



Enterprise Computing Solutions - Education Services

NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com
Phone: +420 597 488 811



Kód:	DÉLKA:	CENA:
OTH_CTSEC	40 Hours (5 DENNÍ)	Kč bez DPH 28,000.00

Description

Tento unikátní 5denní kurz je základní přípravou pro celosvětově uznávanou certifikační zkoušku CompTIA Security+ SY0-601, 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.

Cena školení pořádaného v Bratislavě je 1200 EUR bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem. A jsou vedená ve slovensky.

Toto školení pořádá společnost GOPAS a.s.

Cíle

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 principům 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

Určeno pro

Kurz je určen pokročilým uživatelům počítačů a začínajícím bezpečnostním administrátorům

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.

Program

	Cyklus informační bezpečnosti	
	Základy bezpečnostních politik	
	Ověřovací metody	
1. Základy bezpečnosti	Základy kryptografie	2. Bezpečnostní hrozby a zranitelnosti
Sociální inženýrství		Přehled síťových zařízení z pohledu bezpečnosti
Hrozby fyzického přístupu		Koncept síťové bezpečnosti
Hrozby v síťovém prostředí		Ukázky síťových útoků
Rizika a zranitelnosti bezdrátových sítí		Zabezpečení běžného síťového provozu
Rizika chybně naprogramovaných aplikací	3. Síťová bezpečnost	Zabezpečení infrastruktury bezdrátových sítí
	Základní pravidla zabezpečení stanic	
	Základní pravidla zabezpečení serverů	
	Zabezpečení dat	
	Zabezpečení mobilních zařízení	
4. Zabezpečení aplikací, dat a prvků	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

Koncept PKI

Možnost využití certifikátů

Instalace Enterprise certifikační autority a správa šablon

Zálohování a obnova certifikační autority

Automatické vs. ruční vydávání certifikátů

6. Správa PKI a certifikátů Správa a zálohování privátních klíčů

Auditování v OS

Auditování sítě

IDS/IPS

Honeypots

7. Monitoring bezpečnosti 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

Termíny školení

Termíny školení na vyžádání, [kontaktujte nás prosím](#)

Dodatečné informace

Školení je možné zajistit na míru. [Kontaktujte nás pro bližší informace.](#)