

On line-Training Introduzione alla OT Cyber Security e alla norma IEC 62443 (IK-SEC1)

Breve descrizione

Primo modulo della serie OT Cyber Security che affronta la problematica della cyber security in ambito industriale a livello introduttivo, sia dal punto di vista dei riferimenti cogenti o meno (dove vengono presentati i requisiti in vigore nelle diverse parti del mondo e i framework normativi a disposizione con particolare riferimento alla norma IEC 62443) sia dal punto di vista delle possibili modalità attuative per la gestione della cyber security industriale in azienda, seguendo il processo descritto nella norma stessa. In relazione all'applicazione di quest'ultima, si descriveranno le problematiche che si trovano a gestire gli end user, che sono ovviamente gli attori principali nell'intero processo e che hanno la necessità di valutare e gestire il rischio, implementando sistemi di protezione adeguati e adottando una organizzazione idonea al funzionamento efficace dei processi, il tutto in linea con il livello di rischio identificato. In seguito, si passerà a descrivere quello che è richiesto agli altri attori coinvolti nel processo, dagli integratori e chi fa servizi di assistenza e manutenzione sui sistemi di automazione, fino ai costruttori di sistemi e componenti che, mediante la messa a disposizione di prodotti con prestazioni di security dichiarate, sono chiamati a contribuire al livello di security dei sistemi di automazione industriale, secondo le necessità degli end user.

Obiettivi

Dopo aver frequentato il corso sarai in grado di:

- Sapere quali sono i requisiti cogenti applicabili alla cyber security in ambito industriale
- Capire come è strutturata la norma IEC 62443, principale riferimento mondiale sul tema
- Comprendere che la gestione della cyber security industriale deve essere affrontata con metodo
- Descrivere il processo descritto dalla norma IEC 62443, in riferimento ad un sistema di gestione aziendale
- Capire gli obiettivi e la necessità di un risk assessment in ambito cyber security industriale
- Determinare il livello di sicurezza di un sistema di automazione e controllo industriale
- Capire quali sono gli strumenti a disposizione per la mitigazione del rischio
- Applicare i requisiti tecnici connessi alla protezione di un sistema di automazione e controllo industriale
- Determinare i processi necessari per la gestione delle problematiche di security

Gruppo target

Per il livello generale affrontato, questo corso si intende destinato ad una platea multidisciplinare costituita dalle figure che in azienda possono arrivare a gestire requisiti di cyber security, come uffici commerciali, product manager, uffici tecnici, qualità, risorse umane, acquisti, service e assistenza tecnica.

Contenuti del corso

- Cyber Security, differenze fra OT/IT.
- Quadro legislativo e normativo di riferimento.
- IEC 62443 standards framework e cyber security lifecycle.
- I ruoli e le figure coinvolte.
- Approccio lato End-user, da dove tutto comincia: Risk analysis di alto livello, analisi dei rischi di dettaglio e determinazione security level.
- Dinamica di un attacco, metodi e strumenti
- Security vista come efficace combinazione di contromisure tecniche adeguate e processi efficaci
- Dall'integratore al fornitore di impianti e sistemi di automazione.
- Componente, Sistema e automation solution, differenze e modalità di gestione.
- Lo sviluppo di prodotti sicuri
- Certificazione di sistemi o componenti

Il corso comprende esempi, messi a punto su componenti e sistemi reali, seppur in ambito di laboratorio.

Durante il corso verranno svolte esercitazioni di gruppo e singole, per facilitare e verificare l'apprendimento degli argomenti descritti.

Prerequisiti partecipante

Nessuno.

Sono consigliate conoscenze base dei sistemi di automazione, dei principi di security e dei sistemi di gestione.

Nota

Non è prevista alcuna documentazione.

Tipologia

Formazione online

Durata

8 ore

Lingua

it

