



WPROWADZENIE DO CYBERBEZPIECZEŃSTWA SYSTEMÓW AUTOMATYKI WG IEC 62443 ONLINE

SZKOLENIA ONLINE

Cel szkolenia

Celem jednodniowego szkolenia jest podniesienie świadomości użytkowników systemów automatyki w zakresie cyberbezpieczeństwa. Uczestnicy poznają typowe podatności systemów, sposoby ich identyfikacji oraz zmniejszania powierzchni ataku dostępnej dla cyberprzestępców. Szkolenie to wskazuje standardy wspomagające proces implementacji systemu bezpieczeństwa ze szczególnym naciskiem na standardy grupy IEC 62443. Poza zagadnieniami formalnymi uczestnicy będą mieli okazję zapoznać się z przykładami implementacji systemu bezpieczeństwa zgodnego z koncepcją Defense in depth. Spora dawka wiedzy, podana w skondensowany sposób, z pewnością pozwoli na ocenę systemów zarządzanych przez uczestników pod kątem cyberbezpieczeństwa i świadome zainicjowanie procesu zwiększenia bezpieczeństwa tych systemów.

Atuty szkolenia



Cyberbezpieczeństwo to nie towar
luksusowy



Cyberbezpieczeństwo - jak zacząć?



Ucz się od najlepszych



Szkolenie dedykowane branży OT

Cena katalogowa: 1100.00 zł netto



Czas trwania

6 godz. / 1 dzień



Godziny trwania zajęć

09:00-15:00



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 wektory ataku na systemy automatyki oraz ich potencjalne konsekwencje
- typowe podatności spotykane w systemach automatyki
- różnice pomiędzy systemami IT, a OT wpływające na podejście tematyki cyberbezpieczeństwa
- standardy wspomagające proces zabezpieczania systemów automatyki
- koncepcję bezpieczeństwa systemu zgodną z „Defense in depth”
- koncepcje systemu zarządzania cyberbezpieczeństwem zgodną z IEC 62443
- cykl życia systemu bezpieczeństwa definiowany przez IEC 62443
- cel i oczekiwane wyniki wysokopoziomowego oraz szczegółowego audytu bezpieczeństwa
- składowe systemu przeciwdziałania wykrytym zagrożeniom
- przykłady rozwiązań w zakresie implementacji systemu przeciwdziałania potencjalnym zagrożeniom
- monitorowanie i uaktualnianie systemu automatyki pod kątem bezpieczeństwa cybernetycznego
- reakcja na wykryte zagrożenia i przywracanie działania systemu automatyki

Umiejętności

- wymienić i zidentyfikować typowe podatności w wykorzystywanych lub administrowanych systemach automatyki
- zainicjować proces zabezpieczania systemów automatyki
- zdefiniować etapy implementacji systemu bezpieczeństwa zgodne z IEC62443
- monitorować proces implementacji systemu bezpieczeństwa

Kompetencje społeczne

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

Terminy szkolenia

Uwaga: niektóre terminy tego szkolenia mają niestandardowy czas trwania bądź nie wszystkie odbywają się w naszej siedzibie.

Kwiecień

05/04/2022 - 05/04/2022 *

*zamknięte szkolenie online

Kontakt


Zadzwoń by otrzymać ofertę dla Ciebie

Aneta Nowak [+48 664 441 925](tel:+48664441925)

Program szkolenia

- bieżące trendy w zakresie rozwoju systemów automatyki wpływające na ich bezpieczeństwo cybernetyczne
- typowe podatności oraz wektory ataku na systemy automatyki oraz ich potencjalne konsekwencje
- różnice pomiędzy systemami IT, a OT wpływające na podejście tematyki cyberbezpieczeństwa
- standardy wspomagające proces zabezpieczania systemów automatyki
- koncepcja bezpieczeństwa systemu zgodna z „Defense in depth”
- system zarządzania cyberbezpieczeństwem zgodny z IEC 62443
- cykl życia systemu bezpieczeństwa definiowany przez IEC 62443
- cel i oczekiwane wyniki wysokopoziomowego oraz szczegółowego audytu bezpieczeństwa
- analiza ryzyka
- składowe systemu przeciwdziałania wykrytym zagrożeniom
- przykłady rozwiązań w zakresie implementacji systemu przeciwdziałania potencjalnym zagrożeniom
- monitorowanie i uaktualnianie systemu automatyki pod kątem bezpieczeństwa cybernetycznego
- reakcja 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:


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.