Exam Report: 9.11.3 Practice Questions

Date: 1/28/2020 7:23:31 pm
Time Spent: 0:27

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

DLP can be used to identify sensitive files in a file system and then embed the organization's security policy within the file.

Which of the following DLP implementations travels with sensitive data files when they are moved or copied?

- ~~Endpoint DLP~~
- Network DLP
- File-level DLP
- Cloud DLP

Explanation

File-Level DLP is used to identify sensitive files in a file system and then to embed the organization's security policy within the file so that it travels with the file when it is moved or copied. Since the security policy travels with that file if it's moved or copied, you can continue to control access to the file, such as restricting who it can be transmitted to, even when the file is no longer on your system.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_04]

Question 2: Correct

Sensitive data is monitored by the data loss prevention (DLP) system in four different states. Which of the following is NOT one of the states monitored by DLP?

- While a file with sensitive data is being created.
- While being transmitted to or from cloud-based systems.
- While in use on endpoint systems.
- While in motion as it is transmitted over the network.
- While at rest on a storage medium.

Explanation

DLP does not monitor sensitive data while files are being created.

Sensitive data is monitored by the DLP system in four different states:

- While in use on endpoint systems to monitor and control access to physical devices on workstations or servers.

- While in motion as it is transmitted over the network.
- While at rest on a storage medium.
- While being transmitted to or from cloud-based systems.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_02]

Question 3: Correct

Which of the following is a technology that tries to detect and stop sensitive data breaches, or data leakage incidents, in an organization?

- Data transmission security
- Data hashing
- Data loss prevention
- Public key cryptography

Explanation

Data loss prevention (DLP) is a technology that tries to detect and stop sensitive data breaches, or data leakage incidents, in an organization. DLP is used to prevent sensitive data from being disclosed to an unauthorized person, whether it is deliberate or accidental.

Data transmission security is the use of secure protocols to encrypt data when it is transmitted. Hashing takes a variable-length string (message) and compresses and transforms it into a fixed-length value. When received, the hash is decrypted into the actual output so the recipient can understand the message. Public key infrastructure uses certificates, which are electronic document that uses a digital signature, to bind a public key with an identity.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_01]

Question 4: Correct

Which of the following DLP implementations can be used to monitor and control access to the physical devices on workstations or servers?

- File-level DLP
- Network DLP
- Endpoint DLP
- Cloud DLP

Explanation

Endpoint DLP runs on end user workstations and servers. Endpoint DLP is also referred to as a Chinese Wall solution. It could be something as simple as restricting the use of USB devices. Many endpoint-based systems also provide application controls to prevent confidential information transmission. They also provide some type of immediate feedback to the user. Giving feedback to the user is based on the concept that not all data leakage incidents are malicious. The employee might not realize that the security policy violation notification is appropriate. The intent is to deter the employee from a similar action in the future.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_05]

Question 5: Incorrect

DLP can be implemented as a software or hardware solution that analyzes traffic in an attempt to detect

sensitive data that is being transmitted in violation of an organization's security policies.
Which of the following DLP implementations analyzes traffic for data containing such things as financial documents, social security numbers, or key words used in proprietary intellectual property?

- ~~File-level DLP~~
- Network DLP
- Cloud DLP
- Endpoint DLP

Explanation

Network DLP is a software or hardware solution that is typically installed near the network perimeter. It analyzes network traffic in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies.

References

LabSim for Security Pro, Section 9.11.
[All Questions SecPro2017_v6.exm DLP_03]