Isa

(ISA-IEC 62443 Cybersecurity Maintenance Specialist)

ISA-IEC 62443 Cybersecurity Maintenance Specialist

Total: **100 Questions**

Link:

MYEXAM.FR

Question: 1

What should be included in the forensics portion of an incident response plan?

A. A high-level risk assessment
B. The recommended forensic tool vendor list
C. The designated point of contact for outside media
D. Directives to consider the skill level of personnel who accessed the system

Answer: D

Question: 2

Which is a characteristic of incident response planning policies and procedures?

A. Virtual
B. Colorful
C. Detailed
D. Password-protected

Answer: C

Question: 3

Which statement BEST describes the Four “Ts” of Managing Risk?

A. A set of rules to ensure risks are always insured
B. A framework to increase risk exposure for testing
C. A mandate to eliminate all organizational risk entirely
D. A set of techniques to accept, pass, stop, or reduce risk

Answer: D

Question: 4

Which should be performed during post-incident analysis and forensics?

A. Network traffic capture
B. High-level gap assessment
C. Active vulnerability testing
D. Penetration testing

B. Containment
C. Incident detection
D. Recovery and restoration

Answer: D

Question: 9

Why should IACS security NOT be considered or treated as a project?

A. External regulators cannot perform inspections.
B. Too many parties are involved in cybersecurity to define a proper project.
C. Cybersecurity is a continuously ongoing activity without a specific end-date.
D. New budget requests must be made after each cybersecurity risk assessment.

Answer: C

Question: 10

What is one of the common abilities of HIDS systems?

A. Log analysis
B. Data encryption
C. User authentication
D. Network speed testing

Answer: A

Question: 11

Which is a key topic regarding incident response plans?

A. Incident analysis
B. Zone and conduit diagrams
C. High-level risk assessment
D. Vendor selection

Answer: A

Question: 12

What is a characteristic of site-to-site VPNs?

A. They connect individual user devices to networks.
B. They pass traffic between two trusted networks.
C. They do not require encryption.
D. They are only used for local area networks.

Answer: B

Question: 13

The person who plans and implements a change performs which role in change management?

A. Customer
B. Project manager
C. Change committee
D. Change builder

Answer: D

Question: 14

Which is a key activity in the observation phase of incident management?

A. Observing disaster recovery drills
B. Watching operating system logs for process control errors
C. Watching intrusion detection system (IDS) logs
D. Suggesting revisions to key performance indicators (KPIs) reported to a process historian

Answer: C

Question: 15

Which statement about Snort is true?

A. Snort can be used with Modbus.
B. Snort can be used only with Modbus.
C. Snort can be installed only on Windows 7.
D. Snort is a proprietary intrusion alerting system.

Answer: A

Question: 16

What type of environments does the MITRE ATT&CK framework aim to be applicable to?

A. Isolated test labs
B. Academic institutions
C. Real-world environments
D. Only government networks

Answer: C

Question: 17

Within a change management process, which should be a Change Builder activity?

A. Verify change.
B. Request change.
C. Analyze change impact.
D. Determine costs and benefits.

Answer: A

Question: 18

What is the MAIN goal of change management?

A. To satisfy corporate guidelines
B. To create documentation compliant with ISO 9000
C. To support the processing and traceability of changes to a system
D. To facilitate development of accurate user guides

Answer: C

Question: 19

Which phase includes cybersecurity maintenance, monitoring, and management of change?

A. Assess phase
B. Develop and implement phase
C. Maintain phase
D. Decommissioning phase

Answer: C

Question: 20

In the incident response lifecycle, the step of detection is immediately followed by which step?

A. Remediation
B. Containment
C. Designing countermeasures
D. Post-incident analysis/forensics

Answer: B

Question: 21

Which is a critical step in forensic analysis?

A. Initiate fast responses to incidents.
B. Quickly clean and reinstall the machines/assets.
C. Investigate in an ad hoc fashion because that is how the advanced persistent threat (APT) operates.
D. Investigate the absentee list.

Answer: A

Question: 22

Which of the following is NOT a required attribute for software documentation?

A. License expiration date
B. Function
C. Ease of use
D. Vendor

Answer: C

Question: 23

What is the PRIMARY function of remote access VPNs?

A. To eliminate the need for firewalls

Which is an example of unnecessary software/services removed to harden a system?

A. The operating system
B. Instant messaging services
C. Intrusion detection software
D. Whitelisting software

Answer: B

Question: 28

Which is a centralized identity and access management tool?

A. Web server
B. File Transfer Protocol (FTP) server
C. Remote Authentication Dial-In User Service (RADIUS) server
D. Oracle database

Answer: C

Question: 29

What does the term automation solution refer to in the context of IACS?

A. The policies and procedures necessary to support IACS
B. An integrated set of devices and software applications
C. The realization of a control system at a particular facility
D. The organization accountable for the IACS

Answer: B

Question: 30

A log-based intrusion detection system (LIDS) is often part of the:

A. IACS firewall.
B. IACS software package.
C. Security information and event management (SIEM) system.
D. Programmable logic controller (PLC) or distributed control system (DCS) controller.

Answer: C