Check Point Cybersecurity Bootcamp

Category: Networking & Security | **Vendor:** Check Point

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Certification: Certified Security Administrator R81, Certified Security Expert R81

Course Overview

The Check Point R81.20 Cybersecurity Boot Camp (CCSB) is a volume comprised of the Check Point Certified Security Administrator R81.20 (CCSA) course and a modified Check Point Certified Security Expert R81.20 (CCSE) course.

About This Course

The Check Point R81.20 Cybersecurity Boot Camp (CCSB) is a volume comprised of the Check Point Certified Security Administrator R81.20 (CCSA) course and a modified Check Point Certified Security Expert R81.20 (CCSE) course.

Prerequisites & Entry Requirements

General Prerequisites:

Working knowledge of Unix-like and Windows operating systems and TCP/IP Networking

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Describe the primary components of a Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.
- Explain how communication is secured and how traffic is routed in the Check Point environment.
- Describe the basic functions of the Gaia operating system.
- Identify the basic workflow to install Security Management Server and Security Gateway for a single-domain solution.
- Create SmartConsole objects that correspond to the organization's topology for use in policies and rules.
- Identify the tools available to manage Check Point licenses and contracts, including their purpose and use.
- Identify features and capabilities that enhance the configuration and management of the Security Policy.
- Explain how policy layers affect traffic inspection.
- Articulate how Network Address Translation affects traffic.
- Describe how to configure manual and automatic Network Address Translation (NAT).
- Demonstrate an understanding of Application Control & URL Filtering and Autonomous Threat Prevention capabilities and how to configure these solutions to meet an organization's security requirements.
- Articulate how pre-shared keys and certificates can be configured to authenticate with third party and externally managed VPN Gateways.
- Describe how to analyze and interpret VPN tunnel traffic.
- Configure logging parameters.
- Use predefined and custom queries to filter log results.
- Identify how to monitor the health of supported Check Point hardware using the Gaia Portal and the command line.
- Describe the different methods for backing up Check Point system information and discuss best practices and recommendations for each method

Detailed Course Outline

- Security
- Management
- SmartConsole
- Deployment
- Object Management
- Licenses and Contracts
- Policy Rule and Rulebase
- Policy Packages
- Policy Layers
- Traffic Inspection
- Network Address Translation
- Application Control
- URL Filtering
- Logging
- Snapshots
- Backup and Restore
- Gaia
- Permissions
- Policy Installation
- Advanced Deployments
- Management High Availability
- Advanced Gateway Deployment
- Advanced Policy Configuration
- Advanced User Access Management
- Custom Threat Protection
- Advanced Site-to-Site VPN
- Remote Access VPN
- Mobile Access VPN
- Advanced Security Monitoring
- Performance Tuning
- Advanced Security Maintenance

The following chapters and labs have been tagged as Optional in the CCSE Boot Camp:

- Chapter 6: Custom Threat Prevention
- Chapter 7: Advanced Site-to-Site VPN
- Chapter 10: Advanced Security Monitoring
- Chapter 11: Performance Tuning
- Chapter 12: Advanced Security Maintenance

Skills You Will Learn:

- Describe the primary components of a Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.
- Explain how communication is secured and how traffic is routed in the Check Point environment.
- Describe the basic functions of the Gaia operating system.
- Identify the basic workflow to install Security Management Server and Security Gateway for a single-domain solution.
- Create SmartConsole objects that correspond to the organization's topology for use in policies and rules.
- Identify the tools available to manage Check Point licenses and contracts, including their purpose and use.
- Identify features and capabilities that enhance the configuration and management of the Security Policy.
- Explain how policy layers affect traffic inspection.
- Articulate how Network Address Translation affects traffic.
- Describe how to configure manual and automatic Network Address Translation (NAT).
- Demonstrate an understanding of Application Control & URL Filtering and Autonomous Threat Prevention capabilities and how to configure these solutions to meet an organization's security requirements.
- Articulate how pre-shared keys and certificates can be configured to authenticate with third party and externally managed VPN Gateways.
- Describe how to analyze and interpret VPN tunnel traffic.
- Configure logging parameters.
- Use predefined and custom queries to filter log results.
- Identify how to monitor the health of supported Check Point hardware using the Gaia Portal and the command line.
- Describe the different methods for backing up Check Point system information and discuss best practices and recommendations for each method

Frequently Asked Questions

Q: What delivery options are available for Check Point Cybersecurity Bootcamp?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Check Point Cybersecurity Bootcamp course helps prepare you for the Certified Security Administrator R81, Certified Security Expert R81 certification path.

Q: How many CPD hours does this course provide?

The 5-day Check Point Cybersecurity Bootcamp course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Check Point Cybersecurity Bootcamp training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Check Point Cybersecurity Bootcamp?

Yes, we provide corporate training, dedicated training, and closed classes for Check Point Cybersecurity Bootcamp. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Check Point Cybersecurity Bootcamp, Check Point Training, CCSB

Q: Why choose Nexus Human for Check Point Cybersecurity Bootcamp?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Check Point Cybersecurity Bootcamp training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)