ISA-IEC-62443Q&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.geekcert.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 following provides the overall conceptual basis in the design of an appropriate security program?

Available Choices (select all choices that are correct)

A. Asset model

B. Zone model

C. Reference model

D. Reference architecture

Correct Answer: C

The reference model provides the overall conceptual basis in the design of an appropriate security program. It defines the common terminology, concepts, and models that can be used by all stakeholders responsible for IACS security. The reference model describes the general characteristics of IACS, the typical threats and vulnerabilities, the security lifecycle phases, and the security levels. The reference model also introduces the concepts of zones and conduits, which are used to group and isolate assets with similar security requirements and to control the communication between them. Referenceshttps://www.cisco.com/c/en/us/td/docs/solutions/Verticals/IoT_Security_L ab/IEC62443_WP.pdf https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/IoT_Security_Lab/IEC62443_WP .pdf

QUESTION 2

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 3

Which layer in the Open Systems Interconnection (OSI) model would include the use of the File Transfer Protocol (FTP)?

Available Choices (select all choices that are correct)

A. Application layer

B. Data link layer

C. Session layer

D. Transport layer

Correct Answer: A

The File Transfer Protocol (FTP) is an application layer protocol that moves files between local and remote file systems. It runs on top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection. The control connection is used to send commands and responses between the client and the server, while the data connection is used to transfer the actual file. FTP is one of the standard communication protocols defined by the TCP/IP model and it does not fit neatly into the OSI model. However, since the OSI model is a reference model that describes the general functions of each layer, FTP can be considered as an application layer protocol in the OSI model, as it provides user services and interfaces to the network. The application layer is the highest layer in the OSI model and it is responsible for providing various network services to the users, such as email, web browsing, file transfer, remote login, etc. The application layer interacts with the presentation layer, which is responsible for data formatting, encryption, compression, etc. The presentation layer interacts with the session layer, which is responsible for establishing, maintaining, and terminating sessions between applications. The session layer interacts with the transport layer, which is responsible for reliable end-to-end data transfer and flow control. The transport layer interacts with the network layer, which is responsible for routing and addressing packets across different networks. The network layer interacts with the data link layer, which is responsible for framing, error detection, and medium access control. The data link layer interacts with the physical layer, which is responsible for transmitting and receiving bits over the physical medium. References: File Transfer Protocol (FTP) in Application Layer1 FTP Protocol2 What OSI layer is FTP?3

QUESTION 4

Which is the implementation of PROFIBUS over Ethernet for non-safetv-related communications?

Available Choices (select all choices that are correct)

A. PROFIBUS DP

B. PROFIBUS PA

C. PROFINET

D. PROF1SAFE

Correct Answer: C

PROFINET is the implementation of PROFIBUS over Ethernet for non- safety-related communications. It is a standard for industrial Ethernet that enables real-time data exchange between automation devices, controllers, and higher-level systems. PROFINET uses standard Ethernet hardware and software, but adds a thin software layer that allows deterministic and fast communication. PROFINET supports different communication profiles for different applications, such as motion control, process automation, and functional safety. PROFINET is compatible with PROFIBUS, and allows seamless integration of existing PROFIBUS devices and networks123 References: 1: What is PROFINET? - PI North America

2: PROFINET - Wikipedia 3:

PROFINET Technology and Application - System Description

QUESTION 5

Which of the following attacks relies on a human weakness to succeed?

Available Choices (select all choices that are correct)

A. Denial-of-service

B. Phishing

C. Escalation-of-privileges

D. Spoofing

Correct Answer: B

Phishing is a type of cyberattack that relies on a human weakness to succeed. Phishing is the practice of sending fraudulent emails or other messages that appear to come from a legitimate source, such as a bank, a government agency, or a trusted person, in order to trick the recipient into revealing sensitive information, such as passwords, credit card numbers, or personal details, or into clicking on malicious links or attachments that may install malware or ransomware on their devices. Phishing is a common and effective way of compromising the security of industrial automation and control systems (IACS), as it can bypass technical security measures by exploiting the human factor. Phishing can also be used to gain access to the IACS network, to conduct reconnaissance, to launch further attacks, or to cause damage or disruption to the IACS operations. The ISA/IEC 62443 series of standards recognize phishing as a potential threat vector for IACS and provide guidance and best practices on how to prevent, detect, and respond to phishing attacks. Some of the recommended countermeasures include: Educating and training the IACS staff on how to recognize and avoid phishing emails and messages, and how to report any suspicious or malicious activity. Implementing and enforcing policies and procedures for email and message security, such as using strong passwords, verifying the sender\\'s identity, and not opening or clicking on unknown or unsolicited links or attachments. Applying technical security controls, such as antivirus software, firewalls, spam filters, encryption, and authentication, to protect the IACS devices and network from phishing attacks. Monitoring and auditing the IACS network and devices for any signs of phishing attacks, such as anomalous or unauthorized traffic, connections, or activities, and taking appropriate actions to contain and mitigate the impact of any incidents. References: ISA/IEC 62443-1-1:2009, Security for industrial automation and control systems - Part 1-1: Terminology, concepts and models1 ISA/IEC 62443-2-1:2009, Security for industrial automation and control systems - Part 2-1: Establishing an industrial automation and control systems security program2 ISA/IEC 62443-2-4:2015, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers3 ISA/IEC 62443-3-3:2013, Security for industrial automation and control systems - Part 3-3: System security requirements and security levels4 ISA/IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components5

Test Questions