

Pass Guaranteed GIAC - Accurate GICSP - Global Industrial Cyber Security Professional (GICSP) New Cram Materials



Nowadays, we live so busy every day. Especially for some businessmen who want to pass the GICSP exam and get related certification, time is vital importance for them, they may don't have enough time to prepare for their exam. Some of them may give it up. But our GICSP guide tests can solve these problems perfectly, because our study materials only need little hours can be grasped. Believing in our GICSP Guide tests will help you get the certificate and embrace a bright future. Time and tide wait for no man. Come to buy our test engine.

This format is for candidates who do not have the time or energy to use a computer or laptop for preparation. GIAC GICSP PDF file includes real GIAC GICSP questions, and they can be easily printed and studied at any time. Real4dumps regularly updates its PDF file to ensure that its readers have access to the updated questions.

>> GICSP New Cram Materials <<

2026 Newest GICSP New Cram Materials | GICSP 100% Free 100% Accuracy

The GICSP web-based practice test can accessed online. It means the exam candidates can access it from the browsers like Firefox, Microsoft Edge, Google Chrome, and Safari. The user don't need to install or download any excessive plugins to take the Global Industrial Cyber Security Professional (GICSP) (GICSP) practice test. Mac, Windows, iOS, Android, and Linux support it. The third and last format is the desktop practice test software. The Global Industrial Cyber Security Professional (GICSP) (GICSP) desktop practice test format can be used on Windows computers.

GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q72-Q77):

NEW QUESTION # 72

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

- J. Betray

Answer: J

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 # 73

Implementation of LDAP to manage and control access to your systems is an outcome of which NIST CSF core function?

- A. Respond
- B. Detect
- C. Protect
- D. Identify

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

LDAP (Lightweight Directory Access Protocol) is used to manage authentication and authorization services, controlling user access to systems and resources.

This function aligns with the Protect function (A) of the NIST Cybersecurity Framework (CSF), which focuses on access control, identity management, and protective technology to safeguard systems.

Identify (B) relates to asset management and risk assessment.

Respond (C) deals with incident response.

Detect (D) relates to discovering cybersecurity events.

GICSP maps LDAP implementation as a key protective control to ensure authorized access in ICS environments.

Reference:

GICSP Official Study Guide, Domain: ICS Security Governance & Compliance NIST CSF Framework (Protect Function) GICSP Training on Identity and Access Management

NEW QUESTION # 74

What is a recommended practice for configuring enforcement boundary devices in an ICS control network?

- A. Create one rule for each authorized conversation in a stateless access control list
- B. Enable full packet collection for all allowed and denied traffic rules on next-generation firewalls
- C. Use an egress policy that allows everything out except for that which is explicitly denied
- D. Create a rule which drops inbound packets containing a source address from within the protected network

Answer: B

Explanation:

Enforcement boundary devices like firewalls play a critical role in ICS network security. A best practice is to:

Enable full packet collection for all allowed and denied traffic (B) on next-generation firewalls. This facilitates deep inspection, detailed logging, and auditing, which are vital for detecting anomalous or malicious activity.

Other options are less effective or counterproductive:

(A) Dropping inbound packets with source addresses from the protected network is generally illogical and may disrupt normal traffic.

(C) Stateless access control is less secure and less manageable than stateful inspection.

(D) Default allow egress policies increase risk by permitting unnecessary outbound traffic.

GICSP stresses detailed logging and stateful inspection as core security controls for enforcement points.

Reference:

GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response NIST SP 800-82 Rev 2, Section 5.5 (Network Security and Firewalls) GICSP Training on Network Boundary Protection

NEW QUESTION # 75

An organization wants to use Active Directory to manage systems within its Business and Control system networks. Which of the following is the recommended security practice?

- A. Shared Active Directory domain with fully functional domain controllers for the Business network and a Read-Only Domain Controller for the Control system network
- B. An Active Directory domain for the Business network and a Windows workgroup with a domain controller for the Control system network
- C. Shared Active Directory domain with separate domain controllers for the Business and Control system networks
- D. Separate Active Directory domains for the Business and Control system networks

Answer: A

Explanation:

The recommended best practice is to use a shared Active Directory domain while deploying a Read-Only Domain Controller (RODC) within the Control system network (D). This approach:

Enables centralized management and authentication consistent with the business network Limits the risk of domain controller compromise in the Control network because RODCs do not store sensitive password information and restrict changes Balances security and operational efficiency by isolating sensitive environments while still leveraging AD's capabilities Options A and C increase complexity or risk by fully separating domains or controllers, while B reduces manageability by mixing domain and workgroup systems.

GICSP highlights RODCs as a means to secure domain services in ICS environments where full domain controllers pose a security risk.

Reference:

GICSP Official Study Guide, Domain: ICS Security Governance & Compliance Microsoft Active Directory Best Practices (Referenced in GICSP) GICSP Training on Identity Management and Network Segmentation

NEW QUESTION # 76

What do the following protocols have in common?



- A. Use in RF mesh networks
- B. Use of IPv6 in the network layer
- C. Ability to use asymmetric join methods
- D. Ability to tunnel legacy protocols

Answer: A

Explanation:

WirelessHART, ISA100.11a, and ZigBee are all wireless communication protocols commonly used in industrial automation and control systems. A key characteristic they share is:

They use RF (Radio Frequency) mesh networking (B) to enable devices to communicate through multiple hops, improving reliability and coverage. Mesh networks allow devices to relay messages, creating a robust wireless infrastructure.

Use of IPv6 (A) is specific to some protocols but not common to all three.

Asymmetric join methods (C) and tunneling legacy protocols (D) are not shared features of all three.

The GICSP materials emphasize mesh network topology as a key feature of these protocols in enabling reliable and secure wireless ICS communications.

Reference:

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

- [illegible]

www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes