Isa

(IC34 ISA-IEC 62443 Cybersecurity Design Specialist)

IC34 ISA-IEC 62443 Cybersecurity Design Specialist

Total: **100 Questions**

Link:

MYEXAM.FR

Question: 1

Which protection strategy denies malware from entering an engineering workstation via a Universal Serial Bus (USB) port?

A. Whitelisting
B. Physical port blocking
C. Multifactor authentication
D. Logging off between sessions

Answer: B

Question: 2

What maturity level does a service provider have if the performance can be shown to be repeatable across the organization?

A. 1 – Initial
B. 2 – Managed
C. 3 – Defined
D. 4 – Improving

Answer: C

Question: 3

Which activities likely would be included in cybersecurity robustness testing?

A. Vulnerability scans and network storms
B. Vulnerability scans and packet captures
C. Vulnerability scans and antivirus scans
D. Network storms and verification of security settings

Answer: A

Question: 4

What is NOT a compensating countermeasure?

A. Insurance policy
B. External resource
C. Additional physical security measures
D. Enhanced personnel background checks

B. Need for IT to implement a VPN
C. Connections are Local Area Network (LAN) only
D. Lack of easy remote access to IACS

Answer: A

Question: 9

Which Foundational Requirement (FR) includes account management?

A. FR 1
B. FR2
C. FR3
D. FR4

Answer: A

Question: 10

What should a good risk assessment provide for the entire system as well as for each zone and conduit?

A. Gap assessment report
B. Highest risk consequences
C. System architecture diagrams
D. Conceptual design specification

Answer: B

Question: 11

Network segmentation and DMZs belong to which Foundational Requirement?

A. FR 3 - System integrity (SI)
B. FR 4 - Data confidentiality (DC)
C. FR 5 - Restricted Data Flow (RDF)
D. FR 7 - Resource availability (RA)

Answer: C

Question: 12

Who is accountable for the security of an IACS?

A. The asset owner
B. The product supplier
C. The integration provider
D. The maintenance provider

Answer: A

Question: 13

Which of the following should be installed as a best practice for protecting IACS devices?

A. A firewall with deep packet inspection capabilities
B. A firewall rule allowing unrestricted traffic on ports 0 through 65,535
C. Simple Network Management Protocol Version 1 (SNMPv1) with encryption enabled
D. An intrusion detection system (IDS) with rate limiting turned on

Answer: A

Question: 14

Which is a best practice for device hardening in an IACS?

A. Ignore vendor-specific security guidance.
B. Add network interfaces for ease of maintenance.
C. Enable Hypertext Transfer Protocol (HTTP) access on port 80.
D. Disable remote program changes on programmable logic controllers (PLCs).

Answer: D

Question: 15

Which statement is TRUE with regards to network segments?

A. There cannot be a router inside a zone.
B. All assets have a different Subnet mask.
C. A DMZ is a three-tier network segmentation.
D. There can only be one (1) segment per zone.

Answer: C

D. An employee training program

Answer: B

Question: 20

What are the key considerations for features and capabilities during selection of the correct IACS firewall technology?

A. Type, class, software/firmware installation, and security
B. Type, size, space, and ventilation
C. Type, policy, ports, and connectivity
D. Type, class, intrusion detection system (IDS), and virtual private network (VPN)

Answer: A

Question: 21

What is a key feature of the delay perimeter's countermeasures?

A. Digital surveillance
B. Honey Pot systems
C. Biometric verification
D. Manned security gates

Answer: D

Question: 22

Which safety requirement (SR) is used in FR 7 - Resource Availability?

A. Emergency power
B. Resource management
C. Control system recovery
D. Denial of service protection

Answer: B

Question: 23

What are the two main types of firewalls?

A. Network and host-based
B. Network and packet filter
C. Defense-in-depth and host-based
D. Demilitarized zone (DMZ) and perimeter

Answer: A

Question: 24

In which part of the standard will the system requirements (SR) of a zone be found?

A. ISA/IEC 62443-2-1
B. ISA/IEC 62443-3-2
C. ISA/IEC 62443-3-3
D. ISA/IEC 62443-4-2

Answer: C

Question: 25

Which is a best-practice approach to access control?

A. Employ multiple authentication methods.
B. Configure databases in active/passive clusters.
C. Centralize IACS resources into one virtual local area network (VLAN).
D. Set up demilitarized zone (DMZ) resources on non-routable Internet Protocol (IP) space.

Answer: A

Question: 26

What is the main purpose of a demilitarized zone (DMZ) in network architecture?

A. To prevent direct communication between the enterprise network and email servers
B. To prevent direct communication between the enterprise network and the process control network
C. To prevent direct communication between the enterprise network and to route unclassified military data
D. To prevent access to the developmental network and to quarantine suspicious network traffic

Answer: B


7
Application
6
Presentation
5
Session
3
Network
2
Data Link
1
Physical

A. Control

B. Protocol
C. Transport
D. User

Answer: C

Question: 29

Which organization provides guidance on configuring remote access for industrial control systems?

A. North American Electric Reliability Corporation (NERC)
B. Center for the Protection of National Infrastructure
C. Public Safety Canada
D. All of the above

Answer: D

Question: 30

What BEST describes the use of Self-Signed Certificates?

A. Validating the quality of the service
B. Bypassing the security requirements
C. Creating ease of use in an enterprise
D. Using a printed badge instead of an official passport

Answer: D