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.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

After receiving an approved patch from the JACS vendor, what is BEST practice for the asset owner to follow?

A. If a low priority, there is no need to apply the patch.

B. If a medium priority, schedule the installation within three months after receipt.

C. If a high priority, apply the patch at the first unscheduled outage.

D. If no problems are experienced with the current IACS, it is not necessary to apply the patch.

Correct Answer: C

According to the ISA/IEC 62443 Cybersecurity Fundamentals Specialist resources, patches are software updates that fix bugs, vulnerabilities, or improve performance of a system. Patches are classified into three categories based on their urgency and impact: low, medium, and high. Low priority patches are those that have minimal or no impact on the system functionality or security, and can be applied at the next scheduled maintenance. Medium priority patches are those that have moderate impact on the system functionality or security, and should be applied within a reasonable time frame, such as three months. High priority patches are those that have significant or criticalimpact on the system functionality or security, and should be applied as soon as possible, preferably at the first unscheduled outage. Applying patches in a timely manner is a best practice for maintaining the security and reliability of an industrial automation and control system (IACS). References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 4.3.2, Patch Management ISA/IEC 62443-2-1:2009, Security for industrial automation and control systems - Part 2-1: Establishing an industrial automation and control systems security program, Clause 5.3.2.2, Patch management ISA/IEC 62443-3-3:2013, Security for industrial automation and control systems - Part 3-3: System security requirements and security levels, Clause 4.3.3.6.2, Patch management

QUESTION 2

Using the risk matrix below, what is the risk of a medium likelihood event with high consequence?

		Consequence		
		High	Medium	Low
Likelihood	High	A	B	C
	Medium	B	C	D
	Low	C	D	D

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

According to the ISA/IEC 62443 Cybersecurity Fundamentals, the risk matrix is a tool used to assess the risk of a particular event. The risk matrix is divided into three categories: likelihood, consequence, and risk. The likelihood is the

probability that an event will occur, the consequence is the impact that the event will have, and the risk is the combination of the two. In this case, the risk of a medium likelihood event with high consequence is a high risk, as shown by the red

cell in the matrix. References:

ISA/IEC 62443 Cybersecurity Fundamentals

[ISA/IEC 62443 Cybersecurity Certificate Program] [Cybersecurity Library]

[Using the ISA/IEC 62443 Standard to Secure Your Control Systems]

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 of the following is an element of monitoring and improving a CSMS?

Available Choices (select all choices that are correct)

A. Increase in staff training and security awareness

B. Restricted access to the industrial control system to an as-needed basis

C. Significant changes in identified risk round in periodic reassessments

D. Review of system logs and other key data files

Correct Answer: ACD

According to the ISA/IEC 62443 Cybersecurity Fundamentals Specialist resources, a CSMS is a Cybersecurity Management System that defines the policies, procedures, and practices for managing the security of an industrial automation and control system (IACS). A CSMS should be monitored and improved continuously to ensure its effectiveness and alignment with the changing risk environment and business objectives. Some of the elements of monitoring and improving a CSMS are: Increase in staff training and security awareness: This element involves providing regular and updated training and awareness programs for the staff involved in the operation, maintenance, and security of the IACS. Training and awareness can help improve the skills, knowledge, and behavior of the staff, and reduce the likelihood and impact of human errors, negligence, or malicious actions. Training and awareness can also help foster a positive security culture and increase the staff\\'s engagement and commitment to the CSMS12 Significant changes in identified risk found in periodic reassessments: This element involves conducting periodic risk assessments to identify and evaluate the current and emerging threats, vulnerabilities, and consequences that may affect the IACS. Risk assessments can help determine the appropriate security levels (SLs) and security requirements for the system under control (SuC) and its components. Risk assessments can also help identify any gaps or weaknesses in the existing security measures and controls, and prioritize the actions for risk mitigation or acceptance. Periodic risk assessments can help ensure that the CSMS is responsive and adaptive to the changing risk landscape and business needs13 Review of system logs and other key data files: This element involves collecting, analyzing, and reviewing the system logs and other key data files that record the events and activities related to the IACS. System logs and data files can provide valuable information and insights for security monitoring, detection, response, and recovery. They can also help identify any anomalies, incidents, or breaches that may compromise the security or performance of the IACS. System logs and data files can also help measure and evaluate the effectiveness and efficiency of the CSMS and its processes, and provide feedback and recommendations for improvement14 References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 4.3, Cybersecurity Management System (CSMS) ISA/IEC 62443-2-1:2009, Security for industrial automation and control systems - Part 2-1: Establishing an industrial automation and control systems security program, Clause 5.3.2.1, Training and awareness ISA/IEC 62443-3-2:2020, Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design, Clause 4, Security risk assessment process ISA/IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, Clause 4.3.3.7, Audit and accountabilit

QUESTION 5

Which analysis method is MOST frequently used as an input to a security risk assessment?

Available Choices (select all choices that are correct)

A. Failure Mode and Effects Analysis

B. Job Safety Analysis(JSA)

C. Process Hazard Analysis (PHA)

D. System Safety Analysis(SSA)

Correct Answer: C

A Process Hazard Analysis (PHA) is a systematic and structured method of identifying and evaluating the potential hazards and risks associated with an industrial process. A PHA can help to identify the possible causes and consequences of undesired events, such as equipment failures, human errors, cyberattacks, natural disasters, etc. A

PHA can also provide recommendations for reducing the likelihood and severity of such events, as well as improving the safety and security of the process. A PHA is one of the most frequently used analysis methods as an input to a security risk assessment, as it can help to identify the assets, threats, vulnerabilities, and impacts related to the process, and provide a basis for determining the security risk level and the appropriate security countermeasures. A PHA is also a requirement of the ISA/IEC 62443 standard, as part of the security program development and implementation phase12. References: 1: ISA/IEC 62443-2-1: Security for industrial automation and control systems: Establishing an industrial automation and control systems security program 2: ISA/IEC 62443-3-2: Security for industrial automation and control systems: Security risk assessment for system design