CYBERBEZPIECZEŃSTWO W SYSTEMACH SIEMENS SIMATIC S7

Cyberbezpieczeństwo

Cel szkolenia

Istotą szkolenia jest implementacja, utrzymywanie i aktualizacja mechanizmów bezpieczeństwa urządzeń końcowych, w szczególności systemów wykorzystujących rozwiązania rodziny SIEMENS SIMATIC S7. Na bazie przykładowych konfiguracji kursanci poznają praktyczne metody audytowania systemów automatyki pod kątem podatności na typowe zagrożenia związanych z cyberprzestępczością, zdefiniują politykę bezpieczeństwa oraz zaimplementują ją w modelowym systemie.

Atuty szkolenia

- Cyberbezpieczeństwo to nie towar luksusowy
- Poznaj zawartość na bezpłatnym webinarze
- Praktyczne rozwiązania
- Bogate doświadczenie w zakresie audytowania systemów sieciowych
- Ucz się od najlepszych
- Szkolenie dedykowane branży OT

Cena katalogowa: zł netto

Czas trwania

23 godz. / 3 dni

Godziny trwania zajęć

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

Zalecenia

Znajomość podstaw działania sieci Ethernet oraz ogólna orientacja w zakresie systemów automatyki przemysłowej SIEMENS SIMATIC

Grupa docelowa

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

Efekty kształcenia

Wiedza

- Typowe podatności oraz sposoby źródła zagrożeń dla sieci OT
- Typowe protokoły nie obsługujące zabezpieczeń, zagrożenia związane z ich wykorzystywaniem oraz rozwiązania alternatywne
- Koncepcję budowy i zabezpieczenia sieci OT zgodną z zaleceniami „Defense in depth"
- Standardy związane z bezpieczeństwem sieci
- Typowe podatności oraz możliwości zabezpieczenia systemów sterowania wykorzystujących sterowniki SIEMENS SIMATIC S7
- Sposoby zabezpieczenia dostępu obsługiwane przez typowe urządzenia automatyki
- Dobre praktyki w zakresie bezpiecznego udostępniania danych z urządzeń automatyki systemom nadrzędnym
- Zasady utrzymywania i uaktualniania polityki bezpieczeństwa dotyczącej systemów automatyki

Umiejętności

- Przeprowadzić analizę systemu automatyki SIMATIC pod kątem podatności na typowe zagrożenia
- Zaimplementować podział sieci na segmenty oraz bezpieczną komunikację pomiędzy segmentami
- Wdrożyć mechanizmy zabezpieczenia dostępu do segmentu sieci „z zewnątrz" oraz dostępu do elementów infrastruktury sieciowej „od wewnątrz" w oparciu o SIEMENS SCALANCE S
- Wdrożyć system monitorowania sieci pod kątem urządzeń dołączonych do sieci oraz ich aktywności w oparciu o SIEMENS SINEMA Server/SINEC NMS
- Dobrać komponenty pozwalające na przechwytywanie ruchu sieciowego oraz dokonać analizy przechwyconego ruchu
- Zabezpieczyć dostęp do sterowników SIEMENS SIMATIC S7, zasobów komputera oraz typowych urządzeń automatyki
- Zaimplementować separację na poziomie sieci pomiędzy systemami IT, a OT w oparciu o SIEMENS SCALANCE S
- Wdrożyć system bezpiecznego zdalnego dostępu do systemów automatyki wykorzystujący SIEMENS SINEMA RC

Kompetencje społeczne

- Umiejętność współpracy w zespole odpowiedzialnym za definicje, implementację oraz uaktualnianie polityki bezpieczeństwa dla systemów automatyki wykorzystujących rozwiązania firmy SIEMENS
- Gotowość do wymiany doświadczeń w zakresie tworzenia i uaktualniania polityki bezpieczeństwa dla systemów automatyki
- Gotowość do pogłębiania zdobytej wiedzy i umiejętności w zakresie zabezpieczania systemów automatyki

Terminy szkolenia

Aktualnie nie ma zdefiniowanych terminów dla tego szkolenia.

Jesteś nim zainteresowany? Skontaktuj się z nami.

Kontakt

Zadzwoń by otrzymać ofertę dla Ciebie

Program szkolenia

- Przegląd typowych podatności i źródeł zagrożeń dla systemów automatyki i sieci OT
- Projektowanie i budowa systemów automatyki zgodnie z koncepcją „Defense in depth"
- Standardy związane z bezpieczeństwem sieci
- Typowe podatności oraz możliwości zabezpieczenia systemów sterowania wykorzystujących sterowniki SIEMENS SIMATIC S7
- Monitorowanie infrastruktury sieciowej z wykorzystaniem SIEMENS SINEMA Server/SINEC NMS
- Zabezpieczenie segmentów sieci z wykorzystaniem SIEMENS SCALANCE S
- Zabezpieczenie dostępu do sterowników SIEMENS SIMATIC S7, zasobów komputera oraz typowych urządzeń automatyki
- Przechwytywanie i analiza ruchu sieciowego
- Implementacja systemu bezpiecznego zdalnego dostępu do systemów automatyki w oparciu o SIEMENS SINEMA RC

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.