Zukunftsorientierte
Sicherheit für
Industrieunternehmen

Kaspersky Industrial CyberSecurity Platform

kaspersky BRING ON THE FUTURE

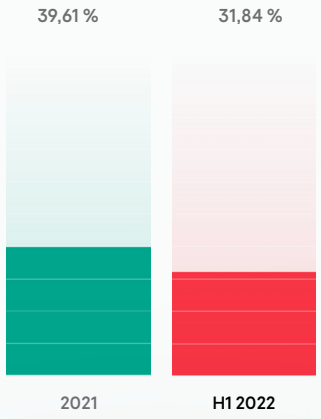
Malware-Angriffe

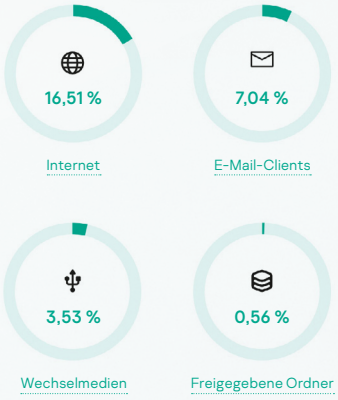
Seit Anfang 2022 wurden fast 30 % der ICS-Computer mit Malware infiziert – fast 10 % weniger als im Vorjahr

Kaspersky ICS-CERT, Juni 2022

Weitere informationen

Prozentsatz der ICS-Computer, auf denen schädliche Objekte seit Anfang 2022 blockiert wurden





Industrieunternehmen gehen Cybersicherheit in ihren IT- und OT-Infrastrukturen unterschiedlich an. Zwar haben die meisten Unternehmen bereits ausgereifte Erkennungs- und Reaktionsmaßnahmen in ihren Unternehmensnetzwerken implementiert – doch wenn es um OT geht, setzen sie normalerweise auf einen veralteten Air Gap-Ansatz. Industriebetriebe werden zunehmend „digitaler" und investieren immer mehr in intelligente Technik, neue Automatisierungssysteme und die digitale Transformation. Dadurch entfällt die Kluft zwischen IT- und OT-Umgebungen – eine Lücke, die bisher verhinderte, dass Cyberbedrohungen industrielle Automatisierungs- und Steuerungssysteme erreichen.

Sie können ein Ziel sein – aber werden Sie nicht zum Opfer

Sie müssen kein Ziel sein, um Opfer von versehentlichen Air Gap-Einbrüchen oder einer Malware-Infektion zu werden. Schon ein einziges Flash-Laufwerk, Mobiltelefon, eine Phishing-E-Mail oder Ransomware kann verheerende Folgen haben. Gleichzeitig kann eine motivierte Hacking-Gruppe in OT-Netzwerke eindringen und erheblichen Schaden an Ausrüstung, Prozessen, Produktion, Sicherheit und Qualität verursachen, oder Informationen stehlen.

Essentielle Cybersicherheit für OT

Schutz von Endpoints

für Standalone- und vernetzte Systeme. Eine sichere und bewährte Lösung sollte dabei helfen, Sicherheitsrichtlinien durchzusetzen, Compliance zu unterstützen, Sicherheitsaudits durchzuführen, Inventar zu verwalten, Patching-Aufgaben durchzuführen und als Endpoint-Sensor präzise Telemetrie zu sammeln

Netzwerkschutz

für Kommunikationstransparenz, Bedrohungserkennung und Asset Management. Das Network Traffic Analysis and Intrusion Detection System steuert die Wirksamkeit der Firewall-Einstellungen, die Netzwerksegmentierung sowie die Einhaltung der Netzwerknutzung und hilft, eine sichere manuelle Reaktion zu gewährleisten

Schulungsprogramme

Machen Sie Ihre Mitarbeiter zur ersten Verteidigungslinie im Unternehmen

Expert Services

Wir helfen Ihnen dabei, Ihre Infrastruktur zu analysieren oder die Auswirkungen eines Vorfalls zu verringern

Weltweite Anerkennung

Frost and Sullivan zeichnete Kaspersky auf der Grundlage einer Analyse des globalen Marktes rund um industrielle (OT/ICS) Cybersicherheit mit dem Global Company of the Year Award 2020 aus

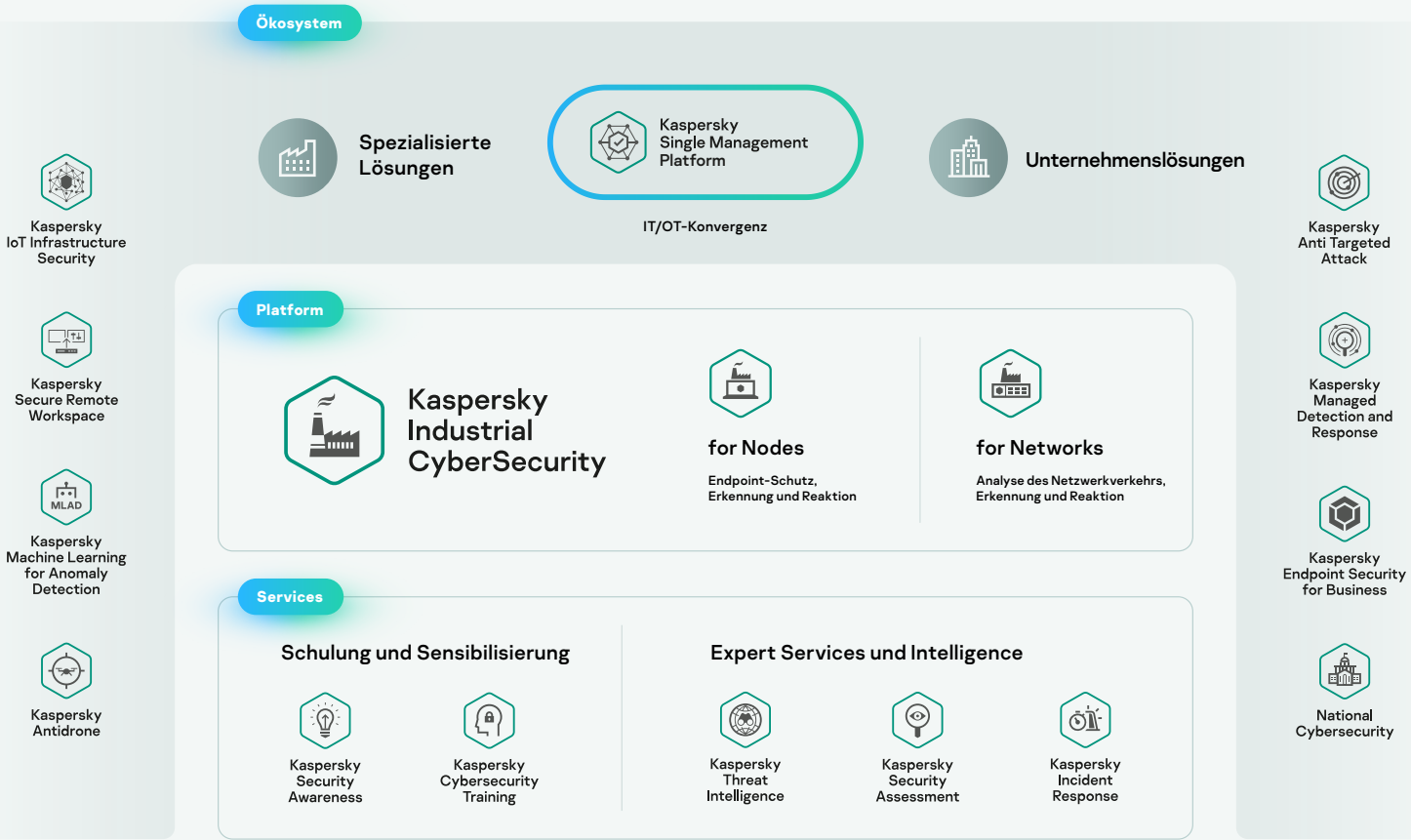
In der jährlichen globalen Umfrage von **VDC** ging Kaspersky als der beste Anbieter in der Kategorie industrielle Cybersicherheit hervor. Die Ergebnisse basieren auf Gesamtbewertungen von über 250 Fachleuten aus dem Bereich Industrieautomatisierung

Angebote von Kaspersky

Die Kaspersky Industrial CyberSecurity (KICS) Platform umfasst nativ integrierte Technologien, Expertenschulungen und Dienstleistungen. So können alle Cybersicherheitsanforderungen von Industrieunternehmen und Betreibern kritischer Infrastrukturen abgedeckt werden.

Die Plattform ist ein Schlüsselelement in einem einzigartigen Ökosystem für Industrieunternehmen, die Folgendes umfasst:

- Die leistungsstarken Unternehmenslösungen von Kaspersky, die IT/OT-Konvergenz und Sicherheit aus einer Hand bieten
- Verschiedene spezialisierte Lösungen für Cyber-Physical Security, industrielle IoT-Sicherheit, maschinelles Lernen, sichere Remote-Arbeitsbereiche und vieles mehr bieten agile Skalierbarkeit



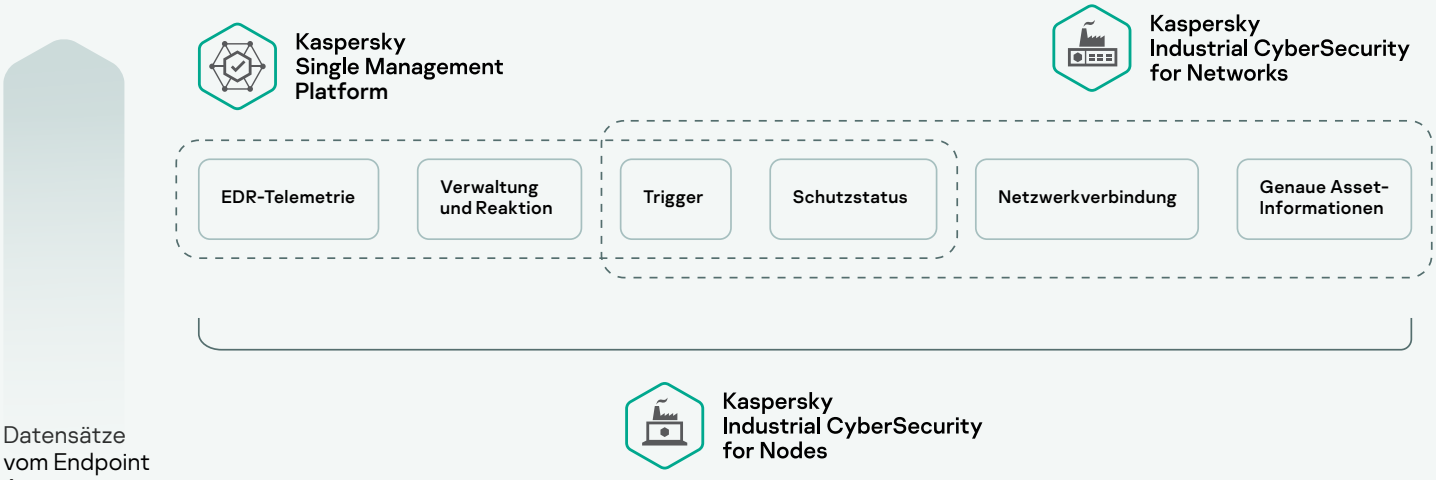
Die Kaspersky Industrial CyberSecurity Platform wird als führender Anbieter in folgenden Kategorien genannt

- OT-Endpoint Security
- OT-Netzwerküberwachung und -transparenz
- Erkennung von Anomalien, Incident Response und Reporting
- OT-Security Services

Bei gemeinsamer Nutzung erhält der Benutzer ein Gesamtbild und den breiteren Kontext: die Kette von Vorfällen auf Netzwerk- und Endpoint-Ebene, präzise Asset-Parameter, Netzwerkkommunikation und eine topografische Karte – sogar von Segmenten, in denen noch kein Traffic Mirroring verfügbar ist.

Produkte

KICS ist eine OT-Cybersicherheitsplattform, die für den umfassenden Schutz von Kernkomponenten des industriellen Automatisierungs- und Steuerungssystems auf allen Ebenen entwickelt wurde. Die nahtlose Integration zwischen Plattform-Komponenten bietet vollständige Sichtbarkeit mehrerer geografisch verteilter OT-Netzwerke und Automatisierungssysteme. Zudem sorgt sie für ein verbessertes Kundenerlebnis, Situationsbewusstsein und Bereitstellungsflexibilität.



KICS for Nodes bietet neben Endpoint Security auch Detection and Response. Kunden profitieren zudem von Compliance Audit- und Endpoint Sensor-Funktionalitäten.

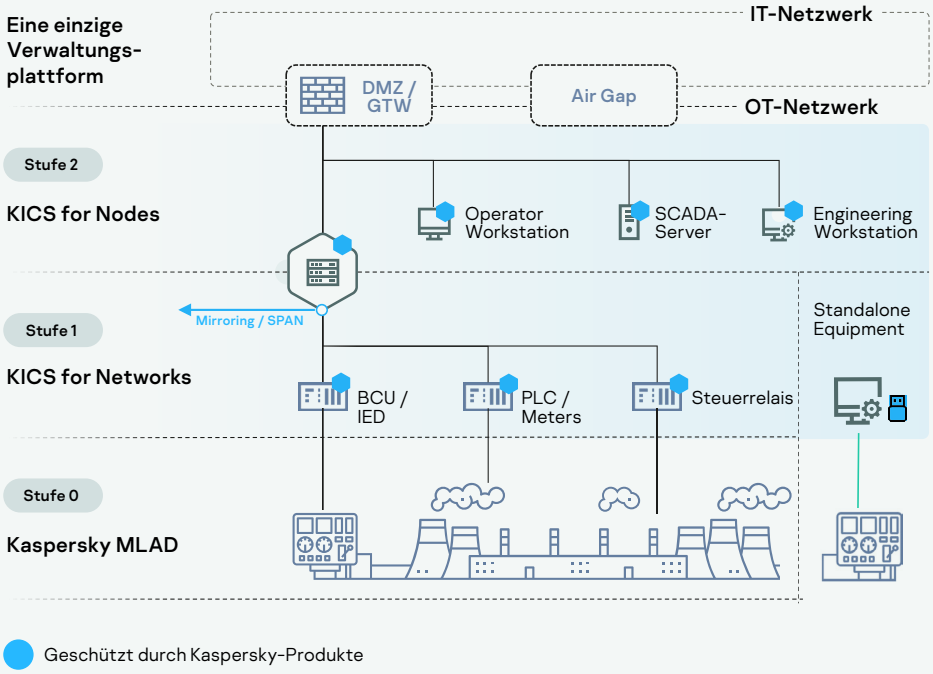
KICS for Networks wurde für die Analyse, Erkennung und Reaktion von OT-Netzwerkverkehr entwickelt.

Die Verwaltungsplattform bietet eine fortschrittliche EDR-Schnittstelle und schnelle Skalierbarkeit für zahlreiche Standorte.

Zusätzliche Funktionen

Die Lösung bietet zahlreiche Zusatzfunktionen. Die Technologie von Network **Active Polling** ermöglicht eine schnelle und präzise Erfassung der Netzwerktopologie und der Asset-Einstellungen. Die Funktion **Endpoint Audit** trägt dazu bei, die Einhaltung der Sicherheitsrichtlinien zu gewährleisten. Dazu gehört die Absicherung aktueller Einstellungen und die Kontrolle von Sicherheitslücken. Die Bereitstellungsmethode **Portable Scanner** von KICS for Nodes hilft, Best Practices von Standalone, Air Gap-Equipment und icherheitsaudits zu etablieren. **Machine Learning for Anomaly Detection** ist ein System zur Echtzeiterkennung von Anomalien, das tief im technologischen Prozess verankert ist.

Die Lösungsarchitektur



Funktionen

Asset Discovery
Identifikation und Bestandsaufnahme passiver OT Assets

Deep Packet Inspection
Analyse der Telemetrie technischer Prozesse – nahezu in Echtzeit

Netzwerkintegritätskontrolle
Erkennt unbefugte Netzwerkhosts und Flows

Intrusion Detection System
Sendet Warnungen über schädliche Netzwerkaktivitäten

Befehlssteuerung
Prüft Befehle über Industrieprotokolle

Externe Integration
Die flexible API-Integration fügt Erkennungs- und Präventionsfunktionen hinzu

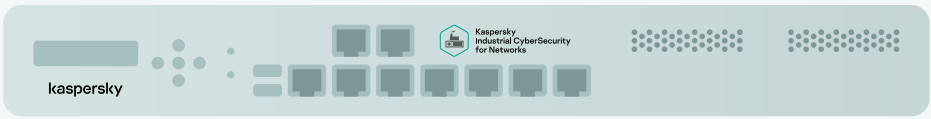
Machine Learning for Anomaly Detection (MLAD)
Erkennt Cyber-Anomalien oder Anomalien physischer Natur über Telemetrie in Echtzeit und über historisches Data-Mining (Rekurrentes neuronales Netz)

Vulnerability Management
Aktualisierbare Datenbank der Schwachstellen in Industrieanlagen, angereichert von Kaspersky ICS CERT

Kaspersky Industrial CyberSecurity for Networks

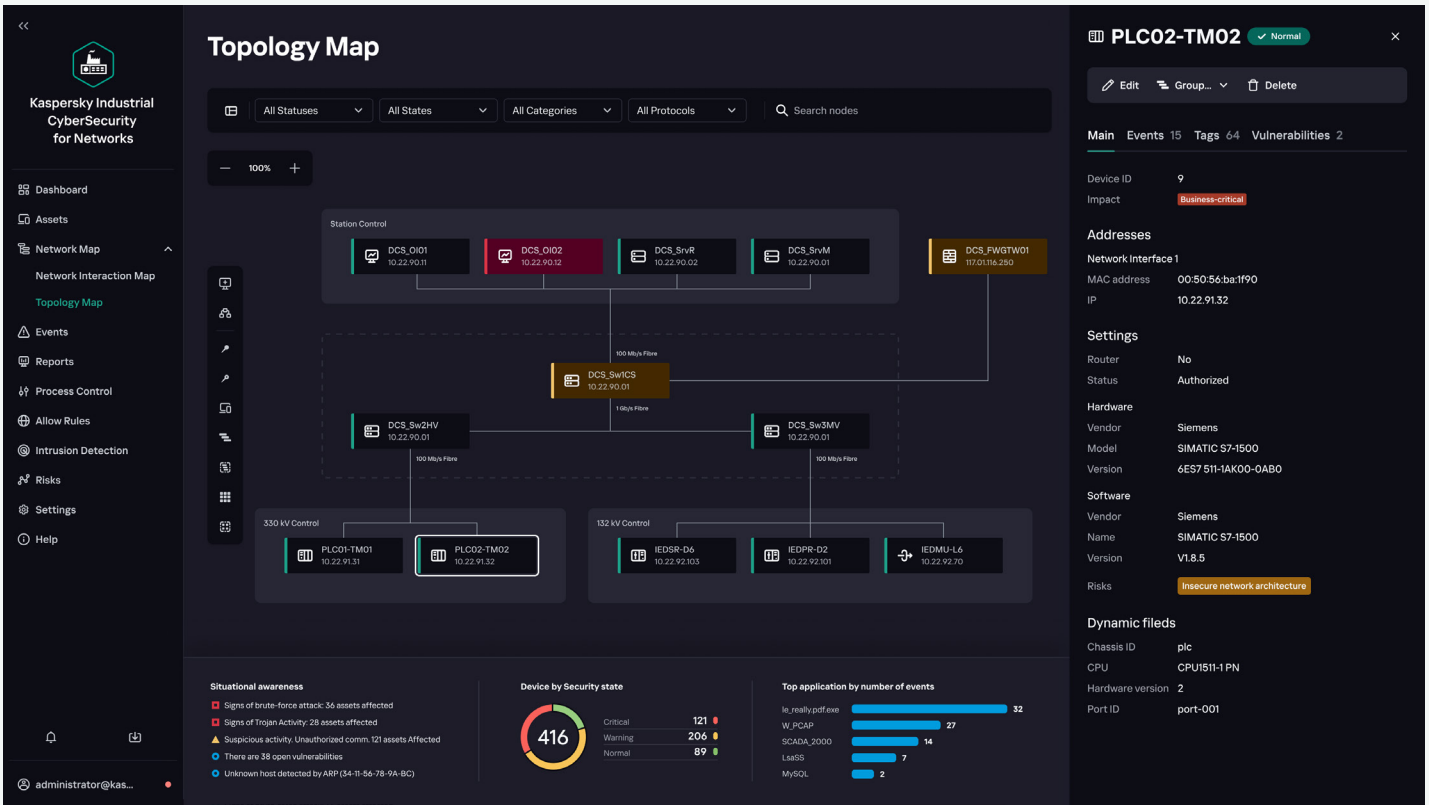
Analyse, Erkennung und Reaktion des OT-Netzwerkverkehrs. Klare Risikotransparenz mit passiver Verkehrsüberwachung, aktivem Polling und Endpoint-Sensoren.

Erkennt Anomalien und Eindringversuche in ICS-Netzwerken in ihren frühen Phasen und sorgt für notwendige Maßnahmen. So können Beeinträchtigungen der industriellen Prozesse verhindert werden.



Die Plattform-unabhängige Lösung lässt sich schnell in die etablierten Sourcing-, Integrations- und Gewährleistungspraktiken integrieren.

Benutzeroberfläche



KICS for Nodes wurde speziell für die strengen Anforderungen verteilter Automatisierungssysteme entwickelt: gemischte und komplexe Umgebungen, lange Betriebszeiten, eigenständige und verbundene Anwendungsfälle, beaufsichtigte und wartungsfreie Instanzen und Priorität der Kontrollverfügbarkeit

Kaspersky Industrial CyberSecurity for Nodes

Bewährte Endpoint Protection, Detection and Response auf Industrie-Ebene. Eine ressourcenschonende und leistungsstarke Lösung für Linux, Windows und Standalone-Systeme.

Industrial Endpoint Protection, Detection and Response

Schützt jeden Endpoint eines modernen, digitalen, verwalteten und verteilten Automatisierungssystems. Die Lösung ermöglicht umfassende Sichtbarkeit von Vorfällen während der Ursachenanalyse. Der Agent sammelt die Endpoint-Telemetriedaten, um eine klare und detaillierte visuelle Darstellung des Fortschritts eines Vorfalls auf Workstations, Servern, Gateways und anderen Endpoints zu erstellen. So kann sichergestellt werden, dass ein Vorfall vollständig behandelt worden ist und sich nicht wiederholt.

Vorteile

Geringe Auswirkung
auf dem geschützten Gerät für die beste Systemleistung

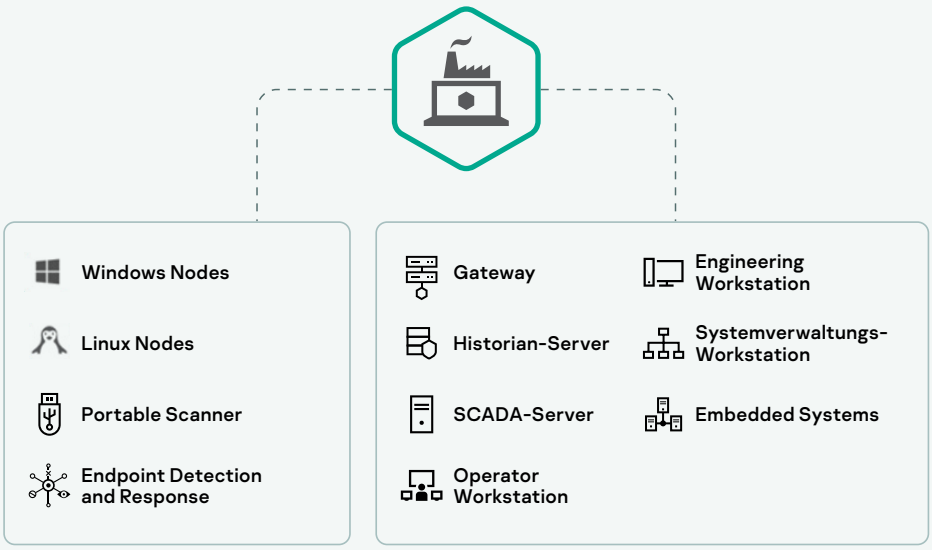
Kompatibilität
mit leistungsschwachen, älteren Computern und Systemen ab Windows XP SP2 und Windows Server 2003 SP1 und höher

Verlängerter Lebenszyklus
bis zu 5 weitere Jahre und erweiterter Support

Volle Funktionalität
für alle MS Desktops, Server und eingebettete Windows-Betriebssysteme

Modulare Bereitstellung
Flexible Optionen und sichere Einstellungen

Deckt gemischte Infrastrukturen ab
Windows-, Linux- und Portable-Varianten



KICS for Nodes Portable Scanner
Setzt eine Cybersicherheitsrichtlinie auf Standalone-Maschinen, Automatisierungssystemen oder Geräten durch, auf denen keine Sicherheitssoftware installiert werden kann. Situationsbewusstsein und OT-Sichtbarkeit – selbst bei eigenständigen Infrastrukturen

Installationsfreie Lösung
KICS for Nodes kann auf einer Reihe zusätzlicher Flash-Laufwerke aktiviert werden. Dies ermöglicht, gleichzeitige On-Demand-Scans auf mehreren Computern während Wartungsfenstern durchzuführen, Endpoint-Daten zu sammeln und sie in einem Bericht zusammenzufassen.

Erfüllung gesetzlicher Auflagen und interner Richtlinien
Der KICS for Nodes Portable Scanner führt Anti-Malware-Compliance-Checks von Geräten durch, die auf einen OT-Standort zugreifen, einschließlich Computern von Drittanbietern. Weder der Geschäftsbetrieb noch andere Sicherheitslösungen werden dadurch beeinträchtigt.

Vorteile

Erkennen der Lage

Systeme / Richtlinienverwaltung

Kill-Chain und Reaktion

Reporting und Benachrichtigung

SIEM-Integration

HMI / MES Integration

Kaspersky Single Management Platform

Die Single Management Platform ist eine zentralisierte Sicherheitsmanagementlösung für die Sicherheitsorchestrierung der gesamten OT-Infrastruktur. Sie liefert eine Übersicht aller geografisch verteilten Assets, angereichert mit Ereignissen, Vorfallsanalysen und mehr. Die Plattform steigert die Effizienz gemischter OT- und IT-Sicherheitsteams erheblich. So arbeiten all Ihre Sicherheitskontrollen im Einklang und ermöglichen eine schnelle und effektive Reaktion.

> Die umfassende Expertise, Professionalität und Leistungsfähigkeit der Lösung konnten im Hersteller-Vergleich klar überzeugen. So konnten wir unsere Sicherheitsstrategie weiter optimieren.
>
> Ondřej Sýkora,
> C&A Manager, Pilsner Urquell

> Dank des Assessments und der Expertise des Kaspersky-Teams konnten wir unseren Schutz gegen Cyberbedrohungen nachhaltig verbessern.
>
> Yu Tat Ming,
> CEO, PacificLight

Expert Services

Unsere Services bilden einen zentralen Teil des KICS-Portfolios. Wir bieten den gesamten Zyklus von Sicherheitsdiensten: von Assessments bis hin zur Vorfallsreaktion.

Industrial Cybersecurity Assessment

Industrial Cybersecurity Assessment: Kaspersky bietet eine minimal invasive Bewertung der industriellen Cybersicherheit mit internem und externem Penetration Testing, Bewertung der OT Security und der Sicherheit der Automatisierungslösung. Die Kaspersky-Experten liefern wichtige Erkenntnisse über die Infrastruktur eines Unternehmens und geben Empfehlungen zur Verbesserung der ICS-Cybersicherheit ab.

Threat Intelligence

Aktuelle, von Kaspersky-Experten erarbeitete Analysen helfen dabei, den Schutz vor zielgerichteten Cyberangriffen zu optimieren. Die Bereitstellung erfolgt in Form von TI-Feeds oder maßgeschneiderten Berichten, die spezielle Kundenanforderungen gemäß regionalen, branchenspezifischen und ICS-Software-Parametern erfüllen.

Incident Response

Bei einem Vorfall sammeln und analysieren Kaspersky-Experten Daten und Malware, rekonstruieren den zeitlichen Ablauf, ermitteln mögliche Quellen und Beweggründe und entwickeln einen detaillierten Behebungsplan. Der Plan umfasst Empfehlungen zum Entfernen von Malware aus den Systemen und zum Zurücksetzen böswilligen Handlungen.

> Kaspersky war am besten geeignet, um unserer ICS-Gruppe professionelle Industrial Cybersecurity-Schulungen bereitzustellen.
>
> Søren Egede Knudsen, Technischer Leiter

Schulung und Sensibilisierung

Industrial CyberSecurity Awareness Training

Interaktive Schulungsmodule und Spiele rund um das Thema Cybersicherheit – vor Ort und online, für Bedienpersonal und ihre Vorgesetzten. Die Teilnehmer erhalten neue Einblicke in die aktuelle Bedrohungslandschaft und Angriffsvektoren, die auf Industrieumgebungen abzielen. Es werden praxisnahe Szenarien durchgearbeitet und Kenntnisse rund um Cybersicherheit erworben.

Expert Training

Die Kurse ICS Penetration Testing und ICS Digital Forensics richten sich an Cybersicherheitsexperten. Die Teilnehmer erwerben alle erforderliche Fähigkeiten zur Durchführung umfangreicher Pentests oder digitaler Forensik in Industrieumgebungen.

Spezialisierte Lösungen

Kaspersky IoT Infrastructure Security

Gewährleistet IoT-Schutz auf Gateway-Ebene basierend auf dem Cyber Immunity-Ansatz von Kaspersky

Mehr erfahren

Kaspersky Antidrone

Schützt den Luftraum vor Drohnen in Einrichtungen jeder Größe

Mehr erfahren

Kaspersky Secure Remote Workspace

Funktionale Thin Client Infrastruktur mit Cyber Immunity

Mehr erfahren

Kaspersky Security CAD

Digitale Modellerstellung von Informationssicherheitssystemen für Design- und Betriebsphasen

Mehr erfahren

Kaspersky Machine Learning for Anomaly Detection

System zur Echtzeiterkennung von Anomalien in industriellen technologischen Prozessen

Mehr erfahren

www.kaspersky.de

Kaspersky Industrial CyberSecurity

Mehr erfahren