Szkolenie: EC-Council
CHFI - Computer Hacking Forensic Investigator

Cel szkolenia:

Szkolenie C|HFI (Computer Hacking Forensic Investigator) od EC-Council przygotowuje specjalistów cyberbezpieczeństwa do prowadzenia skutecznych dochodzeń z zakresu informatyki śledczej (digital forensics) oraz do osiągnięcia w organizacji stanu gotowości kryminalistycznej (forensic readiness). Opracowanie procesu pracy, przygotowanie laboratorium, procedur zabezpieczania materiału dowodowego oraz technik analitycznych jest niezbędne do weryfikacji i wstępnej triage incydentów oraz do właściwego ukierunkowania zespołów reagowania na incydenty. Gotowość kryminalistyczna ma kluczowe znaczenie, ponieważ może przesądzić o tym, czy zdarzenie pozostanie incydentem o ograniczonym wpływie, czy przerodzi się w poważny cyberatak paraliżujący działanie firmy.

To intensywne, praktyczne szkolenie z informatyki śledczej obejmuje ponad 50 laboratoriów, w ramach których uczestnicy pracują na przygotowanych materiałach dowodowych, wykorzystując narzędzia stosowane przez czołowych specjalistów digital forensics na świecie. Program wykracza poza klasyczną analizę sprzętu i pamięci operacyjnej, poruszając aktualne zagadnienia z zakresu informatyki śledczej w chmurze, urządzeń mobilnych i IoT, a także dochodzeń dotyczących ataków na aplikacje webowe oraz analizy złośliwego oprogramowania. C|HFI prezentuje metodyczne podejście do informatyki śledczej, obejmujące m.in. przeszukanie i zabezpieczenie, łańcuch dowodowy (chain of custody), pozyskanie, utrwalenie, analizę oraz raportowanie dowodów cyfrowych.

Uczestnicy poznają różnorodne techniki dochodzeniowe oraz standardowe narzędzia informatyki śledczej. W trakcie nauki pozyskiwania i zarządzania materiałem dowodowym w różnych środowiskach systemowych omawiane są również zasady łańcucha dowodowego oraz procedury prawne wymagane do zabezpieczenia dowodów i zapewnienia ich dopuszczalności w postępowaniu sądowym. Wiedza ta wspiera skuteczne ściganie cyberprzestępców i ograniczanie odpowiedzialności po stronie organizacji będącej ofiarą.

Program dostarcza rzetelnej, praktycznej wiedzy potwierdzanej uznawaną na świecie certyfikacją, wymaganą do rozwoju kariery w obszarze digital forensics i DFIR (Digital Forensics & Incident Response), co przekłada się na zwiększenie atrakcyjności na rynku pracy.

Czego się nauczysz

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

- Podstaw informatyki śledczej, rodzajów cyberprzestępstw i procedur ich badania oraz regulacji i standardów wpływających na prowadzenie dochodzeń z zakresu informatyki śledczej
- Poszczególnych etapów procesu dochodzenia w informatyce śledczej
- Typów nośników danych i ich charakterystyki, procesu uruchamiania systemu i systemów plików w Windows, Linux i macOS, narzędzi do analizy systemów plików, macierzy RAID oraz systemów NAS/SAN, standardów kodowania oraz analizy formatów plików
- Podstaw i metodyki pozyskiwania danych (data acquisition), eDiscovery oraz przygotowania obrazów dysków do badań kryminalistycznych
- Technik antykryminalistycznych (anti-forensics) stosowanych przez atakujących, sposobów ich wykrywania wraz z narzędziami oraz metod przeciwdziałania
- Pozyskiwania danych ulotnych i nieulotnych w systemach Windows, analizy pamięci i rejestru Windows, analizy aplikacji opartych o Electron, informatyki śledczej przeglądarek WWW oraz badania artefaktów systemu Windows (m.in. ShellBags, plików LNK i Jump Lists) oraz dzienników zdarzeń
- Pozyskiwania danych ulotnych i nieulotnych oraz informatyki śledczej pamięci w systemach Linux i macOS
- Podstaw informatyki śledczej sieci, korelacji zdarzeń, wskaźników kompromitacji (IOC) i metod ich identyfikacji na podstawie logów, technik i narzędzi badania ruchu sieciowego, detekcji i analizy incydentów oraz wykrywania i badania ataków bezprzewodowych
- Zagadnień z zakresu informatyki śledczej malware: statycznej i dynamicznej analizy złośliwego oprogramowania, analizy zachowania systemu i sieci oraz analizy ransomware
- Informatyki śledczej aplikacji webowych: zagrożeń i ataków, pracy z logami aplikacyjnymi (np. IIS, Apache) oraz wykrywania i badania ataków na aplikacje WWW
- Zasad działania przeglądarki Tor oraz etapów procesu informatyki śledczej Tor Browser
- Podstaw przetwarzania w chmurze, informatyki śledczej w chmurze i związanych z nią wyzwań, a także podstaw AWS, Microsoft Azure i Google Cloud oraz metodyk prowadzenia dochodzeń w tych środowiskach
- Elementów komunikacji e-mail, kroków badania przestępstw związanych z pocztą elektroniczną oraz informatyki śledczej mediów społecznościowych
- Warstw architektury i procesów uruchamiania urządzeń z Android i iOS, procesu informatyki śledczej urządzeń mobilnych, rodzajów sieci komórkowych, systemu plików karty SIM oraz logicznego i fizycznego pozyskiwania danych z urządzeń Android i iOS
- Rodzajów zagrożeń IoT, problemów bezpieczeństwa, podatności i obszarów powierzchni ataku oraz procesu i wyzwań informatyki śledczej dla IoT

Dla kogo jest CHFI

- Specjaliści ds. cyberbezpieczeństwa (analitycy śledczy i zespoły reagowania na incydenty)
- Funkcjonariusze organów ścigania i prywatni detektywi
- Menedżerowie IT i administratorzy systemów

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

- Specjaliści prawni oraz osoby odpowiedzialne za zgodność (compliance)
- Służby wojskowe i wywiadowcze oraz administracja publiczna

Plan szkolenia:

- Moduł 1 - Informatyka śledcza we współczesnym świecie
  - Zrozumienie podstaw informatyki śledczej (computer forensics)
    - Wprowadzenie do computer forensics
    - Zakres computer forensics
  - Zrozumienie cyberprzestępstw i procedur dochodzeniowych
    - Rodzaje cyberprzestępstw
    - Wpływ cyberprzestępstw na organizację
    - Atrybucja cybernetyczna (cyber attribution)
    - Dochodzenie w sprawach cyberprzestępczości (cybercrime investigation)
  - Dowody cyfrowe i eDiscovery - wprowadzenie
    - Wprowadzenie do dowodów cyfrowych
    - Rodzaje dowodów cyfrowych
    - Rola dowodów cyfrowych
    - Potencjalne źródła materiału dowodowego
    - Zasady dopuszczalności dowodów (rules of evidence)
    - Zasada najlepszego dowodu (best evidence rule)
    - Federal Rules of Evidence
    - ACPO Principles of Digital Evidence
    - Computer forensics a eDiscovery - różnice
    - Role zespołów prawnych i IT w eDiscovery
    - Dobre praktyki postępowania z dowodami cyfrowymi
  - Gotowość kryminalistyczna (forensic readiness)
    - Forensic readiness - definicja i założenia
    - Forensic readiness a business continuity
    - Planowanie forensic readiness
    - Procedury forensic readiness
  - Rola procesów i technologii w computer forensics
    - Computer forensics jako element Incident Response Plan (IRP)
    - Rola computer forensics w działaniach SOC
    - Rola Threat Intelligence w computer forensics

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

- Rola Artificial Intelligence (AI) w computer forensics
- Automatyzacja i orkiestracja w informatyce śledczej (forensics automation and orchestration)

- Role i odpowiedzialności specjalisty informatyki śledczej
  - Potrzeba roli specjalisty informatyki śledczej
  - Role i odpowiedzialności specjalisty informatyki śledczej
  - Cechy dobrego specjalisty computer forensics
  - Kodeks etyki (code of ethics)
  - Współpraca z klientem lub pracodawcą w trakcie dochodzenia
  - Dostęp do zasobów i źródeł wiedzy z obszaru computer forensics
- Wyzwania w dochodzeniach dotyczących cyberprzestępczości
  - Wyzwania, jakie cyberprzestępstwa stawiają przed śledczymi
  - Inne czynniki wpływające na przebieg dochodzeń śledczych
  - Aspekty prawne w computer forensics (legal issues)
  - Aspekty prywatności w computer forensics (privacy issues)
- Standardy i dobre praktyki w informatyce śledczej
  - Normy ISO
  - ENFSI Best Practice Manual for Digital Forensics
- Przepisy prawa i zgodność prawna w informatyce śledczej
  - Rola agencji krajowych i międzynarodowych w dochodzeniach dotyczących cyberprzestępczości
  - Informatyka śledcza a zgodność prawna
  - Inne przepisy istotne dla informatyki śledczej

- Moduł 2 - Proces dochodzenia w informatyce śledczej
  - Zrozumienie procesu dochodzeniowego i jego znaczenia
    - Znaczenie procesu dochodzeniowego w computer forensics
    - Fazy procesu dochodzeniowego w computer forensics
  - Zrozumienie First Response
    - First Response
    - First Responder
    - Roles of First Responder
    - Podstawy First Response
    - First Response w różnych sytuacjach
    - Częste błędy First Respondera
    - Kwestie BHP
  - Zrozumienie fazy pre-investigation
    - Konfiguracja laboratorium computer forensics

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

- Budowanie zespołu dochodzeniowego
- Zrozumienie wymagań sprzętowych i programowych laboratorium forensics
- Walidacja oprogramowania i sprzętu laboratoryjnego
- Zapewnienie jakości (Quality Assurance)
- Tworzenie security content, skryptów, narzędzi lub metod usprawniających procesy forensics

- Zrozumienie fazy Investigation
  - Dokumentowanie miejsca przestępstwa elektronicznego
  - Search and Seizure
  - Evidence Preservation
  - Data Acquisition
  - Data Analysis
  - Case Analysis
- Zrozumienie fazy Post-investigation
  - Reporting
  - Występowanie w roli biegłego sądowego

- Moduł 3 - Dyski i systemy plików
  - Opis różnych typów dysków i ich charakterystyki
    - Omówienie Hard Disk Drive (HDD)
    - Omówienie Solid-State Drive (SSD)
    - Disk Interfaces
  - Wyjaśnienie logicznej struktury dysku
    - Logical Structure of Disks
  - Zrozumienie procesu uruchamiania systemów Windows, Linux i macOS
    - Czym jest proces uruchamiania (boot process)?
    - Kluczowe pliki i komponenty systemowe Windows
    - Windows Boot Process: metoda BIOS-MBR
    - Windows Boot Process: UEFI-GPT
    - macOS Boot Process
    - Linux Boot Process
    - Windows File Systems
    - Linux File Systems
    - macOS File Systems
  - Zrozumienie analizy systemu plików
    - File System Analysis Using Autopsy
    - Analiza systemu plików z użyciem The Sleuth Kit (TSK)

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

- Tworzenie i analiza osi czasu systemu plików z użyciem The Sleuth Kit (TSK)
- Zasady timestampów NTFS w Windows i Linux

- Zrozumienie systemów pamięci masowej
  - RAID Storage System
  - Network-Attached Storage (NAS)
  - Storage Area Network (SAN)
  - Różnice między NAS i SAN
- Zrozumienie standardów kodowania i edytorów hex
  - Character Encoding Standards
  - OFFSET
  - Understanding Hex Editors
  - Understanding Hexadecimal Notation
- Analiza popularnych formatów plików z użyciem edytora hex
  - Image File Analysis: JPEG
  - Image File Analysis: BMP
  - Widok hex popularnych formatów plików graficznych
  - PDF File Analysis
  - Word File Analysis
  - PowerPoint File Analysis
  - Excel File Analysis
  - Widok hex innych popularnych formatów plików
  - Widok hex popularnych formatów plików wideo
  - Widok hex popularnych formatów plików audio

- Moduł 4 - Pozyskiwanie i duplikowanie danych
  - Zrozumienie podstaw pozyskiwania danych (Data Acquisition)
    - Omówienie Data Acquisition
    - Live Acquisition
    - Kolejność ulotności (Order of Volatility)
    - Dead Acquisition
    - Praktyczne reguły (rules of thumb) dla Data Acquisition
    - Typy Data Acquisition
    - Dobór formatu Data Acquisition
  - Zrozumienie eDiscovery
    - eDiscovery
    - Cykl Electronic Discovery Reference Model (EDRM)
    - Monitorowanie i utrzymywanie dokładnych metryk oraz szczegółowego śledzenia

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

informacji związanych z eDiscovery
- eDiscovery Collection Methodologies
- Best Practices for eDiscovery
- eDiscovery Tools

- Zrozumienie metodyki Data Acquisition
  - Data Acquisition Methodology
  - Krok 1: wybór najlepszej metody Data Acquisition
  - Step 2: Select Data Acquisition Tool
  - Step 3: Sanitize Target Media
  - Step 4: Acquire Volatile Data
  - Krok 5: włączenie ochrony przed zapisem (write protection) na nośniku dowodowym
  - Step 6: Acquire Non-volatile Data
  - Step 7: Plan for Contingency
  - Step 8: Validate Data Acquisition
  - Wytyczne i dobre praktyki Data Acquisition
- Przygotowanie pliku obrazu (image) do badania
  - Przygotowanie obrazu (image) do badania
  - Scenariusz 1: badanie obrazów na stacji roboczej forensic z Linux
  - Scenariusz 2: badanie obrazów na stacji roboczej forensic z Windows
  - Scenariusz 3: badanie obrazów na stacji roboczej forensic z macOS
  - Digital Forensic Imaging Tools

- Moduł 5 - Przeciwdziałanie technikom anti-forensics
  - Zrozumienie technik anti-forensics
    - Czym jest anti-forensics?
    - Wyzwania dla forensics wynikające z anti-forensics
  - Omówienie usuwania danych oraz Recycle Bin forensics
    - Technika anti-forensics: usuwanie danych/plików
    - Co dzieje się, gdy plik zostaje usunięty w Windows?
    - Recycle Bin in Windows
  - Przedstawienie technik File Carving i sposobów odzyskiwania dowodów z usuniętych partycji
    - File Carving
    - Odzyskiwanie usuniętych partycji
  - Przegląd technik Password Cracking/Bypassing
    - Anti-forensics Technique: Password Protection
    - Narzędzia do pozyskiwania hashy haseł

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

- Password Cracking Tools
- Bypassing haseł na wyłączonym komputerze (powered-off)
- Narzędzie do resetu hasła administratora i lokalnych użytkowników: PassFab 4WinKey
- Bypassing hasła użytkownika Windows przez uruchomienie Live USB
- Application Password Cracking Tools

- Wykrywanie steganografii, ukrytych danych w strukturach systemu plików, obfuskacji śladów oraz niezgodności rozszerzeń plików
  - Anti-forensics Technique: Steganography
  - Przeciwdziałanie: wykrywanie ukrywania danych w strukturach systemu plików
  - Technika anti-forensics: Alternate Data Streams (ADS)
  - Anti-forensics Technique: Trail Obfuscation
  - Przeciwdziałanie: wykrywanie niezgodności rozszerzeń plików (file extension mismatch) z użyciem Autopsy
- Zrozumienie technik usuwania artefaktów (artifact wiping), wykrywania nadpisanych danych/metadanych oraz szyfrowania
  - Anti-forensics Technique: Artifact Wiping
  - Technika anti-forensics: nadpisywanie danych/metadanych
  - Anti-forensics Technique: Encryption
- Wykrywanie program packers oraz technik minimalizujących footprint
  - Anti-forensics Technique: Program Packers
  - Techniki anti-forensics minimalizujące footprint
  - Anti-forensics Countermeasures

- Moduł 6 - Informatyka śledcza systemu Windows
  - Zrozumienie Windows Forensics
    - Wprowadzenie do Windows Forensics
    - Metodyka Windows Forensics
  - Pozyskiwanie informacji ulotnych (volatile)
    - Pozyskiwanie informacji ulotnych (volatile)
  - Pozyskiwanie informacji nieulotnych (non-volatile)
    - Pozyskiwanie informacji nieulotnych (non-volatile)
  - Wykonywanie analizy pamięci Windows
    - Analiza pamięci Windows
    - Windows Crash Dump
    - Pozyskiwanie pamięci procesu (process memory)
    - Memory Forensics
  - Wykonywanie analizy rejestru Windows

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

- Analiza rejestru Windows
- Windows Registry Analysis Using Magnet AXIOM

- Wykonywanie analizy aplikacji Electron
  - Electron Application Forensics
  - Pozyskiwanie danych z Microsoft Teams
  - Pozyskiwanie danych z WhatsApp
  - Pozyskiwanie danych ze Skype
- Wykonywanie Web Browser Forensics
  - Web Browser Forensics
  - Analiza cache, cookies i historii: Mozilla Firefox
  - Analiza cache, cookies i historii: Google Chrome
  - Analiza cache, cookies i historii: Microsoft Edge
  - Odzyskiwanie danych z trybu Private Browsing i artefaktów przeglądarki
  - Carving plików bazy danych SQLite z użyciem FTK® Imager
- Badanie plików Windows i metadanych
  - Analiza plików Windows
  - Dochodzenie metadanych (metadata investigation)
- Zrozumienie ShellBags, plików LNK i Jump Lists
  - Windows ShellBags
  - Analiza plików LNK
  - Analiza Jump Lists
- Zrozumienie logów tekstowych oraz Windows Event Logs
  - Zrozumienie zdarzeń (events)
  - Typy zdarzeń logowania (logon events)
  - Format pliku Event Log
  - Organizacja rekordów zdarzeń (event records)
  - ELF_LOGFILE_HEADER Structure
  - EventLogRecord Structure
  - Windows 11 Event Logs
  - Ocena zdarzeń zarządzania kontami (account management events)
  - Event Logs
  - Windows Forensics Tools
  - Hashing w PowerShell: użycie Get-FileHash

- Moduł 7 - Informatyka śledcza systemów Linux i macOS
  - Pozyskiwanie informacji ulotnych (volatile) w Linux
    - Wprowadzenie do Linux Forensics

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

- Pozyskiwanie informacji ulotnych (volatile)
- Pozyskiwanie informacji nieulotnych (non-volatile) w Linux
  - Pozyskiwanie informacji nieulotnych (non-volatile)
- Zrozumienie Linux Memory Forensics
  - Linux Memory Forensics
- Zrozumienie Mac Forensics
  - Wprowadzenie do Mac Forensics
  - Mac Forensics Data
  - Mac Log Files
  - Mac Directories
- Pozyskiwanie informacji ulotnych (volatile) w macOS
  - Pozyskiwanie informacji ulotnych (volatile)
- Pozyskiwanie informacji nieulotnych (non-volatile) w macOS
  - Pozyskiwanie informacji nieulotnych (non-volatile)
- Zrozumienie Mac Memory Forensics oraz narzędzi Mac Forensics
  - Mac Memory Forensics
  - APFS Analysis
  - Parsowanie metadanych Spotlight
  - Mac Forensics Tools

- Moduł 8 - Informatyka śledcza sieci
  - Zrozumienie Network Forensics
    - Wprowadzenie do Network Forensics
    - Analiza postmortem i w czasie rzeczywistym (real-time)
    - Ataki sieciowe (network attacks)
    - Indicators of Compromise (IoCs)
    - Gdzie szukać dowodów (evidence)
    - Typy dowodów sieciowych (network-based evidence)
  - Podsumowanie koncepcji korelacji zdarzeń (event correlation)
    - Event Correlation
    - Types of Event Correlation
    - Prerequisites of Event Correlation
    - Event Correlation Approaches
  - Identyfikacja Indicators of Compromise (IoCs) na podstawie logów sieciowych
    - Log Files as Evidence
    - Analyzing Firewall Logs
    - Analyzing IDS Logs

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

- Analyzing Honeypot Logs
- Analyzing Router Logs
- Analyzing DHCP Logs
- Analyzing Cisco Switch Logs
- Analyzing VPN Logs
- Analyzing SSH Logs
- Analyzing DNS Server Logs
- Network Log Analysis Tools

- Badanie ruchu sieciowego (network traffic)
  - Dlaczego badać ruch sieciowy?
  - Pozyskiwanie dowodów z użyciem snifferów
  - Narzędzia do sniffingu
  - Analiza ruchu dla ataku DoS typu TCP SYN Flood
  - Analiza ruchu dla ataku DoS typu SYN-FIN Flood
  - Analiza ruchu dla ataku ICMP Flood
  - Analiza ruchu dla ataku UDP Flood
  - Analiza ruchu dla ataku HTTP Flood
  - Analiza ruchu pod kątem prób FTP Password Cracking
  - Analiza ruchu pod kątem prób SMB Password Cracking
  - Analyze Traffic for Sniffing Attempts
  - Analiza ruchu dla ataku SMTP HELO Flood
  - Analiza ruchu w celu wykrycia aktywności malware
  - Analyze Network Traffic through NetFlow
  - Network Forensic Analysis Using Dshell
  - Tools for Investigating Network Traffic
- Wykrywanie i badanie incydentów z użyciem narzędzi SIEM
  - Centralized Logging Using SIEM Solutions
  - SIEM Solutions
  - Examine Brute-force Attack
  - Examine DoS Attack
  - Examine Malware Activity
  - Badanie prób eksfiltracji danych przez FTP
  - Examine Network Scanning Attempts
  - Examine Ransomware Attack
  - Wykrywanie Rogue DNS Server (DNS Hijacking/DNS Spoofing)
- Zrozumienie Wireless Network Forensics

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

- Wprowadzenie do Wireless Network Forensics
- Wyzwania i ryzyka Wireless Network Forensics
- Types of Wireless Evidence
- Wireless Network Forensics Process

- Wykrywanie i badanie ataków na sieci bezprzewodowe
  - Detect Rogue Access Points
  - Wykrywanie prób spoofingu adresu MAC Access Point
  - Detect Misconfigured Access Points
  - Wykrywanie prób Wi-Fi jamming z użyciem Wireshark
  - Analyze Wireless Packet Captures
  - Analyze Wi-Fi Spectrum
  - Analyze the Wireless Network Report
  - Narzędzia do badania ruchu w sieciach bezprzewodowych

- Moduł 9 - Informatyka śledcza złośliwego oprogramowania (Malware Forensics)
  - Zrozumienie podstawowych pojęć związanych z malware
    - Wprowadzenie do malware
    - Różne sposoby, w jakie malware może dostać się do systemu
    - Najczęstsze techniki wykorzystywane przez atakujących do dystrybucji malware w sieci (web)
    - Komponenty malware
  - Zrozumienie Malware Forensics
    - Wprowadzenie do Malware Forensics
    - Dlaczego analizować malware?
    - Wyzwania analizy malware
    - Artefakty Malware Forensics
    - Indicators of Malware (wskaźniki infekcji)
    - Znaczenie przygotowania kontrolowanego laboratorium do analizy malware
    - Przygotowanie testbedu do analizy malware
    - Narzędzia do analizy malware
    - Dokumentacja przed analizą
    - Rodzaje analizy malware
  - Wykonywanie statycznej analizy malware
    - Statyczna analiza malware: fingerprinting plików
    - Statyczna analiza malware: lokalne i online skanowanie pod kątem malware
    - Statyczna analiza malware: wyszukiwanie ciągów znaków (strings)
    - Statyczna analiza malware: identyfikacja metod packingu/obfuskacji

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

- Statyczna analiza malware: informacje o plikach Portable Executable (PE)
- Statyczna analiza malware: identyfikacja zależności pliku (dependencies)
- Statyczna analiza malware: disassembly malware
- Statyczna analiza malware: analiza plików wykonywalnych ELF
- Statyczna analiza malware: analiza plików wykonywalnych Mach-O

- Analiza podejrzanych dokumentów
  - Analiza podejrzanego dokumentu MS Office
  - Analiza podejrzanego dokumentu MS Excel
  - Analiza podejrzanego dokumentu PDF
- Wykonywanie analizy zachowania systemu (system behavior)
  - Analiza zachowania systemu: monitorowanie artefaktów rejestru (Registry)
  - Analiza zachowania systemu: monitorowanie procesów
  - Analiza zachowania systemu: monitorowanie usług Windows
  - Analiza zachowania systemu: monitorowanie programów startowych (startup)
  - Analiza zachowania systemu: monitorowanie Windows Event Logs
  - Analiza zachowania systemu: monitorowanie wywołań API (API calls)
  - Analiza zachowania systemu: monitorowanie sterowników urządzeń (device drivers)
  - Analiza zachowania systemu: monitorowanie instalacji
  - Analiza zachowania systemu: monitorowanie wywołań systemowych (system calls)
  - Analiza zachowania systemu: monitorowanie zadań zaplanowanych (Scheduled Tasks)
  - Analiza zachowania systemu: monitorowanie plików i folderów
- Wykonywanie analizy zachowania sieci (network behavior)
  - Analiza zachowania sieci: monitorowanie aktywności sieciowej
  - Analiza zachowania sieci: monitorowanie portów
  - Analiza zachowania sieci: monitorowanie DNS
  - Analiza zachowania sieci: monitorowanie aktywności przeglądarki
- Wykonywanie analizy ransomware
  - Ransomware Analysis - BlackCat (ALPHV)

- Moduł 10 - Badanie ataków na aplikacje webowe
  - Zrozumienie Web Application Forensics
    - Wprowadzenie do Web Application Forensics
    - Wyzwania w Web Application Forensics
    - Wskaźniki ataku webowego (web attack indicators)
    - OWASP Top 10 Application Security Risks - 2021
    - Zagrożenia dla aplikacji webowych (web application threats)

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

- Metodyka dochodzenia w przypadku ataków webowych (web attack investigation methodology)
- Zrozumienie logów Internet Information Services (IIS)
  - Architektura IIS Web Server
  - Logi IIS
  - Analiza logów IIS
  - Analiza IIS HTTP Logs z użyciem HttpLogBrowser
  - Narzędzia do analizy logów IIS
- Zrozumienie logów Apache Web Server
  - Architektura Apache Web Server
  - Logi Apache Web Server
  - Apache Access Logs
  - Apache Error Logs
  - Analiza logów Apache Web Server z użyciem Python
  - Narzędzia do analizy logów Apache
- Wykrywanie i badanie różnych ataków na aplikacje webowe
  - Badanie ataku Cross-Site Scripting (XSS)
  - Badanie ataku SQL Injection
  - Badanie ataku Path/Directory Traversal
  - Badanie ataku Command Injection
  - Badanie ataku XML External Entity (XXE)
  - Badanie ataku Brute-force

- Moduł 11 - Informatyka śledcza Dark Web
  - Zrozumienie Dark Web oraz Dark Web Forensics
    - Zrozumienie Dark Web
    - Tor Relays
    - Zasada działania Tor Browser
    - Tor Bridge Node
    - Dark Web Forensics
    - Wyzwania Dark Web Forensics
  - Określenie, jak identyfikować ślady Tor Browser podczas dochodzenia
    - Identyfikacja artefaktów Tor Browser: Command Prompt
    - Identyfikacja artefaktów Tor Browser: Windows Registry
    - Identyfikacja artefaktów Tor Browser: pliki Prefetch
    - Identyfikacja artefaktów Tor Browser: plik places.sqlite
  - Wykonywanie Tor Browser Forensics

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

- Tor Browser Forensics: pozyskiwanie pamięci (memory acquisition)
- Zbieranie memory dumps
- Analiza memory dump: Bulk Extractor
- Forensic analysis memory dumps w celu zbadania artefaktów e-mail (Tor Browser Open)
- Forensic analysis storage w celu pozyskania załączników e-mail (Tor Browser Open)
- Forensic analysis memory dumps w celu zbadania artefaktów e-mail (Tor Browser Closed)
- Forensic analysis storage w celu pozyskania załączników e-mail (Tor Browser Closed)
- Forensic analysis: Tor Browser Uninstalled

- Moduł 12 - Informatyka śledcza w chmurze (Cloud Forensics)
  - Zrozumienie podstawowych pojęć Cloud Computing
    - Wprowadzenie do Cloud Computing
    - Typy usług Cloud Computing
    - Podział odpowiedzialności w chmurze (shared responsibility)
    - OWASP Top 10 Cloud Security Risks
    - Zagrożenia w Cloud Computing
    - Ataki na Cloud Computing
  - Zrozumienie Cloud Forensics
    - Wprowadzenie do Cloud Forensics
    - Zastosowania Cloud Forensics
    - Cybercrime w środowisku chmurowym
    - Cloud Forensics: interesariusze (stakeholders) i ich role
    - Wyzwania Cloud Forensics
  - Zrozumienie podstaw Amazon Web Services (AWS)
    - Wprowadzenie do Amazon Web Services (AWS)
    - Shared Responsibility Model dla AWS
    - Data Storage w AWS
    - Logi w AWS
  - Wykonywanie AWS Forensics
    - Forensic acquisition instancji Amazon EC2: metodyka
    - Zbieranie informacji z użyciem AWS-CLI
    - Badanie CloudWatch Logs
    - Badanie S3 Server Access Logs
    - Badanie AWS CloudTrail pod kątem incydentów IAM
    - Badanie Amazon VPC Flow Logs z użyciem AWS Management Console

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

- Analiza incydentów bezpieczeństwa AWS z użyciem GuardDuty
- Zrozumienie podstaw Microsoft Azure
  - Wprowadzenie do Microsoft Azure
  - Podział odpowiedzialności w Azure
  - Data Storage w Azure
  - Logi w Azure
- Wykonywanie Microsoft Azure Forensics
  - Forensic acquisition VM-ów w Azure: metodyka
  - Analiza Azure Monitor Logs
  - Zbieranie i analiza logów w Azure AD
  - Badanie incydentów bezpieczeństwa z użyciem Microsoft Azure Sentinel
- Zrozumienie podstaw Google Cloud
  - Wprowadzenie do Google Cloud
  - Shared Responsibility w Google Cloud
  - Data Storage w Google Cloud
  - Logi w Google Cloud
- Wykonywanie Google Cloud Forensics
  - Forensic acquisition wolumenów Persistent Disk w GCP: metodyka
  - Analiza Google Workspace Logs
  - Analiza danych logów z użyciem Google Cloud Log Analytics
  - Analiza Google Cloud VPC Flow Logs
  - Badanie incydentów bezpieczeństwa w Google Cloud
  - Badanie incydentów bezpieczeństwa kontenerów w Google Cloud
  - Badanie incydentów bezpieczeństwa opartych o VM w Google Cloud

- Moduł 13 - Informatyka śledcza poczty e-mail i mediów społecznościowych
  - Zrozumienie podstaw poczty e-mail
    - Wprowadzenie do systemu poczty e-mail
    - Komponenty biorące udział w komunikacji e-mail
    - Jak działa komunikacja e-mail?
    - Zrozumienie części składowych wiadomości e-mail
  - Wyjaśnienie dochodzenia w sprawach przestępstw e-mail (email crime investigation) i jego kroków
    - Wprowadzenie do dochodzeń w sprawach przestępstw e-mail
    - Kroki badania przestępstw e-mail (steps to investigate email crimes)
  - Zrozumienie przepisów USA dotyczących przestępstw e-mail
  - Przepisy USA przeciwko przestępstwom e-mail: CAN-SPAM Act

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

- Wyjaśnienie Social Media Forensics
  - Wprowadzenie do Social Media Forensics
  - Przestępstwa w social media
  - Wyzwania Social Media Forensics
  - Ręczne pozyskiwanie danych z platform social media
  - Pozyskiwanie dowodów z platform social media z użyciem WebPreserver
  - Ekstrakcja materiałów wideo (footage) z platform social media
  - Śledzenie aktywności użytkowników w social media z użyciem Social Searcher
  - Budowa i analiza grafów sieci społecznościowych (social network graphs)
  - Narzędzia Social Media Forensics
- Moduł 14 - Informatyka śledcza urządzeń mobilnych (Mobile Forensics)
  - Zrozumienie Mobile Device Forensics
    - Mobile Device Forensics
    - OWASP Mobile Top 10 (najnowsze wydanie)
    - Mobile Attacks
    - Mobile Hardware and Forensics
    - Mobile OS and Forensics
    - Mobile Forensics Challenges
  - Zrozumienie architektury Android i iOS, boot process oraz systemów plików
    - Mobile Device Architecture
    - Android OS Architecture
    - Android Boot Process
    - iOS Architecture
    - iOS Boot Process
    - Android File System
    - iOS File System
  - Zrozumienie procesu Mobile Forensics
    - Mobile Forensics Process
    - Android Forensics Process
    - iOS Forensics Process
  - Badanie danych z sieci komórkowych (cellular network data)
    - Components of Cellular Network
    - Different Cellular Networks
    - Cell Site Analysis: analiza danych operatora (service provider data)
    - CDR Contents
  - Pozyskiwanie systemu plików (file system acquisition)

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

- Subscriber Identity Module (SIM)
- Zrozumienie blokad telefonu, rootowania i jailbreaking urządzeń mobilnych
  - Phone Locking on Android
  - Phone Locking on iOS
  - Rooting of Android Devices
  - Jailbreaking of iOS Devices
- Wykonywanie logical acquisition na urządzeniach mobilnych
  - Logical Acquisition
  - Ekstrakcja danych z urządzeń Android z użyciem Magnet ACQUIRE
  - Cloud Data Acquisition na urządzeniach Android i iOS
  - Cloud Data Acquisition: użycie narzędzi komercyjnych
- Wykonywanie physical acquisition na urządzeniach mobilnych
  - Physical Acquisition
  - SQLite Database Extraction
  - JTAG Forensics
  - Chip-off Forensics
  - Flasher Boxes
- Wykonywanie analizy kryminalistycznej Android i iOS
  - Statyczna i dynamiczna analiza Android Package Kit (APK)
  - Android Logs
  - Examining Android Logs Using Logcat
  - Android Log Analysis Tools
  - Pozyskiwanie artefaktów WhatsApp z urządzeń Android
  - Analiza artefaktów Android Chrome
  - Analiza kryminalistyczna Android: użycie narzędzi komercyjnych
  - Ekstrakcja danych Signal z iOS z użyciem Belkasoft Evidence Center
  - Analiza artefaktów iOS Safari
  - Odszyfrowywanie i analiza iOS Keychains
  - Analiza kryminalistyczna iOS: użycie narzędzi komercyjnych

- Moduł 15 - Informatyka śledcza IoT
  - Zrozumienie pojęć IoT
    - Czym jest IoT?
    - Architektura IoT
    - Problemy bezpieczeństwa IoT
    - OWASP Top 10 IoT Threats
    - OWASP IoT Attack Surface Areas

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

- Ataki na IoT
- Wykonywanie forensics na urządzeniach IoT
  - Wprowadzenie do IoT Forensics
  - Proces IoT Forensics
  - Wyzwania IoT Forensics
  - Wearable IoT Device: Smartwatch
  - IoT Device Forensics: Smart Speaker—Amazon Echo
  - Analiza na poziomie sprzętowym (hardware): JTAG i Chip-off Forensics
  - Ekstrakcja i analiza danych z dronów/UAV
  - Narzędzia IoT Forensics

Wymagania:

Szkolenie jest przeznaczone dla specjalistów IT i informatyki śledczej posiadających podstawową wiedzę z zakresu IT/cyberbezpieczeństwa, informatyki śledczej, reagowania na incydenty oraz wektorów zagrożeń.

Poziom trudności

Certyfikaty:

Uczestnicy otrzymają certyfikaty ukończenia szkolenia podpisane przez EC-Council. Kurs wspiera również przygotowanie do egzaminu certyfikacyjnego CHFI.

Szczegóły egzaminu CHFI v11:

- Kod egzaminu: 312-49
- Liczba pytań: 150
- Czas trwania: 4 godziny
- Dostępność: ECC Exam Portal
- Próg zaliczenia: 60–85%
- Format: pytania wielokrotnego wyboru

Każdy uczestnik autoryzowanego szkolenia CHFI – Computer Hacking Forensic Investigator realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CHFI.

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

Prowadzący:

Certyfikowany instruktor EC-Council (CEI)

Informacje dodatkowe:

Materiały szkoleniowe obejmują oficjalne elektroniczne materiały EC-Council (courseware), 180-dniowy dostęp do iLabs oraz voucher egzaminacyjny.

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