Програма тренінгу з безпеки SCADA/АСУТП

1. Вступ

Курс навчання дозволяє учасникам отримати широкий набір знань для управління безпекою SCADA/АСУТП. Слухачі отримають всі необхідні навички для вирішення найскладніших проблем. Ці навички включають:

- Оцінку ризиків для систем SCADA/АСУТП.
- Управління доступом користувачів і систем.
- Налаштування безпеки мережі.
- Забезпечення відмовостійкості промислових систем.

2. Аудиторія тренінгу

- Фахівці з безпеки SCADA/АСУТП.
- Розробники програмного забезпечення SCADA/АСУТП.
- Системні адміністратори SCADA/АСУТП.
- Аудитори SCADA/АСУТП.

3. Приклад програми тренінгу

Тривалість: 3 дні.

Список тем:

1. Огляд систем SCADA та ICS.
    a) Рівні АСУТП.
    b) Термінологія АСУТП.
    c) IED.
    d) RTU.
    e) PLC.
    f) HMI.
    g) Сховища історичних даних.
    h) Панелі управління й бізнес-додатки.
2. Стандарти (ISA 62443 та інші).
    a) IEC 62443-1-1.
    b) IEC 62443-2-1.
    c) IEC 62443-3-3.
    d) US National Cyber Security Framework.
    e) Cobit 5.
    f) ISO 27001.
    g) NERC.
    h) American Petroleum Institute.
    i) DHS.
    j) Вимоги ФСТЕК.
    k) NIST.
    l) Common Criteria.
    m) КСЗІ.
3. Ключові поняття.
    a) Конфіденційність, цілісність, доступність.
    b) Спостереженість і керованість промислових процесів.
    c) Власники даних, процесів і систем.
    d) Класифікація критичних активів.
    e) Розпорядники систем.

f) Оператори електронних систем.

g) Ешелонований захист.

h) Цілі й метрики безпеки.

i) Інвентаризація.

j) Управління змінами.

4. Промислові мережі.

a) Пристрої в промислових мережах.

b) Струмова петля.

c) Смарт-гріди.

d) Особливості промислових пристроїв (фізична безпека).

e) Радіозв'язок.

f) Безпека мобільного зв'язку.

g) RS-485.

h) RS-232.

i) RS-422.

j) Промисловий Ethernet.

k) Несанкціоновані підключення в промислові мережі (модеми, принтери, USB, Bluetooth тощо).

5. Промислові протоколи.

a) MODBUS.

b) PROFIBUS.

c) OPC.

d) CIP.

e) DNP3.

6. Елементи мережевої безпеки.

a) Зонування.

b) Види міжмережевих екранів.

c) Безпека на рівні L2.

d) Проксі-сервери.

e) Демілітаризована зона.

f) Діоди даних.

g) Математичні моделі в прив'язці до мережевої безпеки.

7. Створення програми забезпечення безпеки.

a) Архітектура безпеки.

b) Стратегія безпеки.

c) Роль керівництва.

d) Моніторинг ефективності програми безпеки.

e) Внутрішній аудит.

f) Бізнес-обґрунтування заходів безпеки.

g) Культура й етика.

h) Інші питання кадрової безпеки.

8. Управління ризиками.

a) Імовірність і збитки.

b) Підходи до управління ризиками.

c) Методології оцінки ризиків.

d) Процеси управління ризиками.

9. Безпека постачальників послуг.

a) Вимоги до постачальників послуг.

b) Безпека ланцюжка поставок.

c) Проведення перевірок постачальників.

d) SLA.

e) NDA.

10. Безпека при розробці та впровадженні систем IT.

a) Життєвий цикл систем IT.

b) Вимоги до IT-систем.

c) Тестування безпеки.

d) Стандарти безпечного кодування.

e) Виведення з експлуатації.

f) CWE.

11. Політики безпеки.

a) Політики, стандарти, процедури й рекомендації.

b) Атрибути документів.

c) Корпоративне сховище документів.

d) Життєвий цикл політики.

e) Види політик.

f) Вимоги до гарної політики.

12. Управління контролем доступу.
    a) Моделі управління доступом.
    b) Дискретне управління.
    c) Мандатне управління.
    d) Рольове управління.
    e) Реалізації політик доступу в різних операційних системах і додатках.
    f) Перегляд доступу.
    g) Розподіл обов'язків.
13. Виявлення атак.
    a) Системи виявлення й запобігання вторгнень.
    b) Системи збору журналів безпеки.
    c) Системи управління подіями безпеки.
    d) Вірусні загрози.
    e) Криміналістика та її особливості для промислових пристроїв.
    f) Профілізація мережі (побудова типових моделей трафіку).
    g) Приховані канали комунікацій шкідливого програмного забезпечення.
14. Управління вразливостями.
    a) Тестування на проникнення.
    b) Тестові лабораторії.
    c) Безпечні параметри сканерів вразливостей.
    d) CVE.
    e) CVSS.
    f) Загартування (hardening) систем.
15. Безпечні комунікації.
    a) Віртуальні приватні мережі.
    b) Підключення віддаленого робочого столу.
    c) Безпека мобільних клієнтів.
    d) Перевірки пристроїв, що підключаються.
    e) Інфраструктура відкритих ключів.
16. Відмовостійкість SCADA/АСУТП і відновлення після збою.
    a) Безперервність операцій і відновлення після катастроф.
    b) Резервне копіювання.
    c) Сценарії катастроф.

d) Стратегії відновлення.

e) Тестування планів безперервності.

f) Ролі в процесі управління безперервністю бізнесу.

Надішліть нам електронного листа info@h-xtech.com або зателефонуйте нам +380996100702, щоб отримати безпеку для вашого промислового середовища та всієї організації!