DUMPSQUEEN

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://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

Which of the following file types would not be evaluated by the Application Control Protection Module?

A. .py scripts

B. .exe files

C. .class files

D. .docx files

ANSWER: D

QUESTION NO: 2

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

QUESTION NO: 3

The maximum disk space limit for the Identified Files folder is reached. What is the expected Deep Security Agent behavior in this scenario?

A. Any existing files are in the folder are compressed and forwarded to Deep Security Manager to free up disk space.

B. Deep Security Agents will delete any files that have been in the folder for more than 60 days.

C. Files will no longer be able to be quarantined. Any new files due to be quarantined will be deleted instead.

D. Deep Security Agents will delete the oldest files in this folder until 20% of the allocated space is available.

ANSWER: D

Explanation:

Explanation

If the limit is reached, the oldest files will be deleted first until 20% of allocated space is freed up.

Explication: Study Guide - page (203)

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

The Intrusion Prevention Protection Module is enabled, its Behavior is set to Prevent and rules are assigned. When viewing the events, you notice that one of Intrusion Prevention rules is being triggered and an event is being logged but the traffic is not being blocked. What is a possible reason for this?

A. The Deep Security Agent is experiencing a system problem and is not processing packets since the "Network Engine System Failure" mode is set to "Fail Open".

B. The network engine is running in Inline mode. In Inline mode, Deep Security provides no protection beyond a record of events.

C. The Intrusion Prevention rule is being triggered as a result of the packet sanity check failing and the packet is being allowed to pass.

D. The default Prevention Behavior in this particular rule may be set to Detect. This logs the triggering of the rule, but does not actually enforce the block.

ANSWER: D

QUESTION NO: 6

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: 7

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: 8

A Deep Security administrator wishes to monitor a Windows SQL Server database and be alerted of any critical events which may occur on that server. How can this be achieved using Deep Security?

A. The administrator could install a Deep Security Agent on the server hosting the Win-dows Server 2016 database and enable the Integrity Monitoring Protection Module. A rule can be assigned to monitor the Windows SQL Server for any modifications to the server, with Alerts enabled.

B. The administrator could install a Deep Security Agent on the server hosting the Win-dows Server 2016 database and enable the Log Inspection Protection Module. A rule can be assigned to monitor the Windows SQL Server for any critical events, with Alerts enabled.

C. The administrator could install a Deep Security Agent on the server hosting the Win-dows Server 2016 database and enable the Intrusion Prevention Protection Module. A Recommendation Scan can be run and any suggested rule can be assigned to monitor the Windows SQL Server for any vulnerabilities, with Alerts enabled.

D. This can not be achieved using Deep Security. Instead, the administrator could set up log forwarding within Window SQL Server 2016 and the administrator could monitor the logs within the syslog device.

ANSWER: B

QUESTION NO: 9

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)