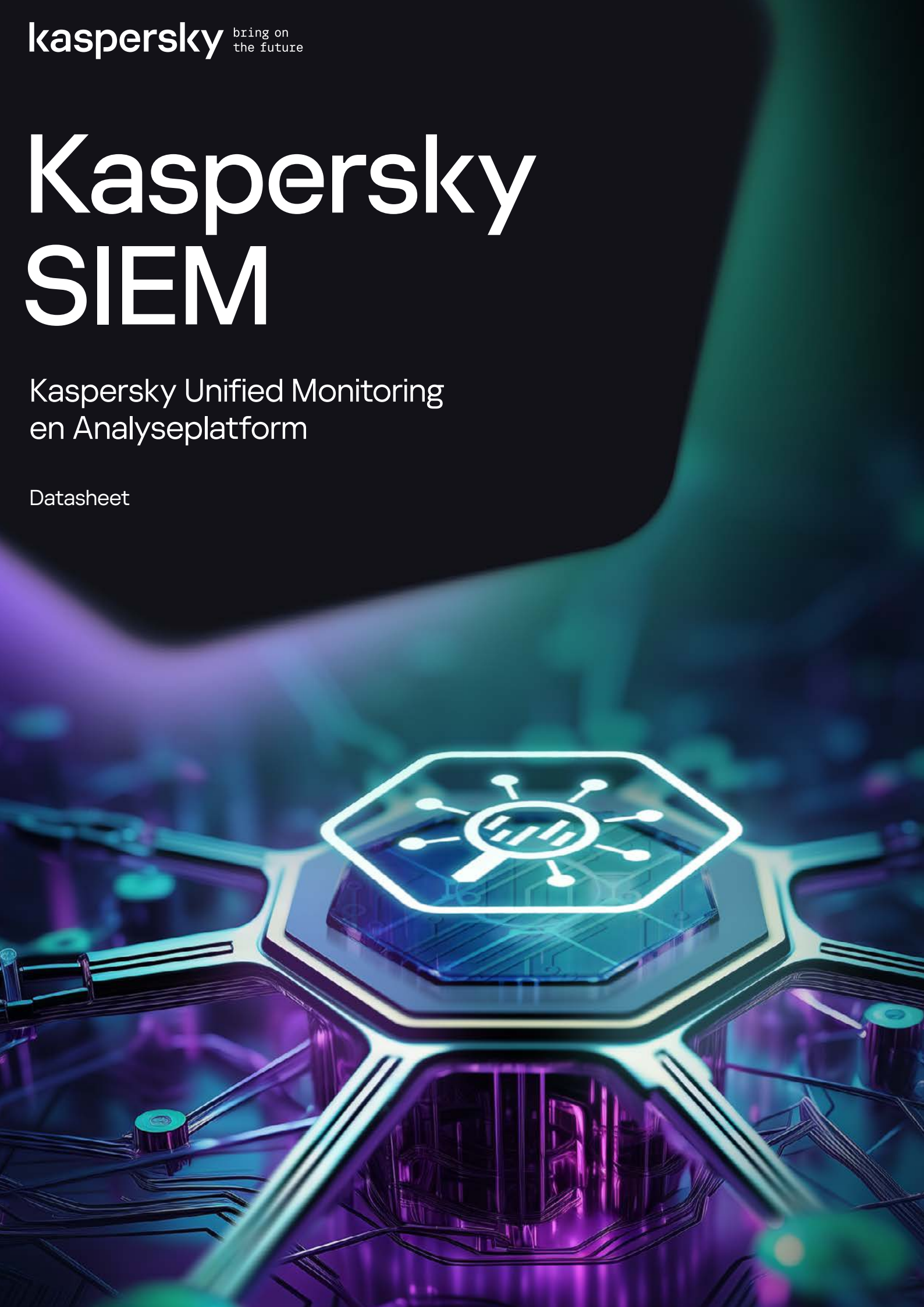
kaspersky bring on the future

Kaspersky SIEM

Kaspersky Unified Monitoring en Analyseplatform

Datasheet



Over Kaspersky SIEM en de architectuur

Kaspersky Unified Monitoring and Analysis Platform is een geïntegreerde next-generation SIEM-oplossing voor het beheren van veiligheidsdata en -events. Het munt uit in het ontvangen, verwerken en bewaren van events rond veiligheidsinformatie, en in het analyseren en correleren van inkomende data. Het platform heeft ook een zoekfunctie, maakt alerts aan bij potentiële bedreigingen en ondersteunt automatische bij alerts en threat hunting.

High-performance modulairearchitectuur verwerkt honderdduizenden events per seconde (EPS) en verlaagt de total cost of ownership (TCO) door de systeemvereisten te ptimaliseren.

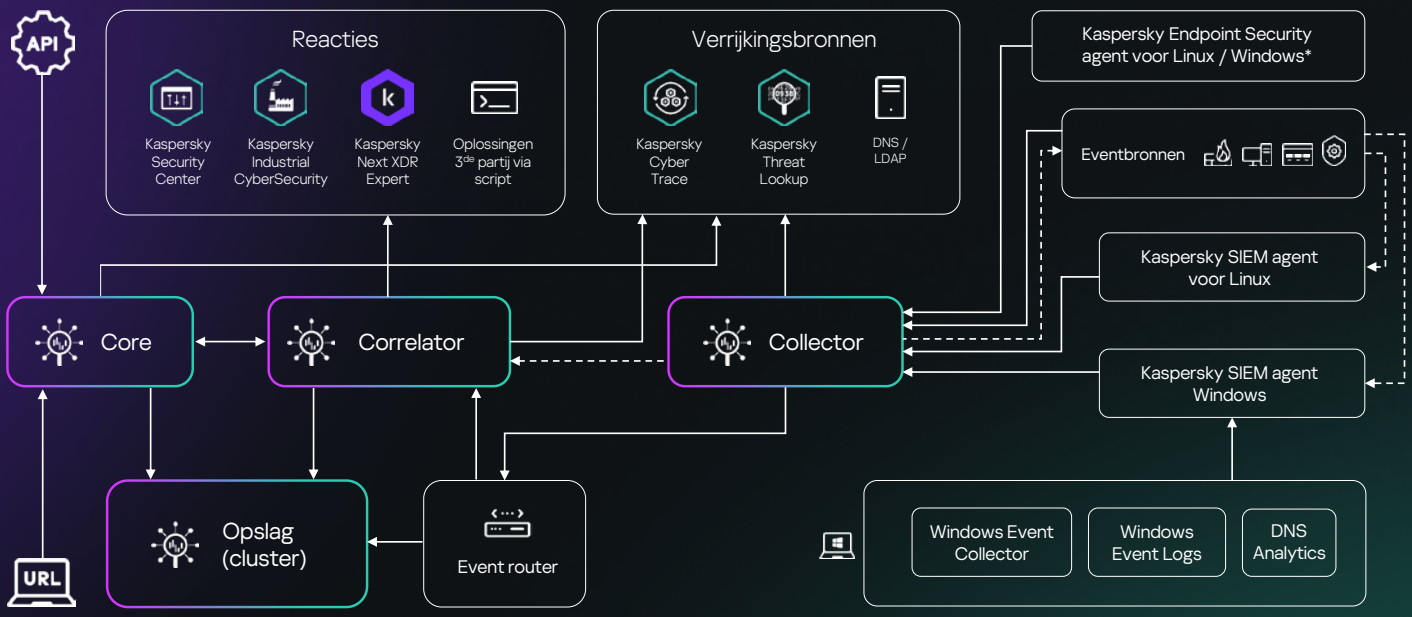
Door producten van derde partijen en van Kaspersky te integreren in een gecentraliseerd systeem voor informatieveiligheid is Kaspersky SIEM een essentieel onderdeel van een uitgebreide verdedigingsstrategie die bedrijfs- en industriële omgevingen kan beschermen en cyberaanvallen kan detecteren, die beginnen in IT en evolueren naar OT-systemen.

Dankzij de microservice-architectuur van de oplossing, kunnen de beheerders de gewenste microservices creëren en configureren om Kaspersky SIEM te gebruiken als een volledig ontwikkeld SIEM- of log management-systeem.

De oplossing ontvangt veiligheidsevents uit verschillende bronnen, waaronder producten van Kaspersky, besturingssystemen, toepassingen van derde partijen, veiligheidstools en verschillende databases, brengt events met elkaar in verband en vult ze aan met data uit threat intelligence feeds om verdachte activiteit in bedrijfsnetwerkinfrastructuren te identificeren en veiligheidsevents tijdig te melden.

Door logs uit alle veiligheidscontroles te verzamelen en de data in realtime te correleren, **verstrekt en brengt Kaspersky SIEM alle informatie samen die noodzakelijk is voor het onderzoeken van en reageren op incidentonderzoek.**

Daarnaast stelt Kaspersky SIEM threat hunters in staat om eerder onbekende dreigingen te ontdekken door operatoren in staat te stellen historische gegevens te analyseren en te correleren, evenals statistische baselines op te stellen om anomalieën te identificeren.



Waarom zou je voor ons kiezen?

Je bespaart tot 50% op hardware- of virtualisatie installatievereisten en verlaagt TCO met een high-performance modulaire oplossing die het consequent beter doet dan de gebruikelijke SIEM-leveranciers op het vak van kostenefficiëntie en kan op elk moment honderdduizenden EPS aan.

Blijf flexibel met onze licentie-opties. Wij tracken de gemiddelde flow EPS per dag na samenvoeging en filtering om overschrijding te vermijden en beperken de toegang tot Kaspersky SIEM niet indien ze zich voordoen.

Geniet van een breed scala aan Kaspersky- en externe integraties met opties voor ingebouwde respons Andere leveranciers kunnen niet concurreren met ons niveau van naadloze integratie met onze eigen producten, waaronder één enkele interface voor Threat Intelligence-integratie, de mogelijkheid om onze endpoint sensors te gebruiken als SIEM-agenten en zoveel meer.

Data voor een langere periode lokaal opslaan, goedkoop en zonder toegevingen te doen, zonder het budget te overschrijden dankzij mogelijkheden voor warme en koude opslag, met behulp van ClickHouse en het Hadoop Distributed File System (HDFS) of lokale disks, terwijl je nog steeds snel in beide gebieden tegelijk kunt zoeken.

Verbetert de gegevensrelevantie en versnelt de detectie en categorisering van incidenten dankzij verrijking met tactische, operationele en strategische bedreigingsintelligentie die wordt aangeboden door ons toonaangevend team van onderzoekers en analisten via het Kaspersky Threat Intelligence Portal.

Ingebouwde multitenancy-ondersteuning waarbij een enkele MSSP in de hoofdinfrastructuur van organisaties het aanmaken van geïsoleerde SIEM mogelijk maakt voor tenants die hun eigen gebeurtenissen ontvangen en verwerken.

Waarom Kaspersky?

Kaspersky SIEM maakt gebruik van de jarenlange opgebouwde kennis en verfijnde vaardigheden van de 5 Centers of Expertise.

Meer informatie

27

We bouwen **al meer dan 27 jaar** tools en bieden diensten om je veilig te houden met onze Meest geteste, Meest bekroonde technologieën.

Meer informatie

We zijn een **wereldwijd privé-cyberbeveiligingsbedrijf** met duizenden klanten en partners over de hele wereld. We staan voor transparantie en onafhankelijkheid.

Meer informatie

Kaspersky Unified Monitoring and Analysis Platform

Meer informatie

www.kaspersky.nl

#kaspersky
#bringonthefuture