



Free Questions for **PSE-Endpoint** by **braindumpscollection**

Shared by **Contreras** on **24-05-2024**

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A retail company just purchased Traps for its 8,000 endpoints. Many of its users work remotely. The company is not using any VPN solution, but would still like to manage all endpoints regardless where they are.

Which two aspects should be part of the recommendation? (Choose two.)

Options:

- A-** As each ESM Core server can handle up to 30,000 endpoints, use at least 1 ESM Core server internally and 1 ESM core server in the DMZ for external endpoints.
- B-** Placing an ESM Core server in the DMZ or in a cloud hosting service allows external endpoints to connect to it, even without a VPN client.
- C-** Protection for remote endpoints is currently not supported. Since the ESM servers can only be installed in an internal network, endpoints without VPN will not be able to connect to it.
- D-** If there is no connection to the ESM Core server, Traps agents automatically connect to WildFire and endpoints are fully protected. No additional ESM Core servers are needed.

Answer:

A, B

Question 2

Question Type: MultipleChoice

A large manufacturer is planning to roll out Traps to 75,000 endpoints. Their environment consists of three major sites with 24,000 endpoints each, plus about 3,000 remote endpoints in smaller remote locations using always-on VPN connections to a single one of the major sites. The customer wants to minimize network traffic between the major sites, but all endpoints have internet access. The customer is looking for a centrally managed solution with common reporting and management for all endpoints in the environment.

Which design option would be appropriate for this environment?

Options:

- A-** Place the Traps database, ESM Console and two ESM core servers in the large site hosting the VPN gateway, and force all endpoints to use VPN at all times.
- B-** Place the Traps database, ESM Console and seven ESM core servers in a public-cloud environment where the ESM Core servers are accessible from the internet.
- C-** Place a Traps database, ESM Console and an ESM core server in each of the three large sites.
- D-** Place the Traps database and ESM Console in one of the major sites, and one ESM core server in each of the three major sites.

Answer:

D

Question 3

Question Type: MultipleChoice

An administrator receives an alert indicating the ESM service is not starting on the ESM Server. When the administrator tries to start the service manually, the administrator receives an error. "The Endpoint Security Manager service on Local Computer started and then stopped."

What is the cause of the failure?

Options:

- A-** The Account assigned to the service does not have 'Log on as a batch job' permissions on the machine.
- B-** The Account assigned to the service does not have "Log on as a service' permissions on the machine.
- C-** The Account assigned to the service is not the Local Administrator on the machine.
- D-** The Account assigned to the service is not an Active Directory Domain user.

Answer:

B

Question 4

Question Type: MultipleChoice

A customer has an environment with the following:

- * 1,000 agents communicating over SSL with two servers - one containing the ESM Server and another one where the ESM Console is installed
- * BitsUploads resides on the ESM Console server
- * ESM Server and Console are using the default pods for communication

In a scenario where a file is failing to be uploaded from macOS, which three reasons could be directly related to the failure? (Choose three.)

Options:

- A-** Traps agent is not able to check in with the ESM Server
- B-** The rate of upload is lower than 100Kb/S

- C- The BITS address in the ESM is incorrect
- D- Port 2125 is blocked on the server which hosts BitsUploads
- E- Port 443 is blocked on the server which hosts BitsUploads

Answer:

A, C, E

Question 5

Question Type: MultipleChoice

An administrator can check which two indicators to verify that Traps for Mac is running correctly on an installed endpoint? (Choose two.)

Options:

- A- Use cytool from the command line interface to display the running Traps agent services.
- B- In the Activity Monitor, verify that CyveraService is running
- C- Ping other Traps agents from the macOS agent
- D- Verify that the Traps agent icon is displayed on the macOS finder bar.

Answer:

B, D

Question 6

Question Type: MultipleChoice

Which set of modules must be loaded and configured when using Metasploit?

Options:

A- Attacker, payload

B- Exploit, payload

C- Exploit, malware

D- Malware, host

Answer:

C

Question 7

Question Type: MultipleChoice

There are two custom policy rules in ESM Console. Policy rule number 1000 turns ROP off for winword.exe. Policy rule number 1001 turns ROP on for winword.exe

What is the ROP module status for winword.exe?

Options:

- A- Due to the collision in the policy rules, ROP is enabled in notification mode.
- B- The lower numbered policy rule takes precedence. ROP is off for winword.exe
- C- The higher numbered policy rule takes precedence. ROP is on for winword.exe
- D- The default policy rule takes precedence over both policy rules 1000 and 1001 and disables ROP for winword.exe

Answer:

B

Question 8

Question Type: MultipleChoice

Which two enhanced key usage purposes are necessary when creating an SSL certificate for an ESM server? (Choose two.)

Options:

- A- File Recovery
- B- Server Authentication
- C- Client Authentication
- D- Key Recovery

Answer:

B, C

Question 9

Question Type: MultipleChoice

An administrator is testing an exploit that is expected to be blocked by the JIT Mitigation EPM protecting the viewer application in use. No prevention occurs, and the attack is successful.

In which two ways can the administrator determine the reason for the missed prevention? (Choose two.)

Options:

- A-** Check in the HKLM\SYSTEM\Cyvera\Policy registry key and subkeys whether JIT Mitigation is enabled for this application
- B-** Check if a Just-In-Time debugger is installed on the system
- C-** Check that the Traps libraries are injected into the application
- D-** Check that all JIT Mitigation functions are enabled in the HKLM\SYSTEM\Cyvera\Policy\Organization\Process\Default registry key

Answer:

A, C

Question 10

Question Type: MultipleChoice

Which MSI command line parameters will successfully install a Traps agent using SSL and pointed to server ESM?

Options:

- A- msiexec /i c:\traps.msi /qn TRAPS_SERVER=ESM USE_SSL_PRIMARY=1
- B- msiexec /i c:\traps.msi /qn CYVERA_SERVER=ESM USE_SSL_PRIMARY=1
- C- msiexec /i c:\traps.msi /qn ESM_SERVER=ESM USE_SSL_PRIMARY=1
- D- msiexec /x c:\traps.msi /qn SERVER=ESM USE_SSL_PRIMARY=1

Answer:

B

Question 11

Question Type: MultipleChoice

An administrator has installed Traps 4.0. The administrator wants to test the malware protections provided. What sample should they use to test the protections provided by Traps?

Options:

- A- A sample with a low number of hits in Virus Total
- B- A toolbar package known to be flagged as grayware by Traps

C- A sample known to generate false positives in the production environment

D- An MS Office document which contains a ransomware macro

Answer:

D

To Get Premium Files for PSE-Endpoint Visit

<https://www.p2pexams.com/products/pse-endpoint>

For More Free Questions Visit

<https://www.p2pexams.com/palo-alto-networks/pdf/pse-endpoint>

