Fonctionnalités

# Kaspersky SIEM

kaspersky bring on the future

# Sommaire

# Marché de la sécurité informatique et de la gestion des événements

Les responsables de la cybersécurité dans les organisations sont confrontés à de nombreux défis, notamment un nombre croissant de tentatives d'intrusion dans leur infrastructure, une pénurie de personnel dans le domaine de la cybersécurité et des attaques de plus en plus complexes.

En outre, les organisations doivent se conformer aux exigences réglementaires liées à la conservation des données, aux audits et aux enquêtes sur les incidents, ce qui a une incidence sur le marché mondial de la gestion des données d'entreprise (SIEM).

Les organisations sont également contraintes de classer les alertes de cyberattaques par priorité et de les trier plus efficacement en raison de leur croissance et de leur complexité croissante.

En outre, les conditions de travail à distance ont conduit les entreprises à adopter des applications SaaS et à permettre aux employés d'apporter leurs propres appareils (PAP), ce qui souligne la nécessité d'étendre la visibilité du réseau au-delà du périmètre traditionnel.

Enfin, trouver des experts en sécurité informatique est un défi sur le marché actuel. Les entreprises cherchent à optimiser leurs ressources et à améliorer l'efficacité de leur cybersécurité. Par conséquent, les organisations veulent que leurs équipes SOC disposent de données de renseignement facilement accessibles et exploitables.

## Selon le rapport Kaspersky Human Factor360

**77 %** des entreprises ont subi au moins une violation de cybersécurité, et nombre d'entre elles en ont subi jusqu'à six au cours de cette période

**41 %** des entreprises admettent présenter des faiblesses dans leurs infrastructures de cybersécurité et prévoient d'augmenter leurs investissements dans ce domaine à l'avenir

En savoir plus

# 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.

# Kaspersky Unified Monitoring and Analysis Platform comprend les modules suivants

Un **noyau** doté d'une interface utilisateur graphique centralisée afin de contrôler et surveiller les paramètres des composants du système. Il est possible d'accéder à la plateforme à partir de solutions tierces en utilisant l'API.

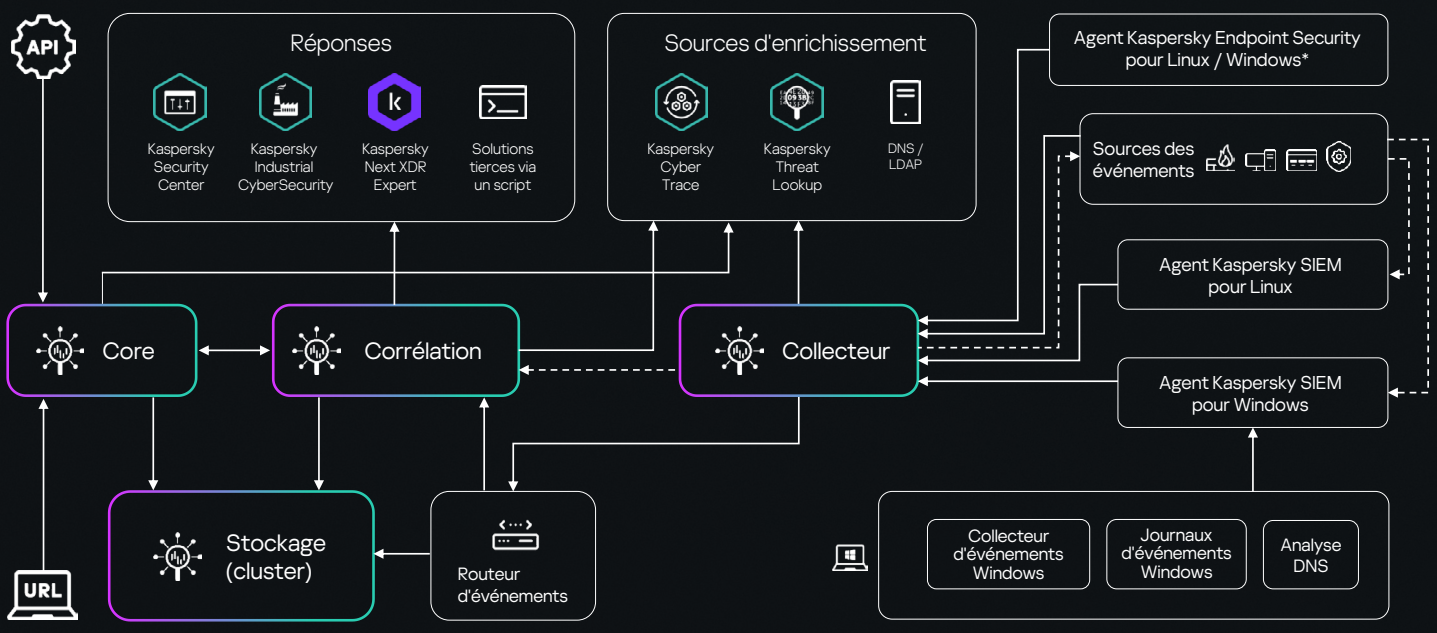
Les règles de corrélation sont utilisées pour détecter des séquences particulières d'événements traités et prendre certaines mesures après la reconnaissance, telles que la création d'événements/alertes de corrélation ou l'interaction avec une liste active. Le **corrélateur** utilise des listes actives pour effectuer les actions requises après avoir analysé les événements normalisés reçus des collecteurs, puis génère des alertes basées sur des critères de corrélation.

Un ou plusieurs **collecteurs** reçoivent des événements de sources externes et les traitent au préalable : ils les normalisent (les transforment en un format unique), les filtrent, les agrègent et les enrichissent de données provenant de sources externes à l'aide de dictionnaires, d'appels au service DNS et d'autres outils.

**On utilise le stockage** pour stocker les événements normalisés afin qu'ils puissent être rapidement et continuellement accessibles à partir du SIEM pour extraire des données analytiques.

**Les agents** transmettent les événements bruts des postes de travail et des serveurs aux collecteurs SIEM. L'envoi des événements du journal Windows directement au collecteur est désormais possible dans Kaspersky Endpoint Security for Windows 12.6 ou Linux 12.2. Cette fonction réduit considérablement la quantité de travail nécessaire pour intégrer les sources d'événements au système SIEM de Kaspersky.

**Les routeurs d'événements** réduisent la charge sur les liaisons et le nombre de ports ouverts sur les pare-feu en recevant les événements de manière régulière et sans retard lorsque les collecteurs sont installés dans des bureaux distants à faible bande passante ou sur des liaisons de données déjà occupées.



# Fonctionnalités de Kaspersky SIEM

Connecteurs intégrés et personnalisés vers des centaines de sources de Kaspersky et de fournisseurs tiers, avec des mises à jour et des améliorations régulières.

Intégration de sources d'événements externes avec création gratuite de connecteurs supplémentaires par l'équipe de Kaspersky Professional Services.

Requêtes de recherche rapides et rapports prêts à l'emploi sur les événements liés à la sécurité.

Stockage local sécurisé des journaux à des fins de conformité réglementaire et d'enquête sur les incidents.

Kaspersky SIEM prend en charge les recherches d'événements dans plusieurs systèmes de stockage afin d'aider les opérateurs à trouver plus rapidement et plus facilement les événements pertinents dans les clusters de stockage distribués.

## Surveiller, traiter et stocker les informations relatives aux événements de sécurité

Kaspersky Unified Monitoring and Analysis Platform reçoit les événements des journaux et normalise les données provenant de différentes sources d'événements pour les rendre cohérentes. Ces événements liés à la sécurité de l'information peuvent être des tentatives de connexion, des interactions avec des bases de données ou des diffusions d'informations par des capteurs. Ils sont collectés dans l'ensemble de l'infrastructure informatique protégée de l'entreprise. Alors qu'un événement isolé peut sembler anodin, plusieurs événements isolés pris dans leur ensemble donnent une image plus large d'une activité malveillante qu'il est possible d'utiliser pour identifier des problèmes de sécurité.

Le lac de données, notre stockage local centralisé, fournit une plateforme pour la collecte, l'indexation et l'analyse des journaux provenant de diverses sources, notamment les solutions de sécurité (EPP, FW, IAM, etc.), les systèmes d'exploitation, les applications d'entreprise (systèmes RH, outils bureautiques), les systèmes de sécurité physique (systèmes de contrôle d'accès automatisés), et d'autres appareils.

Les événements sont transmis au corrélateur pour être analysés, puis stockés pour être conservés après avoir été filtrés et agrégés. Pour identifier les alertes, le collecteur reçoit les événements de la part des sources, les traite et les achemine vers le stockage, le corrélateur et/ou des services tiers. Les événements bruts sont transmis des postes de travail et des serveurs aux collecteurs SIEM (dans certains cas par des agents) et peuvent être envoyés à d'autres systèmes pour une analyse supplémentaire.

Les événements de corrélation sont produits par la solution lors de la reconnaissance d'un événement particulier ou d'une série d'événements liés. Ils sont également analysés et conservés. Si un événement ou une séquence d'événements indique une menace pour la sécurité, Kaspersky SIEM génère une alerte contenant des informations sur cette menace et toute autre information pertinente que les spécialistes de la sécurité doivent prendre en compte.

Des protocoles de transport fiables, avec chiffrement optionnel, sont utilisés pour transférer les événements entre les modules. Le système peut utiliser une diode de données pour collecter des données à partir de segments isolés.

Kaspersky SIEM permet une gestion centralisée des ressources en fournissant un large inventaire des serveurs, des postes de travail et des appareils réseau. La plateforme peut collecter des données sur les vulnérabilités des ressources à partir de sources telles que les analyseurs de vulnérabilités, puis les corréler avec les données de catégorie des ressources pour identifier les menaces. Les fournisseurs de services de sécurité disposent ainsi d'une visibilité sur l'ensemble des ressources.

Pour aider les analystes, la couverture de la matrice MITRE ATT&CK par les règles est affichée pour mieux évaluer le niveau de sécurité.

Plus de 650 règles de corrélation préconfigurées visant à détecter les scénarios d'attaque sont régulièrement mises à jour par les serveurs de Kaspersky avec les recommandations de MITRE en matière de cartographie et de réponse.

Amélioration de la pertinence des données grâce à l'enrichissement des données analytiques recueillies sur le portail Kaspersky Threat Intelligence Portal (à l'aide de Kaspersky Threat Lookup et de Kaspersky CyberTrace).

Les données relatives aux ressources et à l'infrastructure sont collectées par Kaspersky Security Center et des sources tierces.

Les utilisateurs peuvent comparer un événement à des valeurs groupées, agrégées, moyennes, maximales et minimales pour une période donnée en utilisant la fonctionnalité d'exploration de données de ClickHouse. Cela permet d'étendre considérablement les capacités de la logique de détection sans nécessiter la création de nombreuses règles de service.

Pour faciliter la création et l'édition de contenu, nous permettons aux utilisateurs de déterminer à l'avance les règles de corrélation auxquelles la modification envisagée s'appliquera avant de modifier les critères de filtrage.

## Corrélation en temps réel et historique des événements de sécurité

Kaspersky SIEM effectue une corrélation croisée en temps quasi réel en utilisant des règles personnalisées pour identifier les attaques et les menaces, ainsi que des centaines de règles prédéfinies développées par le SOC Kaspersky, l'une des équipes de recherche des menaces actives les plus performantes et les plus expérimentées du secteur. Les experts de Kaspersky SOC sont titulaires de nombreux certificats confirmant leur haut niveau d'expertise et de connaissances.

Les événements sont **corrélés en temps réel**. Le corrélateur analyse les événements normalisés, crée des alertes conformément aux règles de corrélation et gère toutes les opérations de la liste active.

Le principe de fonctionnement du corrélateur repose sur l'analyse de la signature des événements, ce qui signifie que chaque événement est traité conformément aux règles de corrélation définies par l'utilisateur. Le logiciel génère un événement de corrélation et l'envoie au stockage lorsqu'il trouve une série d'événements qui répondent aux exigences de la règle de corrélation. L'utilisateur peut adapter les règles de corrélation aux résultats d'une analyse antérieure en envoyant l'événement de corrélation au corrélateur pour une analyse supplémentaire. Les résultats des règles de corrélation peuvent être utilisés par d'autres règles de corrélation. Par exemple, plusieurs alertes mineures peuvent générer une alerte plus importante (plusieurs tentatives de force brute peuvent être analysées pour découvrir un incident de force brute de grande envergure).

La plateforme utilise les données historiques pour repérer les tendances, trouver des menaces qui n'avaient pas été identifiées auparavant et repérer les attaques qui ont été négligées par certains éléments de sécurité, ce qui permet d'améliorer la détection globale des menaces.

Des solutions tierces ou des produits intégrés tels que **Kaspersky Endpoint Detection and Response** assurent la détection côté capteur. En ajustant les paramètres des produits, les utilisateurs peuvent contrôler ce processus et obtenir des données télémétriques et des événements que ces produits ont déjà traités grâce à leur propre logique de détection.

Le moteur de corrélation de la solution intègre une détection au niveau de la plateforme. Grâce au puissant moteur de corrélation de la plateforme, les utilisateurs peuvent créer des règles de corrélation adaptables. Des règles prêtes à l'emploi et des packages de normalisation sont également disponibles pour prendre en charge les produits tiers commercialement accessibles, qui sont constamment élargis et mis à jour.

Le principe de fonctionnement du corrélateur repose sur l'analyse de la signature des événements, ce qui signifie que chaque événement est traité conformément aux règles de corrélation définies par l'utilisateur. Le logiciel génère un événement de corrélation et l'envoie au stockage lorsqu'il trouve une série d'événements qui répondent aux exigences de la règle de corrélation.

La recherche de menaces permet de découvrir des menaces jusqu'alors inconnues en permettant aux opérateurs d'analyser et de corréler des données historiques à l'aide d'une puissante base de données organisée en colonnes.

Les utilisateurs peuvent facilement localiser les filtres, les règles et les dictionnaires qui sont tous unifiés par un seul tag en utilisant la fonction de recherche basée sur les tags. Le stockage de l'historique de requêtes des recherches permet à l'utilisateur d'accéder facilement à ses requêtes antérieures.

La plateforme peut stocker des données pendant une période prolongée sans dépasser le budget alloué au coûteux matériel de stockage, grâce aux options de stockage à chaud et à froid utilisant ClickHouse et le système de fichiers distribués Hadoop (HDFS) ou des disques locaux.

Les administrateurs peuvent éviter les problèmes d'espace dans le sous-système de disque à l'aide de paramètres flexibles : la profondeur de stockage des événements peut être définie en gigaoctets en tant que pourcentage de l'espace disque, en plus du paramètre des jours.

## Stockage des données relatives aux événements de sécurité

On utilise le module de stockage de Kaspersky SIEM pour stocker les événements normalisés afin d'accéder rapidement et continuellement aux données analytiques à partir de **Kaspersky Unified Monitoring and Analysis Platform**.

ClickHouse garantit la continuité et la rapidité de l'accès. Le stockage est connecté à un service de stockage Kaspersky SIEM via un cluster ClickHouse. Des disques de stockage à froid peuvent également être ajoutés aux clusters ClickHouse.

Les utilisateurs peuvent ajouter de l'espace dans les stockages pour regrouper les événements stockés en fonction d'un attribut spécifique. Cela permet aux administrateurs de définir des durées de stockage différentes pour les événements en fonction de leurs caractéristiques uniques.

Kaspersky Unified Monitoring and Analysis Platform gère également la compression des données afin de réduire considérablement l'utilisation de l'espace disque sans compromettre la récupération des données. La solution Kaspersky couvre deux domaines : l'un pour la recherche rapide de données et l'autre pour le stockage d'une grande quantité de données.

La plateforme comporte deux sections distinctes : l'une pour le stockage à froid qui peut être réalisé sur le système de fichiers distribués Hadoop ou sur des disques locaux, et l'autre pour le stockage opérationnel à l'aide de ClickHouse. Cette séparation est transparente pour les utilisateurs.

Sans avoir à passer d'une archive à l'autre, les opérateurs peuvent créer des requêtes de recherche dans une interface unique et concentrer tous leurs efforts sur l'enquête. Cette approche permet de **réduire le coût de possession du système** tout en maintenant une excellente expérience pour l'utilisateur. La plateforme prend en charge les recherches d'événements dans plusieurs systèmes de stockage afin d'aider les opérateurs à trouver plus rapidement et plus facilement les événements pertinents dans les clusters de stockage distribués.

Les organisations peuvent rester conformes aux exigences réglementaires en matière de conservation des données, d'audit et d'enquête sur les incidents en collectant et en stockant les journaux provenant de diverses sources en toute sécurité. En outre, le stockage centralisé et structuré permet aux entreprises de récupérer et d'analyser facilement les journaux en cas de besoin.



## Capacités de réponse intégrées

La fonctionnalité de réponse intégrée utilisant les produits Kaspersky augmente l'efficacité de la sécurité. Par exemple, pour étendre les capacités de réponse des points de terminaison, Kaspersky SIEM peut être couplé à Kaspersky Endpoint Detection and Response pour gérer l'isolation réseau des ressources et les règles de prévention, ou exécuter des applications et des scripts. Ces actions de réponse peuvent être exécutées manuellement ou automatiquement sur les ressources avec l'agent Kaspersky Endpoint Security.

La collecte automatisée d'informations d'inventaire (logiciels installés, vulnérabilités, équipements, propriétaires des ressources, etc.) peut aider à contextualiser les événements liés à la sécurité de l'information et assister les enquêtes sur les incidents.

Kaspersky SIEM utilise Kaspersky CyberTrace, une plateforme complète de renseignement sur les menaces, qui prend en charge des dizaines de flux de données sur les menaces prêts à l'emploi (commerciaux et publics) pour diffuser automatiquement en temps réel l'enrichissement des événements avec des informations contextuelles sur les indicateurs de compromission.

Les modules d'intelligence artificielle de Kaspersky SIEM permettent une détection rapide des activités suspectes dans l'infrastructure

## Outils d'intelligence artificielle et de machine learning

Kaspersky utilise des algorithmes prédictifs, des techniques de regroupement, des réseaux neuronaux, des techniques de modélisation statistique et des algorithmes experts pour accroître l'efficacité de ses produits en détectant les menaces plus rapidement et en classant les détections par ordre de priorité avec précision.

Les équipes de surveillance et d'intervention peuvent hiérarchiser les alertes et se concentrer sur la prévention des dommages potentiels, vérifiés par des systèmes de big data et d'IA. Le module d'IA facilite le triage en analysant les données historiques, en hiérarchisant les alertes entrantes et en fournissant des scores de risque basés sur l'IA pour les ressources. Cette approche permet de générer des hypothèses valables qui peuvent être utilisées pour des recherches proactives.

La plateforme utilise des règles de corrélation définies par l'utilisateur pour relier les événements en temps réel. Son module de corrélation applique des algorithmes d'intelligence artificielle pour détecter les activités anormales telles que les pics soudains de trafic ou les accès multiples aux services signalant un incident potentiel, ce qui permet une détection précoce avant que les dommages ne se produisent.

Kaspersky SIEM intègre également les données de Kaspersky Threat Intelligence, générées à l'aide des technologies d'IA et de big data. La base de données est continuellement enrichie par les résultats des analyses manuelles des APT, les données opérationnelles du Darknet, les informations de Kaspersky Security Network et les résultats des analyses régulières des nouveaux programmes malveillants.

Toutes ces technologies aident les utilisateurs à minimiser les dommages potentiels causés par les cyber-incidents et à augmenter le MTTR et le MTTD.

## Une visualisation exceptionnelle, au moyen de tableaux de bord et de rapports, présente les données sous les formats les plus exploitables pour identifier les tendances, les modèles et les événements anormaux.

Grâce à des widgets personnalisables facilitant la visualisation et l'affichage des indicateurs, les analystes peuvent hiérarchiser les incidents, déterminer les causes profondes et répondre aux menaces plus efficacement, tandis que les organisations peuvent suivre l'efficacité de leurs opérations de sécurité, identifier les tendances et évaluer la santé globale de leur système de sécurité.

Les utilisateurs peuvent enrichir les données des champs d'événements avec le contenu des dictionnaires, des tables, des attributs des ressources et des comptes, et utiliser ces données pour la recherche et la visualisation. Ils peuvent ainsi élaborer des tableaux de bord et des rapports avec des données plus contextuelles.

Cette solution permet aux utilisateurs de créer leurs propres widgets avec des paramètres ajustables, ainsi que des mises en page avec **divers groupes de widgets :**

### Principaux indicateurs d'alerte

(gravité, priorité et état)

- Ressources concernées
- Notifications récentes
- Principales sources de données ayant le plus grand nombre d'alertes
- Alertes attribuées à des opérateurs spécifiques
- Utilisateurs et/ou appareils concernés
- Alertes par stratégie

### Indicateurs clés d'incidents

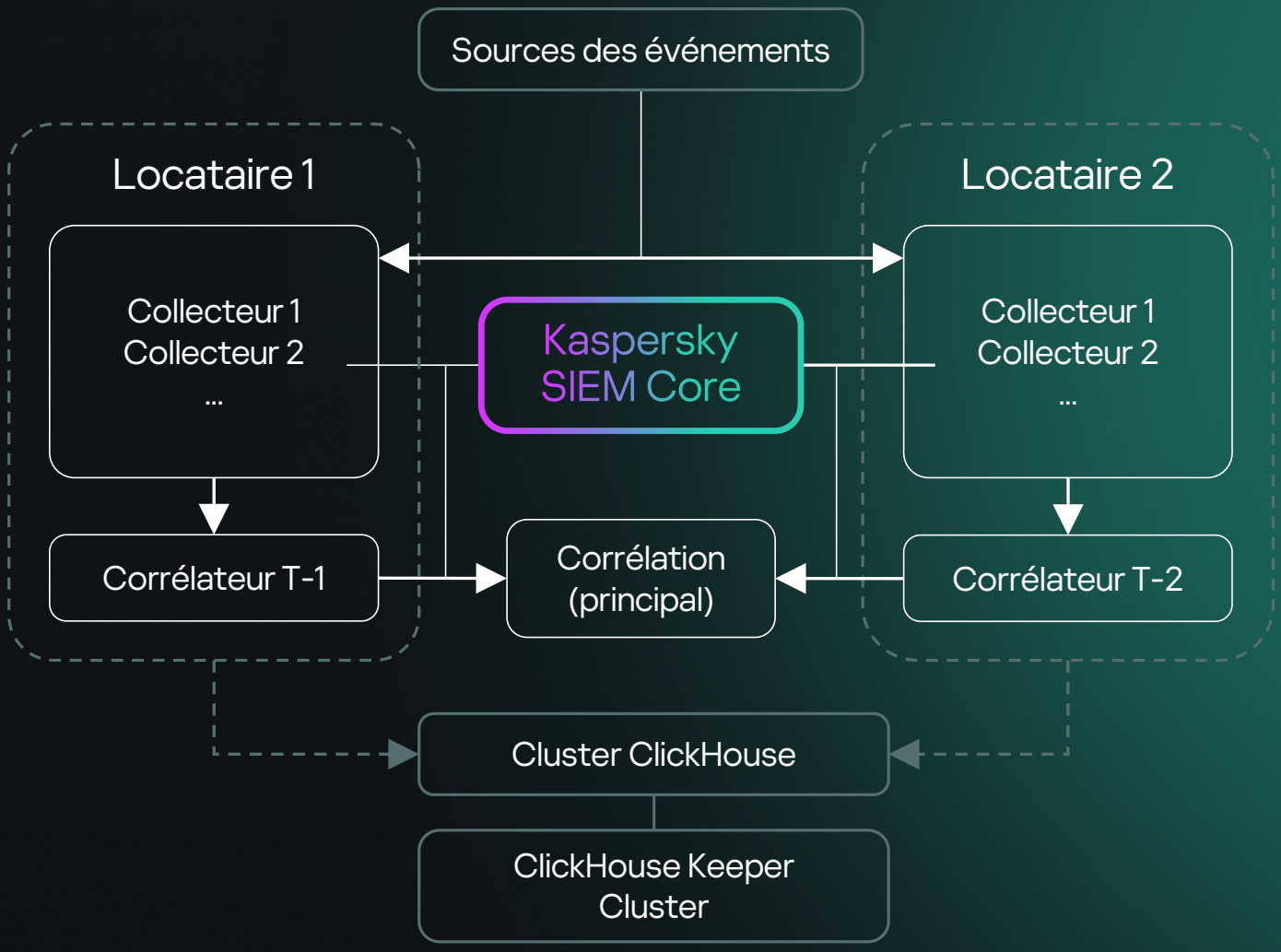
(gravité et affectation)

- Appareils concernés
- Principales adresses IP internes et externes par débit de flux net (BytesIn)
- Nœuds principaux pour la gestion à distance (ports 3389, 22)
- Total des octets NetFlow pour les ports internes
- Principales sources en fonction du nombre d'événements, de catégories, de ressources et d'utilisateurs

## Architecture multi-clients

Kaspersky SIEM offre une assistance multi-clients complète, ce qui signifie que les utilisateurs d'un client ne peuvent pas voir les données (événements, alertes, incidents, etc.) d'un autre. En mode multi-location, une seule instance de l'application Kaspersky SIEM déployée dans l'organisation principale permet d'isoler les filiales afin qu'elles puissent recevoir et traiter leurs propres événements.

Le système est administré de manière centralisée dans l'interface principale, et les locataires fonctionnent de manière indépendante en n'ayant accès qu'à leurs propres ressources, services et paramètres. Les événements liés aux différents clients sont stockés séparément. Les utilisateurs peuvent accéder à plusieurs locataires simultanément. L'administrateur général peut également définir quelles données relatives aux locataires seront affichées dans les différentes parties de l'interface Web.




La plateforme propose un système basé sur des filtres pour distribuer les événements vers des espaces. L'accès des utilisateurs aux événements est désormais défini au niveau de l'espace. Cela permet un contrôle granulaire de l'accès aux événements au sein d'un même client.

Le système est géré de manière centralisée via l'interface principale, tandis que les locataires fonctionnent indépendamment les uns des autres et n'ont accès qu'à leurs propres ressources, services et paramètres. Les événements des locataires sont stockés séparément.

## Large gamme d'intégrations prêtes à l'emploi

Kaspersky Unified Monitoring and Analysis Platform est parfaitement intégré aux solutions et technologies Kaspersky pour permettre une utilisation coordonnée et efficace des produits. Les fournisseurs tiers ne peuvent pas égaler notre niveau de fluidité en ce qui concerne l'intégration de nos propres produits ; laquelle inclut une interface unique pour l'intégration de Threat Intelligence, la capacité d'utiliser nos Endpoint Sensors comme agents SIEM, etc.

**Kaspersky Anti Targeted Attack**

**Kaspersky Endpoint Detection and Response** *

**Kaspersky Security Center**

**Kaspersky Secure Mail Gateway**

**Kaspersky Web Traffic Security**

**Kaspersky Threat Lookup**

**Kaspersky Industrial CyberSecurity for Networks**

**Kaspersky Industrial CyberSecurity for Nodes**

**Kaspersky Automated Security Awareness Platform**

et bien plus encore

L'intégration du riche portefeuille de services **Kaspersky Threat Intelligence** permet d'identifier et de hiérarchiser les menaces et d'accéder rapidement à des informations contextuelles sur les nouvelles attaques, les indicateurs de compromission, et les tactiques et techniques des pirates informatiques.

* Des intégrations sont possibles avec Kaspersky Endpoint Detection and Response Expert, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Next EDR Foundations, Kaspersky Next EDR Optimum et Kaspersky Next EDR Expert

Kaspersky SIEM excelle dans la réception de données (journaux) provenant d'autres systèmes et appareils. Pour faciliter une mise en œuvre rapide sans le coût supplémentaire de la configuration des règles d'analyse des sources, la plateforme propose une large gamme d'intégrations prêtes à l'emploi pour intégrer les produits Kaspersky ainsi que des produits tiers :

## Par domaine de sécurité

- Protection des terminaux (solutions EPP et EDR)
- Protection des emails et du trafic Internet (protection des emails, NDR, FW/NGFW, UTM, IDS)
- Security Awareness
- Charge de travail dans le cloud (CASB, CWPP)
- Threat Intelligence (CTI)
- Sécurité de l'identité (IAM, PAM)
- Sécurité OT / IoT
- Prévention des pertes de données

## Par type de données

- XML
- Syslog
- CSV
- JSON
- SQL
- CEF
- Valeur essentielle
- RegExp
- NetFlow v5
- NetFlow v9
- IPFIX

## Par type de transport

- TCP
- UDP
- NetFlow
- sFlow
- NATS JetStream
- Kafka
- HTTP
- SQL (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird, ClickHouse, Elasticsearch)
- Fichier
- Diode
- FTP
- NFS
- WMI
- WEC
- ETW (analyse DNS)
- SNMP
- SNMP Traps
- VMware API
- MS Office 365

## Par fournisseur

- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilon
- Ayehu
- Barracuda Networks
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- Check Point
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- Deep Instinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- ESET
- F5 BIG-IP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion soft
- Intralinks
- Juniper Networks
- Kemp Technologies
- Kerio
- Lieberman Software
- MariaDB
- Microsoft
- MikroTik
- Minerva Labs
- NetIQ
- NETSCOUT
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto Networks
- Penta Security
- Proofpoint
- Radware
- Recorded Future
- ReversingLabs
- SailPoint
- SentinelOne
- SonicWall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro Trustwave
- VMWare
- Vormetric
- WatchGuard
- Windchill FRACAS
- Zettaset
- Zscaler
- etc.

Des intégrations supplémentaires peuvent être développées par l'équipe de Kaspersky Professional Services ou par des partenaires, y compris en utilisant les API des produits connectables. Consultez la liste complète des sources d'événements prises en charge.

Liste complète

**Kaspersky Premium Support**

# Support Premium pour Kaspersky SIEM

Le support Premium pour Kaspersky SIEM est fourni avec les licences Premium et Premium Plus, garantissant une réponse rapide et une assistance de haute qualité pour tous les problèmes afin de maintenir le bon fonctionnement de votre Kaspersky SIEM

| Communication | Support Standard | Licence Premium | Licence Premium Plus |
|---|---|---|---|
| Compte d'entreprise (portail Web) | ● | ● | ● |
| Téléphone | | ● | ● |
| Email | | ● | ● |

| Services | | | |
|---|---|---|---|
| Analyseurs personnalisés pour Kaspersky SIEM | | 5 | 10 |
| Assistance à distance pour diagnostiquer le problème | | ● | ● |
| Transmission prioritaire des demandes d'assistance | | Élevée | Plus élevée |
| Correctifs privés | | | ● |
| Services techniques (TAM) dédiés | | | ● |
| Rapports d'état émanant du TAM | | | Rapport trimestriel |

| Temps de réponse | | | |
|---|---|---|---|
| Problèmes critiques | Pas d'accord de niveau de service (SLA) | 2 heures (24/7) | 30 minutes (24/7) |
| Problèmes majeurs | Pas d'accord de niveau de service (SLA) | 6 heures (8/5) | 4 heures (24/7) |
| Problèmes intermédiaires | Pas d'accord de niveau de service (SLA) | 8 heures (8/5) | 6 heures (8/5) |
| Problèmes mineurs | Pas d'accord de niveau de service (SLA) | 10 heures (8/5) | 8 heures (8/5) |

### Réponse rapide

Les demandes sont classées par ordre de priorité avec des accords de niveau de service stricts pour une résolution plus rapide et plus fiable des problèmes

### Analyseurs personnalisés

Des analyseurs personnalisés permettent au SIEM de traiter des formats de journaux uniques provenant de vos sources de données spécifiques

### Responsable de Compte Technique (TAM) dédié

Avec la licence Premium Plus, un TAM gère tous les problèmes avec une responsabilité accrue

### Correctifs privés

Avec la licence Premium Plus, obtenez des corrections et correctifs personnalisés, conçus pour des problèmes particuliers

# 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.

Les entreprises du monde entier s'appuient sur la plateforme Kaspersky Unified Monitoring and Analysis Platform pour développer des processus de sécurité de l'information complets qui améliorent l'efficacité de la cybersécurité.

En savoir plus

# Kaspersky a utilisé son propre SIEM pour découvrir des programmes malveillants inconnus ciblant les appareils iOS

En surveillant le trafic de notre propre réseau Wi-Fi d'entreprise dédié aux appareils mobiles à l'aide de la Kaspersky Unified Monitoring and Analysis Platform, nous avons détecté une activité suspecte provenant de plusieurs téléphones basés sur iOS.

Comme il est impossible d'examiner les appareils iOS modernes de l'intérieur, nous avons créé des sauvegardes hors ligne des appareils en question, les avons analysés à l'aide de mvt-ios du Mobile Verification Toolkit et avons découvert des traces de compromission.

Apple a réagi en publiant des mises à jour de sécurité pour remédier à quatre vulnérabilités de type zero-day identifiées par les chercheurs de Kaspersky :

CVE-2023-32434, CVE-2023-32435, CVE-2023-38606, CVE-2023-41990

Ces vulnérabilités affectent une large gamme de produits Apple, dont les iPhone, les iPod, les iPad, les appareils macOS, les Apple TV et les Apple Watch. Kaspersky a également informé Apple de l'exploitation d'une fonctionnalité matérielle, que l'entreprise a ensuite atténuée.

# 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