

# Frequent GIAC GICSP Updates & GICSP Valid Test Guide



info@cbtproxy.com

## Top 5 Skills You Will Learn with the GIAC GICSP Certification Program



We provide free PDF demo of our GICSP practice questions download before purchasing our complete version. After purchasing we provide one year free updates and one year customer service on our GICSP learning materials. Also we promise "Pass Guaranteed" with our GICSP training braindump. Our aim is to make our pass rate high up to 100% and the ratio of customer satisfaction is also 100%. If you are looking for valid GICSP preparation materials, don't hesitate, go ahead to choose us.

Pass4Leader is subservient to your development. And our experts generalize the knowledge of the exam into our products showing in three versions. PDF version of GICSP exam questions - support customers' printing request, and allow you to have a print and practice in papers. Software version of GICSP learning guide - supporting simulation test system, and remember this version support Windows system users only. App/online version of GICSP mock quiz - Being suitable to all kinds of equipment or digital devices, and you can review history and performance better.

>> **Frequent GIAC GICSP Updates** <<

## Simplest Format of GIAC GICSP Exam PDF Practice Materials

You may want to own a GICSP certificate to prove that you are competent and boost excellent practical abilities in some certain area. Thus you will be regarded as the capable people and be respected. Passing the test GICSP certification can help you realize your goals and if you buy our GICSP Guide Torrent you will pass the GICSP exam easily. Our GICSP exam questions are written by the most professional experts, so the quality of our GICSP learning material is wonderful. And we always keep our GICSP study guide the most updated for you to pass the exam.

## GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q31-Q36):

### NEW QUESTION # 31

During a plant upgrade an architect needs to connect legacy IEDs to a new TCP/IP instrumentation LAN. The IEDs only have RS-232 communication interfaces available. What would best be used to connect the IEDs?

- A. Industrial switch
- B. Data diode
- **C. Communications Gateway**
- D. Engineering workstation

**Answer: C**

Explanation:

Legacy devices using RS-232 interfaces require a communications gateway (C) to translate between the serial communication protocol and the new TCP/IP network.

A data diode (A) is a unidirectional security device, not a protocol translator.

An engineering workstation (B) is a computer, not a protocol conversion device.

An industrial switch (D) operates at the Ethernet layer and does not perform protocol conversion.

GICSP emphasizes gateways as essential for integrating legacy ICS devices into modern IP networks while maintaining protocol integrity.

Reference:

GICSP Official Study Guide, Domain: ICS Fundamentals & Architecture

NIST SP 800-82 Rev 2, Section 3.4 (Legacy Protocol Integration)

GICSP Training on ICS Network Architecture and Protocols

### NEW QUESTION # 32

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

- A. Allows the administrator to create custom groups of computers
- B. Requires the clients to connect to the Internet to download patches
- C. Inventories both hardware and software within an Active Directory domain

**Answer: A**

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

### NEW QUESTION # 33

During a plant upgrade an architect needs to connect legacy IEDs to a new TCP/IP instrumentation LAN. The IEDs only have RS-232 communication interfaces available. What would best be used to connect the IEDs?

- A. Industrial switch
- B. Data diode
- C. Communications Gateway
- D. Engineering workstation

**Answer: C**

Explanation:

Legacy devices using RS-232 interfaces require a communications gateway (C) to translate between the serial communication protocol and the new TCP/IP network.

A data diode (A) is a unidirectional security device, not a protocol translator.

An engineering workstation (B) is a computer, not a protocol conversion device.

An industrial switch (D) operates at the Ethernet layer and does not perform protocol conversion.

GICSP emphasizes gateways as essential for integrating legacy ICS devices into modern IP networks while maintaining protocol integrity.

Reference:

GICSP Official Study Guide, Domain: ICS Fundamentals & Architecture

NIST SP 800-82 Rev 2, Section 3.4 (Legacy Protocol Integration)

GICSP Training on ICS Network Architecture and Protocols

### NEW QUESTION # 34

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

- A. Performing forensics analysis on a system and eradicating malware
- B. Discovering malicious activity on the network using multiple sensors
- C. Limiting user access to only those network resources necessary for them to do their jobs

- D. Restoring from backup a system that had been compromised

**Answer: A**

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

### NEW QUESTION # 35

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

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

**Answer: D**

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 # 36

.....

In this way, the GIAC GICSP certified professionals can not only validate their skills and knowledge level but also put their careers on the right track. By doing this you can achieve your career objectives. To avail of all these benefits you need to pass the Global Industrial Cyber Security Professional (GICSP) (GICSP) exam which is a difficult exam that demands firm commitment and complete GIAC GICSP exam questions preparation.

**GICSP Valid Test Guide:** <https://www.pass4leader.com/GIAC/GICSP-exam.html>

Success in the GICSP Global Industrial Cyber Security Professional (GICSP) exam validates and upgrades your skills in GIAC GICSP technologies, With our high-accuracy GICSP test guide, our candidates can become sophisticated with the exam content, Most of the candidates remain confused about the format of the actual GICSP exam and the nature of questions therein, You can feel at ease to purchase our GICSP Valid Test Guide - Global Industrial Cyber Security Professional (GICSP) torrent training.

When a system joins a domain, the Domain Admins group is added GICSP to this group, but it can be removed, Companies cancelled orders, quit hiring, and stopped paying suppliers.

Success in the GICSP Global Industrial Cyber Security Professional (GICSP) exam validates and upgrades your skills in GIAC GICSP technologies, With our high-accuracy GICSP test guide, our candidates can become sophisticated with the exam content.

