Kod szkolenia: **HL948S**

Tytuł szkolenia: **Zarządzanie Strategią Bezpieczeństwa Informacji**

Information Security Governance and Policies

Dni: 2

Authorized HP Training Reseller

Opis:

Ten dwudniowy kurs pokazuje profesjonalistom IT oraz oficerom bezpieczeństwa jak utworzyć oraz efektywnie zarządzać strategią bezpieczeństwa w organizacji. Uczestnicy poznają jak regulacje zgodności, standardy firmowe oraz najlepsze aktyki mogą doprowadzić do stworzenia odpowiedniej polityki bezpieczeństwa. Ten kurs skupia się na realnych implementacjach, a także pomaga przygotować się do egzaminów Security+ and CISSP.

Wymagania

Uczestnictwo w kursie Enterprise Security Foundation (HL945S) lub równoważna wiedza.

Informacje dodatkowe

Szkolenie może być zrealizowane w języku polskim lub angielskim. Uczestnicy otrzymują akredytowane materiały szkoleniowe w języku angielskim.

Program szkolenia:

Moduł 1: Wprowadzenie.

- Polityka Bezpieczeństwa i zarządzania.
- Logistyka.
- Profil uczestników.
- Kilka słów o certyfikacji.

Moduł 2: Bezpieczeństwo Informacji.

- Bezpieczeństwo to w 10% produkty a w 90% procesy.
- Koszty cyberprzestępstw.
- Wytyczne i prawo w US, Kanadzie i APEC.
- Ochrona danych w Europie.
- Poufność, Integralność, Dostępność (CIA).
- Ryzyko.
- Analiz wpływu na organizację.
- Ocena ryzyka i bilans ryzyka.
- Zagrożenia i podatności.
- Zabezpieczenia.
- Ocena wartości zasobów.

Moduł 3: Zdefiniuj swoja strategię bezpieczeństwa.

- Strategia bezpieczeństwa a biznes.
- Wymagania zgodności: reguły bezpieczeństwa HIPAA.
- Przykłady.
- Relacje pomiędzy misją organizacji, kulturą korporacji oraz strategią bezpieczeństwa i polityką.
- Wdrożenie koncepcji bezpieczeństwa i ryzyka w kontekście wymagań organizacji.
- Ocena wymagań organizacji w celu zbudowania strategii bezpieczeństwa.
- Proces wdrażania strategii zarządzania bezpieczeństwem.

Moduł 4: Zarządzanie bezpieczeństwem.

- Polityka bezpieczeństwa i zarządzanie.
- Silne bezpieczeństwo jako przewaga konkurencji.
- Przykład jako ocena propozycji.
- Rola Oficera Bezpieczeństwa.
- Rola zarządu jako element sukcesu wdrożenia planu bezpieczeństwa.
- Inne ważne role: zbuduj swój zespół.

Moduł 5: Struktura polityki bezpieczeństwa

- Atrybuty dobrej polityki bezpieczeństwa.
- Różnice pomiędzy politykami a procedurami.
- Zgodność.
- Wymagania bezpieczeństwa w HIPAA.
- Standard bezpieczeństwa danych PCI.
- Dyrektywa UE 2009/136/EC.
- Regulacja IT - India 2000.
- Rola zgodności z wymaganiami we wdrażaniu polityk.

Moduł 6: Polityki w Twojej strategii bezpieczeństwa.

- 10 najważniejszych polityk SANS.
- Wybrane polityki bezpieczeństwa pozwolą Ci rozpocząć.
- Polityka dostępu.
- Polityka dostępu do sieci.
- Polityka zdalnego dostępu.
- Polityka urządzeń osobistych.
- Polityka oceny ryzyka.
- Polityka planowania na wypadek awarii.
- Polityka bezpieczeństwa fizycznego.
- Polityka kontroli dostępu.
- Retencja danych oraz polityka deklasyfikacji.
- Rozważania na temat zgodności (HIPAA).
- 6 praw zgodności.
- Wpływ regulacji zgodności na konkretne polityki.
- Jakich polityki bezpieczeństwa wymaga twoja organizacja.

Moduł 7: Ramy budowania polityki.

- Dlaczego używać wytycznych?
- Ramy struktur Twoich polityk.
- ISC(2) 10 domen jako ramy/przykład.
- ISO 17799:2000.
- PCI.
- Identyfikacja polityk.
- ISO 27001.
- Przygotowanie podstawowych polityk bezpieczeństwa używając standardów organizacyjnych, jako wytyczne.