Szkolenie: Compendium CE

ICS Industrial Control Systems cyber-attacks and proactive defense

Cel szkolenia:

Szkolenie ma na celu dostarczenie uczestnikom informacji związanych z budową, organizacją systemów przemysłowych, ich zabezpieczeniem i zarządzaniem, cyberbezpieczeństwem ICS, przedstawienie „dobrych praktyk" i standardów międzynarodowych oraz sektorowych związanych z zabezpieczeniem systemów przemysłowych. Elementem szkolenia jest przedstawienie wybranych wektorów ataków na systemy przemysłowe, taktyki i techniki działania grup cyberprzestępczych oraz sposoby przeciwdziałania i zarządzania organizacją w trakcie ataku.

Plan szkolenia:

- Systemy przemysłowe ICS
  - Środowisko przemysłowe, SCADA, HMI, PLC
  - Bezpieczeństwo – model referencyjny
  - Zależność i współdziałanie systemów OT/IT
  - Wyzwania dla cyberbezpieczeństwa
  - Analiza i zarządzanie ryzykiem ICS
  - Warsztaty – analiza ryzyka zgodnie z NERC CIP (Critical Infrastructure Protection)
    - Jesteś „właścicielem fabryki" i co powinieneś wiedzieć o zagrożeniach
    - Zarządzanie ryzykiem jak to zrobić z CIP
    - Co o mojej firmie wie SHODAN oraz „inni"
    - Cyberatak na system produkcyjny
- Zagrożenia dla systemów ICS
  - Wybrane ataki na systemy przemysłowe
  - Cyberzagrożenia – MITRE ATT@CK
  - Organizacja obrony systemów, „active defence"
  - Warsztaty – analiza ataku na system ICS, projektowanie bezpiecznego „środowiska"
    - Analiza PCAP z Wireshark, gdzie atakujący zostawił ślad
    - Analiza wektora ataku z MITRE ICS
    - Rekonfiguracja, odpowiedź na cyberatak, zalecenia do zmiany
    - DRP i BCP w ICS
- Reagowanie i zarządzanie incydentami ICS

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Reakcje i zarządzanie incydentem
- Organizacja i zadania SOC/CSIRT (CERT)
- BCP i DR w systemie organizacji reakcji na cyberataki
- Warsztaty - Analiza powłamaniowa w systemie ICS
  - Analiza powłamaniowa – Remnux, IoC.
  - Analiza PDF – SecurityOnion.
  - BlueTeam, CSIRT w akcji MISP, Yara rules.

- Organizacja i zabezpieczenie systemów ICS
  - Pracownik, zarządzający w środowisku IT/OT – odpowiedzialność i współpraca
  - Standardy i procedury, strategia cyberbezpieczeństwa ICS
  - Audyt cyberbezpieczeństwa (NIST, CIP, UKSC)
  - Warsztaty – „case study” analiza po incydencie, rekomendacje, strategia podejmowanych zmian/usprawnień
    - o Właścieiel firmy przemysłowej buduje bezpieczne środowisko
    - o Projektowanie zmian do środowiska ICS
    - o Segmentacja, separacja, dioda, “zero-trust”, “defence in depth”, „air-gap” ICS
    - o Pentesty – czy to działa?

Wymagania:

Podstawowa znajomość terminów dotyczących cyberbezpieczeństwa; systemów operacyjnych Windows, Linux; znajomość protokołów TCP/IP oraz funkcjonowania urządzeń sieciowych, znajomość modelu OSI, zagadnień związanych z przemysłem oraz wymaganiami dla bezpieczeństwa związanych ze standardami i dobrymi praktykami.

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat wystawiony imiennie oraz na firmę, sygnowany przez Compendium Centrum Edukacyjne.

Punkty CPE (CISSP) za udział w szkoleniu:

Uczestnicy tego szkolenia, którzy posiadają aktualną certyfikację System Security Certified Practitioner (SSCP) lub Certified Information Systems Security Professional (CISSP) mogą zdobyć jeden punkt Continuing Professional Education (CPE) za każdą godzinę szkolenia (1 CPE za pełną godzinę

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

edukacyjną, co daje 6 CPE za standardowy dzień szkolenia w Compendium CE - ale nie więcej niż 8 CPE dziennie). W celu przyznania punktów CPE członkowie (ISC) 2 muszą samodzielnie zgłosić udział w naszym szkoleniu do (ISC)2 i muszą zachować dowód udziału (certyfikat uczestnictwa w szkoleniu) w przypadku konieczności potwierdzenia tego faktu w (ISC)2. Więcej informacji pod adresem https://www.isc2.org/cpes/default.aspx (dostęp tylko dla członków (ISC)2).

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001