Una piattaforma XDR (Extended Detection and Response) per la completa sicurezza industriale

Kaspersky Industrial CyberSecurity

kaspersky bring on the future

Sotto attacco malware

Nel primo trimestre del 2024, un totale di 30 incidenti di cybersecurity sono stati confermati pubblicamente dalle organizzazioni interessate o dai funzionari responsabili, di cui il 64,5% nel settore manifatturiero.

Kaspersky ICS-CERT, giugno 2024

Per saperne di più

Panorama delle minacce industriali

La nuova realtà per i proprietari e gli operatori di infrastrutture industriali viene plasmata da fattori quali il crescente interesse degli hacktivisti nei sistemi di automazione, gli elevati requisiti normativi, la convergenza IT-OT e l'aumento della varietà di cyberattacchi nel settore industriale (nel primo trimestre del 2024 le soluzioni Kaspersky hanno bloccato malware di 10.865 famiglie diverse su sistemi di automazione industriale).

La proliferazione delle tecnologie digitali, solitamente considerata un aspetto positivo, elimina il divario tra gli ambienti IT e OT che proteggeva questi ultimi dai cybercriminali. Se da un lato una semplice unità flash introdotta nell'ambiente ICS può compromettere seriamente il core business di un'azienda, dall'altro 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, tutto questo rende la cybersecurity nel settore industriale una sfida ardua.

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

Settore petrolifero, del gas e chimico

La digitalizzazione dell'esplorazione, dell'estrazione, del trasporto e della raffinazione, è un fattore competitivo per queste aziende, implica l'integrazione di IIoT, droni e robot, e la messa in campo di soluzioni 5G, blockchain e VR che espongono il fianco alle azioni dannose.

Manifatturiero

Nel migliorare la redditività, queste aziende utilizzano tecnologie all'avanguardia, espandono la connettività, sfruttano il cloud ed esplorano scenari di convergenza IT-OT, il tutto allargando l'esposizione a minacce in continua evoluzione.

Settore minerario e metallurgico

Pilastro del mondo manifatturiero con importanza nazionale, il settore minerario e metallurgico deve bilanciare le spese introducendo al contempo automazione e tecnologie digitali. Essendo una risorsa preziosa sia per gli hacktivisti che per gli autori degli attacchi ad alto potenziale, non può ammettere compromessi alla cybersecurity.

Energia, reti di distribuzione e servizi pubblici

Le tecnologie digitali ed emergenti sono essenziali per guidare la transizione energetica pur mantenendo le infrastrutture tradizionali che costituiscono ancora la spina dorsale della maggior parte degli impianti energetici. Allo stesso tempo, però, rappresentano il rischio maggiore e richiedono sforzi straordinari in termini di cybersecurity.

Gli attacchi ai sistemi industriali, in particolare ICS e SCADA, sono in aumento. Nel frattempo, le odierne cyberminacce rivolte agli ambienti industriali sembrano fare scudo contro le soluzioni tradizionali. In questo contesto, Kaspersky offre un approccio completo per tutti questi settori. Scoprite sul nostro sito Web le storie di successo dei nostri clienti, le informazioni sul panorama delle minacce e le offerte dedicate a specifici scenari.

Oggi è più importante che mai scegliere un partner affidabile, con una profonda conoscenza delle sovrapposizioni tra cybersecurity industriale e aziendale e con la capacità di fornire una varietà di tecnologie di sicurezza all'avanguardia.

I principali bersagli di attacchi di tipo APT includeranno:

Proprietari e operatori di infrastrutture critiche

Le organizzazioni strategicamente importanti dei settori petrolifero, gas, chimico, energetico e dei servizi di pubblica utilità rischiano conseguenze potenziali notevolmente maggiori derivanti da interferenze operative

Manifatturiero fondamentale

Da un singolo stabilimento fino a realtà su scala nazionale o internazionale, queste aziende, comprese quelle dei settori metallurgico e minerario, agricolo e manifatturiero globale, sono impegnate in operazioni ad alto rischio che comportano costi significativi in caso di manomissione

Ulteriori informazioni sugli attacchi APT e finanziari al settore industriale all'inizio del 2024

Per saperne di più

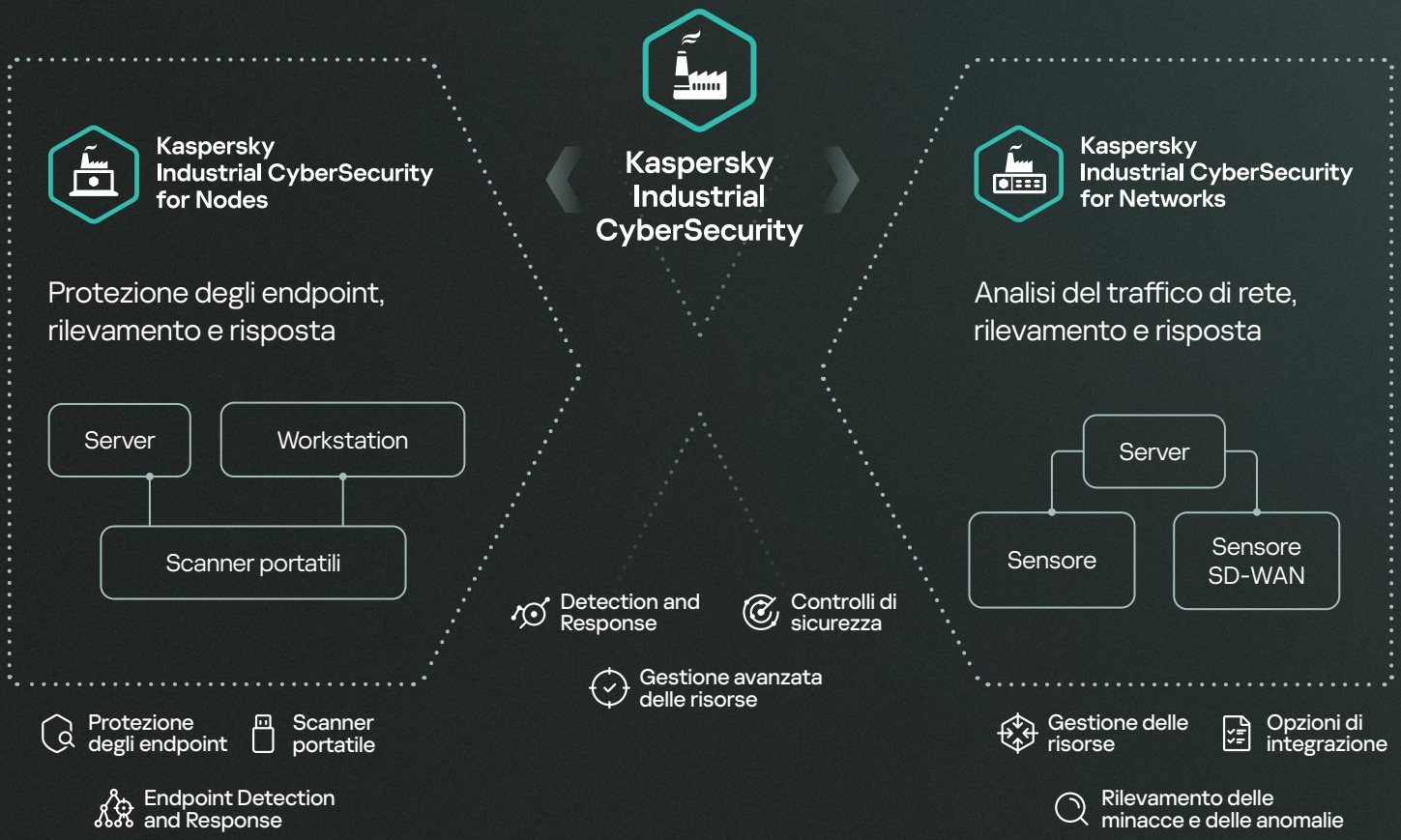
Tecnologie di sicurezza ICS avanzate

Il divario tra gli ambienti IT e OT che un tempo proteggeva questi ultimi dai cybercriminali si sta sempre più riducendo, motivo per cui una soluzione di sicurezza completa di livello enterprise fornita da un unico fornitore a salvaguardia delle infrastrutture critiche è ormai un must per i proprietari e gli operatori di sistemi cyber-fisici. **La piattaforma XDR nativa Kaspersky Industrial CyberSecurity (KICS)**, composta dai componenti KICS for Networks e KICS for Nodes, protegge le reti e i sistemi di automazione industriale.

KICS for Networks è un prodotto di analisi, rilevamento e risposta al traffico che offre monitoraggio delle reti industriali, rilevamento delle intrusioni e gestione dei rischi, offrendo al contempo il controllo centralizzato dei nodi delle reti industriali per individuare vulnerabilità e accertare la conformità agli standard di settore. **KICS for Nodes** offre protezione, rilevamento e risposta degli endpoint di livello industriale con controlli di conformità basati su OVAL*. Questa soluzione modulare e a basso impatto è compatibile con Linux, Windows, sistemi legacy, sistemi autonomi e PLC. In versione Portable Scanner protegge macchinari autonomi e dispositivi di terzi senza necessità di installazione.

Insieme, questi componenti formano la piattaforma KICS XDR che offre audit, un inventario centralizzato delle risorse e gestione rischi, consentendo la scalabilità della sicurezza su infrastrutture diversificate e distribuite tramite un'unica piattaforma con una vista ed analisi completa sugli incidenti rilevati.

La piattaforma XDR KICS consente agli utenti di avere una panoramica e un contesto più ampio su elementi quali catene di incidenti a livello di rete e di endpoint, parametri esatti impostati all'interno dei dispositivi industriali, comunicazione di rete e mappe topologiche anche da segmenti in cui il mirroring del traffico non è ancora disponibile.



* OVAL (Open Vulnerability and Assessment Language)

Punti di applicazione della piattaforma

Convergenza degli ambienti OT e IT

DMZ / GTW

Ambiente IT

Ambiente OT

Kaspersky Industrial CyberSecurity for Nodes

- Workstation operatore
- Server SCADA
- Workstation tecnico
- Gateway ICS

Apparecchiature di rete

SPAN

Kaspersky Industrial CyberSecurity for Networks

- BCU (Bay Control Unit)
- IED (Intelligent Electronic Device)
- PLC (Programmable Logic Controller)
- Relay protection e safety instrumented system (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 usa una rete neurale per monitorare simultaneamente una grande varietà 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

Soluzione di monitoraggio della rete industriale e di analisi del traffico. Abilita l'ispezione approfondita dei pacchetti (DPI) dei protocolli industriali proprietari. Disponibile come software o appliance virtuale.

KICS for Networks identifica 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 adottate le azioni necessarie per prevenire qualsiasi impatto negativo sui processi industriali.

Gestione delle risorse

Rilevamento delle risorse
Ottenete informazioni sulle vostre risorse con un database delle vulnerabilità, la definizione delle priorità dei rischi e il polling attivo sicuro

Visibilità della rete
Monitorate il traffico, create mappe topologiche e tracciate la postura della rete nel tempo per la massima visibilità

Set di strumenti per l'analisi del traffico
Tracciate e analizzate le sessioni di rete archiviando o esportando tutto il dettaglio del traffico raccolto

Vantaggi

- Specializzato per applicazioni e protocolli industriali. Supporto nativo ad un'ampia gamma di protocolli OT, dispositivi industriali ed attacchi di rete. Possibilità di importare progetti esterni
- Regole preimpostate per la configurazione dei controlli di sicurezza
- Interfaccia intuitiva e report personalizzabili
- Completa consapevolezza dei rischi su tutta l'infrastruttura anche se distribuita
- Acquisisce campioni di traffico da più fonti: sensori di rete propri, sensori SD-WAN, sensori endpoint e sonde portatili

Ecosistema e integrazioni

Ecosistema
Sbloccate le estese capacità dell'ecosistema Kaspersky scegliendo l'integrazione con le seguenti soluzioni e il nostro approccio unificato alla cybersecurity multi-prodotto:

- Kaspersky Next XDR Expert
Per saperne di più

- Kaspersky IoT Secure Gateway (KISG)
Per saperne di più

- Kaspersky Machine Learning per il rilevamento delle anomalie (MLAD)
Per saperne di più

- Kaspersky Software-Defined Wide Area Network (SD-WAN)
Per saperne di più

Gestite tutti gli elementi dell'ecosistema tramite un'unica console

Integrazioni di terze parti
Compatibilità perfetta con una moltitudine di strumenti e piattaforme di sicurezza esterne

Rilevamento delle minacce e delle anomalie

Rilevamento delle intrusioni
Rilevamento basato sulla firma e un motore statistico che rileva tentativi di brute force o di scansione

Controllo dell'integrità della rete
Il sistema apprende le normali interazioni di rete fornendo allarmi per ogni deviazione

Rilevamento delle anomalie
Rileva anomalie di base a livello di pacchetto e di protocollo.
Può essere accompagnato da MLAD

DPI dei protocolli industriali
Mantiene il controllo dei processi e dei comandi e traccia in modo efficiente i dati di telemetria

Correlazione degli eventi
Associa gli eventi di sicurezza alla classificazione MITRE e a una singola kill chain

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 negli odierni sistemi di automazione digitale, gestiti e distribuiti. 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, dando visibilità agli amministratori dei sistemi di automazione che un incidente sia stato completamente gestito e che non si verificherà più.

Protezione degli endpoint

Prevenzione in tempo reale delle minacce
Scansioni personalizzate e on-demand per unità rimovibili e aree critiche per prevenire exploit e proteggere i file

Controllo delle attività locali
Funzionalità di controllo del dispositivo e del Wi-Fi. Assicurate integrità al progetto PLC per una piena consapevolezza delle attività locali

Controllo delle attività di rete
Gestite i firewall sugli host e garantite la protezione dalle minacce bloccando le sessioni di rete

Monitoraggio del sistema
Verificate l'integrità dei file, tracciate l'accesso al registro, rilevate le minacce nei registri di sistema per garantire la sicurezza del sistema operativo

Rilevamento e risposta degli endpoint

Rilevamento
Scansiona indicatori di compromissione (IoC), funzionalità complete di monitoraggio e reportistica

Risposta
Impedisce l'esecuzione, mette in quarantena/elimina file, avvia/termina processi, isola reti e altro ancora

Nodi Windows
Scanner portatile
Nodi Linux
Audit Agent

Scanner portatile

Scanner anti-malware
Scansioni anti-malware delle apparecchiature autonome e di tutti i computer introdotti nel sito industriale senza necessità di installazione

Scansione OVAL Applicate il criterio di sicurezza informatica su macchine autonome con scansioni manuali di vulnerabilità e conformità

Acquisizione dei pacchetti
Acquisite e analizzate il traffico di rete per ottenere la massima visibilità, anche su infrastrutture isolate

Inventario delle risorse di base
Raccogliete dati completi su hardware e software sfruttando una soluzione a impatto zero

Vantaggi

- Basso impatto sui dispositivi protetti, consumo di risorse ottimizzate
- Compatibilità con sistemi operativi legacy e fornitori di automazione industriale
- Configurazione di sicurezza di base e opzioni avanzate per proteggere gli host da qualsiasi tipo di minaccia
- Distribuzione modulare e impostazioni non invasive
- Supporto PLC: Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4; Schneider Electric Modicon M340, M580; dispositivi CODESYSV3; Fastwel CPM723-01
- Opzioni di licenza flessibili, da 1 mese a 5 anni
- Preimpostazioni di configurazione verificate ed efficienti per i sistemi industriali più diffusi

Gateway
Server Historian
Server SCADA
Workstation operatore
Sistemi integrati
Workstation di gestione del sistema
Workstation di programmazione

Piattaforma KICS e oltre

Cybersecurity unificata nei segmenti industriali e aziendali

OT XDR nativo

I componenti principali di Kaspersky Industrial Cybersecurity, KICS for Networks e KICS for Nodes, sono appositamente progettati per funzionare insieme in modo ottimale nel nostro ecosistema e offrire un'esperienza unificata e coesa. Se acquistati insieme, formano una piattaforma XDR nativa che offre ulteriori preziose funzionalità multiprodotto.

Gestione avanzata delle risorse

Inventario hardware degli endpoint
Visibilità completa su tutti i dispositivi connessi nell'infrastruttura a garanzia di un monitoraggio accurato delle risorse e di una migliore gestione della sicurezza

Inventario di applicazioni, utenti e patch
Informazioni dettagliate sulle distribuzioni software, sugli accessi degli utenti e sullo stato delle patch. Dati arricchiti per una corretta gestione e riduzione delle potenziali vulnerabilità

Monitoraggio del traffico degli endpoint
Monitoraggio continuo dei flussi di dati su ciascun endpoint per rilevare rapidamente schemi insoliti o potenziali minacce e garantire una risposta rapida alle attività sospette

Controlli di sicurezza

Scansione delle vulnerabilità
Esegue la scansione approfondita delle risorse per valutare i punti deboli della sicurezza, migliorare la consapevolezza del rischio, consentire una risposta tempestiva e rafforzare la complessiva strategia di sicurezza

Controlli di conformità
Controllo basato su agenti e senza agenti per la conformità agli standard di settore OVAL e XCCDF*. Un editor completamente funzionale, un database di report centralizzato, un contenitore protetto per le credenziali dei nodi e altro ancora

Controllo della configurazione
Garanzia di configurazioni di risorse sicure, monitoraggio delle modifiche contro i rischi di sicurezza e mantenimento dell'integrità di base per le risorse hardware e software

Detection and Response

Rilevamento
Identificazione delle minacce migliorata e semplificata tramite correlazione degli eventi host-rete da una singola vista sulla kill chain. Integrazione dei dati di avviso di rete per approfondimenti sugli incidenti

Risposta
Solida mitigazione delle minacce tramite prevenzione dell'esecuzione, isolamento dell'host e quarantena dei file. Le integrazioni con il firewall migliorano ulteriormente la capacità di rispondere in modo rapido ed efficace agli incidenti di sicurezza

OT XDR aperto

Ampliate la funzionalità delle soluzioni EDR con un motore di correlazione, risposte automatiche e connettori di terze parti. Potenziate la piattaforma KICS con la soluzione Kaspersky XDR Core per sbloccare:

- Monitoraggio completo e correlazione degli eventi di sicurezza informatica (SIEM), integrazione con diversi sistemi
- Gestione e integrazione della threat intelligence

Convergenza IT-OT XDR

Andate oltre e abbracciate la convergenza definitiva IT-OT. Combinate la piattaforma KICS con il nostro pacchetto Kaspersky Next XDR Expert, sfruttate la funzionalità Kaspersky di protezione degli endpoint per ottenere i seguenti vantaggi:

- Un singolo grafico di indagine, uso di playbook e gestione degli incidenti tramite Kaspersky Single Management Platform
- Protezione avanzata per l'infrastruttura IT (IT XDR)

XDR industriale

Kaspersky Industrial CyberSecurity

Per saperne di più

Kaspersky Single Management Platform

XDR aziendale

Kaspersky Next XDR Expert

Per saperne di più

* XCCDF (Extensible Configuration Checklist Description Format)

Oltre 27 anni di esperienza e petabyte di dati sulle minacce

ICS CERT

ICS CERT: divisione internazionale di ricerca nell'ambito della sicurezza IoT/OT

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

Oltre 200 certificati di compatibilità con soluzioni da fornitori di automazione

Comprovata efficacia della tecnologia, conformità agli standard e ai requisiti

Clienti in tutto il mondo

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Per saperne di più

www.kaspersky.it

#kaspersky
#bringonthefuture