Szkolenie: Mile2
C)NFE - Certified Network Forensics Examiner

DOSTĘPNE TERMINY

2024-09-16 | 5 dni | Kraków / Wirtualna sala
2024-09-16 | 5 dni | Virtual Classroom
2024-12-16 | 5 dni | Virtual Classroom
2024-12-16 | 5 dni | Warszawa / Wirtualna sala

Cel szkolenia:

Neutralne produktowo szkolenie Mile2 **C)NFE Certified Network Forensics Examiner**, które początkowo zostało opracowane dla jednej z agencji rządowych USA wraz z towarzyszącą mu certyfikacją **CNFE** (**Certified Network Forensics Examiner**) ma na celu poszerzenie wiedzy z **informatyki śledczej** o tematykę sieci komputerowych.

W trakcie szkolenia uczestnicy przechodzą przez ponad 20 modułów związanych z tematyką sieciowej **informatyki śledczej** oraz praktyczne laby przedstawiające rzeczywiste sytuacje. W szczególności poruszone zostają tematy dotyczące: badania i odzyskiwanie danych z ruchu sieciowego, przechwytywania ruchu, analizy, ataków na sieci bezprzewodowe, wykorzystania SNORT'a. Kurs koncentruje się również na centralnym zbieraniu i analizie logów.

Po ukończeniu szkolenia uczestnicy będą:

- posiadać wiedzę potrzebną do przeprowadzania analizy śledczej bazującej na dowodach sieciowych
- posiadać wiedzę, która pomoże prawidłowo i profesjonalnie przedstawiać wyniki badań w postaci raportów
- przygotowani do **egzaminu CNFE**

Kurs skierowany jest do:

- pracowników działów bezpieczeństwa IT
- kierowników działów informatycznych
- agentów/funkcjonariuszów policji
- właścicieli danych
- administratorów systemów IT
- Osoby prowadzący dochodzenia śledcze w których badane są dowody sieciowe
- Wszystkich osób zainteresowanych tematyką informatyki śledczej

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

Akredytacje i wyróżnienia

Mile2® jest:

- AKREDYTOWANE przez NSA CNSS 4011-4016
- WSKAZANE przez NIST / Homeland Security NICCS's Cyber Security Workforce Framework
- ZAAKCEPTOWANE przez FBI Cyber Security Certification Requirement list (Tier 1-3)

Plan szkolenia:

- Pojęcia dotyczące dowodów cyfrowych
- Wyzwania związane z dowodami sieciowymi
- Metodyka śledcza sieciowego
- Dowody oparte na danych sieciowych
- Podstawy sieci
- Protokoły internetowe
- Fizyczne przechwytywanie ruchu
- Oprogramowanie do przechwytywania ruchu
- Przechwytywania ruchu na żywo
- Analiza
- Protokół warstwy 2
- Bezprzewodowe punkty dostępowe
- Przechwytywanie i analiza ruchu bezprzewodowego
- Ataki na sieci bezprzewodowe
- NIDS Snort
- Scentralizowane logowanie i Syslog
- Badanie urządzeń sieciowych
- Web proxy i szyfrowanie
- Skanowanie w tunelu sieciowym
- Wykrywanie złośliwego oprogramowania

Laboratorium:

- Moduł 4, 5 i 6: Praca z plikami z przechwyconym ruchem (pcap files)
- Moduł 7, 8, 9 10, 11: Pozyskiwanie dowodów
- Moduł 12, 13, 14: Pozyskiwanie dowodów w ruchu bezprzewodowym
- Moduł 15: Systemy IDS/IPS w zadaniach analizy śledczej

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Moduł 16 i 21: Sieciowa analiza śledcza i dzienniki śledcze
- Moduł 17 i 18: SSL i szyfrowanie
- Moduł 20: Wykrywanie złośliwego oprogramowania

Wymagania:

- Posiadanie dowolnego **certyfikatu** z zakresu **informatyki śledczej** np. **CDFE Certified Digital Forensics Examiner** lub równoważnej wiedzy.
- Dwa lata doświadczenia związanego z **bezpieczeństwem IT**
- Znajomość modelu **TCP/IP** w praktyce

Poziom trudności

Certyfikaty:

Uczestnicy szkolenia otrzymują **certyfikat** ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę **Mile2**. Ponadto kurs ten przygotowuje uczestników do **certyfikowanego egzaminu Certified Network Forensics Examiner**, który jest realizowany za pośrednictwem systemu egzaminacyjnego Mile2 (Mile2 Assessment & Certification System "MACS"),

Egzamin trwa 2 godziny i składa się z 100 pytań wielokrotnego wyboru.

Każdy uczestnik autoryzowanego C)NFE - Certified Network Forensics Examiner otrzymuje bezpłatny voucher na egzamin CNFE.

Prowadzący:

Autoryzowany instruktor Mile2 (Certified Mile2 Instructor).

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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