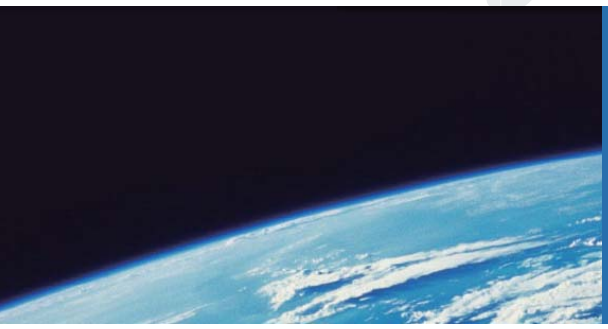
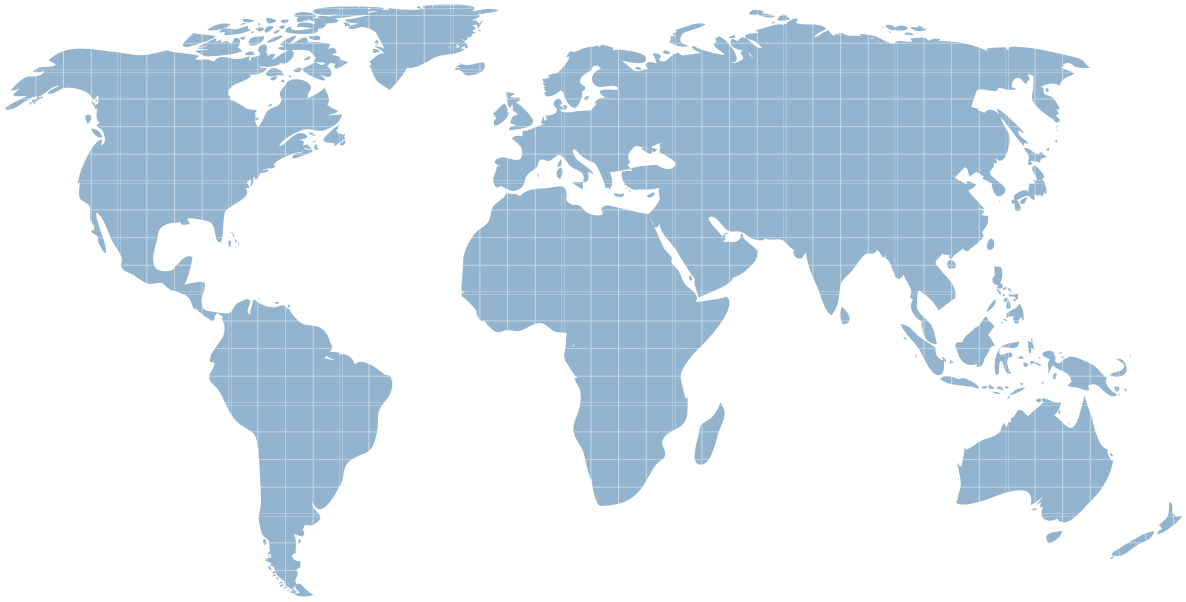


ITTEST

QUESTION & ANSWER

Guías de estudio precisos, Alta tasa de paso!



Ittest ofrece información actualizada de forma gratuita en un año!

http://www.ittest.es/

Exam : **PSE Endpoint Associate**

Title : PSE: Endpoint Associate training for Traps 4.0

Version : DEMO

1.What does ROP stand for?
A. Return-Oriented Programming
B. Rules of Prevention
C. Restriction on Process
D. Retained Original Process
Answer: A

2.The Traps product and documentation use the terms "malware" and "exploit" in a very specific way. Which two statements are true? (Choose two.)
A. Exploits attempt to take advantage of a vulnerability in code.
B. The primary vector for exploits is .exe files.
C. Malware consists of application data files containing malicious code.
D. Malware consists of malicious executable files that do not rely on exploit techniques.
Answer: A,C

3.Which three file types will be uploaded automatically to WildFire for examination? (Choose three.)
A. Application data files that trigger preventions
B. Executables with no previous verdict in the ESM deployment
C. Executables with a verdict overridden by the administrator
D. Executables allowed to run because their publisher is trusted
E. Executables allowed to run by local analysis
F. Application data files opened by the end user
Answer: A,E,F

4.Which two statements about troubleshooting installation and upgrade problems are true? (Choose two.)
A. A common cause of ESM Server installation problems is the failure to confirm connectivity to WildFire before running the installer.
B. A common cause of Traps endpoint agent installation problems is the failure to configure the SSL option correctly.
C. ESM Server services will shut down if they are not licensed within 24 hours of being started.
D. Use MSIEXEC with appropriate flags to get more logging detail at installation time.
Answer: A,B

5.Which statement about Malware verdicts is true?
A. If WildFire is not available when the active ESM server tries to reach it for a verdict on a file, the endpoint will get a verdict from local analysis.
B. If the ESM server is not available when the Traps agent tries to reach it for a verdict on a file, the file status is marked as Benign.
C. The end user can use the Traps console to override a verdict of Malicious.
D. Local analysis verdicts take precedence over WildFire verdicts.
Answer: A