

La qualità Schmersal entra nel campo della Security

OT CYBERSECURITY PRODOTTI E SERVIZI

NEW



OT CYBERSECURITY

PRODOTTI

ROUTER VPN E FIREWALL



1



ROUTER VPN

eWon Cosy

- Segregazione del traffico LAN della macchina
- Controllo locale della connettività remota da parte dell'utente finale, con interruttore a chiave esterno
- Aumento della sicurezza grazie all'uscita digitale che segnala una connessione attiva da remoto
- Connessioni in uscita non intrusive che non richiedono modifiche alla rete esistente

2



FIREWALL

Stormshield SNI2.0

- Sicurezza operativa (hardware, bypass e alimentazione ridondata)
- Adatto per ambienti operativi difficili (guida DIN, IP30)
- Manutenzione remota in tutta sicurezza delle vostre macchine e dei vostri dispositivi (VPN SSL / IPsec)
- Protezione delle comunicazioni di rete (DPI, IPS/IDS, Packet Filtering)

3



SMART FIREWALL

Anybus Defender

- Router e firewall
- Interfaccia grafica
- Security by design
- Learning mode



SCHMERSAL
THE DNA OF SAFETY

OT CYBERSECURITY

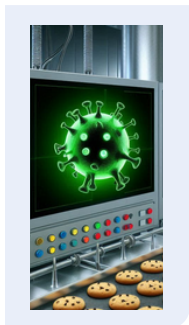
SERVIZI

FORMAZIONE BASE E AVANZATA

CORSO SECURITY OT

Durata 8h - Fruizione: in presenza (anche presso i clienti), online.

Dedicato alla sicurezza informatica delle apparecchiature OT/ICS, fornisce le nozioni di base per il personale coinvolto nella progettazione e gestione degli impianti.



Introduzione alla Cyber Security OT

L'impatto della sicurezza informatica - Gli scenari e le tecnologie - Terminologia
Le caratteristiche delle applicazioni ICS e SCADA

Gli aspetti della sicurezza informatica

Quali sono gli obiettivi di un attacco - Le diverse tipologie di attacchi
I rischi per l'Azienda - Il ruolo del personale, interno ed esterno - Le vulnerabilità dei prodotti di Automazione - Esempio d'uso tramite laboratorio virtuale

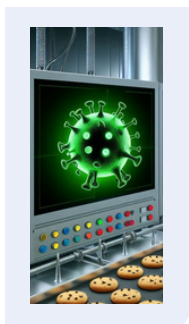
Gli strumenti di protezione

La sicurezza del Sistema Operativo e delle periferiche - L'analisi delle vulnerabilità e il penetration testing
La gestione unificata del rischio tramite sistemi SIEM e UTM

CORSO SECURITY OT AVANZATO

Durata 8h - Fruizione: in presenza (anche presso i clienti), online.

Dedicato alla sicurezza informatica delle apparecchiature OT/ICS come risultato di oltre 20 anni di esperienza su sistemi SCADA, PLC, DCS. Affronta in modo approfondito i temi della cybersecurity applicata al contesto industriale.



Le basi del networking e della sicurezza

Tipologie di reti e zone - Gli elementi di una rete
I protocolli di comunicazione sicuri - Concetti base di crittografia e hashing

La protezione dell'impianto – Secure Network Architecture

Segmentazione, segregazione e isolamento delle reti - La virtualizzazione
Tunneling e VPN - Il monitoraggio dell'architettura OT/ICS

Le best practices

Decalogo della sicurezza - La normativa IEC62443
Il processo di "Incident Response"

OT CYBERSECURITY

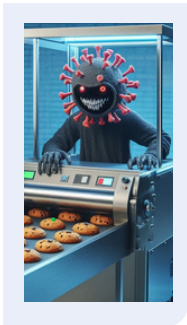
SERVIZI

SECURE PLC & ASSESSMENT

CORSO SECURE PLC PROGRAMMING

Durata 8h - Fruizione: in presenza (anche presso i clienti), online.

Comprendere gli aspetti della cybersecurity specifici per le applicazioni OT, Individuare i potenziali rischi cyber di un impianto di automazione.

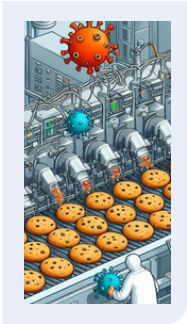


La programmazione sicura del PLC

- Programmazione modulare e strutturata
- Monitoraggio del funzionamento corretto del PLC
- Gestione sicura del ciclo di esecuzione del programma e di ripristino
- Gestione e ottimizzazione della memoria del PLC
- Check di integrità del software e dei dati
- Validazione di input/output e delle risorse interne (timers, counters, blocchi funzione) Interazione sicura con dispositivi HMI e SCADA
- Monitoraggio, log e gestione di alerts ed eventi
- Comunicazione sicura con altri device

CONSULENZA PER OEM E SYSTEM INTEGRATOR

Il Security Assessment è fondamentale per valutare l'attuale postura di sicurezza dell'azienda e dei macchinari



Assessment interno

- Controlla se i processi di sicurezza sono presenti, documentati e applicati
- Controlla se l'azienda è pronta a reagire ad un incidente di sicurezza
- Valuta se l'azienda è in grado di identificare ed analizzare anomalie
- Controlla se gli utenti sono formati su come segnalare potenziali rischi di sicurezza
- Verifica che l'azienda sia compliant con le normative in materia di cybersecurity

Assessment dei macchinari per la marcatura CE

- Controlla se i processi di sicurezza sono presenti, documentati e applicati
- Verifica la loro corretta configurazione, la segmentazione della rete, la gestione utenti
- Verifica conformità ai requisiti della norma IEC 62443.
- Verifica che la macchina sia compliant con le normative in materia di cybersecurity

CONSULENZA PER CLIENTI FINALI

- Controlla se i processi di sicurezza sono presenti, documentati e applicati
- Controlla se l'azienda è pronta a reagire ad un incidente di sicurezza
- Valuta se l'azienda è in grado di identificare ed analizzare anomalie
- Controlla se gli utenti sono formati su come segnalare potenziali rischi di sicurezza
- Verifica che l'azienda sia compliant con le normative in materia di cybersecurity