ISA-IEC-62443 Q&As

ISA/IEC 62443 Cybersecurity Fundamentals Specialist

Pass ISA ISA-IEC-62443 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/isa-iec-62443.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISA Official Exam Center

QUESTION 1

Which of the ISA 62443 standards focuses on the process of developing secure products?

Available Choices (select all choices that are correct)

A. 62443-1-1

B. 62443-3-2

C. 62443-3-3

D. 62443-4-1

Correct Answer: D

The ISA/IEC 62443 series of standards is divided into four main parts, each covering a different aspect of industrial automation and control systems (IACS) cybersecurity1: Part 1: Terminology, Concepts, and Models Part 2: Policies and Procedures Part 3: System Requirements Part 4: Component Requirements The part 4 of the series focuses on the requirements for the secure development and maintenance of products that are used in IACS, such as controllers, sensors, actuators, network devices, software applications, and cloud services. The part 4 consists of two standards1:

QUESTION 2

Which of the following tools has the potential for serious disruption of a control network and should not be used on a live system?

Available Choices (select all choices that are correct) A. Remote desktop

B. Vulnerability scanner

C. FTP

D. Web browser

Correct Answer: B

A vulnerability scanner is a tool that scans a network or a system for known vulnerabilities, such as misconfigurations, outdated software, or weak passwords. A vulnerability scanner can provide valuable information for improving the security posture of a system, but it can also cause serious disruption of a control network if used on a live system. This is because a vulnerability scanner may generate a large amount of network traffic, consume system resources, trigger alarms, or even crash devices by exploiting vulnerabilities. Therefore, a vulnerability scanner should not be used on a live system without proper authorization and precautions. A vulnerability scanner should only be used on a test or isolated network, or during a scheduled maintenance window with minimal impact on the system operation. References: ISA/IEC 62443 Standards to Secure Your Industrial Control System, Module 5: Assessing the Current Security Level, Slide 25.

QUESTION 3

Within the National Institute of Standards and Technoloqv Cybersecuritv Framework v1.0 (NIST CSF), what is the status of the ISA 62443 standards?

Available Choices (select all choices that are correct)

A. They are used as informative references.

B. They are used as normative references.

C. They are under consideration for future use.

D. They are not used.

Correct Answer: A

The NIST CSF is a voluntary framework that provides a set of standards, guidelines, and best practices to help organizations manage cybersecurity risks. The NIST CSF consists of five core functions: Identify, Protect, Detect, Respond, and Recover. Each function is further divided into categories and subcategories that describe specific outcomes and activities. The NIST CSF also provides informative references that link the subcategories to existing standards, guidelines, and practices that can help organizations achieve the desired outcomes. The informative references are not mandatory or exhaustive, but rather serve as examples of possible sources of guidance. The ISA 62443 standards are used as informative references in the NIST CSF v1.0 for several subcategories, especially in the Protect and Detect functions. The ISA 62443 standards are a series of standards that provide a framework for securing industrial automation and control systems (IACS). The ISA 62443 standards cover various aspects of IACS security, such as terminology,concepts, requirements, policies, procedures, and technical specifications. The ISA 62443 standards are aligned with the NIST CSF in terms of the core functions and the risk-based approach. Therefore, the ISA 62443 standards can provide useful guidance and best practices for organizations that use IACS and want to implement the NIST CSF. References: NIST Cybersecurity Framework - Official Site1 Framework for Improving Critical Infrastructure Cybersecurity - Version 1.02 ISA/IEC 62443 Standards - Official Site3 ISA/IEC 62443 Compliance and Scoring | Centraleyes4

QUESTION 4

At Layer 4 of the Open Systems Interconnection (OSI) model, what identifies the application that will handle a packet inside a host?

Available Choices (select all choices that are correct)

A. ATCP/UDP application ID

B. A TCP/UDP host ID

C. ATCP/UDP port number

D. ATCP/UDP registry number

Correct Answer: C

At layer 4 of the OSI model, also known as the transport layer, the application that will handle a packet inside a host is identified by a TCP/UDP port number. A port number is a 16-bit integer that is assigned to a specific application or service that runs on a host. Port numbers are used to multiplex and demultiplex the data streams that are exchanged between hosts and end systems. Multiplexing is the process of combining multiple data streams into one, while demultiplexing is the process of separating one data stream into multiple ones. Port numbers are part of the header of the transport layer protocol data unit (PDU), which is called a segment for TCP and a datagram for UDP. The header contains the source port number and the destination port number, which indicate the applications that are involved in the communication. For example, if a host sends a packet to another host using the HTTP protocol, which runs on port 80 by default, the source port number would be a random number chosen by thesender, and the destination port number would be 80. The receiver would then use the destination port number to demultiplex the packet and deliver it to the

HTTP application. Port numbers are divided into three ranges: well-known ports (0-1023), registered ports (1024-49151), and dynamic or private ports (49152-65535). Well-known ports are reserved for common and standardized applications and services, such as HTTP (80), FTP (21), and SSH (22). Registered ports are assigned by the Internet Assigned Numbers Authority (IANA) to specific applications and services that request them, such as Skype (49175) and Minecraft (25565). Dynamic or private ports are not assigned by any authority and can be used by any application or service that needs them, such as ephemeral ports that are used for temporary connections. The other options are not valid identifiers for the application that will handle a packet inside a host at layer 4 of the OSI model. A TCP/UDP application ID is not a term that is used in the OSI model or the TCP/IP model. A TCP/UDP host ID is not a term that is used in the OSI model or the TCP/IP model, and it would be more appropriate for layer 3, which is the network layer, where the host is identified by an IP address. A TCP/UDP registry number is not a term that is used in the OSI model or the TCP/IP model, and it would be more appropriate for layer 5, which is the session layer, where the registry number is used to identify a session between two hosts. References: Transport Layer | Layer 4 | The OSI-Model1 OSI model - Wikipedia2 What is Layer 4 of the OSI Model? | Glossary | A10 Networks3 What Are the 7 Layers of the OSI Model? | Webopedia4

QUESTION 5

Which is a commonly used protocol for managing secure data transmission on the Internet?

Available Choices (select all choices that are correct)

A. Datagram Transport Layer Security (DTLS)

B. Microsoft Point-to-Point Encryption

C. Secure Telnet

D. Secure Sockets Layer

Correct Answer: AD

Datagram Transport Layer Security (DTLS) and Secure Sockets Layer (SSL) are both commonly used protocols for managing secure data transmission on the Internet. DTLS is a variant of SSL that is designed to work over datagram protocols such as UDP, which are used for real-time applications such as voice and video. SSL is a protocol that provides encryption, authentication, and integrity for data transmitted over TCP, which is used for reliable and ordered delivery of data. Both DTLS and SSL use certificates and asymmetric cryptography to establish a secure session between the communicatingparties, and then use symmetric cryptography to encrypt the data exchanged. DTLS and SSL are widely used in web browsers, email clients, VPNs, and other applications that require secure communication over the Internet. References: ISA/IEC 62443 Standards to Secure Your Industrial Control System, Module 3: Introduction to Cryptography, pages 3-5 to 3-7 Using the ISA/IEC 62443 Standards to Secure Your Control System, Chapter 6: Securing Communications, pages 125-126