Training: Check Point
Check Point Certified Troubleshooting Administrator (CCTA)

TRAINING GOALS:

This course provides students with the fundamental skills to effectively troubleshoot Quantum Security Management Servers and Security Gateways that run on the Gaia operating system. After an introduction to troubleshooting, the fundamentals of traffic monitoring and packet captures are covered followed by packet capture analysis using both CII and Wireshark. The focus then shifts to processes, SmartConsole, log collection, Identity Awareness, and Application Control and URL Filtering troubleshooting.

Target Audience

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

NIST/NICE Work Role Categories

- Implementation & Operation
- Protection & Defense

CONSPECT:

- 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

        - 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

REQUIREMENTS:

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

- Check Point Deployment Administrator (suggested)
- Check Point Certified Security Administrator (recommended)

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Check Point Software Technologies Ltd. (course completion).

This course additionally helps prepare for CCTA R82 exam #156-583 available at Pearson VUE test centers www.vue.com/checkpoint . Note: A valid or expired CCSA/CCSE certification is required to take the CCTA exam.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

TRAINER:

Authorized Check Point Software Technologies Ltd. Trainer

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007