modèles de travail hybrides, mais les méthodes des cybercriminels évoluent également. La main-d'œuvre et les ressources de calcul sont de plus en plus distribuées, et l'infrastructure informatique en constante évolution offre aux acteurs malveillants de nouvelles opportunités d'exploiter les potentielles failles et vulnérabilités, augmentant alors les coûts organisationnels engendrés par les fuites de données. Même avec une posture de sécurité forte, les entreprises courent plus de risques dans ce type d'environnement.

La cybersécurité proactive

Parce que les cybercriminels trouvent sans cesse de nouveaux moyens de s'infiltrer dans les systèmes protégés et voler des données, les entreprises subissent des pressions internes et externes pour développer des protections plus stratégiques et proactives contre les cyberattaques. Par ailleurs, les mesures de sécurité et de confidentialité des données qu'elles mettent en place doivent respecter un ensemble exhaustif de règles et réglementations.

La multiplication des réglementations de sécurité et de confidentialité touche tous les secteurs d'activité et toutes les régions. Par exemple, le Règlement général sur la protection des données (RGPD) de l'Union européenne définit des règles strictes pour la collecte, l'utilisation et la protection des données personnelles. À Singapour, le Cybersecurity Act de établit un cadre qui oblige les propriétaires d'infrastructures hébergeant des données critiques à suivre des meilleures pratiques concernant, entre autres, la gouvernance, le contrôle des accès, et la détection et la résolution des incidents. En Argentine, la Dirección Nacional de Ciberseguridad élabore des politiques nationales pour protéger les infrastructures de données critiques et améliorer la prévention des incidents de sécurité, ainsi que les processus de détection, résolution et récupération. Aux États-Unis, les administrations publiques sont tenues de déployer des architectures Zero Trust pour tenir les objectifs de cybersécurité du gouvernement fédéral d'ici fin 2024.

Renforcer vos défenses

L'identification des vulnérabilités constitue la première étape pour améliorer une stratégie de cybersécurité. Trop souvent, les erreurs humaines et un manque d'information peuvent compromettre la sécurité, y compris lorsque des stratégies globales sont déjà en place. En cas d'absence de contrôle, une erreur, même mineure, risque de mettre en péril les systèmes, aggravant de ce fait un problème déjà complexe. C'est ce qui conduit les entreprises à adopter l'automatisation comme un moyen d'améliorer la fiabilité de leur stratégie de sécurité et de limiter les risques.

Dans ce livre numérique, nous étudierons les effets des risques introduits par les erreurs humaines sur la lutte contre la cybercriminalité. Nous verrons aussi comment renforcer la sécurité et libérer les équipes informatiques d'un grand nombre de tâches chronophages grâce à des stratégies automatisées d'atténuation des risques de cybermenaces.

Le coût global de la cybercriminalité

24,5 %

Hausse du nombre de failles significatives en 2021[1]

4,35 milliards de dollars

Coût moyen global d'une fuite de données[2]

60 %

Pourcentage d'entreprises ayant augmenté leurs tarifs à cause d'une fuite de données[2]

1. ThoughtLab, « Cybersecurity Solutions for a Riskier World », 2022
2. IBM, « Rapport 2022 sur le coût d'une violation de données », juillet 2022

02 La sécurité est l'affaire de tous

L'erreur est humaine

Même au sein des équipes informatiques, bien souvent, les individus sous-estiment ou comprennent mal les vulnérabilités de leurs systèmes et les risques qui en découlent pour la sécurité. Cette incapacité à évaluer précisément les risques peut engendrer des coûts importants pour les organisations.

Prenons un exemple : une panne de production survient au niveau d'un pare-feu, ce qui oblige l'ingénieur concerné à mettre à jour manuellement une politique en urgence. Si ce changement permet effectivement de résoudre la panne, il offre cependant un nouveau vecteur d'attaque aux cybercriminels.

Dans ce scénario, la modification manuelle et dans l'urgence de la configuration du pare-feu peut avoir des effets négatifs entraînant un coût pour l'entreprise : corruption des données, violation des réglementations gouvernementales et sectorielles en matière de sécurité des données, interruption des services et arrêt du système.

Application des correctifs, mise à jour des pare-feu, paramétrage et application des droits d'administrateur... L'infrastructure de sécurité repose sur tellement d'aspects susceptibles de défaillir lorsqu'ils sont gérés manuellement. Et comme les cybercriminels identifient et exploitent de mieux en mieux les vulnérabilités, traiter ces tâches de façon entièrement manuelle peut avoir des conséquences néfastes voire irréversibles.

Le manque de compétences, un risque supplémentaire

La rareté des compétences en matière de cybersécurité ne fait qu'augmenter le risque d'erreurs humaines lors de l'exécution de tâches manuelles. Il n'y a tout simplement pas assez de personnel compétent et formé pour évaluer et traiter ces risques de sécurité. Selon l'étude (ISC)[2] Cybersecurity Workforce Study, il faudrait 2,72 millions de professionnels en plus pour répondre à la pénurie mondiale de spécialistes en cybersécurité[3].

Face à cette pénurie chronique de talents, les entreprises ont plus de difficultés à gérer les risques de manière adéquate. Déjà surchargées, leurs équipes informatiques n'ont pas le temps d'appliquer des processus de sécurité, et encore moins de les définir.

Doter les équipes de sécurité d'outils d'automatisation

Pour lutter contre la cybercriminalité, il est devenu essentiel d'apporter une réponse face aux risques accrus causés par les processus manuels de sécurité et la pénurie de personnel qualifié. L'automatisation semble être une solution prometteuse. Comme nous le verrons plus en détail, l'automatisation des processus de sécurité offre ce niveau de cohérence, de précision et d'évolutivité si indispensables dans l'entreprise.

Les risques liés aux mesures de sécurité manuelles

« Les entreprise ayant automatisé totalement la sécurité avec l'IA ont été en mesure de détecter et contenir les failles beaucoup plus rapidement que celles qui n'ont pas réalisé ces déploiements[4] . »

3. Étude (ISC)[2] Cybersecurity Workforce Study, « A Resilient Cybersecurity Profession Charts the Path Forward », 2021
4. IBM, « Rapport 2022 sur le coût d'une violation de données », juillet 2022

03 Défis courants liés à la gestion des risques

Les organismes publics doivent mieux gérer les risques

Pour garantir la confidentialité, l'intégrité et la disponibilité des informations officielles, les organismes publics doivent être capables d'identifier et de gérer les risques, de façon efficace et précise. L'évolution incessante des menaces exige une certaine flexibilité quant au profil de risque et à la posture de sécurité. L'automatisation de l'exploitation s'avère essentielle pour répondre rapidement à ces changements.

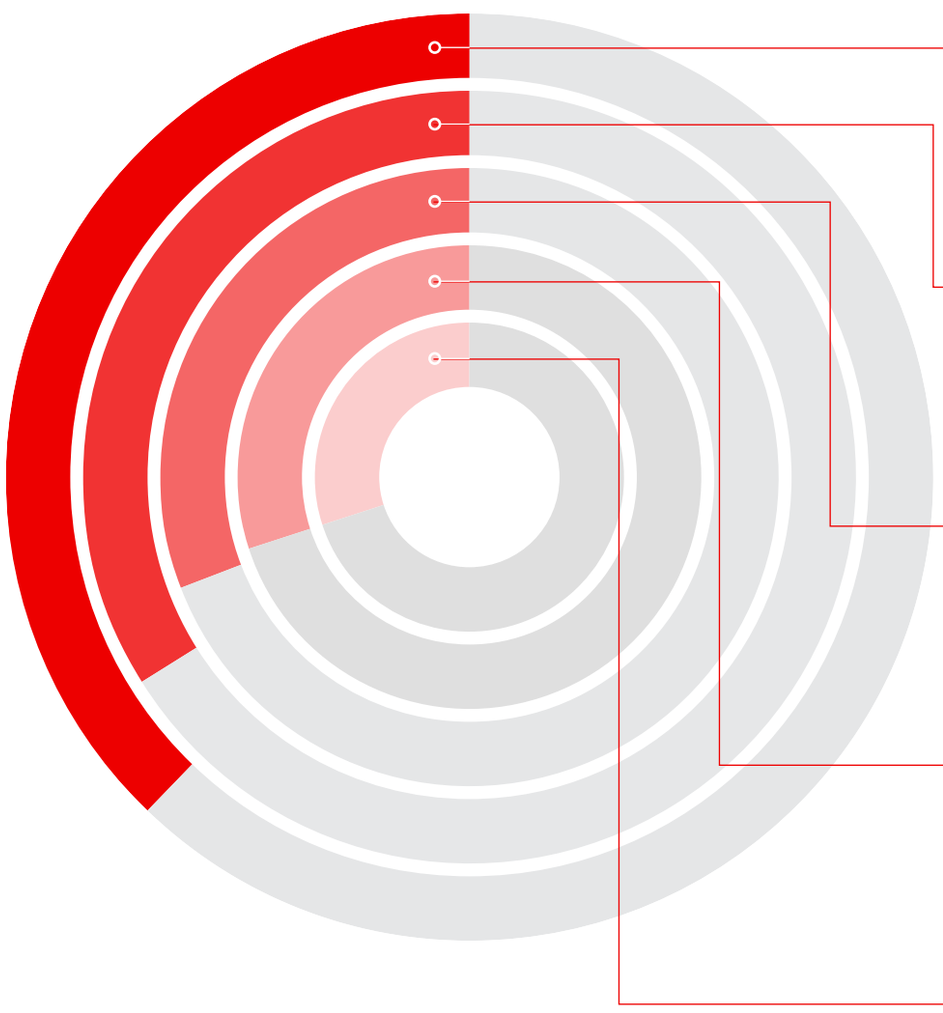
Les freins au changement

Les organismes publics qui souhaitent améliorer la sécurité font face à différents défis, notamment en lien avec la gestion des changements, et se posent de nombreuses questions. Voici les plus fréquentes :

- Comment faire évoluer nos équipes pour mettre en œuvre de nouvelles initiatives de cybersécurité ?
- Comment aider nos différents services à appliquer les nouveaux protocoles de sécurité ?
- Comment mieux protéger nos systèmes existants, qui fournissent des services essentiels, et en même temps adopter les stratégies modernes de sécurité dont nous avons besoin ?
- Pouvons-nous mettre en place des stratégies de type Zero Trust dans les architectures existantes ?

Au lieu d'appréhender l'évolution de la sécurité comme une difficulté, les entreprises peuvent la considérer comme une opportunité de repenser leurs pratiques et d'appliquer des protocoles plus rigoureux.

Défis courants de la cybersécurité



38%

Suivre l'évolution rapide des menaces de sécurité[5]

34%

Sensibiliser aux risques et comportements[5]

31%

Renforcer la posture de cybersécurité interne[5]

30%

Se former[5]

30%

Gérer les conséquences juridiques/financières des fuites de données[5]

5. « State of the Channel 2021, » CompTIA, août 2021

04 Renforcer votre posture de sécurité avec l'automatisation

Les aspects couverts par les réglementations

Dans tous les secteurs d'activité et toutes les régions, les réglementations et initiatives de cybersécurité couvrent des sujets communs, à savoir la confidentialité des données, le contrôle des accès, ainsi que la détection, la protection et la résolution des incidents. Certaines réglementations expliquent comment mettre en œuvre une stratégie de sécurité. Cependant, la plupart définissent seulement des lignes directrices et les résultats attendus. Les entreprises doivent donc trouver le moyen de se conformer du mieux qu'elles peuvent à ces règles en fonction de leur situation, de leurs effectifs actuels et de leur infrastructure.

L'automatisation de la sécurité peut aider les organismes publics et les entreprises à lutter contre la cybercriminalité et à se mettre en conformité. En automatisant des tâches répétitives et récurrentes, les équipes de cybersécurité se concentrent sur des tâches plus essentielles et stratégiques. L'automatisation libère aussi les équipes informatiques des tâches qui augmentent les risques d'erreur humaine et menacent davantage la sécurité.

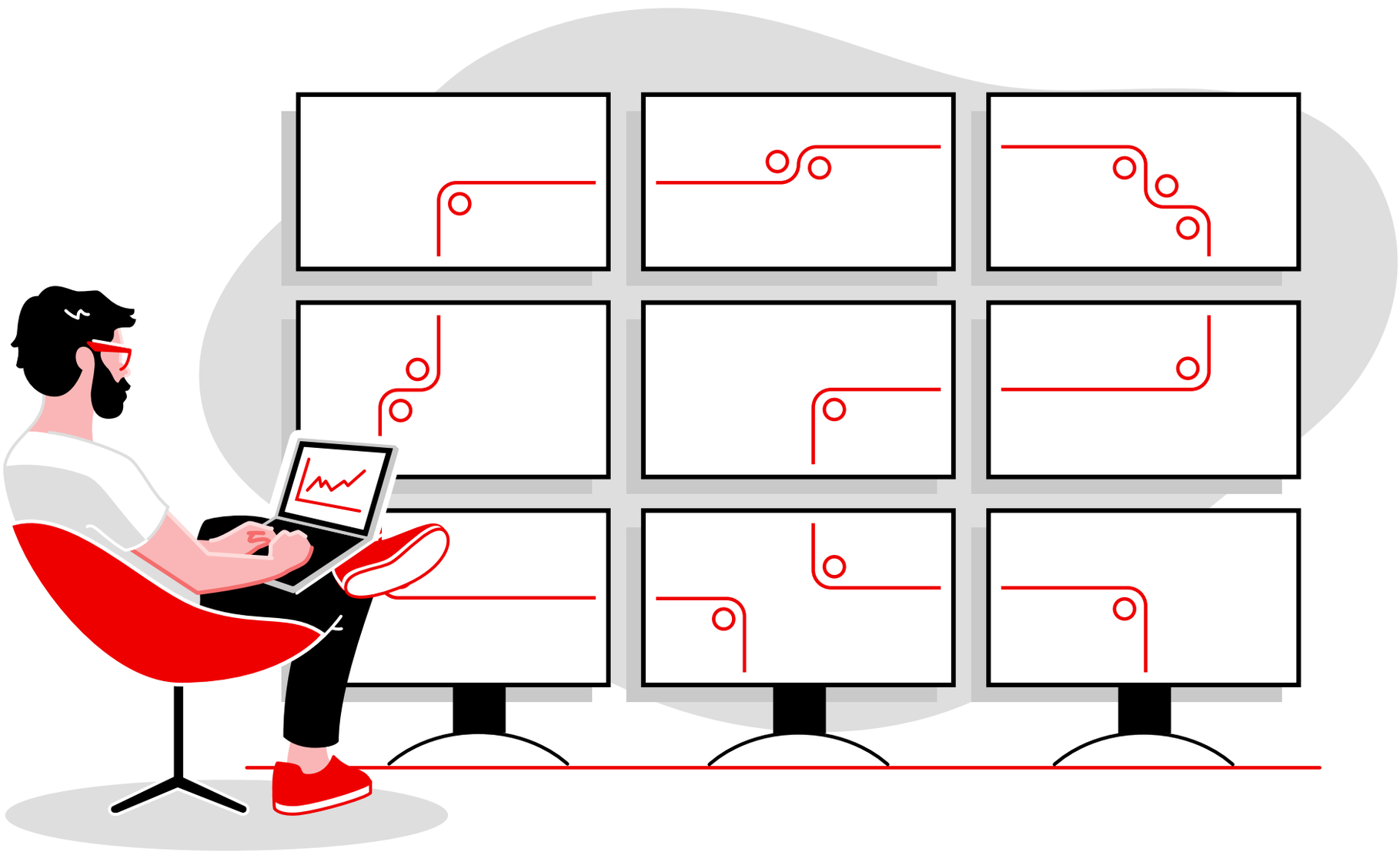
L'automatisation de la sécurité connecte les équipes

L'automatisation de la sécurité consiste en diverses pratiques qui relient les équipes et les domaines au sein de l'entreprise afin de mieux gérer les risques, se défendre contre les cybermenaces et atténuer l'impact des incidents. Par exemple, les analystes de la sécurité peuvent automatiser la résolution des incidents et les mesures de correction. Les équipes d'exploitation peuvent appliquer automatiquement des correctifs aux systèmes et assurer la conformité, et les administrateurs réseau configurer et gérer un contrôle des accès au réseau.

L'automatisation de la sécurité contribue aussi à l'optimisation de la collaboration entre les équipes sécurité et informatiques et les autres services de l'entreprise, qui sont également soumises à des réglementations de sécurité (comme les ressources humaines, le service client et le service juridique). En effet, la plupart des entreprises ont l'obligation de vérifier leurs contrôles de sécurité et signaler les incidents informatiques, par exemple. Les auditeurs exigent des preuves de conformité, mais ils n'interagissent pas toujours directement avec les systèmes de sécurité de l'entreprise. Avec l'automatisation des processus de sécurité, il est possible d'intégrer des systèmes de journalisation externes et de garder une trace de ses actions, ce qui permet de fournir les rapports et autres preuves demandés par les auditeurs.

Mieux gérer les risques avec l'automatisation

L'automatisation des processus métier clés peut vous aider à renforcer votre posture active et passive de sécurité. Dans les sections suivantes, nous aborderons différents domaines où l'automatisation de la sécurité peut faciliter votre mise en conformité et apporter de réels bénéfices à votre entreprise, peu importe la région où vous vous trouvez.



Résolution des incidents et correction

En 2022, il fallait en moyenne 277 jours pour identifier et maîtriser une fuite de données[6]. En-deçà de 200 jours, le coût moyen d'une telle fuite diminue de 26,5 %[6]. Néanmoins, la détection et la correction manuelles des failles avec plusieurs plateformes, outils et environnements sont des tâches difficiles, chronophages et sujettes aux erreurs.

La résolution d'un incident implique de prendre les mesures nécessaires pour interrompre la progression d'une faille. Une fois la faille découverte, les équipes de sécurité doivent réagir rapidement et dans l'ensemble de l'entreprise pour la maîtriser. Toutefois, les mesures de résolution comprennent souvent de nombreuses tâches manuelles sur des systèmes non connectés, ce qui ralentit la correction et laisse votre entreprise vulnérable aux attaques pendant plus longtemps.

En codifiant vos actions de correction dans des playbooks reproductibles et pré-approuvés, l'automatisation des processus de sécurité permet de traiter les incidents plus rapidement. Vous pouvez accélérer certaines tâches, par exemple : bloquer les adresses IP ou domaines des pirates, autoriser le trafic non menaçant, « geler » les informations d'identification compromises, ou encore isoler les charges de travail suspectes le temps d'un examen plus approfondi afin de minimiser les dommages causés par l'incident.

Correctifs et mises à jour des systèmes

Pour éviter les attaques, de nombreuses normes de cybersécurité recommandent aux entreprises de régulièrement appliquer des correctifs et mettre à niveau leurs systèmes et applications. Or, exécutées manuellement, ces tâches sont toujours sujettes aux erreurs humaines et peuvent s'avérer particulièrement chronophage dans les grandes entreprises.

L'importance d'un traitement rapide

277 jours

Temps moyen nécessaire pour identifier et stopper une fuite de données en 2022[6]

26,5 %

Réduction des coûts avec la détection et l'identification des fuites de données en 200 jours ou moins[6]

L'application de correctifs est un excellent cas d'utilisation pour l'automatisation des workflows. Plutôt que de gérer manuellement les tests, les vérifications préliminaires et le déploiement des correctifs, les entreprises peuvent automatiser la vérification et l'évaluation. Ainsi, elles s'assurent que toutes les étapes du processus s'effectuent de manière fluide et efficace, avec les mesures de sécurité adaptées en arrière-plan.

Gestion des privilèges et des informations d'identification

Les informations d'identification volées ou compromises sont la cause la plus fréquente des fuites de données[6]. En centralisant et en contrôlant les accès privilégiés et les informations d'identification, vous pourrez réduire les risques et veiller au respect des réglementations en matière de confidentialité et sécurité des données.

Appliquez le principe du moindre privilège pour autoriser uniquement les accès dont les utilisateurs ont réellement besoin. Même si vous devrez vérifier et réévaluer les droits d'accès actuels pour chaque utilisateur, les répercussions en cas de vol ou compromission d'informations d'identification seront moindres.

Lorsque les informations d'identification sont centralisées, il n'est plus nécessaire de les injecter directement dans les applications, là où elles sont les plus vulnérables. L'automatisation des workflows associés aux accès privilégiés ne rend pas seulement le processus plus gérable, fiable et cohérent : elle permet de poser les bases d'une architecture et d'une approche de type Zero Trust.

Mise en conformité et application des politiques

44 % des failles de sécurité les plus importantes subies par les entreprises provenaient essentiellement d'erreurs de configuration[7]. Les systèmes mal configurés sont plus vulnérables aux attaques. Et en l'absence de contrôles stricts des modifications, les systèmes pourtant configurés de manière adéquate lors du provisionnement peuvent également devenir vulnérables avec le temps.

En appliquant des politiques pendant tout le cycle de vie de vos systèmes et applications, vous vous assurez que ceux-ci sont correctement configurés au départ et qu'ils le restent. L'automatisation aide à accomplir cette tâche rapidement et à grande échelle, tout en améliorant la cohérence de vos différents systèmes et environnements distribués. Vous pouvez également automatiser le contrôle des modifications pour vérifier que les demandes de changement sont bien approuvées, enregistrer les actions de modification et générer des rapports pour les audits.

6. IBM, « Rapport 2022 sur le coût d'une violation de données », juillet 2022
7. ThoughtLab, « Cybersecurity Solutions for a Riskier World », 2022

Architectures Zero Trust

En automatisant chacun des domaines cités précédemment, votre entreprise acquiert une expérience précieuse et pose les bases d'une architecture Zero Trust. Le modèle d'architecture Zero Trust ne se limite pas à la protection du périmètre, il sécurise chaque ressource sur le réseau. Aucun acteur, système, réseau ou service intervenant à l'intérieur ou à l'extérieur du périmètre de sécurité n'est considéré comme fiable de manière implicite. Pour établir une confiance explicite lorsqu'un utilisateur ou un sujet souhaite se connecter à une ressource, la session doit être authentifiée et autorisée.

La gestion des identités et des accès est au cœur des architectures Zero Trust. Chaque sujet qui veut interagir avec une ressource doit demander un accès pour cette interaction spécifique, et le risque inhérent à l'interaction doit être évalué avant d'autoriser l'accès. Cette évaluation repose notamment sur une analyse de l'identité et des attributs du sujet. Vous devez déterminer les informations contextuelles : qui demande l'accès et à quelles ressources, la finalité de la transaction et les mesures à appliquer pour limiter cet accès.

Une fois l'accès accordé, vous devez stocker, gérer, organiser et mettre à jour les identités et les attributs liés de manière cohérente et sécurisée. La plupart des entreprises utilisent un ou plusieurs systèmes de gestion des identités et des privilèges pour administrer ces informations. Il est aussi important de réévaluer en permanence les accès accordés pour garantir leur validité au fil du temps.

Comme une évaluation des risques est requise à chaque interaction, les approches Zero Trust impliquent de collecter de grandes quantités de données et d'informations, à l'échelle de l'infrastructure et de l'entreprise. C'est là que l'automatisation devient indispensable. Premièrement, le nombre d'interactions est trop élevé pour que les équipes informatiques puissent les gérer elles-mêmes. Si chaque interaction devait être évaluée manuellement, il serait impossible d'attribuer rapidement l'accès aux ressources.

Ensuite, l'automatisation facilite la collecte des données provenant de systèmes disparates. Par exemple, toute demande d'accès à une application interne par un membre de l'équipe nécessite de collecter et vérifier un minimum d'informations : le dossier d'embauche sur le système des ressources humaines, les données d'identité sur le système informatique, et l'état et la localisation de la personne sur son ordinateur. Grâce à la plateforme d'automatisation qui relie des systèmes et domaines qui, habituellement, n'interagissent pas (ou ne peuvent pas interagir) entre eux, il est possible de rassembler et d'analyser plus facilement et rapidement les informations. Si besoin, vous pouvez même envoyer ces informations à une solution de gestion des informations et des événements de sécurité (SIEM) et à d'autres systèmes de sécurité centralisés.

Enfin, l'automatisation permet de répondre de manière dynamique aux événements et aux changements d'état associés aux utilisateurs. Lorsqu'un utilisateur quitte l'entreprise ou change de poste, avec l'automatisation orientée événements, ses accès sont immédiatement mis à jour sur tous les systèmes. Vous n'avez plus à attendre l'exécution manuelle de cette action.

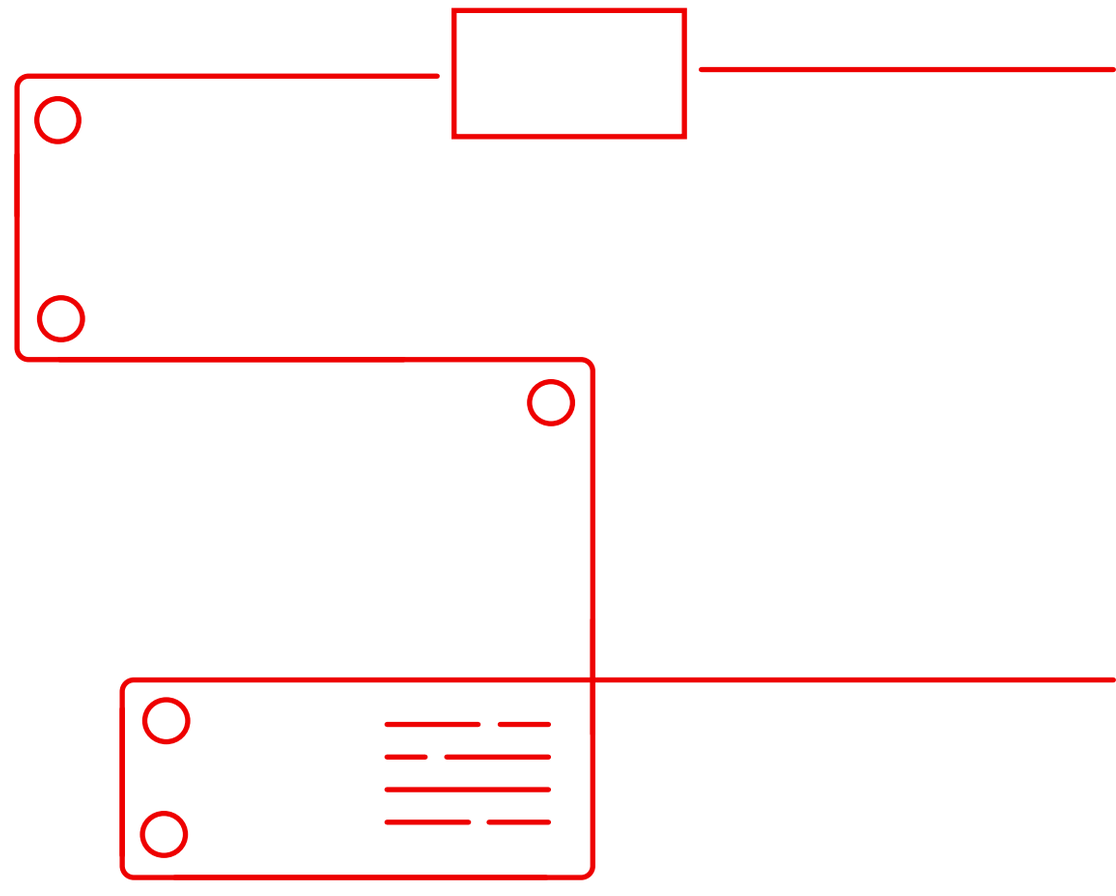
Les avantages des approches Zero Trust

20,5 %

Économie sur les fuites de données grâce à une architecture Zero Trust[8]

1,65 million de dollars

Économie moyenne sur les fuites de données grâce à une architecture Zero Trust mature par rapport aux entreprises qui n'en ont pas déployée[8]



8. IBM, « Rapport 2022 sur le coût d'une violation de données », juillet 2022

05 Notre rôle dans la cybersécurité

Élaborer une stratégie de sécurité tournée vers l'avenir

Avec un modèle de maturité de la cybersécurité basé sur l'automatisation, vous pouvez mettre en place des mesures concrètes pour remplacer les processus manuels, gérer les risques et améliorer votre posture de sécurité, rapidement et de manière itérative. Nous proposons des solutions qui aident à automatiser les processus manuels afin de limiter les risques d'oublis liés à des équipes informatiques surchargées et en sous-effectif. Nos produits Open Source vous apportent flexibilité et évolutivité dans l'ensemble de vos architectures et environnements cloud. Vous pouvez ainsi renforcer votre sécurité aujourd'hui et vous préparer aux incertitudes de demain.

Red Hat Ansible Automation Platform

La solution Red Hat Ansible® Automation Platform repose sur un langage d'automatisation facile à lire qui transforme des processus manuels complexes en workflows automatisés. Ansible Automation Platform permet à vos équipes informatiques d'automatiser et d'intégrer des protocoles de sécurité dans toute l'entreprise. Avec cette plateforme, votre entreprise peut examiner les menaces et y répondre de manière coordonnée et unifiée, en utilisant des contenus d'automatisation certifiés et personnalisés. Exemples de processus que vous pouvez automatiser :

- La mise à jour et la correction des CVE (Common Vulnerabilities and Exposures)
- Le déploiement des contrôles d'applications
- La sauvegarde, la restauration et la vérification

La solution Ansible Automation Platform fournit un cadre stable et axé sur la sécurité pour le déploiement et l'exploitation de processus automatisés à l'échelle de l'entreprise, du cloud hybride à la périphérie du réseau. Elle permet à toutes les équipes d'une entreprise (développement, exploitation, sécurité, réseau) de créer, partager et gérer du contenu et des playbooks d'automatisation. Les responsables informatiques peuvent fournir des consignes aux différentes équipes sur l'application de l'automatisation, tandis que les créateurs de processus automatisés exploitent leurs connaissances actuelles pour l'écriture des tâches.

La solution Ansible Automation Platform peut aussi constituer un point d'intégration des solutions de sécurité qui utilisent le contenu de partenaires certifiés tels que CyberArk, IBM et Splunk, ce qui permet de gérer et d'intégrer d'autres technologies de sécurité de façon automatisée.

En savoir plus sur Red Hat Ansible Automation Platform >

Red Hat Enterprise Linux

La solution Red Hat Enterprise Linux® fournit une base sur laquelle vous pouvez faire évoluer vos applications et déployer des technologies émergentes, que ce soit sur des systèmes bare metal, virtuels, cloud ou d'edge computing. Tout cela en maintenant la cohérence de vos mesures de sécurité.

Red Hat Enterprise Linux relève les défis liés à la sécurité grâce à une approche pratique qui s'articule autour de trois axes :

- Réduction des risques : gérez la sécurité et réduisez les risques de faille avant que vos données, vos systèmes ou votre réputation ne soient atteints.
- Renforcement de la sécurité : automatisez les contrôles de sécurité et maintenez-les dans la durée, à grande échelle, en évitant autant que possible les temps d'arrêt.
- Mise en conformité : rationalisez les normes de conformité dans les environnements fortement réglementés.

Red Hat Enterprise Linux intègre également des politiques de sécurité qui respectent de nombreuses normes et réglementations, notamment la certification Critères communs, la norme FIPS (Federal Information Processing Standard) 140 et les directives STIG (Secure Technical Implementation Guidelines). Ces politiques vous aident à mieux gérer les risques grâce à l'application automatisée et cohérente des contrôles de sécurité aux nouveaux services numériques.

En savoir plus sur Red Hat Enterprise Linux >

Red Hat

Précédent

Renforcez votre sécurité avec Red Hat

Red Hat vous aide à améliorer la sécurité de vos services numériques

Nous pouvons vous aider à automatiser la mise en conformité avec les normes réglementaires et directives, ainsi qu'à optimiser la gestion des risques avec l'intégration automatisée de solutions de sécurité.

Pour en savoir plus, contactez-nous dès maintenant >