Microsoft Security

Trois raisons de passer à la protection intégrée contre les menaces

Table des matières

Présentation

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

La sécurité arrive à un tournant majeur. Les cyberattaques deviennent de plus en plus sophistiquées et les entreprises sont toujours empêtrées dans des pénuries de talents et des difficultés d'équilibrage des coûts pour gérer les 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 disparates 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 la portée des défis actuels en matière de sécurité semble parfois écrasante, 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 intégrée de bout en bout de la protection contre les cybermenaces qui aidera les entreprises à faire ce qui suit :

Raison 1 : En faire plus avec moins

Regroupez 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, même débutants, plus performants que jamais.

Raison 3 : Augmenter la productivité des employés

Protégez votre entreprise d'une manière qui permette à vos employés 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 nuage 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 n° 1

En faire plus avec moins

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, il est alors souvent plus difficile pour les professionnels de la sécurité d'identifier les menaces et d'y répondre rapidement. 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 en aire plus avec moins, une approche intégrée, comme les solutions SIEM et XDR de Microsoft, peut s'avérer utile. Une telle approche permet de réduire la complexité en regroupant les outils individuels. De plus, étant donné qu'elle est native du nuage, 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 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.** »
>
> **Jonathan Cassar**
> Directeur général de la technologie, MITA

1,6 million de dollars

économisés chaque année grâce au regroupement des fournisseurs

Microsoft a chargé Forrester Consulting de réaliser une étude Total Economic Impact™ (TEI) et d'examiner le rendement du capital investi (RCI) potentiel que les entreprises peuvent réaliser en déployant Microsoft SIEM et XDR. Voici quelques-unes des principales conclusions pour une entreprise composite hypothétique comptant 8 000 employés au total et 10 professionnels de la sécurité :

- **Économiser près de 1,6 million de dollars par an grâce au regroupement des fournisseurs.** L'investissement dans Microsoft SIEM et XDR permet à l'entreprise composite de réduire le coût de son ancien SIEM (560 000 $), de l'infrastructure sur place associée (plus de 360 000 $), de trois solutions ponctuelles XDR (192 000 $), ainsi que du coût permanent de la main-d'œuvre pour les gérer (480 000 $).

- **Réduire le risque d'une violation matérielle de 60 %.** Grâce à des flux de travail d'enquête et de réponse de sécurité plus efficaces, à une meilleure automatisation des réponses de sécurité et à une meilleure protection de tous les environnements informatiques, y compris la protection multinuage, l'entreprise composite réduit le risque de violations, pour un impact annuel de 1,6 million de dollars économisés.

- **Générer un RCI de 207 %.** Des entretiens représentatifs et des analyses financières ont révélé qu'une entreprise composite économise 17,68 millions de dollars sur trois ans pour un investissement de 5,76 millions de dollars, constituant ainsi une valeur nette actuelle (VAN) de 11,92 millions de dollars.

Raison n° 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.

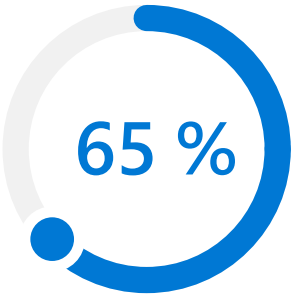
Songez, par exemple, qu'un signal unique de faible niveau peut ne pas attirer beaucoup l'attention d'un SIEM classique. Mais à l'aide de l'intelligence artificielle, un SIEM natif du nuage peut comparer automatiquement ce signal à des signaux provenant d'autres sources au sein de l'organisation, corrélant 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.

Ensuite, le système normalise, analyse et met en corrélation les données, tout en fournissant un contexte sur la façon dont la cyberattaque a pénétré dans l'infrastructure, ainsi que la chronologie de sa propagation. Cela permet aux équipes des SOC de visualiser la violation à partir d'une seule console et de la traiter efficacement.

> Beaucoup de RSSI 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**
> Chef de la sécurité de l'information et de la protection de la vie privée, Thycotic

Une entreprise ne devrait pas avoir besoin d'une expertise approfondie pour tirer parti de 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'enquête sur les menaces.

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

- **Réduction du temps d'enquête sur les menaces de 65 % et du temps de réponse aux menaces de 88 %.** L'approche intégrée de Microsoft SIEM et XDR en matière d'enquête sur les menaces de sécurité et de réponse à celles-ci rend ces flux de travail plus efficaces pour les professionnels de la sécurité de l'entreprise composite. Ils n'ont plus besoin de passer par de multiples outils pour détecter les menaces, et les fonctions d'automatisation de la sécurité améliorent encore les flux de travail 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 flux de travail des autres professionnels de la sécurité. Comme les journaux SIEM sont intégrés dans l'ensemble de la suite de solutions, la création de classeurs est presque automatisée. De plus, le système de connexion unique permet aux nouveaux professionnels de la sécurité d'être intégrés près de 16 semaines plus rapidement.

Raison n° 3

Augmenter la productivité des employés

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

En plus de permettre d'en faire plus avec moins et d'augmenter l'efficacité SecOps, une solution intégrée SIEM et XDR peut aider votre entreprise à améliorer la productivité des utilisateurs finaux.

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 employés 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 au travers d'appareils personnels ou le libre partage de données confidentielles 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, nos envoyés ne s'en rendent même pas compte quand nous réagissons à une menace**, c'est d'ailleurs un bel indicateur de réussite. »
>
> **Rick Gehringer**
> Responsable informatique, Wedgewood

Presque
68 000

Microsoft SIEM et XDR ont amélioré la productivité d'autres employés de près de 68 000 heures par an au total.

Une approche intégrée de SIEM et XDR vous aide à offrir des expériences utilisateur fluides qui garantissent la productivité et la sécurité de vos employés, à tous les niveaux de leur expérience quotidienne. 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 composite hypothétique comptant 8 000 employés au total a montré une augmentation de la productivité de ses employés en déployant Microsoft SIEM et XDR :

- **Amélioration de la productivité d'autres employés de près de 68 000 heures par an au total.** Microsoft SIEM et XDR préviennent les impacts négatifs sur les autres employés causés par des processus de sécurité inefficaces. Par exemple, l'entreprise composite 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. Elle permet également un dépannage à distance basé sur la sécurité sur les machines des employés et réduit le nombre d'agents de sécurité en cours d'exécution sur ces machines, ce qui permet d'économiser près de 64 000 heures par an en matière de productivité des utilisateurs finaux.

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

Obtenez 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 nuages 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 profonds et continus dans la détection et l'analyse des cybermenaces, ainsi que sur les connaissances d'experts et une visibilité sur 43 billions de signaux chaque jour. Grâce à l'intégration de ces produits, les équipes SOC disposent de plus de contexte que jamais auparavant pour traquer et résoudre plus rapidement les cybermenaces critiques :

Microsoft Sentinel

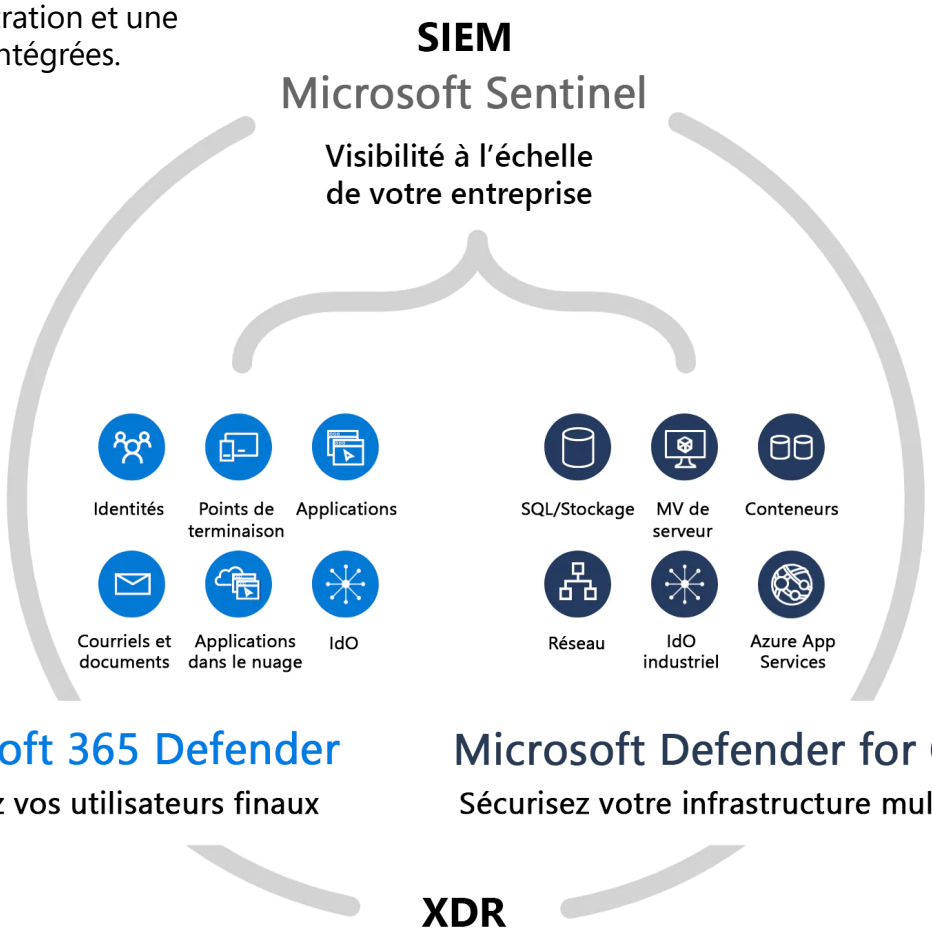
Bénéficiez d'une vue d'ensemble de votre entreprise avec la plateforme SIEM native du nuage de Microsoft. Agrégez des données de sécurité provenant de pratiquement n'importe quelle source et appliquez l'IA pour distinguer les fausses alertes des événements légitimes, corréler les alertes à travers des 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, courriels, données et applications infonuagiques grâce aux fonctionnalités XDR. Enquêtez sur les attaques et répondez aux cybermenaces 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 for Cloud

Protégez vos charges de travail multinuage et de nuage 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.



N’ajoutez pas la sécurité comme une option. Intégrez-la à 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 nuage.

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

Microsoft Security