SCOR

Implementace a správa hlavních bezpečnostních technologií Cisco

Popis:

Tento autorizovaný pětidenní kurz je zaměřen na implementaci a správu bezpečnostních technologií včetně síťové bezpečnosti, cloudové bezpečnosti, bezpečnosti obsahu, bezpečnosti koncových bodů, zabezpečený síťový přístup, viditelnost, detekce a vynucování pravidel.

Absolvent kurzu bude umět:

- Popsat koncepty informační bezpečnosti a bezpečnostní strategie v síti
- Popsat různé druhy útoků na aplikace, koncové body sítě a stanice
- Popsat různé technologie pro zabezpečení sítí a jak se doplňují při ochraně proti útokům
- Nastavovat Cisco ASA a Cisco Firewpower Next-Generation Firewall
- Nastavit zabezpečení elektronické pošty pomocí Cisco Email Security Appliance
- Nastavit zabezpečení pomocí Cisco Web Security Appliance
- Popsat možnosti, modely nasazení, správu politik a konzoly Cisco Umbrella
- Vybrat a nastavit site-to-site VPN technologie pomocí Cisco ASA a Cisco FirePower NGFW
- Nasadit vzdálený přístup (remote access) využitím 802.1x a EAP autentizace
- Nastavit různé bezpečnostní funkcionality pro ochranu řídící, správcovské a datové vrstvy (Control/management/Data plane) na Cisco zařízeních jako jsou switche a routery
- Znát základy bezpečnosti a rizik cloud computingu a jak zabezpečit Cloudové prostředí

Požadavky pro absolvování kurzu:

- Účast na kurzu CCNA certifikaci, nebo adekvátní znalosti
- Znalosti základních bezpečnostních konceptů

Kurz určen pro:

- Síťové administrátory
- Zájemce o zkoušku 350-701 SCOR, která je součástí CCNP Security (Cisco Certified Network Professional), CCIE Security a Cisco Certified Specialist - Security Core

Literatura:

Všichni účastníci školení obdrží originál studijních certifikovaných materiálů Cisco.

Technické vybavení:

Všechna cvičení jsou prováděna ve virtuálním laboratorním prostředí, vyvinutém a dodaném speciálně pro toto školení firmou Cisco. Všechny učebny jsou vybaveny nadstandardními počítači připojenými k Internetu, učebny jsou prostorné, klimatizované, bezbariérové a s připojením na Wi-Fi. V případě zájmu lze školení absolvovat online live.

Osnova:

- Popis technologií pro zabezpečení sítě
- Nasazení Cisco ASA Firewall
- Nasazení Cisco Firepower Next-generation Firewall
- Nasazení Email Content Security
- Nasazení Web Content Security
- Popis VPN technologií a kryptografických konceptů (VPN – Virtuální privátní sítě)
- Úvod do Site-to-Site VPN
- Nasazení Cisco IOS VTI point-to-point IPSec VPN
- Úvod do Cisco Secure Remote Access VPN řešení (řešení pro vzdálený přístup uživatelů)
- Nasazení SSL VPN na Cisco ASA a Cisco FirePower NGFW
- *Popis bezpečnostních konceptů **
- *Popis útoků na TCP/IP **
- *Popis útoků na síťové aplikace **
- *Popis útoků na koncové body **
- *Nasazení Cisco Umbrella **
- *Popis řešení Cisco Secure Network Access **
- *Popis 802.1x autentizace **
- *Nastavení 802.1x autentizace **
- *Popis technologií pro zabezpečení koncových bodů **
- *Nasazení Cisco AMP pro koncové body **
- *Úvod do ochrany síťové infrastruktury **
- *Nasazení bezpečnosti Control plane **
- *Nasazení bezpečnosti na 2. vrstvě **
- *Nasazení bezpečnosti na 3. vrstvě **
- *Nasazení bezpečnosti Management plane **
- *Nasazení telemetrie komunikace **
- *Nasazení Cisco Stealthwatch Enterprise **
- *Popis cloudových útoků **
- *Zabezpečení cloudu **
- *Nasazení Cisco Stealthwatch Cloud **
- *Popis SDN **

** Body osnovy psané kurzívou jsou dle oficiálních osnov společnosti Cisco definované jako samostudium.*

Kontaktujte nás
OKsystem a.s., Na Pankráci 1690/125, 140 00 Praha 4
(+420) 236 072 111 skoleni@oksystem.cz www.okskoleni.cz