Exam : **ISA-N_Retake**

Title : PCI Internal Security Assessor Retake

Version : DEMO

1.Which systems must have anti-malware solutions'
A. All CDE systems, connected systems. NSCs. and security-providing systems
B. All portable electronic storage
C. All systems that store PAN
D. Any in-scope system except for those identified as not at risk from malware
Answer: D
Explanation:
According to the PCI DSS v3.2.1 Quick Reference Guide1, any in-scope system except for those identified as not at risk from malware must have anti-malware solutions installed and configured according to best practices. This is one of the requirements for preventing malware infections that could compromise cardholder data.

2.A retail merchant has a server room containing systems that store encrypted PAN data.
The merchant has implemented a badge access-control system that identities who entered and exited the room on what date and at what time There are no video cameras located in the server room Based on this information, which statement is true regarding PCI DSS physical security requirements?
A. The badge access-control system must be protected from tampering or disabling
B. The merchant must install video cameras in addition to the existing access-control system
C. Data from the access-control system must be securely deleted on a monthly basis
D. The merchant must install motion-sensing alarms in addition to the existing access-control system
Answer: A
Explanation:
PCI DSS Requirement 9.1.1 requires entities to use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment (CDE)1. A badge access-control system is one example of such a control, as it can identify who entered and exited the server room and when. However, this control is only effective if it is protected from tampering or disabling by unauthorized persons, as PCI DSS Requirement 9.1.2 states1. Otherwise, the access-control system could be bypassed or compromised, allowing unauthorized access to the systems that store encrypted PAN data. Therefore, the badge access-control system must be protected from tampering or disabling, as stated in option A.
The other options are not true regarding PCI DSS physical security requirements for a server room. Option B is not true because PCI DSS does not mandate the use of video cameras in addition to the existing access-control system, although it is a recommended best practice2.
Option C is not true because PCI DSS does not specify a data retention period for the access-control system, although it requires entities to retain audit trail history for at least one year, with a minimum of three months immediately available for analysis3.
Option D is not true because PCI DSS does not require the use of motion-sensing alarms in addition to the existing access-control system, although it is another recommended best practice2.
References:
PCI DSS v3.2.1
PCI DSS Requirement 9: Upping Your Physical Security
PCI DSS Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

3.What do PCI DSS requirements for protecting cryptographic keys include?

A. Public keys must be encrypted with a key-encrypting key.
B. Data-encrypting keys must be stronger than the key-encrypting key that protects it.
C. Private or secret keys must be encrypted, stored within an SCD or stored as key components
D. Key-encrypting keys and data-encrypting keys must be assigned to the same key custodian
Answer: C
Explanation:
According to the PCI DSS v3.2.1 Quick Reference Guide1, private or secret keys must be encrypted, stored within an SCD or stored as key components. This is one of the requirements for ensuring secure encryption and authentication.

4.Could an entity use both the Customized Approach and the Defined Approach to meet the same requirement?
A. No because a single approach must be selected
B. No. because only compensating controls can be used with the Defined Approach
C. Yes if the entity uses no compensating controls
D. Yes if the entity is eligible to use both approaches
Answer: C
Explanation:
an entity can use both the Customized Approach and the Defined Approach to meet the same requirement, as long as it uses compensating controls to address any weaknesses or gaps in the customized control. This is one of the requirements for ensuring that an entity can use both approaches when appropriate.

5.In accordance with PCI DSS Requirement 10. how long must audit logs be retained?
A. At least 1 year, with the most recent 3 months immediately available
B. At least 2 years, with the most recent 3 months immediately available
C. At least 2 years with the most recent month immediately available
D. At least 3 months with the most recent month immediately available
Answer: A
Explanation:
According to the PCI DSS v3.2.1 Quick Reference Guide1, audit logs must be retained for at least 1 year, with the most recent 3 months immediately available. This is one of the requirements for ensuring that audit logs are available for review and analysis.