Corso - 06/05/2025

Cybersecurity per l'automazione industriale

Norme, minacce e come difendersi

Obiettivi

Il corso fornisce una panoramica approfondita sulla Cybersecurity, con particolare attenzione ai sistemi industriali e alle nuove normative di settore.
Si analizzeranno i metodi e gli strumenti per identificare le minacce, valutare le vulnerabilità ed implementare strategie di difesa efficaci nei contesti OT.
L'obiettivo è quello di rendere i partecipanti consapevoli delle sfide della sicurezza informatica e fornire loro strumenti concreti per proteggere infrastrutture e impianti industriali.

Programma

6 Maggio - 9.00-13.00, online.

- Dalla Safety alla Cybersecurity: l'evoluzione della sicurezza nelle macchine industriali e nei sistemi robotizzati.
- Nuove Regolamentazioni:
    - Nord America: il National Electrical Code (NEC 2023)
    - Europa: il Nuovo Regolamento Macchine e le norme di Tipo C
- Confronto tra Approcci Europei e Nord Americani: requisiti essenziali per la connessione sicura di macchine e impianti.
- Norme EN di Tipo C: impatti della cybersecurity su robot industriali e macchine per il packaging.
- Connessione Sicura di Macchinari e Impianti: Best Practice e Soluzioni.
- Casi Pratici e Applicazioni sul Campo.

7 Maggio - 9.00-13.00, online.

- La digitalizzazione e la Cybersecurity.
- Minacce, Attaccanti e Impatti.
- Trend Attuali in Cybersecurity.
- Introduzione alla Direttiva NIS2.
- Strategie di Difesa e Best Practice.
- Caso di Studio: Phishing, cos'è e come proteggersi.

9 Maggio - 9.00/18.00 C/O Villa Marchetti, Modena.

- Introduzione ai Sistemi Cyber-Fisici e differenze con l'IT.
- Sistemi di Controllo Industriale nell'Industria 5.0 (architettura, componenti, attacchi storici, requisiti, minacce).
- Esposizione e Vulnerabilità nei Sistemi Industriali.
- Lo Standard IEC 62443 e la sicurezza OT.
- Analisi del Rischio nei Sistemi Industriali.
- Difesa e Best Practice per la sicurezza OT.
- Laboratorio VAPT
    - Introduzione alle vulnerabilità
    - Stima di una vulnerabilità (CVE e CVSS)
    - Introduzione al Vulnerability Assessment: Processo, Strumenti e Scansioni
    - Introduzione al Penetration test: Cos'è e metodologie
    - Sessione Hands-on (Richiede PC con almeno 75 GB liberi)

Ulteriori informazioni

La quota di partecipazione è comprensiva di materiale didattico in formato digitale, attestato di partecipazione in formato digitale e pranzo di lavoro per la giornata i venerdì 9 maggio.
Si intendono aziende associate quelle aderenti alle associazioni: ACIMAC, ACIMALL, AMAPLAST, FEDERTEC E UCIMA.

Destinatari

- Professionisti del settore industriale e manifatturiero
- IT & OT Security Manager
- Ingegneri e tecnici di automazione e controllo
- Responsabili della sicurezza aziendale e compliance
- Consulenti e auditor di cybersecurity
- Operatori di infrastrutture critiche e utility

Durata
16 ore

Quota di adesione:
600,00 € + IVA a persona per le aziende associate
750,00 € + IVA a persona per le aziende non associate

Date e Sedi di svolgimento
06/05/2025 09.00-13.00 - ONLINE
07/05/2025 09.00-13.00 - ONLINE
09/05/2025 09.00-18.00 - Modena