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

The Risk Analysis category contains background information that is used where?

Available Choices (select all choices that are correct)

A. Many other elements in the CSMS

B. (Elements external to the CSMS

C. Only the Assessment element

D. Only the Risk ID element

Correct Answer: A

The Risk Analysis category contains background information that is used to identify and assess the risks associated with the cyber-physical system (CPS) under consideration. This information includes the system description, the threat model, the vulnerability analysis, the risk assessmentmethod, and the risk acceptance criteria. The Risk Analysis category is used as an input for many other elements in the CSMS, such as the Risk ID, Risk Reduction, Risk Acceptance, and Risk Monitoring elements. The Risk Analysis category provides the basis for the risk management process and helps to ensure a consistent and systematic approach to cybersecurity in the CPS. References: Using the ISA/IEC 62443 Standards to Secure Your Control System, page 13 [ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide], page 34

QUESTION 2

Which is a role of the application layer?

Available Choices (select all choices that are correct)

A. Includes protocols specific to network applications such as email, file transfer, and reading data registers in a PLC

B. Includes user applications specific to network applications such as email, file transfer, and reading data registers in a PLC

C. Provides the mechanism for opening, closing, and managing a session between end- user application processes D. Delivers and formats information, possibly with encryption and security

Correct Answer: A

The application layer is the topmost layer of the OSI model, which provides the interface between the user and the network. It includes protocols specific to network applications such as email, file transfer, and reading data registers in a PLC. These protocols deliver and format information, possibly with encryption and security, to ensure reliable and meaningful communication between differentapplications. The application layer does not include user applications, which are separate from the network protocols. The application layer also does not provide the mechanism for opening, closing, and managing a session between end-user application processes, which is the function of the session layer. References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, page 181 Using the ISA/IEC 62443 Standards to Secure Your Control System, page 82

QUESTION 3

What are the two sublayers of Layer 2?

Available Choices (select all choices that are correct)

A. HIDS and NIDS

B. LLC and MAC

C. OPC and DCOM

D. VLAN and VPN

Correct Answer: B

Layer 2 of the OSI model is the data link layer, which is responsible for transferring data frames between nodes on a network segment. The data link layer is divided into two sublayers: logical link control (LLC) and media access control (MAC). The LLC sublayer deals with issues common to both dedicated and broadcast links, such as framing, flow control, and error control. The MAC sublayer deals with issues specific to broadcast links, such as how to access the shared medium and avoid collisions. The LLC and MAC sublayers are not related to the ISA/IEC 62443 cybersecurity standards, which focus on the security of industrial automation and control systems (IACS). References:https://www.baeldung.com/cs/data-link-sub-layers https://bing.com/search?q=Layer+2+sublayers

QUESTION 4

Which of the following is the BEST reason for periodic audits?

Available Choices (select all choices that are correct)

A. To confirm audit procedures

B. To meet regulations

C. To validate that security policies and procedures are performing

D. To adhere to a published or approved schedule

Correct Answer: C

Periodic audits are an essential part of the ISA/IEC 62443 cybersecurity standards, as they help to verify the effectiveness and compliance of the security program. According to the ISA/IEC 62443-2-1 standard, periodic audits should be conducted to evaluate the following aspects1: The security policies and procedures are consistent with the security requirements and objectives of the organization The security policies and procedures are implemented and enforced in accordance with the security program The security policies and procedures are reviewed and updated regularly to reflect changes in the threat landscape, the IACS environment, and the business needs The security performance indicators and metrics are measured and reported to the relevant stakeholders The security incidents and vulnerabilities are identified, analyzed, and resolved in a timely manner The security awareness and training programs are effective and aligned with the security roles and responsibilities of the personnel The security audits and assessments are conducted by qualified and independent auditors The security audit and assessment results are documented and communicated to the appropriate parties The security audit and assessment findings and recommendations are addressed and implemented in a prioritized and systematic way Periodic audits are not only a means to meet regulations or adhere to a schedule, but also a way to validate that the security policies and procedures are performing as intended and achieving the desired security outcomes. Periodic audits also help to identify gaps and weaknesses in the security program and provide opportunities for improvement and enhancement. References: Periodic audits are an essential part of the ISA/IEC 62443 cybersecurity standards, as they help to verify the effectiveness and compliance of the security program. According to the ISA/IEC 62443-2-1 standard, periodic audits should be conducted

to evaluate the following aspects1: The security policies and procedures are consistent with the security requirements and objectives of the organization The security policies and procedures are implemented and enforced in accordance with the security program The security policies and procedures are reviewed and updated regularly to reflect changes in the threat landscape, the IACS environment, and the business needs The security performance indicators and metrics are measured and reported to the relevant stakeholders The security incidents and vulnerabilities are identified, analyzed, and resolved in a timely manner The security awareness and training programs are effective and aligned with the security roles and responsibilities of the personnel The security audits and assessments are conducted by qualified and independent auditors The security audit and assessment results are documented and communicated to the appropriate parties The security audit and assessment findings and recommendations are addressed and implemented in a prioritized and systematic way Periodic audits are not only a means to meet regulations or adhere to a schedule, but also a way to validate that the security policies and procedures are performing as intended and achieving the desired security outcomes. Periodic audits also help to identify gaps and weaknesses in the security program and provide opportunities for improvement and enhancement. References:

QUESTION 5

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.