kod szkolenia: SPLUS+ / PL AA 5d

Warsztaty z CompTIA Security + (przygotowanie do egzaminu SY0-601)

CompTIA Security+ to międzynarodowy certyfikat potwierdzający wiedzę i umiejętności dotyczące zagadnień z zakresu bezpieczeństwa IT. Jest honorowany na całym świecie nie tylko w branży IT ale również przez instytucje publiczne oraz różne organizacje międzynarodowe.

Przeznaczenie szkolenia

Szkolenie skierowane do administratorów sieci, osób odpowiedzialnych za infrastrukturę informatyczną oraz każdego, kto planuje podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji.
Osoby nie będące specjalistami z zakresu bezpieczeństwa IT będą mogły zwiększyć świadomość dotyczącą zagrożeń oraz poznać różne metody ataków na systemy i sieci teleinformatyczne powszechnie stosowane przez hakerów.
Również specjaliści ds. bezpieczeństwa informatycznego, audytorzy i tzw. security officers będą mogli ugruntować, usystematyzować bądź uzupełnić swoją wiedzę z zakresu cyberbezpieczeństwa.

Korzyści wynikające z ukończenia szkolenia

Szkolenie dostarczy uczestnikom wiedzy z zakresu m.in. analizy ryzyka, planowania ciągłości działania, bezpieczeństwa informacyjnego, bezpieczeństwa systemów i sieci teleinformatycznych.
Ponadto uczestnicy poznają najczęściej wykorzystywane narzędzia i metody zabezpieczania systemów i sieci teleinformatycznych oraz danych w nich przetwarzanych. Poznają również szerokie spektrum różnych metod i narzędzi, którymi posługują się cyberprzestępcy.

Oczekiwane przygotowanie słuchaczy

Ogólna znajomość zagadnień informatycznych oraz pojęć związanych z sieciami komputerowymi i umiejętność sprawnej obsługi komputera. Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.

Język szkolenia

- Szkolenie: polski
- Materiały: angielski

Szkolenie obejmuje

Autoryzowany podręcznik: The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601) eBook

Czas trwania

5 dni / 35 godzin

Agenda szkolenia

- Role w bezpieczeństwie
- Analiza zagrożeń i ocena bezpieczeństwa
- Inżynieria społeczna i złośliwe oprogramowanie
- Podstawowe pojęcia i koncepcje kryptograficzne
- Infrastruktura klucza publicznego
- Bezpieczne uwierzytelnianie, kontrola zarządzania tożsamością i kontem
- Bezpieczna architektura sieciowa
- Urządzenia zabezpieczające sieć
- Bezpieczne protokoły sieciowe
- Bezpieczeństwo hosta

- Bezpieczeństwo rozwiązań mobilnych
- Koncepcja bezpiecznych aplikacji
- Bezpieczeństwo rozwiązań w chmurze
- Podstawowe pojęcia dotyczące prywatności i ochrony danych
- Reagowanie na incydent
- Kryminalistyka cyfrowa
- Zarządzanie ryzykiem i planowanie ciągłości działania
- Koncepcje budowania cyberodporności
- Bezpieczeństwo fizyczne
- Omówienie egzaminu CompTIA Security +