Szkolenie: Mile2
C)IHE - Certified Incident Handling Engineer

DOSTĘPNE TERMINY

2026-11-16 | 5 dni | Warszawa / Wirtualna sala *(Termin gwarantowany, Last minute)*
2026-12-14 | 5 dni | Virtual Classroom

Cel szkolenia:

Neutralne produktowo szkolenie Mile2 **C)IHE Certified Incident Handling Engineer** ma na celu pomóc pracownikom odpowiedzialnym za obsługę incydentów (**Incident Handlers**), **administratorom systemowym** oraz wszelkim **inżynierom ds. bezpieczeństwa** w zrozumieniu jak planować, tworzyć i wykorzystywać swoje systemy, aby zapobiegać atakom, wykrywać je i właściwie reagować na nie.

Podczas tego szczegółowego szkolenia uczestnicy poznają krok po kroku metody stosowane przez hakerów na całym świecie, najnowsze wektory ataku oraz sposoby ochrony przed nimi, procedury postępowania w przypadku incydentu (w tym opracowanie procesu od początku do końca i ustanowienie zespołu do obsługi incydentów), strategie dla każdego rodzaju ataku, odzyskiwanie po nich danych i wiele więcej.

Ponadto uczestnicy będą mogli korzystać z wielu praktycznych ćwiczeń laboratoryjnych, które skupiają się na tematach takich jak rozpoznanie, ocena podatności przy użyciu Nessus, podsłuchiwanie sieci, manipulowanie aplikacjami internetowymi, złośliwe oprogramowanie i korzystanie z Netcat oraz kilka dodatkowych scenariuszy dla systemów Windows i Linux.

Absolwenci szkolenia Mile2 **C)IHE Certified Incident Handling Engineer** zdobywają wiedzę na temat bezpieczeństwa w realnym świecie, która umożliwia im rozpoznawanie słabych punktów, wykorzystywanie niedoskonałości systemu i ochronę przed zagrożeniami. Kurs obejmuje te same cele co szkolenie SANS® Security 504 i również przygotowuje uczestników do uzyskania **certyfikatów GCIH® oraz CIHE**.

Po ukończeniu szkolenia:

Uczestnicy kursu **Mile2 Certified Incident Handling Engineer** są w sposób kompetentny są przygotowani do **egzaminu certyfikacyjnego CIHE** jak również prezentują znajomość realnych zagadnień bezpieczeństwa, która umożliwia im rozpoznawanie zagrożeń oraz wykrywanie słabości systemów. W razie wystąpienia incydentu są przygotowani do podjęcia odpowiednich działań: identyfikacji ataku, powstrzymania i ograniczenia jego skutków, wykrycia przyczyn czy podjęcia odpowiednich działań naprawczych.

Kurs C)IHE skierowany jest do:

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

- pracownik ds. organizacyjnych środków ochrony informacji
- inżynierów i administratorów systemowych
- inżynierów bezpieczeństwa sieci
- administratorów systemów IT
- audytorów i kontrolerów
- pracowników instytucji rządowych
- dostawców rozwiązań bezpieczeństwa i konsultantów, które chcą być na bieżąco z ogólnymi ramami dotyczącymi bezpieczeństwa informacji

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:

- Wyjaśnienie pojęcia - obsługa incydentów
- Zagrożenia, podatności i exploity
- Przygotowanie
- Pierwsza reakcja
- Ograniczanie
- Eliminacja
- Odzyskiwanie
- Kontynuacja
- Doświadczony zespół reagowania na incydenty bezpieczeństwa komputerowego
- Zaawansowane - analiza plików dziennika zdarzeń
- Zaawansowane - złośliwe oprogramowanie, rootkity i botnety
- Zaawansowane - analiza artefaktów

Laboratorium:

- Wprowadzenie do narzędzi
- Ataki Cybernetyczne - sieci
- Ataki cybernetyczne - aplikacja internetowa
- Ataki cybernetyczne - wirusy
- System ticketowy

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

- Pakiet SysInternals
- Tworzenie i zarządzanie planem działania CSIRT
- Analiza logów
- Exploity i DoS
- Trojan Stuxnet: Analiza pamięci z Volatitlity
- Znajdowanie podatności

Wymagania:

- Minimum 12 miesięcy doświadczenia z technologiami sieciowymi
- Dobra znajomość protokołu TCP/IP
- Znajomość produktów firmy Microsoft
- Podstawowa znajomość systemów Linux i umiejętność pracy w tym środowisku jest niezbędna

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 Incident Handling Engineer**, 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 szkolenia C)IHE - Certified Incident Handling Engineer otrzymuje bezpłatny voucher na egzamin CIHE.

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. 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