

Free PDF Quiz 2026 GIAC Latest GICSP: Trustworthy Global Industrial Cyber Security Professional (GICSP) Source



Research has found that stimulating interest in learning may be the best solution. Therefore, the GICSP prepare guide' focus is to reform the rigid and useless memory mode by changing the way in which the GICSP exams are prepared. Our Soft version of GICSP practice materials combine knowledge with the latest technology to greatly stimulate your learning power. By simulating enjoyable learning scenes and vivid explanations, users will have greater confidence in passing the qualifying GICSP exams.

Are you staying up for the GICSP exam day and night? Do you have no free time to contact with your friends and families because of preparing for the exam? Are you tired of preparing for different kinds of exams? If your answer is yes, please buy our GICSP Exam Questions, which is equipped with a high quality. We can make sure that our products have the ability to help you pass the exam and get the according GICSP certification.

>> Trustworthy GICSP Source <<

GICSP Test Pdf - Reliable GICSP Dumps Ppt

Perhaps it was because of the work that there was not enough time to learn, or because the lack of the right method of learning led to a lot of time still failing to pass the GICSP examination. Whether you are the first or the second or even more taking GICSP examination, our GICSP exam prep not only can help you to save much time and energy but also can help you pass the exam. In the other words, passing the exam once will no longer be a dream.

GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q30-Q35):

NEW QUESTION # 30

Use diff to compare the Fisherman and NOLA text files located in the GIAC directory on the Desktop. Which word exists in one file, that does not exist in the other?

- A. Grateful
- B. Teacher
- C. Inspire
- D. Species
- E. Open
- F. Betray
- G. Resource
- H. Directions
- I. Express
- J. Distort

Answer: F

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

This question tests basic command-line skills, specifically using diff to compare text files, which is a common task in cybersecurity to detect differences or anomalies in configuration or log files.

The diff command outputs lines that are unique to either file or lines that differ between files. One would examine the output to see which of the listed words appear exclusively in one file.

According to GICSP principles in Cybersecurity Operations, understanding file comparison helps detect unauthorized changes or identify unique data in forensic investigations.

Based on typical file comparisons in such practical exams, the word "Betray" is often used as an example of a word present in one file but not in another, reflecting a critical difference.

NEW QUESTION # 31

How is a WirelessHART enabled device authenticated?

- A. Using a join key to send an encrypted request for the shared network key
- B. Using the vendor hard-coded master key to obtain a link key
- C. Using a WPA2 pre-shared key entered by an administrator
- D. Using a PIN combined with the device MAC address

Answer: A

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

NEW QUESTION # 32

Which type of device is the following configuration setting from?

deny modbus function write-multiple-holdingregisters

- A. NIDS
- B. Application firewall
- C. SIEM
- D. Network firewall

Answer: B

Explanation:

The configuration line denies a specific Modbus function code, which is a command-level filter for industrial protocols.

This type of control is typical of an application firewall (D) designed to understand and filter industrial control system protocols at the application layer.

A network firewall (A) typically filters traffic based on IP addresses, ports, and protocols, but not protocol function codes.

NIDS (B) detects and alerts on suspicious traffic but does not usually enforce blocking rules.

SIEM (C) collects and analyzes logs, not real-time blocking.

GICSP emphasizes the role of application-layer firewalls in protecting ICS protocols like Modbus.

Reference:

NEW QUESTION # 33

An organization has their ICS operations and networking equipment installed in the Purdue model level 3. Where should the SIEM for this equipment be placed in relation to the existing Level 3 devices?

- A. On a different subnet in Level 3
- B. On the same subnet in Level 3
- **C. On a management subnet in Level 4**
- D. On a management subnet in Level 2

Answer: C

Explanation:

According to the Purdue model and best practices outlined in GICSP, Level 4 corresponds to the enterprise or business network, often containing management and security monitoring infrastructure such as Security Information and Event Management (SIEM) systems.

Placing the SIEM on a management subnet in Level 4 (B) keeps monitoring tools separated from the operational control network (Level 3), reducing the risk that a compromised Level 3 device could affect the security infrastructure itself. It also allows the SIEM to collect logs from multiple network segments securely and apply enterprise-wide analysis.

This segregation supports defense-in-depth and aligns with GICSP's emphasis on secure network segmentation and monitoring.

Reference:

GICSP Official Study Guide, Domain: ICS Security Architecture & Design
NIST SP 800-82 Rev 2, Section 5.5 (Network Architecture)
GICSP Training Materials on Network Segmentation and SIEM Deployment

NEW QUESTION # 34

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. Place the cyber security devices on their own subnet**
- B. Move the cyber security devices to a DMZ
- C. Add a firewall to segregate the cyber security devices

Answer: A

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

NEW QUESTION # 35

.....

GICSP Test Pdf: <https://www.dumpsreview.com/GICSP-exam-dumps-review.html>

I don't recommend a blanket approach, because each web site is its own GICSP entity with its own set of requirements, Managing Internet Security and Acceleration, 100% Money Back Guarantee - A Guarantee For Your Exam.

Extreme high quality, The GICSP exam training dumps is essential tool to prepare for GICSP actual test.

- [illegible]