ISA

ISA-IEC-62443-IC37M

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

Latest Version: 6.0

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 6

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: 7

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: 8

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: 9

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: 10

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.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer