

Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com Phone: +31 20 582 6109



Check Point Deployment Administrator (CPDA) R82 - Now Available

CODE: LENGTH: PRICE:

CKT CPDA R82 16 Hours (2 days) Request Price

Description

This course provides students with the fundamental knowledge, skills, and hands-on experience needed to deploy a new Quantum Security Environment. Students learn how to install and perform basic configuration of SmartConsole, the Gaia Operating System, a Security Management Server, and a Security Gateway. Additionally, students learn how to create a basic policy, deploy a Security Gateway Cluster, configure a Dedicated Log Server, perform maintenance tasks including System Backups and Snapshots and batch import Objects and Rules.

Audience

- Deployment Administrators
- Security Administrators
- Security Consultants

Prerequisites

Base Knowledge

- Unix-like and/or Windows OS
- Internet Fundamentals
- Networking Fundamentals
- · Networking Security
- System Administration
- TCP/IP Networking
- Text Editors in Unix-like OS

Check Point Courses

· No prerequisite courses

Programme

Module 1: Introduction to Quantum Security

• Identify the primary components of a Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.

Module 2: Quantum Security Architecture

• Identify key considerations when planning a new Quantum Security deployment.

Lab Tasks

- · Verify the Check Point Hosts
- Document the Network Environment
- Verify the A-GUI Client Host

Module 3: Primary Security Management Server Deployment

· Identify the basic workflow, guidelines, and best practices for a Primary Security Management Server deployment.

Lab Tasks

- Install the Gaia Operating System
- Configure the Primary Security Management Server
- Deploy SmartConsole

Module 4: Security Gateway Deployment

• Identify the basic workflow, guidelines, and best practices for a Security Gateway deployment.

Lab Tasks

- Run the First Time Wizard on the Security Gateway
- · Create a Security Gateway Object
- Test SIC and Install Licenses

Module 5: Policy Fundamentals

- Describe the essential elements of a Security Policy.
- · Identify features and capabilities that enhance the configuration and management of the Security Policy.

Lab Tasks

- Create an Access Control Policy Package
- · Add and Modify a Rule in the Access Control Policy

Module 6: Security Gateway Cluster Deployment

· Identify the basic workflow, guidelines, and best practices for a Security Gateway Custer deployment.

Lab Tasks

- Reconfigure the Security Environment
- Configure Cluster Members as Security Gateways
- Configure Cluster Member Interfaces
- · Add Members to the Clusters
- Add Licenses to the Cluster Members

Module 7: Dedicated Log Server Deployment

· Identify the basic workflow, guidelines, and best practices for a dedicated Log Server deployment.

Lab Tasks

- · Configure a dedicated Log Server
- · Add a dedicated Log Server

Module 8: Maintenance Fundamentals

- Explain the purpose of a regular maintenance strategy.
- Identify the basic workflow, guidelines, and best practices for Backup/Restore, Snapshot Management, Load/Save Configuration, Hardware Health Monitoring, and Software Updates.

Lab Tasks

- Collect and Download System Backups
- · Collect and Download Snapshots

Module 9: Batch Import of Security Environment Components

- Describe purpose of a batch import and give import use cases.
- · Identify the basic workflow, guidelines, and best practices for a batch import.

Lab Tasks

- · Import and Create Host Objects
- Import and Create Network Objects
- Import and Create Group Objects
- Import and Create Access Control Rules

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.