

## Szkolenie: Compendium CE Zabezpieczanie i monitoring sieci komputerowych



### Cel szkolenia:

Zapoznanie się z systemami zapewniającymi **bezpieczeństwo zasobów sieciowych**: zapory ogniowe, systemy IDS/ IPS, honeypoty, systemy monitorujące wymianę informacji. Omówienie sposobów analizowania ruchu sieciowego, logów i prawidłowej identyfikacji zdarzeń. Przedstawienie metod bezpiecznego gromadzenia logów i zarządzania nimi.

### Plan szkolenia:

- Podstawy zabezpieczania sieci - systemy Firewall
  - typy Firewalli
  - konfiguracja Firewalla
  - ustalanie zestawu reguł Firewalla
  - systemy UTM
- Konfiguracja urządzeń sieciowych pod kątem monitorowania i analizy ruchu
- Systemy wykrywania włamań
  - IDS hostowy
  - IDS sieciowy
  - określanie zasad monitorowania zdarzeń
  - reakcje na incydent
- HoneyPot - „garnek miodu”
  - typy honeypotów
  - instalacja i konfiguracja
- Kontrola ruchu sieciowego
  - analiza ruchu sieciowego
  - natężenie ruchu i statystyki
  - SNMP w analizie ruchu sieciowego
  - RMON
  - Netflow
  - Sflow
- Zarządzanie logami
  - logi systemowe
  - logi z systemów bezpieczeństwa

- strategia archiwizacji logów
- Warsztaty:
  - Instalacja i konfiguracja zapory ogniowej
  - Instalacja i konfiguracja systemów IDS/IPS
  - Instalacja i konfiguracja honeypota
  - Analiza ruchu sieciowego

## Wymagania:

Znajomość protokołów TCP/ IP, modelu sieci według OSI i zagadnień sieciowych, podstawy administracji systemu Windows, podstawy administracji systemów Linux/Unix.

## Poziom trudności



## Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat wystawiony imiennie oraz na firmę, sygnowany przez Compendium Centrum Edukacyjne.

## Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.

## Informacje dodatkowe:

- Punkty CPE (CISSP) za udział w szkoleniu:

Uczestnicy tego szkolenia, którzy posiadają aktualną **certyfikację System Security Certified Practitioner (SSCP)** lub **Certified Information Systems Security Professional (CISSP)** mogą zdobyć jeden punkt Continuing Professional Education (CPE) za każdą godzinę szkolenia (1 CPE za pełną godzinę edukacyjną, co daje 6 CPE za standardowy dzień szkolenia w Compendium CE - ale nie więcej niż 8 CPE dziennie). W celu przyznania punktów CPE członkowie (ISC) 2 muszą samodzielnie zgłosić udział w naszym szkoleniu do (ISC)2 i muszą zachować dowód udziału (certyfikat uczestnictwa w szkoleniu) w przypadku konieczności potwierdzenia tego faktu w (ISC)2. Więcej informacji pod adresem <https://www.isc2.org/cpes/default.aspx> (dostęp tylko dla członków (ISC)2).