

## Training: Check Point SandBlast Network



FORM OF TRAINING	MATERIALS	PRICE	DURATION
Traditional	Digital materials	860 EUR	1 day
Traditional	CTAB Tablet	960 EUR	1 day

### 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

2019-11-25 | 1 day | Warszawa

### TRAINING GOALS:

This course provides an understanding of basic concepts and skills necessary to configure and implement **Check Point SandBlast technology**.

#### WHO SHOULD ATTEND?

Technical professionals who support, install, deploy or administer Check Point Software Blades.

#### COURSE OBJECTIVES AND TOPICS INCLUDE:

- Threat Anatomy
  - Discuss the current threat landscape and security challenges.
  - Understand the components of an attack.
  - Learn how threat actors avoid traditional security methods.
  - Understand CPU and OS-level sandbox technologies.
- SandBlast Threat Emulation
  - Identify the different SandBlast Zero-Day components..
  - Discuss various file emulation processes and mechanisms.
  - Understand the three file emulation deployment options.
- SandBlast Threat Extraction
  - Understand how SandBlast Zero-Day Protection protects organizations from threats via Threat Extraction.
  - Learn essential Threat Extraction settings and configurations.

- ThreatCloud Emulation Service
  - Learn how file emulation works when using ThreatCloud.
  - Discuss the different ThreatCloud components.
- Deployment Scenarios
  - Learn about various SandBlast Zero-Day Protection deployment implementations.
  - Understand how System Administrators can utilize local emulation and/or ThreatCloud in different situations.
- SandBlast Troubleshooting
  - Identify essential command line tools for monitoring Threat Emulation and Threat Extraction.
  - Learn how to troubleshoot Threat

## CONSPECT:

- Threat Anatomy
- SandBlast Threat Emulation
- SandBlast Threat Extraction
- ThreatCloud Emulation Service
- Deployment Scenarios
- SandBlast Troubleshooting

## Lab exercises:

- Understanding Vulnerabilities
  - Learn about software vulnerabilities.
  - Understand the CVSS scores for vulnerabilities.
  - See how malware can bypass sandboxing.
- Working with Threat Emulation
  - Activate local emulation and make the system ready to emulate files.
  - Use the command line to emulate files from the local file system.
  - View Threat Emulation logs using SmartView Tracker.
  - View and create reports using SmartEvent.
  - Confirm the Security Gateway acts as an MTA.
- Working with Threat Extraction
  - Activate Threat Extraction on an MTA-enabled Security Gateway.
  - Confirm how Threat Extraction delivers safe content.
- Working with ThreatCloud
  - Identify how to configure Security Gateway to offload file emulation to ThreatCloud.

- Review the related forensic report.

## REQUIREMENTS:

Persons attending this course should have a:

- [CCSA](#)
- Basic knowledge of networking
- 6 months to 1 year of experience with Check Point products recommended

## Difficulty level



## CERTIFICATE:

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

## TRAINER:

Authorized Check Point Software Technologies Ltd. Trainer.