ISA.ISA-IEC-62443.v2024-12-23.q58

Exam Code:	ISA-IEC-62443
Exam Name:	ISA/IEC 62443 Cybersecurity Fundamentals Specialist
Certification Provider:	ISA
Free Question Number:	58
Version:	v2024-12-23
# of views:	1723
# of Questions views:	580
https://www.freepdfdumps.com/ISA.ISA-IEC-62443.v2024-12-23.q58.html	

NEW QUESTION: 1
Which of the following is a recommended default rule for IACS firewalls?
Available Choices (select all choices that are correct)
A. Allow traffic directly from the IACS network to the enterprise network.
B. Allow IACS devices to access the Internet.
C. Allow all traffic by default.
D. Block all traffic by default.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which communications system covers a large geographic area?
Available Choices (select all choices that are correct)
A. Campus Area Network (CAN)
B. Local Area Network (LAN)
C. Storage Area Network
D. Wide Area Network (WAN)
Answer: D (LEAVE A REPLY)
A Wide Area Network (WAN) is a communications system that covers a large geographic area, such as a city, a country, or even several countries or continents1. WANs are often used to connect local area networks (LANs) and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations2. WANs use various communication infrastructures, such as public telephone lines, undersea cables, and communication satellites, to transmit data over long distances1. WANs are typically established with leased telecommunication circuits or less costly circuit switching or packet switching methods2. WANs are often built by Internet service providers, who provide connections from an organization's LAN to the Internet2.

The Internet itself may be considered a WAN2. References: Hardware and network technologies - CCEA LAN and WAN - BBC, Wide area network
- Wikipedia.

NEW QUESTION: 3
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
Answer: B (LEAVE A REPLY)
The best practice for detection-in-depth according to ISA/IEC 62443 involves layering different types of security controls that operate effectively under multiple scenarios and across various zones within an environment. IDS (Intrusion Detection Systems) sensors deployed across multiple zones within a production environment exemplify this strategy. By positioning sensors in various strategic locations, organizations can monitor for anomalous activities and potential threats throughout their network, thus enhancing their ability to detect and respond to incidents before they escalate. This deployment aligns with the ISA/IEC 62443 focus on comprehensive coverage and redundancy in cybersecurity mechanisms, contrasting with relying solely on perimeter defenses or single-point security solutions.

NEW QUESTION: 4
What type of security level defines what a component or system is capable of meeting?
Available Choices (select all choices that are correct)
A. Achieved security level
B. Capability security level
C. Design security level
D. Target security level
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
Which is the BEST deployment system for malicious code protection?
Available Choices (select all choices that are correct)
A. Network segmentation
B. IACS protocol converters
C. Application whitelistinq (AWL) OD.
D. Zones and conduits
Answer: C (LEAVE A REPLY)

Application whitelisting (AWL) is a technique that allows only authorized applications to run on a system, and blocks any unauthorized or malicious code from executing. AWL is one of the most effective methods for preventing malware infections and reducing the attack surface of a system. AWL can be implemented at different levels, such as the operating system, the network, or the application itself. AWL is especially useful forindustrial automation and control systems (IACS), which often run on legacy or proprietary platforms that are not compatible with traditional antivirus software or other security solutions. AWL can also help protect IACS from zero-day attacks, which exploit unknown vulnerabilities that have not been patched or detected by security vendors. AWL is recommended by the ISA/IEC 62443 standards as a key component of malicious code protection for IACS. According to the standards, AWL should be applied to all IACS components that support it, and should be configured and maintained according to the security policies and procedures of the organization. AWL should also be complemented by other security measures, such as network segmentation, zones and conduits, and patch management, to provide a defense-in-depth approach to IACS security. References:
* ISA/IEC 62443-3-3:2013, System security requirements and security levels, Section 5.2.3.41
* ISA/IEC 62443-2-1:2010, Establishing an industrial automation and control systems security program, Section 4.3.3.6.42
* ISA/IEC 62443-4-2:2019, Technical security requirements for IACS components, Section 4.2.3.43
* ISA/IEC 62443-3-2:2020, Security risk assessment for system design, Section 7.3.3.44
* ISA/IEC 62443-4-1:2018, Product development requirements, Section 5.2.3.45

NEW QUESTION: 6
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
Answer: (SHOW ANSWER)
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

NEW QUESTION: 7
Which of the following refers to internal rules that govern how an organization protects critical system
resources?
Available Choices (select all choices that are correct)
A. Formal guidance
B. Security policy
D- Code of conduct
C. Legislation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
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
Answer: A,D (LEAVE A REPLY)
Monitoring and improving a Cybersecurity Management System (CSMS) as per ISA/IEC 62443 standards involves several key activities that ensure the system remains effective and responsive to emerging threats.
Two critical elements of this ongoing process are:
* A. Increase in staff training and security awareness:Regular training and increasing security awareness among staff are vital to maintaining a secure operating environment. This proactive measure helps in reducing human error and enhancing the ability to respond effectively to cybersecurity incidents.
* D. Review of system logs and other key data files:Continuous review and analysis of system logs and other relevant data files are essential for detecting, investigating, and responding to potential security incidents. This monitoring helps in identifying anomalies that may indicate a security breach or operational issues needing attention.

NEW QUESTION: 9
What is a commonly used protocol for managing secure data transmission over a Virtual Private Network (VPN)?
Available Choices (select all choices that are correct)
A. HTTPS
B. IPSec
C. MPLS

D. SSH

Answer: B (LEAVE A REPLY)

IPSec is a commonly used protocol for managing secure data transmission over a VPN. IPSec stands for Internet Protocol Security and it is a set of standards that define how to encrypt and authenticate data packets that travel between two or more devices over an IP network. IPSec can operate in two modes: transport mode and tunnel mode. In transport mode, IPSec only encrypts the payload of the IP packet, leaving the header intact. In tunnel mode, IPSec encrypts the entire IP packet and encapsulates it in a new IP header. Tunnel mode is more secure and more suitable for VPNs, as it can protect the original source and destination addresses of the IP packet from eavesdropping or spoofing. IPSec uses two main protocols to provide security services: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides data integrity and source authentication, but not confidentiality. ESP provides data integrity, source authentication, and confidentiality. IPSec also uses two protocols to establish and manage security associations (SAs), which are the parameters and keys used for encryption and authentication: Internet Key Exchange (IKE) and Internet Security Association and Key Management Protocol (ISAKMP). IKE is a protocol that negotiates and exchanges cryptographic keys between two devices. ISAKMP is a protocol that defines the format and structure of the messages used for key exchange and SA management.

References:

* ISA/IEC 62443-3-3:2018, Section 4.2.3.7.1, VPN1
* ISA/IEC 62443-4-2:2019, Section 4.2.3.7.1, VPN
* ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 5.3.2, VPN
* ISA/IEC 62443 Cybersecurity Fundamentals Specialist Exam Specification, Section 5.3.2, VPN

NEW QUESTION: 10

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 based on the organization's risk assessment.

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

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 11

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

Available Choices (select all choices that are correct)

A. Aligning all resources to provide a broad technical gauntlet

B. Applying multiple countermeasures in a layered or stepwise manner

C. Requiring a minimum distance requirement between security assets

D. Using countermeasures that have intrinsic technical depth.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
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
Answer: B (LEAVE A REPLY)
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

NEW QUESTION: 13
Which of the following PRIMARILY determines access privileges for user accounts?
Available Choices (select all choices that are correct)
A. Authorization security policy
B. Technical capability
C. Users' desire for ease of use
D. Common practice
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
Which statement is TRUE regarding Intrusion Detection Systems (IDS)?
Available Choices (select all choices that are correct)
A. They are effective against known vulnerabilities.
B. Modern IDS recognize IACS devices by default.
C. They are very inexpensive to design and deploy.
D. They require a small amount of care and feeding
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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
Answer: A (LEAVE A REPLY)
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

orconfiguration of the component or system, but rather on its inherent capabilities.
References:
* IEC 62443 - Wikipedia

NEW QUESTION: 16
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
Answer: A,C (LEAVE A REPLY)
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:
* The increase in attacks on Industrial Automation and Control Systems (IACS) can be attributed to several factors, including: A.Use of proprietary communications protocols:These can pose security risks because they may not have been designed with security in mind and are often not as well-tested against security threats as more standard

protocols. C.Knowledge of exploits and tools readily available on the Internet:The availability of information about vulnerabilities and exploits on the internet has made it easier for attackers to target IACS.
* The other options, B and D, are incorrect because: B. The move towards commercial off-the-shelf (COTS) systems, protocols, and networks actually increases risk because these systems are more likely to be known and targeted by attackers, compared to proprietary systems which might benefit from security through obscurity. D. There is actually an increase in risk with more personnel with system knowledge because it enlarges the attack surface - each individual with system knowledge can potentially become a vector for an attack, either maliciously or accidentally.

NEW QUESTION: 17
Security Levels (SLs) are broken down into which three types?
Available Choices (select all choices that are correct)
A. SL-1, SL-2, and SL-3
B. Target.capability, and achieved
C. Target.capacity, and achieved
D. Target.capability, and availability
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
What is the FIRST step required in implementing ISO 27001?
Available Choices (select all choices that are correct)
A. Create a security management organization.
B. Implement strict security controls.
C. Perform a security risk assessment.
D. Define an information security policy.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
Multiuser accounts and shared passwords inherently carry which of the followinq risks?

Available Choices (select all choices that are correct)
A. Privilege escalation
B. Race conditions
C. Unauthorized access
D. Buffer overflow
Answer: (SHOW ANSWER)

NEW QUESTION: 20
What are the connections between security zones called?
Available Choices (select all choices that are correct)
A. Firewalls
B. Conduits
C. Pathways
D. Tunnels
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21
Safety management staff are stakeholders of what security program development?
Available Choices (select all choices that are correct)
A. CSMS
B. SPRP
C. CSA
D. ERM
Answer: A (LEAVE A REPLY)
Safety management staff are stakeholders of the CSMS, which stands for Cybersecurity Management System. The CSMS is a framework for managing the cybersecurity of industrial automation and control systems (IACS) based on the ISA/IEC 62443-2-1 standard1. The CSMS defines the objectives, policies, metrics, and governance for the overall ICS security program2. The CSMS also includes the processes for risk assessment, security design, implementation, monitoring, and improvement3. Safety management staff are involved in the CSMS development and implementation, as they are responsible for ensuring the safety of the IACS and the people, environment, and assets that depend on it. Safety management staff need to coordinate with the security management staff to align the safety and security requirements, identify and mitigate the safety risks arising from cyber threats, and monitor and respond to safety incidents caused by cyberattacks.
References:
* 1: ISA/IEC 62443-2-1: Establishing an Industrial Automation and Control Systems Security Program, ISA, 2010.
* 2: A Practical Approach to Adopting the IEC 62443 Standards - ISAGCA

* 3: ISA ISA-IEC-62443 ISA/IEC 62443 Cybersecurity Fundamentals Specialist Online Training - Exam4Training
* [4]: Using the ISA/IEC 62443 Standards to Secure Your Control System, ISA, 2018.

NEW QUESTION: 22
Which of the following is an element of monitoring and improving a CSMS?
Available Choices (select all choices that are correct)
A. Significant changes in identified risk round in periodic reassessments
B. Review of system logs and other key data files
C. Increase in staff training and security awareness
D. Restricted access to the industrial control system to an as-needed basis
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
Which of the following is the underlying protocol for Ethernet/IP?
Available Choices (select all choices that are correct)
A. Building Automation and Control Network (BACnet)
B. Common Industrial Protocol
C. Highway Addressable Remote Transducer (HART)
D. Object Linking and Embedding (OLE) for Process Control
Answer: (SHOW ANSWER)
Ethernet/IP is an industrial network protocol that adapts the Common Industrial Protocol (CIP) to standard Ethernet. CIP is an object-oriented protocol that provides a unified communication architecture for various industrial automation applications, such as control, safety, security, energy, synchronization and motion, information and network management. CIP defines a set of messages and services for interacting with devices and data on the network, as well as a set of device profiles for consistent implementation of automation functions across different products. Ethernet/IP uses the transport and control protocols of standard Ethernet, such as TCP/IP and IEEE 802.3, to define the features and functions for its lower layers. Ethernet/IP also uses UDP to transport I/O messages and supports various network topologies, such as star, linear, ring and wireless.
Ethernet/IP is one of the leading industrial protocols in the United States and is widely used in a range of industries, such as factory, hybrid and process. Ethernet/IP is managed by ODVA, Inc., a global trade and standards development organization. References:
* EtherNet/IP - Wikipedia
* EtherNet/IP | ODVA Technologies | Industrial Automation

NEW QUESTION: 24
Which of the following attacks relies on a human weakness to succeed?
Available Choices (select all choices that are correct)
A. Escalation-of-privileges

B. Phishing
C. Spoofing
D. Denial-of-service
Answer: (SHOW ANSWER)

NEW QUESTION: 25
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
Answer: (SHOW ANSWER)
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 assessment method, 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

NEW QUESTION: 26
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
Answer: (SHOW ANSWER)
The ISA-99/IEC 62443 standards for industrial automation and control systems security categorize network and system components into different levels based on their operational context. The correct name from the provided options for one of these levels is Level 3: Operations Management. This level typically encompasses systems that manage production control systems, including batch management, production scheduling, and overall factory operations. The other levels listed, such as Supervisory Control and Process, refer to different aspects of the system but are not named correctly in the options provided. Level 1 is correctly referred to as
"Basic Control," and Level 4 should be "Business Logistics" instead of "Process."

NEW QUESTION: 27
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
Answer: A (LEAVE A REPLY)
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

NEW QUESTION: 28
Which is a commonly used protocol for managing secure data transmission on the Internet?
Available Choices (select all choices that are correct)
A. Secure Sockets Layer
B. Datagram Transport Layer Security (DTLS)

C. Secure Telnet
D. Microsoft Point-to-Point Encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 29
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
Answer: (SHOW ANSWER)
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:

NEW QUESTION: 30
What.are the two elements of the risk analysis category of an IACS?
Available Choices (select all choices that are correct)
A. Business recovery and risk elimination or mitigation
B. Risk evaluation and risk identification
C. Business rationale and risk identification and classification
D. Business rationale and risk reduction and avoidance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
What is the FIRST step required in implementing ISO 27001?
Available Choices (select all choices that are correct)
A. Create a security management organization.
B. Define an information security policy.
C. Implement strict security controls.

D. Perform a security risk assessment.
Answer: D (LEAVE A REPLY)
The first step in implementing ISO 27001, an international standard for information security management systems (ISMS), is to perform a security risk assessment. This initial step is critical as it helps identify the organization's information assets that could be at risk, assess the vulnerabilities and threats to these assets, and evaluate their potential impacts. This risk assessment forms the foundation for defining appropriate security controls and measures tailored to the organization's specific needs. Starting with a risk assessment ensures that the security controls implemented are aligned with the actual risks the organization faces, making the ISMS more effective and targeted.ISA/IEC 62443 Cybersecurity Fundamentals References:
* Although ISO 27001 is not part of ISA/IEC 62443, it shares common principles in cybersecurity management by starting with a comprehensive understanding and assessment of security risks, which is a fundamental aspect in both standards for setting up effective security practices.

NEW QUESTION: 32
Which of the following is an activity that should trigger a review of the CSMS?
Available Choices (select all choices that are correct)
A. Security incident exposing previously unknown risk.
B. Budgeting
C. New technical controls
D. Organizational restructuring
Answer: A (LEAVE A REPLY)

NEW QUESTION: 33
What is OPC?
Available Choices (select all choices that are correct)
A. An open standard protocol for real-time field bus communication between automation technology devices

B. An open standard protocol for the communication of real-time data between devices from different manufacturers
C. An open standard serial communications protocol widely used in industrial manufacturing environments
D. A vendor-specific proprietary protocol for the communication of real-time plant data between control devices
Answer: B (LEAVE A REPLY)
OPC stands for Open Platform Communications, and it is a series of standards and specifications for industrial telecommunication based on Object Linking and Embedding (OLE) for process control. It allows the communication of real-time data between devices from different manufacturers using various data transportation technologies, such as Microsoft's OLE, COM, DCOM, .NET, XML, and TCP123. OPC is not a protocolitself, but rather a standardized approach for data connectivity supported by the OPC Foundation3. OPC is widely used in industrial automation and control systems, as well as other industries, to achieve interoperability and integration between different applications and devices3.
A is incorrect, because OPC is not a field bus protocol, but rather a standard for data exchange between devices that may use different field bus protocols, such as Modbus, Profibus, or Ethernet/IP2. C is incorrect, because OPC is not a serial communications protocol, but rather a standard that can use various data transportation technologies, including serial, Ethernet, or wireless2. D is incorrect, because OPC is not a vendor-specific proprietary protocol, but rather an open standard that can be implemented by any vendor or device that supports the OPC specifications3. References: 1: Open Platform Communications - Wikipedia 2: What is OPC Protocol - The Automization 3: What is OPC? - OPC Foundation

NEW QUESTION: 34
Which is the BEST practice when establishing security zones?
Available Choices (select all choices that are correct)
A. Security zones should contain assets that share common security requirements.
B. Security zones should align with physical network segments.
C. Assets within the same logical communication network should be in the same security zone.
D. All components in a large or complex system should be in the same security zone.
Answer: (SHOW ANSWER)
Security zones are logical groupings of assets that share common security requirements based on factors such as criticality, consequence, vulnerability, and threat. Security zones are used to apply the principle of defense in depth, which means creating multiple layers of protection to prevent or mitigate cyberattacks. By creating security zones, asset owners can isolate the most critical or sensitive assets from the less critical or sensitive ones, and apply different levels of security controls to each zone according to the risk assessment.

Security zones are not necessarily aligned with physical network segments, as assets within the same network may have different security requirements. For example, a network segment may contain both a safety instrumented system (SIS) and a human-machine interface (HMI), but the SIS has a higher security requirement than the HMI. Therefore, the SIS and the HMI should be in different security zones, even if they are in the same network segment. Similarly, assets within the same logical communication network may not have the same security requirements, and therefore should not be in the same security zone. For example, a logical communication network may span across multiple physical locations, such as a plant and a corporate office, but the assets in the plant may have higher security requirements than the assets in the office. Therefore, the assets in the plant and the office should be in different security zones, even if they are in the same logical communication network. Finally, all components in a large or complex system should not be in the same security zone, as this would create a single point of failure and expose the entire system to potential cyberattacks. Instead, the components should be divided into smaller and simpler security zones, based on their security requirements, and the communication between the zones should be controlled by conduits.
Conduits are logical or physical connections between security zones that allow data flow and access control.
Conduits should be designed to minimize the attack surface and the potential impact of cyberattacks, by applying security controls such as firewalls, encryption, authentication, and authorization. References:
* How to Define Zones and Conduits1
* Securing industrial networks: What is ISA/IEC 62443?2
* ISA/IEC 62443 Series of Standards3

NEW QUESTION: 35
What is the name of the missing layer in the Open Systems Interconnection (OSI) model shown below?

A. User
B. Transport
C. Control
D. Protocol
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
Which is the BEST deployment system for malicious code protection?
Available Choices (select all choices that are correct)
A. Network segmentation
B. Application whitelistinq (AWL) OD.
C. IACS protocol converters
D. Zones and conduits
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which factor drives the selection of countermeasures?
Available Choices (select all choices that are correct)
A. Foundational requirements
B. Output from a risk assessment
C. Security levels
D. System design
Answer: B (LEAVE A REPLY)
The selection of countermeasures is driven by the output from a risk assessment, which identifies the risks and their associated likelihood and consequences for each zone and conduit in the industrial automation and control system (IACS). The risk assessment also

determines the target security level (SL-T) for each zone and conduit, which represents the desired level of protection against the identified threats. The countermeasures are then selected based on the SL-T and the existing security level (SL-A) of the zone and conduit, as well as the cost and feasibility of implementation. The countermeasures should aim to reduce the risk to an acceptable level by increasing the SL-A to meet or exceed the SL-T. References: ISA/IEC 62443-3-2:2018 - Security risk assessment for system design, ISA/IEC 62443-3-3:2013 - System security requirements and security levels, ISA/IEC 62443 Cybersecurity Fundamentals Specialist Training Course

NEW QUESTION: 38
Which policies and procedures publication is titled Patch Manaqement in the IACS Environment?
Available Choices (select all choices that are correct)
A. ISA-TR62443-2-3
B. ISA-TR62443-1-4
C. ISA-62443-3-3
D. ISA-62443-4-2
Answer: (SHOW ANSWER)
ISA-TR62443-2-3 is the technical report that describes the requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program. Patch management is the process of applying software updates to fix vulnerabilities, bugs, or performance issues in the IACS components. Patch management is an essential part of maintaining the security and reliability of the IACS environment. The technical report provides guidance on how to establish a patch management policy, how to assess the impact and risk of patches, how to test and deploy patches, and how to monitor and audit the patch management process. References: 1, 2, 3

NEW QUESTION: 39
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. Well-documented security policies and procedures
B. Defense-in-depth approach to designing
C. Aligned development process
D. Aligned needs of industrial users
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
What is a feature of an asymmetric key?

Available Choices (select all choices that are correct)
A. Has lower network overhead
B. Uses different keys
C. Uses a continuous stream
D. Shares the same key OD.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
What are the four main categories for documents in the ISA-62443 (IEC 62443) series?
Available Choices (select all choices that are correct)
A. General. Policies and Procedures. System, and Component
B. End-User, Integrator, Vendor, and Regulator
C. Assessment. Mitigation. Documentation, and Maintenance
D. People. Processes. Technology, and Training
Answer: A (LEAVE A REPLY)
The ISA/IEC 62443 series of standards is organized into four main categories for documents, based on the topics and perspectives that they cover. These categories are: General, Policies and Procedures, System, and Component12.
* General: This category covers topics that are common to the entire series, such as terms, concepts, models, and overview of the standards1. For example, ISA/IEC 62443-1-1 defines the terminology, concepts, and models for industrial automation and control systems (IACS) security3.
* Policies and Procedures: This category focuses on methods and processes associated with IACS security, such as risk assessment, system design, security management, and security program development1. For example, ISA/IEC 62443-2-1 specifies the elements of an IACS security management system, which defines the policies, procedures, and practices to manage the security of IACS4.
* System: This category is about requirements at the system level, such as security levels, security zones, security lifecycle, and technical security requirements1. For example, ISA/IEC 62443-3-3 specifies the system security requirements and security levels for zones and conduits in an IACS5.
* Component: This category provides detailed requirements for IACS products, such as embedded devices, network devices, software applications, and host devices1. For example, ISA/IEC 62443-4-2 specifies the technical security requirements for IACS components, such as identification and authentication, access control, data integrity, and auditability.
The other options are not valid categories for documents in the ISA/IEC 62443 series of standards, as they either do not reflect the structure and scope of the standards, or they mix different aspects of IACS security that are covered by different categories. For example, end-user, integrator, vendor, and regulator are not categories for documents, but rather roles or stakeholders that are involved in IACS security. Assessment, mitigation,

documentation, and maintenance are not categories for documents, but rather activities or phases that are part of the IACS security lifecycle. People, processes, technology, and training are not categories for documents, but rather elements or dimensions that are essential for IACS security.
References:
* ISA/IEC 62443 Series of Standards - ISA1
* IEC 62443 - Wikipedia2
* ISA/IEC 62443-1-1: Concepts and models3
* ISA/IEC 62443-2-1: Security management system4
* ISA/IEC 62443-3-3: System security requirements and security levels5
* ISA/IEC 62443-4-2: Technical security requirements for IACS components

NEW QUESTION: 42
What are three possible entry points (pathways) that could be used for launching a cyber attack?
Available Choices (select all choices that are correct)
A. LAN, portable media, and wireless
B. LAN, WAN, and hard drive
C. LAN, portable media, and hard drives
D. LAN, power source, and wireless OD.
Answer: (SHOW ANSWER)

NEW QUESTION: 43
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.
Answer: C (LEAVE A REPLY)
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 critical impact 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

NEW QUESTION: 44
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.
Answer: A (LEAVE A REPLY)
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 & Scoring | Centraleyes4

NEW QUESTION: 45
Which of the following is an activity that should trigger a review of the CSMS?
Available Choices (select all choices that are correct)
A. Budgeting
B. New technical controls
C. Organizational restructuring
D. Security incident exposing previously unknown risk.
Answer: B,C,D (LEAVE A REPLY)
According to the ISA/IEC 62443-2-1 standard, a review of the CSMS should be triggered by any changes that affect the cybersecurity risk of the industrial automation and control system (IACS), such as new technical controls, organizational restructuring, or security incidents1. Budgeting is not a trigger for CSMS review, unless it impacts the cybersecurity risk level or the CSMS itself2. References: 1: ISA/IEC 62443-2-1:2010, Section 4.3.3.3 2: A Practical Approach to Adopting the IEC 62443 Standards, ISAGCA Blog3

NEW QUESTION: 46
Who must be included in a training and security awareness program?
Available Choices (select all choices that are correct)
A. Vendors and suppliers
B. Employees
C. All personnel
D. Temporary staff
Answer: (SHOW ANSWER)
Modbus over Ethernet, also known as Modbus/TCP, is a protocol that encapsulates the Modbus/RTU data string inside the data section of the TCP frame. It then sets up a client/server exchange between nodes, using TCP/IP addressing to establish connections1. This makes it easy to manage in a firewall, because the firewall can filter the traffic based on the source and destination IP addresses and the TCP port number. The default TCP port for Modbus/TCP is 502, but it can be changed if needed. Modbus/TCP does not use any other ports or protocols, so the firewall rules can be simple and specific. References:
* 8: Open Modbus/TCP Specification, RTA Automation, 2010.
* [9]: Modbus Application Protocol Specification V1.1b3, Modbus Organization, 2012.

NEW QUESTION: 47
Which of the following is the underlying protocol for Ethernet/IP?
Available Choices (select all choices that are correct)
A. Highway Addressable Remote Transducer (HART)
B. Object Linking and Embedding (OLE) for Process Control
C. Common Industrial Protocol
D. Building Automation and Control Network (BACnet)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
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
Answer: C (LEAVE A REPLY)
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

NEW QUESTION: 49
Which is the PRIMARY responsibility of the network layer of the Open Systems Interconnection (OSI)
model?
Available Choices (select all choices that are correct)
A. Gives transparent transfer of data between end users
B. Provides the rules for framing, converting electrical signals to data
C. Forwards packets, including routing through intermediate routers
D. Handles the physics of getting a message from one device to another
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which of the following is the BEST example of detection-in-depth best practices?
Available Choices (select all choices that are correct)
A. Role-based access control and VPNs
B. Firewalls and unexpected protocols being used
C. Role-based access control and unusual data transfer patterns
D. IDS sensors deployed within multiple zones in the production environment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
Security Levels (SLs) are broken down into which three types?
Available Choices (select all choices that are correct)
A. SL-1, SL-2, and SL-3
B. Target.capability, and achieved
C. Target.capability, and availability
D. Target.capacity, and achieved
Answer: (SHOW ANSWER)
Security Levels (SLs) are a way of expressing the security performance of an industrial automation and control system (IACS) or its components. SLs are broken down into three types: target, capability, and achieved1.
* Target SL is the level of security performance that is required for a system or component to protect against a specific threat scenario. The target SL is determined by conducting a risk assessment that considers the likelihood and impact of potential security incidents1.
* Capability SL is the level of security performance that a system or component can provide based on its design and implementation. The capability SL is determined by evaluating the security functions and features of the system or component against a set of security requirements1.

* Achieved SL is the level of security performance that a system or component actually provides in its operational environment. The achieved SL is determined by verifying that the system or component is properly installed, configured, maintained, and monitored1. References: ISA/IEC 62443 Standards to Secure Your Industrial Control System, page 3-4.

NEW QUESTION: 52
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 under consideration for future use.
B. They are used as normative references.
C. They are used as informative references.
D. They are not used.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
Using the risk matrix below, what is the risk of a medium likelihood event with high consequence?

		Consequence		
		High	Medium	Low
Likelihood	High	A	B	C
	Medium	B	C	D
		C	D	D

A. Option A
B. Option C
C. Option B
D. Option D
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
Which is a physical layer standard for serial communications between two or more devices?
Available Choices (select all choices that are correct)
A. RS235
B. RS432
C. RS232

D. RS435
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
Which communications system covers a large geographic area?
Available Choices (select all choices that are correct)
A. Storage Area Network
B. Campus Area Network (CAN)
C. Local Area Network (LAN)
D. Wide Area Network (WAN)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 56
Which is a common pitfall when initiating a CSMS program?
Available Choices (select all choices that are correct)
A. Organizational lack of communication
B. Insufficient documentation due to lack of good follow-up
C. Immediate jump into detailed risk assessment
D. Failure to relate to the mission of the organization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
Which of the following is an element of security policy, organization, and awareness?
Available Choices (select all choices that are correct)
A. Product development requirements
B. Staff training and security awareness
C. Technical requirement assessment
D. Penetration testing
Answer: B (LEAVE A REPLY)
According to the ISA/IEC 62443-2-1 standard, security policy, organization, and awareness is one of the four foundational requirements for an IACS security management system. It defines the "policies, procedures, and organizational structure necessary to support the security program" 1. One of the elements of this requirement is staff training and security awareness, which involves "providing appropriate security education and training to all personnel who have access to or are responsible for IACS components" 1. This element aims to ensure that the staff are aware of the security risks, policies, and procedures, and are able to perform their roles and responsibilities in a secure manner. Staff training and security awareness can include topics such as security principles, threats and vulnerabilities, incident response, password management, physical security, and social engineering 2. References:
* ISA/IEC 62443 Series of Standards - ISA

* Security of Industrial Automation and Control Systems - ISAGCA

NEW QUESTION: 58
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. Power lines, cabinet enclosures, and protective grounds
C. Wiring, routers, switches, and network management devices
D. Ferrous, thickwall, and threaded conduit including raceways
Answer: C (LEAVE A REPLY)