ISA-IEC-62443$^{\text{Q\&As}}$

ISA/IEC 62443 Cybersecurity Fundamentals Specialist

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

QUESTION 1

Which of the following is an element of security policy, organization, and awareness?

Available Choices (select all choices that are correct)

A. Product development requirements

B. Staff training and security awareness

C. Technical requirement assessment

D. Penetration testing

Correct Answer: B

According to the ISA/IEC 62443-2-1 standard, security policy, organization, and awareness is one of the four foundational requirements for an IACS security management system. It defines the "policies, procedures, and organizational structure necessary to support the security program" 1. One of the elements of this requirement is staff training and security awareness, which involves "providing appropriate security education and training to all personnel who have access to or are responsible for IACS components" 1. This element aims to ensure that the staff are aware of the security risks, policies, and procedures, and are able to perform their roles and responsibilities in a secure manner. Staff training and security awareness can include topics such as security principles, threats and vulnerabilities, incident response, password management, physical security, and social engineering 2. References: ISA/IEC 62443 Series of Standards - ISA Security of Industrial Automation and Control Systems - ISAGCA

QUESTION 2

Which activity is part of establishing policy, organization, and awareness?

Available Choices (select all choices that are correct)

A. Communicate policies.

B. Establish the risk tolerance.

C. Identify detailed vulnerabilities.

D. Implement countermeasures.

Correct Answer: A

According to the ISA/IEC 62443 Cybersecurity Fundamentals Specialist course, establishing policy, organization, and awareness is one of the four steps of the IACS cybersecurity lifecycle. This step involves defining the cybersecurity policies, roles, and responsibilities, as well as communicating them to the relevant stakeholders. It also involves establishing the risk tolerance level, which is the acceptable level of risk for the organization. Communicating policies and establishing the risk tolerance are both activities that are part of this step. Identifying detailed vulnerabilities and implementing countermeasures are activities that belong to the next steps of the lifecycle, which are assessing the current situation and implementing the cybersecurityprogram, respectively. References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist course, Module 2: IACS Cybersecurity Lifecycle1

QUESTION 3

Which steps are included in the ISA/IEC 62443 assess phase?

Available Choices (select all choices that are correct)

A. Cybersecurity requirements specification and detailed cyber risk assessment

B. Cybersecurity requirements specification and allocation of IACS assets to zones and conduits

C. Detailed cyber risk assessment and cybersecurity maintenance, monitoring, and management of change

D. Allocation of IACS assets to zones and conduits, and detailed cyber risk assessment

Correct Answer: D

According to the ISA/IEC 62443 standards, the assess phase of the IACS cybersecurity lifecycle consists of two steps: allocation of IACS assets to zones and conduits, and detailed cyber risk assessment. The first step involves identifying and documenting the IACS assets and grouping them into logical zones based on their security requirements and functions. The second step involves performing a cybersecurity vulnerability and risk assessment for each zone and conduit, using the information from the previous step and the cybersecurity requirements specification from the identify phase. The assess phase aims to identify and understand the high-risk vulnerabilities that require mitigation in the design phase. References: ISA/IEC 62443-2-1:2010 - Establishing an industrial automation and control systems security program, section 4.3.2; Cybersecurity Training | ISA England Section

QUESTION 4

Which is the BEST deployment system for malicious code protection?

Available Choices (select all choices that are correct)

A. Network segmentation

B. IACS protocol converters

C. Application whitelistinq (AWL) OD.

D. Zones and conduits

Correct Answer: C

Application whitelisting (AWL) is a technique that allows only authorized applications to run on a system, and blocks any unauthorized or malicious code from executing. AWL is one of the most effective methods for preventing malware infections and reducing the attack surface of a system. AWL can be implemented at different levels, such as the operating system, the network, or the application itself. AWL is especially useful for industrial automation and control systems (IACS), which often run on legacy or proprietary platforms that are not compatible with traditional antivirus software or other security solutions. AWL can also help protect IACS from zero-day attacks, which exploit unknown vulnerabilities that have not been patched or detected by security vendors. AWL is recommended by the ISA/IEC 62443 standards as a key component of malicious code protection for IACS. According to the standards, AWL should be applied to all IACS components that support it, and should be configured and maintained according to the security policies and procedures of the organization. AWL should also be complemented by other security measures, such as network segmentation, zones and conduits, and patch management, to provide a defense-in-depth approach to IACS security. References: ISA/IEC 62443-3-3:2013, System security requirements and security levels, Section 5.2.3.41 ISA/IEC 62443-2-1:2010, Establishing an industrial automation and control systems security program, Section 4.3.3.6.42 ISA/IEC 62443-4-2:2019, Technical security requirements for IACS components, Section 4.2.3.43 ISA/IEC

62443-3-2:2020, Security risk assessment for system design, Section 7.3.3.44 ISA/IEC 62443-4-1:2018, Product development requirements, Section 5.2.3.45

QUESTION 5

What is the name of the protocol that implements serial Modbus over Ethernet?

Available Choices (select all choices that are correct)

A. MODBUS/CIP

B. MODBUS/Ethernet

C. MODBUS/Plus

D. MODBUS/TCP

Correct Answer: D

MODBUS/TCP is the name of the protocol that implements serial Modbus over Ethernet. MODBUS/TCP is a variant of the Modbus protocol that uses the Transmission Control Protocol (TCP) as the transport layer to encapsulate Modbus messages and send them over Ethernet networks. MODBUS/TCP preserves the Modbus application layer and data model, which means that serial Modbus devices can communicate with MODBUS/TCP devices through a gateway or a converter. MODBUS/TCP is widely used in industrial automation and control systems, as it offers high performance, interoperability, and compatibility with existing Modbus devices. References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 3.1.21; MODBUS Application Protocol Specification V1.1b3, Section 1.1