Contributo dei laboratori

Metodologico

Dal rischio astratto a una valutazione fondata su evidenze

- La valutazione si basa su evidenze tecniche osservabili e misurabili
- Le evidenze raccolte alimentano roadmap di miglioramento che integrano sicurezza, resilienza e adeguamento
- Sperimenta l'integrazione tra sicurezza, resilienza e conformità superando l'attuale impostazione: la sicurezza come questione tecnica, la resilienza come business continuity, la conformità come adempimento normativo.

Operativo

Dalla sperimentazione alla capacità di governo e resilienza

- Permette test-before-invest, Proof of Concept, esercitazioni e simulazioni di incidente senza introdurre rischi sulla linea produttiva.
- Supporta la valutazione della resilienza misurando rilevazione, comunicazione, risposta e tempi di ritorno a livelli accettabili di servizio
- Favorisce la collaborazione tra imprese, PA, fornitori, integratori, partner tecnologici e ricerca in un contesto neutro.

Contributo dei laboratori InrimaONE

Governance, monitoraggio e controllo

Un unico punto di controllo per conformità, rischio, allarmi e reporting.

Assessment di Conformità

Gap analysis automatizzata rispetto ai requisiti NIS2, con identificazione delle priorità d'intervento.

Gestione del Rischio

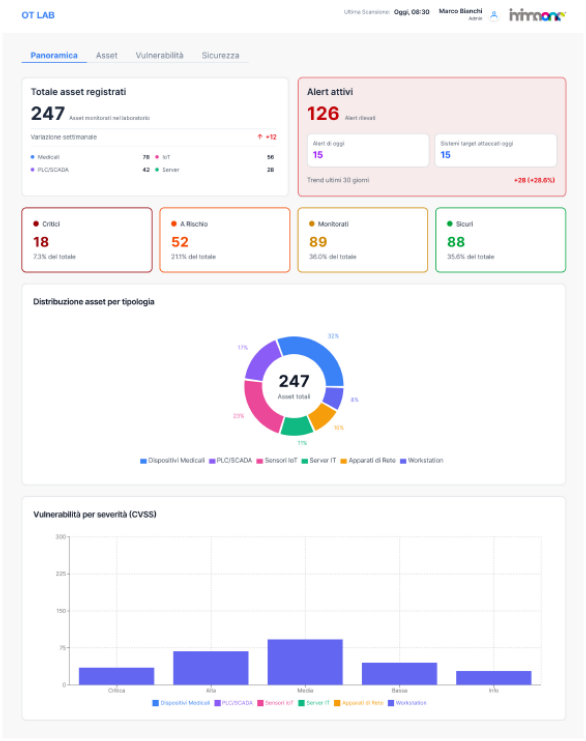
Monitoraggio continuo delle vulnerabilità e sistema integrato di incident management.

Allarmi

Alert raccolti dai sistemi diversi e presentati in un'unica dashboard.

Cruscotti di Controllo

Dashboard interattive con KPI di conformità e reportistica automatizzata per audit interni ed esterni.



I servizi del laboratorio

Dalla valutazione del rischio alla protezione operativa: un'offerta integrata per la sicurezza IT/OT

CONOSCERE E VALUTARE

- CyberSecurity Assessment Organizzativo
- **CyberSecurity Assessment Operativo**
- Professional Advice: NIS2, CRA, ISO/IEC
- Security Awareness
- Incident Readiness

PROTEGGERE E MONITORARE

- Progettazione ed implementazione di soluzioni di sicurezza (NGFW, PAM, CASB…)
- Asset Management IT/OT
- Network Protection & Monitoring
- Deception
- Microsegmentation
- Dark Web Monitoring
- **IT/OT SOC**

RISPONDERE E RIPRISTINARE

- CSIRT – **Incident Handling & Response** IT/OT
- Penetration Test
- Vulnerability Management (identificazione E patching)
- Recovery