

Attività selettiva per la visibilità OT completa

Riduzione della mancata conformità e taglio dei costi con le attività di conformità automatica su vasta scala

Le parti interessate e i titolari delle risorse ICS per la sicurezza informatica della tecnologia operativa (OT) possono avere punti ciechi nell'ambito della propria rete che una soluzione di sicurezza informatica ICS completamente passiva non è in grado di risolvere. Informazioni incomplete sulle risorse e visibilità sui dispositivi possono lasciare le reti esposte a un rischio informatico e operativo elevato.

Con il sensore attivo eyeInspect, i titolari delle risorse OT dispongono dei dati contestuali sul dispositivo necessari per semplificare l'analisi delle minacce con meno dashboard e più avvisi fruibili, per un'analisi più efficace e una conformità su vasta scala.

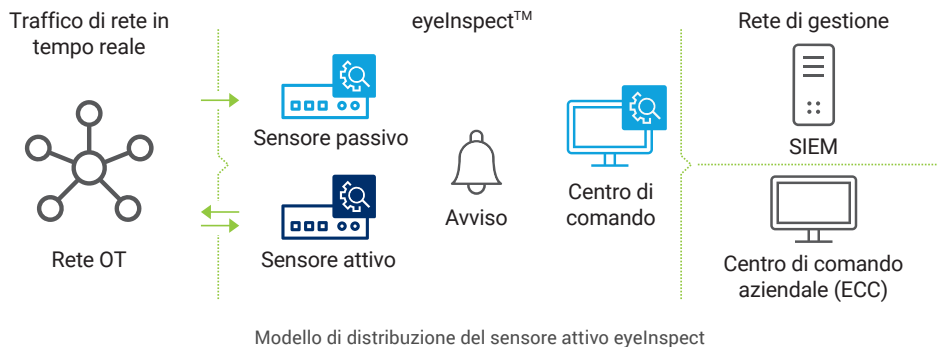
Il 79% delle organizzazioni con una rete SCADA/ICS ha subito una violazione negli ultimi 24 mesi. ¹

FORRESTER



Sensore attivo eyeInspect: vedere ogni cosa

Il sensore attivo eyeInspect (già SilentDefense™) unisce il rilevamento passivo delle anomalie con le capacità di sicurezza informatica attive per estendere in modo non intrusivo la visibilità di rete ICS e le informazioni operative. Fornito come componente separato e opzionale, il sensore attivo eyeInspect interroga selettivamente host specifici in base a una o più caratteristiche estese di inventario delle risorse. Questo livello di visibilità aggiuntivo migliora anche sensibilmente il monitoraggio della conformità e le attività di segnalazione con la funzione di confronto con i valori di riferimento delle risorse.



SENSORE ATTIVO EYEINSPECT

- Stabilisce i requisiti standard di risorse e gruppi di risorse a fronte dei criteri di conformità per le verifiche di conformità automatiche e on demand.
- Automatizza le verifiche di conformità e la documentazione per NERC CIP e altri framework di conformità.
- Fornisce un inventario dettagliato delle risorse e informazioni sul fingerprinting dei dispositivi come patch installate, applicazioni installate o porte aperte e servizi.
- Migliora la sensibilizzazione situazionale delle reti OT e ICS.
- Tutela le apparecchiature sensibili utilizzando criteri di scansione specifici per OT del sensore attivo.

Casi d'uso del sensore attivo

Rilevamento completo sui dispositivi e sulle reti

Il sensore attivo eyeInspect interroga in modo sicuro e selettivo host specifici sulla rete ICS per potenziare la visibilità sulle risorse e fornire inventari più completi che includono, a titolo indicativo, stato dell'host, versione del sistema operativo, fabbricante, software e applicazioni, numeri di serie, comportamento utente di rete e patch installate.

Valutazione completa di rischio e vulnerabilità

Un processo automatico non intrusivo di raccolta di informazioni sulle minacce consente alle parti interessate in ambito di sicurezza informatica di valutare i rischi e le vulnerabilità potenziali ancora più nel dettaglio. Il sensore attivo eyeInspect arricchisce i dettagli di avviso con preziosi dati contestuali che non sarebbero diversamente stati visibili unicamente con una soluzione passiva.

Confronto con i valori di riferimento delle risorse e automazione della conformità

Il sensore attivo eyeInspect consente il confronto con i valori di riferimento delle risorse e permette così agli utenti di confrontare le singole risorse e i gruppi di risorse a fronte di specifici criteri normativi e misure di conformità, come NERC CIP 007 e 010. Con il sensore attivo eyeInspect, gli utenti possono esportare selettivamente tutte le informazioni per creare facilmente una documentazione periodica dello stato della rete, consentendo di ridurre i costi di esercizio e il rischio di sanzioni pecuniarie per violazione della conformità in base a standard quali NERC CIP e la Direttiva NIS.

Vedere non basta.
Bisogna proteggere.

Contattaci oggi stesso per difendere subito il tuo ambiente EoT.

forescout.com/platform/eyeInspect

info-italia@forescout.com

Tel. (internazionale) +1-408-213-3191