Check Point
SOFTWARE TECHNOLOGIES LTD

SANDBLAST TRAINING

Check Point SandBlast

SANDBLAST ZERO-DAY PROTECTION – WORKSHOP (One Day Course)

GETTING A STEP AHEAD OF THE UNKNOWN

Zero-day and advanced persistent threats use the element of surprise to bypass traditional security, making these threats difficult to protect against—and very popular with hackers. Traditional sandboxing was designed to help with these types of threats, but cybercriminals have evolved their techniques, creating evasive malware that can avoid detection by many sandbox solutions. As a result, many organizations find themselves taking reactive steps to counteract infection, rather than preventing it in the first place.

To get ahead, enterprises need a multi-faceted prevention strategy that combines proactive protection that eliminates threats before they reach users, and state-of-the-art CPU-level exploit detection to expose even the most highly camouflaged threats.

COURSE GOAL:

Provide an understanding of basic concepts and skills necessary to configure and implement Check Point SandBlast technology

COURSE TOPICS

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

COURSE OBJECTIVES

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.

Chapter 5: 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 Emulation and Threat Extractioni performance.

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.