

Free PDF Trend - Useful Deep-Security-Professional - Study Trend Micro Certified Professional for Deep Security Materials



P.S. Free 2026 Trend Deep-Security-Professional dumps are available on Google Drive shared by PassTestking:
<https://drive.google.com/open?id=17ACnyNI58IzQhijk6MutHAc6kGUn-O35>

For candidates who are going to buying the Deep-Security-Professional exam dumps online, you may concern more about the personal information. If you choose us, your personal information will be protected well. Once you buy Deep-Security-Professional exam materials of us, we will send the downloading link to you automatically, and you can start your training immediately. Once the order finish, your personal information such as your name and your email address will be concealed. In addition, Deep-Security-Professional Exam Dumps provide you with free update for 365 days, namely you can get the latest information about the exam.

Trend Deep-Security-Professional Certification Exam is one of the most sought-after certifications in the field of IT security. Trend Micro Certified Professional for Deep Security certification is designed for professionals who are looking to validate their knowledge and expertise in Trend Micro's Deep Security platform. Trend Micro Certified Professional for Deep Security certification exam is administered by Trend Micro and is open to anyone who has completed the required training.

Trend Deep-Security-Professional certification is highly valued in the IT industry, particularly among employers who use Trend Micro's Deep Security product. Trend Micro Certified Professional for Deep Security certification provides a competitive edge to professionals seeking employment in the cybersecurity field, as well as those who want to advance their careers. Additionally, the certification is a testament to an individual's commitment to ongoing professional development and staying up-to-date on the latest trends and technologies in the cybersecurity field.

New Deep-Security-Professional Test Duration, Deep-Security-Professional Reliable Dumps Files

If your job is very busy and there is not much time to specialize, and you are very eager to get a Deep-Security-Professional certificate to prove yourself, it is very important to choose a very high Deep-Security-Professional learning materials like ours that passes the rate. I know that the 99% pass rate of our Deep-Security-Professional Exam simulating must have attracted you. Do not hesitate anymore. You will never regret buying our Deep-Security-Professional study engine!

Trend Micro Certified Professional for Deep Security is a certification exam that is designed for IT professionals who want to become experts in implementing and managing Trend Micro's Deep Security solution. Deep-Security-Professional Exam is intended for those who already have experience with network and security administration and want to further their knowledge in this area.

Trend Micro Certified Professional for Deep Security Sample Questions (Q62-Q67):

NEW QUESTION # 62

How can you prevent a file from being scanned for malware?

- A. Enable "File Types scanned by IntelliScan" in the Malware Scan Configuration properties in the Deep Security Manager Web console. Click "Scan All Except" and type the filename to exclude from the scan.
- B. Add the file to the Exclusions list in the "Allowed Spyware/Grayware Configuration".
- **C. Add the file to the Exclusions list in the Malware Scan Configuration.**
- D. Edit the "Scan Exclusions" section of the dsa.properties configuration file on the Deep Security Agent computer to include the file name. Save the configuration file and restart the Deep Security Agent service.

Answer: C

Explanation:

To exclude files from malware scans, add them to the Exclusions list in the Malware Scan Configuration via the Deep Security Manager Web console. This is the official and recommended method.

From the official documentation:

"Files or folders added to the Exclusions list in the Malware Scan Configuration will not be scanned for malware." References:

Trend Micro Deep Security Anti-Malware Guide: Scan Exclusions

Deep Security Help: Excluding Files from Scans

NEW QUESTION # 63

Which of the following statements is true regarding Event Tagging?

- A. Only a single tag can be assigned to an Event.
- B. Adding a tag to an Event modifies the Event data by adding fields, including the name of the tag, the date the tag was applied, and whether the tag was applied manually or automatically
- C. Events can be automatically deleted based on tags.
- **D. Events can be tagged automatically if they are similar to known good Events.**

Answer: D

NEW QUESTION # 64

Which of the following statements is false regarding Firewall rules using the Bypass action?

- A. Firewall rules using the Bypass action allow incoming traffic to skip both Firewall and Intrusion Prevention analysis.
- **B. Applying a Firewall rule using the Bypass action to traffic in one direction automatically applies the same action to traffic in the other direction.**
- C. Firewall rules using the Bypass action do not generate log events.
- D. Firewall rules using the Bypass action can be optimized, allowing traffic to flow as efficiently as if a Deep Security Agent was not there.

Answer: B

Explanation:

Firewall rules using Bypass have the following noteworthy characteristics:

- * Bypass skips both Firewall and Intrusion Prevention analysis.
- * Since stateful inspection is for bypassed traffic, bypassing traffic in one direction does not automatically bypass the response in the other direction. As a result firewall rules using Bypass are always created in pairs, one for incoming traffic and another for outgoing.
- * Firewall rules using Bypass will not be logged. This is not a configurable behavior.
- * Some firewall rules using Bypass are optimized, in that traffic will flow as efficiently as if the Deep Security Agent/Deep Security Virtual Appliance was not there.

Explication: Study Guide - page (236)

NEW QUESTION # 65

Based on the configuration setting highlighted in the exhibit, what behavior can be expected during a malware scan?

□

- A. With the highlighted setting enabled, Deep Security Agents will scan files for known viruses and malware using patterns and any files deemed suspicious will be submitted to a configured Deep Discovery Analyzer for further analysis.
- **B. With the highlighted setting enabled, Deep Security Agents will scan files for viruses and malware using supplementary aggressive detection pattern files.**
- C. With the highlighted setting enabled, Deep Security Agents will scan files for unknown malware using Predictive Machine Learning.
- D. With the highlighted setting enabled, Deep Security Agents will scan files for known malware as well as newly encountered malware by accessing the Suspicious Objects List.

Answer: B

Explanation:

The highlighted option specifies, "Scan for exploits against known critical vulnerabilities and aggressive detection of unknown suspicious exploits." This means the agent uses additional, more aggressive detection patterns to identify not just known exploits but also suspicious and unknown exploit techniques in document files. Predictive Machine Learning and Suspicious Objects List are separate features, and Deep Discovery Analyzer integration is not referenced by this setting.

Reference:

Trend Micro Deep Security Administrator's Guide, Document Exploit Protection Section

NEW QUESTION # 66

What is the role of Apex Central in the Connected Threat Defense infrastructure?

- A. Apex Central stores suspicious files that are awaiting submission to the Deep Discovery Analyzer.
- B. Apex Central submits suspicious files to Deep Discovery Analyzer for further analysis.
- C. Apex Central distributes Deep Security policies to Agents on the protected Servers.
- **D. Apex Central compiles the Suspicious Objects List based on the result of file analysis in Deep Discovery Analyzer.**

Answer: D

Explanation:

□

- 1 Deep Security Agents are configured with rules to enable detection of malware on the protected computers.
- 2 Objects deemed to be suspicious are gathered and submitted to Deep Security Manager.
- 3 Deep Security Manager submits the suspicious objects to Deep Discovery Analyzer for analysis.
- 4 Deep Discovery Analyzer executes and observes the suspicious object in a secure, isolated virtual sandbox environment.
- 5 Deep Discovery Analyzer pushes the analysis results to Trend Micro Apex Central, where an action can be specified for the file based on the analysis. Once the action is specified, a list of emerging threats called a Suspicious Object List is created or updated. Other Trend Micro products, such as Apex One, Deep Discovery Inspector or Deep Discovery Email Inspector, may also be connected to Trend Micro Apex Central and be able to update the list.
- 6 Deep Security Manager receives the list of suspicious objects from Apex Central.
- 7 The list is forwarded to Deep Security Agents where protection against the suspicious object is applied. Anti-Malware policies define how suspicious objects are to be handled.

Explication: Study Guide - page (387)

• • • • •

- 2026 Latest PassTesting Deep-Security-Professional PDF Dumps and Deep-Security-Professional Exam Engine Free Share:
<https://drive.google.com/open?id=17ACmYNI58IzQhijk6MutHAc6kGUu-O35>