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

I-DFFR | Digital Forensics & First Response

Авторський курс від ISSP

Триденний курс для спеціалістів, який дає практичні навички з використання інструментів пошуку доказів зловмисних дій; допомагає ознайомитись зі стандартами здійснення цифрових розслідувань, а також організувати процес отримання, зберігання і надання цифрових доказів.

Для кого:

- Пентестери
- Спеціалісти з безпеки інфраструктури
- Аналітики безпеки
- Ті, хто здійснює дослідження цифрових злочинів

Слухачам потрібно:

- Бути впевненим користувачем ПК
- Мати досвід в адмініструванні операційних систем
- Мати знання про мережеві технології

Даний курс допоможе:

- Ознайомитись зі стандартами та особливостями організації збору цифрових доказів вчинення незаконних дій.
- Ознайомитись та отримати практичні навички з використання інструментів пошуку доказів зловмисних дій.
- Ознайомитись з процесом отримання, зберігання цифрових доказів і надання звітів для судового розгляду.

Програма курсу:

1. **Що таке комп'ютерні розслідування?**

- Розуміння цифрових доказів
- Цифрова експертиза та її роль для SOC
- Ролі та обов'язки розслідувача цифрових злочинів
- Складності розслідування кіберзлочинів

2. **Як правильно організувати цифрове розслідування.**

- Попереднє розслідування
- Оперативне реагування
- Стадія розслідування
- Стадія пост-розслідування

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

3. Накопичувачі та файлові системи

- Види накопичувачів та їх характеристики
- Логічна структура диску
- Процес завантаження різних операційних систем
- Інструменти дослідження файлової системи
- Системи зберігання інформації
- Стандарти кодування та HEX-редактори
- Аналіз популярних форматів файлів

4. Збір та отримання даних

- Процес збору даних
- Методологія збору даних
- Підготовка файлу образу для дослідження

5. Боротьба з техніками зловмисників

- Методи боротьби з діями зловмисників
- Видалення даних та дослідження Recycle Bin
- Методи вилучення файлів та способи відновлення доказів з видалених розділів
- Методи протистояння парольному захисту
- Стеганографія та обфускація як методи зловмисників
- Знищення артефактів, метаданих та шифрування
- Програми-пакувальники та методи мінімізації залишення слідів
- Контрзаходи зловмисним діям (у форензиці)

6. Отримання доказів з ОС Windows

- Збір короткочасної та довгострокової інформації
- Аналіз пам’яті та реєстру
- Аналіз інформації браузерів
- Текстові журнали та журнали подій Windows

7. Отримання доказів з Linux-систем

- Використання TSK для аналізу образів файлової системи
- Дослідження пам'яті Linux

- Цифрові розслідування в Mac OS

8. Отримання доказів з мережі

- Розслідування в мережі
- Логування та готовність розслідування в мережі
- Концепція кореляції подій
- Визначення показників компрометації (IOCs) з журналів мережі
- Дослідження трафіку мережі
- Виявлення інцидентів та перевірка інструментів SIEM
- Моніторинг та протистояння атакам бездротової мережі

9. Отримання доказів з хмари та контейнерні технології.

- Базові концепції хмарних обчислень
- Цифрові розслідування в хмарах
- Основи Amazon Web Services (AWS)
- Як розслідувати інциденти безпеки в AWS
- Основи Microsoft Azure
- Як розслідувати інциденти безпеки в Azure
- Методологія цифрових розслідувань для контейнерів і мікросервісів

Формат навчання:
3 дні, з 10:00 до 17:30, з перервами на обід та кава-паузи.

Мова викладання:
Українська.

Тренер курсу
Юрій Самохвалов - інструктор-методолог Тренінгового Центру ISSP, акредитований інструктор EC-Council, Cisco. Сертифікований спеціаліст за напрямками OSINT, етичного хакінгу, аналітики з кібербезпеки, побудови захищеної інфраструктури та розслідування комп'ютерних злочинів, також є автором низки курсів з кібербезпеки, як для початківців, так і для спеціалістів. Досвід Юрія включає проектування, реалізацію та менеджмент мережевої інфраструктури компанії, проектування та реалізація структурних і безпекових проектів для замовників з комерційного та державного секторів.