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

Check Point Certified Security Administrator (CCSA) R82

Kód:	DÉLKA:	CENA:
CKT_CCSA_R82	24 Hours (3 DENNÍ)	Kč bez DPH 33,500.00

Description

Tento kurz poskytuje studentům základní znalosti, dovednosti a praktické zkušenosti potřebné ke konfiguraci, správě a monitorování stávajícího prostředí Quantum Security. Studenti se naučí, jak přistupovat k portálu Gaia a rozhraní příkazového řádku Gaia, spravovat přístup administrátorů, vytvářet a konfigurovat síťové objekty, vytvářet nové bezpečnostní politiky, konfigurovat vrstvy v definovaném pořadí a sdílenou vloženou vrstvu, analyzovat síťový provoz a monitorovat stav systému, konfigurovat identifikační povědomí (Identity Awareness), zvýšit úroveň zabezpečení pomocí inspekce HTTPS, konfigurovat řízení aplikací a filtrování URL a nastavit autonomní prevenci hrozeb.

Určeno pro

• Security Administrators
• Security Engineers
• Security Analysts
• Security Consultants
• Security Architects

Vstupní znalosti

Base Knowledge
• Unix-like and/or Windows OS
• Internet Fundamentals
• Networking Fundamentals
• Networking Security
• System Administration
• TCP/IP Networking
Check Point Courses
• Check Point Deployment Administrator (suggested)

Program

Module 1: Introduction to Quantum Security
• Identify the primary components of the Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.
Lab Tasks
• Explore Gaia on the Security Management Server
• Explore Gaia on the Dedicated Log Server
• Explore Gaia on the Security Gateway Cluster Members
• Connect to SmartConsole
• Navigate GATEWAYS & SERVERS Views
• Navigate SECURITY POLICIES Views
• Navigate LOGS & EVENTS Views
• Navigate MANAGE & SETTINGS Views

Module 2: Administrator Account Management
• Explain the purpose of SmartConsole administrator accounts.
• Identify useful features for administrator collaboration, such as session management, concurrent administration, and concurrent policy installation.
Lab Tasks

• Create New Administrators and Assign Profiles
• Test Administrator Profile Assignments
• Manage Concurrent Administrator Sessions
• Take Over Another Session and Verify Session Status

Module 3: Object Management
• Explain the purpose of SmartConsole Objects.
• Give examples of SmartConsole Physical and Logical Objects.
Lab Tasks
• View and Modify GATEWAYS & SERVERS Objects
• View and Modify Network Objects
• View and Modify Service Objects

Module 4: Security Policy Management
• Explain the purpose of Security Policies.
• Identify the essential elements of a Security Policy.
• Identify features and capabilities that enhance the configuration and management of the Security Policy.
Lab Tasks
• Verify the Security Policy
• Modify Security Policies
• Install the Standard Security Policy
• Test the Security Policy

Module 5: Policy Layers
• Demonstrate an understanding of the Check Point policy layer concept.
• Explain how policy layers affect traffic inspection.
Lab Tasks
• Add an Ordered Layer
• Configure and Deploy the Ordered Layer Rules
• Test the Ordered Layer Policy
• Create an Inline DMZ Layer
• Test the Inline DMZ Layer

Module 6: Security Operations Monitoring
• Explain the purpose of Security Operations Monitoring.
• Tune the Log Server configuration.
• Use predefined and custom queries to filter the logging results.
• Monitor the state of Check Point systems.
Lab Tasks
• Configure Log Management
• Enhance Rulebase View, Rules, and Logging
• Review Logs and Search for Data
• Configure the Monitoring Blade
• Monitor the Status of the Systems

Module 7: Identity Awareness
• Explain the purpose of the Identity Awareness solution.
• Identify the essential elements of Identity Awareness.
Lab Tasks
• Adjust the Security Policy for Identity Awareness
• Configure the Identity Collector
• Define the User Access Role
• Test Identity Awareness

Module 8: HTTPS Inspection
• Explain the purpose of the HTTPS Inspection solution.
• Identify the essential elements of HTTPS Inspection.
Lab Tasks
• Enable HTTPS Inspection
• Adjust Access Control Rules
• Deploy the Security Gateway Certificate
• Test and Analyze Policy with HTTPS Inspection

Module 9: Application Control and URL Filtering
• Explain the purpose of the Application Control and URL Filtering solutions.
• Identify the essential elements of Application Control and URL Filtering.
Lab Tasks
• Adjust the Access Control Policy

• Create and Adjust Application Control and URL
• Test and Adjust the Application Control and URL Filtering Rules

Module 10: Threat Prevention Fundamentals
• Explain the purpose of the Threat Prevention solution.
• Identify the essential elements of Autonomous Threat Prevention.
Lab Tasks
• Enable Autonomous Threat Prevention
• Test Autonomous Threat Prevention

Termíny školení

Datum	Místo konání	Časové pásmo	Jazyk	Typ	Garance termínu	CENA
16 Feb 2027	Praha	CET	Čeština	Classroom		Kč bez DPH 33,500.00
13 Sep 2027	Praha	CEDT	Čeština	Classroom		Kč bez DPH 33,500.00
23 Nov 2027	Praha	CET	Čeština	Classroom		Kč bez DPH 33,500.00
16 Feb 2027	Virtual Classroom	CET	Čeština	Instructor Led Online		Kč bez DPH 33,500.00
11 May 2027	Virtual Classroom	CEDT	Čeština	Instructor Led Online		Kč bez DPH 33,500.00
13 Sep 2027	Virtual Classroom	CEDT	Čeština	Instructor Led Online		Kč bez DPH 33,500.00
23 Nov 2027	Virtual Classroom	CET	Čeština	Instructor Led Online		Kč bez DPH 33,500.00

Dodatečné informace

Školení je možné zajistit na míru. Kontaktujte nás pro bližší informace.