SIEMENS

On line-Training OT Cyber Security e IEC 62443 - corso completo (IK-SECCOM)

Breve descrizione

Modulo che comprende tutti gli argomenti IEC 62443 per un corso completo sulla norma e tutte le sue parti rilevanti. Partendo dalle problematiche di cyber security in ambito industriale e dalle tipiche vulnerabilità e modalità di attacco normalmente utilizzate in ambito industriale, si descriverà il framework normativo IEC 62443. Il ruolo principale in questo scenario l'avrà l'end user che essenzialmente deve proteggere la propria infrastruttura secondo un approccio risk based incentrato sulla valutazione dei rischi cyber e che trova attuazione nel cyber security management system, il cosiddetto CSMS. La norma presenta inoltre requisiti tecnici per infrastrutture, sistemi di controllo e componenti che sono a disposizione di integratori e costruttori per la progettazione e implementazione di requisiti di security. Inoltre, tali requisiti forniscono la base per dotare componenti e sistemi di determinate capability di security in funzione del parametro security level in modo da fornire a integratori e end user prodotti idonei ad essere integrati per obiettivi di security definiti. La norma insiste molto anche sulla parte governance con requisiti legati a sistemi di gestione per quanto riguarda l'end user, l'integratore e di product development per quanto riguarda costruttori di componenti e sistemi.

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
- Applicare i requisiti tecnici connessi alla protezione di un sistema di automazione e controllo industriale
- Capire le modalità per lo sviluppo sicuro di prodotti la gestione di integratori e fornitori.

Gruppo target

Il corso ha un contenuto completo e fornisce il giusto livello di approfondimento su tutte le tematiche della IEC 62443 per tutti gli attori coinvolti. Si adatta a chi deve implementare sistemi di governance in azienda sia a livello end user che integratori o costruttori sia a chi deve definire e implementare requisiti tecnici per architetture, sistemi e componenti.

Contenuti del corso

- Cyber Security, differenze fra OT/IT.
- Quadro legislativo e normativo di riferimento.
- IEC 62443 standards framework e cyber security lifecycle.
- 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
- Dall'integratore al fornitore di impianti e sistemi di automazione.
- Componente, Sistema e automation solution, differenze e modalità di gestione.
- Requisiti tecnici per componenti e sistemi
- Product develpment lifecycle destinato ai costruttori.
- Certificazione di sistemi o componenti.

Prerequisiti partecipante

Nessuno in particolare. Auspicabile: conoscenze base dei sistemi di automazione, dei principi di security e dei sistemi di gestione.

Nota

- 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.
- Non è prevista alcuna documentazione*.

Tipologia

Formazione online

Durata

16 ore

Lingua

it