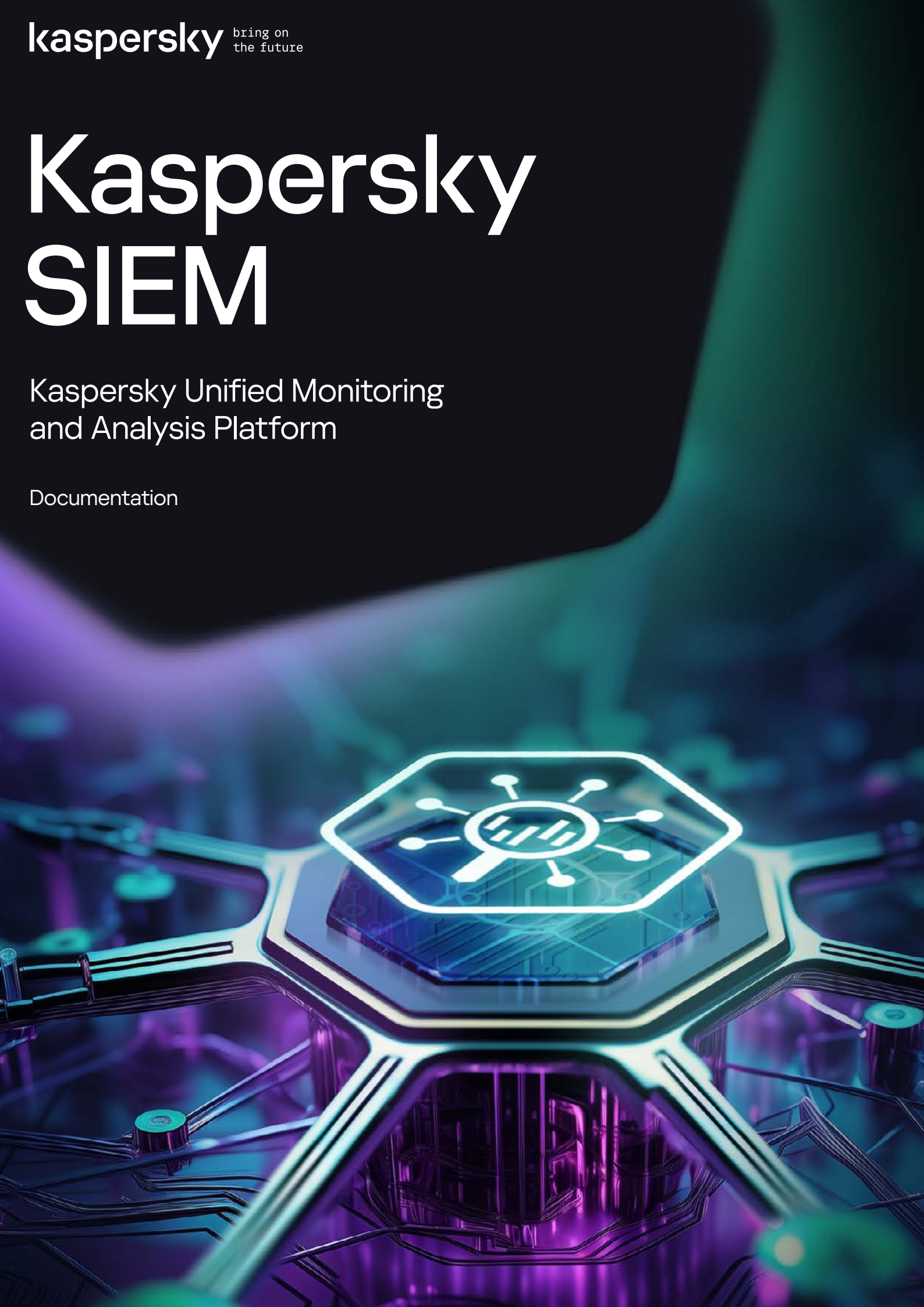
kaspersky bring on the future

Kaspersky SIEM

Kaspersky Unified Monitoring and Analysis Platform

Documentation



À propos de Kaspersky SIEM et de son architecture

Kaspersky Unified Monitoring and Analysis Platform est une solution SIEM intégrée de nouvelle génération destinée à la gestion des données et des événements de sécurité. Elle excelle dans la réception, le traitement et le stockage des événements liés aux informations de sécurité, ainsi que dans l'analyse et la corrélation des données entrantes. La plateforme dispose également d'une fonction de recherche, génère des alertes lorsque des menaces sont détectées, et prend en charge les réponses automatisées aux alertes générées et la recherche des menaces.

L'architecture modulaire haute performance permet de traiter des centaines de milliers d'événements par seconde (EPS) sur chaque instance et de réduire le coût total de possession (TCO) en optimisant les exigences du système.

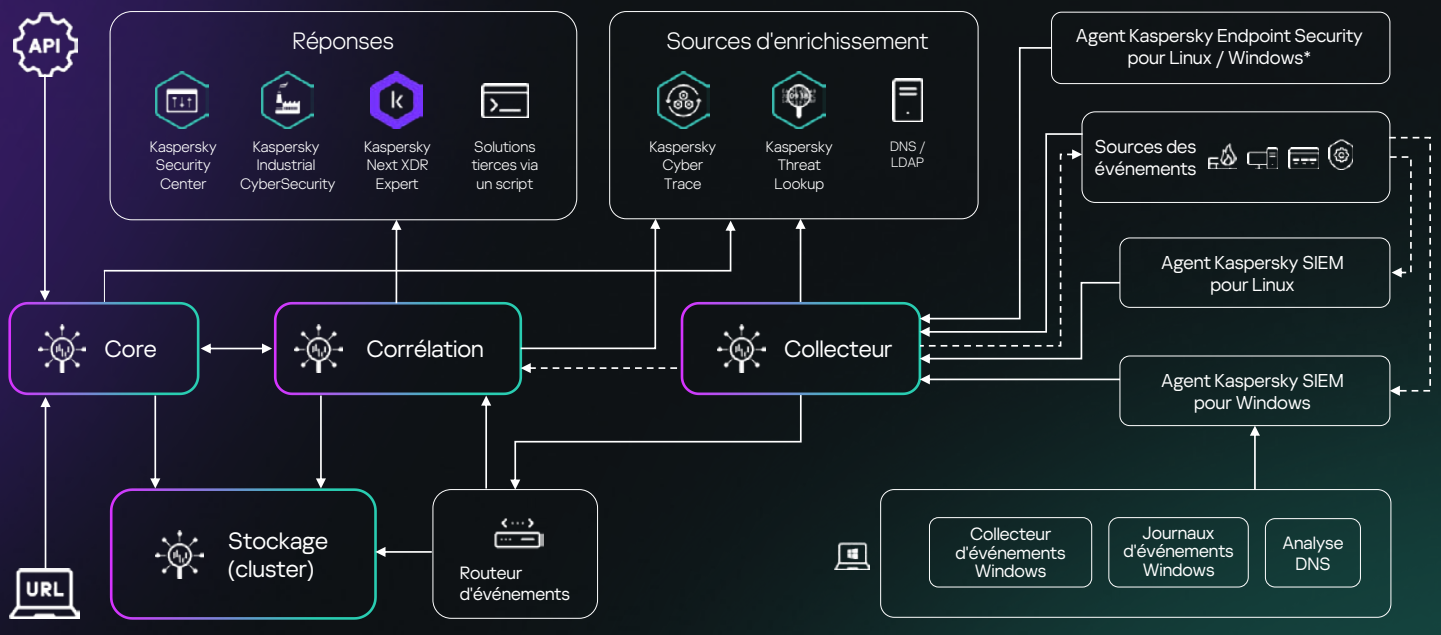
En intégrant des produits tiers et des solutions Kaspersky dans un système centralisé de sécurité de l'information, Kaspersky SIEM se révèle être l'élément essentiel d'une stratégie de défense globale capable de sécuriser les environnements d'entreprise et industriels, ainsi que de détecter les cyberattaques qui commencent dans les systèmes informatiques et se propagent aux systèmes opérationnels OT.

Grâce à l'architecture en micro-services de la solution, les administrateurs peuvent créer et configurer les micro-services dont ils ont besoin pour utiliser Kaspersky SIEM comme un système SIEM à part entière ou un système de gestion des journaux.

La solution reçoit des événements de sécurité provenant de diverses sources, notamment des produits Kaspersky, des systèmes d'exploitation, d'applications tierces, d'outils de sécurité et diverses bases de données. Elle met les événements en corrélation les uns avec les autres et les enrichit de données provenant de sources de Threat Intelligence afin d'identifier les activités suspectes dans les infrastructures des réseaux d'entreprise et de fournir une notification en temps opportun des incidents de sécurité.

En collectant les journaux de tous les contrôles de sécurité et en corrélant les données en temps réel, **Kaspersky SIEM agrège et fournit toutes les informations nécessaires à l'enquête et à la réponse aux incidents.**

En outre, Kaspersky SIEM permet aux chercheurs de menaces de découvrir des menaces jusqu'alors inconnues en permettant aux opérateurs d'analyser et de corréler les données historiques, mais aussi d'établir des lignes de base statistiques pour identifier les anomalies.



Pourquoi nous choisir ?

Économisez jusqu'à 50 % sur les besoins en matériel ou en installation de virtualisation et réduisez le coût total de possession (TCO) grâce à une solution modulaire haute performance qui surpasse constamment les fournisseurs SIEM traditionnels en matière de rentabilité et peut gérer des centaines de milliers d'EPS sur chaque instance.

Restez flexible grâce à nos options de licensing. Nous suivons le flux moyen d'EPS par jour après agrégation et filtrage pour limiter les dépassements et ne pas restreindre l'accès à Kaspersky SIEM au cas où ils se produiraient.

Bénéficiez d'un large éventail d'intégrations Kaspersky et tierces avec des options de réponse intégrées. Les autres fournisseurs ne peuvent pas égaler notre niveau d'intégration transparente avec nos propres produits, qui inclut une interface unique dédiée à l'intégration de la Threat Intelligence, la possibilité d'utiliser nos fournisseurs de terminaux en tant qu'agents SIEM, et bien d'autres choses encore.

Stockez les données localement de manière économique et fiable, sans dépasser votre budget pendant une période prolongée grâce à des options de stockage à chaud et à froid utilisant ClickHouse et le système de fichiers distribués Hadoop (HDFS) ou des disques locaux, tout en ayant la possibilité d'effectuer des recherches rapides dans les deux zones simultanément.

Améliorez la pertinence des données, accélérez la détection et le triage grâce à l'enrichissement d'une Threat Intelligence tactique, opérationnelle et stratégique fournie par notre équipe de chercheurs et d'analystes de renommée mondiale via le Portail Threat Intelligence de Kaspersky.

Profitez de la multi-location intégrée avec un MSSP et une solution adaptée aux grandes entreprises qui offre une prise en charge native de plusieurs entités où une installation SIEM unique dans l'infrastructure principale des entreprises permet de créer des SIEM isolés pour les clients qui reçoivent et traitent leurs propres événements.

Pourquoi Kaspersky ?

Kaspersky SIEM bénéficie des années de connaissances accumulées et des compétences affinées des 5 centres d'expertise.

En savoir plus

27

Depuis **plus de 27 ans**, nous développons des outils et fournissons des services visant à assurer votre sécurité grâce à nos technologies les plus testées et les plus primées.

En savoir plus

Nous sommes une **entreprise privée mondiale de cybersécurité** qui compte des milliers de clients et de partenaires dans le monde entier, engagée envers la transparence et l'indépendance.

En savoir plus

Kaspersky Unified Monitoring and Analysis Platform

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture