Vendor:ISA

Exam Code:ISA-IEC-62443

Exam Name:ISA/IEC 62443 Cybersecurity Fundamentals Specialist

Version: Demo

QUESTION 1

Which is one of the PRIMARY goals of providing a framework addressing secure product development life-cycle requirements?

Available Choices (select all choices that are correct)

A. Aligned development process

B. Aligned needs of industrial users

C. Well-documented security policies and procedures

D. Defense-in-depth approach to designing

Correct Answer: A

One of the primary goals of providing a framework addressing secure product development life-cycle requirements is to ensure that the development process of industrial automation and control systems (IACS) products is aligned with the security objectives and requirements of the ISA/IEC 62443 series of standards. The framework defines a secure development life-cycle (SDL) that covers all the phases of product development, from security requirements definition, to secure design, implementation, verification, validation, defect management, patch management, and product end-of-life. The framework also provides guidance on how to document and demonstrate compliance with the SDL requirements, as well as how to assess the security performance of the products using security levels. By following the framework, product suppliers can improve the security of their products and reduce the risk of vulnerabilities and exploits that may compromise the safety, integrity, reliability, and security of IACS. References: ISA/IEC 62443-4-1:2018, Security for industrial automation and control systems - Part 4-1: Product security development life-cycle requirements1 ISA/IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components2

QUESTION 2

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 3

In an IACS system, a typical security conduit consists of which of the following assets?

Available Choices (select all choices that are correct)

A. Controllers, sensors, transmitters, and final control elements

B. Wiring, routers, switches, and network management devices

C. Ferrous, thickwall, and threaded conduit including raceways

D. Power lines, cabinet enclosures, and protective grounds

Correct Answer: B

A security conduit is a logical or physical grouping of communication channels connecting two or more zones that share common security requirements1. A zone is a grouping of systems and components based on their functional, logical, and physical relationship that share common security requirements1. Therefore, a security conduit consists of assets that enable or facilitate communication between zones, such as wiring, routers, switches, and network managementdevices. Controllers, sensors, transmitters, and final control elements are examples of assets that belong to a zone, not a conduit. Ferrous, thickwall, and threaded conduit including raceways are physical structures that may enclose or protect wiring, but they are not part of the communication channels themselves. Power lines, cabinet enclosures, and protective grounds are also not part of the communication channels, but rather provide power or protection to the assets in a zone or a conduit. References: 1: Key Concepts of ISA/IEC 62443: Zones and Security Levels | Dragos

---

QUESTION 4

What is a feature of an asymmetric key?

Available Choices (select all choices that are correct)

A. Uses a continuous stream

B. Uses different keys

C. Shares the same key OD.

D. Has lower network overhead

Correct Answer: B

An asymmetric key is a feature of asymmetric cryptography, also known as public-key cryptography, which is a method of encrypting and decrypting data using two differentkeys: a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret by the owner. The public key and the private key are mathematically related, but it is computationally infeasible to derive one from the other. Asymmetric cryptography can be used for various purposes, such as digital signatures, key exchange, and encryption. For example, if Alice wants to send a message to Bob, she can use Bob\\'s public key to encrypt the message, and only Bob can decrypt it using his private key. Alternatively, if Bob wants to prove that he is the author of a message, he can use his private key to sign the message, and anyone can verify it using his public key. Asymmetric cryptography has some advantages over symmetric cryptography, which uses the same key for both encryption and decryption. For instance, asymmetric cryptography does not require a secure channel to distribute the keys, and it can provide non-repudiation and authentication. However, asymmetric cryptography also has some drawbacks, such as higher computational complexity, larger key sizes, and higher network overhead. References: ISA/IEC 62443-3-3:2018, Section 4.2.3.6.1, Cryptography1 ISA/IEC 62443-4-2:2019, Section 4.2.3.6.1, Cryptography ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 5.3.1, Cryptography ISA/IEC 62443 Cybersecurity Fundamentals Specialist Exam Specification, Section 5.3.1, Cryptography

---

QUESTION 5

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 6

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

C. Process Hazard Analysis (PHA)

D. System Safety Analysis(SSA)

Correct Answer: C

A Process Hazard Analysis (PHA) is a systematic method of identifying and evaluating the potential hazards associated with an industrial process. A PHA can help to identify the sources of cyber threats, the consequences of cyber incidents, and the existing safeguards and mitigation measures. A PHA is most frequently used as an input to a security risk assessment because it provides a comprehensive and structured overview of the process and its risks, which can then be used to determine the security level targets and security countermeasures for the industrial automation and control system (IACS). A PHA can also help to align the security objectives with the safety objectives of the process, and to ensure that the security measures do not compromise the safety or operability of the process. References: ISA/IEC 62443 Standards to Secure Your Industrial Control System, page 10 Using the ISA/IEC 62443 Standard to Secure Your Control System, page 17

QUESTION 7

In which layer is the physical address assigned?

Available Choices (select all choices that are correct)

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 7

Correct Answer: B

According to the OSI model, the physical address is assigned in the layer 2, also known as the data link layer. The physical address is a unique identifier for each device on a network, such as a MAC address or a serial number. The data link layer is responsible for transferring data between adjacent nodes on a network, using the physical address to identify the source and destination of each frame. The data link layer also provides error detection and correction, flow control, and media access control. References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist Exam Prep, section 2.2; ISA/IEC 62443 Standards to Secure Your Industrial Control System, section 3.1.2.

QUESTION 8

Which statement is TRUE regarding Intrusion Detection Systems (IDS)?

Available Choices (select all choices that are correct)

A. Modern IDS recognize IACS devices by default.

B. They are very inexpensive to design and deploy.

C. They are effective against known vulnerabilities.

D. They require a small amount of care and feeding

Correct Answer: C

Intrusion detection systems (IDS) are tools that monitor network traffic and detect suspicious or malicious activity based on predefined rules or signatures. They are effective against known vulnerabilities, as they can alert the system administrators or security personnel when they encounter a match with a known attack pattern or behavior. However, IDS have some limitations and challenges, especially when applied to industrial automation and control systems (IACS). Some of these are: Modern IDS do not recognize IACS devices by default, as they are designed for general-purpose IT networks and protocols. Therefore, they may generate false positives or negatives when dealing with IACS-specific devices, protocols, or traffic patterns. To overcome this, IDS need to be customized or adapted to the IACS environment and context, which may require additional expertise and resources. They are not very inexpensive to design and deploy, as they require careful planning, configuration, testing, and maintenance. They also need to be integrated with other security tools and processes, such as firewalls, antivirus, patch management, incident response, etc.Moreover, they may introduce additional costs and risks, such as network performance degradation, data privacy issues, or legal liabilities. They are not effective against unknown or zero-day vulnerabilities, as they rely on predefined rules or signatures that may not cover all possible attack scenarios or techniques. Therefore, they may fail to detect novel or sophisticated attacks that exploit new or undiscovered vulnerabilities. To mitigate this, IDS need to be complemented with other security measures, such as anomaly detection, threat intelligence, or machine learning. They require a significant amount of care and feeding, as they need to be constantly updated, tuned, and monitored. They also generate a large amount of data and alerts, which may overwhelm the system administrators or security personnel. Therefore, they need to be supported by adequate tools and processes, such as data analysis, alert filtering, prioritization, correlation, or visualization. References: ISA/IEC 62443-2-1:2010 - Establishing an industrial automation and control system security program, ISA/IEC 62443-3-3:2013 - System security requirements and security levels, ISA/IEC 62443 Cybersecurity Fundamentals Specialist Training Course, [Enhancing Modbus/TCP-Based Industrial Automation and Control Systems Security Using Intrusion Detection Systems]

QUESTION 9

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

QUESTION 10

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

QUESTION 11

What type of security level defines what a component or system is capable of meeting?

Available Choices (select all choices that are correct)

A. Capability security level

B. Achieved security level

C. Design security level

D. Target security level

Correct Answer: A

According to the IEC 62443 standard, a capability security level (SL-C) is defined as "the security level that a component or system is capable of meeting when it is properly configured and protected by an appropriate set of security countermeasures" 1. A component or system can have different SL-Cs for different security requirements, depending on its design and implementation. The SL-C is determined by testing the component or system against a set of security test cases that correspond to the security requirements. The SL-C is not dependent on the actual operational environment or configuration of the component or system, but rather on its inherent capabilities. References: IEC 62443 - Wikipedia

---

QUESTION 12

Which characteristic is MOST closely associated with the deployment of a demilitarized zone (DMZ)?

Available Choices (select all choices that are correct)

A. Level 4 systems must use the DMZ to communicate with Level 3 and below.

B. Level 0 can only interact with Level 1 through the firewall.

C. Internet access through the firewall is allowed.

D. Email is prevented, thereby mitigating the risk of phishing attempts.

Correct Answer: A

According to the ISA/IEC 62443 standard, a demilitarized zone (DMZ) is a network segment that is logically between the internal and external networks, and its purpose is to enforce the internal network\\'s information assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from external attacks1. The standard also defines five levels of network segmentation, from Level 0 (process) to Level 4 (enterprise), and recommends that Level 4 systems must use the DMZ to communicate with Level 3 (site control) and below, as shown in the figure below2. This way, the DMZ acts as a buffer zone that prevents direct access from the internet to the industrial control systems (ICS) and allows only authorized traffic to pass through the firewalls. References: 1: demilitarized zone (DMZ) - Glossary | CSRC 2: Industrial DMZ Infrastructure - Siemens