DUMPSARENA

Trend Micro Certified Professional for Deep Security Exam

Trend Micro Deep-Security-Professional

Version Demo

Total Demo Questions: 9

Total Premium Questions: 80

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following are valid methods for pre-approving software updates to prevent Ap-plication Control Events from being triggered by the execution of the modified software? Select all that apply.

A. Once the inventory scan has run when Application Control is first enabled, there is no way to update the inventory to incorporate modified software.

B. Software updates performed by a Trusted Updater will be automatically approved.

C. Edit the inventory database file (AC.db) on the Agent computer to include the hash of the newly updated software. Save the change and restart the Deep Security Agent. The software updates will now be approved.

D. Maintenance mode can be enabled while completing the updates.

ANSWER: B D

Explanation:

Explanation

Normally, you will want Application Control to alert you when there are any unexpected software updates. However, some updates are expected and you will need provide allowances for these up-dates. Two methods for pre-approving software updates includes maintenance mode and trusted installers.

Explication: Study Guide - page (303-304)

QUESTION NO: 2

How is caching used by the Web Reputation Protection Module?

A. Caching is used by the Web Reputation Protection Module to temporarily store the credibility score for a Web site. The retrieved credibility score is cached in case the score for the Web site is required again for the life of the cache.

B. Caching is used by the Web Reputation Protection Module to temporarily store the pages that make up the Web site. The Web site is cached in case the site is visited again for the life of the cache.

C. Caching is used by the Web Reputation Protection Module to keep track of Web sites that are added to the Allowed list. Any sites added to the Allowed list will be accessible by protected servers regardless of their credibility score.

D. Caching is used by the Web Reputation Protection Module to keep track of Allowed and Blocked Web sites. Any sites that are Allowed or Blocked do not require the retrieval of a credibility score from the Trend Micro Web Reputation Service.

ANSWER: A

QUESTION NO: 3

Which Deep Security Protection Modules can be used to provide runtime protection for the Kubernetes and Docker platforms? Select all that apply.

A. Intrusion Prevention

B. Log Inspection

C. Integrity Monitoring

D. Anti-Malware

ANSWER: A B C

Explanation:

Explanation

Container users can benefit from Kubernetes and Docker platform protection at runtime with Intrusion Prevention, Integrity Monitoring and Log Inspection rules using the Deep Security Agent installed on the host. The Deep Security Intrusion Prevention approach allows you to inspect both east-west and north-south traffic between containers and platform layers like Kubernetes.

Explication: Study Guide - page (353)

QUESTION NO: 4

Which of the following statements correctly describes Smart Folders?

A. Smart Folders identify the folders that will be scanned when a Real-Time, Manual or Scheduled malware scan is run.

B. Smart Folders are a collection of subfolders containing the policy settings that are ap-plied to child policies or directly to Computers.

C. Smart Folders act as a saved search of computers which is executed each time the folder is clicked to display its contents.

D. Smart Folders are the containers used to store the results of Recommendation Scans. Once a Recommendation Scan has completed, and administrator can click a Smart Folder and select which of the recommended rules to apply.

ANSWER: C

Explanation:

Explanation

Smart Folders are used to group your computers dynamically. The computers displayed in a Smart Folder are determined by a set of custom rules, that act as a saved search which is executed each time you click on the folder to display its contents. This allows administrators to easily filter and group computers by these defined properties.

Explication: Study Guide - page (127)

QUESTION NO: 5

Which of the following are valid methods for forwarding Event information from Deep Secu-rity? Select all that apply.

A. Simple Network Management Protocol (SNMP)

B. Deep Security Application Programming Interface (API)

C. Amazon Simple Notification Service (SNS)

D. Security Information and Event Management (SIEM)

ANSWER: A C D

Explanation:

Explanation

You can configure Deep Security Manager to instruct all managed computers to send logs to a SI-EM, Amazon Simple Notification Service or SNMP computers.

Explication: Study Guide - page (322)

QUESTION NO: 6

Which of the following statements is true regarding the use of the Firewall Protection Module in Deep Security?

A. The Firewall Protection Module can check files for certain characteristics such as compression and known exploit code.

B. The Firewall Protection Module can identify suspicious byte sequences in packets.

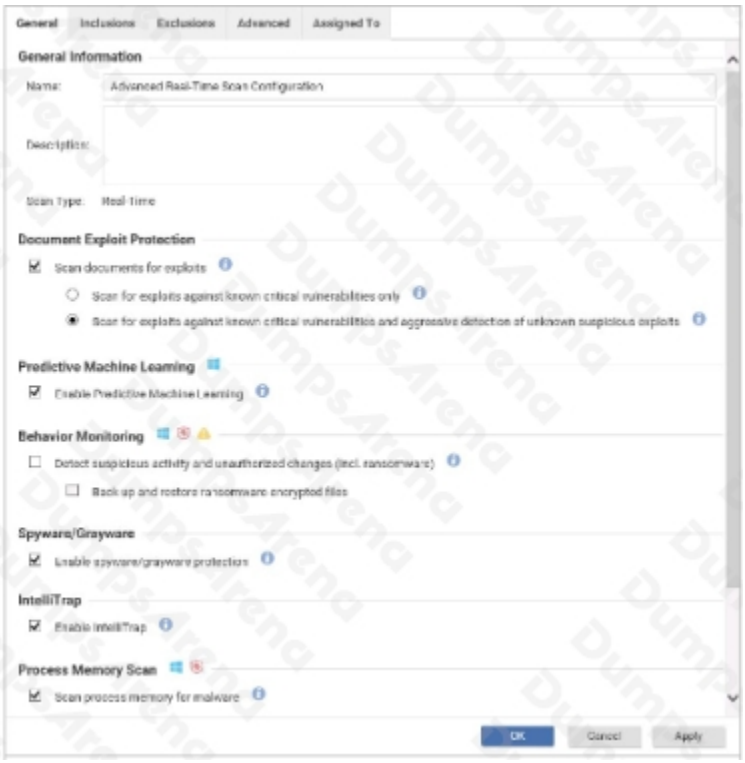
C. The Firewall Protection Module can detect and block Cross Site Scripting and SQL In-jection attacks.

D. The Firewall Protection Module can prevent DoS attacks coming from multiple systems.

ANSWER: D

QUESTION NO: 7

Based on the Malware Scan Configuration displayed in the exhibit, which of the following statements is false.



A. Any document files that display suspicious behavior will be submitted and executed in a sandbox environment on a Deep Discover Analyzer device.

B. Deep Security Agents using this Malware Scan Configuration will not monitor for compromised Windows processes.

C. Deep Security Agents will only be able to identify malware in files by using patterns downloaded from the Smart Protection Network.

D. Internet access is required to properly enable the features identified in this configuration.

ANSWER: B

Explanation:

Explanation

Configure Malware Scan

QUESTION NO: 8

Which of the following statements correctly identifies the purpose of the Integrity Monitoring Protection Module?

A. The Integrity Monitoring Protection Module monitors traffic to verify the integrity of incoming traffic to identify protocol deviations, packets fragments and other protocol anomalies.

B. The Integrity Monitoring Protection Module monitors critical operating system objects such as services, processes, registry keys and ports to detect and report malicious or unexpected changes.

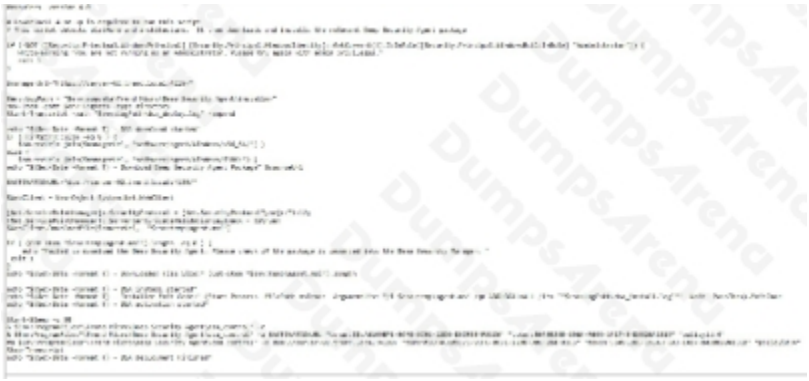
C. The Integrity Monitoring Protection Module monitors incoming traffic to confirm the integrity of header information including packet source and destination details.

D. The Integrity Monitoring Protection Module monitors and analyzes the integrity of application logs to identify tampering, corruption and other suspicious modifications to the logs.

ANSWER: B

QUESTION NO: 9

Based on the script displayed in the exhibit, which of the following statements are correct? Select all that apply.



A. Deep Security Agents deployed using this script will be activated against Tenant 0 in a multi-tenant environment.

B. This script will deploy the Deep Security Agent on a server, but will not automatically activate it.

C. Deep Security Agents deployed using this script are activated against a specific tenant.

D. Deep Security Agents deployed using this script will be assigned a specific policy when activated.

ANSWER: C D