CYBERBEZPIECZEŃSTWO SYSTEMÓW AUTOMATYKI WG IEC 62443

Cyberbezpieczeństwo

Cel szkolenia

Szkolenie dotyczy implementacji i wdrożenia systemu zarządzania cyberbezpieczeństwem instalacji przemysłowych zgodnie ze standardem IEC 62443. Uczestnik pozna poszczególne etapy cyklu życia tego systemu, ich składowe w odniesieniu do poszczególnych części standardu. Uczestnik będzie potrafił przeprowadzić i nadzorować proces wdrażania oraz utrzymywania systemu cyberbezpieczeństwa instalacji przemysłowej, w zależności od rozmiaru systemu czy organizacji. W trakcie szkolenia kursant pozna nie tylko wymagania formalne oraz sprzętowe związane z implementacją systemu bezpieczeństwa, ale również aspekty organizacyjne i biznesowe, stanowiące nieodłączną część tego procesu. Zdobyta na szkoleniu wiedza może być wykorzystana we wszystkich systemach automatyki niezależnie od producenta.

Atuty szkolenia

Bogate doświadczenie w zakresie audytowania systemów sieciowych

Szkolenie dedykowane branży OT

Cena katalogowa: 6000.00 zł netto

Czas trwania

35 godz. / 5 dni

Godziny trwania zajęć

pierwszy dzień 9:00-16:00
następne 8:00-16:00
ostatni 8:00-12:00

Zalecenia

Ogólna znajomość systemów automatyki, wskazana znajomość zagadnień sieciowych

Grupa docelowa

- Menedżerowie działów automatyki, utrzymania ruchu, IT
- Administratorzy sieci Ethernet, systemów sterowania, SCADA
- użytkownicy systemów automatyki

Efekty kształcenia

Wiedza

- bieżące trendy w zakresie rozwoju systemów automatyki wpływające na cyberbezpieczeństwo
- typowe podatności, wektory ataku na systemy automatyki oraz ich potencjalne konsekwencje
- różnice pomiędzy systemami IT oraz OT wpływające na podejście do zagadnień cyberbezpieczeństwa
- standardy wspomagające proces zabezpieczania systemów automatyki
- koncepcje systemu zarządzania cyberbezpieczeństwem zgodną z IEC 62443
- cykl życia systemu bezpieczeństwa definiowany w IEC 62443
- cel i oczekiwane wyniki wysokopoziomowego oraz szczegółowego audytu bezpieczeństwa
- zasady podziału systemu na strefy oraz połączenia pomiędzy strefami
- zasady przeprowadzania szczegółowej analizy ryzyka dla systemu automatyki
- składowe systemu przeciwdziałania wykrytym zagrożeniom
- przykłady w zakresie polityki i procedur bezpieczeństwa
- przykłady rozwiązań sprzętowych w zakresie implementacji systemu przeciwdziałania potencjalnym zagrożeniom
- zasady monitorowania i uaktualniania systemu bezpieczeństwa
- zasady reakcji na wykryte zagrożenia i przywracanie działania systemu automatyki

Umiejętności

- wymienić i zidentyfikować typowe podatności w wykorzystywanych lub administrowanych systemach automatyki
- zainicjować i nadzorować proces zabezpieczania systemów automatyki
- zdefiniować etapy implementacji systemu bezpieczeństwa zgodne z IEC 62443
- wykonać inwentaryzację urządzeń tworzących system komunikacyjny
- przeprowadzić wstępny audyt bezpieczeństwa systemu automatyki
- dokonać podziału systemu na strefy oraz połączenia pomiędzy strefami
- dobrać rozwiązania sprzętowe w zakresie zabezpieczenia obwodowego wydzielonych stref w systemie automatyki oraz połączeń pomiędzy tymi strefami
- skonfigurować przykładowe zapory sieciowe z uwzględnieniem zapór filtrujących ruch na poziomie protokołów przemysłowych
- skonfigurować przykładowy system detekcji intruzów (IDS)

Kompetencje społeczne

- zdolność do inicjowania oraz monitorowania procesu podnoszenia poziomu cyberbezpieczeństwa systemu automatyki

Terminy szkolenia

Wrzesień	14/09/2020 - 18/09/2020

Październik	26/10/2020 - 30/10/2020
Listopad	23/11/2020 - 27/11/2020

Kontakt

Zadzwoń by otrzymać ofertę dla Ciebie

Hanna Łysiak +48 664 441 921

Program szkolenia

- Przegląd typowych podatności i źródeł zagrożeń dla systemów automatyki i sieci OT
- System zarządzania cyberbezpieczeństwem zgodny z IEC 62443
- Implementacja koncepcji „Defense in depth"
- Cykl życia systemu bezpieczeństwa definiowany przez IEC 62443
- Audyt systemu automatyki pod kątem cyberbezpieczeństwa, analiza i wykorzystanie wyników audytu
- Zasady podziału systemu na strefy oraz połączenia pomiędzy strefami
- Zasady przeprowadzania szczegółowej analizy ryzyka dla systemu automatyki
- Przykłady w zakresie polityki i procedur bezpieczeństwa
- Przykłady rozwiązań sprzętowych i programowych w zakresie implementacji systemu przeciwdziałania potencjalnym zagrożeniom
- Zasady monitorowania i uaktualniania systemu bezpieczeństwa
- Zasady reakcji na wykryte zagrożenia i przywracanie działania systemu automatyki

INTEX Sp. z o.o.
44-102 Gliwice, ul. Portowa 4

Tel: +48 32 230 75 16
Fax: +48 32 230 75 17

www.intex.com.pl
intex@intex.com.pl

Odwiedź nasz profil:
facebook

INTEX Sp. z o.o. NIP 631-000-88-84, Zarej. pod nr KRS 0000134132
w Sądzie Rejonowym w Gliwicach, X Wydział Gospodarczy Krajowego
Rejestru Sądowego. Kapitał zakładowy 200.000 PLN.
Bank Polska Kasa Opieki S.A. 21 1240 1343 1111 0000 2337 5017

- Statusy Approved Partner firmy SIEMENS Automation and Drives oraz Centrum Szkoleniowego SIEMENS dla technologii komunikacyjnych PROFIBUS, PROFINET, AS-i, OPC.
- Akredytacje PROFIBUS&PROFINET INTERNATIONAL Competence Center jako pierwsze i jedyne w kraju, PROFIBUS&PROFINET INTERNATIONAL Training Center jako trzecie na świecie.
- Członkostwo w Stowarzyszeniu PROFIBUS PNO Polska od początku jego powstania.
- Certyfikat zarządzania jakością według normy PN-EN ISO 9001:2015 w zakresie projektowania i organizacji szkoleń z zakresu automatyki przemysłowej
- Akredytacja i wpis do Bazy Usług Rozwojowych.