Szkolenie: Compendium CE
Informatyka śledcza (computer forensics) - specjalista

Cel szkolenia:

Celem kursu **Informatyka śledcza (computer forensics) - specjalista** jest zapoznanie się z aktualnymi regulacjami prawa krajowego oraz międzynarodowego związanymi z **przestępczością komputerową** - **cyberprzestępczością**. Przedstawienie procesu opracowywania procedur reakcji na incydenty w oparciu o normy międzynarodowe z uwzględnieniem **polityki bezpieczeństwa** przedsiębiorstwa. Dostarczenie wiedzy potrzebnej do budowy i organizacji pracy zespołu reagowania na incydenty oraz zapoznanie z wymaganiami dotyczącymi przygotowania do prowadzenia działań związanych z incydentem w tym wykorzystania **informatyki śledczej**.

Jednocześnie uczestnicy szkolenia będą mogli nabyć umiejętności samodzielnego odszukiwania śladów włamania, odzyskiwania utraconych danych oraz przeprowadzania kompleksowej analizy incydentu w oparciu o wcześniej zebrane informacje. Uczestnik szkolenia pozna zbiór praktycznych zasad i reguł, które wdrożone w przedsiębiorstwie, zmniejszają ryzyko włamań i utraty firmowych danych. Dodatkowo, zapozna się z najczęściej wykorzystywanymi przez cyberprzestępców scenariuszami włamań do komputerów działających w oparciu o systemy operacyjne z rodziny **Microsoft Windows** i **GNU/Linux**.

Ponadto uczestnicy zapoznają się z aktualnymi aplikacjami oraz urządzeniami, które wspierają prowadzenie **śledztwa informatycznego** - **analizę powłamaniową**. Zostanie im dostarczona wiedza, w jaki sposób postępować z dowodami cyfrowymi oraz jak planowo prowadzić wszystkie czynności podczas analizy i w jaki sposób je dokumentować.

Plan szkolenia:

- Definicje przestępczości komputerowej - cyberprzestępczości funkcjonujące w literaturze przedmiotu.
- Klasyfikacja i podział cyberprzestępczości dokonywanej przez organizacje i instytucje międzynarodowe.
- Ochrona systemów komputerowych w wybranych przepisach prawa krajowego:
  - Ustawa Kodeks Karny
  - Ustawa o ochronie danych osobowych
  - Ustawa o ochronie własności intelektualnej
  - Ustawa o świadczeniu usług drogą elektroniczną.
- Klasyfikacje osób naruszających bezpieczeństwo systemów informatycznych, motywy ich działania oraz stosowane metody działania.

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

- Procedury postępowania w przypadku wystąpienia i ujawnienia incydentu, reakcja na incydent w oparciu o politykę bezpieczeństwa, organizacja zespołu reagowania. Terminologia związana z incydentem, analiza po włamaniowa oraz śledztwem komputerowym.
- Wytyczne i standardy określające prowadzenie analizy po włamaniowej, śledztwa komputerowego oraz zabezpieczanie dowodów cyfrowych.
- Zabezpieczanie danych cyfrowych w systemach informatycznych w tym:
  - działania w ramach tzw. TRIAGE -
  - Zabezpieczanie danych ulotnych w działającym systemie
  - Zabezpieczanie danych cyfrowych w systemie statycznym (wyłączonym)
  - Zabezpieczenia danych zdalnie (Cloud)
  - Zabezpieczanie danych sieciowych
  - Zabezpieczanie danych w systemach „Big Data”.
- Formaty stosowanych obrazów informatyki śledczej wraz ze sposobami ich weryfikacji.
- Dokumentowanie i przechowywanie dowodów cyfrowych na potrzeby dalszego postepowania po incydencie.
- Wyposażenie techniczne, sprzętowe i programowe, niezbędne w śledztwie informatycznym.
- Analiza logów systemowych. Ustalenie historii wykonywanych operacji. Śledzenie zmian w systemie.
- Wykrywanie rootkitów, backdorów, keyloggerów, koni trojańskich i innych anomalii systemowych.
- Analiza komunikatorów systemowych, przegląd historii odwiedzanych stron WWW i analiza poczty elektronicznej.
- Analiza potencjalnych kanałów dostępu do badanego komputera.
- Ukrywanie danych na dysku twardym. Sposoby ukrywania danych oraz metody ich ujawniania.
- Steganografia - ukrywanie tajnych informacji w "zwykłych" plikach. Dostęp do informacji zaszyfrowanych.
- Metody omijania haseł systemowych. Programy łamiące hasła zabezpieczające dostęp do plików.
- Odzyskiwanie danych usuniętych z dysku twardego, płyt CD/DVD, kart pamięci oraz pendrive'ów.
- Aplikacje i programy używane do odzyskiwania danych.
- Bezpieczne i trwałe usuwanie danych. Procedury kasowania danych oznaczonych klauzulą poufne i ściśle tajne.

- Laboratorium:
  - W trakcie szkolenia będą prowadzone ćwiczenia zapoznające z tematyką informatyki śledczej oraz możliwości jej wykorzystania w identyfikacji dowodów elektronicznych. W trakcie ćwiczeń wykorzystane zostaną programy i aplikacje stosowane przez organy ścigania na całym świecie. Każdy z uczestników mając odpowiednio wyposażoną stację komputerową przeprowadzi śledztwo informatyczne, którego celem będzie ustalenie i odpowiednia prezentacja dowodów działania cyberprzestępcy.

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

Wymagania:

- Dobra znajomość systemów MS Windows oraz systemów Linux/UNIX.
- Podstawowa znajomość infrastruktury klucza publicznego.
- Podstawowa wiedza z dziedziny sieci komputerowych (Internet):
  - Znajomość modelu ISO/OSI i zasad funkcjonowania protokołów TCP/IP, UDP, ICMP
  - Znajomość funkcjonowania i wykorzystania urządzeń (hub, switch, router, firewall, IDS/IPS)
  - Doświadczenie w korzystaniu z usług sieciowych (IM, poczta elektroniczna, strony WWW)

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują **certyfikat** sygnowany przez **Compendium Centrum Edukacyjne**.

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.

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