06.03.24 | 11.00 WEBINAR

Sicurezza delle Infrastrutture Industriali, priorità per la continuità produttiva

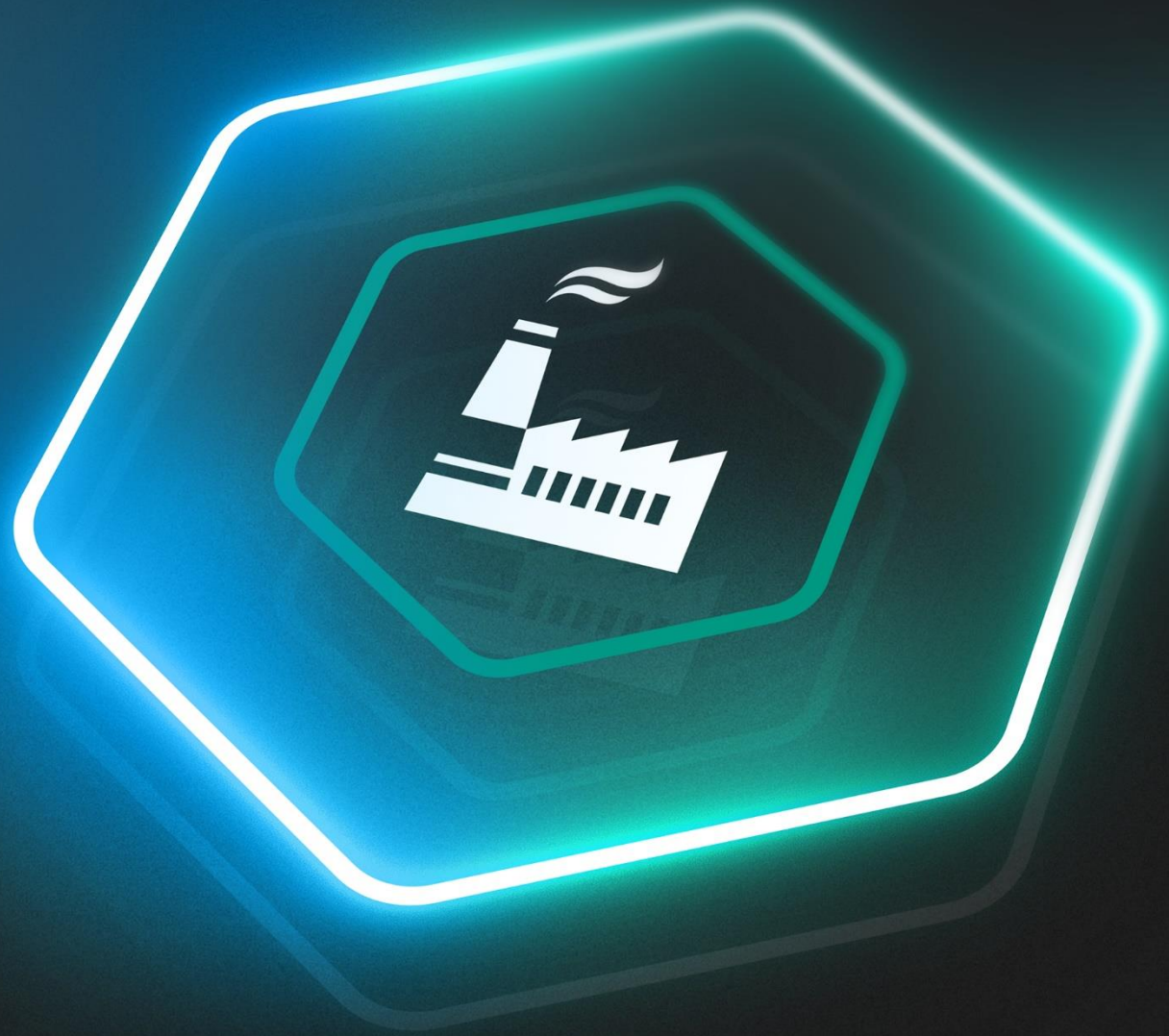
Kaspersky Industrial CyberSecurity

Simone Mulattieri

Senior Presales Manager

kaspersky

Kaspersky Industrial CyberSecurity



kaspersky

NIS 2.0

La Direttiva NIS 2 (2022/2555) è entrata in vigore dal 17 gennaio 2023 e gli Stati Membri dovranno attuarla entro il 17 ottobre 2024.

Tra i vari obiettivi, la direttiva NIS 2 richiede agli operatori dei settori chiave di mettere in atto **misure di sicurezza** e di riportare eventuali incidenti.

- **Gestione degli incidenti**
- **Formazione**
- **Efficaci misure di cybersecurity**
- **Gestione dei rischi/vulnerabilità**

Come possiamo iniziare a prepararci?

- Valutare se e in che misura si è soggetti agli obblighi di cybersecurity previsti dalla Direttiva NIS 2.
- Seguire le informazioni e le raccomandazioni delle autorità di sicurezza informatica Nazionali.
- Valutare e successivamente sviluppare le misure tecniche, operative e organizzative per gestire i rischi connessi alla sicurezza dei sistemi di rete e informativi.

kaspersky

IT-OT Convergence

Kaspersky
OT CyberSecurity

Kaspersky
Extended Detection
and Response

Technologies

Specialized Solutions

- Kaspersky Antidrone
- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity

- for Nodes — Endpoint protection, detection and response
- for Networks — Network Traffic Analysis, Detection and Response

KICS XDR

KasperskyOS solutions

- Kaspersky IOT Secure Gateway
- Kaspersky Secure Remote Workspace
- Kaspersky Automotive Secure Gateway

Knowledge

Cyber hygiene

- Kaspersky Security Awareness

Threat intelligence

- Kaspersky ICS Threat Intelligence

Training

- Kaspersky ICS CERT Training

Expertize

Discovery

- Kaspersky ICS Security Assessment

Managed Service

- Kaspersky Incident Response Readiness

Response

- Kaspersky Managed Detection and Response

kaspersky

Piattaforma XDR nativa per la protezione dei sistemi di automazione industriale

kaspersky

Kaspersky Industrial CyberSecurity for Nodes

Protezione endpoint all-in-one di livello industriale, Agente EDR e sensore endpoint

kaspersky

KICS for Nodes. Opzioni e applicazione

Windows

Portable Scanner

Linux

Audit Agent

Gateway

Engineering workstation

Historian Server

System management workstation

SCADA server

Embedded systems

Operation workstation

Punti chiave

Kaspersky Industrial CyberSecurity for Nodes

- Compatibilità* con i Vendor di automazione Industriale
- Supporto SO Legacy da Windows XP SP2
- Modalità non-blocking (statistic mode) disponibile
- Nessun reboot (installazione, update o upgrade)
- Air-gapped database update
- Soluzioni sviluppate per OT
- Consumo di risorse di sistema personalizzabili

* Maggiori info: **certification**

kaspersky

KICS for Nodes. Componenti

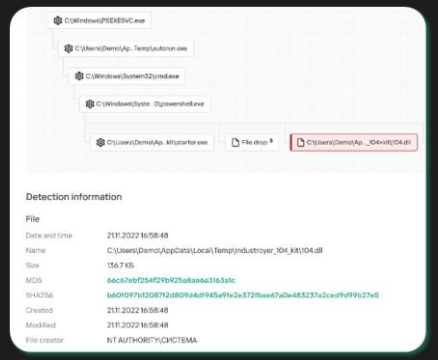
Windows Nodes

- Anti-Malware
- Application Launch Control
- 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
- Portable Scanner
- Security Audit
- EDR Agent
- Endpoint Sensor (Integration with KICS for Networks)

Industrial Endpoint Protection

kaspersky

KICS for Nodes. EDR Agent



Kaspersky Industrial CyberSecurity for Nodes

EDR

EDR telemetry

Management & Response

Alerts

Kill-chain

Kaspersky Single Management Platform

Kaspersky Industrial CyberSecurity for Networks

Endpoint Detection and Response (EDR) a livello industriale

Gestibile dalla Single Management Platform (ICS EDR) e KICS for Networks come parte della piattaforma OT XDR

Capacità EDR in aggiunta all'EPP dedicato al mondo industrial a partire da Win XP SP2

Strumenti investigativi di sicurezza

Risposta rapida a minacce complesse ed evasive prima che si verifichino danni

Detection e telemetria per l'analisi della root-cause:

- File, processi, registri e telemetrie delle comunicazioni network
- Visualizzazione delle Alert kill-chain
- Indicatori di Compromissione

Opzioni di Risposta:

- Prevent execution
- Quarantine file
- Isolate host
- IoC Scan / Retro-Scan

kaspersky

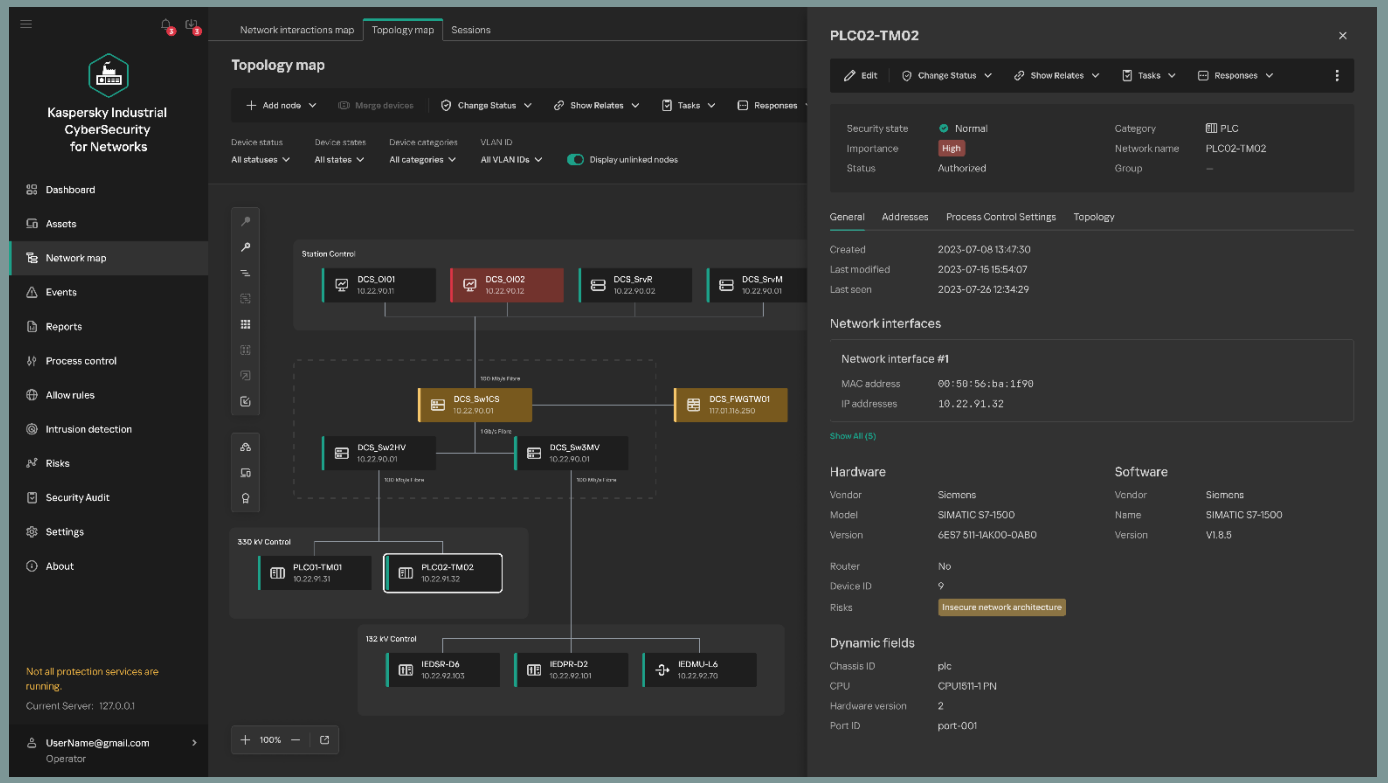
Kaspersky Industrial CyberSecurity for Networks

Discovery e visualizzazione delle reti industriali, gestione del rischio e rilevamento delle minacce

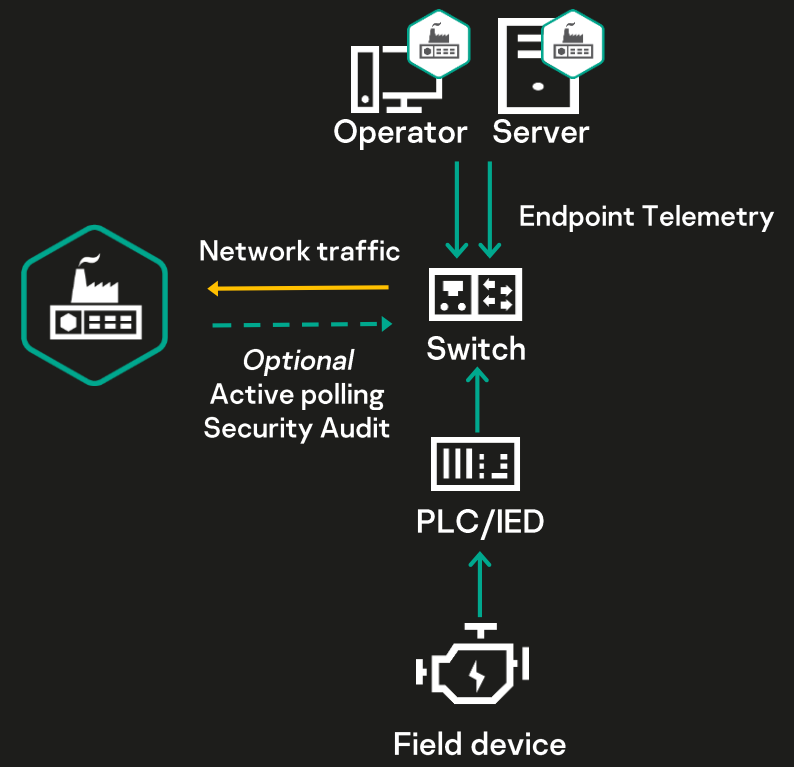
kaspersky

Interfaccia di KICS for Networks e modalità di deploy

Software o virtual appliance



Analisi del Traffico di rete, Detection & Response



Connessione passiva alla network ICS

kaspersky

KICS for Networks. Tecnologie

Kaspersky Industrial CyberSecurity for Networks

XDR

- Eventi correlati della rete e degli endpoint.
- Arricchimento degli eventi di rete con le telemetria degli endpoint.
- Rilevamento avanzato delle minacce + visualizzazione kill-chain.
- Disponibilità di task di risposta.

Asset Inventory

- Inventario automatico degli asset e raccolta dati utilizzando metodi passivi e attivi.

Network Inventory & Visualization

- Mappa delle comunicazioni di rete.
- Diagramma della topologia di rete.

Vulnerability & Risk Assessment

- Vulnerabilità OT e gestione del rischio.
- Risk score e priorità automatici.
- Consigli per la risoluzione dei rischi.
- Link alle risorse dei fornitori ICS.

Network Anomaly Detection

- Controllo dell'integrità della rete con monitoraggio della variazione dalla baseline e rilevamento di attività di rete dannose e/o sospette.

OT Process Control & Deep Packet Inspection

- Estrazione dei dati dai payload industriali.
- Controllo del processo in tempo reale.
- Controllo dei comandi industriali.
- Monitoraggio avanzato dei processi OT da parte di Kaspersky MLAD.

Integration & Data Exchange

- Informazioni centralizzate.
- Integrazione con Kaspersky e terze parti o sistemi interni (IEC 104, OPC, CEF, Syslog, API-based connector).

kaspersky

Security Audit

Security audit per Windows e Linux, network device

Task di gruppo o singoli, eseguibili manualmente o schedulati

Editor funzionale completo per controlli dei parametri di conformità

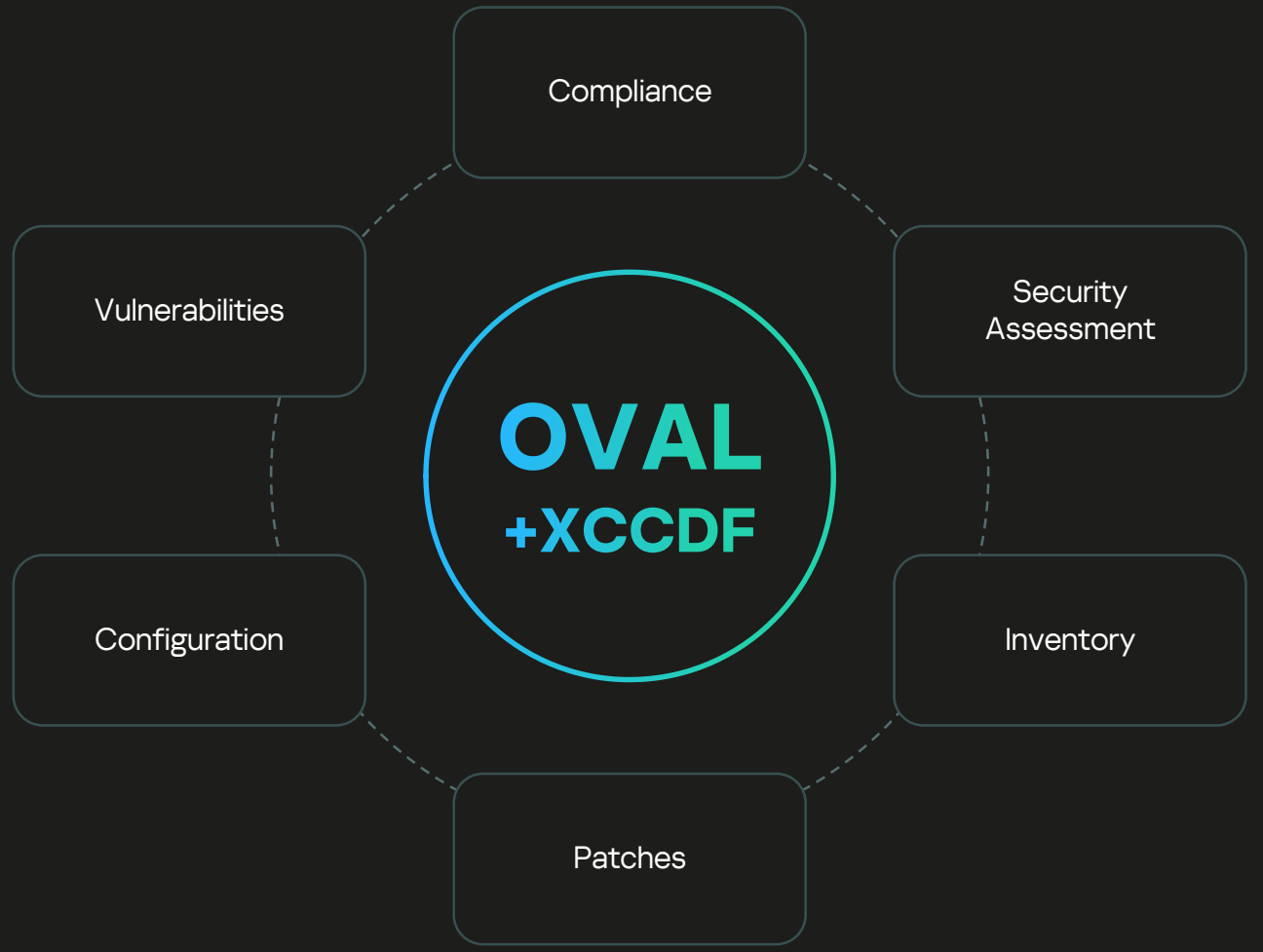
Database delle vulnerabilità SCADA integrato, fornito da Kaspersky ICS CERT

Industry standard – Open Vulnerability and Assessment Language (OVAL) + XCCDF

Supporta qualsiasi database OVAL di terze parti o personalizzato

Tutti i report, la cronologia dei risultati delle valutazioni e i dati effettivi sulle risorse in un unico posto

Gestore delle credenziali protetto per audit senza agenti



kaspersky

Scenari futuri cross-product

KICS + MDR

- Protezione gestita 24 ore su 24 contro le minacce evasive odierne.
- Flessibilità per adattarsi ad ogni settore industriale ed esigenza organizzativa.
- Investimento in sicurezza OT conveniente e giustificato in termini di costi/benefici.

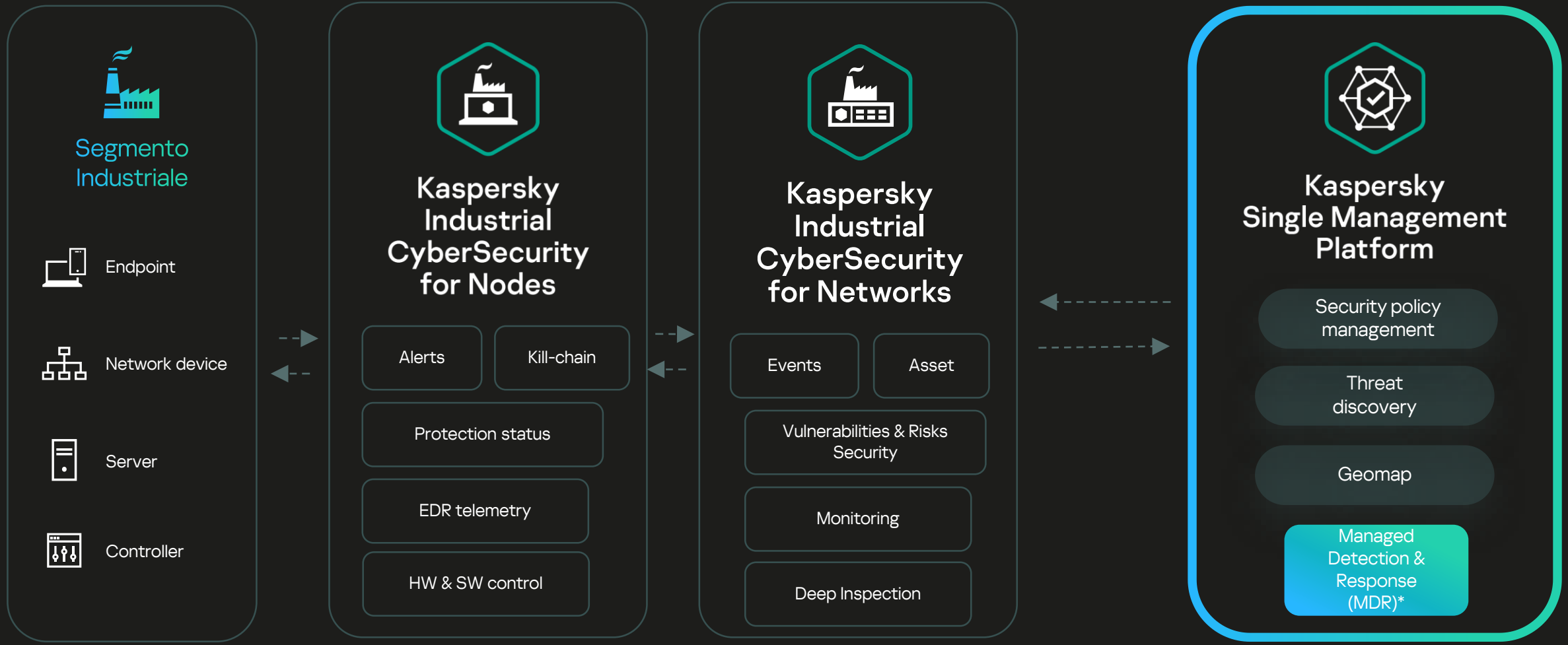
KICS + SD-WAN

- Facile scalabilità.
- Gestione efficace.
- Ottimizzazione dei costi.
- Sicurezza centralizzata.

kaspersky

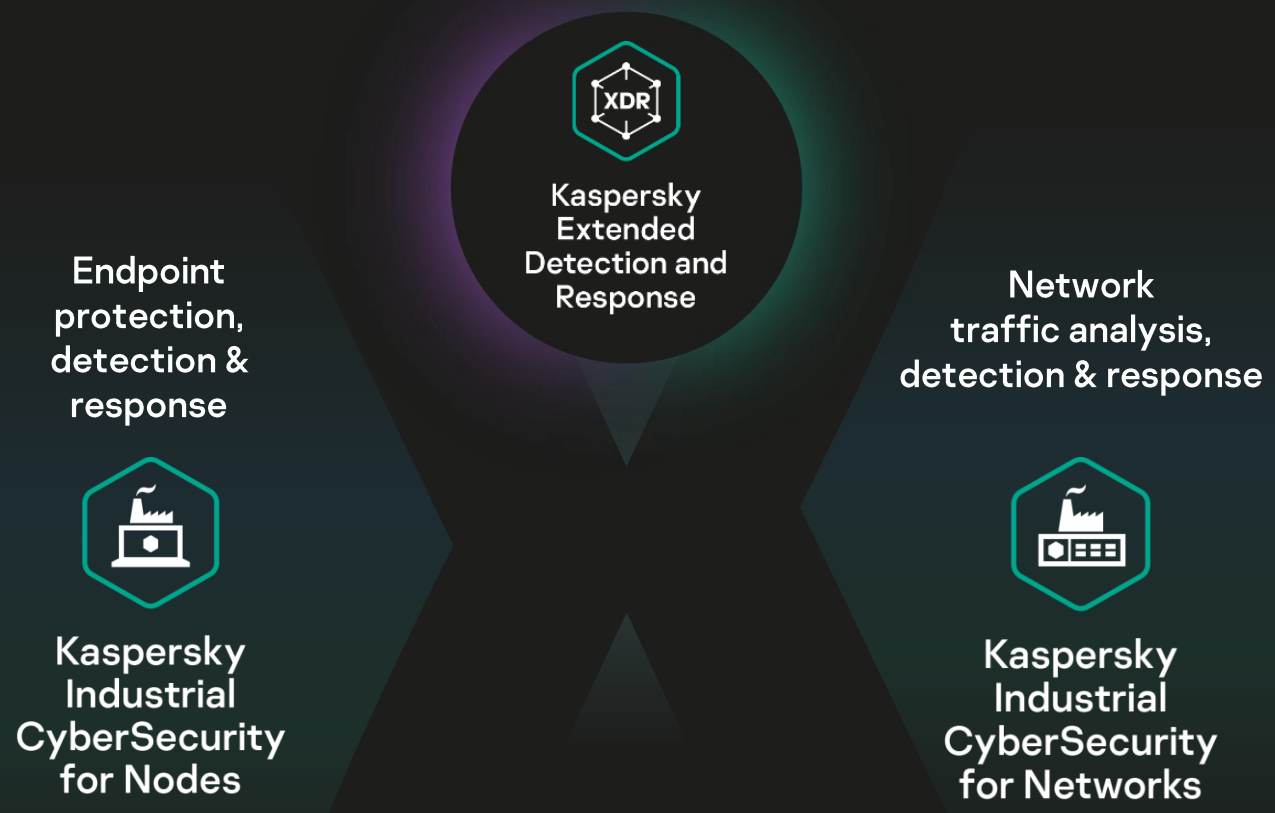
Integrazione avanzata

XDR



* Lancio previsto nel corso del 2024

Composizione KICS XDR



- Singola console
- Integrazioni native
- Scenari cross-product
- Asset inventory & visibility
- Threat Detection
- Kill-chain investigation
- Azioni di risposta
- Security Audit

kaspersky