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.certbus.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 2

What is the definition of "defense in depth" when referring to

Available Choices (select all choices that are correct)

A. Using countermeasures that have intrinsic technical depth.

B. Aligning all resources to provide a broad technical gauntlet

C. Requiring a minimum distance requirement between security assets

D. Applying multiple countermeasures in a layered or stepwise manner

Correct Answer: D

Defense in depth is a concept of cybersecurity that involves applying multiple layers of protection to a system or network, so that if one layer fails, another layer can prevent or mitigate an attack. Defense in depth is based on the principle that no single security measure is perfect or sufficient, and that multiple countermeasures can provide redundancy and diversity of defense. Defense in depth can also increase the cost and complexity for an attacker, as they have to overcome more obstacles and exploit more vulnerabilities to achieve their goals. Defense in depth is one of

the key concepts of the ISA/IEC 62443 series of standards, which provide guidance and best practices for securing industrial automation and control systems (IACS). The standards recommend applying defense in depth strategies at different levels of an IACS, such as the network, the system, the component, and the policy and procedure level. The standards also define different zones and conduits within an IACS, which are logical or physical groupings of assets that share common security requirements and risk levels. By applying defense in depth strategies to each zone and conduit, the security of the entire IACS can be improved. References: ISA/IEC 62443-1-1:2009, Security for industrial automation and control systems - Part 1-1: Terminology, concepts and models1 ISA/IEC 62443-3-3:2013, Security for industrial automation and control systems - Part 3-3: System security requirements and security levels2 ISA/IEC 62443-4-1:2018, Security for industrial automation and control systems - Part 4-1: Product security development life-cycle requirements3 ISA/IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components4

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

Which of the following PRIMARILY determines access privileges for user accounts?

Available Choices (select all choices that are correct)

A. Users\\' desire for ease of use

B. Authorization security policy

C. Common practice

D. Technical capability

Correct Answer: B

Authorization security policy is the primary factor that determines access privileges for user accounts. Authorization security policy is the function of specifying access rights or privileges to resources, which is related to general information security and computer security, and to access control in particular1. Authorization security policy defines who can access what resources, under what conditions, and for what purposes. Authorization security policy should be aligned with the business objectives and security requirements of the organization, and should be enforced by appropriate mechanisms and controls. Authorization security policy should also be reviewed and updated regularly to reflect changes in the environment, threats, and risks2. Authorization security policy is an essential part of the ISA/IEC 62443 standard, which provides a framework for securing industrial automation and control systems (IACS). The standard defines four security levels (SL) that represent the degree of protection against threats, and specifies the security capabilities that should be implemented for each SL. The standard also provides guidance on how to conduct a security risk assessment, how to define security zones and conduits, and how to apply security policies and procedures to the IACS environment34 . References:https://bing.com/search?q=authorization+security+policy https://learn.microsoft.com/enus/aspnet/core/security/authorization/policies?view=aspnetcore-7.0

QUESTION 5

Which of the following is a recommended default rule for IACS firewalls?

Available Choices (select all choices that are correct)

A. Allow all traffic by default.

B. Allow IACS devices to access the Internet.

C. Allow traffic directly from the IACS network to the enterprise network.

D. Block all traffic by default.

Correct Answer: D

A recommended default rule for IACS firewalls is to block all traffic by default, and then allow only the necessary and authorized traffic based on the security policy and the zone and conduit model. This is also known as the principle of least privilege, which means granting the minimum access required for a legitimate purpose. Blocking all traffic by default provides a higher level of security and reduces the attack surface of the IACS network. The other choices are not recommended default rules for IACS firewalls, as they may expose the IACS network to unnecessary risks. Allowing all traffic by default would defeat the purpose of a firewall, as it would not filter any malicious or unwanted traffic. Allowing IACS devices to access the Internet would expose them to potential cyber threats, such as malware, phishing, or denial-of-service attacks. Allowing traffic directly from the IACS network to the enterprise network would bypass the demilitarized zone (DMZ), which is a buffer zone that isolates the IACS network from the enterprise network and hosts services that need to communicate between them. References: ISA/IEC 62443 Standards to Secure Your Industrial Control System training course1 ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide2 Using the ISA/IEC 62443 Standard to Secure Your Control Systems3

QUESTION 6

How many security levels are in the ISASecure certification program?

Available Choices (select all choices that are correct)

A. 2

B. 3

C. 4

D. 5

Correct Answer: C

The ISASecure certification program is based on the ISA/IEC 62443 standards, which define four security levels (SL) for industrial automation and control systems (IACS). The security levels range from SL 1 to SL 4, with SL 1 being the lowest and SL 4 being the highest. Each security level represents a set of security requirements and countermeasures that can protect an IACS from a certain level of threat. The ISASecure certification program offers three types of product certifications: Component Security Assurance (CSA), IIoT Component Security Assurance (ICSA), and System Security Assurance (SSA). Each product certification has four security assurance levels (SAL) that correspond to the security levels defined in the ISA/IEC 62443 standards. The ISASecure certification program also offers two types of process certifications: Security Development Lifecycle Assurance (SDLA) and IACS Security Assurance (IACSSA). Each process certification has four certification levels that correspond to the security levels defined in the ISA/IEC 62443 standards. Therefore, the ISASecure certification program has four security levels for both product and process certifications. References: ISASecure - IEC 62443 Conformance Certification - Official Site1 Certifications - ISASecure2 ISA Security Compliance Institute3

QUESTION 7

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 8

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 9

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 10

What is defined as the hardware and software components of an IACS?

Available Choices (select all choices that are correct) A. COTS software and hardware

B. Electronic security

C. Control system

D. Cybersecuritv

Correct Answer: C

According to the ISA/IEC 62443-1-1 standard, an industrial automation and control system (IACS) is defined as a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an

industrial process. The hardware and software components of an IACS include the control system, which is the combination of control devices, networks, and applications that perform the control functions for the industrial process. The control

system may consist of various types of devices, such as distributed control systems (DCS), programmable logic controllers (PLC), supervisory control and data acquisition (SCADA) systems, human-machine interfaces (HMI), remote terminal

units (RTU), intelligent electronic devices (IED), sensors, actuators, and other field devices. The control system may also use commercial off-the-shelf (COTS) software and hardware, such as operating systems, databases, firewalls, routers,

switches, and servers, to support the control functions and communication.

References:

ISA/IEC 62443-1-1:2009, Security for industrial automation and control systems - Part 1-1: Terminology, concepts and models, Clause 3.2.11 ISA/IEC 62443-2-1:2010, Security for industrial automation and control systems - Part 2-1:

Establishing an industrial automation and control systems security program, Clause 3.2.12

QUESTION 11

Why is patch management more difficult for IACS than for business systems?

Available Choices (select all choices that are correct)

A. Overtime pay is required for technicians.

B. Many more approvals are required.

C. Patching a live automation system can create safety risks.

D. Business systems automatically update.

Correct Answer: C

Patch management is the process of applying software updates to fix security vulnerabilities, improve functionality, or enhance performance. Patch management is an essential part of cybersecurity, as unpatched systems can be exploited by

malicious actors. However, patch management for industrial automation and control systems (IACS) is more challenging than for business systems, because patching a live automation system can create safety risks. According to the ISA/IEC

62443 standards, patching an IACS may have the following potential impacts1:

Patching may introduce new vulnerabilities or errors that compromise the availability, integrity, or confidentiality of the IACS. Patching may affect the functionality or performance of the IACS, causing unexpected or undesired behavior, such

as process shutdowns, slowdowns, or failures.

Patching may require downtime or reduced operation of the IACS, which may affect production, quality, or profitability.

Patching may require additional resources, such as personnel, equipment, or testing facilities, which may not be readily available or affordable. Therefore, patch management for IACS requires careful planning, testing, and validation before

applying patches to the operational environment. The ISA/IEC 62443 standards provide guidance and best practices for patch management in the IACS environment, such as1:

Establishing a patch management program that defines roles, responsibilities, policies, and procedures for patching IACS components and systems. Identifying and prioritizing the IACS assets that need patching, based on their criticality,

vulnerability, and risk level.

Evaluating and verifying the patches for compatibility, functionality, and security before applying them to the IACS.

Implementing and documenting the patching process, including backup, recovery, and rollback procedures, in case of patch failure or adverse effects. Monitoring and auditing the patching activities and outcomes, and reporting any issues or

incidents.

References: 1: ISA TR62443-2-3 - Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment

QUESTION 12

Which of the following is the BEST example of detection-in-depth best practices?

Available Choices (select all choices that are correct)

A. Firewalls and unexpected protocols being used

B. IDS sensors deployed within multiple zones in the production environment

C. Role-based access control and unusual data transfer patterns

D. Role-based access control and VPNs

Correct Answer: D

Packet filter firewalls are the simplest type of firewalls that examine each incoming packet and compare its source, destination, and ports with a predefined set of rules. If the packet matches the rules, it is allowed to pass through the firewall; otherwise, it is blocked or dropped. Packet filter firewalls do not inspect the packet structure, sequence, or content beyond the header information. They also do not keep track of the relationships between packets in a session, which means they cannot detect attacks that span multiple packets or connections. Packet filter firewalls are fast and efficient, but they have limited security capabilities and cannot protect against application-layer attacks or sophisticated threats. References: ISA/IEC 62443-3-3:2018, Section 4.2.3.2.11; ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 5.2.12

QUESTION 13

Which of the following is a cause for the increase in attacks on IACS?

Available Choices (select all choices that are correct)

A. Use of proprietary communications protocols

B. The move away from commercial off the shelf (COTS) systems, protocols, and networks

C. Knowledge of exploits and tools readily available on the Internet

D. Fewer personnel with system knowledge having access to IACS

Correct Answer: C

One of the reasons for the increase in attacks on IACS is the availability of information and tools that can be used to exploit vulnerabilities in these systems. The Internet provides a platform for hackers, researchers, and activists to share their knowledge and techniques for compromising IACS. Some examples of such information and tools are: Stuxnet: A sophisticated malware that targeted the Iranian nuclear program in 2010. It exploited four zero-day vulnerabilities in Windows and Siemens software to infect and manipulate the programmable logic controllers (PLCs) that controlled the centrifuges. Stuxnet was widely analyzed and reported by the media and security experts, and its source code was leaked online1. Metasploit: A popular penetration testing framework that contains modules for exploiting various IACS components and protocols. For instance, Metasploit includes modules for attacking Modbus, DNP3, OPC, and Siemens S7 devices2. Shodan: A search engine that allows users to find devices connected to the Internet, such as webcams,

routers, printers, and IACS components. Shodan can reveal the location, model, firmware, and configuration of these devices, which can be used by attackers to identify potential targets and vulnerabilities3. ICS-CERT: A website that provides alerts, advisories, and reports on IACS security issues and incidents. ICS-CERT also publishes vulnerability notes and mitigation recommendations for various IACS products and vendors4. These sources of information and tools can be useful for legitimate purposes, such as security testing, research, and education, but they can also be misused by malicious actors who want to disrupt, damage, or steal from IACS. Therefore, IACS owners and operators should be aware of the threats and risks posed by the Internet and implement appropriate security measures to protect their systems. References:

QUESTION 14

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 15

What does the abbreviation CSMS round in ISA 62443-2-1 represent?

Available Choices (select all choices that are correct)

A. Control System Management System

B. Control System Monitoring System

C. Cyber Security Management System

D. Cyber Security Monitoring System

Correct Answer: C

The abbreviation CSMS stands for Cyber Security Management System in ISA 62443-2-1. This standard defines the elements necessary to establish a CSMS for industrial automation and control systems (IACS) and provides guidance on how to develop those elements123. A CSMS is a collection of policies, procedures, practices, and personnel that are responsible for ensuring the security of IACS throughout their lifecycle24. References: 1: ISA/IEC 62443 Series of Standards - ISA 2: ISA 62443-2-1 - Security for industrial automation and control systems, Part 2-1: Establishing an Industrial Automation and Control Systems Security Program | GlobalSpec 3: IEC 62443-2-1:2010 | IEC Webstore | cyber security, smart city 4: Structuring the ISA/IEC 62443 Standards - ISAGCA