



CYBER SECURITY

Check Point Security

Administration

PROGRAM

(CCNA)



Let's be a **Check Point Expert.**

We are system administrator or network expert. Let's gain **CCSA - Certified Check Point Security Administration.**

To gain the CCSA certification is the first step forward to the profession of CSP: Cyber Security Practitioner. So, let's go ahead.



CCSA - Certified Check Point Security Administration PROGRAM

Target audience and Prerequisites:

Systems Administrators, Support Analysts, Security Engineers, Network Engineers, Any other IT professional with General knowledge of TCP/IP, and working knowledge of Windows, UNIX, network technology, and the Internet.

Orientation:

Technical, Hands On

Class & Missions Hours:

40 class and LAB hours

Format:

5 days meetings

Certifications Options:

Check Point CCSA

Course Objectives

If you need to support, install, deploy or administer Check Point Software Blades, you will learn the skills necessary to work with Check Point Security Administration featuring R77 GAiA:

1. Introduction to check point technology
2. Deployment platforms
3. Introduction to the security policy
4. Monitoring traffic and connections
5. Using SmartUpdate
6. User management and authentication
7. Identity awareness
8. Introduction to Check Point VPNs

Introduction

Check Point Security Administration (R77 GAiA) provides you with an understanding of the basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades. During this course, you will configure a Security Policy and learn about managing and monitoring a secure network, upgrading and configuring a Security Gateway, and implementing a virtual private network. This course prepares learners for CCSA exam #156-215.77.

The Successful graduate will have Firewall Administration capabilities and Information Security essentials understanding - the first step in a Cyber Security Practitioner career.

After taking Course: next step

After the course, the participant can chose his next step:

1. Starting works as a junior System Administrator or as a Network Administrator.
2. Complete more recommend preliminary courses such as: "**LPI Linux Essentials**" course and / or "**Python Code**" course.
3. Starting "next step" Cyber Profession course, chose one of the above options:
 - A. **CSP: Cyber Security Practitioner** Course.
 - B. **SOC-IR: (Security Operation Center) Operator** Course.
 - C. **CSTP: Cyber Security Technology (Architect) Professional: Course.**
 - D. **CSPT: Cyber Security Penetration Tester (Hacking Defined Experts A, B, C).** Before this course, the candidate should complete his knowledge in Linux Essentials and Python code.



CCSA - Certified Check Point Security Administration PROGRAM

Curriculum:

CCSA - Check Point Security Administration	50	Module 3: Security Gateway Inspection Architecture
<p>Check Point Security Administration (R77 GAiA) provides you with an understanding of the basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades. During this course, you will configure a Security Policy and learn about managing and monitoring a secure network, upgrading and configuring a Security Gateway, and implementing a virtual private network. This course prepares learners for CCSA exam #156-215.77.</p>		Module 3: INSPECT Engine Packet Flow
Module 1: Check Point Security Management		Module 4: Deployment Considerations
<ul style="list-style-type: none"> • Check Point Security Management • Architecture (SMART) • SmartConsole • Security Management Server • Security Gateway 		<ul style="list-style-type: none"> • Standalone Deployment • Distributed Deployment • Standalone Full HA • Bridge Mode
Module 2: The Check Point Firewall		Module 5: Check Point SmartConsole Clients
<ul style="list-style-type: none"> • OSI Model • Mechanism for controlling Network traffic. • Packet Filtering • Stateful Inspection • Application Intelligence 		<ul style="list-style-type: none"> • SmartDashboard • Smartview Tracker • SmartLog • SmartEvent • SmartView Monitor • SmartReporter • SmartUpdate • SmartProvisioning • SmartEndpoint
		Module 6: Security Management Server
		<ul style="list-style-type: none"> • Managing Users in SmartDashboard • Users Database
		Module 7: Securing Channels of Communication
		<ul style="list-style-type: none"> • Secure Internal Communication • Testing the SIC Status • Resetting the Trust State

We invented a methodology for cyber education, because nobody else did it.



What can I do after taking this course? The next step.

After the course, you can chose your next step among the described options:

1. Starting works as a Check Point Administrator.

2. Complete more recommend preliminary courses such as: "LPI Linux Essentials" course and / or "Python Code" course.



3. Starting "next step" Cyber Profession course: CSP: Cyber Security Practitioner Course.

The Cyber Security Practitioner is responsible for implementing the organization's cyber protection, and has the specific perspective of the following aspects:

1. The installation, operation and maintenance of cyber protection products.
2. The implementation of routine security procedures.
3. First level identification and treatment in cyber events based on types of threats and attacks.
4. May includes International Certification such as CompTIA Security+, or (ISC)² SSCP.

This is in recognition of understanding of the activities, needs and corporate objectives.



4. Starting "next step" Cyber Profession course: SOC-IR: (Security Operation Center) Operator Course.

A SOC-IR specialist is responsible for critical core subjects in operating cyber monitoring centers and primary response teams. The SOC Operator

performs the prelaminar necessary actions when a cyber event is identified.



5. Starting "next step" Cyber Profession course: CSTP: Cyber Security Technology (Architect) Professional: Course.

A person with an academic background, wide-ranging and profound theoretical knowledge, who is in charge of:

1. Designing technological solutions for cyber protection in the organization combining technologies and security methods.
2. Adjusting cyber protection products and integrating them in the IT infrastructure, including storage and backup.
3. Accompanying the process of handling security events with a technology standpoint, acknowledging the organization activities, needs and objectives.
4. May includes International Certification such as CompTIA Security+, or (ISC)² SSCP.
5. This is in recognition of understanding of the activities, needs and corporate objectives.



6. Starting "next step" Cyber Profession course: CSPT: Cyber Security Penetration Tester

Before this course, the candidate should complete his knowledge in Linux Essentials and Python code.

An Expert with wide and up dated knowledge as well as practical abilities in vulnerabilities detection and penetration testing in cyber systems.

