White paper
Product

Kaspersky SIEM

kaspersky bring on the future

Contents

Veiligheidsinformatie en Markt voor Event Management 3

Over Kaspersky SIEM en de architectuur 4

Functies Kaspersky SIEM 6

- Informatie over veiligheidsevents beheren, verwerken en bewaren .....
- Real-time en historische correlatie van veiligheidsevents .....
- Data-opslag van veiligheidsevents .....
- Geïntegreerde antwoordcapaciteiten .....
- AI en machine learning-tools .....
- Uitstekende visualisering met dashboards en rapporten .....
- Multitenancy-architectuur .....
- Uitgebreid scala out-of-the-box integraties .....

Premium ondersteuning voor Kaspersky SIEM 13

Waarom zou je voor ons kiezen? 14

Kaspersky gebruikte zijn eigen SIEM om eerder onbekende malware te onthullen 15

Markt voor veiligheidsinformatie en eventbeheer

Diensthoofden cyberbeveiliging in organisaties worden met tal van uitdagingen geconfronteerd, waaronder steeds meer pogingen om in de infrastructuur binnen te dringen, een tekort aan personeel en steeds complexere aanvallen.

Daarnaast moeten ondernemingen regelgeving volgen in verband met het bewaren van data, auditing en incidentonderzoek, wat een impact heeft op de globale SIEM-markt.

Organisaties staan ook onder druk om meldingen van cyberaanvallen in te delen volgens prioriteit en efficiënter te filteren, omdat ze zich steeds vaker voordoen.

Daarnaast heeft het telewerken ertoe geleid dat ondernemingen SaaS-toepassingen moeten implementeren en werknemers de kans moeten bieden hun eigen toestellen mee te brengen (BYOD), waardoor de behoefte aan meer netwerkzichtbaarheid achter de traditionele perimeter toeneemt.

Tot slot is het ook niet eenvoudig om op de huidige arbeidsmarkt gekwalificeerde veiligheidsexperts te vinden. Ondernemingen zijn op zoek naar manieren om hun resources te optimaliseren en de efficiëntie van cyberveiligheid te verbeteren. Organisaties willen dan ook graag vlot toegankelijke en bruikbare intelligence data voor hun SOC-teams.

Volgens het Kaspersky Human Factor 360 Verslag

77%

van de ondernemingen werden geconfronteerd met ten minste één inbreuk op de cyberveiligheid, en voor sommige liep dat aantal op tot zes

41%

van de ondernemingen hebben gaten in hun cyberveiligheid infrastructuur en plannen hun investeringen tijdens de komende periode op te trekken

Meer informatie

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 optimaliseren.

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.

Het Kaspersky Unified Monitoring en Analyseplatform omvat de volgende componenten

Een **Kern**met een gecentraliseerde grafische gebruikersinterface voor het regelen en bewaken van de instellingen van systeemonderdelen. Het platform is toegankelijk vanaf oplossingen van derde partijen die de API gebruiken.

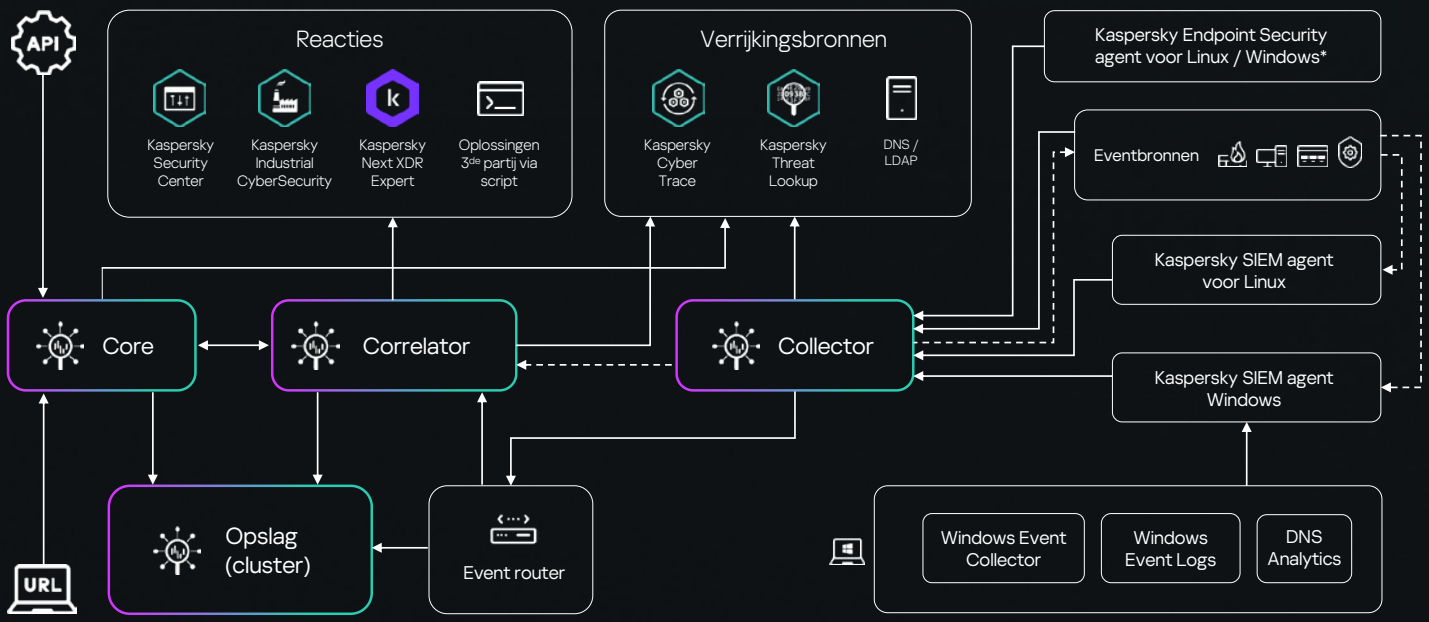
Er worden correlatieregels gebruikt om specifieke sequenties van verwerkte gebeurtenissen te detecteren en bepaalde acties uit te voeren na herkenning, zoals het creëren van correlatie-events/ alerts of het interageren met een actieve lijst. De **Correlator** gebruikt actieve lijsten om de vereiste acties uit te voeren na het analyseren van genormaliseerde events die werden ontvangen van alle collectors en genereert alerts op basis van correlatiecriteria.

Een of meerdere **Collectors** ontvangen events van externe bronnen en preprocessen ze: normaliseren (omzetten in één formaat), filteren, aggregeren en verrijken met data van externe bronnen d.m.v. woordenboeken, oproepen naar de DNS-service, en andere tools.

De storage wordt gebruikt om genormaliseerde events op te slaan zodat ze snel en permanent toegankelijk zijn via SIEM voor het extraheren van analytische data.

Agenten sturen ruwe events door van workstations en servers naar SIEM-collectors. Het verzenden van Windows-logevents is voortaan mogelijk in Kaspersky Endpoint Security voor Windows 12.6 of Linux 12.2. Dit verlaagt aanzienlijk de hoeveelheid werk die noodzakelijk is voor het integreren van eventbronnen met het SIEM-systeem van Kaspersky.

Event routers verlagen de belasting van links en het aantal poorten die worden geopend op firewalls doordat events gestaag worden ontvangen, zonder vertraging, wanneer de collectors worden geplaatst in kantoren op afstand met een lage brandbreedte of datalinks die al in gebruik zijn.



Functionaliteit Kaspersky SIEM

Geïntegreerde connectors op maat naar honderden bronnen van Kaspersky en derde partijen met regelmatige updates en verbeteringen.

Integratie van externe eventbronnen met gratis aanmaken van extra connectoren door het Kaspersky Professional Services team.

Snelle zoekopdrachten en verslagen over veiligheidsevents.

Lokale veilige opslag van logs met inachtneming van de regelgeving en het onderzoek van incidenten.

Kaspersky SIEM ondersteunt het zoeken naar events in verschillende opslagruimtes om operatoren te helpen sneller en makkelijker relevante events te vinden in verspreide opslagclusters.

Informatie over veiligheidsevents monitoren, verwerken en opslaan.

Kaspersky Unified Monitoring en Analyseplatform ontvangt events van logs en normaliseert data uit verschillende eventbronnen om ze aan elkaar aan te passen.. Deze informatieveiligheidsevents kunnen inlogpogingen omvatten, interacties met databases of verzending van sensorinformatie en worden verzameld in de volledige beschermde IT-infrastructuur van de onderneming. Terwijl een individueel event mogelijk niet significant lijkt, geven verschillende individuele events een duidelijker beeld van kwaadaardige activiteit die kan worden gebruikt om veiligheidsproblemen op te sporen.

Data lake, onze gecentraliseerde lokale opslagruimte, biedt een platform voor het verzamelen, indexeren en analyseren van logs van verschillende bronnen, incl. veiligheidsoplossingen (EPP, FW, IAM, enz.), besturingssystemen, zakelijke toepassingen (HR-systemen, kantoortoepassingen), fysieke veiligheidssystemen (systemen voor automatische toegangscontrole) en andere toestellen.

Events worden naar de correlator verstuurd voor analyse en opslag voor retentie, zodra ze zijn gefilterd en samengevoegd. Om alerts te identificeren, ontvangt de collector events uit bronnen, verwerkt ze en stuurt ze door naar opslag, correlator en/of diensten van derde partijen. Ruwe events worden doorgestuurd van workstations en servers naar SIEM-collectors (in bepaalde gevallen door agenten) en kunnen naar andere systemen worden verstuurd voor bijkomende analyse.

Correlatie-events worden geproduceerd door de oplossing na herkenning van een specifiek event of reeks gerelateerde events en worden ook geanalyseerd en bewaard. Indien een event of opeenvolging van events wijst op een mogelijke veiligheidsdreiging, maakt Kaspersky SIEM een alert aan met informatie over de dreiging en andere relevante informatie die veiligheidsspecialisten in acht moeten nemen.

Betrouwbare transportprotocols, met optionele encryptie, worden gebruikt voor de transfer van events tussen componenten. Het systeem kan een datadiode gebruiken om data uit geïsoleerde segmenten te halen.

Kaspersky SIEM maakt gecentraliseerd asset management mogelijk door een ruim assortiment aan servers, workstations en netwerkapparaten aan te bieden. Het platform kan data verzamelen over kwetsbare assets uit bronnen als kwetsbaarheidsscanners en ze correleren met data over de assetcategorie om bedreigingen te identificeren. Dat biedt de veiligheidsteams een betere kijk op het volledige assetlandschap.

Om analisten te ondersteunen wordt dekking van de MITRE ATT&CK matrix d.m.v. regels weergegeven zodat het veiligheidsniveau beter kan worden ingeschat.

650+ gepreconfigureerde correlatieregels voor het detecteren van aanvalsscenario's worden door de servers van Kaspersky regelmatig geüpdatet met MITRE mapping en antwoordaanbevelingen.

Verbeterde datarelevantie dankzij verrijking met analytische data, verzameld uit het Kaspersky Threat Intelligence Portal (met behulp van Kaspersky Threat Lookup en Kaspersky CyberTrace).

Data over assets en infrastructuur is afkomstig uit het Kaspersky Security Center en bronnen van derde partijen.

Gebruikers kunnen een event vergelijken met gegroepeerde, samengevoegde, gemiddelde, maximale en minimale waarden voor een specifieke periode, met behulp van de ClickHouse-functie voor data mining. Dat breidt de mogelijkheden voor detectielogica aanzienlijk uit, zonder dat er verschillende serviceregels moeten worden aangemaakt.

Om het creëren van content en editing te vereenvoudigen, bieden we gebruikers de kans om van tevoren na te gaan welke correlatieregels de beoogde wijziging zal toepassen alvorens wijzigingen aan de filtercriteria aan te brengen.

Real-time en historische correlatie van veiligheids events

Kaspersky SIEM voert nagenoeg real-time cross-correlatie uit d.m.v. regels voor het identificeren van aanvallen en bedreigen en honderden voorgedefinieerde regels ontwikkeld door Kaspersky SOC, een van de meest succesvolle en ervaren actieve teams voor bedreigingsopsporing in de sector. Kaspersky SOC experts beschikken over honderden attesten die het hoge niveau van hun kennis en knowhow bevestigen.

De events worden**in real time gecorreleerd**. De correlator analyseert genormaliseerde events, maakt alerts aan in overeenstemming met de correlatieregels en verwerkt alle actieve lijstverrichtingen.

Het werkingsprincipe van de correlator is gebaseerd op de analyse van de handtekening van het event, zodat elk event wordt verwerkt in overeenstemming met de gebruikersspecifieke correlatieregels. De software genereert een correlatie-event en verstuurt het naar de opslag waar het een reeks events aantreft die beantwoorden aan de vereisten van de correlatieregel. De gebruiker kan de correlatieregels zo instellen dat ze worden getriggerd door het resultaat van een eerdere analyse, door het correlatie-event naar de correlator te sturen voor extra analyse. De resultaten van de correlatieregel kunnen door andere correlatieregels worden gebruikt. Zo kunnen verschillende kleinere alerts een groter alert genereren (verschillende brutale pogingen kunnen worden geanalyseerd om een groot incident met brutale kracht te identificeren)

Het platform gebruikt historische data om trends op te sporen, bedreigingen te vinden die eerder onopgemerkt bleven en aanvallen te identificeren die door bepaalde veiligheidselementen over het hoofd werden gezien, wat de algemene bedreigingsdetectie verbetert.

Oplossingen van derde partijen of geïntegreerde producten **Kaspersky EndpointDetectie en Respons** staan in voor detectie door sensoren. Door de productinstellingen aan te passen,

De correlatietool van de oplossing beschikt over platformdetectie. Dankzij de krachtige correlatietool van het platform kunnen gebruikers aanpasbare correlatieregels creëren. Ook zijn er kant-en-klare regels en normalisatiepakketten beschikbaar ter ondersteuning van commercieel toegankelijke producten van derde partijen die permanent worden uitgebreid en geüpdatet.

Het werkingsprincipe van de correlator is gebaseerd op de analyse van de handtekening van het event, zodat elk event wordt verwerkt in overeenstemming met de gebruikersspecifieke correlatieregels. De software genereert een correlatie-event en verstuurt het naar de opslag waar het een reeks events aantreft die beantwoorden aan de vereisten van de correlatieregel.

Het detecteren van bedreigingen om eerder onbekende bedreigingen te ontdekken door operatoren de kans te bieden historische data te analyseren en correleren met behulp van een krachtige, kolomgebaseerde database.

Gebruikers kunnen vlot filters, woordenboeken en regels lokaliseren die met één enkele tag worden aangeduid door middel van de taggebaseerde zoekfunctie. Door het opslaan van de zoekgeschiedenis kan de gebruiker makkelijk eerdere opdrachten terugvinden.

Het platform kan data opslaan gedurende een langere periode zonder over het budget te gaan dankzij de warme en koude opslagopties met behulp van ClickHouse en de Hadoop Distributed File System (HDFS) of lokale schijven.

Beheerders kunnen dagelijks ruimtegebrek in het subsysteem van de schijf vermijden dankzij flexibele instellingen: de diepte van de bewaarde events kan worden ingesteld in gigabytes als een percentage van de schijfruimte, maar ook in dagen.

Data-opslag van veiligheidsevents

De opslagcomponent van Kaspersky SIEM wordt gebruikt voor het opslaan van genormaliseerde events teneinde snel en permanent toegang te krijgen tot analytische data van het **Kaspersky Unified Monitoring en Analyseplatform**.

ClickHouse waarborgt continuïteit en snelle toegang. De opslag is verbonden met een Kaspersky SIEM opslagdienst via een ClickHouse cluster. Ook koude opslagdisks kunnen worden toegevoegd aan ClickHouse clusters.

Gebruikers kunnen ruimte toevoegen in de opslagruimtes voor in groep opgeslagen events op basis van een specifiek attribuut. Op die manier kunnen beheerders verschillende opslatijden instellen voor events op basis van hun specifieke kenmerken.

Kaspersky Unified Monitoring en Analyseplatform werkt ook met datacompressie om de schijfruimte dramatisch te verkleinen zonder het terugvinden van data te bemoeilijken. Twee domeinen worden ondersteund door de oplossing van Kaspersky: een voor het snel terugvinden van data en een ander voor de opslag van grote hoeveelheden data.

Het platform bestaat uit twee afzonderlijke delen: een voor koude opslag op het Hadoop Distributed File System of op lokale schijven, en het andere voor operationele opslag met behulp van ClickHouse. Deze opsplitsing is transparant voor gebruikers.

Operatoren hoeven niet te schakelen tussen archieven en kunnen zoekopdrachten aanmaken in één enkele interface zodat ze hun volledige aandacht aan de opzoeking kunnen besteden. Dit **verlaagt de cost of ownership van het systeem** en behoudt een uitstekende gebruikerservaring. Het platform ondersteunt zoekopdrachten in verschillende opslagruimtes om operatoren te helpen sneller en makkelijker relevante events te vinden in verspreide opslagclusters.

Organisaties kunnen de regelgevingsvereisten voor dataretentie, auditing en incidentenonderzoek naleven, door logs van verschillende bronnen veilig te verzamelen en op te slaan. Daarnaast maakt gecentraliseerde en gestructureerde opslag het makkelijker voor ondernemingen om logs indien nodig terug te vinden en te analyseren.

Kaspersky Next XDR Expert

Een ruimer aanbod van antwoordcapaciteiten via playbooks is beschikbaar in Kaspersky Next XDR Expert.

Meer informatie

Geïntegreerde antwoordcapaciteiten

Ingebouwde antwoordfunctionaliteit die gebruikmaakt van producten van Kaspersky verhoogt de veiligheidsefficiëntie. Zo kan Kaspersky SIEM worden gekoppeld aan Kaspersky Endpoint Detection and Response om de antwoordcapaciteiten ui te breiden, en zo de netwerkisolatie van assets en preventieregels te beheren of toepassingen en scripts uit te voeren. Deze antwoordacties kunnen manueel of automatisch worden uitgevoerd op assets met de Kaspersky Endpoint Security agent.

Geautomatiseerde verzameling van inventarisinformatie (geïnstalleerde software, kwetsbaarheden, uitrusting, asseteigenaars enz.) kunnen helpen om de informatieveiligheidsevents te contextualiseren en te helpen bij incidentonderzoek.

Kaspersky SIEM ondersteunt Kaspersky CyberTrace, een full-featured platform met bedreigingsinformatie dat tientallen out-of-the-box datafeeds rond bedreigingen ondersteunt (commercieel en openbaar) om de verrijking van events in realtime te streamen met contextinformatie over gevaarsindicatoren.

De AI-componenten van Kaspersky SIEM maken een snelle detectie mogelijk van verdachte activiteit in de infrastructuur

AI en machine learning-tools

Kaspersky maakt gebruik van voorspellende algoritmen, clusteringtechnieken, neurale netwerken, statistische modelleringstechnieken en deskundige algoritmen om de doeltreffendheid van onze producten te verhogen door bedreigingen sneller te detecteren en detecties nauwkeurig te prioriteren.

Monitoring- en responsteams kunnen waarschuwingen prioriteren en zich richten op het voorkomen van potentiële schade, gecontroleerd door big data en AI-systemen. De AI-module helpt bij triage door historische gegevens te analyseren, prioriteit te geven aan inkomende waarschuwingen en op AI gebaseerde risicoscores voor bedrijfsmiddelen te geven. Deze aanpak helpt bij het genereren van waardevolle hypotheses die kunnen worden gebruikt voor proactieve zoekopdrachten.

Het platform gebruikt door de gebruiker gedefinieerde correlatieregels om gebeurtenissen in realtime te koppelen. De correlatiemodule past algoritmen van kunstmatige intelligentie toe om afwijkende activiteiten te detecteren, zoals plotselinge verkeerspieken of meervoudige toegang tot services die duiden op een potentieel incident.

Kaspersky SIEM bevat ook gegevens van Kaspersky Threat Intelligence, die worden gegenereerd met behulp van AI en big data-technologieën. De database wordt voortdurend verrijkt met de resultaten van handmatige APT-analyses, operationele Darknet-gegevens, informatie van Kaspersky Security Network en inzichten uit regelmatige nieuwe malware-analyses.

AI deze technologieën helpen gebruikers om potentiële schade door cyberincidenten te minimaliseren en MTTR en MTTD te verhogen.

Uitstekende visualisatie met dashboards en rapporten presenteert gegevens in de meest bruikbare indelingen om trends, patronen en afwijkende gebeurtenissen te identificeren.

Met aanpasbare widgets voor eenvoudige visualisatie en weergave van indicatoren kunnen analisten incidenten prioriteren, hoofdoorzaken bepalen en efficiënter reageren op bedreigingen, terwijl organisaties de effectiviteit van hun beveiligingsactiviteiten kunnen volgen, trends kunnen identificeren en de algehele gezondheid van hun beveiligingssysteem kunnen beoordelen.

Gebruikers kunnen gegevens uit gebeurtenisvelden verrijken met de inhoud van woordenboeken, tabellen, bedrijfsmiddelen en accountkenmerken en deze gegevens gebruiken voor zoekopdrachten en visualisatie. Dit helpt bij het bouwen van dashboards en rapporten met meer contextuele gegevens.

Deze oplossing helpt gebruikers hun eigen widgets te maken met aanpasbare instellingen, evenals lay-outs met **verschillende widgetgroepen:**

Belangrijkste alert metrics

(ernst, prioriteit en status)

- Getroffen assets
- Recente meldingen
- Belangrijkste databronnen met de meeste alerts
- Alerts toegewezen aan specifieke operatoren
- Getroffen gebruikers en/of apparaten
- Alerts per policy

Belangrijkste incident-indicatoren

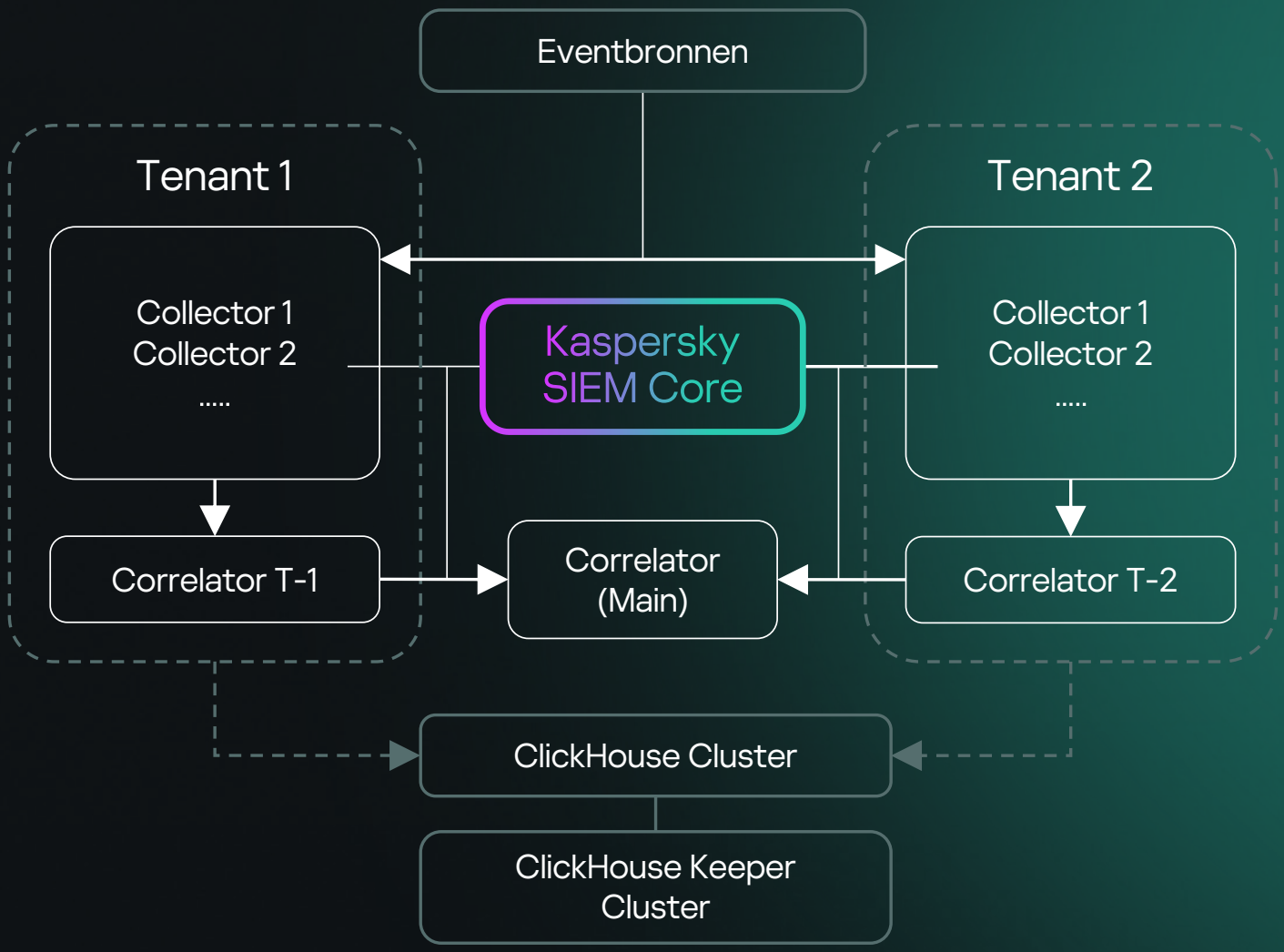
(ernst en toewijzing)

- Getroffen apparaten
- Top interne en externe IP's op basis van Netflow-verkeersvolume (Bytesln).
- Belangrijkste knooppunten voor beheer op afstand (poorten 3389, 22).
- Totaal aantal NetFlow-bytes voor interne poorten
- Topbronnen gebaseerd op aantal gebeurtenissen, categorieën, bedrijfsmiddelen en gebruikers

Multitenancy-architectuur

Kaspersky SIEM biedt volledige ondersteuning voor multitenancy, wat betekent dat gebruikers in de ene tenant de gegevens (gebeurtenissen, waarschuwingen, incidenten, enz.) van een andere tenant niet kunnen zien. In multitenancy-modus maakt één instantie van de Kaspersky SIEM-applicatie in de hoofdorganisatie het mogelijk om filialen te isoleren, zodat ze hun eigen events ontvangen en verwerken.

Het systeem wordt centraal beheerd via de hoofdinterface en tenants werken onafhankelijk met alleen toegang tot hun eigen resources, services en instellingen. Tenant-gerelateerde gebeurtenissen worden apart opgeslagen. Gebruikers kunnen gelijktijdig toegang krijgen tot meerdere tenants. De algemene beheerder kan ook specificeren welke tenantgegevens worden weergegeven in verschillende delen van de webinterface.



Het platform biedt een filtergebaseerd systeem voor het distribueren van gebeurtenissen naar ruimtes. Gebruikerstoegang tot evenementen wordt nu ingesteld op ruimteniveau. Dit maakt granulaire controle mogelijk van de toegang tot evenementen binnen één tenant.

Het systeem wordt centraal beheerd via de hoofdinterface, terwijl tenants onafhankelijk van elkaar opereren en alleen toegang hebben tot hun eigen resources, services en instellingen. De events van tenants worden apart opgeslagen.

Uitgebreid scala out-of-the-box integraties

Kaspersky Unified Monitoring and Analysis Platform is grondig geïntegreerd met oplossingen en technologieën van Kaspersky voor een gecoördineerd gebruik van producten met verbeterde efficiëntie. Leveranciers van derden kunnen niet tippen aan ons niveau van naadloze integratie met onze eigen producten, waaronder een enkele interface voor Threat Intelligence-integratie, de mogelijkheid om onze endpointsensoren te gebruiken als SIEM-agenten en nog veel meer.

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

en meer

Integratie met het uitgebreide portfolio van <**Kaspersky Threat Intelligence**-services helpt bij het identificeren en prioriteren van bedreigingen en krijgt snel toegang tot contextuele informatie over nieuwe aanvallen, compromisindicatoren en tactieken en technieken van aanvallers.

* Inclusief mogelijke integraties met Kaspersky Endpoint Detection and Response Expert, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Next EDR Foundations, Kaspersky Next EDR Optimum, Kaspersky Next EDR Expert

Kaspersky SIEM blinkt uit in het ontvangen van gegevens (logs) van andere systemen en apparaten. Om een snelle implementatie mogelijk te maken zonder de extra kosten van het opzetten van regels voor bronanalyse, wordt het platform geleverd met een groot aantal kant-en-klare integraties voor Kaspersky-producten en producten van derden:

Per beveiligingsdomein

- Endpoint Protection (EPP & EDR oplossingen)
- E-mail en internet verkeerbescherming (e-mailbescherming, NDR, FW / NGFW, UTM, IDS)
- Beveiligingsbewustwording
- Cloud workload (CASB, CWPP)
- Veiligheidsinformatie (CTI)
- Identiteitsbeveiliging (IAM, PAM)
- OT/IoT-beveiliging
- Preventie van gegevensverlies (DLP)

By data type

- XML
- Syslog
- CSV
- JSON
- SQL
- CEF
- Key-Value
- RegExp
- NetFlow v5
- NetFlow v9
- IPFIX

Per transporttype

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

Aanvullende integraties kunnen worden ontwikkeld door het Kaspersky Professional Services team of partners, onder andere door gebruik te maken van de API's van koppelbare producten. Bekijk de volledige lijst met ondersteunde gebeurtenisbronnen.

Volledige lijst

Per leverancier

- 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
- enz.

Kaspersky Premium Support

Premium Support voor Kaspersky SIEM

Kaspersky Premium Support voor Kaspersky SIEM wordt geleverd met zowel Premium- als Premium Plus-licenties, waardoor je verzekerd bent van snelle respons en hoogwaardige assistentie bij problemen, zodat je Kaspersky SIEM probleemloos blijft werken.

Communicatie	Standaard-ondersteuning	Premium licentie	Premium Plus licentie
Account onderneming (webportaal)	●	●	●
Telefoon		●	●
E-mail		●	●

Service			
Custom parsers voor Kaspersky SIEM		5	10
Verbinding op afstand om een probleem te diagnosticeren		●	●
Escalatie van ondersteuningsverzoeken op basis van prioriteit		Hoog	Hoogst
Privépatches			●
Dedicated Technical Account Manager (TAM)			●
Statusverslagen van TAM			Kwartaalrapport

Reactietijden			
Kritieke problemen	Geen SLA	2 uur (24/7)	30 min (24/7)
Problemen hoog niveau	Geen SLA	6 uur (8/5)	4 uur (24/7)
Problemen niveau medium	Geen SLA	8 uur (8/5)	6 uur (8/5)
Problemen niveau laag	Geen SLA	10 uur (8/5)	8 uur (8/5)

Snel antwoord

Verzoeken krijgen prioriteit met strikte SLA's voor een snellere en betrouwbare oplossing van problemen

Aangepaste parsers

Met aangepaste parsers kan SIEM unieke logformaten van uw specifieke gegevensbronnen verwerken

Toegewijd TAM-team

Met de Premium Plus licentie beheert een TAM alle problemen met extra aansprakelijkheid.

Privépatches

Krijg patches op maat, ontwikkeld voor specifieke problemen, met de Premium Plus licentie

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.

Ondernemingen over de hele wereld vertrouwen op het Kaspersky Unified Monitoring and Analysis Platform om uitgebreide informatiebeveiligingsprocessen te ontwikkelen die de efficiëntie van cyberbeveiliging verbeteren.

Meer informatie

Kaspersky gebruikte zijn eigen SIEM om voorheen onbekende malware gericht op iOS-apparaten te ontdekken

Tijdens het monitoren van het netwerkverkeer van ons eigen zakelijke Wi-Fi-netwerk speciaal voor mobiele apparaten met behulp van het Kaspersky Unified Monitoring and Analysis Platform, ontdekten we verdachte activiteit afkomstig van meerdere iOS-telefoons.

Omdat het onmogelijk is om moderne iOS-apparaten van binnenuit te onderzoeken, hebben we offline back-ups gemaakt van de apparaten in kwestie, deze onderzocht met mvt-ios van de Mobile Verification Toolkit en sporen van compromittering ontdekt.

Apple reageerde door beveiligingsupdates uit te brengen om vier zero-day kwetsbaarheden te verhelpen die door onderzoekers van Kaspersky waren ontdekt:

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

Deze kwetsbaarheden hebben invloed op een groot aantal Apple producten, waaronder iPhones, iPods, iPads, macOS-apparaten, Apple TV's en Apple Watches. Kaspersky heeft Apple ook op de hoogte gesteld van de uitbuiting van een hardwarefunctie, die het bedrijf vervolgens heeft gemitigeerd.

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