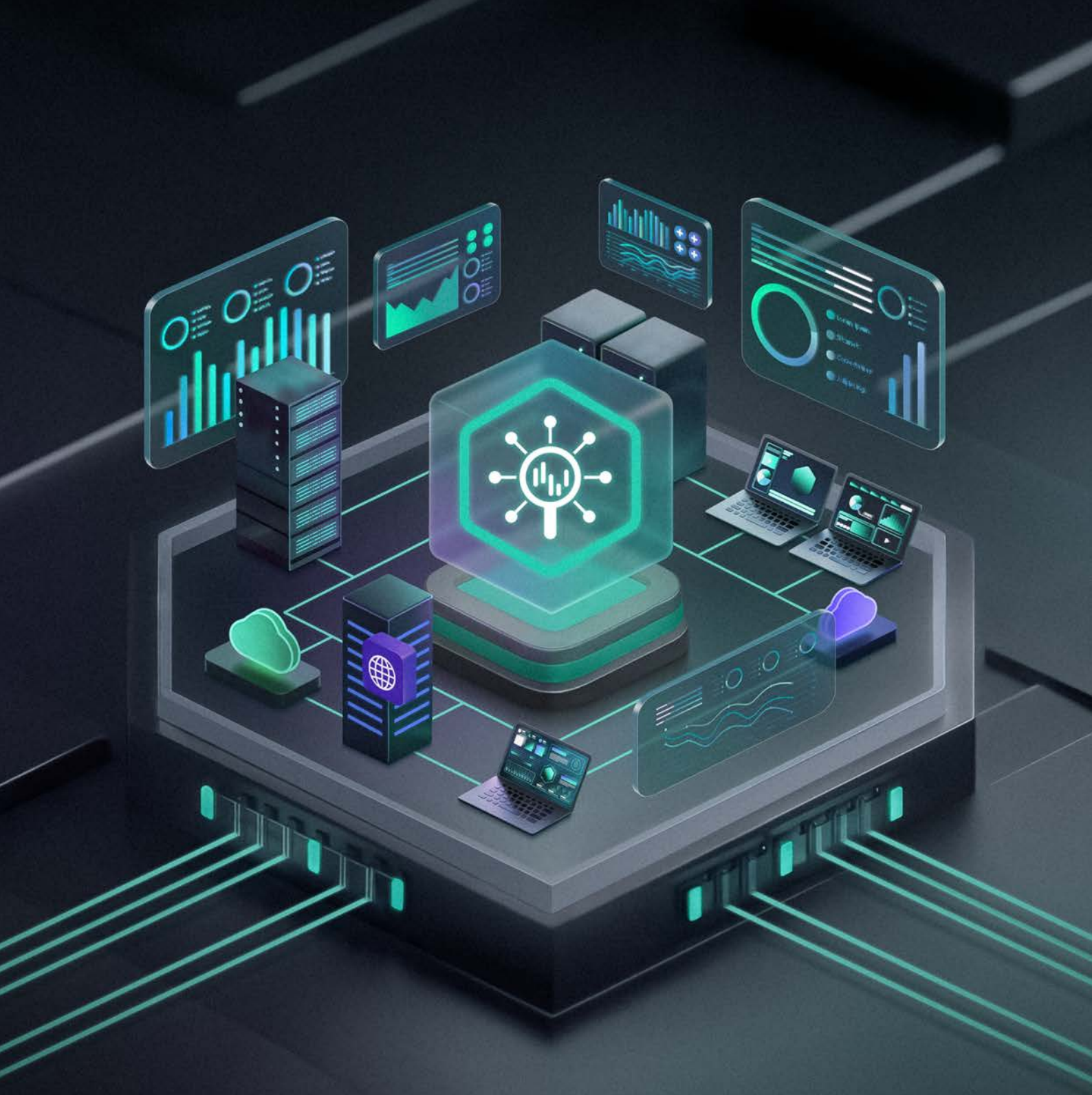


Datasheet

Kaspersky SIEM

Transformeer je beveiligingspraktijken met onze geavanceerde oplossing, mogelijk gemaakt door AI en uitgebreid met dreigingsinformatie van wereldklasse

kaspersky bring on the future

Kaspersky SIEM is voor organisaties met complexe IT-infrastructuren, enorme hoeveelheden aan gegevens en strikte wettelijke vereisten. Het product is MSSP-gereed met ingebouwde multitenancy-ondersteuning.

Deze organisaties erkennen dat effectieve beveiliging niet alleen afhangt van preventie, maar ook van de mogelijkheid om in realtime bedreigingen in diverse systemen te detecteren, analyseren en erop te reageren.

Maximaliseer de impact van je beveiligingsactiviteiten

Grote organisaties hebben steeds meer te maken met geavanceerde, hardnekkige bedreigingen (APT). In 2024 werden APT's in een op de vier bedrijven gedetecteerd en waren ze verantwoordelijk voor 43% van alle incidenten met grote ernst[1]. De gevolgen zijn kostbaar, variërend van bedrijfsonderbreking tot financiële verliezen en langdurige reputatieschade.

Beveiligingsteams staan onder ongekende druk. Beschermingssystemen genereren enorme hoeveelheden gegevens, wat de opslagkosten hoog laat oplopen en SIEM-implementaties duur maakt. Er is een tekort aan bekwame experts en tegelijkertijd lopen bestaande teams over met werk: 70% van de Security Operation Centers (SOC) heeft moeite om de stroom aan waarschuwingen bij te houden[2]. De complexiteit van het beheren van SIEM-systemen zet de al beperkte resources nog verder onder druk.

Zelfs de meest ervaren Security Operation Centers lopen het risico aan efficiëntie en impact in te boeten zonder de AI-tools van tegenwoordig om ze te helpen snel duidelijkheid te krijgen en zich te richten op wat er het meest toe doet.

Voorzie je team van AI-gedreven SIEM, ondersteund door dreigingsinformatie van wereldklasse

Kaspersky SIEM is een geavanceerde oplossing, ontworpen om je beveiligingsteam te helpen inkomende beveiligingsgegevens te beheren en te analyseren. Het blinkt uit in het volgende:

- Gebeurtenissen uit verschillende bronnen, waaronder Kaspersky-producten, besturingssystemen, externe toepassingen, beveiligingstools en databases, verzamelen, verwerken en bewaren.
- Inkomende gegevens in realtime analyseren, correleren en ze verrijken met toonaangevende dreigingsinformatie om verdachte activiteit te detecteren.
- Tijdig waarschuwen om snel incidentenonderzoek en -respons mogelijk te maken.
- Gegevens bewaren voor een langere periode zonder het budget voor prijzige hardwareopslag te overschrijden, met dank aan opties voor 'hot- en cold-opslag' met naadloze, gelijktijdige zoekfunctionaliteit.

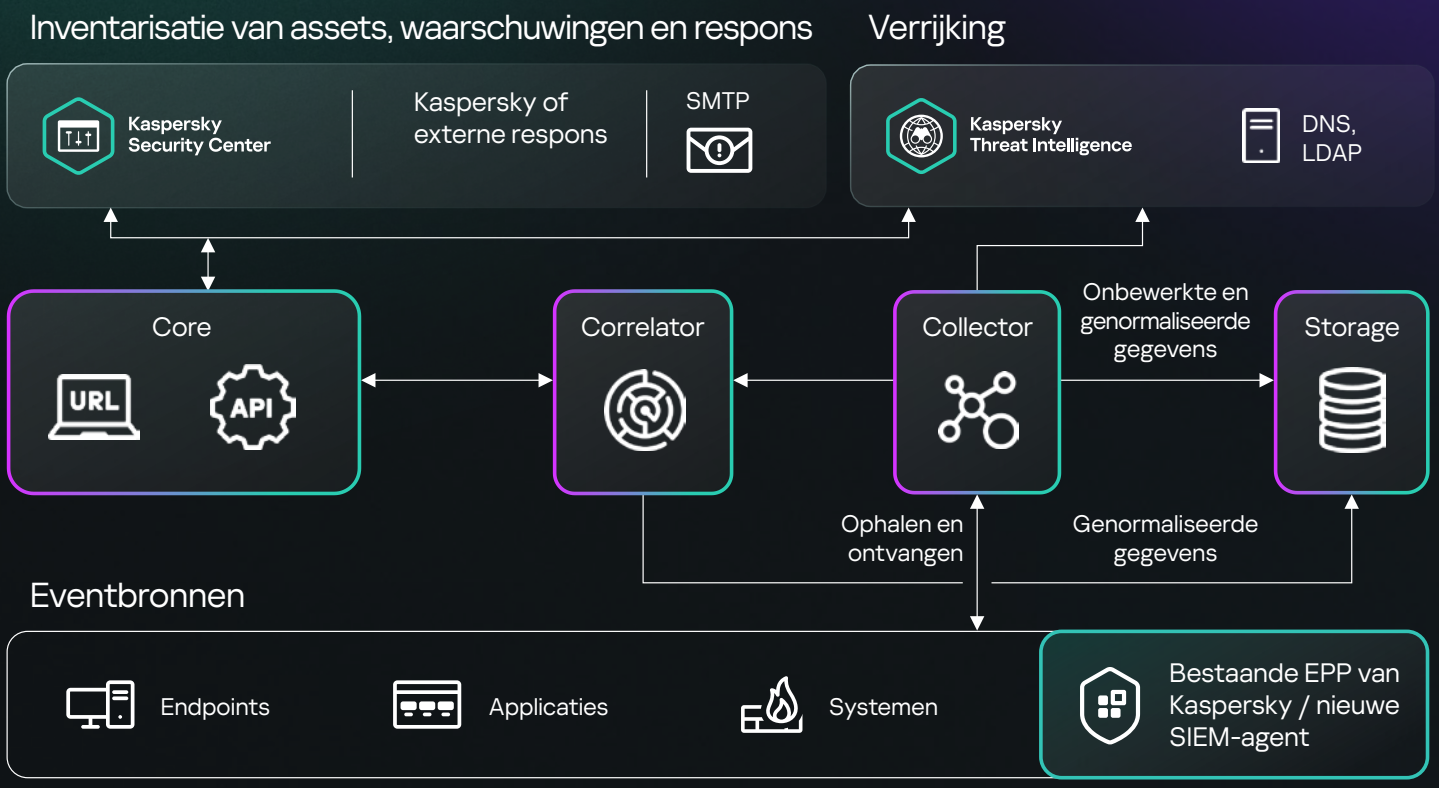
Door logboeken uit beveiligingsbronnen samen te voegen en ze in realtime te correleren, geeft Kaspersky SIEM je analisten volledig inzicht en de context die nodig is om efficiënt te handelen.

Het biedt geavanceerde zoek- en analysemogelijkheden waarmee je opspoorders van dreigingen bedreigingen kunnen ontdekken die voorheen onbekend waren. Historische gegevensanalyse en statistische baselines met de UEBA-regelset voor detectie helpen je team afwijkingen te herkennen en geavanceerde aanvallen te stoppen.

Met Kaspersky SIEM krijgt je SOC het inzicht, de informatie en de efficiëntie die het nodig heeft om de massa aan gegevens om te zetten in bruikbare beveiligingsinzichten. De oplossing werkt zonder internetverbinding, om volledige datasoevereiniteit te garanderen.

1 Kaspersky Managed Detection and Response-analistenrapport voor 2024
2 Kaspersky-rapport: Het portret van de moderne informatiebeveiligingsprofessional, 2024

Hoe het werkt



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

Kaspersky SIEM is ontwikkeld op een Open Single Management Platform[3], waarbij zowel Kaspersky-producten als externe producten in een gecentraliseerd beveiligingssysteem worden geïntegreerd. Het vormt een essentieel onderdeel van een uitgebreide verdedigingsstrategie, waarmee zakelijke en industriële omgevingen worden beschermd en cyberaanvallen worden gedetecteerd die zich van IT- naar OT-systemen verplaatsen.

Wat Kaspersky SIEM zo bijzonder maakt

Maximaliseert prestaties, minimaliseert de kosten

Bespaar tot wel 50% op de kosten voor hardware en virtualisatie en verlaag de TCO met een hoogwaardiger, modulair SIEM dat beter presteert dan oudere oplossingen en honderdduizenden EPS per instantie afhandelt.

Eén geïntegreerd Kaspersky-ecosysteem

Maak gebruik van meer dan 200 vooraf geconfigureerde Kaspersky-integraties en externe integraties met ingebouwde responsopties. Ons naadloze ecosysteem biedt één interface voor dreigingsinformatie, gebruikt endpointsensoren als SIEM-agenten en levert integratiemogelijkheden die andere leveranciers niet kunnen evenaren.

Ingebouwde SOC-expertise

Toegang tot meer dan 700 vooraf geconfigureerde detectieregels die elke 3 maanden worden bijgewerkt met MITRE-afstemming en responsbegeleiding: allemaal ontwikkeld door Kaspersky SOC, een van de meest ervaren teams in de sector op het gebied van dreigingsopsporing.

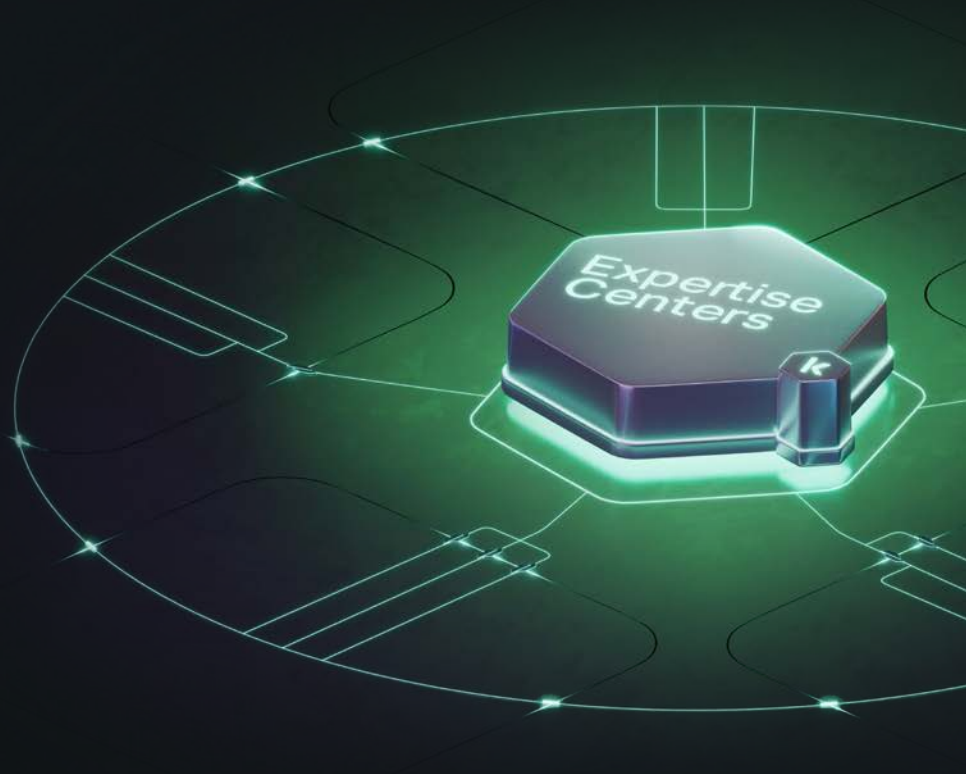
Dreigingsdetectie op basis van AI

Componenten die met AI zijn uitgebreid herkennen snel verdachte activiteit in je infrastructuur met AI-detectie van DLL-hijacking, op AI gebaseerde risicoscores van assets en meer. Deze functies verbeteren detectienauwkeurigheid, verlagen het aantal false positives en minimaliseren de impact van cyberincidenten, wat helpt je MTTD en MTTR te verbeteren.

3 Kaspersky Next XDR Expert, wat wordt aangedreven door dit platform, breidt mogelijkheden uit met geavanceerde dreigingsopsporing, geautomatiseerde draaiboeken en gestroomlijnd casebeheer.

Kaspersky SIEM maakt gebruik van jarenlange opgebouwde kennis en verfijnde vaardigheden van Kaspersky-expertisecentra: vijf gespecialiseerde, samengevoegde hubs ter bevordering van de cyberbeveiliging.

Meer informatie



Kaspersky SIEM komt met 24/7 Premium ondersteuning en services, waaronder aangepaste integraties van Kaspersky Professional Services en vertrouwde partners, die gebruikmaken van de API-mogelijkheden van verbonden producten.

We bieden kant-en-klare implementatie, naadloze migratie-ondersteuning en voortdurende expertise om ervoor te zorgen dat je maximaal profiteert van je SIEM-implementatie.

Kaspersky SIEM

www.kaspersky.com

Meer informatie

#kaspersky
#bringonthefuture