CompTIA

CS0-002 Exam

CySA+

Questions & Answers

(Demo Version - Limited Content)

Version: 19.0

Question: 1

An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform.

Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

A. FaaS
B. RTOS
C. SoC
D. GPS
E. CAN bus

Answer: E

Explanation:

Question: 2

An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply.

Which of the following would BEST identify potential indicators of compromise?

A. Use Burp Suite to capture packets to the SCADA device's IP.
B. Use tcpdump to capture packets from the SCADA device IP.
C. Use Wireshark to capture packets between SCADA devices and the management system.
D. Use Nmap to capture packets from the management system to the SCADA devices.

Answer: C

Explanation:

Question: 3

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

A. Human resources

B. Public relations
C. Marketing
D. Internal network operations center

Answer: B

Explanation:

Question: 4

An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability.

Which of the following would be the MOST appropriate to remediate the controller?

A. Segment the network to constrain access to administrative interfaces.
B. Replace the equipment that has third-party support.
C. Remove the legacy hardware from the network.
D. Install an IDS on the network between the switch and the legacy equipment.

Answer: A

Explanation:

Question: 5

A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.

Which of the following is the main concern a security analyst should have with this arrangement?

A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
C. Development phases occurring at multiple sites may produce change management issues.
D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Answer: D

Explanation:

Reference: https://www.eetimes.com/how-to-protect-intellectual-property-in-fpgas-devices-part- 1/#

Thank You for trying CS0-002 PDF Demo

Start Your CS0-002 Preparation