

Kaspersky OT CyberSecurity

Eine Komplettlösung für ausfallsichere
cyber-physische Systeme





Kaspersky OT CyberSecurity

Resilienz durch Expertise



Industrietechnologie

Robuste Sicherheitslösungen für die Industrie – getestet, compliant und zertifiziert



Praktisches Wissen

Zuverlässige Bedrohungsanalysen und umfassende Schulungen zur Cybersicherheit für Industrieunternehmen



Praxiserfahrung

Ein umfassendes Angebot an professionellen Dienstleistungen für eine robuste und ganzheitliche Cybersicherheit



Kaspersky Next
XDR Expert

IT-OT-Konvergenz

IT XDR

Technologien

Spezialisierte Lösungen



Kaspersky
Antidrone



Kaspersky
Machine Learning
for Anomaly Detection



Kaspersky
SD-WAN



Kaspersky
Industrial
CyberSecurity

Native OT XDR



for Nodes

Endpoint-Schutz,
Erkennung und Reaktion



for Networks

Analyse des
Netzwerkverkehrs,
Erkennung und Reaktion

Kaspersky OS-Lösungen



Kaspersky
Thin Client



Kaspersky
Automotive
Secure Gateway

Wissen

Cyberhygiene



Kaspersky
Security
Awareness

Threat Intelligence



Kaspersky
ICS Threat
Intelligence

Training



Kaspersky
ICS CERT
Training

Expertise

Erkennung



Kaspersky
ICS Security
Assessment

Reaktion



Kaspersky
Incident
Response

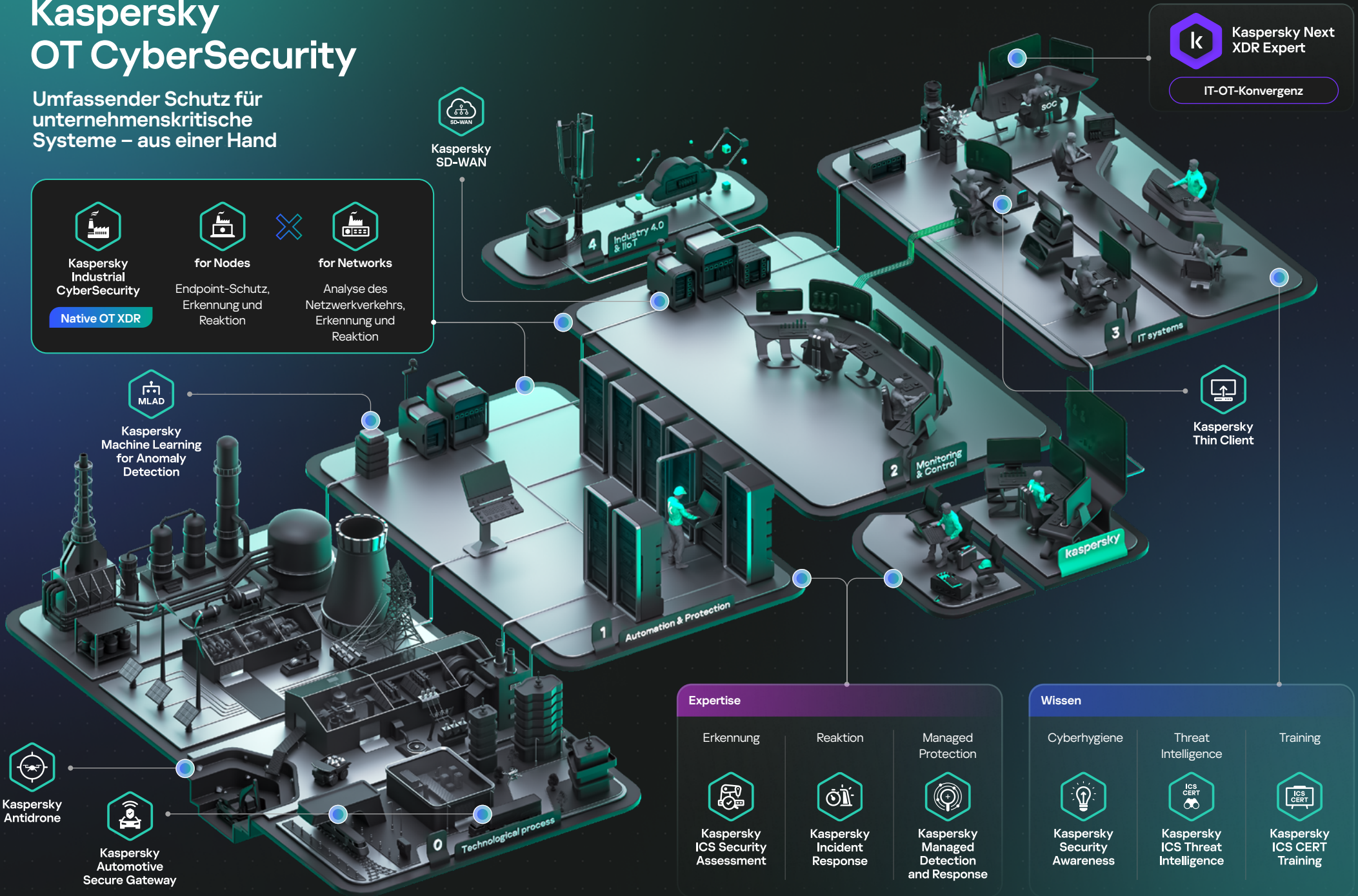
Managed Protection



Kaspersky
Managed
Detection
and Response

Kaspersky OT CyberSecurity

Umfassender Schutz für unternehmenskritische Systeme – aus einer Hand





Kaspersky Industrial CyberSecurity

360°-Transparenz und volle Kontrolle über potenzielle Risiken

- **Bestandsaufnahme von Assets und Netzwerktransparenz:** Alle angeschlossenen Geräte und deren Konfigurationen nachverfolgen. Erstellen Sie ein Netzwerkdiagramm und analysieren Sie die Datenflüsse.
- **Neutralisierung von Bedrohungen:** Identifizieren und minimieren Sie Bedrohungen über Hosts und Netzwerke hinweg. Gewinnen Sie Einblicke in Ursachen und sichere Gegenmaßnahmen.
- **Risikobewertung:** Bewerten Sie Schwachstellen und überwachen Sie Änderungen an den Sicherheitseinstellungen für Hosts, Netzwerkgeräte und Controller.

Wichtigste Vorteile



Geprüfte und bewährte Kompatibilität mit über 200 industriellen Automatisierungssystemen und -geräten



Die nahtlos integrierte OT-XDR-Plattform wurde speziell für kritische Infrastrukturen entwickelt und bewältigt zahlreiche Herausforderungen.



Eine Lösung mit geringem Ressourcenbedarf, die weder die Systemleistung noch die Prozesskontinuität beeinträchtigt



KICS und seine Kerntechnologien werden branchenführenden Audits unterzogen



ISA/IEC 62443-4-1



SOC 2 Type 2



ISO/IEC 27001



GB 42250-2022



Kaspersky Next XDR Expert

Umfassender Schutz für alle industriellen und firmeninternen Bereiche Ihres Unternehmens

Die enge Integration mit Kaspersky Next XDR Expert eröffnet der Kaspersky Industrial CyberSecurity-Plattform neue Anwendungsszenarien. Dazu gehört die Interaktion mit Lösungen von Drittanbietern sowie erweiterte Ermittlungs- und Reaktionsfunktionen. Die Integration trägt dazu bei, Ihr Unternehmen an der Schnittstelle zwischen Industrie und Unternehmenswelt zu schützen.

Sicherheitsteams erhalten einen umfassenden Überblick über den Verlauf eines Vorfalls und identifizieren die Ursachen, um ähnliche Vorfälle in Zukunft zu verhindern.

Wichtigste Vorteile



Sicherheit und Datenhoheit für konvergierte, ressourcenintensive IT/OT/IoT-Infrastrukturen



Die native Interoperabilität innerhalb des Kaspersky-Produktportfolios erlaubt eine besonders nahtlose Integration

Datenquellen

Kaspersky-Lösungen

Drittanbieter

xFlows

Ereignisse

Integrationen



**Kaspersky
Anti Targeted
Attack**
NDR Enhanced



**Kaspersky
Threat Intelligence**



**Kaspersky
Managed Detection
and Response**

Daten

Response

und weitere Integrationen
von Kaspersky oder
Drittanbietern auf Anfrage

Kaspersky Next XDR Expert

Open Single Management Platform

Endpoint Detection
and Response

Untersuchungs-
Diagramm

Erkennung von
Bedrohungen und
Kreuzkorrelation

Protokollverwaltung
und Datenspeicher

Dashboards
und Berichte

Playbooks

Fallmanagement

Zentralisiertes
Asset
Management

Drittanbieteran-
bindung

Deployment
Toolkit

Daten

Response

EDR mit Sandbox, E-Mail- und Hybrid Security

Security Awareness, Sandbox, E-Mail-
und Hybrid Cloud Security



**Kaspersky
Automated Security
Awareness Platform**



**Kaspersky
Security for
Mail Server**



**Kaspersky
Hybrid Cloud
Security**



**Kaspersky
Sandbox**



Kaspersky Machine Learning for Anomaly Detection

Frühzeitige Erkennung von Anomalien und vorausschauende Analysen

- Erkennt Gerätefehler und menschliches Versagen, lange bevor sie kritische Ausmaße annehmen, und trägt so dazu bei, Ausfälle und Unfälle zu verhindern.
- Erkennt ungewöhnliche Handlungen von Mitarbeitern oder Vorgänge an Geräten, die auf einen gezielten Angriff oder Sabotage hindeuten könnten.
- Erkennt komplexe Anomalien in cyber-physischen Systemen anhand geringfügiger Abweichungen mehrerer Prozessparameter.

Integration in externe Systeme



Kaspersky MLAD empfängt Prozessdaten von KICS für Netzwerke, industrielle Automatisierungssysteme und IoT-/IIoT-Geräte



Der MLAD-Ereignisprozessor tauscht CEF-Nachrichten mit externen Quellen aus. Dazu zählen SIEM-Systeme, IIoT- und Netzwerkgeräte.



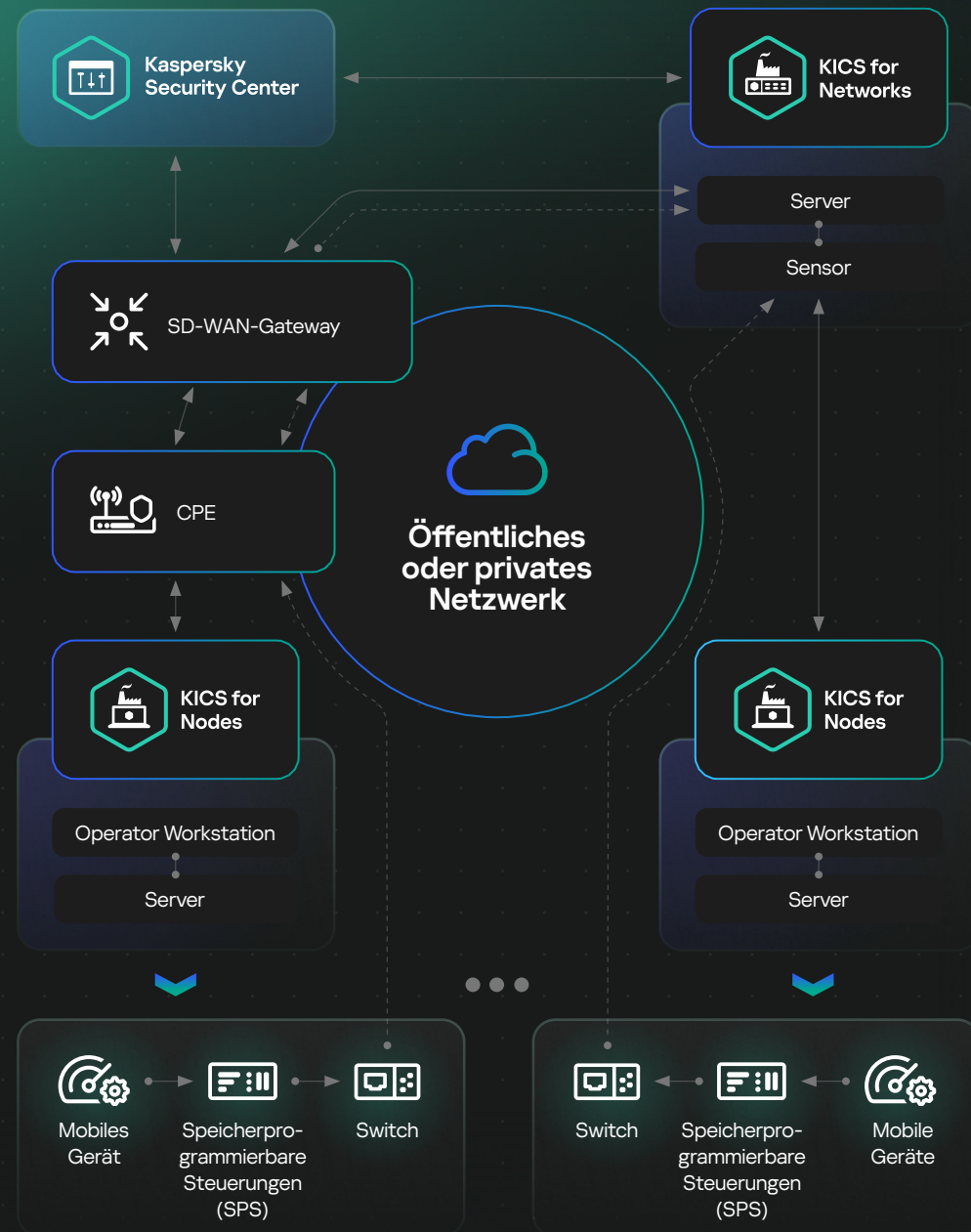
IACS – Industrial Automation and Control Systems
SIEM – Security Information and Events Management

IIoT – Industrial Internet of Things
IoT – Internet of Things (Internet der Dinge)



Mithilfe der SD-WAN-Infrastruktur kann KICS industriellen Datenverkehr erfassen, ein zentralisiertes Monitoring bereitstellen und verteilte industrielle Objekte und Systeme schützen.

- Einfache Skalierbarkeit
- Kostenoptimierung
- Praktische Verwaltung
- Zentralisierte Sicherheit



→ SPAN → Netzwerkverkehr; Node-Telemetrie; Steuerung

**Kaspersky
Antidrone**

Lösung für Drohnenüberwachung und -abwehr

Kaspersky Antidrone verringert das Risiko von Betriebsunterbrechungen in Industrieunternehmen, indem es das Eindringen unbefugter Drohnen in deren Gelände verhindert. Das System scannt automatisch den Luftraum, erkennt Drohnen und klassifiziert sie. Informationen zum aktuellen Geschehen werden in der Weboberfläche angezeigt. Im Falle einer Bedrohung und sofern dies zulässig ist, können die Betreiber die Drohne außer Gefecht setzen.

Kaspersky Antidrone ist eine modulare Lösung, die in Industrieanlagen jeder Größe eingesetzt werden kann. Sie unterstützt zudem einen Identifikationsmodus, der eine Unterscheidung zwischen autorisierten und nicht autorisierten Drohnen ermöglicht. So können Organisationen ihre eigenen Drohnen störungsfrei betreiben und gleichzeitig den Zugang unautorisierter unbemannter Luftfahrzeuge zum Einsatzbereich verhindern.

Wichtigste Vorteile



Mit Kaspersky Antidrone lassen sich Radar-, HF-Scanner, Kameras und Störsender verschiedener Hersteller in einem einzigen, einheitlichen System kombinieren und koordinieren.



Die Multi-Sensor-Fusion verbessert die Erkennungssicherheit bei unübersichtlichen, störungsreichen oder schlechten Sichtverhältnissen erheblich.



Hardwaresensoren



Radar



Video



RF



Entschärfung

Andere Arten von Detektions- und Abwehrgeräten

Software

**Kaspersky
Antidrone**

Weboberfläche



Kaspersky Thin Client

Sichere Infrastruktur für Remote- und virtuelle Desktops

Risiko

Nutzerarbeitsplätze gehören zu den häufigsten Zielen von Cyberangriffen

Lösung

Kaspersky Thin Client ist eine Lösung zum Aufbau einer verwalteten und funktionsfähigen Thin-Client-Infrastruktur auf Basis des Kaspersky-eigenen Mikrokern-Betriebssystems KasperskyOS.

Da sie weder über eine aktive Kühlung noch über bewegliche Teile verfügen, bieten Thin Clients in Produktionsumgebungen eine äußerst zuverlässige Leistung.

Wichtigste Vorteile



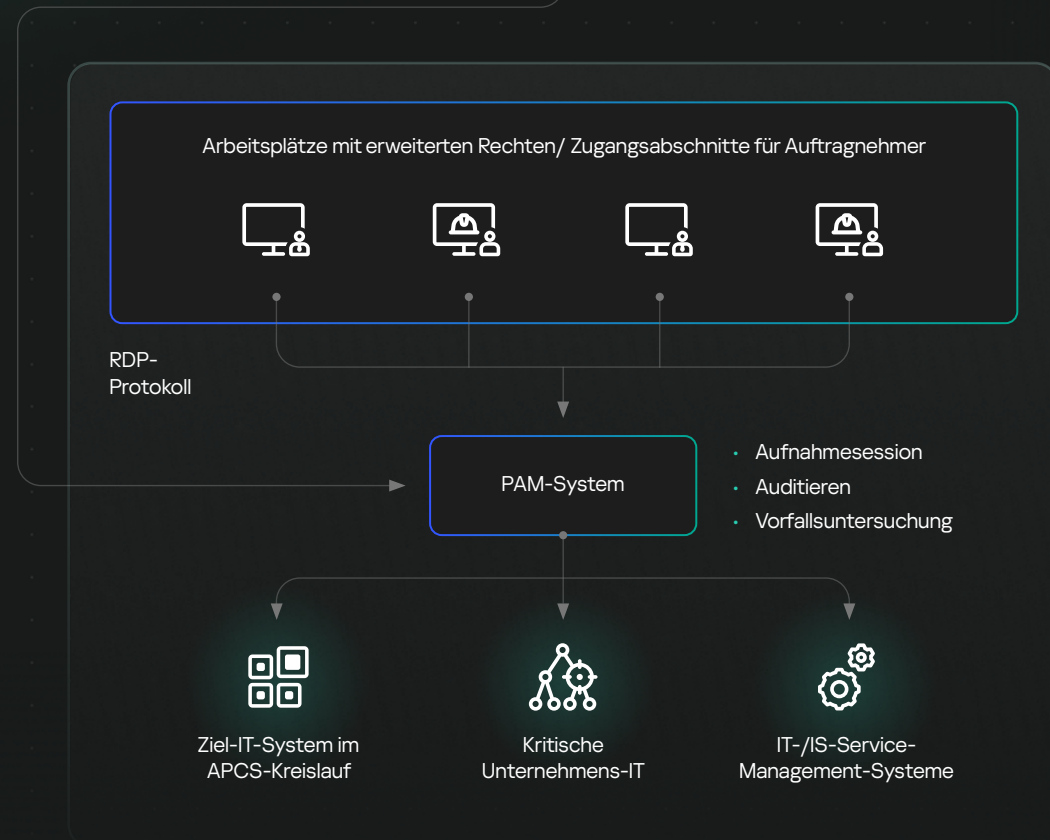
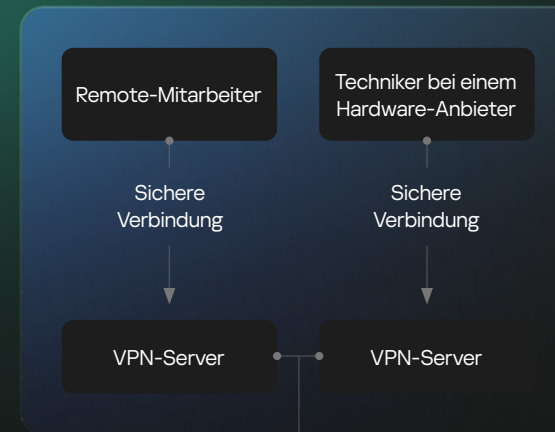
Security by Design



Zentrale Verwaltungsplattform für IS und IT



Integration der Infrastruktur in nur 2 Minuten





Kaspersky Automotive Secure Gateway

Entwicklung zuverlässiger IT-Systeme für vernetzte Fahrzeuge

- Sicheres Software-Gateway für vernetzte Fahrzeuge, das zudem die Funktionen einer Telematik-Steuereinheit (TCU) übernimmt
- Sicherheit auf Betriebssystemebene
- Einhaltung der neuesten Anforderungen zur Gewährleistung der Cybersicherheit und Sicherheit von Fahrzeugen (ISO 26262, ISO/SAE 21434, UN R155, UN R156, Uptane)
- Einhaltung der neuesten Anforderungen zur Gewährleistung der Cybersicherheit und Sicherheit von Fahrzeugen (ISO 26262, ISO/SAE 21434, UN R155, UN R156, Uptane)
- Einführung von Ferndiagnose, sicheren drahtlosen Steuergeräte-Updates und anderen Telematikdiensten

Wichtigste Vorteile

- 🛡️ Höchste Sicherheit und Cyberimmunität für Branchen mit strengen Anforderungen an die Informationssicherheit
- 🔄 Die Integration eines sicheren Gateways und einer Telematik-Steuereinheit in einer einzigen Lösung trägt zur Kostensenkung bei
- 📶 Spezielle Protokolle helfen Mobilfunkkosten zu optimieren

Cloud-Infrastruktur



Update-Server (OTA)



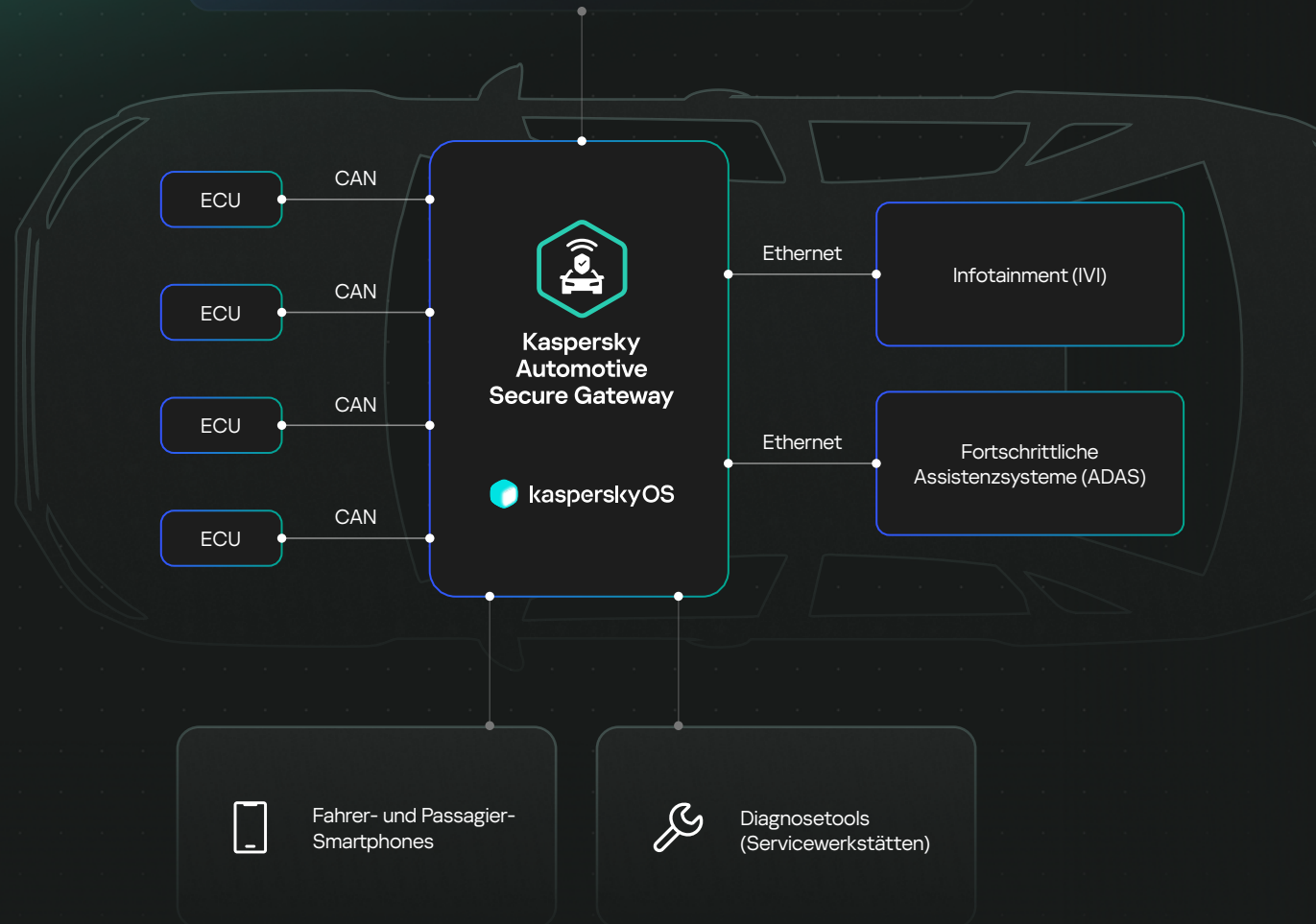
Telematik-Plattform/
Flottenmanagement



Ferndiagnose,
(Remote diagnostics,
RVD)



Security Operations Center
(Vehicle SOC)





Kaspersky ICS Threat Intelligence

Wir geben Ihnen umfassende Einblicke in Bedrohungen und Schwachstellen der industriellen Cybersicherheit. Dadurch ermöglichen wir eine fundierte Risikobewertung sowie die Erkennung, Analyse und Bearbeitung von Sicherheitsvorfällen.

Unterstützt durch das umfassende Fachwissen und die Erfahrung von Kaspersky ICS CERT, dem ersten privaten CERT für industrielle Cybersicherheit.

Wichtigste Vorteile



Schnelle Erkennung von Bedrohungen und umfangreiche analytische Funktionen



Effizientere Untersuchungen und proaktives Threat Hunting



Umfassende Informationen über Bedrohungen und Schwachstellen schaffen eine Basis für fundierte Entscheidungen

Kaspersky Threat-Intelligence-Lösungen und -Dienste

Machine-Readable Threat Intelligence

Kaspersky Threat Data Feeds





Kaspersky Threat Data Feeds



Der Kaspersky Threat Data Feed Service liefert Echtzeit-Bedrohungsdaten, die Industrieunternehmen dabei helfen, ihre Netzwerke und Systeme vor Cyberbedrohungen zu schützen. Die ICS-Datenfeeds enthalten Informationen zu bekannten schädlichen Dateien und den neuesten bekannten Sicherheitslücken, die nachweislich in industriellen Steuerungssystemen ausgenutzt werden können. Im Kontext betrachtet helfen diese Daten dabei, das Gesamtbild zu erkennen und die Fragen nach „Wer, Was, Wo und Wann“ zu beantworten. So ist es möglich, Gegner zu identifizieren, schnellere Entscheidungen zu treffen und effektiv zu reagieren.

Wichtigste Vorteile



Verbesserte, beschleunigte Vorfallreaktion und forensische Funktionen



Noch umfassenderer Schutz



Verhindert die Exfiltration von sensiblen Werten und geistigem Eigentum

Sie profitieren von:

Kaspersky ICS Hashes Data Feed

Aktuelle Threat Intelligence für ICS und andere in der OT eingesetzte Systeme zur Vereinfachung und Automatisierung der zeitnahen Erkennung und Untersuchung von Angriffen

Prävention

Erkennung

Analyse

Kaspersky ICS Vulnerability Data Feed

Geprüfte und aufbereitete Daten zu Schwachstellen, die in der Software und Hardware von ICS-Systemen und anderen in industriellen Umgebungen eingesetzten Systemen entdeckt wurden. Die Daten werden in einem maschinenlesbaren Format bereitgestellt.

Prävention

Erkennung

Analyse

ICS Vulnerability Data Feed im OVAL-Format

Ein regelmäßig aktualisierter Feed mit OVAL-Definitionen zur automatischen Erkennung bekannter Schwachstellen in SCADA-Systemen und anderer Industriesoftware

Erkennung



Kaspersky ICS Intelligence Reporting



Kaspersky ICS Threat Intelligence Reporting liefert detaillierte Informationen und erhöht das Bewusstsein für schädliche Kampagnen, die auf Unternehmen abzielen. Außerdem liefert es Informationen über Schwachstellen in den gängigsten branchenweiten Kontrollsystemen und den zugrunde liegenden Technologien. Maßgeschneiderte, detaillierte Informationen für Industrieunternehmen helfen Kunden dabei, wichtige Ressourcen – darunter Software- und Hardwarekomponenten – zu schützen. Dies gewährleistet die Sicherheit und Kontinuität technologischer Prozesse.

Die Berichte werden über das **Kaspersky Threat Intelligence Portal** bereitgestellt und sind auch über eine API verfügbar.

Wichtigste Vorteile



Erkennen Sie bekannte Bedrohungen und wehren Sie diese wirksam ab. So schützen Sie kritische Anlagen sowie die Sicherheit und Kontinuität technologischer Prozesse.



Korrelieren Sie erkannte bösartige oder verdächtige Aktivitäten mit den Forschungsergebnissen von Kaspersky. Dadurch können Sie Vorfälle bestimmten Kampagnen zuordnen und Bedrohungen identifizieren.

Sie profitieren von:



APT-Berichte

Berichte über neue APT- und umfangreiche Angriffskampagnen, die auf Unternehmen abzielen, sowie Updates zu aktiven Bedrohungen



Identifizierte Schwachstellen

Berichte über Schwachstellen, die von Kaspersky in den gängigsten Produkten für industrielle Kontrollsysteme, dem industriellen Internet der Dinge und Infrastrukturen in verschiedenen Branchen entdeckt wurden



Die Bedrohungslandschaft

Berichte über wesentliche Veränderungen in der Bedrohungslandschaft für branchenweite Kontrollsysteme sowie über neu entdeckte kritische Faktoren mit Auswirkungen auf die ICS-Sicherheitsniveaus und das ICS-Bedrohungsrisiko. Dabei werden auch regionale, länderspezifische und branchenspezifische Informationen berücksichtigt.



Schwachstellenanalyse und -minderung

Unsere Ratgeber enthalten praktisch umsetzbare Empfehlungen von Kaspersky-Experten, um Schwachstellen in Ihrer Infrastruktur zu ermitteln und Risiken zu senken.



Kaspersky Ask the Analyst



Kaspersky Ask The Analyst ergänzt das Threat Intelligence-Portfolio. Mit diesem Service können Sie sich an Experten wenden, um Unterstützung und nützliche Informationen zu bestimmten Bedrohungen und Schwachstellen zu erhalten, mit denen Sie konfrontiert sind oder an denen Sie Interesse haben. Anhand dieser Daten können Sie Ihre Abwehrmaßnahmen gegen Bedrohungen verbessern, die sowohl Ihr Unternehmen als Ganzes als auch Ihre industrielle Infrastruktur betreffen.

Wichtigste Vorteile



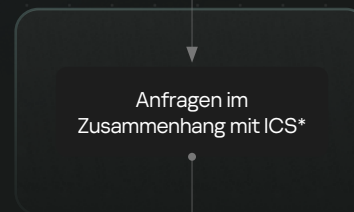
Zugang zu führenden Experten für Bedrohungsdaten, darunter Experten für industrielle Sicherheit von Kaspersky ICS CERT



Personalisierte und detaillierte Kontextinformationen für effektive Untersuchungen



Detaillierte Anweisungen durch unsere Experten zur schnellen Reaktion auf Bedrohungen und Schwachstellen



Kompetenzfelder



Bedrohungsanalyse
im Darknet



Informationen über APTs und
Crimeware-Bedrohungen



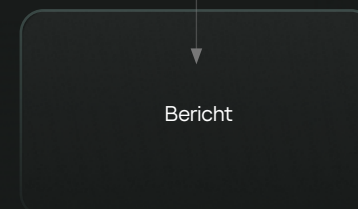
Malware-Analyse



Beschreibung der Bedrohungen,
Schwachstellen und der damit verbundenen
Indicators of Compromise

* Zusätzliche Informationen zu veröffentlichten Berichten:

- Informationen zu ICS-Sicherheitslücken
- Statistiken zu Bedrohungen für Prozessleitsysteme und neue Trends nach Region und Branche
- Analyse von Malware, die auf ICS abzielt
- Informationen zu gesetzlichen Vorgaben und Standards





Kaspersky Security Awareness



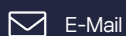
Kaspersky ICS CERT Training

Machen Sie Ihre Mitarbeiter zu einer menschlichen Firewall

Das Kaspersky Security Awareness-Portfolio trägt dazu bei, eine starke Kultur der Cybersicherheit auf allen Ebenen Ihres Unternehmens zu etablieren:

- **Kaspersky Interactive Protection Simulation (KIPS)** – eine spielbasierte Simulation, die speziell auf industrielle Szenarien zugeschnitten ist (Stromerzeugung, Öl- und Gasindustrie, Petrochemie usw.). Diese zeigt, wie sich Cybersicherheit auf die Unternehmensleistung auswirkt, und ermöglicht Führungskräften, die Auswirkungen strategischer Entscheidungen zu erleben.
- **Kaspersky Automated Security Awareness Platform (ASAP)** – fördert durch interaktive Schulungen und simulierte Phishing-Angriffe ein sicheres Verhalten in der gesamten Belegschaft und vermittelt den Mitarbeitern grundlegende Kenntnisse und Fähigkeiten im Bereich der industriellen Cybersicherheit.
- **Kaspersky Executives Training** – ein praxisorientierter Kurs, der Entscheidungsträgern und Fachbereichsleitern ein klares Verständnis der Cybersicherheitslandschaft vermittelt.

Wichtige behandelte Themen



E-Mail



Webseiten und Internet



Passwörter und Konten



Social Media und Messenger-Apps



Industrial Cybersecurity



PC-Sicherheit



Mobilgeräte



Vertrauliche Daten



DSGVO



Physische Datensicherheit



Sicherheit von Bankkarten und PCI DSS



KI und neuronale Netzwerke



Personenbezogene Daten

Praxisorientiertes Lernen

Mit unserem ICS-Schulungsprogramm richten wir uns an Fachleute aus den Bereichen IT, OT und Informationssicherheit sowie an Führungskräfte und andere Mitarbeitende. Das Programm soll ihnen dabei helfen, ihr Wissen über industrielle Cybersicherheit zu erweitern und spezielle praktische Fähigkeiten zu erwerben.

Praktische Tipps von Kaspersky-Experten



Digitale Forensik und Vorfallreaktion



Untersuchung von Sicherheitslücken in OT-/IoT-Geräten und industrieller Software



Funktionsübergreifendes Training für IT-, OT- und IS-Experten





Kaspersky ICS Security Assessment

Stärkung der Cyberresilienz in OT-Umgebungen

Risiko

Eine einzige Sicherheitslücke reicht aus, damit Cyberkriminelle die Kontrolle über ein gesamtes industrielles System übernehmen können

Lösung

Ein umfassender Ansatz zur Erkennung von Sicherheitslücken und Schwachstellen in industriellen Infrastrukturen

Wichtigste Vorteile

- Verstärken Sie Maßnahmen zum Schutz von Bedienern, Technikern und weiteren Mitarbeitern
- Erkennen Sie Schwachstellen, die Hacker ausnutzen könnten, um Fertigungslinien, Produktionsanlagen oder Robotersysteme lahmzulegen
- Schützen Sie Konstruktionsentwürfe, Projekte und Programme gegen Diebstahl
- Verhindern Sie Vorfälle, die die Produktqualität oder -sicherheit beeinträchtigen könnten

Kasperskys Ansatz zur Bewertung der industriellen Sicherheit



Externer Penetrationstest
Black-Box oder Grey-Box

Internet

Industrielle (OT)-Infrastruktur

- Netzwerkarchitektur und -Hardware
- Industrielösungen, Workstations und Server
- Geräte und Komponenten

Geräte und
Komponenten



OT-Sicherheitsanalyse

- White-Box-Tests
- Angriffssimulation
- Assessment

Unternehmenseigenes LAN, MES



Interner Penetrationstest
Black-Box oder Grey-Box

Testumgebung



Sicherheitsanalyse von Hardware-
und Softwarekomponenten

- White-Box-Tests
- Zero-Day-Schwachstellen
- Hardening Guides



Kaspersky Managed Detection and Response

KI trifft menschliche Expertise

- Kontinuierliche Erkennung, Aufdeckung und Beseitigung von Bedrohungen, die auf Ihr Industrieunternehmen abzielen
- Senkung der Sicherheitskosten, da keine neuen Cybersicherheitsspezialisten eingestellt werden müssen
- Profitieren Sie von allen wesentlichen Vorteilen eines SOC, ohne selbst eines aufbauen zu müssen

22 % unserer Kunden kommen aus dem Industriesektor
Lesen Sie den [MDR Analyst Report](#), um mehr zu erfahren

Wichtigste Vorteile



Proaktive Erkennung von Bedrohungen: Patentierte Angriffsindikatoren helfen dabei, versteckte Bedrohungen innerhalb des Steuerungssystems zu identifizieren



Automatisierte und geführte Reaktion (mit umfassender forensischer Untersuchung und Malware-Analyse auf Abruf)



Die Cybersicherheitsexpertise von ICS wird von einem der erfolgreichsten und erfahrensten Teams für proaktive Bedrohungserkennung der Branche getragen





Kaspersky Incident Response

Bewältigung der Folgen einer Sicherheitsverletzung

Risiko

Vorfälle, die kritische Infrastruktur betreffen, erfordern Fachwissen für die Durchführung von Maßnahmen in Industrieanlagen. Falsche und vorzeitige Maßnahmen können den Schaden durch einen Angriff erheblich vergrößern.

Lösung

- Schnelle Beseitigung der Folgen eines Vorfalls durch das Global Emergency Response Team von Kaspersky
- Unterstützung während des gesamten Zyklus der Vorfalluntersuchung und -bewältigung
- Analyse, Datenerfassung und Fehlerbehebung auf Basis unserer eigenen innovativen Tools
- Fachwissen auf Abruf und Wissensaustausch mit Ihren Teams

Serviceaufbau



Incident Response

Untersuchung und Beseitigung von Bedrohungen



Digitale Forensik

Analyse digitaler Beweisführung



Malware-Analyse

Verschaffen Sie sich einen detaillierten Überblick über die bei einem Angriff verwendeten Dateien

Entdecken Sie die Anatomie der Cyberwelt mit dem [globalen Report](#) von Kaspersky Security Services



Schutz, auf den Sie vertrauen können



Mehr als 30 Jahre Erfahrung und Petabytes an Bedrohungsdaten



ICS CERT – unsere eigene internationale OT-/IoT-Sicherheitsforschungsabteilung



Bewährte Expertise in der IT/OT-Sicherheitsbranche mit zahlreichen Auszeichnungen und Erfolgen



Über 200 Zertifizierungen zur Interoperabilität mit Lösungen von Automatisierungsanbietern



Die Technologie ist nachgewiesen effizient und erfüllt die Branchenstandards und -anforderungen



Weitere
Informationen
zu OT-Lösungen

Weitere
Informationen
zu IT-Lösungen

Kontakt