CompTIA Security+

Course code: CTSEC

Tento unikátní 5denní kurz je základní přípravou pro celosvětově uznávanou certifikační zkoušku CompTIA Security+ SY0-701, která je dnes standardem pro IT certifikaci v oblasti bezpečnosti. Jedná se o úvodní školení v oblasti správy bezpečnosti počítačových sítí a operačních systémů na platformě OS Windows. Uchazeči získají souhrnný přehled IT bezpečnostních řešení a získají možnost si prakticky vyzkoušet implementaci různých bezpečnostních opatření. Díky vedoucí úloze bezpečnosti v IT prostředí všech firem a dlouholeté tradici této certifikační zkoušky je CompTIA Security + školení bezesporu zásadní výhodou pro IT pracovníky na všech pozicích.

Pro koho je kurz určen

Kurz je určen pokročilým uživatelům počítačů a začínajícím bezpečnostním administrátorům

Co vás naučíme

- Porozumět základním konceptům identifikace a řešení bezpečnostních rizik
- Porozumět základním konceptům kryptografie a správně je využívat – symetrické klíče, certifikáty
- Získáte přehled nejzranitelnějších částí síťové infrastruktury TCP/IP a jejich řešení
- Porozumíte prinipům ochrany e-mailové komunikace, vzdálených připojení VPN, bezdrátových sítí a dalších metod komunikace
- Porozumíte principům ověřování identity
- Jak nastavovat uživatelské skupiny, jejich práva a přístupová oprávnění
- Implementovat bezpečnostní opatření a updaty
- Porozumíte základním konceptům bezpečnostních politik od zajištění fyzické bezpečnosti po zachování chodu firmy
- Vytváření bezpečnostní dokumentace a security incident handling

Požadované vstupní znalosti

Uchazeči by měli mít znalosti na úrovni certifikace CompTIA A+, Network+ nebo ekvivalentní praktické zkušenosti v oblasti administrace sítí a operačních systémů Microsoft. Uchazeči by měli mít velmi dobré zkušenosti v oblasti konfigurace sítě.

Osnova kurzu

1. Základy bezpečnosti

- Cyklus informační bezpečnosti
- Základy bezpečnostních politik
- Ověřovací metody
- Základy kryptografie

2. Bezpečnostní hrozby a zranitelnosti

- Sociální inženýrství
- Hrozby fyzického přístupu
- Hrozby v síťovém prostředí
- Rizika a zranitelnosti bezdrátových sítí
- Rizika chybně naprogramovaných aplikací

3. Síťová bezpečnost

- Přehled síťových zařízení z pohledu bezpečnosti
- Koncept síťové bezpečnosti
- Ukázky síťových útoků
- Zabezpeční běžného síťového provozu
- Zabezpečení infrastruktury bezdrátových sítí

4. Zabezpečení aplikací, dat a prvků

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Základní pravidla zabezpečení stanic
- Základní pravidla zabezpečení serverů
- Zabezpečení dat
- Zabezpečení mobilních zařízení
- Možnost zabezpečení aplikací

5. Správa identit a přístupu
   - Typy autentizací
   - Smart karty a tokeny
   - Strategie skupin
   - Správa přístupu pomocí ACL
   - RADIUS server a 802.1x
   - VLAN management
   - Správa přístupu do VPN
   - WPA1/2 Enterprise
6. Správa PKI a certifikátů
   - Koncept PKI
   - Možnost využití certifikátů
   - Instalace Enterprise certifikační autority a správa šablon
   - Zálohování a obnova certifikační autority
   - Automatické vs. ruční vydávání certifikátů
   - Správa a zálohování privátních klíčů
7. Monitoring bezpečnosti
   - Auditování v OS
   - Auditování sítě
   - IDS/IPS
   - Honeypots
   - Antiviry
8. Zajištění dostupnosti, zachování chodu firmy a incident response
   - Základní koncepty zajištění funkčnosti firmy
   - SLA
   - Vysoká dostupnost
   - Zálohování a obnova
   - Co dělat, když dojde k napadení firmy

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk