

Training: Check Point
Check Point Certified Security Expert (CCSE) R80.20

FORM OF TRAINING	MATERIALS	PRICE	DURATION
Traditional	Digital materials	1200 EUR	3 days
Traditional	CTAB Tablet	1300 EUR	3 days

LOCATIONS

Krakow - 5 Tatarska Street, II floor, hours: 9:00 am - 4:00 pm

Warsaw - 17 Bielska Street, hours: 9:00 am - 4:00 pm

TRAINING TERMS

2019-08-28 | 3 days | Kraków *(Guaranteed Dates)*

2019-10-02 | 3 days | Warszawa

2019-12-09 | 3 days | Warszawa

TRAINING GOALS:

Validate your understanding and skills necessary to configure and optimally manage **Check Point Next Generation Firewalls**

Expert users and resellers who need to perform advanced deployment configurations of Check Point Software Blades are the target group for this training.

CONSPECT:

- Advanced Gaia
- Advanced Firewall
- Automation & Orchestration
- Advanced ClusterXL
- VRRP Clusters
- SecureXL: Security Acceleration
- CoreXL: Multicore Acceleration
- Multiple Traffic Queues
- The SmartEvent Solution
- Identifying an Event
- Monitoring the Network

- Investigating Security Events
- Remediating Security Events
- Reporting Security Events
- Preventative Measures
- SmartEvent Example
- High Availability Environment
- Mobile Access Software Blade
- Mobile Access Deployment
- Choosing Remote Access Solutions
- Remote Access Options
- Check Point Capsule
- Mobile Access Policy
- The Threat Landscape
- Intrusion Prevention System (IPS)
- Antivirus
- Anti-Bot
- Sandboxing
- SandBlast Zero-Day Protection
- SandBlast Deployment
- SandBlast Deployment Options
- Mobile Threat Prevention

Exercises

- Lab 1.1 Upgrading a SMS to R80.10
- Lab 1.2 Applying Check Point Hotfixes
- Lab 1.3: Configuring a New Security Gateway Cluster
- Lab 1.4: Core CLI Elements of Firewall Administration
- Lab 1.5: Configuring Manual NAT
- Lab 2.1 Managing Objects using the Check Point API
- Lab 3.1 Enabling Check Point VRRP
- Lab 3.2 Deploying a Secondary Security Management Server
- Lab 4.1 Viewing the Chain Modules
- Lab 4.2 Working with Secure XL
- Lab 4.3 Working with CoreXL
- Lab 5.1 Evaluating Threats with SmartEvent
- Lab 6.1 Managing Mobile Access

- Lab 7.1 Understanding IPS Protections
- Lab 7.2: Deploying IPS Geo Protections
- Lab 7.3: Reviewing Threat Prevention Settings and Protections
- Lab 7.4: Deploying Threat Emulation and Threat Extraction

REQUIREMENTS:

- **CCSA training/certification.**
- Working knowledge of Windows, UNIX, networking, TCP/IP, and the Internet.

Difficulty level



CERTIFICATE:

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

This course helps to prepare for **CCSE exam** #156-315.80 available at [Pearson VUE test centers](#). It contains 100 multiple-choice, scenario-based questions. A passing score is 70% or higher. Students should have at least 1 year experience with Check Point products before challenging the exam. Depending on your certification history passing **CCSA exam** might be also required.

TRAINER:

Authorized Check Point Software Technologies Ltd. Trainer.