Una piattaforma XDR
per la protezione completa
delle aziende del settore
industriale

Kaspersky Industrial CyberSecurity

kaspersky BRING ON THE FUTURE

Cyberminacce affrontate da ICS e imprese industriali

Attacchi malware

Dall'inizio del 2023, circa il 35% dei computer associati ai sistemi ICS ha subito attacchi malware: quasi il 5% in meno rispetto all'anno precedente.

Kaspersky ICS CERT, ottobre 2023

Per saperne di più

La nuova realtà per i proprietari e gli operatori di infrastrutture industriali è caratterizzata dal crescente interesse degli hacktivisti per i sistemi di automazione, dagli elevati requisiti normativi, dalla convergenza IT-OT e dall'aumento della varietà di attacchi informatici nel settore industriale (un aumento di quasi il 50% nel primo semestre del 2023 rispetto al secondo semestre del 2022, secondo le statistiche di Kaspersky ICS CERT).

L'avvento delle tecnologie digitali, solitamente considerato un aspetto positivo, elimina il gap tra gli ambienti IT e OT che proteggeva questi ultimi dai criminali informatici. Mentre una singola unità flash introdotta nell'ambiente ICS può compromettere seriamente il core business di un'azienda, un gruppo di hacker motivato può penetrare nelle reti OT e causare danni considerevoli e/o rubare informazioni preziose. Insieme all'evoluzione degli standard di automazione da raccomandazioni comuni a requisiti legislativi e con la crescente necessità di condividere le best practice e gestire i rischi, questo rende la cybersecurity delle imprese industriali una sfida molto ardua.

Secondo le previsioni di Kaspersky ICS CERT, le organizzazioni seguenti settori si troveranno ad affrontare cyberattacchi con una frequenza sempre maggiore:

I principali bersagli degli attacchi APT includeranno:

Proprietari e operatori di infrastrutture critiche
Le organizzazioni pubbliche o governative di importanza strategica devono affrontare le maggiori potenziali conseguenze derivanti dalle interferenze operative

Operatori industriali di alto profilo
Da un singolo stabilimento a strutture su scala nazionale o internazionale, queste aziende svolgono operazioni ad alto rischio, che comportano costi significativi per gli incidenti

Settore petrolifero, del gas e chimico

L'elevato valore dei dati e dei sistemi controllati da queste aziende le rende un obiettivo allettante per il ransomware e gli autori di attacchi che puntano a interrompere le operazioni o manipolare i prezzi.

Manifattura industriale di alto profilo

Queste imprese svolgono un ruolo critico a livello sociale e dispongono di dati preziosi che possono essere sfruttati a scopo di lucro, con ingenti danni economici e in termini di reputazione.

Settore minerario e metallurgico

Il settore minerario e metallurgico viene preso di mira per le risorse preziose, l'impatto finanziario e le supply chain interconnesse.

Energia, reti di distribuzione e servizi pubblici

Il ruolo chiave che l'energia, le reti di distribuzione e i servizi pubblici svolgono nella nostra vita quotidiana è la ragione principale degli attacchi volti a creare caos o esercitare influenza.

La stabilità dei processi di produzione e aziendali, nonché la protezione di risorse preziose, sono direttamente correlate allo sviluppo sostenibile delle imprese industriali e delle infrastrutture critiche. Gli attacchi ai sistemi industriali, in particolare ICS e SCADA, sono in aumento. Nel frattempo, le moderne minacce informatiche rivolte agli ambienti industriali sembrano essere immuni alle soluzioni tradizionali.

Scegliere un partner affidabile, con una profonda conoscenza delle sovrapposizioni tra cybersecurity industriale e aziendale e la capacità di fornire una gamma completa di tecnologie di sicurezza all'avanguardia, non è mai stato così importante.

Scoprite di più sulle tattiche, tecniche e procedure (TTP) più comuni degli attacchi contro le organizzazioni industriali

Per saperne di più

La piattaforma XDR KICS consente agli utenti di avere una panoramica e un contesto più ampi su elementi come: catena di incidenti a livello di rete ed endpoint, esatti parametri delle risorse, comunicazione di rete e mappe topologiche anche da segmenti in cui il mirroring del traffico non è ancora disponibile.

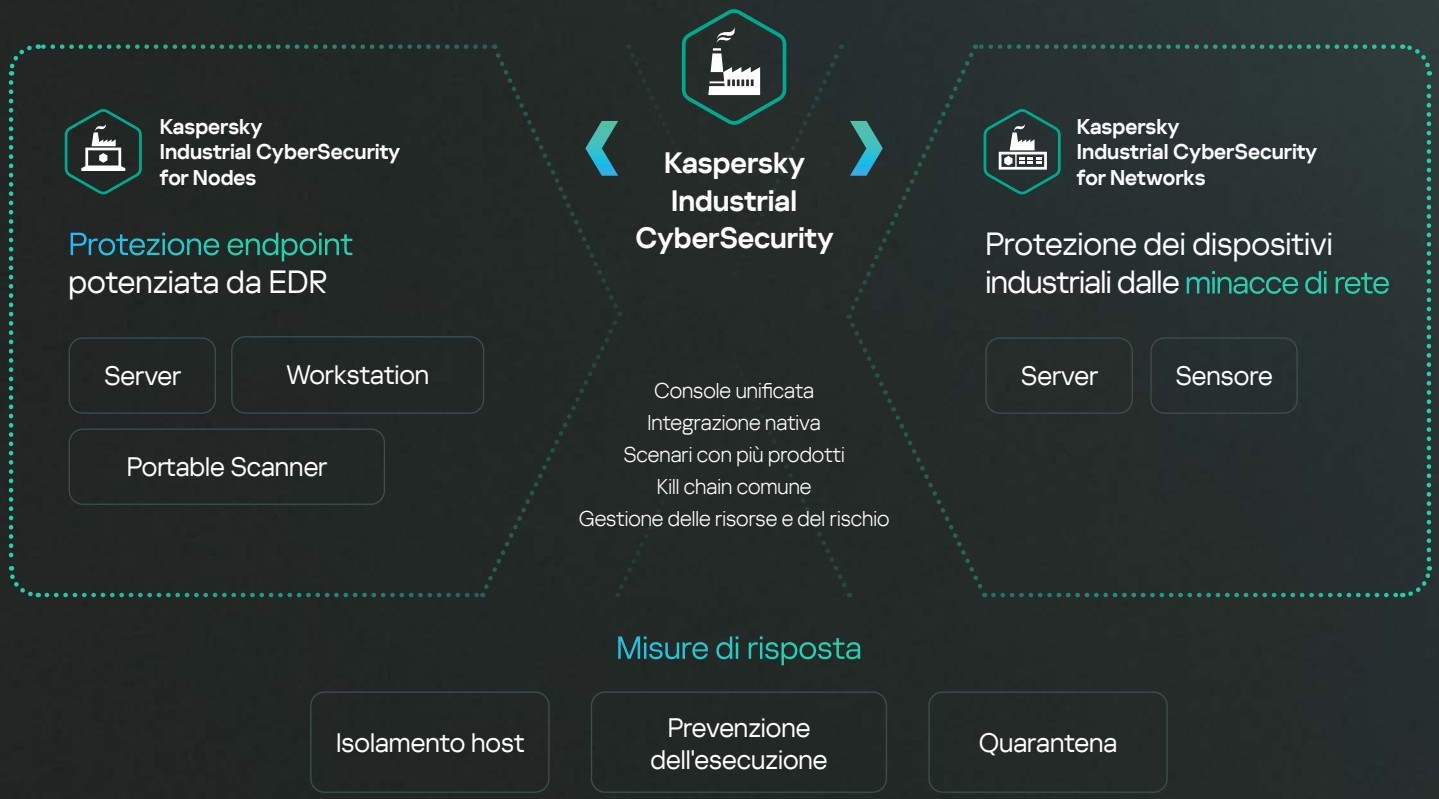
Endpoint sensor

- Stato della protezione
- Security Audit
- Comunicazioni di rete
- Trasmissione di dati di telemetria dell'host
- Monitoraggio delle apparecchiature
- Incident response

Tecnologie di sicurezza ICS avanzate

Kaspersky Industrial CyberSecurity (KICS) è una piattaforma XDR (Extended Detection and Response) nativa per le imprese industriali, appositamente progettata e certificata per proteggere apparecchiature, risorse e reti OT critiche dalle cyberminacce. La piattaforma comprende tecnologie integrate che proteggono i componenti principali del sistema di controllo e automazione industriale a tutti i livelli. KICS for Nodes è un software di protezione degli endpoint, rilevamento e riposta con funzionalità di controllo conformità e sensore endpoint. KICS for Networks è progettato per l'analisi del traffico di rete OT, per il rilevamento e la risposta. La piattaforma integra una funzione di gestione centralizzata a livello di sito, essenziale per adattare le operazioni di sicurezza OT a un volume elevato di infrastrutture industriali di grandi dimensioni, diversificate e geograficamente distribuite.

La perfetta integrazione tra i componenti della piattaforma, offre la piena visibilità di più sistemi di automazione e reti OT distribuiti in diverse posizioni, offrendo una migliore esperienza del cliente, consapevolezza situazionale e flessibilità della distribuzione. Grazie alle funzionalità Extended Detection and Response, la piattaforma KICS consente la convergenza IT-OT e offre numerosi vantaggi per il singolo fornitore.



Punti di applicazione della piattaforma

Convergenza degli ambienti OT e IT

DMZ / GTW

Ambiente IT

Ambiente OT

Kaspersky Industrial CyberSecurity for Nodes

- Operator Workstation
- Server SCADA
- Engineer Workstation
- Gateway ICS

Network equipment

SPAN

Kaspersky Industrial CyberSecurity for Networks

- BCU (Bay Control Unit)
- IED (Intelligent Electronic Device)
- PLC (Programmable Logic Controller)
- Sistema strumentato di protezione e sicurezza relè (SIS)
- Nodi isolati (controllo manuale con KICS Portable Scanner)

Rilevamento precoce delle anomalie e analisi predittiva

Kaspersky MLAD (Kaspersky Machine Learning for Anomaly Detection) è un sistema innovativo che utilizza una rete neurale per monitorare simultaneamente un'ampia gamma di dati di telemetria. Rileva i guasti delle apparecchiature e gli errori umani, contribuendo a prevenire problemi e incidenti, identifica le azioni dei dipendenti o le operazioni delle apparecchiature atipiche come segni di un attacco specializzato o di un sabotaggio e combina il rilevamento delle anomalie con l'analisi predittiva delle condizioni e del ciclo di vita delle apparecchiature.

Per saperne di più

Livello fisico

Protezione con i prodotti Kaspersky

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Una soluzione proprietaria a livello di protocollo per il monitoraggio della rete industriale e l'analisi del traffico, fornita come software o come dispositivo virtuale.

KICS for Networks individua anomalie e intrusioni nel sistema ICS in una fase iniziale, mostra come si sviluppa l'attacco sulla rete e nei nodi (kill chain EDR e telemetria) e garantisce che vengano intraprese le azioni necessarie per prevenire qualsiasi impatto negativo sui processi industriali.

La soluzione aiuta a rilevare e classificare i rischi in base ai dati sulle vulnerabilità e sulle connessioni di rete, nonché al ruolo delle varie risorse, per prevenire gli incidenti.

Vantaggi

Inventario delle risorse

Inventario automatico delle risorse e raccolta dei dati con l'utilizzo di metodi passivi e attivi di raccolta dati

Network Inventory and Visualization

- Network communications map
- Network topology diagram

Valutazione di rischi e vulnerabilità

- Gestione di rischi e vulnerabilità specifici per OT
- Assegnazione automatica di punteggi e priorità
- Suggerimenti per la risoluzione dei rischi

Rilevamento di anomalie di rete

Controllo dell'integrità della rete con monitoraggio della deviazione dalla linea di base e rilevamento di attività di rete dannose e sospette

Controllo dei processi OT e analisi approfondita dei pacchetti (DPI)

- Estrazione dei dati sul payload industriale
- Real-time process control
- Industrial command control
- Monitoraggio dei processi OT avanzati tramite Kaspersky MLAD

Scambio di dati e integrazione

- Informazioni centralizzate
- Integrazione con i sistemi dei clienti o di Kaspersky e di terze parti (connettori basati su API, IEC 104, OPC, CEF, Syslog)

Centralized compliance dei nodi delle reti industriali

KICS for Networks offre un controllo centralizzato dei nodi della rete industriale, compresi il controllo agent-based (tramite KICS for Nodes) e agentless dell'hardware di rete e degli endpoint per le vulnerabilità e la conformità con gli standard di settore OVAL* e XCCDF**.

- Controllo automatico della sicurezza centralizzata per nodi Windows, Linux e dispositivi di rete
- Controllo della conformità. Editor con funzionalità complete per controlli e parametri di conformità
- Tutti i report e i dati sulle risorse sono disponibili in una singola posizione: la base di risorse di KICS for Networks
- Archivio protetto per le credenziali dei nodi
- Supporto per qualsiasi database OVAL personalizzato o di terze parti
- Database integrato sulle vulnerabilità SCADA da ICS CERT

* OVAL (Open Vulnerability and Assessment Language)
** XCCDF (Extensible Configuration Checklist Description Format)

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

Rilevamento e risposta, protezione degli endpoint certificata e testata, di livello industriale. Una soluzione stabile e compatibile a basso impatto per sistemi Linux, Windows e standalone.

KICS for Nodes protegge tutti gli endpoint in un sistema di automazione moderno, digitale, gestito e distribuito. La soluzione raccoglie la telemetria per creare una rappresentazione visiva chiara e dettagliata dell'avanzamento di un incidente su workstation, server, gateway e altri endpoint, garantendo agli amministratori dei sistemi di automazione che un incidente sia stato completamente gestito e che non si verificherà più.

KICS for Nodes Portable Scanner applica un criterio di cybersecurity su macchinari standalone, sistemi di automazione o apparecchiature in cui non è possibile installare software di sicurezza. Ha un impatto operativo molto basso e non interferisce con le soluzioni di sicurezza esistenti.

- Soluzione Installation-free che fornisce la massima consapevolezza della situazione e visibilità OT anche per un'infrastruttura standalone.
- Consente di eseguire scansioni su richiesta su più macchine contemporaneamente durante le finestre di manutenzione e fornisce pratici report.
- Esegue controlli di conformità anti-malware delle apparecchiature che accedono a un sito OT, inclusi i computer di fornitori di terze parti.

- Device Control
- File Integrity Control
- PLC Integrity Control
- Anti-Cryptor
- Exploit prevention
- Network Threat Prevention
- Windows Log inspector
- Wi-Fi Control
- Firewall Management
- Registry Monitor
- Security Audit
- Agente EDR
- Sensore endpoint (integrazione con KICS for Networks)

- Windows Nodes
- Linux Nodes
- Portable Scanner
- Audit Agent

- Gateway
- Server Historian
- Server SCADA
- Operator workstation
- Engineering workstation
- Workstation di gestione dei sistemi
- Embedded systems

Vantaggi

Basso impatto

- Basso impatto sui dispositivi protetti per prestazioni superiori del sistema
- Nessun riavvio richiesto per l'installazione, l'aggiornamento o l'upgrade
- Disponibilità della modalità solo rilevamento
- Utilizzo delle risorse di sistema ottimizzabile

Compatibilità

- Supporto dei sistemi operativi legacy a partire da Windows XP SP2 e Windows Server 2003 SP1
- Compatibilità con i fornitori di soluzioni di automazione industriale
- Portable Scanner come opzione senza installazione

Protezione estesa

- Protezione contro malware, ransomware ed exploit
- Analisi dei log
- Controllo firewall
- Tecnologia EDR ICS integrata
- Aggiornamenti dei database air-gapped

Distribuzione modulare

- Opzioni flessibili e impostazioni sicure non intrusive progettate per OT
- L'architettura modulare consente di selezionare solo i componenti di protezione richiesti

Supporto PLC

- Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4
- Schneider Electric Modicon M340, M580
- Dispositivi basati su CODESYS V3
- Fastwel CPM723-01

Verifica

- OVAL audit completo di sicurezza e conformità basato su standard aperti

Fattori di efficacia di Kaspersky XDR

Comprensione contestuale di caratteristiche uniche, requisiti, sistemi specializzati, protocolli e considerazioni operative

L'integrazione con ICS consente visibilità e analisi complete del traffico di rete industriale e del comportamento del sistema

Threat Intelligence specifica per OT per sfruttare l'esperienza di Kaspersky nell'area della protezione dalle minacce per gli ambienti industriali

Personalizzazione e configurazione per adattare la soluzione alle specifiche esigenze di tolleranza al rischio, architettura di rete e conformità normativa

Un **unico fornitore** per ottenere il massimo in termini di supporto e collaborazione, inclusa la fornitura tempestiva di aggiornamenti e patch

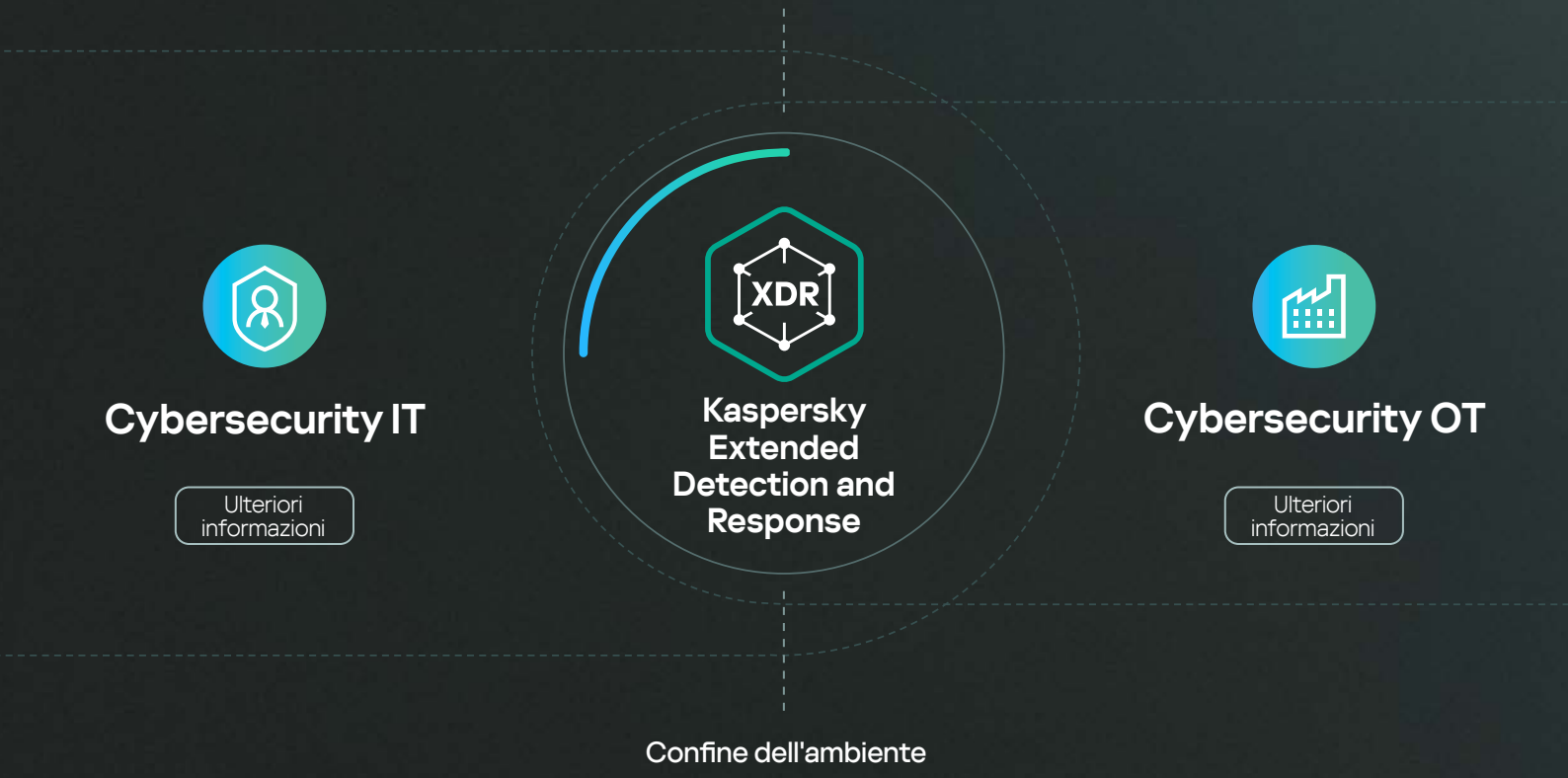
Cybersecurity unificata nei segmenti industriali e aziendali

Gli attacchi ai sistemi industriali, in particolare ICS e SCADA, sono in aumento. Scegliere un partner affidabile, con una profonda conoscenza delle sovrapposizioni tra cybersecurity industriale e aziendale e la capacità di fornire una gamma completa di tecnologie di sicurezza all'avanguardia, non è mai stato così importante.

Kaspersky XDR è lo strumento perfetto per creare un ambiente di lavoro sicuro e privo di minacce. La sua compatibilità con un'ampia varietà di prodotti di sicurezza facilita la creazione di un cyberspazio sicuro, fornendo opzioni specifiche di settore per la vostra azienda e proteggendola da qualsiasi minaccia, grande o piccola. Le opzioni di integrazione di Kaspersky XDR consentono di fornire una visione unificata e completa delle minacce, dotando il vostro team di sicurezza di tutti gli strumenti e i dati necessari per proteggere l'azienda dalle minacce attuali e potenziali.

Ulteriori informazioni

Convergenza IT-OT con Kaspersky Hybrid XDR



Oltre 26 anni di esperienza e petabyte di dati sulle minacce

ICS CERT

ICS CERT - security research division internazionale nell'ambito della sicurezza IoT/OT

Comprovata esperienza nel settore della sicurezza IT/OT con numerosi riconoscimenti e risultati

Oltre 100 certificati di interoperabilità con le soluzioni dei fornitori di soluzioni di automazione

Comprovata efficacia della tecnologia, conformità agli standard e ai requisiti

Clienti in tutto il mondo

ROSATOM · NORNICKEL · EuroChem · NLMK · TATNEFT · ROSSETI · Wintershine · alperia · PacificLight · КазМунайГаз · AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Ulteriori informazioni

www.kaspersky.it

#kaspersky
#bringonthefuture