PassQueen
a.k.a dumpsqueen.com

Trend Micro Certified Professional for Deep Security Exam

Trend Micro Deep-Security-Professional

Version Demo

Total Demo Questions: 11

Total Premium Questions: 113

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which of the following object types can be monitored by Integrity Monitoring rules? Select all that apply.

A. Files

B. Directories

C. Windows Registry keys and values

D. Network connections

ANSWER: A B C

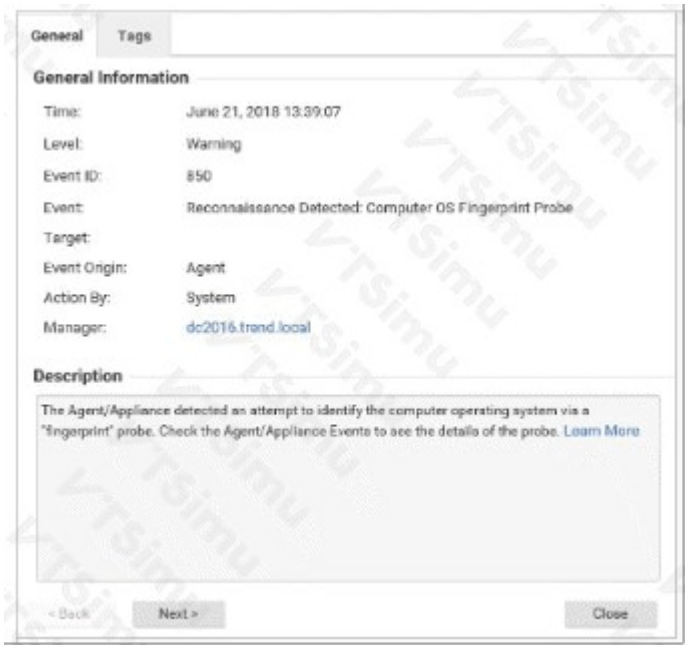
Explanation:

Integrity Monitoring rules can monitor important system objects for additions, modifications, deletions, and other changes. Supported objects include **files**, **directories**, **Windows Registry keys**, and **Windows Registry values**. Monitoring these objects helps administrators identify unexpected changes to operating-system files, application configurations, and critical registry settings.

Network connections are evaluated by network protection capabilities such as Firewall and Intrusion Prevention, not by Integrity Monitoring. See the Trend Micro Deep Security Integrity Monitoring documentation.

QUESTION NO: 2

Based on the details of event displayed in the exhibit, which of the following statements is false?



A. You can instruct the Deep Security Agents and Appliances to block traffic from the source IP address for a period of time.

B. You can create a firewall rule to permanently block traffic from the originating IP ad-dress.

C. The scan may be generated from an IP address which may be known to you. If so, the source IP address can be added to the reconnaissance whitelist.

D. The Intrusion Prevention Protection Modules must be enabled to detect reconnaissance scans.

ANSWER: D

Explanation:

The statement “The Intrusion Prevention Protection Modules must be enabled to detect reconnaissance scans.” is false because reconnaissance scan detection is a Deep Security Firewall capability, not a requirement of the Intrusion Prevention module. The Firewall module analyzes connection activity for behavior associated with port scans and address scans, generating reconnaissance-scan events when its configured scan-detection thresholds are met. Firewall settings can also be used to configure the response to detected reconnaissance activity, including temporarily blocking the scanning source and defining exclusions for trusted scanners or other known source addresses. Intrusion Prevention provides signature- and protocol-based protection against exploits, vulnerabilities, and malicious traffic, but enabling it is not a prerequisite for Firewall reconnaissance-scan detection. Therefore, an event identifying reconnaissance activity is handled through the Firewall protection functionality and its associated configuration. Trend Micro documents Firewall protection and its detection settings in the Deep Security online help: Firewall protection. Additional product documentation is available from the Deep Security 20 online help.

QUESTION NO: 3

Which of the following statements is true regarding Maintenance Mode in the Application Control protection Module?

A. While in Maintenance Mode, all Block and Allow rules are ignored while new or updated applications are added to the software inventory

B. When in Maintenance Mode, the Application Control Protection Module will continue to block software identified in Block rules, but will allow new and changed applications to be added to the software inventory.

C. When enabled, Maintenance Mode rescans the protected computer to rebuild the soft-ware inventory. Any new or changed software will be included in this rebuilt inventory.

D. Maintenance Mode can be configured as a Scheduled Event. In this scenario, all soft-ware upgrades will be performed at the same time every day to avoid creating Alerts for normal software updates.

ANSWER: B

Explanation:

When in Maintenance Mode, the Application Control Protection Module will continue to block software identified in Block rules, but will allow new and changed applications to be added to the software inventory. Maintenance Mode is intended for planned and legitimate system changes, such as software installation, patching, or upgrades. During this period, Application Control learns the new or modified executable files and updates its software inventory, preventing expected maintenance activity from being treated as an unauthorized change. Importantly, Maintenance Mode does not suspend explicit blocking policy: software that matches an Application Control Block rule remains prohibited. This preserves protection against known unwanted or disallowed applications even while administrators are making approved changes. After Maintenance Mode ends, the newly inventoried software can be evaluated and managed through the normal Application Control rules and inventory processes. Trend Micro documents Maintenance Mode as the mechanism for permitting expected software changes while retaining enforcement of Block rules, rather than as a complete bypass of Application Control policy. See Trend Micro’s Application Control Maintenance Mode documentation and its Application Control documentation.

QUESTION NO: 4

Which of the following update content can be distributed by a Deep Security Relay? Select all that apply.

A. Security updates

B. Deep Security Agent software packages

C. Deep Security Virtual Appliance software packages

D. Policy settings

ANSWER: A B C

Explanation:

Deep Security Relays retrieve approved content from their configured update source and make it available to Deep Security components in the local environment. A Relay can distribute **security updates**, **Deep Security Agent software packages**, and **Deep Security Virtual Appliance software packages**. This reduces repeated downloads over constrained WAN or Internet connections.

Policy settings are distributed by Deep Security Manager through Agent-Manager communication, not by a Relay. See the Trend Micro Deep Security Relay documentation and the Deep Security update documentation.

QUESTION NO: 5

How does Smart Scan vary from conventional pattern-based anti-malware scanning?

A. Smart Scan improves the capture rate for malware scanning by sending features of suspicious files to a cloud-based server where the features are compared to known malware samples.

B. Smart Scan shifts much of the malware scanning functionality to an external Smart Protection Server.

C. Smart Scan is performed in real time, where conventional scanning must be triggered manually, or run on a schedule.

D. Smart Scan identifies files to be scanned based on the content of the file, not the extension.

ANSWER: B

Explanation:

Smart Scan shifts much of the malware scanning functionality to an external Smart Protection Server. This is the defining architectural difference from conventional scan methods, in which the endpoint relies primarily on locally stored pattern files for malware identification. With Smart Scan, the Deep Security Agent retains a lightweight set of local patterns and uses them for an initial lookup. When further reputation or pattern matching is needed, it submits file-related identification data to Smart Protection infrastructure, which can be an on-premises Smart Protection Server or a Trend Micro-hosted service. The server performs the more extensive pattern lookup and returns a detection decision to the agent.

This design reduces the size of the pattern content that must be kept and updated on every protected computer. It also centralizes substantial pattern-matching work, helping conserve endpoint disk space and administrative update overhead while retaining malware protection. The agent still participates in scanning and enforcement; Smart Scan is not simply a cloud-only scan. Rather, it combines local intelligence with a Smart Protection source for the broader lookup capability. Trend Micro documents the Smart Scan architecture and its use of Smart Protection services in the Deep Security Smart Scan documentation and the Smart Protection Server documentation.

QUESTION NO: 6

Multi-tenancy is enabled in Deep Security and new tenants are created. Where does the new tenant data get stored when using SQL Server as the Deep Security database?

A. The new tenant data is added to the existing SQL Server database.

B. An additional table is created for each new tenant in the existing database in the SQL Server database to store its data.

C. An additional database is created in SQL Server for each new tenant to store its data.

D. An additional user is created for each new tenant in the SQL Server database to store its data.

ANSWER: C

Explanation:

An additional database is created in SQL Server for each new tenant to store its data. Deep Security multi-tenancy separates tenant data at the database level when the Deep Security Manager uses Microsoft SQL Server (and similarly when it uses PostgreSQL). The deployment has a primary Deep Security database that holds the manager's central data and configuration, while each tenant receives its own separate database. This design provides strong tenant isolation: tenant-specific policies, computers, events, and configuration data are maintained independently rather than being intermingled in shared tables. The Manager creates and manages the tenant database as part of the tenant-provisioning process, using the database connection and permissions configured for Deep Security. This SQL Server behavior differs from Oracle deployments, where tenant separation is implemented through database users and their associated tables within the Oracle database. For SQL Server, however, the relevant storage unit for a newly created tenant is a distinct additional database. Trend Micro documents multi-tenant deployment and database considerations in its Deep Security documentation: Deep Security multi-tenant deployments and Deep Security database installation and configuration.

QUESTION NO: 7

Your organization would like to implement a mechanism to alert administrators when files on a protected servers are modified or tampered with. Which Deep Security Protection Module should you enable to provide this functionality?

A. The Integrity Monitoring Protection Module

B. The File Inspection Protection Module

C. Deep Security can not provide this type of functionality

D. The Intrusion Prevention Protection Module

ANSWER: A

Explanation:

The Integrity Monitoring Protection Module is correct because it is designed to detect and report changes to the integrity of important system objects on protected servers. Administrators can create or apply integrity monitoring rules that watch designated files, directories, registry keys, and other supported objects. When a monitored file is created, modified, deleted, renamed, or otherwise changed, Deep Security records the event and can generate alerts or notifications for administrators. This provides the file-change visibility needed to identify possible tampering, unexpected configuration changes, or unauthorized modification of critical operating system and application files. Integrity monitoring works by establishing a baseline for monitored objects and comparing subsequent scans or real-time events against that baseline, depending on the platform and configured rule. It is therefore the appropriate Deep Security capability for file integrity monitoring and alerting. Trend Micro describes Integrity Monitoring as a control for monitoring critical files and registry values for unexpected changes, helping organizations meet security and compliance objectives. See the Trend Micro Deep Security Integrity Monitoring documentation and the Deep Security Integrity Monitoring overview.

QUESTION NO: 8

Which of the following statements is true regarding Intrusion Prevention rules?

A. Intrusion Prevention rules can block unrecognized software from executing.

B. Intrusion Prevention rules check for the IP addresses of known malicious senders within a packet

C. Intrusion Prevention rules can detect or block traffic associated with specific applica-tions, such as Skype or file-sharing utilities.

D. Intrusion Prevention rules monitor the system for changes to a baseline configuration.

ANSWER: C

Explanation:

Intrusion Prevention rules can detect or block traffic associated with specific applica-tions, such as Skype or file-sharing utilities. In Deep Security, Intrusion Prevention provides network-based protection by inspecting traffic and comparing it with

rule definitions. Beyond vulnerability shielding, rule definitions can identify particular protocols, applications, and traffic behaviors. This enables an administrator to apply a rule in detect-only mode for visibility or in prevent mode to actively block matching traffic, depending on the policy action and the rule configuration. Application-related intrusion prevention rules are useful where an organization needs to control or gain visibility into the use of peer-to-peer, messaging, remote-access, or other application traffic on protected hosts. Rule assignment and the selected action determine whether a matching connection is merely logged or is interrupted. Trend Micro documents Intrusion Prevention as a Deep Security protection module that inspects network traffic for defined threats and supports both detection and prevention actions. The product documentation also describes managing and assigning IPS rules through policies and computers, which is how application-traffic rules are enabled for the relevant workloads. See Trend Micro's Intrusion Prevention documentation and the Deep Security Intrusion Prevention overview.

QUESTION NO: 9

Which of the following are valid reasons for deploying Deep Security Relays in a remote network location? Select all that apply.

A. To provide a local source of security updates for Deep Security Agents.

B. To reduce repeated update downloads across a WAN connection.

C. To distribute policy settings immediately after an administrator saves a policy.

D. To collect and store all Events generated by protected computers.

ANSWER: A B

Explanation:

Deep Security Relays provide a local source for software and security updates. Agents in a remote or bandwidth-constrained location can retrieve applicable content from a Relay instead of each downloading the same content across a WAN connection. This reduces repeated external downloads and can improve update efficiency for the protected computers at that location.

Relays retrieve approved update content from their configured upstream source and distribute it to Deep Security components. They do not distribute policies or replace Deep Security Manager as the central management component. See the Deep Security Relay documentation.

QUESTION NO: 10

Which of the following are valid methods for initiating or maintaining Recommendation Scans for a protected computer? Select all that apply.

A. Run a Recommendation Scan manually from Deep Security Manager.

B. Enable Ongoing Scans for regular reassessment.

C. Restart the Deep Security Agent service.

D. Reset the Deep Security Agent.

ANSWER: A B

Explanation:

An administrator can manually run a Recommendation Scan to evaluate the current operating system, installed applications, and available protection rules for a protected computer. Ongoing Scans can also be enabled to repeat this assessment regularly, which helps keep recommendations current as software, patches, and security rule content change.

Restarting an Agent or enabling a protection module does not by itself represent the configured ongoing recommendation-scan workflow. Recommendation results identify applicable rules, but the rules must still be assigned manually unless

automatic application of recommendations is enabled. See the Trend Micro Deep Security Recommendation Scans documentation.

QUESTION NO: 11

Which of the following Deep Security Protection Modules require a Deep Security Agent installed inside the protected workload? Select all that apply.

A. Application Control

B. Integrity Monitoring

C. Log Inspection

D. Firewall

ANSWER: A B C

Explanation:

Application Control, **Integrity Monitoring**, and **Log Inspection** require a Deep Security Agent because they need local access to executable files, file-system objects, registry objects, and operating-system or application log sources. The agent performs the monitoring and enforcement functions within the protected workload.

Firewall can be provided in supported agentless VMware deployments through the Deep Security Virtual Appliance and VMware integration. See the Trend Micro Deep Security protection modules documentation and the agentless protection documentation.