Microsoft Security

3 raisons de passer à la protection intégrée contre les menaces

Sommaire

Introduction

L'entreprise moyenne utilise aujourd'hui plus de 30 outils de sécurité différents, souvent disjoints et ajoutés en option.

La sécurité arrive à un tournant majeur. Les cyberattaques sont de plus en plus sophistiquées et les entreprises luttent contre la pénurie de talents et l'équilibre des coûts relatifs à la gestion des contraintes du travail hybride.

En parallèle, le marché de la sécurité est plus fragmenté et complexe que jamais. L'entreprise moyenne utilise aujourd'hui plus de 30 outils de sécurité différents, souvent disjoints et ajoutés en option, offrant une visibilité limitée et des informations inadéquates aux centres d'opérations de sécurité (SOC).

Les responsables de la sécurité et de la conformité veulent mieux comprendre les nouveaux risques et menaces, mais ils ont également besoin de savoir ce qui fonctionne, ce qui ne fonctionne pas et quelles sont les lacunes.

Bien que les défis en matière de sécurité paraissent parfois insurmontables, les RSSI qui cherchent à améliorer l'efficacité de leurs opérations de sécurité ont tout lieu d'être optimistes. La réponse se trouve dans une approche de bout en bout intégrée de la protection contre les cybermenaces et voici pourquoi :

Raison 1 : Aller plus loin avec moins de ressources

Renforcez vos solutions ponctuelles et réduisez la charge des opérations de sécurité (SecOps).

Raison 2 : Permettre aux professionnels SecOps de se concentrer sur les tâches à forte valeur ajoutée

Utilisez des outils qui améliorent l'efficacité et rendent les analystes plus performants que jamais.

Raison 3 : Augmenter la productivité du personnel

Protégez votre entreprise d'une manière qui permette à vos collaborateurs de créer et d'innover sans crainte.

Cette approche est rendue possible par l'intégration d'une solution de détection et de réponse étendue (XDR) à un système d'informations de sécurité et gestion des événements (SIEM) natif du Cloud qui utilise l'intelligence artificielle (IA) et les capacités d'automatisation. La solution intégrée peut aider votre SOC à devenir plus prédictif, proactif et préventif contre les attaques sur toute votre entreprise.

Raison 1

Aller plus loin avec moins de ressources

En consolidant vos outils avec la solution intégrée de Microsoft, vous pouvez également économiser en ne payant que ce que vous utilisez.

De nombreuses entreprises ont adopté une approche de la sécurité consistant à se concentrer sur les meilleures solutions ponctuelles. Malheureusement, cette approche rend souvent plus difficile pour les professionnels de la sécurité d'identifier et de répondre rapidement aux menaces. Elle peut également finir par avoir un impact négatif sur les dépenses informatiques et la productivité des utilisateurs finaux.

Pour les entreprises qui cherchent à faire plus avec moins de ressources, une approche intégrée, telle que les solutions SIEM et XDR de Microsoft, peut s'avérer utile. Une telle approche permet de réduire la complexité en consolidant les outils individuels. De plus, étant donné qu'elle est native du Cloud, elle peut également améliorer les performances et la mise à l'échelle.

En consolidant vos outils avec la solution intégrée de Microsoft, vous pouvez également économiser en ne payant que ce que vous utilisez. Vous pouvez également réduire les frais généraux SecOps nécessaires à la gestion des solutions en augmentant l'automatisation et l'intégration.

> Il n'est jamais trop difficile d'adopter de nouveaux outils de sécurité, car on sait d'avance que les lacunes seront importantes. Mais on se rend vite compte que des outils de différents fournisseurs ont parfois les mêmes fonctions. Cela peut être souhaitable pour les contrôles et les équilibres, mais **peut aussi engendrer d'importants frais inutiles.** »
>
> **Jonathan Cassar**
> Directeur général de la technologie, MITA

1,6 million de dollars

économisés chaque année grâce à la consolidation des fournisseurs

Microsoft a chargé Forrester Consulting de réaliser une étude Total Economic Impact™ (TEI) et d'examiner le retour sur investissement (ROI) potentiel que les entreprises peuvent réaliser en déployant Microsoft SIEM et XDR. Voici quelques-unes des principales conclusions pour une entreprise témoin comptant 8 000 collaborateurs au total et 10 professionnels de la sécurité :

- **Près d'1,6 million de dollars économisés par an grâce à la consolidation des fournisseurs.** Grâce à l'investissement dans Microsoft SIEM et XDR, l'entreprise témoin a pu réduire le coût de son ancien SIEM (560 000 $), de l'infrastructure sur site associée (plus de 360 000 $), de trois solutions ponctuelles XDR (192 000 $), ainsi que le coût de la main-d'œuvre pour gérer ces solutions (480 000 $).

- **Réduction du risque de violation matérielle de 60 %.** Grâce à une meilleure efficacité des tâches associées aux enquêtes et aux réponses de sécurité, à une meilleure automatisation des réponses de sécurité et à une meilleure protection de tous les environnements informatiques, y compris la protection multicloud, l'entreprise témoin a pu réduire le risque d'infraction et a ainsi économisé 1,6 million de dollars par an.

- **207 % de retour sur investissement.** Des entretiens représentatifs et des analyses financières ont révélé qu'une entreprise témoin a pu économiser 17,68 millions de dollars sur trois ans pour un investissement de 5,76 millions de dollars, ce qui constitue une valeur nette actuelle (VAN) de 11,92 millions de dollars.

Raison 2

Permettre aux professionnels SecOps de se concentrer sur les tâches à forte valeur ajoutée

Il est essentiel d'intégrer les stratégies SIEM et XDR pour corréler les alertes, hiérarchiser les plus grandes menaces et coordonner les actions dans l'ensemble de l'entreprise.

Les équipes SecOps sont submergées par la quantité de signaux qu'elles doivent analyser, y compris de nombreux signaux de basse fidélité qui sont difficiles, voire impossibles, à détecter manuellement et à atténuer. À mesure que les menaces augmentent, il est difficile pour un SOC surchargé de suivre le rythme, surtout lorsqu'il essaie d'analyser des données provenant de plusieurs solutions ponctuelles. Il ne suffit pas d'allouer davantage de ressources pour combler les lacunes, car il est toujours difficile de trouver suffisamment de professionnels qualifiés dans le secteur de la sécurité.

C'est pourquoi il est essentiel d'intégrer SIEM et XDR pour corréler les alertes, hiérarchiser les plus grandes menaces et coordonner les actions à l'échelle de l'entreprise avec une IA et une automatisation avancées pour détecter et contrer les menaces de manière proactive.

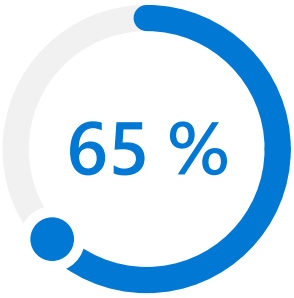
Par exemple, un signal unique de bas niveau attirera difficilement l'attention d'un SIEM classique. Mais à l'aide de l'intelligence artificielle, un SIEM natif du Cloud peut comparer automatiquement ce signal à des signaux provenant d'autres sources au sein de l'organisation, corrélant ainsi plusieurs ensembles de données pour trouver des attaques à plusieurs étapes.

L'intégration de SIEM et XDR libère les ressources SecOps tout en donnant plus de capacités et de confiance aux analystes, même débutants.

Le système normalise, analyse et corrèle ensuite les données, tout en fournissant le contexte sur l'entrée de la cyberattaque dans l'infrastructure, ainsi que la chronologie de sa propagation. Cela permet aux équipes SOC de visualiser la violation (à partir d'une seule console) et de la corriger efficacement.

> Beaucoup de DSI ne se rendent pas compte de **l'intensité de la charge qu'ils imposent à leurs équipes avec 20 écrans** ou outils ponctuels différents, sans parler des coûts annuels associés... Nous avons ainsi grandement réduit cette charge en passant par un seul fournisseur. »
>
> **Terence Jackson**
> Responsable de la sécurité de l'information et de la protection des données personnelles, Thycotic

Une entreprise ne devrait pas avoir besoin d'une expertise approfondie pour exploiter la valeur d'une solution de sécurité. L'intégration de SIEM et XDR libère les ressources SecOps tout en donnant plus de capacités et de confiance aux analystes, même débutants.



L'approche intégrée de Microsoft SIEM et XDR a réduit de 65 % le temps d'investigation des menaces.

L'étude Forrester Total Economic Impact™ (TEI) commandée par Microsoft a montré ce type d'efficacité SecOps dans son entreprise témoin :

- **Réduction du temps d'investigation des menaces de 65 % et du temps de réponse aux menaces de 88 %.** L'approche intégrée de Microsoft SIEM et XDR en matière d'investigation et de réponse aux menaces de sécurité rend ces charges de travail plus efficaces pour les professionnels de la sécurité de l'entreprise témoin. Ils n'ont plus besoin de passer par de multiples outils pour identifier les menaces, et les fonctions d'automatisation de la sécurité améliorent encore les flux de réponse.

- **Réduction de 90 % du temps de création d'un nouveau classeur et de 91 % du temps d'intégration de nouveaux professionnels de la sécurité.** L'approche intégrée de Microsoft SIEM et XDR rend également plus efficaces les charges de travail des autres professionnels de la sécurité. Les journaux SIEM étant intégrés dans l'ensemble de la suite de solutions, la création de classeurs est presque automatisée. De plus, le nouveau système de connexion unique permet d'intégrer les nouveaux professionnels de la sécurité plus rapidement et de gagner ainsi 16 semaines.

Raison 3

Augmenter la productivité du personnel

Une solution SIEM et XDR intégrée peut aider votre entreprise à améliorer la productivité des utilisateurs finaux.

Non seulement une solution intégrée SIEM et XDR permet d'en faire plus avec moins de ressources et d'augmenter l'efficacité SecOps, mais elle peut aussi aider l'entreprise à améliorer la productivité de son personnel.

Comme les équipes SecOps le savent très bien, si les systèmes de sécurité sont trop compliqués, les gens ne s'en serviront pas. Ainsi, lorsque les expériences utilisateur entravent la productivité des collaborateurs au lieu de l'accroître, elles sont susceptibles d'exposer l'organisation à davantage de risques de sécurité et à des coûts plus élevés. Les mots de passe faibles ou perdus, l'accès non sécurisé via des appareils personnels ou le libre partage de données sensibles ne constituent que quelques-uns des défis à relever.

> [Par le passé], nous n'y allions pas de main morte lorsque quelqu'un soupçonnait la présence d'un problème. Nous fermions tout, nous bloquions tous les accès, ce qui a eu un impact négatif sur notre activité. Tout le monde s'en rendait compte, car brusquement, tout était à l'arrêt temporairement. Grâce à Microsoft Sentinel, nous avons un scalpel qui nous permet d'agir avec une extrême précision sur les seuls lieux où se trouvent les problèmes. **En général, quand nous réagissons à une menace cela passe totalement inaperçu.** C'est d'ailleurs un bel indicateur de réussite. »
>
> **Rick Gehringer**
> Responsable informatique, Wedgewood

Augmentation de près de

68 000

heures par an

Grâce à Microsoft SIEM et XDR, la productivité du personnel a augmenté de près de 68 000 heures par an.

Une approche intégrée de SIEM et XDR permet d'offrir des expériences fluides qui garantissent la productivité et la sécurité du personnel, dans toutes les tâches quotidiennes. Elle permet de réduire les impacts négatifs sur votre productivité, comme le fait de devoir désactiver des services ou d'isoler, puis de réimager les machines. Mais l'intégration de SIEM et XDR peut également créer des gains de productivité pour les utilisateurs finaux. Elle fournit par exemple un support de sécurité plus en libre-service, de meilleurs tableaux de bord et rapports, ainsi qu'une plus grande réactivité et des temps de démarrage plus rapides, car moins d'agents de sécurité sont nécessaires.

Dans l'étude Forrester Total Economic Impact™ (TEI) commandée par Microsoft, l'entreprise témoin comptant 8 000 collaborateurs au total a montré une augmentation de la productivité de ses collaborateurs en déployant Microsoft SIEM et XDR :

- **Amélioration de la productivité du personnel de près de 68 000 heures par an.** Microsoft SIEM et XDR préviennent les impacts négatifs sur les collaborateurs causés par des processus de sécurité inefficaces. Par exemple, l'entreprise témoin économise 4 000 heures par an, grâce aux mises à jour et aux recommandations de sécurité en total libre-service pour les professionnels de l'informatique. Il est également possible d'effectuer un dépannage à distance sur les machines des collaborateurs et ainsi de réduire le nombre d'agents de sécurité nécessaires pour l'exécution de ces machines, ce qui permet d'économiser près de 64 000 heures de travail par an.

La sécurité est devenue un élément essentiel de la réussite technologique. C’est pourquoi les entreprises ont besoin de mesures de sécurité qui renforcent la résilience contre les attaques modernes, afin de protéger et de favoriser la productivité et l’innovation, qui stimulent la croissance.

Obtenir une protection intégrée contre les cybermenaces avec SIEM et XDR

Cette intégration de produits de pointe permet de prévenir, de détecter et de contrer les cybermenaces grâce à une solution unique complète.

Microsoft propose la première et la seule solution intégrée SIEM et XDR, offrant une visibilité de bout en bout sur tous les clouds et toutes les plateformes. Cette intégration de produits de pointe permet de prévenir, de détecter et de contrer les cybermenaces grâce à une solution unique complète.

Microsoft SIEM et XDR exploitent la puissance de l'IA et de l'automatisation. Ils reposent sur des investissements importants et continus dans la détection et l'analyse des cybermenaces, ainsi que sur les connaissances d'experts et une visibilité sur 43 trillions de signaux chaque jour. Grâce à l'intégration de ces produits, les équipes SOC disposent de plus de contexte pour traquer et résoudre plus rapidement les cybermenaces critiques :

Microsoft Sentinel

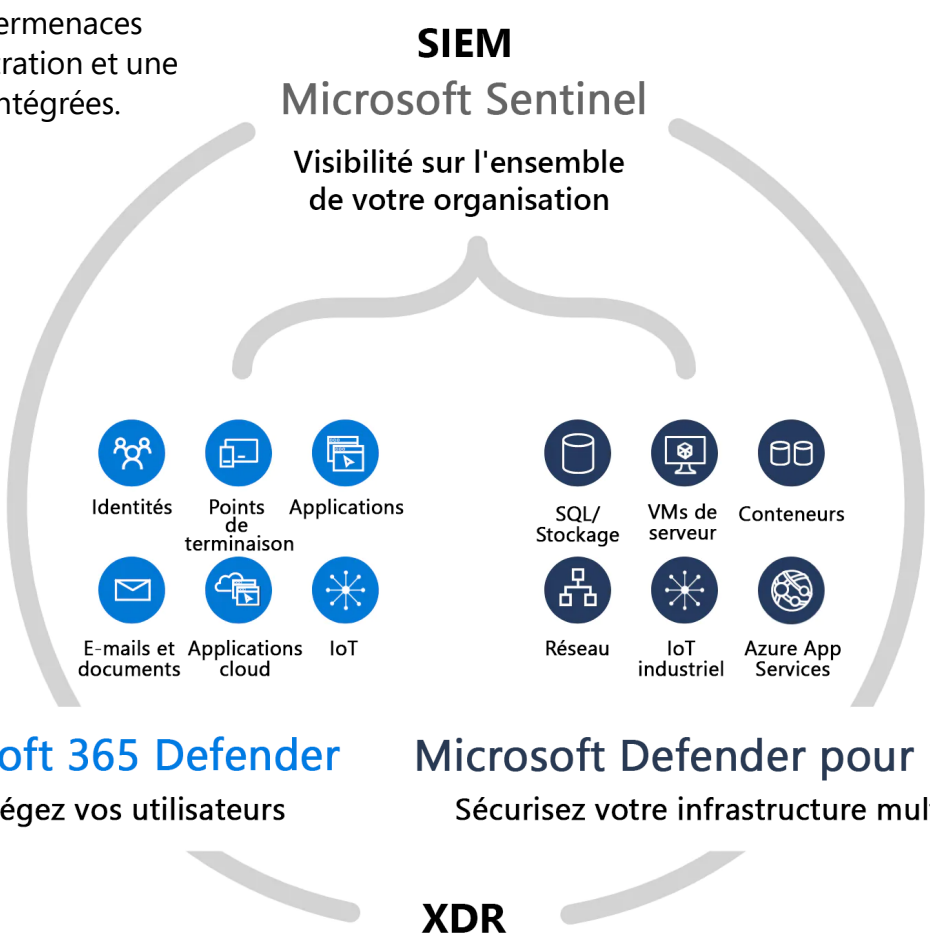
Bénéficiez d'une vue d'ensemble de votre entreprise avec la plateforme SIEM native du Cloud de Microsoft. Agrégez des données de sécurité provenant de pratiquement n'importe quelle source et appliquez l'IA pour distinguer les fausses alertes des événements légitimes, corréler les alertes à travers des chaînes de cyberattaque complexes et accélérer la réponse aux cybermenaces avec une orchestration et une automatisation intégrées.

Microsoft Defender XDR

Prévenez et détectez les cyberattaques sur vos identités, points de terminaison, applications, e-mails, données et applications cloud grâce aux fonctionnalités XDR. Enquêtez et répondez aux cyberattaques avec une protection prête à l'emploi, la meilleure de sa catégorie. Recherchez les menaces et coordonnez facilement votre réponse à partir d'un seul tableau de bord.

Microsoft Defender pour le cloud

Protégez vos charges de travail multicloud et de Cloud hybride avec des capacités XDR intégrées. Sécurisez vos serveurs, votre stockage, vos bases de données, vos conteneurs, etc. Concentrez-vous sur ce qui compte le plus grâce aux alertes hiérarchisées.



La sécurité n'est pas un bonus. Elle doit faire partie intégrante de vos systèmes.

Mettez les bons outils et les bonnes informations entre les mains des bonnes personnes. Défendez-vous contre les attaques modernes avec une solution intégrée de bout en bout, native du cloud.

En savoir plus sur la protection intégrée contre les cybermenaces avec les solutions SIEM et XDR de Microsoft >

Microsoft Security