Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Woluwedal 30, 1932 Sint-Stevens-Woluwe

Email: education.ecs.benelux@arrow.com
Phone: +32 2 332 19 57

Check Point Certified Security Administrator (CCSA) & Troubleshooting Administrator (CCTA) Bundle R82 (includes180 days lab access)

CODE:	LENGTH:	PRICE:
CKT_CCSACCTA_R82	40 Hours (5 days)	€3,000.00

Description

This 5-day comprehensive training bundle combines two essential Check Point certification courses:

- Check Point Certified Security Administrator (CCSA) R82 (3 Days)
- Check Point Certified Troubleshooting Administrator (CCTA) R82 (2 Days)

This course provides students with the critical knowledge and hands-on experience required to successfully configure, manage, and troubleshoot Check Point Quantum Security environments running on the Gaia operating system. Participants will transition seamlessly from foundational management to advanced diagnostic techniques, ensuring a robust and optimized security infrastructure.

Audience

- Security Administrators
- Security Engineers
- Security Analysts
- Security Consultants
- Security Architects

NIST/NICE Work Role Categories

- Implementation & Operation
- Protection & Defense

Prerequisites

Base Knowledge:

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

Check Point Course:

- Check Point Deployment Administrator (suggested)

Programme

Agenda CCSA:
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 Task3

- 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

Agenda CCTA:
Module 1: Introduction to Troubleshooting

- Identify the principles of troubleshooting methodology.
- Understand how to use the OSI (Open Systems Interconnection) model for cause isolation.
- Identify resources available to troubleshoot Check Point Security Gateways and Security Management Servers that run on the Gaia operating system.

Lab Tasks

- Analyze Resources and Performance
- Analyze System Information with CPStat
- Analyze Statistical Data with CPView
- Collect CPInfo Output on the Security Management Server
- Collect CPInfo Output on the Security Gateway
- Analyze the CPInfo Output

Module 2: Traffic Monitoring Fundamentals

- Describe the functions of packet captures.
- Describe how logs and monitoring are used when troubleshooting.
- Investigate and troubleshoot potential traffic flow issues.
- Monitor network activity and performance.

Lab Tasks

- Analyze Logs
- Trace Rules and Craft Policy
- Test Policy and NAT Rules
- Examine Routing and State Logging

Module 3: Packet Capture Fundamentals

- Understand the impact of packet captures and packet capture limitations.
- Understand the use and limitations of four tools that can be used when capturing packets.
- Investigate and troubleshoot potential traffic flow issues using packet captures.
- Monitor network activity and performance using packet captures.

Lab Tasks

- Capture Traffic with the FW Monitor Expression Filter
- Capture Traffic with the FW Monitor Simple Filter
- Capture Traffic with the tcpdump Utility
- Capture Traffic with Check Point PCAP

Module 4: Packet Capture Analysis Using CLI

- Identify command line output formats for tcpdump, cppcap, fw monitor -e, and fw monitor -F.
- Identify cppcap flags and their impact on output verbosity.
- Understand how CPMonitor can be used during packet capture analysis.
- Analyze packet captures in CLI.

Lab Tasks

- Create Issues

- Troubleshoot Fundamental Traffic Issues
- Troubleshoot Policy Configuration Issues
- Troubleshoot Routing Issues
- Troubleshoot NAT Issues
- Restore the environment

Module 5: Packet Capture Analysis Using Wireshark

- Understand Wireshark coloring rules and the modifications you can make.
- Identify file saving methodology for captures being analyzed in Wireshark.
- Analyze packet captures in Wireshark.

Lab Tasks

- Configure Wireshark for use with Check Point
- Save Packet Captures
- Analyze FW Monitor Packet Captures in Wireshark
- Analyze Interface Packet Captures in Wireshark

Module 6: Check Point Processes Troubleshooting Processes Troubleshooting

- Demonstrate an understanding of user space, kernel space, and Check Point User Space Firewall processes.
- Investigate and troubleshoot process issues.

Lab Tasks

- Verify Process States
- Analyze Process Connectivity

Module 7: SmartConsole Troubleshooting

- Investigate and troubleshoot issues with Check Point SmartConsole.

Lab Tasks

- Activate the Bad Actor
- Troubleshoot SmartConsole Login Issues
- Restore the Environment

Module 8: Log Collection Troubleshooting

- Troubleshoot log collection issues and interrupted communications.

Lab Tasks

- Activate the Bad Actor
- Troubleshoot Gateway Log Connectivity
- Troubleshoot the Security Management Server Log Collection
- Restore the Environment

Module 9: Identity Awareness Troubleshooting

- Identify and use the appropriate troubleshooting commands/tools to resolve advanced Identity Awareness issues.

Lab Tasks

- Activate the Bad Actor
- Troubleshoot Identity Awareness
- Restore the Environment

Module 10: Application Control and URL Filtering Troubleshooting

- Investigate and troubleshoot Application Control and URL Filtering issues.

Lab Tasks

- Activate the Bad Actor
- Troubleshoot URL Filtering

- Restore the Environment

Test and Certification

Certify your Skills Visit Pearson Vue at vue.com/checkpoint.

- Certification Exam#: 156-215.82 (CCSA)
- Certification Exam#: 156-583 (CCTA)

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.