Check Point IPS/AV/ABOT Immersion R81.20 Update

Table of Contents

Welcome & Introduction

- Your Instructor: **Timothy Hall, CISSP**
  - Worked with Check Point products since 1997, Check Point instructor since 2004
  - Founder of Shadow Peak Inc, a Check Point Authorized Training Center (ATC) (http://www.shadowpeak.com)
  - Link to all CheckMates Posts and Link to all CPUG Posts
  - Creator and exclusive instructor for the R81.20 Gateway Performance Optimization class
  - Also creator of the self-guided video training series "Gaia 3.10 Immersion" and "Max Capture: Know Your Packets"
  - Author of Book “Max Power 2020: Check Point Firewall Performance Optimization”

Check Point IPS/AV/ABOT Immersion Class Details

- Prerequisites: Basic systems and networking knowledge.
- We will be working with the R81.20, Jumbo HFA 8 Check Point code.
- The main focus of this course is the R81.20 code running on Check Point appliances (models 2200-28XXX), open hardware, and some types of virtualized environments.
- The material presented in this course will also apply to CloudGuard gateways subject to the specific limitations detailed in sk170418: Check Point **R81.10 Known Limitations** and to a lesser degree Section 7 of this SK: sk141173: Check Point R80.20 with Gaia 3.10 for CloudGuard and Open Server Security Gateways.
- Hyperlinks shown in this document are “hot” and can be clicked to show the specified resource in your web browser.
- *Please note that this material can be taught by Mr. Hall as a live, 3-day class complete with real lab exercises for a minimum of 5 attendees. Contact sales@shadowpeak.com for more information.*

List of Class Modules

- Module 0 – Crash Course: The Basics of Check Point Objects, Policies & Logging (optional)
- Module 1 – History of IDS/SmartDefense/IPS/AV/ABOT
- Module 2 – Working with IPS Protections
- Module 3 – Working with AV/ABOT Protections
- Module 4 – Threat Prevention Profiles & Policy Layers
- Module 5 – Updatable Geo Objects & Geo Protection/Policy
- Module 6 – HTTPS Inspection
- Module 7 – Log Analysis, Packet Captures & Creating Exceptions/Exclusions
- Module 8 – Threat Prevention Correlated Views & Reports
- Module 9 – IPS/AV/ABOT Updates
- Module 10 –Threat Prevention Monitoring & Alerts
- Module 11 – Advanced IPS/AV/ABOT Features & Troubleshooting Techniques
- Module 12 – Threat Prevention Performance Optimization
- Module 13 – Autonomous Threat Prevention