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.pass4itsure.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

Which is a PRIMARY reason why network security is important in IACS environments?

Available Choices (select all choices that are correct)

A. PLCs are inherently unreliable.

B. PLCs are programmed using ladder logic.

C. PLCs use serial or Ethernet communications methods.

D. PLCs under cyber attack can have costly and dangerous impacts.

Correct Answer: D

Network security is important in IACS environments because PLCs, or programmable logic controllers, are devices that control physical processes and equipment in industrial settings. PLCs under cyber attack can have costly and dangerous impacts, such as disrupting production, damaging equipment, compromising safety, and harming the environment. Therefore, network security is essential to protect PLCs and other IACS components from unauthorized access, modification, or disruption. The other choices are not primary reasons why network security is important in IACS environments. PLCsare not inherently unreliable, but they can be affected by environmental factors, such as temperature, humidity, and electromagnetic interference. PLCs are programmed using ladder logic, which is a graphical programming language that resembles electrical schematics. PLCs use serial or Ethernet communications methods, depending on the type and age of the device, to communicate with other IACS components, such as human- machine interfaces (HMIs), supervisory control and data acquisition (SCADA) systems, and distributed control systems (DCSs). 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 2

Which of the following ISA-99 (IEC 62443) Reference Model levels is named correctly?

Available Choices (select all choices that are correct)

A. Level 1: Supervisory Control

B. Level 2: Quality Control

C. Level 3: Operations Management

D. Level 4: Process

Correct Answer: AC

The ISA-99 (IEC 62443) Reference Model levels are based on the Purdue Enterprise Reference Architecture (PERA) and describe how data flows through industrial networks. The levels are as follows1:

Level 0: The physical process, where the actual production or operation takes place.

Level 1: Basic control, where sensors and actuators monitor and manipulate the physical process.

Level 2: Supervisory control, where human-machine interfaces (HMIs) and controllers coordinate and optimize the basic control functions. Level 3: Operations management, where production scheduling, inventory management, quality

control, and other functions are performed. Level 4: Business planning and logistics, where enterprise resource planning (ERP), customer relationship management (CRM), and other business functions are performed.

Therefore, the correct names for level 1 and level 3 are supervisory control and operations management, respectively. Level 2 is not quality control, but supervisory control. Level 4 is not process, but business planning and logistics.

References: 1: Key Concepts of ISA/IEC 62443: Zones and Security Levels | Dragos

QUESTION 3

Which statement is TRUE reqardinq application of patches in an IACS environment?

Available Choices (select all choices that are correct)

A. Patches should be applied as soon as they are available.

B. Patches should be applied within one month of availability.

C. Patches never should be applied in an IACS environment.

D. Patches should be applied based on the organization\\'s risk assessment.

Correct Answer: D

Patches are software updates that fix bugs, vulnerabilities, or improve performance or functionality. Patches are important for maintaining the security and reliability of an IACS environment, but they also pose some challenges and risks. Applying patches in an IACS environment is not as simple as in an IT environment, because patches may affect the availability, integrity, or safety of the IACS. Therefore, patches should not be applied blindly or automatically, but based on the organization\\'s risk assessment. The risk assessment should consider the following factors: 1 The severity and likelihood of the vulnerability that the patch addresses The impact of the patch on the IACS functionality and performance The compatibility of the patch with the IACS components and configuration The availability of a backup or recovery plan in case the patch fails or causes problems The testing and validation of the patch before applying it to the production system The communication and coordination with the stakeholders involved in the patching process The documentation and auditing of the patching activities and results References: ISA TR62443-2-3 - Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment

QUESTION 4

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 5

Which layer in the Open Systems Interconnection (OSI) model would include the use of the File Transfer Protocol (FTP)?

Available Choices (select all choices that are correct)

A. Application layer

B. Data link layer

C. Session layer

D. Transport layer

Correct Answer: A

The File Transfer Protocol (FTP) is an application layer protocol that moves files between local and remote file systems. It runs on top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection. The control connection is used to send commands and responses between the client and the server, while the data connection is used to transfer the actual file. FTP is one of the standard communication protocols defined by the TCP/IP model and it does not fit neatly into the OSI model. However, since the OSI model is a reference model that describes the general functions of each layer, FTP can be considered as an application layer protocol in the OSI model, as it provides user services and interfaces to the network. The application layer is the highest layer in the OSI model and it is responsible for providing various network services to the users, such as email, web browsing, file transfer, remote login, etc. The application layer interacts with the presentation layer, which is responsible for data formatting, encryption, compression, etc. The presentation layer interacts with the session layer, which is responsible for establishing, maintaining, and terminating sessions between applications. The session layer interacts with the transport layer, which is responsible for reliable end-to-end data transfer and flow control. The transport layer interacts with the network layer, which is responsible for routing and addressing packets across different networks. The network layer interacts with the data link layer, which is responsible for framing, error detection, and medium access control. The data link layer interacts with the physical layer, which is responsible for transmitting and receiving bits over the physical medium. References: File Transfer Protocol (FTP) in Application Layer1 FTP Protocol2 What OSI layer is FTP?3

ISA-IEC-62443 PDF Dumps ISA-IEC-62443 VCE Dumps ISA-IEC-62443 Braindumps