Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: education.ecs.baltic@arrow.com
Phone: 0870 251 1000

Check Point Certified Security Expert (CCSE) & Troubleshooting Expert (CCTE) Bundle R81.20

CODE:	LENGTH:	PRICE:
CKT_CCSECCTE_R81.20	40 Hours (5 days)	€4,430.00

Description

This bundle course covers the following two Check Point training courses:
Check Point Certified Security Expert (CCSE) R81.20 (3 days)
And
Check Point Certified Troubleshooting Expert (CCTE) R81.20 (2 days)

Audience

- Technical professionals who support, install deploy or administer Check Point products.
- Security experts and Check Point resellers who desire to obtain the necessary knowledge required to perform more advanced troubleshooting skills while managing their security environments.

Programme

Objectives CCSE:

- Identify basic interfaces used to manage the Check Point environment.
- Identify the types of technologies that Check Point supports for automation.
- Explain the purpose of the Check Management High Availability (HA) deployment.
- Identify the workflow followed to deploy a Primary and solution Secondary servers.
- Explain the basic concepts of Clustering and ClusterXL, including protocols, synchronization, connection stickyness.
- Identify how to exclude services from synchronizing or delaying synchronization.
- Explain the policy installation flow.
- Explain the purpose of dynamic objects, updatable objects, and network feeds.
- Understand how to manage user access for internal and external users.
- Describe the Identity Awareness components and configurations.
- Describe different Check Point Threat Prevention solutions.
- Articulate how the Intrusion Prevention System is configured.
- Obtain knowledge about Check Point’s IoT Protect.
- Explain the purpose of Domain-based VPNs.
- Describe situations where externally managed certificate authentication is used.
- Describe how client security can be provided by Remote Access.
- Discuss the Mobile Access Software Blade.
- Explain how to determine if the configuration is compliant with the best practices.
- Define performance tuning solutions and basic configuration workflow.
- Identify supported upgrade and migration methods and procedures for Security Management Servers and dedicated Log and SmartEvent Servers.
- Identify supported upgrade methods and procedures for Security Gateways.

Exercises CCSE:

- Navigate the Environment and Using the Management API
- Deploy Secondary Security Management Server
- Configure a Dedicated Log Server
- Deploy SmartEvent
- Configure a High Availability Security Gateway Cluster
- Work with ClusterXL
- Configure Dynamic and Updateable Objects

- Verify Accelerated Policy Installation and Monitoring Status
- Elevate Security with HTTPS Inspection
- Deploy Identity Awareness
- Customize Threat Prevention
- Configure a Site-to-Site VPN with an Interoperable Device
- Deploy Remote Access VPN
- Configure Mobile Access VPN
- Monitor Policy Compliance
- Report SmartEvent Statistics
- Tuning Security Gateway Performance

Objectives CCTE:

- Identify and use Linux-based and Check Point commands and tools for system monitoring, file editing, and file viewing.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Management Server and API Server issues.
- Investigate and troubleshoot traffic or security-related issues using logs and events monitoring tools.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Security Gateway issues.
- Demonstrate an understanding of advanced troubleshooting tools and techniques for kernel debugging.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Access Control issues.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Identity Awareness issues.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Site-to-Site VPN Troubleshooting issues.
- Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Client-toSite VPN Troubleshooting issues.

Exercises CCTE:

- Collect and read live and historical CPView data.
- Troubleshoot CPM and SmartConsole login issues.
- Restore a Management High Availability environment from a temporary Primary Down condition.
- Troubleshoot SmartLog processes.
- Collect and interpret user mode debugs.
- Collect and interpret kernel debugs.
- Debug Unified Policy Inspection in kernel to understand match process.Debug the Identity Awareness user mode processes.
- Collect and interpret Site-to-Site VPN Debugs.
- Collect and interpret Remote Access VPN Debugs.

Follow on courses

If you already attended our CCSA + CCTA courses and successfully passed the respective exams:
Attend two additional Infinity Specialization courses and pass their exams to automatically become a Check Point Certified Security Master Elite (CCSM Elite).
If you are already holding a CCSA and you successfully passed the CCSE and CCTE exam:
Attend three additional Infinity Specialization courses and pass their exams to automatically become a Check Point Certified Security Master Elite (CCSM Elite).

Test and Certification

This course bundle prepares you for exams #156-315.81.20 (CCSE) and #156-587 (CCTE) at www.VUE.com/checkpoint
Note:
Exam vouchers need to be purchased separately at additional cost.

Further Information

Please note that Check Point only offer e-kit courseware for training courses. Each delegate will be provided with an official set of e-kit courseware approximately 1 week prior to the start date of the course.

Session Dates

On request. Please Contact Us

Additional Information

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