Informatyka śledcza (kod: FORENSICS-IT)

Opis i cel szkolenia

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Szkolenie przeznaczone przede wszystkim dla osób odpowiadających za techniczną stronę postępowań i czynności wyjaśniających: zespołów IT i bezpieczeństwa w służbach i administracji publicznej, pracowników prowadzących kontrole wewnętrzne i audyty, a także administratorów, którzy w praktyce jako pierwsi mają kontakt ze sprzętem — i od których zależy, czy materiał będzie w ogóle nadawał się do dalszej analizy. Największa część nieodwracalnych szkód w materiale dowodowym często powstaje w pierwszej godzinie, jeszcze zanim ktokolwiek nazwie sytuację postępowaniem.

Program zajęć prowadzi przez pełny proces: od decyzji, czy komputer wolno wyłączyć, przez wykonanie kopii binarnej i zabezpieczenie danych ulotnych, po analizę i raport. Uczestnik pracuje na obrazach nośników i zrzutach pamięci — odtwarza aktywność użytkownika z artefaktów systemu, wydobywa dane z Volume Shadow Copy, pliku stronicowania i pamięci operacyjnej, buduje oś czasu zdarzeń i dokumentuje wnioski w formie, która nadaje się do przedstawienia przełożonemu, kontroli albo organowi. Metodykę opieramy na uznanych standardach postępowania z dowodem elektronicznym, bo w tej dziedzinie powtarzalność procedury jest równie ważna jak sam wynik.

Osobny dział poświęcamy urządzeniom mobilnym: różnicy między ekstrakcją logiczną a fizyczną, karcie SIM, temu, co realnie da się odzyskać z systemu plików telefonu, oraz temu, gdzie przebiega granica naszych możliwości.

Pracujemy warsztatowo. Na narzędziach o otwartym kodzie źródłowym i bezpłatnych. Przy czym jest to świadoma decyzja, a nie oszczędność - uczestnik wychodzi z umiejętnościami, które może zastosować u siebie od razu. I co również istotne, bez postępowania zakupowego na licencje, czy też bez uzależnienia od jednego dostawcy oprogramowania.

Tam, gdzie w praktyce biegłych często używa się specjalistycznego sprzętu - pokazujemy, co dane narzędzie robi i czym różni się od metody dostępnej bez posiadania dostępu do tego narzędzia/sprzętu.

Uwaga: niniejsze szkolenie nie nadaje uprawnień biegłego sądowego. Uczymy tego, co specjalista, administrator IT, czy pracownik odpowiedniej instytucji powinien umieć samodzielnie zrobić; oraz tego, w którym momencie sprawę należy przekazać dalej - i jak jej wcześniej nie zepsuć.

Czas trwania

3 dni

Program

1. Informatyka śledcza — cele, założenia i dowód elektroniczny
   - — Cele i zakres informatyki śledczej; czym ta dziedzina nie jest
   - — Dowód elektroniczny: definicja, rola i znaczenie w postępowaniu
   - — Założenia informatyki śledczej i ich praktyczne konsekwencje
   - — Rodzaje śledztw komputerowych i postępowań wewnętrznych
   - — Reguły i zasady przeprowadzania analizy śledczej
   - — Normy i standardy w informatyce śledczej
   - — Łańcuch dowodowy i dokumentowanie czynności od pierwszej minuty
   - — Zagadnienia prawne i etyka pracy z materiałem dowodowym
2. Proces analizy śledczej i warsztat pracy

- Procesy analizy śledczej krok po kroku
- Narzędzia sprzętowe wykorzystywane przez śledczych: blokery zapisu, duplikatory, stacje robocze
- Oprogramowanie śledcze: klasy narzędzi, kryteria doboru, rozwiązania otwarte i komercyjne
- Przygotowanie stanowiska i środowiska badawczego
- Najczęstsze błędy pierwszej godziny i ich skutki dla wartości dowodowej

3. Kopia binarna — podstawa całego procesu
   - Czym jest kopia binarna i dlaczego bez niej nie ma dowodu
   - Formaty obrazów nośników i ich zastosowania
   - Suma kontrolna: po co ją liczyć, kiedy i jak weryfikować
   - Wykonanie kopii binarnej w środowisku lokalnym — ćwiczenie
   - Wykonanie kopii binarnej w środowisku sieciowym — ćwiczenie
   - Kopie binarne komputerów Apple i ograniczenia współczesnego sprzętu
   - Zabezpieczanie materiału dowodowego z nośników zaszyfrowanych
   - Przechowywanie dowodu elektronicznego i zabezpieczenie kopii roboczych
4. Live Forensics i dane ulotne
   - Kiedy nie wolno wyłączyć komputera i dlaczego
   - Proces zabezpieczenia materiału dowodowego w trybie Live Forensics
   - Zabezpieczanie danych i informacji ulotnych — triage
   - Zrzut pamięci operacyjnej — ćwiczenie
   - Zabezpieczanie dysków, poczty elektronicznej, stron internetowych i pozostałych nośników
5. Analiza pamięci operacyjnej
   - Co realnie da się odtworzyć ze zrzutu pamięci RAM
   - Procesy, połączenia sieciowe, wstrzyknięcia i ślady po uruchomionym oprogramowaniu
   - Analiza pamięci RAM — ćwiczenie
   - Analiza zawartości pliku stronicowania i pliku hibernacji
6. Artefakty systemu operacyjnego
   - Analiza i zabezpieczanie danych z Volume Shadow Copy — ćwiczenie
   - Analiza Prefetch i śladów uruchamiania programów
   - Różnice w analizie kosza systemowego w kolejnych systemach operacyjnych
   - Sygnatury i znaczniki czasowe; wyszukiwanie plików po czasie
   - Artefakty aktywności użytkownika: rejestr, przeglądarki, komunikatory, poczta
7. Prowadzenie sprawy: od danych do wniosków
   - Zakładanie nowej sprawy i porządkowanie materiału
   - Analiza danych, listy kontrolne i filtrowanie
   - Analiza osi czasu zdarzeń
   - Wyszukiwanie z wykorzystaniem wyrażeń regularnych
   - Tagowanie i zaawansowane wyszukiwanie informacji
   - Wyszukiwanie i analiza złośliwego oprogramowania w zabezpieczonym materiale
8. Automatyzacja pracy śledczego
   - Które czynności warto zautomatyzować, a których nie wolno
   - Budowa własnego narzędzia wspierającego analizę — ćwiczenie
   - Weryfikacja wyników pracy narzędzi automatycznych
9. Analiza urządzeń mobilnych
   - Mobile forensics: definicja, proces i różnice wobec analizy komputerów
   - Karta SIM: zawartość, logiczna ekstrakcja danych — ćwiczenie
   - Klonowanie kart SIM i przyczyny niekompletności danych w klonie
   - Ekstrakcja logiczna: system plików z urządzeń mobilnych
   - Ekstrakcja fizyczna: zakres możliwych do odzyskania danych

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

- Różnice między ekstrakcją logiczną a fizyczną i konsekwencje wyboru metody
- Praktyczna analiza urządzeń mobilnych — ćwiczenie na przygotowanym materiale
- Analiza systemu plików urządzenia mobilnego
- Wyszukiwanie artefaktów jailbreak w urządzeniach iPhone
- Pomijanie zabezpieczeń kodem PIN i wzorem: możliwości, granice i ryzyka
- Narzędzia do odczytu i przeglądania raportów z ekstrakcji urządzeń mobilnych

10. Raport i przedstawienie materiału dowodowego
    - Sprawozdawczość: co musi znaleźć się w dokumentacji czynności
    - Raportowanie wyników analizy
    - Przedstawienie materiału dowodowego z wykorzystaniem raportów interaktywnych
    - Prezentacja ustaleń odbiorcy nietechnicznemu
    - Najczęstsze błędy podważające wartość dowodową materiału

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Przeznaczenie i wymagania

Szkolenie jest kierowane przede wszystkim do osób takich, jak:

- zespoły IT i bezpieczeństwa w instytucjach publicznych, urzędach i jednostkach samorządowych;
- pracownicy służb i podmiotów prowadzących czynności wyjaśniające oraz dochodzeniowe;
- osoby prowadzące kontrole wewnętrzne, audyty i postępowania dyscyplinarne, w których materiałem jest zapis cyfrowy;
- administratorzy systemów i sieci, którzy jako pierwsi zabezpieczają sprzęt i dane po zdarzeniu;
- specjaliści bezpieczeństwa i IT odpowiadający za reagowanie na incydenty i analizę powłamaniową;
- administratorzy w organizacjach i instytucjach publicznych realizujących wymogi z zakresu cyberbezpieczeństwa;
- oraz wszelkie inne osoby przygotowujące się do pracy w obszarze informatyki śledczej i analizy powłamaniowej.

Odnośnie uczestników, zakładamy posiadanie praktycznego doświadczenia w IT, w szczególności w administracji komputerami, systemami, czy sieciami. Nie wymagamy natomiast żadnej znajomości zagadnień informatyki śledczej — szkolenie w tym zakresie prowadzone jest od podstaw.

Spodziewamy się:

- praktycznej znajomości systemów Windows, mile widziana - znajomość również podstaw systemu Linux;
- znajomości wiersza poleceń;
- podstawowej wiedzy o sieciach komputerowych i systemach pocztowych.

Nie jest wymagane żadne wcześniejsze doświadczenie w informatyce śledczej, **ani wiedza prawnicza**.

Wszelkie niezbędne obrazy nośników i materiały do ćwiczeń udostępniają Państwu nasi trenerzy.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Cena szkolenia

2890 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.