Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.

ISA-IEC-62443-IC37M Practice Questions
ISA-IEC-62443-IC37M Practice Test
ISA-IEC-62443-IC37M Practice Exam
ISA-IEC-62443-IC37M Exam Questions
ISA-IEC-62443-IC37M Study Guide

killexams.com

ISA

ISA-IEC-62443-IC37M

ISA/IEC 62443 Cybersecurity Maintenance Specialist (Certificate 4) (IC37)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/ISA-IEC-62443-IC37M

Question: 1221

You are tasked with monitoring the effectiveness of the IACS security program. Which of the following should be your primary focus?

A. The amount of budget allocated to cybersecurity
B. The number of systems connected to the network
C. The frequency of security audits
D. Employee compliance with security protocols

Answer: D

Explanation: Employee compliance with security protocols should be the primary focus, as it directly impacts the effectiveness of the IACS security program.

Question: 1222

When the Product Supplier provides technical support to resolve a cybersecurity issue found during maintenance, which of the following should be included?

A. Root cause analysis and mitigation recommendations
B. Immediate deployment of fixes without Asset Owner notification
C. Updated security advisories and patch release notes
D. Post-implementation validation guidelines

Answer: A,C,D

Explanation: Root cause analysis, advisories, and validation guidelines ensure effective issue resolution. Immediate deployment without notification is not consistent with collaboration best practices.

Question: 1223

In ISA/IEC 62443 secure maintenance, how should maintenance zone boundaries be defined and protected?

A. Establish firewalls enforcing strict policies on maintenance conduits
B. Permit all inbound traffic for ease of maintenance troubleshooting
C. Use network segmentation to isolate maintenance devices from production
D. Disable intrusion detection systems in maintenance zones to avoid interference

Answer: A,C

Explanation: Firewalls and segmentation maintain zone integrity. Permitting all traffic and disabling IDS undermine security.

Question: 1224

Which of the following should be included in an incident response plan to address potential cybersecurity incidents effectively?

A. A list of all software applications used
B. Procedures for communication and escalation
C. A detailed inventory of hardware assets
D. Employee performance metrics

Answer: B

Explanation: Procedures for communication and escalation should be included in an incident response plan to address potential cybersecurity incidents effectively. Clear communication channels are vital for coordinated responses.

Question: 1225

In a scenario where a new vulnerability is discovered in a control system component, what are key steps to maintain cybersecurity during maintenance?

A. Immediately removing and isolating the affected component without consulting the asset owner
B. Implementing compensating controls to reduce risk while permanent fixes are evaluated
C. Maintaining detailed change logs including the reason for mitigation and timelines
D. Communicating the vulnerability status and risk acceptance to asset owners and stakeholders

Answer: B,C,D

Explanation: Isolating without consultation may disrupt processes. Compensating controls reduce immediate risk. Detailed logs support compliance and auditability. Transparent communication ensures informed risk management by owners.

Question: 1226

Baseline script for EtherCAT frame errors in robotics IACS per 62443-3-1, using R with ggplot for 10-day plot, excluding errors <1%?

A. library(ggplot2); df <- read.csv("ecat_errors.csv"); df$date <- as.Date(df$date); baseline <- df[df$error_rate < 0.01,]; ggplot(baseline, aes(date, error_rate)) + geom_line() + labs(title="10d Baseline")
B. errors <- read.csv("robot_logs.csv")[1:10,]; ggplot(errors[errors$rate<1,], aes(x=day, y=frame_error)) +

geom_smooth() + theme_minimal()
C. df = read.csv("iacs_ecat.csv"); subset(df, date >= Sys.Date()-10 & pct_error <1) |> ggplot(aes(date, pct)) + geom_bar()
D. ecat_df <- read.csv("10d_errors.csv"); filter(ecat_df, error<0.01) |> ggplot + line(aes(time, rate))

Answer: A

Explanation: Baselines per 62443-3-1 use visualization for trends. The script library(ggplot2); df <- read.csv("ecat_errors.csv"); df$date <- as.Date(df$date); baseline <- df[df$error_rate < 0.01,]; ggplot(baseline, aes(date, error_rate)) + geom_line() + labs(title="10d Baseline") filters <1% errors over 10 days, plots line for robotics EtherCAT normalcy.

Question: 1227

During development of an incident response plan per ISA/IEC 62443-2-1, which roles should be clearly defined for effective communication during an incident?

A. Incident Commander responsible for overall response coordination
B. Legal Advisor to handle compliance and regulatory matters
C. System Operators authorized to execute recovery steps
D. External vendors to perform forensic analysis in all incidents

Answer: A,B,C

Explanation: The plan must define core response roles such as Incident Commander, Legal Advisor, and System Operators for coordinated actions. External vendors are involved as needed, not necessarily in all incidents.

Question: 1228

In a wind turbine SCADA, testing CVE-2026-5740 injection patch (Schneider EVLink, CVSS 8.5) uses Multipass VMs on Ubuntu host per ISA/IEC 62443-2-3. Which commands?

A. multipass launch --name turbine-test --cpus 2 --mem 4G --network name=ot-isolated; multipass transfer patch.deb turbine-test:
B. multipass exec turbine-test -- sudo dpkg -i patch.deb; multipass exec turbine-test -- python3 -m unittest discover -v -s tests/
C. Cleanup: multipass delete --purge turbine-test if test_inject.py reports vulns post-patch.
D. Bridge to host br0 for shared storage during tests.

Answer: A,B,C

Explanation: Launch with isolated network and resources creates safe env. Exec chains install, then runs unittest for coverage. Purge on failures maintains lab cleanliness.

Question: 1229

In the context of cybersecurity monitoring, what does the term "false positive" refer to?

A. A legitimate threat that is not detected
B. A missed security update
C. A successful security breach
D. An alert generated for a non-threat event

Answer: D

Explanation: A "false positive" refers to an alert generated for a non-threat event, which can lead to unnecessary investigations and resource allocation.

Question: 1230

An aerospace manufacturing IACS experiences configuration drift in firewall rules post-cloud migration, allowing east-west traversal with risk 7/10 exceeding 5/10. Implementing ISA/IEC 62443-2-1, which actions ensure risk reduction?

A. Use Ansible playbooks with tasks "template src=firewall.j2 dest=/etc/fw.rules" for idempotent config enforcement.
B. Manually review rules weekly without automation.
C. Align configs to SL-T 3 via baseline templates cross-referenced to CIS benchmarks in 2024 updates.
D. Integrate with CMDB for drift detection via API polling every 15 minutes.

Answer: A, C, D

Explanation: Configuration management (SR 3.2) in ISA/IEC 62443-2-1 emphasizes automation, baselines, and monitoring for drift; manual reviews alone are error-prone and insufficient for complex IACS.

Question: 1231

During daily handovers at a pharmaceutical batching facility in 2026, operators report anomalous HMI response times linked to unmonitored IoT sensors. Integrating cybersecurity per ISA/IEC 62443-2-1, what setting adjustment in the network management console should the maintenance specialist apply?

A. Activate STP root guard on switches connected to HMI
B. Configure ACLs to rate-limit IoT multicast to 10 packets/sec
C. Set SNMPv3 community strings with privacy encryption for polling
D. Enable NetFlow export to analytics engine for sensor traffic baselining

Answer: D

Explanation: Asset owner responsibilities include integrating monitoring like NetFlow baselining into daily operations to detect anomalies, as per ISA/IEC 62443-2-1, ensuring alignment with performance metrics for security effectiveness.

Question: 1232

When performing an incident response tabletop exercise focused on malware spreading via USB devices, which key response steps should be validated?

A. Verification of removable media scanning policies effectiveness
B. Activation of network segmentation to isolate affected segments
C. Immediate permanent disconnection of all USB ports on ICS devices
D. Conducting forensic analysis on the infected media

Answer: A,B,D

Explanation: Effective scanning, network isolation, and forensic analysis are critical. Permanent disconnection without justification could impair operations.

Question: 1233

Which functions are essential in a patch management system designed for industrial automation environments?

A. Patch deployment scheduling aligned with operational shifts
B. Automatic rollback of patches without administrator approval
C. Integration with asset inventory databases
D. Single sign-on for all patch management actions

Answer: A,C,D

Explanation: Scheduling with shifts reduces impact, asset integration tracks affected systems, and SSO helps secure access. Automatic rollback without approval can cause unintended disruptions.

Question: 1234

Facing a supply chain disruption in a manufacturing plant compliant with ISA/IEC 62443-2-3, the team identifies CVE-2026-26383 (CVSS 9.0) in Johnson Controls' iSTAR tool, risking unauthorized access to assembly line PLCs. Prioritization must balance vendor delays. Which step aligns with the standard's process?

A. Ignore due to external factors, logging as 'non-actionable'.
B. Halt all operations until patch arrives with 'shutdown-emergency --vuln CVE-2026-26383'.
C. Use 'prioritize-delayed --cve CVE-2026-26383 --mitigate interim --timeline extended' to adjust for supply issues while applying compensating controls.
D. Patch unrelated systems first via 'random-update --exclude critical'.

Answer: C

Explanation: ISA/IEC 62443-2-3 supports flexible prioritization, allowing extended timelines for supply-

constrained critical patches while mandating interim mitigations like network segmentation. The command 'prioritize-delayed --cve CVE-2026-26383 --mitigate interim --timeline extended' implements this, documenting adjustments per the standard's lifecycle model to maintain security posture without unnecessary halts in manufacturing.

Question: 1235

A steel mill's IACS audit reveals outdated antivirus definitions on Level 2 servers, vulnerable to 2026 ransomware variants with risk 9/10 over 5/10 tolerable. Which actions align with ISA/IEC 62443-2-1 for program establishment and risk mitigation?

A. Automate EDR deployment with policy "scan-on-access enable" and real-time reporting to CSMS dashboard.
B. Defer updates until manual approval post-production shift.
C. Establish a patch baseline matrix cross-referenced to NIST SP 800-40r4 via the 2024 standard tables.
D. Configure exclusions for all .plc files without risk justification documentation.

Answer: A, C

Explanation: The updated standard requires automated protections (SR 5.2) and baseline policies (FR 3) for timely risk reduction; deferrals and un justified exclusions compromise integrity in high-availability IACS environments.

Question: 1236

A manufacturing facility in 2026 integrates IIoT sensors into its DCS for predictive maintenance, requiring secure procedure documentation per ISA/IEC 62443-4-2 CR 3.3. During routine sensor calibration, a zero-day vulnerability in the OPC UA server exposes confidential process data. Which elements must be incorporated into the maintenance procedure to uphold system integrity?

A. Implement role-based access control (RBAC) with least privilege for calibration tools
B. Use encrypted backups of configuration files with AES-256 and store offsite
C. Perform automated vulnerability scanning using Nessus with custom IACS plugins pre-calibration
D. Verify sensor firmware against vendor-provided SBOM using CycloneDX format

Answer: B, C, D

Explanation: ISA/IEC 62443-4-2 emphasizes encrypted backups with AES-256 for confidentiality in maintenance, automated scanning with tools like Nessus tailored for IACS to detect zero-days, and SBOM verification via standards like CycloneDX to ensure firmware integrity; RBAC supports access but is secondary to direct integrity measures in procedure documentation.

Question: 1237

2026 CSA Top Threats note IAM vulns in IACS. Patching with Okta. What API call enforces MFA?

A. PUT /me.
B. GET /users.
C. DELETE /groups/1.
D. POST /api/v1/policies { "name": "MFA Policy", "type": "MFA", "settings": { "enforce": true } }.

Answer: D

Explanation: Policy API enforces MFA, aligning with ISA/IEC 62443-3-3 IAM for cloud IACS. It mitigates credential threats per CSA.

Question: 1238

During operations review at a textile factory IACS, backup integrity checks fail 15% of tests, risk 7.8/10 vs. 4/10. Required actions?

A. Implement checksum validation scripts "rsync --checksum --dry-run".
B. Skip checks to save time.
C. Align to SR 8.2 with automated alerting on failures.
D. Rotate media quarterly with offsite vaulting.

Answer: A, C, D

Explanation: Recovery validation (SR 8) demands rigorous, alerted testing; skipping undermines resilience in the security program.

Question: 1239

Which of the following actions is critical when restoring systems after a cybersecurity incident?

A. Ensuring that vulnerabilities are addressed before restoration
B. Restoring systems without analysis
C. Ignoring previous incident logs
D. Only restoring data from the most recent backup

Answer: A

Explanation: Ensuring that vulnerabilities are addressed before restoration is critical when restoring systems after a cybersecurity incident. This step prevents the same vulnerabilities from being exploited again.

Question: 1240

In a petrochemical refinery's IACS, the maintenance specialist observes anomalous Modbus TCP traffic patterns via the integrated Snort IDS engine, showing a 25% deviation from the established baseline of 120 packets/second during normal HMI polling operations. Per ISA/IEC 62443-3-3 foundational requirements, which of the following actions must the specialist take to establish and verify an updated baseline for threat

detection in this zone

A. Capture a 72-hour rolling average of traffic using Wireshark filters for Modbus function codes 0x01 and 0x03, then recalibrate the anomaly threshold to ±15% via the IDS configuration file /etc/snort/rules/local.rules
B. Conduct a zone-specific risk assessment under SR 1.1, documenting the deviation in the CSMS audit log with timestamp 2026-10-29T14:30:00Z and correlating it to potential DoS vectors before updating the baseline
C. Isolate the affected conduit by applying ACL rules on the Cisco OT switch (e.g., access-list 101 deny tcp any host 192.168.1.10 eq 502) and perform a full system reboot to reset ephemeral states without baseline adjustment
D. Integrate AI-driven behavioral analytics from Nozomi Guardian to automate baseline recalibration, setting parameters for machine learning model retraining on historical data from the past 30 days with a confidence score >0.85

Answer: A, B

Explanation: Capturing a 72-hour rolling average of Modbus traffic using Wireshark for specific function codes ensures accurate representation of normal behavior, allowing recalibration of the anomaly threshold in Snort to detect deviations effectively, aligning with ISA/IEC 62443-3-3's emphasis on baseline establishment for resilient operations. Conducting a zone-specific risk assessment under SR 1.1 documents the deviation in the CSMS audit log, correlating it to threats like DoS, which is essential for verifying and updating baselines to maintain target security levels without disrupting operations.

Question: 1241

A 2026 renewable energy farm's inverter maintenance procedures, per ISA/IEC 62443-2-1, document remote parameter tuning via MQTT, hit by a replay attack altering voltage setpoints. Which steps ensure system integrity?

A. Append nonces and timestamps to MQTT payloads with HMAC validation
B. Validate tuning parameters against XML schemas pre-application
C. Deploy HSM for key generation during tuning sessions
D. Conduct post-tuning simulations in SPICE models

Answer: A, B

Explanation: Documented procedures under ISA/IEC 62443-2-1 require nonces/timestamps with HMAC for anti-replay integrity and schema validation for parameter correctness; HSM and simulations enhance security but are not essential for basic integrity steps.

Question: 1242

When conducting vulnerability assessments, what should be the primary focus of the scanning process in an IACS environment?

A. Finding known vulnerabilities
B. Detecting unauthorized devices

C. Identifying software versions
D. Evaluating user access levels

Answer: A

Explanation: The primary focus of the scanning process in an IACS environment should be on finding known vulnerabilities that could be exploited.

Question: 1243

Refinery flare system monitoring flags SL-C(3) shortfall post-firmware flash to v3.7. Actions?

A. Integrity check: sfk md5 flare_fw.v37.bin == known_good_hash
B. Rebaseline SR 6.1: verify resource availability post-flash in test env
C. Incident report: template fill 'Firmware_SL_Drop' with root cause 'hash_mismatch'
D. Reboot sequence: shutdown -r +1 flare_controller

Answer: A, B, C

Explanation: ISA/IEC 62443-2-1 integrates via integrity, SR verification, reporting; reboot is basic ops.

Question: 1244

What is the primary goal of training personnel on secure maintenance practices?

A. To reduce maintenance costs
B. To enhance system performance
C. To prevent unauthorized changes and ensure compliance
D. To streamline maintenance processes

Answer: C

Explanation: The primary goal of training personnel on secure maintenance practices is to prevent unauthorized changes and ensure compliance with security protocols, thereby protecting system integrity.

Question: 1245

A pharmaceutical plant's batch control system scan via Dragos Platform detects CVE-2026-32433 (CVSS 10.0, Erlang SSH RCE) on an IoT sensor aggregator and CVE-2026-59287 (CVSS 9.8, WSUS RCE) on a recipe management server. The aggregator feeds Level 3 MES, and the server is segmented but uses shared accounts. Per 62443-2-1, which remediation approaches align with OT exploitability prioritization?

A. Deploy a proxy conduit for the aggregator to filter SSH requests, tracking as a compensating control in the inventory
B. Prioritize server patching within 10 days due to shared account risks amplifying lateral movement in MES

integration
C. Decommission the aggregator without assessment, as its CVSS mandates immediate removal
D. Apply configuration hardening to the server by enabling WSUS approval workflows and audit logging

Answer: A, B, D

Explanation: Proxy conduits filter SSH in IoT aggregators, a safe OT remediation for high-CVSS flaws per 62443-2-1. Shared accounts elevate server priority for patching, addressing exploitability in integrated systems. Hardening with workflows and logging prevents unauthorized approvals; decommissioning without assessment risks production gaps in batch controls.

Question: 1246

In a recent patch cycle for a critical ICS server, performance degradation was noticed post-update. According to ISA/IEC 62443-2-3, what steps should be followed to address this?

A. Revert the patch using rollback procedures immediately
B. Continue usage while monitoring the system for further issues
C. Investigate the root cause in the isolated test environment
D. Update patch testing criteria to include performance benchmarks

Answer: A,C,D

Explanation: Immediate rollback protects operational integrity, followed by root cause analysis in testing to prevent recurrence. Testing criteria updates ensure future patches are evaluated for similar performance impact. Continued use without mitigation is risky.

Question: 1247

In the context of ongoing operations, what is the primary benefit of aligning cybersecurity practices with asset owner responsibilities?

A. Reduced operational costs
B. Improved stakeholder trust
C. Enhanced regulatory compliance
D. Increased system availability

Answer: B

Explanation: Aligning cybersecurity practices with asset owner responsibilities primarily enhances stakeholder trust, as it demonstrates a commitment to security and risk management.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, 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.

Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllbus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.