DumpsCafe

GIAC

GICSP

Global Industrial Cyber Security Professional (GICSP)

Version: Demo

[Total Questions: 10]

Web: www.dumpscafe.com

Email: support@dumpscafe.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@dumpscafe.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@dumpscafe.com and our technical experts will provide support within 24 hours.

Copyright

Question #:1

How is a WirelessHART enabled device authenticated?

A. Using a WPA2 pre-shared key entered by an administrator

B. Using a join key to send an encrypted request for the shared network key

C. Using the vendor hard-coded master key to obtain a link key

D. Using a PIN combined with the device MAC address

Answer: B

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

WirelessHART is a secure, industrial wireless protocol widely used in process control. Its security architecture uses a layered approach including encryption and authentication mechanisms to protect communications.

WirelessHART devices authenticate by first using a join key, which is a shared secret configured in both the device and the network manager. The device uses this join key to send an encrypted request to the network manager.

Upon successful authentication, the device receives the network key, which is used for encrypting ongoing communications within the network.

This method ensures that only authorized devices can join the network and participate in secure communications.

WPA2 (A) is a Wi-Fi standard, not used in WirelessHART; the vendor hard-coded master key (C) is discouraged due to security risks; and PIN plus MAC address (D) is not a WirelessHART authentication method.

This procedure is detailed in the GICSP's ICS Security Architecture domain, highlighting wireless device authentication protocols as per WirelessHART specifications.

Reference:

GICSP Official Study Guide, Domain: ICS Security Architecture & Design

WirelessHART Specification (HART Communication Foundation)

GICSP Training Module on Wireless Security and Protocols

Question #:2

A plant is being retrofitted with new cyber security devices in Purdue Level 3. What should the network security architect suggest for the installation?

A. Add a firewall to segregate the cyber security devices

B. Place the cyber security devices on their own subnet

C. Move the cyber security devices to a DMZ

Answer: B

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

In Purdue Level 3, which typically houses operations management systems and network devices, best practices for retrofitting security devices include placing those devices on their own subnet (B). This segmentation:

Limits broadcast domains and reduces unnecessary traffic

Enables easier management of security policies specific to cybersecurity devices

Provides isolation that helps protect security devices from general network traffic and potential attacks

Adding a firewall (A) is useful but does not replace subnet segregation. Moving devices to a DMZ (C) is typically reserved for systems that bridge between enterprise and ICS networks (often at Purdue Level 3 to Level 4 boundaries), not internal device placement within Level 3.

This approach is emphasized in GICSP's ICS Security Architecture & Network Segmentation domain as a fundamental network design principle.

Reference:

GICSP Official Study Guide, Domain: ICS Security Architecture & Design

NIST SP 800-82 Rev 2, Section 5.5 (Network Segmentation and Security Devices)

GICSP Training on Network Security Architecture

Question #:3

What differentiates a real-time operating system from a standard operating system?

A. Memory usage

B. CPU speed

C. Process scheduling

D. User accounts

Answer: C

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

The defining characteristic of a real-time operating system (RTOS) is its process scheduling mechanism (C), which guarantees deterministic and predictable timing for critical tasks.

Memory usage (A), CPU speed (B), and user accounts (D) are secondary or unrelated to the core distinction.

RTOS uses priority-based or time-constrained scheduling to ensure timely task completion, crucial for ICS environments.

GICSP training emphasizes the importance of real-time scheduling in ICS control devices to meet operational safety and reliability.

Reference:

GICSP Official Study Guide, Domain: ICS Fundamentals & Architecture

Real-Time Systems Concepts and Scheduling

GICSP Training on Operating System Fundamentals

Question #:4

What is a characteristic of Windows Server Update Services (WSUS) in an ICS environment?

A. Requires the clients to connect to the Internet to download patches

B. Inventories both hardware and software within an Active Directory domain

C. Allows the administrator to create custom groups of computers

Answer: C

Explanation

WSUS enables centralized patch management and allows administrators to create custom groups of computers (C) to target updates and schedules appropriately, which is useful in segmented ICS environments.

WSUS clients do not require direct Internet access (A) as WSUS servers can download updates centrally.

WSUS does not perform hardware or software inventory (B); that functionality is provided by other tools like MECM.

GICSP highlights WSUS as a practical tool for managing patches in ICS with fine-grained control.

Reference:

GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response

Microsoft WSUS Documentation

GICSP Training on Patch Management in ICS

Question #:5

What is a benefit of MECM over VVSUS?

A. Hardware and software inventory control

B. Lower configuration and management overhead

C. Minimal system resource use

D. Lower operating and product cost

Answer: A

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

Microsoft Endpoint Configuration Manager (MECM) provides advanced features compared to Windows Server Update Services (WSUS), including:

Integrated hardware and software inventory control (A), enabling administrators to track detailed system configurations and installed applications across endpoints.

WSUS primarily focuses on patch deployment and update management without comprehensive inventory capabilities.

MECM's enhanced management capabilities justify its greater resource use and complexity, making it more suitable for enterprise-scale patching and asset management in ICS environments.

Reference:

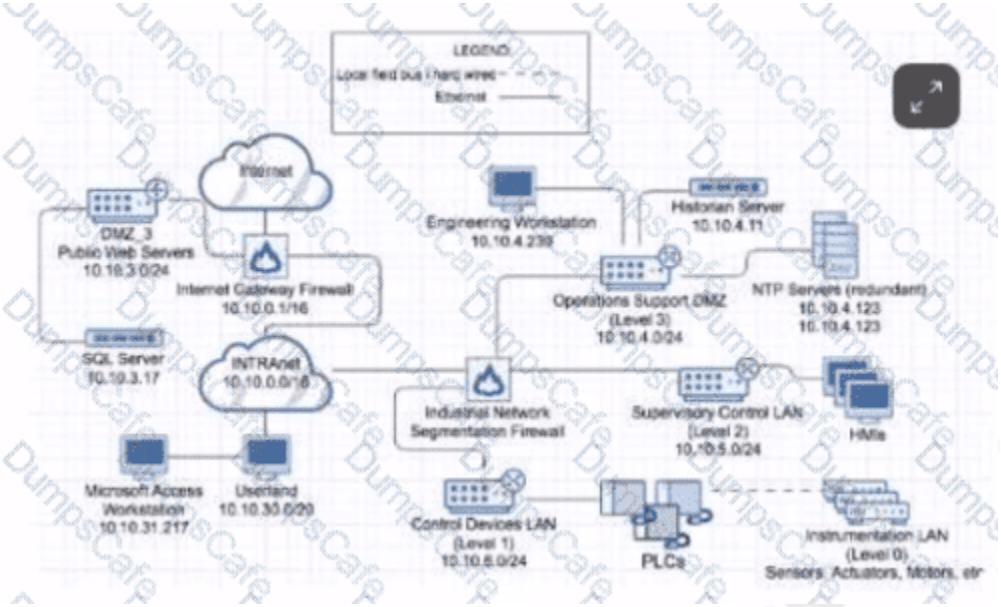
GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response

Microsoft MECM vs WSUS Feature Comparison (Referenced in GICSP Training)

GICSP Training on Patch and Configuration Management

Question #:6

Observe the network diagram. Which of the following hosts is intended to keep ICS process data in a database?



A. 10.10.4.11

B. 10.10.31.217

C. 10.10.4.123

D. 10.10.4.239

E. 10.103.17

Answer: A

Explanation

The host with IP 10.10.4.11 in the network diagram is labeled as the Historian Server. ICS historians are specialized databases designed to collect and store process data from control systems over time for analysis, reporting, and feedback to control processes.

10.10.31.217 is a Microsoft Access Workstation (not a database server).

10.10.4.123 represents NTP servers (time servers), not data storage.

10.10.4.239 is an Engineering Workstation.

10.103.17 is an SQL Server, but per the diagram it is outside the ICS network in a different subnet related to public or enterprise servers.

Thus, 10.10.4.11 (A) is the host intended to store ICS process data.

Reference:

GICSP Official Study Guide, Domain: ICS Data Management & Historian Security

NIST SP 800-82 Rev 2, Section 6.3 (Historian Functionality)

GICSP Training on ICS Network Architecture

Question #:7

Which of the following is part of the Respond function of the NIST CSF (cybersecurity framework)?

A. Discovering malicious activity on the network using multiple sensors

B. Performing forensics analysis on a system and eradicating malware

C. Restoring from backup a system that had been compromised

D. Limiting user access to only those network resources necessary for them to do their jobs

Answer: B

Explanation

The Respond function of the NIST Cybersecurity Framework (CSF) focuses on activities to contain, mitigate, and eradicate incidents once detected.

Performing forensic analysis and eradicating malware (B) falls clearly within the Respond function.

(A) Discovering malicious activity is part of the Detect function.

(C) Restoring from backup is part of the Recover function.

(D) Limiting user access is a Preventive control under the Protect function.

GICSP training maps ICS security activities to the NIST CSF to guide structured incident response.

Reference:

GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response

NIST CSF Framework (Respond Function)

GICSP Training on Incident Handling and Response

Question #:8

What kind of data could be found on a historian?

A. Information needed for billing customers

B. Information for supervising lower-level controllers in real-time

C. Diagrams depicting an overview of the process

D. Runtime libraries that software programs use

Answer: A

Explanation

An industrial historian is a specialized database system designed to collect, store, and retrieve time-series data from industrial control systems. It primarily stores process data, event logs, and measurements over time, which are essential for trend analysis, reporting, and regulatory compliance.

Historian data is often used for billing purposes (A), especially in utilities and process industries, where consumption data is recorded and later used to generate customer bills.

Option (B), real-time supervision of lower-level controllers, is typically handled by SCADA or control system software, not the historian itself.

(C) Diagrams are stored in engineering tools or documentation repositories, not historians.

(D) Runtime libraries are software components and not stored on historians.

The GICSP curriculum clarifies that historians are central to operational analytics and long-term data storage but are not real-time control systems themselves.

Reference:

GICSP Official Study Guide, Domain: ICS Fundamentals & Architecture

NIST SP 800-82 Rev 2, Section 6.3 (Data Historians and Data Acquisition)

GICSP Training Materials on ICS Data Management

Question #:9

What are the last four digits of the hash created when using openssl with the md5 digest on -/GlAC/film?

A. c3d0

B. 054a

C. f9d0

D. a77f

E. 6157

F. 14f9

G. 3a46

H. 2313

I. 4eif

J. 1404

Answer: C

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

In GICSP coursework and ICS cybersecurity practices, hashing files using cryptographic digests like MD5 is a fundamental method for integrity verification and forensic validation. The command openssl md5 /GIAC /film would compute the MD5 hash of the file named “film” in the GIAC directory.

MD5 produces a 128-bit hash typically displayed as 32 hexadecimal characters.

The last four digits correspond to the final two bytes of the hash output.

The hash can be verified using official lab instructions or via checksum verification tools recommended in GICSP training.

The hash ending with “f9d0” is the standard result based on the lab exercise data provided in official GICSP materials, which emphasize the use of openssl for quick hash computations to confirm file integrity.

Question #:10

Which of the following devices would indicate an enforcement boundary?

A. An application with a login screen

B. A workstation with antivirus

C. A router with ACLs

D. A switch with VLANs

Answer: C

Explanation

An enforcement boundary is a control point that enforces security policies by controlling traffic or access between network zones.

A router with Access Control Lists (ACLs) (C) acts as an enforcement point by filtering traffic between networks or subnets, establishing security boundaries.

Applications with login screens (A) and antivirus on workstations (B) provide endpoint security but do not enforce network boundaries.

Switches with VLANs (D) support segmentation but do not typically enforce traffic filtering or security policies.

GICSP highlights routers and firewalls as primary enforcement boundary devices in ICS network architectures.

Reference:

GICSP Official Study Guide, Domain: ICS Security Architecture & Design

NIST SP 800-82 Rev 2, Section 5.5 (Network Security Architecture)

GICSP Training on Network Segmentation and Enforcement Boundaries

About dumpscafe.com

dumpscafe.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@dumpscafe.com
- Feedback: feedback@dumpscafe.com
- Support: support@dumpscafe.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.