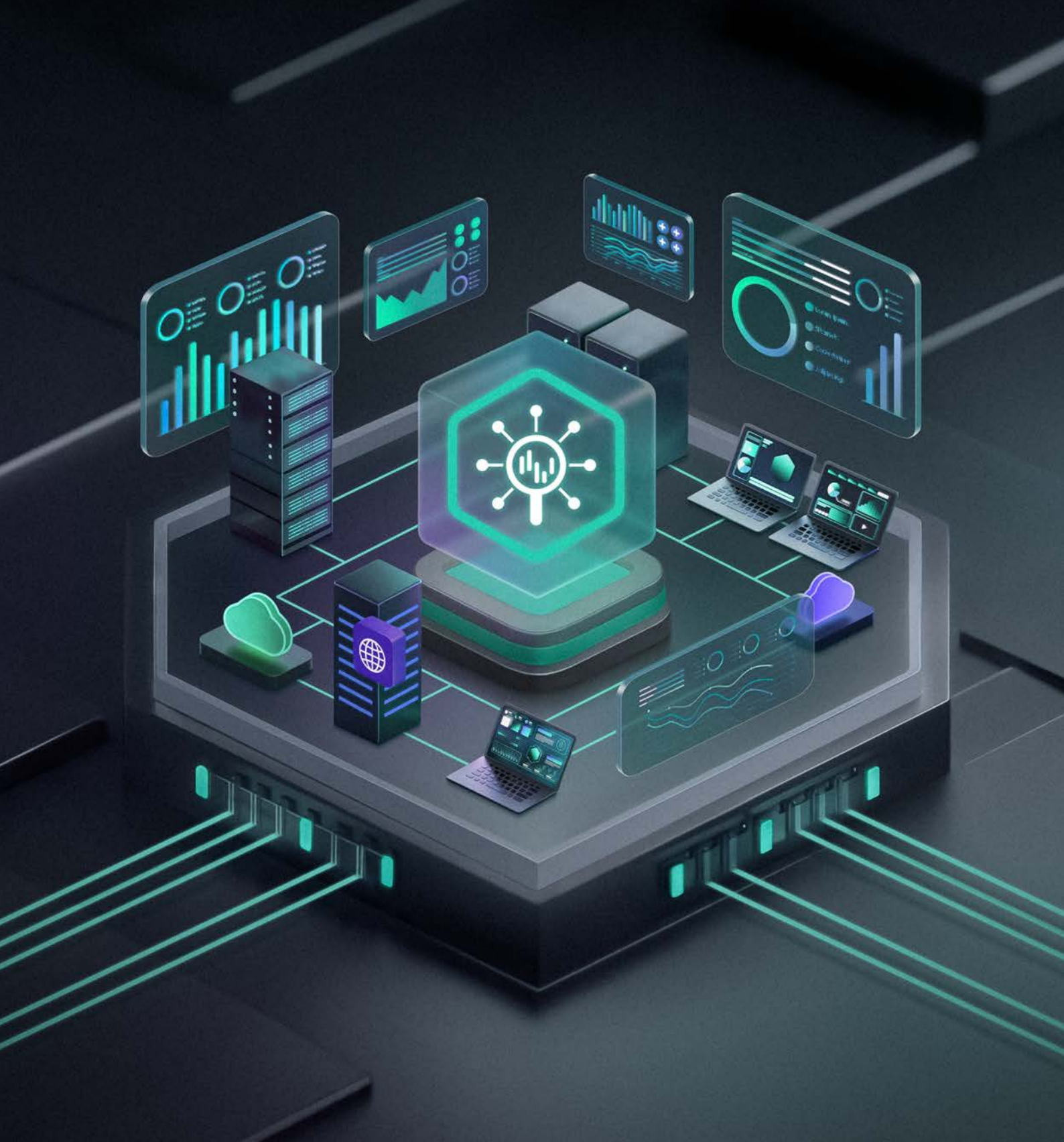


Documentation

Kaspersky SIEM

Transformez vos opérations de sécurité avec notre solution de nouvelle génération, assistée par l'IA et enrichie d'une Threat Intelligence de pointe

kaspersky bring on the future

Kaspersky SIEM est destiné aux organisations disposant d'infrastructures informatiques complexes, traitant de grands volumes de données et soumises à des exigences réglementaires strictes. Le produit est prêt pour pour les MSSP et intègre nativement la prise en charge intégrée du multitenant.

Ces organisations reconnaissent qu'une sécurité efficace dépend non seulement de la prévention, mais aussi de la capacité à détecter, analyser et répondre aux menaces en temps réel sur différents systèmes.

Maximisez l'impact de vos opérations de sécurité.

Les grandes entreprises sont confrontées à un nombre croissant de menaces persistantes avancées (APT). En 2024, des APT ont été détectées dans une entreprise sur quatre et ont représenté 43 % de tous les incidents de haute gravité[1]. Les conditions sont coûteuses, allant de l'interruption des activités aux pertes financières et à l'atteinte à la réputation à long terme.

Les équipes de sécurité sont soumises à une pression record. Les systèmes de protection génèrent d'énormes volumes de données, ce qui augmente les coûts de stockage et rend les déploiements SIEM coûteux. Les spécialistes se font rares, tandis que les équipes existantes sont débordées : 70 % des centres d'opérations de sécurité (SOC) peinent à suivre le rythme effréné des alertes[2]. En outre, la complexité de l'administration des systèmes SIEM met à rude épreuve des ressources déjà limitées.

Même les centres d'opérations de sécurité les plus avancés risquent de perdre en efficacité sans les outils modernes basés sur l'IA leur permettant de faire abstraction du bruit et de se concentrer sur l'essentiel.

Équipez votre équipe d'un SIEM optimisé par l'IA et renforcé par une Threat Intelligence de premier plan

Kaspersky SIEM est une solution de nouvelle génération conçue pour aider votre équipe de sécurité à gérer et à analyser les données de sécurité entrantes. Voici ses points forts :

- Collecte, traitement et stockage d'événements provenant de diverses sources, y compris les produits Kaspersky, les systèmes d'exploitation, les applications tierces, les outils de sécurité et les bases de données.
- Analyse et corrélation des données entrantes en temps réel, enrichies par une Threat Intelligence de pointe afin de détecter toute activité suspecte.
- Alertes régulières pour une enquête et une réponse rapides en cas d'incident.
- Stockage des données pendant une période prolongée sans dépasser le budget alloué au matériel de stockage coûteux, grâce à des options de stockage à chaud et à froid avec fonctionnalité de recherche simultanée transparente.

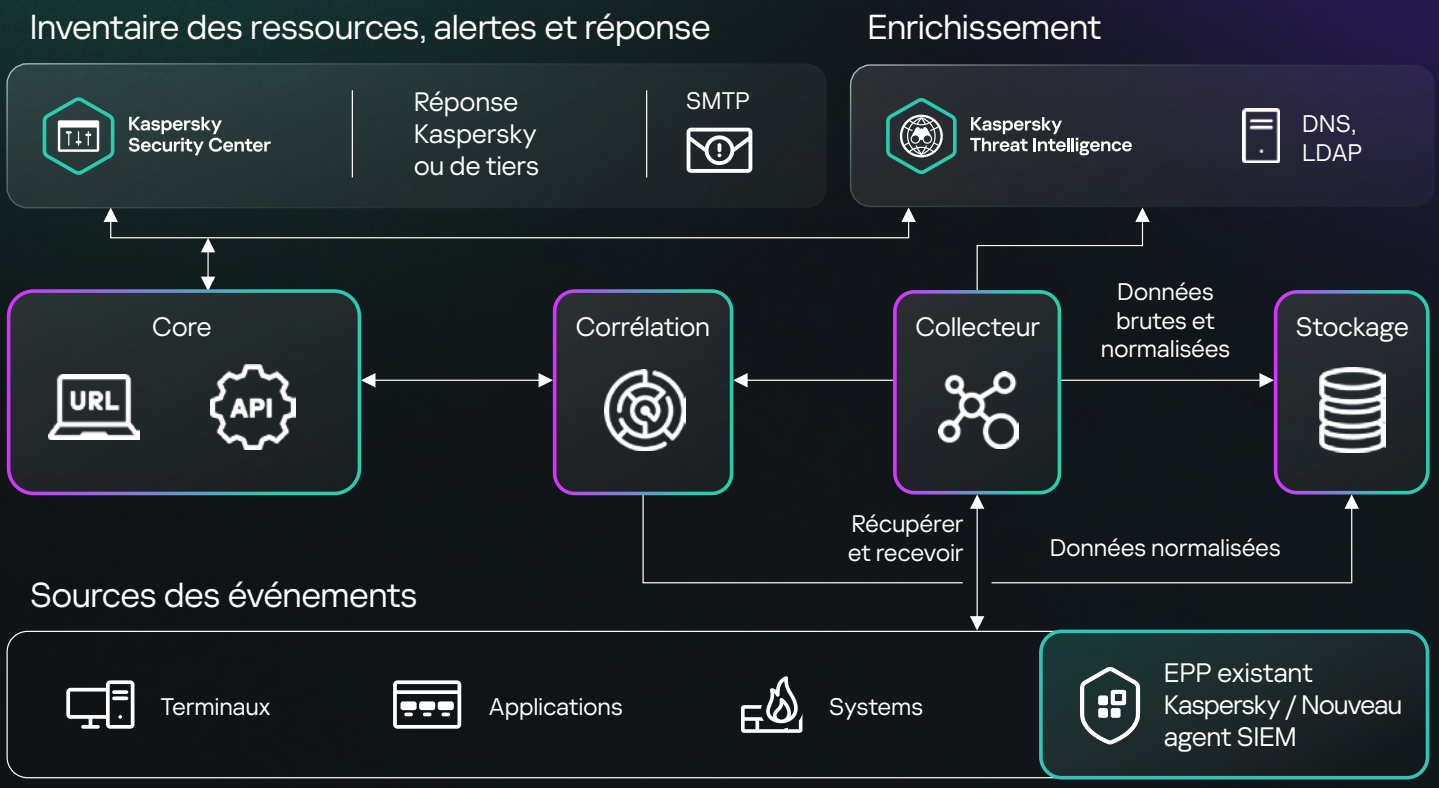
En unifiant les journaux provenant de sources de sécurité et en les corrélant en temps réel, Kaspersky SIEM offre à vos analystes la visibilité et le contexte nécessaires pour réagir efficacement.

La solution offre des fonctionnalités avancées de recherche et d'analyse qui permettent à vos chercheurs de menaces de découvrir des menaces jusque-là inconnues. L'analyse des données historiques et l'établissement de bases de référence statistiques à l'aide de l'ensemble de règles de détection UEBA aident votre équipe à identifier les anomalies et à bloquer les attaques complexes.

Grâce à Kaspersky SIEM, votre SOC bénéficie de la visibilité, des informations et de l'efficacité dont elle a besoin pour transformer des données volumineuses en informations de sécurité exploitables. La solution peut fonctionner sans connexion Internet, garantissant ainsi une souveraineté totale sur les données.

1 Rapport des analystes de Kaspersky Managed Detection and Response pour 2024
2 Rapport Kaspersky : Le portrait du professionnel moderne de la sécurité informatique, 2024

Comment ça fonctionne ?



Grâce à l'architecture en microservices de la solution, vos administrateurs peuvent créer et configurer les microservices dont ils ont besoin afin d'utiliser Kaspersky SIEM comme un outil SIEM à part entière ou un comme un système de gestion des journaux.

Kaspersky SIEM repose sur une plateforme Open Single Management Platform[3], qui intègre à la fois les produits Kaspersky et ceux de tiers dans un système de sécurité centralisé. Cette solution est une composante essentielle d'une stratégie de défense globale, qui vise à protéger les environnements d'entreprise et industriels, et à détecter les cyberattaques qui se propagent des systèmes informatiques vers les systèmes OT.

Ce qui différencie Kaspersky SIEM

Optimise les performances, minimise les coûts

Réduisez les coûts liés au matériel et à la virtualisation jusqu'à 50 % et diminuez le coût total de possession grâce à un SIEM modulaire de haute performance qui dépasse les solutions existantes et traite des centaines de milliers d'EPS par instance.

Un seul écosystème Kaspersky intégré

Profitez de plus de 200 intégrations préconfigurées pour Kaspersky et des solutions tierces, avec des options de réponse intégrées. Notre écosystème homogène offre une interface dédiée à la Threat Intelligence, utilise des capteurs de terminaux comme agents SIEM et offre des possibilités d'intégration inégalées par les autres fournisseurs.

Expertise SOC intégrée

Profitez de plus de 700 règles de détection préconfigurées, mises à jour chaque trimestre avec le mappage MITRE et des conseils d'intervention, toutes développées par Kaspersky SOC, l'une des équipes de recherche de menaces les plus expérimentées du secteur.

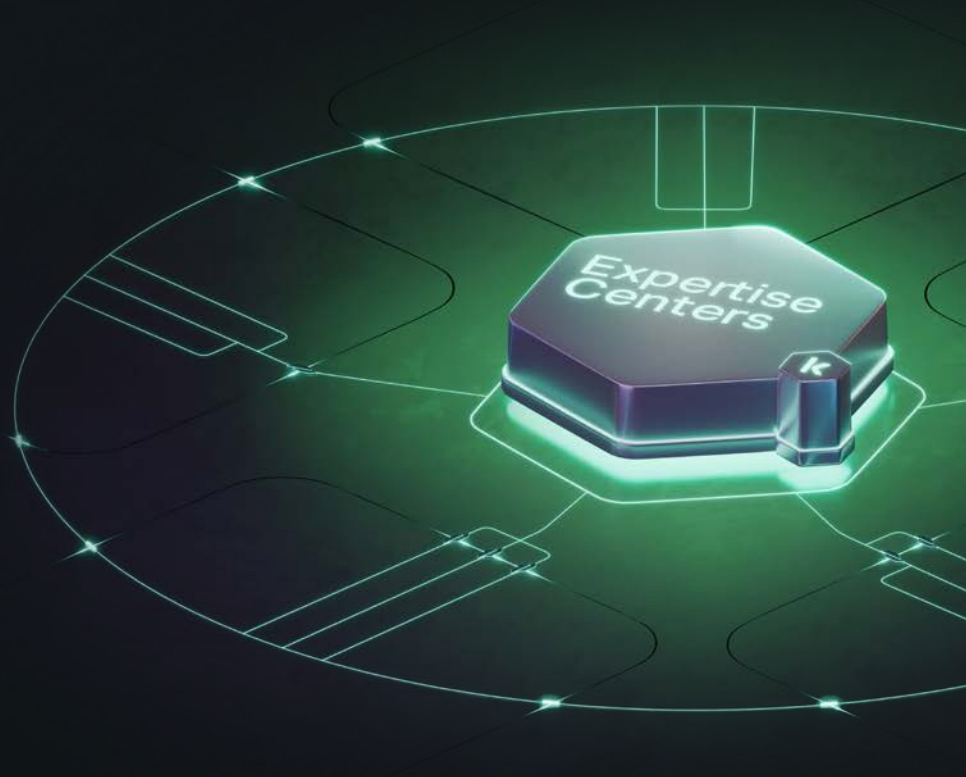
Détection des menaces assistée par l'IA

Les modules optimisés par l'IA permettent d'identifier rapidement les activités suspectes au sein de votre infrastructure, grâce à la détection par l'IA des détournements de DLL, à l'évaluation des risques des ressources basée sur l'IA, et bien plus. Ces fonctionnalités améliorent la précision des détections, réduisent le nombre de faux positifs et minimisent l'impact des cyberincidents, contribuant ainsi à améliorer le temps moyen de détection et de réponse.

3 Kaspersky Next XDR Expert, optimisé par cette plateforme, élargit ses fonctions grâce à la recherche avancée de menaces, à des guides automatisés et à une gestion simplifiée des cas.

Kaspersky SIEM repose sur les connaissances accumulées au fil des années et les compétences affinées des centres d'expertise Kaspersky, cinq pôles spécialisés et unifiés dédiés à l'amélioration de la cybersécurité.

En savoir plus



Kaspersky SIEM est fourni avec une assistance et des services Premium 24 h/24, 7 j/7, y compris des intégrations personnalisées fournies par Kaspersky Professional Services ou des partenaires de confiance, tirant parti des fonctions API des produits connectés.

Nous fournissons une mise en œuvre clé en main, une assistance à la migration transparente et une expertise continue pour vous garantir de tirer le meilleur parti de votre déploiement SIEM.

Kaspersky SIEM

www.kaspersky.fr

En savoir plus

#kaspersky
#bringonthefuture