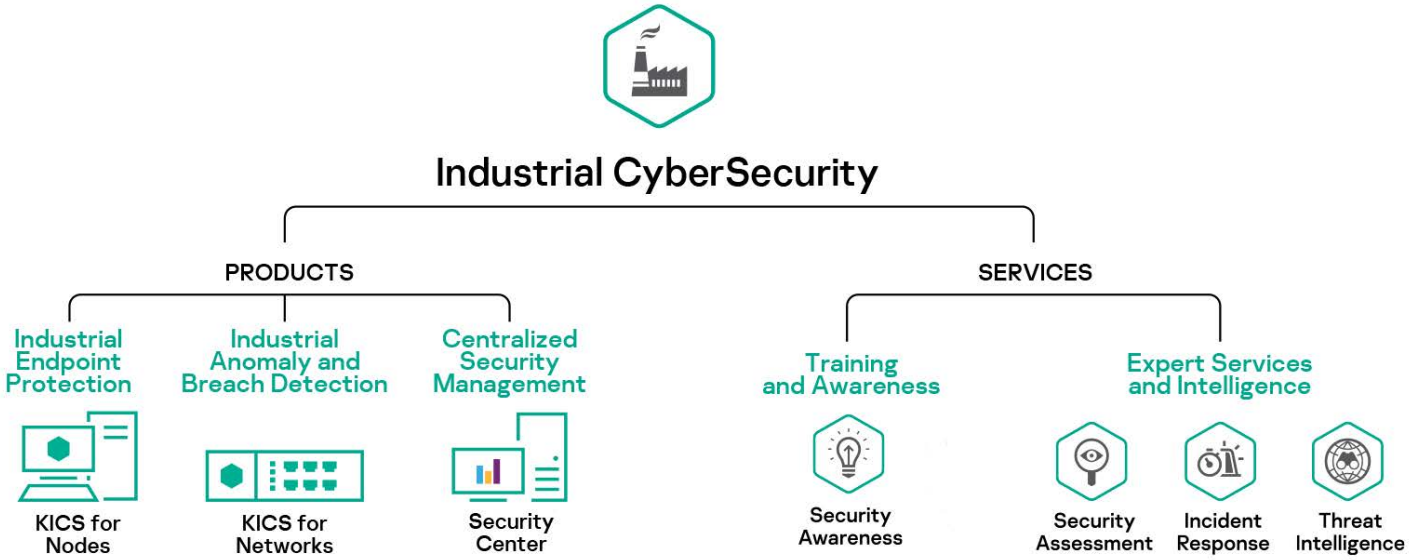
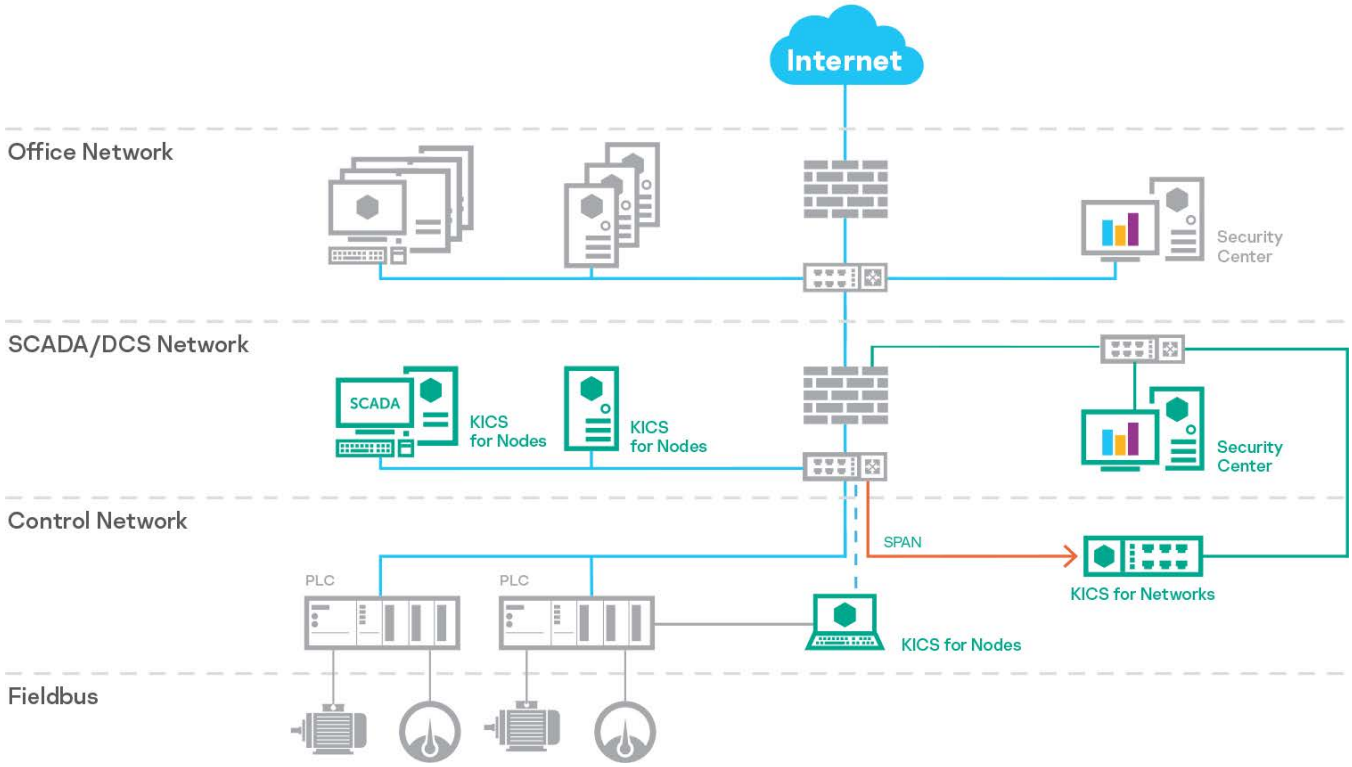
Prodotti

I prodotti KICS sono progettati per proteggere in modo completo gli elementi industriali dell'organizzazione: KICS for Nodes è rivolto agli endpoint industriali, mentre KICS for Networks monitora la sicurezza della rete industriale.



Esempio struttura soluzioni KICS



KICS for Networks

I benefici:

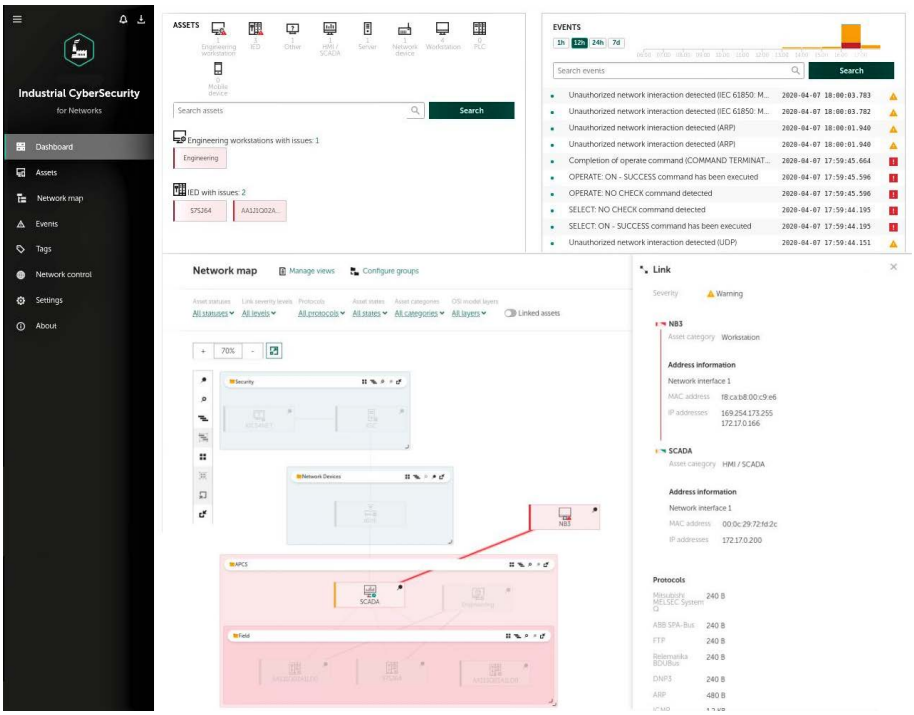
- **Asset discovery**
  Identificazione e inventario passivo degli asset OT
- **Deep packet inspection**
  Analisi quasi in tempo reale delle telemetrie dei processi tecnici
- **Network integrity control**
  Rilevamento di host e flussi di rete non autorizzati
- **Intrusion detection system**
  Invia avvisi su attività di rete dannose
- **Command control**
  Ispeziona i comandi dei protocolli industriali
- **External systems**
  Capacità rilevamento esterno tramite integrazione API
- **Machine learning for anomaly detection (MLAD)**
  trova anomalie cyber o fisiche grazie a in telemetria in tempo reale e data mining dello storico (ricorrente rete neurale)

KICS for Networks rileva anomalie e intrusioni già dalle loro fasi iniziali all'interno delle reti ICS (Industrial Control System) e garantisce che vengano intraprese le azioni necessarie per prevenire qualsiasi anomalia che possa impattare negativamente sui processi industriali.

KICS for Networks è una soluzione indipendente dal fornitore dei dispositivi industriali.

L'interfaccia KICS for Networks visualizza un dashboard in tempo reale e una mappa di rete, che consente di intervenire sulle risorse ed eventi di sicurezza.

Esempio di KICS for Networks appliance e Interfaccia



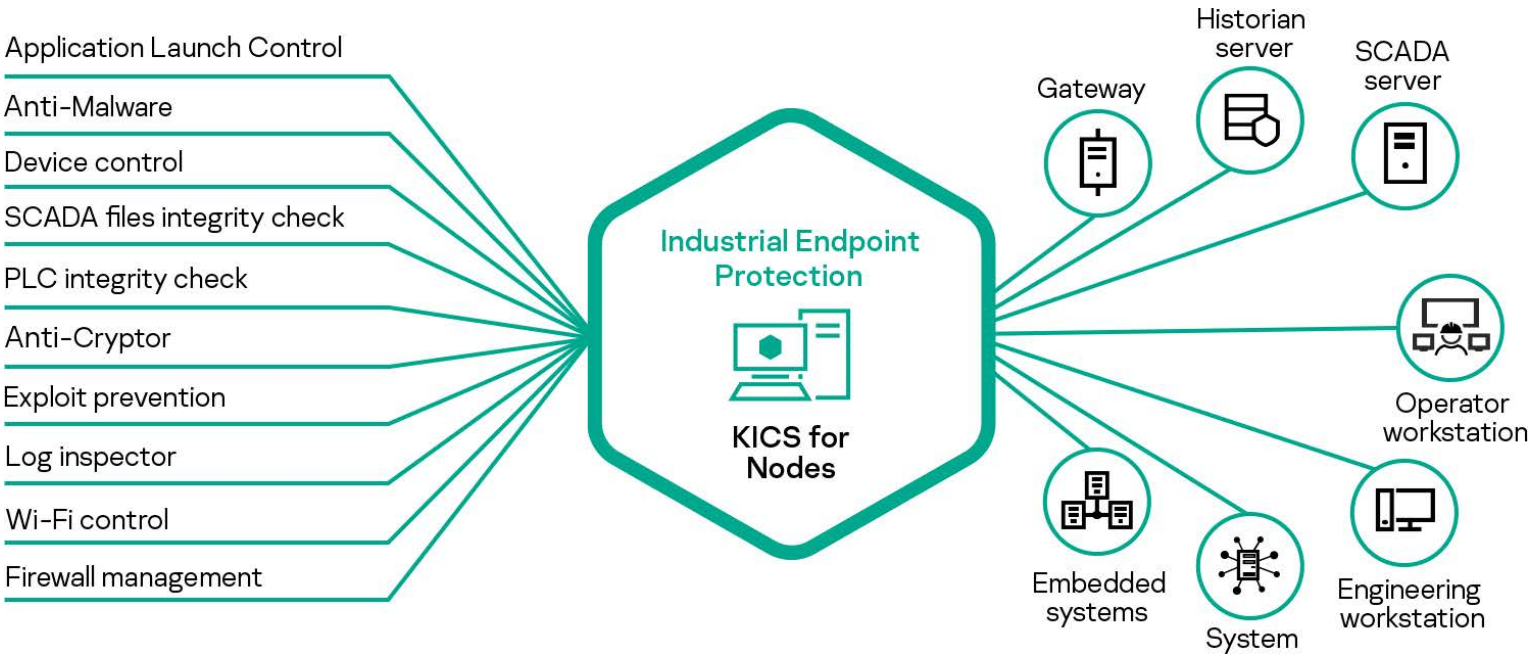
KICS for Nodes

I benefici:

- Basso impatto sui dispositivi protetti
- Massima compatibilità (es. SCADA, PLC, DCS)
- Supporto Microsoft Windows e Linux
- Protezione Malware avanzatoControllo dell'ambiente

KICS for Nodes è stato appositamente progettato per un consumo minimo risorse. Costruito per sistemi di sicurezza e embedded, la sua architettura modulare permette di installare solo i componenti protettivi desiderati.

I componenti protettivi possono essere configurati per la modalità di prevenzione delle minacce o in modalità di solo rilevamento. Questo approccio è ideale per sistemi legacy, macchine a basse prestazioni che richiedono il massimo della potenza di calcolo disponibile.



Security Center

Security Center è una soluzione centralizzata di gestione della sicurezza. Fornisce il controllo e la visibilità dei processi industriali anche su più siti.

- **Gestione dei sistemi**
  - Raccolta dati di sistema centralizzata
  - Distribuzione del Software centralizzata
  - Rilevamento delle vulnerabilità e gestione delle patch
  - Capacità di gestione di molteplici client
- **Gestione delle politiche**
  - Gestione delle politiche di sicurezza centralizzata
  - Pianificazione ed esecuzione di attività a distanza
- **Integrazione dashboard MES**
  - Stato di sicurezza e trasferimento delle informazioni a host compatibili IEC 104/OPC 2.0
- **Segnalazione e notifica**
  - Registrazione degli eventi
  - Dashboard e report
  - Notifiche SMS/e-mail
- **HMI integration**
- **Integrazione SIEM**
  - Arcsight, Splunk, Qradar
  - Syslog server

Servizi Industrial Cybersecurity

Industrial Cybersecurity Assessment

Valutazione della sicurezza informatica della struttura industriale, compresi penetration test esterni e interni di soluzioni OT e di automazione. Vengono forniti approfondimenti e raccomandazioni su come rafforzare la sicurezza informatica della struttura ICS.

Threat Intelligence

Analisi aggiornate raccolte da esperti aiutano a migliorare la protezione da attacchi informatici industriali mirati. Fornito come TI feed o report personalizzati, possono soddisfare specifiche esigenze in base al parametri software regionali, industriali e ICS.

Incident Response

In caso di incidente di sicurezza informatica, i nostri esperti raccoglieranno e analizzeranno i dati, ricostruiranno la sequenza temporale dell'incidente, determineranno le possibile fonti e motivazioni, e svilupparanno un piano di riparazione. Viene offerto inoltre un servizio di analisi del malware in cui gli esperti classificheranno qualsiasi campione malware fornito, analizzandone le funzioni e il comportamento per sviluppare raccomandazioni e un piano per la sua rimozione dai sistemi e per annullare eventuali azioni dannose.

Industrial Cybersecurity awareness training

Formazione On-site, moduli interattivi online e simulazione di scenari relativi a sicurezza informatica per coloro che interagiscono con i sistemi informatici industriali. I partecipanti otterrano una visione aggiornata dell'attuale panorama delle minacce e vettori di attacco che prendono di mira specificamente ambienti industriali, esplorando scenari pratici e acquisendo capacità di lavoro cybersafe.