I-CSO - CyberSecurity Operations

Про програму:

Курс охоплює основні знання і навички у всіх областях безпеки в кіберпросторі, а також орієнтовано на підготовку IT-фахівців для отримання навичок при виконанні завдань аналітиків з кібербезпеки.

Для кого:

Даний курс орієнтовано на підготовку IT-фахівців для роботи аналітиками з кібербезпеки в Центрах моніторингу та управління безпекою (SOC).

Учасникам потрібно мати такі знання і навички:

- Базові знання про Windows і Linux
- Основні принципи роботи в мережі
- Загальні відомості про двійкові та 16-річні числові системи
- Знання основних принципів програмування
- Базові навички роботи з запитами SQL

Даний курс допоможе:

- Підготувати безпечне середовище для діяльності та аналізу кібербезпеки.
- Виконувати аналіз мережевих протоколів і служб
- Навчитись надавати пояснення, як працює мережева інфраструктура
- Навчитись класифікувати різні типи мережевих атак
- Використовувати засоби моніторингу мережі для виявлення атак на мережні протоколи та служби.
- Навчитись застосовувати різні способи запобігання несанкціонованого доступу до комп'ютерних мереж, хостів і даних
- Проводити оцінювання попереджень про безпеку мережі
- Виконувати аналіз мережевого вторгнення, з метою виявлення скомпрометованих хостів та вразливостей.
- Навчитись застосовувати моделі реагування для вирішення інцидентів безпеки

Тренер:

Самохвалов Юрій – інструктор-експерт з мережевих технологій за світовими сертифікаціями, активний учасник підготовки портфоліо курсів з кібербезпеки як для початківців, так і для спеціалістів, сертифікований дизайнер СКС за критеріями Raichle-de-Massari. Досвід Юрія включає проектування, реалізацію та менеджмент мережевої інфраструктури компанії, розвернення та рішень з IT-безпеки для різних галузей, серед яких державники та гірничозбагачувальний сектор.

10/14 Radyshcheva Str., 03124, Kyiv, Ukraine
Tel.:+380 44 594 80 18; training@issp.com
www.issp.training

Програма курсу:

День 1:

1. Кібербезпека та SOC
2. Інструментарій ОС Windows
3. Інструментарій ОС Linux
4. Мережева інфраструктура

День 2:

5. Принципи забезпечення безпеки мережі
6. Поглиблений аналіз мережевих атак
7. Захист мережі
8. Криптографія та PKI

День 3:

9. Захист та аналіз кінцевих пристроїв
10. Моніторинг безпеки
11. Аналіз інформації про вторгнення
12. Реагування на інциденти та їх обробка

Формат навчання

З 10.00 до 17.30, з перервою на обід та кава-паузи

Мова викладання

Українська, російська