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

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

QUESTION 3

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 4

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 5

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

Latest ISA-IEC-62443 Dumps | ISA-IEC-62443 Practice Test | ISA-IEC-62443 Exam Questions