Een beveiligingsplatform voor duurzaamheid en digitale transformatie van industriële ondernemingen

Kaspersky Industrial CyberSecurity Platform

kaspersky BRING ON THE FUTURE

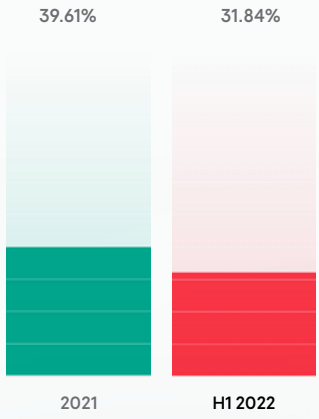
Aangevallen door malware

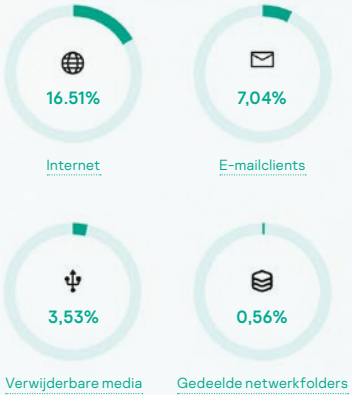
Sinds begin 2022 werd bijna 30% van de computers verwant met ICS aangevallen door malware, een verlaging van 10% ten opzichte van het voorgaande jaar

Kaspersky ICS-CERT, juni 2022

Meer informatie

Percentage van ICS-computers waarop kwaadaardige objecten werden geblokkeerd sinds begin 2022





Industriële ondernemingen hebben een andere benadering tot cyberbeveiliging in hun IT- en OT-infrastructuren (operationele technologie). De meeste ondernemingen maken binnen hun bedrijfsinfrastructuur gebruik van verouderde functies voor detectie en respons, maar voor hun OT vertrouwen deze ondernemingen vaak op verouderde en geïsoleerde methodes. Industriële ondernemingen worden steeds 'digitaler' en investeren steeds meer in slimme technologieën en automatiseringssystemen naar een digitale transformatie. Dit verkleint in werkelijkheid de traditionele leemte tussen IT- en OT-omgevingen. Een leemte die wordt gebruikt om te voorkomen dat cyberdreigingen de industriële beheersystemen binnendringen.

U bent misschien een doelwit, maar u hoeft geen slachtoffer te zijn

U hoeft geen doelwit te zijn om het slachtoffer te worden van onbedoelde inbreuken of malware-infecties. Eén USB-flashstation, mobiele telefoon, phishing-e-mail of ransomware in de ICS-omgeving kan al voldoende zijn om de kernactiviteiten van een onderneming ernstig aan te tasten. Tegelijkertijd kan een gemotiveerde hackgroep OT-netwerken binnendringen en aanzienlijke schade aanrichten aan apparatuur, processen, productie, veiligheid en kwaliteit, of waardevolle informatie stelen.

Essentiële cyberbeveiliging voor OT

Endpointbescherming

voor alleenstaande en verbonden systemen. Een veilige en geteste oplossing kan helpen om het beveiligingsbeleid af te dwingen, naleving te ondersteunen, beveiligingsaudits uit te voeren, inventaris te beheren, patching-taken uit te voeren en nauwkeurige telemetrie te verzamelen als eindpuntsensor

Netwerkbescherming

voor communicatiezichtbaarheid, detectie van dreigingen en assetbeheer. Het systeem voor netwerkverkeersanalyse en inbreukdetectie cotntroleert de doeltreffendheid van firewallinstellingen, netwerksegmentatie en naleving van het netwerkgebruik en helpt bij een veilige handmatige respons

Trainingsprogramma's

voor medewerkers om incidenten te voorkomen en de menselijke factor (menselijke fouten) te beperken.

Deskundige services

om de infrastructuur te onderzoeken, een deskundige analyse uit te voeren en de impact van een incident te beperken.

Wereldwijde erkenning

Frost & Sullivan beloonde Kaspersky met de 2020 Global Company of the Year Award op basis van een analyse van de wereldwijde industriële (OT/ICS) markt voor cyberbeveiliging.

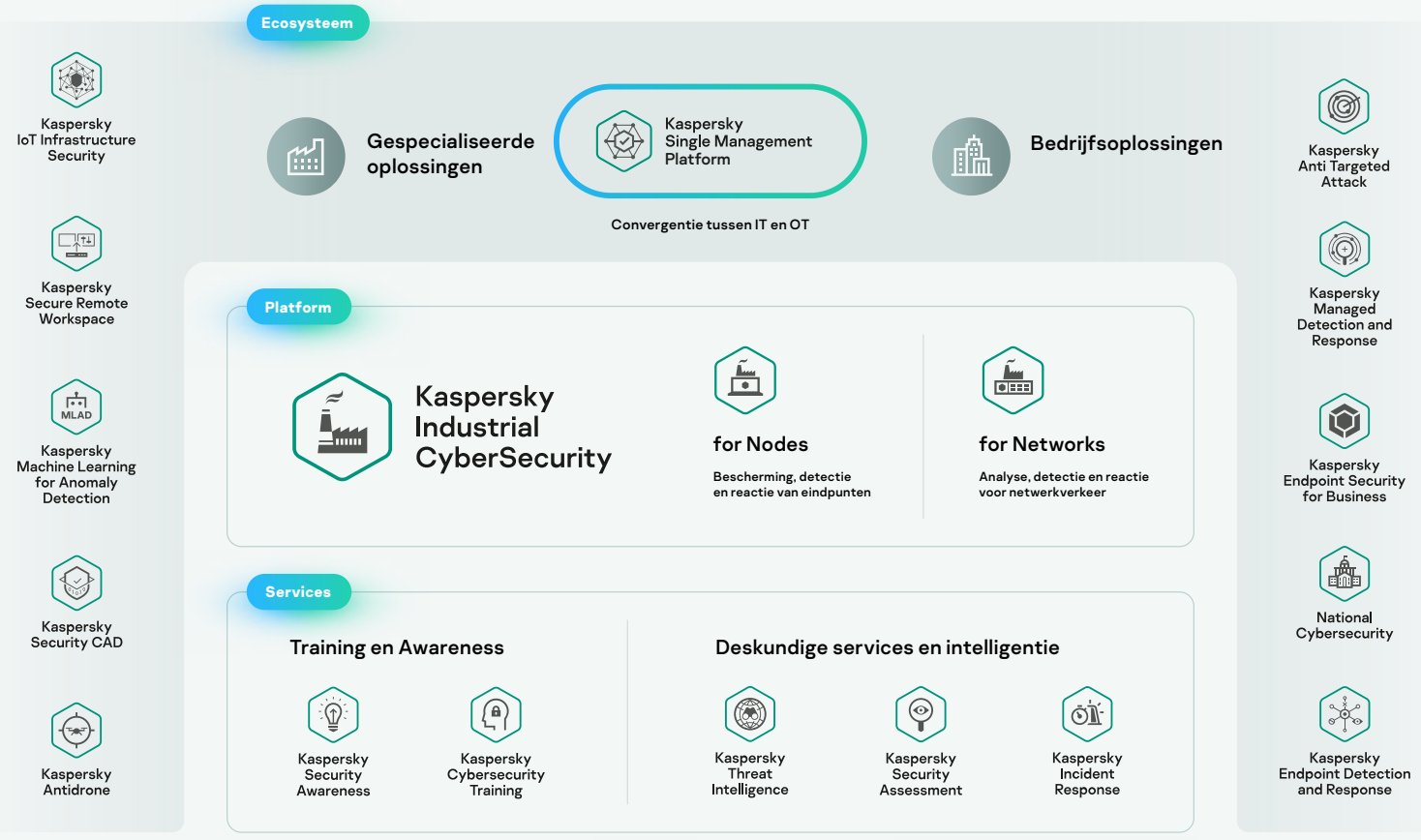
In het jaarlijkse wereldwijde onderzoek van **VDC** was Kaspersky de topleverancier in de categorie industriële cyberbeveiliging, gebaseerd op algemene beoordelingen van meer dan 250 gekwalificeerde professionals in industriële automatisering

Wat Kaspersky levert

Het Kaspersky Industrial CyberSecurity (KICS) Platform van native geïntegreerde technologieën, samen met onze portfolio deskundige trainingen en services, voorzien in alle cyberbeveiligingsbehoeften van industriële ondernemingen en operators van kritieke infrastructuur.

Het platform is een sleutelelement in een uniek ecosysteem voor industriële ondernemingen, bestaande uit:

- De beste bedrijfsoplossingen van Kaspersky, die echte convergentie tussen IT en OT leveren en de verschillende voordelen bieden van een benadering van een enkele leverancier
- De verschillende gespecialiseerde oplossingen voor fysieke cyberbeveiliging, industriële IOT-beveiliging, machine learning, veilige externe werkplaatsen etc, zorgen voor onbeperkte, flexibele schaalbaarheid



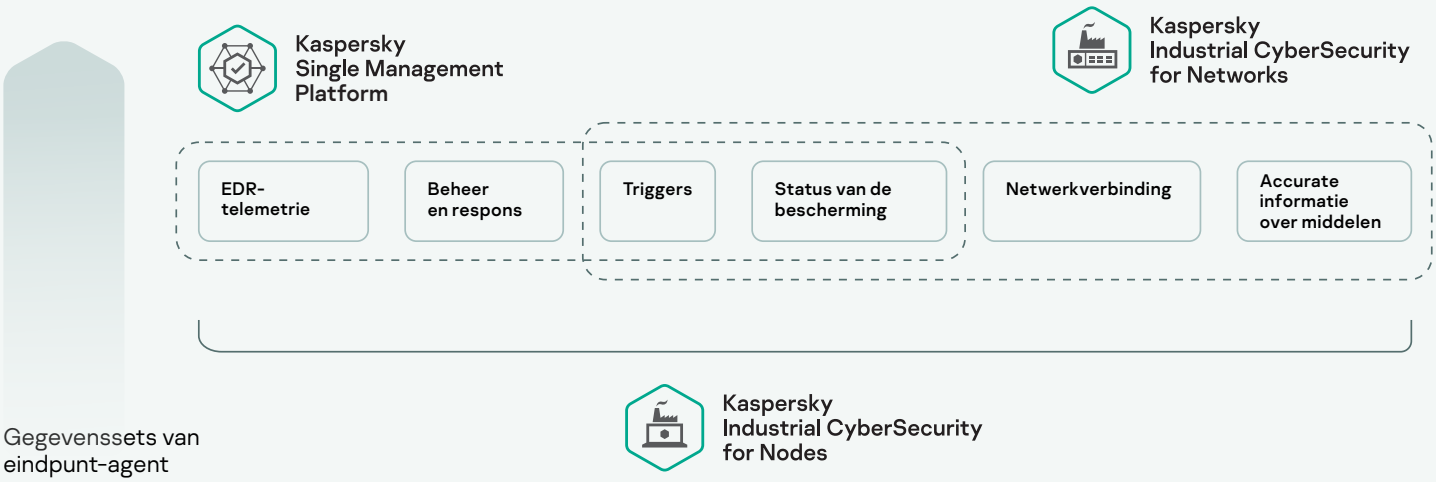
Kaspersky Industrial CyberSecurity-platform is een leider in de volgende categorieën:

- OT-eindpuntbeveiliging
- Inzicht in en overzicht van het OT-netwerk;
- Detectie van afwijkingen, respons op incidenten en rapportage;
- Beveiligingsservices voor OT

Wanneer ze samen worden gebruikt, levert dit een zicht op het grotere geheel en de bredere context voor de gebruiker: keten van incidenten op netwerk- en eindpuntniveau, nauwkeurige parameters van middelen, netwerkcommunicatie en topologiekaarten, zelfs van segmenten waar verkeersmirroring nog niet beschikbaar is en meer.

Producten

KICS is een OT-cyberbeveiligingsplatform ontworpen voor uitgebreide bescherming van de belangrijkste componenten van industriële automatisering en besturingssystemen op elk niveau. Naadloze integratie tussen platformcomponenten biedt volledige zichtbaarheid van meerdere geografisch verspreide OT-netwerken en automatiseringssystemen. Dit zorgt voor een verbeterde klantervaring, situationeel bewustzijn en implementatieflexibiliteit.



KICS for Nodes is software voor eindpuntbeveiliging, detectie en reactie met functies voor nalevingscontrole en eindpuntsensors.

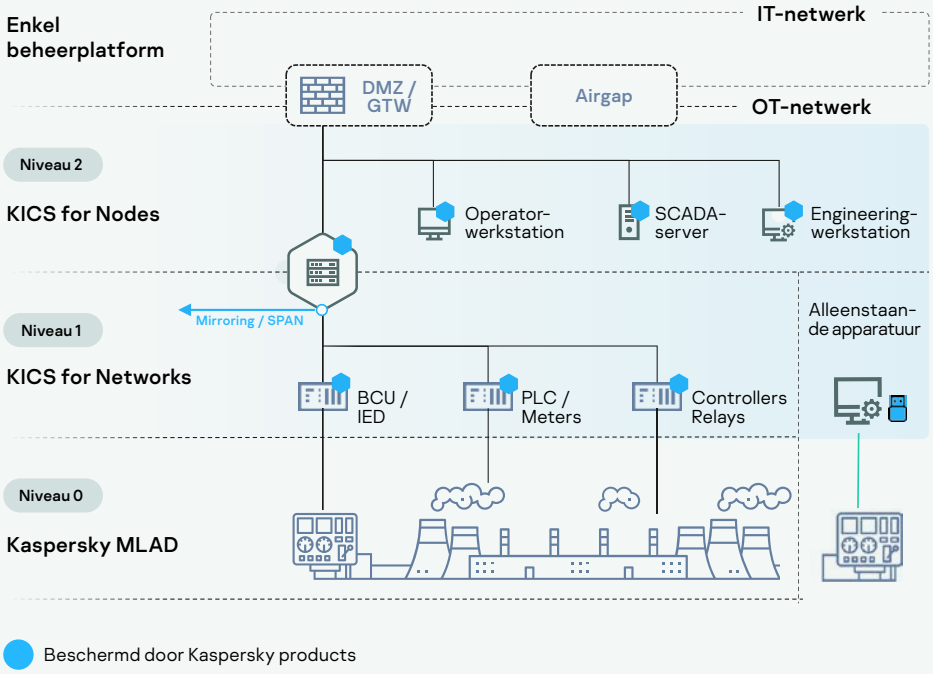
KICS for Networks is ontworpen voor analyse, detectie en respons van OT-netwerkverkeer.

Het enkele beheerplatform brengt een geavanceerde EDR-interface en snelle schaalbaarheid naar tal van locaties.

Bijkomende functies

De oplossing biedt tal van extra functies. Technologie voor de **actieve peiling** van netwerken maakt nauwkeurige verzameling mogelijk van instellingen voor netwerktopologie en middelen. De functie voor **eindpunt-audit** helpt om naleving van het beveiligingsbeleid te waarborgen, inclusief de beveiliging van de huidige instellingen en bewaking van kwetsbaarheden. Met de methode voor **draagbare scanners** van KICS for Nodes kunnen best practices worden vastgelegd voor de beveiligingsaudits van alleenstaande, onafhankelijke apparatuur. **Machine learning voor detectie van afwijkingen** is een systeem voor de vroege detectie van afwijkingen diep in het technologische proces.

Oplossingsarchitectuur



Kenmerken

Assetdetectie
Passieve OT-assetidentificatie en inventarisatie

Deep packet-inspectie
Uitgebreide inspectie van pakketten, vrijwel in realtime analyse van technische procestelemetrie

Netwerkintegriteitscontrole
Detecteert ongeautoriseerde netwerkhosts en -stromen

Intrusion Detection System
Stuurt waarschuwingen over kwaadaardige netwerkactiviteiten

Command control
Inspecteert opdrachten over industriële protocollen

Externe integratie
Flexibele API-integratie voegt detectie- en preventiemogelijkheden toe

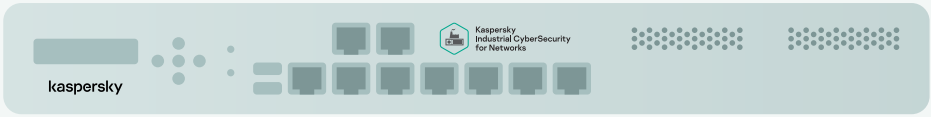
Machine learning voor de detectie van afwijkingen (MLAD)
Herkent fysieke of cybergerelateerde afwijkingen dankzij telemetrische en historische datamining in real time (herhalend neuraal netwerk)

Vulnerability Management
Een bij te werken database met kwetsbaarheden in industriële apparaten, mogelijk gemaakt door Kaspersky ICS CERT

Kaspersky Industrial CyberSecurity for Networks

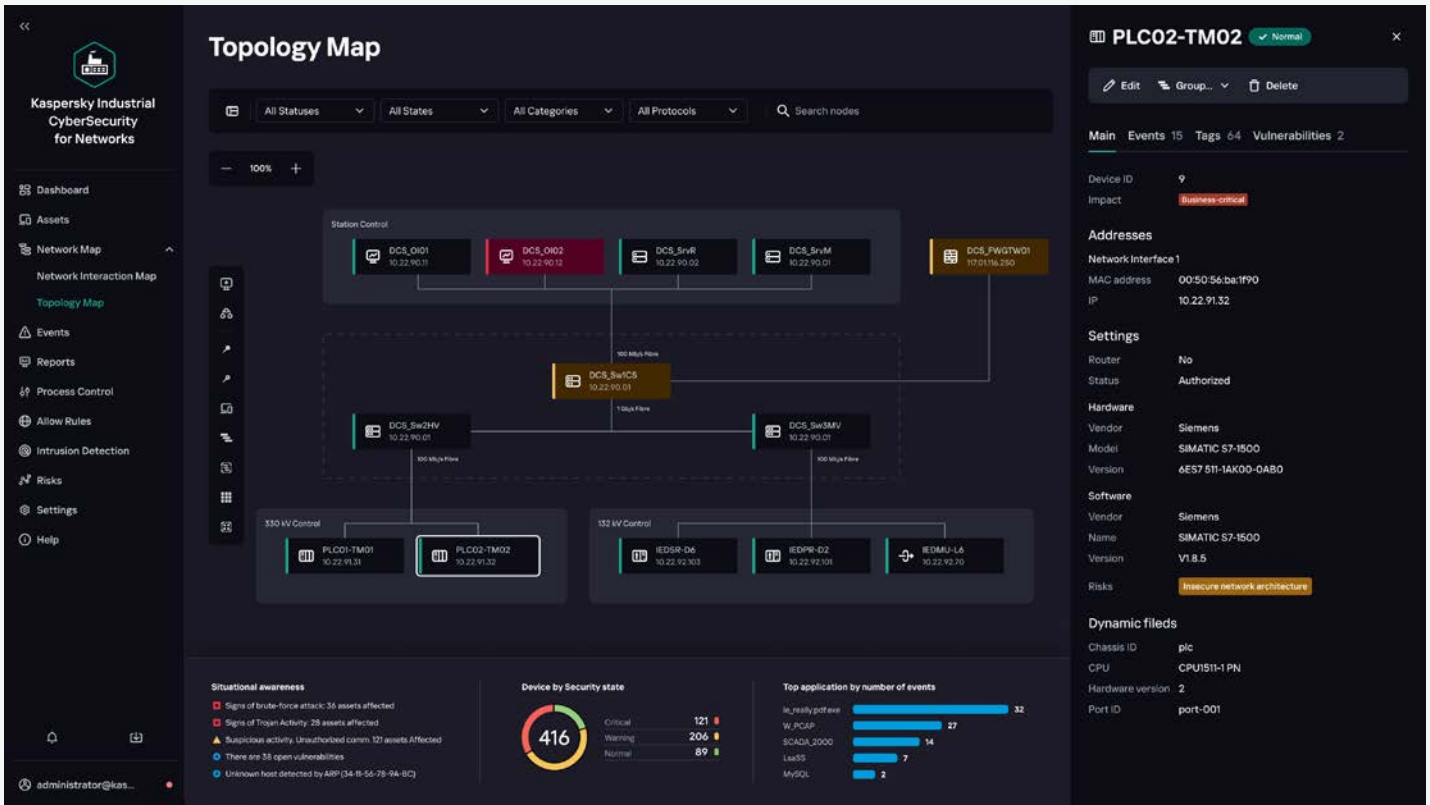
Analyse, detectie en respons voor OT-netwerkverkeer Duidelijke zichtbaarheid van risico's met passieve verkeersmonitoring, actieve peiling en eindpuntsensoren.

Detecteert afwijkingen en inbreuken binnen ICS-netwerken in vroege fasen en zorgt ervoor dat de benodigde acties worden genomen om een negatieve impact op industriële processen te voorkomen.



Apparaatonafhankelijke oplossing die snel en optimaal kan worden geïntegreerd in de gevestigde sourcing-, integratie- en garantiepraktijken van onze klanten.

Interface



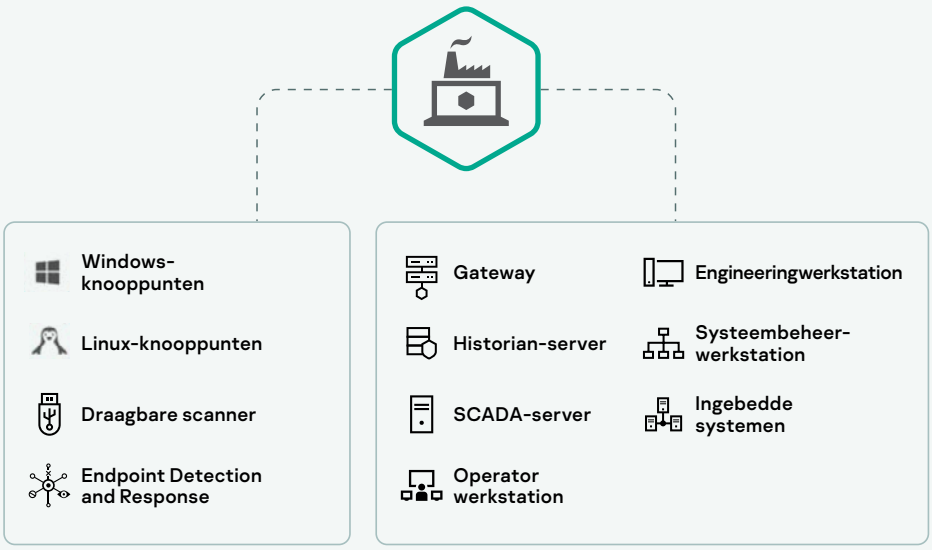
KICS for Nodes werd speciaal ontworpen voor de strikte eisen van verspreide automatiseringssystemen: gemengde en gecompliceerde omgevingen, langere gebruiksduur, alleenstaande en verbonden use-cases, bewaakte en onderhoudsvrije instanties en prioriteit van beschikbaarheid ten koste van alles

Kaspersky Industrial CyberSecurity for Nodes

Industriële, geteste en gecertificeerde bescherming, detectie en respons voor eindpunten. Een compatibele en stabiele oplossing met geringe impact voor Linux, Windows en alleenstaande systemen.

Bescherming, detectie en respons voor industriële eindpunten

Beschermt elk eindpunt van een modern, digitaal, beheerd en verspreid automatiseringssysteem. Het onthult nieuwe niveaus van zichtbaarheid van incidenten in het analyseproces van de hoofdoorzaak. De agent verzamelt telemetrie van het eindpunt om een duidelijk en gedetailleerd visueel beeld te scheppen van de voortgang van een incident op werkstations, servers, gateways en andere eindpunten. Zo kunnen beheerders van automatiseringssystemen weten dat een incident volledig is afgehandeld en zich niet meer zal herhalen.



Voordelen

Geringe impact
op beschermde apparatuur voor beste systeemprestaties

Compatibel
met computers met lage prestaties van vorige generaties en systemen van Windows XP SP2 en Windows Server 2003 SP1 en hoger

Langere levensduur
met licenties en uitgebreide ondersteuning tot 5 jaar

Volledige functionaliteit
voor alle MS Desktop, Server en Embedded Windows-besturingssystemen

Modulaire implementatie
Flexibele opties en veilige, niet-intrusieve instellingen

Voor gemengde infrastructuren
Windows, Linux en draagbare varianten

KICS for Nodes draagbare scanner
Dwingt een cyberbeveiligingsbeleid af op alleenstaande machines, automatiseringssystemen of apparatuur waarop geen beveiligingssoftware kan worden geïnstalleerd. Ultiem situationeel bewustzijn en OT-zichtbaarheid, zelfs vanuit een alleenstaande infrastructuur.

Installatievrije oplossing
KICS for Nodes kan worden geactiveerd op een aantal extra flashstations voor draagbare scanners. Dit helpt om gelijktijdige on-demand scans uit te voeren op meerdere machines tijdens onderhoudsperiodes, om eindpuntgegevens te verzamelen en deze te ordenen in een handig en overzichtelijk rapport.

Naleving van regelgeving en intern beleid
KICS for Nodes draagbare scanner voert antimalware-nalevingscontroles uit van apparatuur die toegang heeft tot een OT-site, inclusief computers van externe partijen. Het heeft een erg lage operationele voetafdruk en hindert de bestaande beveiligingsoplossingen niet.

Voordelen

Situationeel bewustzijn

Systemen / beleidsbeheer

Kill-chain en respons

Rapportage en meldingen

SIEM-integratie

HMI / MES-integratie

Kaspersky
Single Management
Platform

Het enkele beheerplatform is een gecentraliseerde oplossing voor beveiligingsbeheer voor het organiseren van de volledige OT-infrastructuur, met een kaart van alle op geografische wijze verspreide assets, aangevuld met gebeurtenissen, incidentanalyses en nog veel meer. Het verhoogt de efficiëntie van gemengde OT- en IT-beveiligingsteams. Een plek waar al uw beveiligingscontroles in harmonie samenwerken, zodat u snel en nauwkeurig kunt reageren.

Deskundige services

Ons pakket services vormt een belangrijk onderdeel van het KICS-portfolio. Wij zorgen voor de volledige cyclus van beveiligingsservices, van beoordeling van industriële cyberbeveiliging tot incidentrespons.

Industriële cyberbeveiliging

Beoordeling van industriële cyberbeveiliging: Kaspersky biedt een beoordeling van industriële cyberbeveiliging met minimale overlast, waaronder een test voor interne en externe binnendringing, beoordeling van OT-beveiliging en een beoordeling van de beveiliging van de automatiseringsoplossing. Experts van Kaspersky bieden waardevol inzicht in de infrastructuur van de onderneming en geven aanbevelingen voor het versterken van de ICS-cyberbeveiliging.

Dreigingsinformatie

Up-to-date analyses verzameld door experts van Kaspersky helpen de bescherming van klanten tegen doelgerichte industriële cyberaanvallen te verbeteren. Geleverd als IT-feeds of op maat gemaakte rapporten die aan de behoeften van de klant voldoen op basis van regionale, industriële en ICS-softwareparameters.

Afhandeling van incidenten

In geval van een incident verzamelen en analyseren Kaspersky-experts gegevens en malware. Ze reconstrueren de tijdlijn van het incident, bepalen mogelijke bronnen en oorzaken en ontwikkelen een gedetailleerd herstelplan. Dit plan omvat aanbevelingen voor het verwijderen van malware van de systemen van de klant en het omkeren van kwaadaardige acties.

> In tegenstelling tot andere leveranciers heeft Kaspersky ervaring met het ICS-cyberbeveiligingsdomein, een uitgebreide oplossing en een professionele werkwijze. Het product biedt ons enorme toegevoegde waarde en een zorgeloze toekomst wat betreft de beveiligingsstrategie van onze onderneming.
>
> Ondřej Sýkora,
> C&A manager, Plzeňský Prazdroj

> Door de opdracht uit te voeren en te leren van de experts van het Kaspersky-team, hebben we onze bescherming tegen cyberdreigingen kunnen verbeteren.
>
> Yu Tat Ming,
> CEO, PacificLight

Training en bewustwording

> Kaspersky was het beste bedrijf om professionele vaardigheidstraining op het gebied van industriële cybersecurity te leveren voor onze ICS-groep.
>
> Søren Egede Knudsen,
> Chief Technical Officer

Bewustwordingstraining voor industriële cyberbeveiliging

Interactieve training en games over cyberbeveiliging, op locatie en online, voor medewerkers die werken met industriële computersystemen en hun managers. Deelnemers krijgen nieuwe inzichten in de huidige dreigingen en verspreidingsmechanismen die zich specifiek richten op industriële omgevingen, gaan aan de slag met praktijkgerichte scenario's en ontwikkelen vaardigheden in cyberbeveiliging.

Deskundige traningsprogramma's

Trainingen in ICS Penetration Testing en ICS Digital Forensics zijn bedoeld voor professionals in cyberbeveiliging. Deelnemers ontwikkelen geavanceerde vaardigheden die benodigd zijn om uitgebreide pentests of digitale forensische analyses uit te voeren in industriële omgevingen.

Gespecialiseerde ecosystemen voor oplossingen

Kaspersky IoT Infrastructure Security

Beschermt het Internet of Things op gatewayniveau op basis van de Cyber Immunity-benadering van Kaspersky

Meer informatie

Kaspersky Antidrone

Beschermt het luchtruim tegen drones bij faciliteiten van elke omvang

Meer informatie

Kaspersky Secure Remote Workspace

Functionele thin client-infrastructuur met Cyber Immunity

Meer informatie

Kaspersky Security CAD

Digitale modellering van informatiebeveiligingssystemen voor ontwerp- en exploitatiefasen

Meer informatie

Kaspersky Machine Learning for Anomaly Detection

Systeem voor vroege detectie van afwijkingen in industriële technologische processen

Meer informatie

www.kaspersky.com

Kaspersky Industrial CyberSecurity

Meer informatie