Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

ISA-IEC-62443-IC34M MCQs
ISA-IEC-62443-IC34M Exam Questions
ISA-IEC-62443-IC34M Practice Test
ISA-IEC-62443-IC34M TestPrep
ISA-IEC-62443-IC34M Study Guide

killexams.com

ISA

ISA-IEC-62443-IC34M

IACS Cybersecurity Design & Implementation (IC34) (Certificate 3)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/ISA-IEC-62443-IC34M

Question: 1471

Which best practices should be included in a hardening guide for a cloud-based service?

A. Enabling multi-factor authentication
B. Using public access for all services
C. Regularly reviewing access logs
D. Configuring security groups and firewalls

Answer: A,C,D

Explanation: Best practices for a cloud-based service hardening guide include enabling multi-factor authentication, regularly reviewing access logs, and configuring security groups and firewalls. Using public access for all services poses a security risk.

Question: 1472

When identifying Systems under Control (SuCs), which of the following should be considered first?

A. The age of the technology
B. The criticality of the system to operations
C. The budget available for cybersecurity
D. The number of users accessing the system

Answer: B

Explanation: The criticality of the system to operations should be considered first when identifying Systems under Control (SuCs), as it directly impacts the prioritization of cybersecurity efforts.

Question: 1473

In assessing supplier CRS, which of the following should be evaluated to ensure effective risk management?

A. The supplier's financial stability
B. The supplier's incident response capabilities
C. The number of employees in the supplier's organization
D. The supplier's compliance with industry standards

Answer: B,D

Explanation: Evaluating the supplier's incident response capabilities and compliance with industry standards are critical for ensuring effective risk management in supplier CRS, while financial stability and employee count are secondary considerations.

Question: 1474

What is the primary objective of implementing a Cybersecurity Risk Strategy for products?

A. To mitigate vulnerabilities in the product lifecycle
B. To enhance product sales
C. To reduce production costs
D. To comply with environmental regulations

Answer: A

Explanation: The primary objective of implementing a Cybersecurity Risk Strategy for products is to mitigate vulnerabilities throughout the product lifecycle, ensuring ongoing security from development through deployment and maintenance.

Question: 1475

In the context of maintaining system integrity, which SRs should be implemented to protect against malware threats?

A. SR 3.5
B. SR 4.4
C. SR 2.8
D. SR 1.7

Answer: A,B

Explanation: SR 3.5 emphasizes secure software practices to mitigate malware risks, while SR 4.4 focuses on ensuring that systems are monitored for malware activity.

Question: 1476

For a 2025 rail signaling SuC, serial trainline interfaces use RS-422 with Ethernet gateways, prone to ground loops crossing physical boundaries. ISA/IEC 62443-3-2 requires what isolation technique?

A. Install opto-isolators with 2500V rating and common-mode rejection filters.
B. Configure 'galvanic barrier' modules and separate power domains per zone.
C. Deploy balanced differential drivers with 100-ohm termination networks.
D. Use twisted shielded pairs with drain wire grounded at receiving end only.

Answer: B

Explanation: ISA/IEC 62443-3-2 physical partitioning includes galvanic isolation; barrier modules eliminate ground potentials in serial-Ethernet conduits, preventing faults in the SuC scope for safety-critical rail applications.

Question: 1477

Aerospace ground support IACS (ISA/IEC 62443-3-3), SL-T = 3 for telemetry conduit. Validation?

A. Replay attack on ARINC 429 bus using custom FPGA replay, verifying sequence number mismatch drop.
B. Cryptographic test: Decrypt sample packet with wrong key, confirming padding oracle avoidance.
C. Incident drill: Simulate breach, measuring response time from alert to isolation <15 min.
D. Metric calc: SL-A = (FR1 score 3 + FR2 2)/7 = 2.7 ≥3? No, apply compensation.

Answer: A, B, C

Explanation: Replay verifies sequence SR 4.4; key test upholds crypto FR 3; drill tests response FR 4, with metric adjustment for SL-A.

Question: 1478

What is the most effective way to ensure that all integrated systems adhere to cybersecurity best practices?

A. Establish a continuous monitoring and improvement process
B. Implement a single oversight committee

C. Conduct annual audits only
D. Rely on third-party assessments

Answer: A

Explanation: Establishing a continuous monitoring and improvement process is the most effective way to ensure adherence to cybersecurity best practices, as it allows for ongoing evaluation and adjustment to emerging threats and vulnerabilities.

Question: 1479

A company is reviewing its patch management policy and wants to improve response times to vulnerabilities. Which strategies should be considered?

A. Implementing a risk-based prioritization approach
B. Increasing the frequency of vulnerability scans
C. Establishing a dedicated patch management team
D. Automating the patch deployment process

Answer: A,B,C,D

Explanation: A risk-based prioritization approach helps focus on the most critical vulnerabilities, increasing the frequency of scans identifies issues sooner, establishing a dedicated team ensures accountability, and automating deployment can significantly reduce response times.

Question: 1480

In a scenario where a system is compromised due to a third-party component, what is the best course of action to improve future CRS for suppliers?

A. Increase penalties for non-compliance
B. Conduct more frequent audits of all suppliers
C. Enhance supplier selection criteria based on security
D. Implement a zero-trust architecture immediately

Answer: C

Explanation: Enhancing supplier selection criteria based on security will help ensure that future suppliers are vetted for their cybersecurity practices, reducing the risk of similar

incidents occurring again.

Question: 1481

Scenario: Cement kiln control faces jamming attacks. FR 3 SL-C (1) mapping to SR 3.1; basic params?

A. Checksum validation on packets
B. Signed EtherNet/IP messages
C. Timeout on stalled sessions
D. Unencrypted broadcasts

Answer: A, C

Explanation: SR 3.1 baseline includes CRC checks and 30s timeouts, protecting basic integrity without advanced signing in SL 1 per tables.

Question: 1482

An automotive plant's robot cell IACS detects beaconing to C2 via ROS topics at T+10min. Playbook's analysis phase mandates what YARA rule deployment for topic payloads?

A. YARA: strings $c2 = /ros_topic:\s*malicious\.com/; condition: $c2 in (filesize <1MB).
B. rule ROS_Beacon { strings: $beacon = { 52 4F 53 5F 43 32 }; condition: $beacon and uint32(0) == 0xdeadbeef }.
C. Deploy rule { meta: description="ROS C2"; strings: $s1 = "POST /beacon"; condition: all of them and pe.imphash() == known }.
D. Sigma rule to Splunk: title: ROS Beaconing; detection: event.code=ros_publish AND dest_ip external.

Answer: B

Explanation: YARA rules for custom protocols like ROS target beacons, aligning with SR 6.2-3 malware detection, for playbook-based threat hunting.

Question: 1483

Cement kiln control verifies FR 1 SL-T=4. Conduit 13 SR 1.5 (Auth revocation).

Mappings?

A. OCSP responder configs for real-time cert revocation checks.
B. Revocation drill report, propagating CRL updates in <1 minute across 100 nodes.
C. Kiln temperature profiles.
D. Clinker grind fineness.

Answer: A, B

Explanation: OCSP configs enable timely revocation. Drill report verifies propagation.

Question: 1484

In the context of cybersecurity, what does "SL-T" represent?

A. Security Level Threshold
B. Security Level Test
C. Security Level Target
D. Security Level Transmission

Answer: C

Explanation: SL-T stands for Security Level Target, which indicates the desired security level that a system should achieve to be considered compliant with cybersecurity requirements.

Question: 1485

In a scenario where an organization uses DNP3 for communication, which of the following actions should be taken to secure the protocol?

A. Implementing encryption for DNP3 messages
B. Allowing DNP3 traffic from any source
C. Monitoring DNP3 traffic for unusual patterns
D. Restricting DNP3 access to known devices only

Answer: A,C,D

Explanation: Implementing encryption, monitoring traffic, and restricting access to known devices are critical for securing DNP3. Allowing traffic from any source increases

vulnerability.

Question: 1486

A cybersecurity team is tasked with integrating a new system into an existing infrastructure. What is a critical consideration for ensuring compliance with ISA/IEC 62443?

A. The aesthetic design of the new system
B. The compatibility of the new system with legacy systems
C. The cost of the new system
D. The marketing strategy for the new system

Answer: B

Explanation: Ensuring compatibility of the new system with legacy systems is critical for compliance, as it helps maintain security across the infrastructure and prevents potential vulnerabilities during integration.

Question: 1487

Scenario: A data center's 2025 BMS uses conduit diagrams for BACnet/IP to chillers amid quantum threats. Which configurations update trust for post-quantum?

A. BACnet secure transport with Kyber-1024 key exchange in conduits
B. Legacy BACnet without encryption for device discovery
C. Diagrams with conduit annotations for NIST PQC migration paths
D. Implicit trust for Who-Is/I-Am services without cert pinning

Answer: A, C

Explanation: Kyber PQC secures BACnet against quantum, with migration annotations guiding updates; legacy and implicit services remain vulnerable.

Question: 1488

What is a critical factor to consider when developing a verification and validation plan?

A. The number of personnel available for testing

B. The timeline for project completion
C. The specific security requirements being validated
D. The historical context of previous validations

Answer: C

Explanation: The specific security requirements being validated are a critical factor to consider when developing a verification and validation plan. This ensures that the plan is focused and relevant to the security needs of the system.

Question: 1489

Semiconductor fab verifies FR 6 SL-T=3 in Conduit 10. SR 6.2 (Monitoring). Mappings?

A. Nagios config files for threshold alerts (e.g., CPU>90% triggers page).
B. Trend analysis report from Zabbix, detecting anomalies in wafer etcher traffic.
C. Wafer defect maps.
D. Etch rate metrics.

Answer: A, B

Explanation: Nagios configs enable proactive monitoring. Zabbix report shows event detection.

Question: 1490

In a petrochemical plant's OT network, a legacy Windows Server 2019 HMI system running SCADA software experiences anomalous process control signals during a simulated cyber-physical attack. To harden the host against unauthorized code execution per CIS Benchmark Level 2 for Windows Server 2019 (v1.2.1, updated 2025), the cybersecurity specialist must configure a Group Policy Object (GPO) to enforce code signing requirements. Which command, executed via PowerShell in an elevated session, correctly applies this hardening by enabling strict code integrity for kernel-mode drivers and user-mode binaries?
A. New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\CI\Policy" -Name "VerifiedAndReputablePolicyState" -Value 1 -PropertyType DWord; Restart-Computer
B. Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\CI\Policy" -Name "Option" -Value 1; Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\CI\Policy" -Name "PolicyVerificationFlags" -Value 3; Restart-Computer

C. Set-MpPreference -EnableControlledFolderAccess Enabled; Set-MpPreference -AttackSurfaceReductionRules_Ids "56a863a9-875e-4185-98a7-b882c64b5ce5" -AttackSurfaceReductionRules_Actions 1
D. Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value 1; Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "ConsentPromptBehaviorAdmin" -Value 2

Answer: B

Explanation: The command in option D configures Windows Code Integrity (CI) policy via registry keys to enforce strict code signing, requiring all kernel-mode drivers and user-mode executables to be digitally signed by trusted authorities, aligning with CIS Benchmark 18.9.8.1 (Ensure 'Code Integrity' is set to 'Enabled') for Level 2 hardening in OT environments. This prevents unsigned or tampered code from executing, mitigating risks like the anomalous signals observed, while the restart ensures policy application without disrupting HMI functionality if staged during maintenance.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.