

KillTest

Higher Quality, Better Service!



Q&A

<http://www.killtest.com>

We offer free update service for one year.

Exam : 156-590

Title : Check Point Certified Threat
Prevention Specialist
(CTPS)

Version : DEMO

1.Which process is responsible for Archive Scanning?

- A. zipscn
- B. psl_dlp
- C. gzscn_proc
- D. dlpu

Answer: A

2.That Tracking option can be used to capture additional data for analysis by Check Point TAC?

- A. Alert
- B. Forensics
- C. SNMP
- D. User Defined

Answer: B

3.What is the purpose of the Profile Cleanup option?

- A. It lets you start over by removing all administrator overrides.
- B. It merges protection settings from multiple profiles into the Optimized Profile.
- C. It serves as a cleanup policy if none of the protection matches the packets.
- D. It eliminates protections automatically which hasn't been used for a predefined amount of time.

Answer: A

4.Which is NOT true of Threat Prevention policy application?

- A. Only applied after traffic is accepted by Access Control Policy
- B. Traffic is matched against all applicable layers at the same time
- C. Only applies first matched rule
- D. Applied as ordered layer

Answer: B

5.What is the recommended setting for Anti-Virus and why?

- A. Background because it is Post-infection
- B. Hold because it is Pre-infection and inspects a limited subset of traffic
- C. Hold because it inspects a limited subset of traffic
- D. Background because it inspects a large subset of traffic

Answer: B