# GICSP Sample Questions Answers, GICSP Materials

SANS GICSP (Study Questions for SANS GICSP) CORRECTLY ANSWERED 2024

Access Control Models Answer - Information Flow
Non Interference

Confidentiality of Stored Information
- Bell-LaPadula (Mandatory Access Control)
- Access Matrix (Read, Write or Execute or R/W/X)
- Take-Grant (Rights = Create, Revoke, Take and Grant

Integrity of Stored Information
- Biba Integrity Model (Bell-LaPadula upside down)
- Clark-Wilson

Mandatory Access Control (MAC) Answer - Permissions to objects are managed centrally by an administrator. Is an access policy determined by the system, rather than by the owner. Organizations use this in multilevel systems that process highly sensitive data such as classified govt or military.

Examples: 1) Rule-based, 2) Lattice Model

Discretionary Access Control (DAC) Answer - Is an access policy determined by the owner of a file (or other resource). The owner decides who's allowed access to a file and what privileges they have.

Role Based Access Control (RBAC) Answer - A method of implementing discretionary access controls in which access decisions are based on group membership, according to organization or functional roles.

LDAP - Lightweight Directory Access Protocol Answer - An Internet Protocol (IP) and data storage model that supports authentication and directory functions. It is a remote access authentication protocol. Vendors = Microsoft Active Directory, CA eTrust Directory, Apache Directory Server, Novell eDirectory, IBM SecureWay and Tivoli Directory Server, Sun Directlry Server. OpenLDAP and tinyldap open source versions.

User Account Answer - Allows a user to authenticate to system services and be granted authorization to access them; however, authentication does not imply authorization.

Service Account Answer - Is an account that a service on your computer uses to run under and access resources. This should not be a user's personal account. Can also

Successful people are never satisfying their current achievements. So they never stop challenging themselves. If you refuse to be an ordinary person, come to learn our GICSP preparation questions. Our GICSP study materials will broaden your horizons and knowledge. Many people have benefited from learning our GICSP learning braindumps. Most of them have realized their dreams and became successful.

There is always a fear of losing the GICSP exam and this causes you may loss your money and waste the time. There is no such issue if you study our GICSP exam questions. Your money and exam attempt is bound to award you a sure and definite success if you study with our GICSP Study Guide to prapare for the exam. According to our data, our pass rate of the GICSP practice engine is high as 98% to 100%. So if you choose our GICSP learning quiz, you will pass for sure.

**>> GICSP Sample Questions Answers <<**

## Free PDF 2025 GIAC Pass-Sure GICSP Sample Questions Answers

Our GICSP study materials are designed by many experts in the field of qualification examination, from the user's point of view, combined with the actual situation of users, designed the most practical learning materials, so as to help customers save their valuable time. Whether you are a student or a working family, we believe that no one will spend all their time preparing for GICSP Exam, whether you are studying professional knowledge, doing housework, looking after children, and so on, everyone has their own life, all of which have to occupy your time to review the exam.

# GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q50-Q55):

**NEW QUESTION # 50**
Which of the following is typically performed during the Recovery phase of incident response?

- A. Finding the root cause or vector used by the attacker to gain entry and maintain access.
- B. Updating the organization's security policies to prevent future breaches.
- C. Patching and configuring systems to meet established secure configuration standards.
- D. Making a forensic image of the system(s) involved in the incident.

**Answer: C**

Explanation:
The Recovery phase in incident response focuses on restoring systems to normal operations and strengthening defenses:
Patching and configuring systems to meet secure standards (B) is a typical recovery activity to prevent recurrence.
Updating security policies (A) is usually part of the Post-Incident Activities or Governance.
Root cause analysis (C) is typically part of the Investigation or Analysis phase.
Forensic imaging (D) is part of the Containment and Eradication phases for evidence preservation.
GICSP aligns recovery activities with system hardening and return to normal operations.
Reference:
GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response NIST SP 800-61 Rev 2 (Incident Handling Guide) GICSP Training on Incident Response Lifecycle

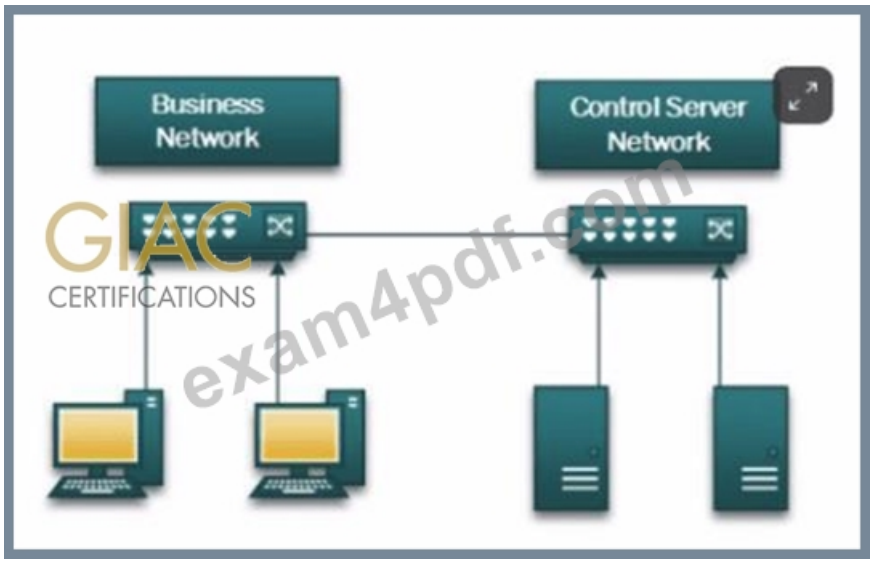
**NEW QUESTION # 51**
For application-aware firewalls filtering traffic between trust zones, which of the following policies should be applied to a packet that doesn't match an existing rule?

- A. Default deny
- B. Default alert
- C. Application deny list
- D. Application allow list

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In the context ofIndustrial Control Systems (ICS)andOT network security, the principle of least privilege and explicit access control is fundamental for protecting critical infrastructure assets. According to the GICSP framework, when usingapplication-aware firewallsbetween different trust zones (e.g., corporate network to OT network), any traffic that doesnot explicitly match a defined ruleshould be blocked by default. This is referred to as the"default deny" policy.
* Default denymeans that unless traffic is explicitly allowed by firewall rules, it should be denied. This ensures that no unknown or unauthorized packets traverse trust boundaries, reducing the attack surface significantly.
* Thedefault alertoption (A) is useful for monitoring but does not prevent unauthorized access, so it's insufficient as a security control.
* Application deny list(C) andapplication allow list(D) refer to sets of permitted or denied applications, but the firewall still needs an overarching policy to handle unmatched packets; that policy must be deny for safety.
This approach is emphasized in theICS Security Architecture and Network Segmentationdomain of GICSP, reinforcing that all unknown or unexpected network traffic should be blocked unless explicitly permitted by policy. This aligns withNIST SP 800-82 Rev 2guidance on ICS security, which GICSP incorporates.
Reference:
Global Industrial Cyber Security Professional (GICSP) Official Study Guide, Domain: ICS Security Architecture & Design NIST SP 800-82 Rev 2: Guide to Industrial Control Systems (ICS) Security, Section 5.5 (Network Architecture) GICSP Training Materials, Firewall & Network Segmentation Best Practices Module

**NEW QUESTION # 52**
Based on the following diagram, how many Active Directory domains should be created for this network?




- A. One domain with separate groups within
- B. Two separate domains within the same tree
- C. Two separate domains without a trust relationship
- D. One domain with transitive trust

**Answer: A**

Explanation:
The diagram shows two networks (Business Network and Control Server Network) connected by a switch, suggesting a single organization's infrastructure with logical segmentation.
Best practices per GICSP for ICS and enterprise network integration recommend a single Active Directory domain with groups and organizational units to separate roles and permissions. This approach simplifies management, maintains centralized authentication, and supports role-based access control.
Creating multiple domains (B or C) introduces unnecessary complexity and potential trust relationship issues.
A transitive trust (D) is relevant when multiple domains exist, which is not required here.
The GICSP framework supports minimizing complexity in domain design to reduce attack surfaces while maintaining proper segmentation through groups and policies.
Reference:
GICSP Official Study Guide, Domain: ICS Security Governance & Compliance Microsoft Active Directory Best Practices (Referenced in GICSP) GICSP Training on Identity and Access Management

**NEW QUESTION # 53**
How is a WirelessHART enabled device authenticated?

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

**Answer: D**

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 # 54**
An engineer has analyzed a subsystem of a power plant and identified physical and logical inputs that could expose the subsystem to unauthorized access. What has the engineer defined?

- A. A threat model
- B. A vulnerability scan
- C. An attack surface
- D. A risk analysis

**Answer: C**

Explanation:
By identifying all the points where a system could be accessed or attacked (physical or logical), the engineer has defined the attack surface (B).
A vulnerability scan (A) is an automated tool-based assessment.
A risk analysis (C) evaluates the likelihood and impact of threats.
A threat model (D) outlines potential threat actors and attack paths but not specifically all input points.
Understanding the attack surface is critical to designing effective ICS security controls, as emphasized in GICSP.
Reference:
GICSP Official Study Guide, Domain: ICS Risk Management
GICSP Training on Threat Modeling and Vulnerability Assessment
NIST SP 800-30 (Risk Assessment Guide)

**NEW QUESTION # 55**
.....

- GICSP Pass-Sure Materials: Global Industrial Cyber Security Professional (GICSP) - GICSP Training Guide - GICSP Quiz Torrent □ Search for （ GICSP ） and download it for free on 【 www.passtestking.com 】 website □Training GICSP Pdf
- Pass Guaranteed GIAC - Accurate GICSP - Global Industrial Cyber Security Professional (GICSP) Sample Questions Answers □ Search for { GICSP } and obtain a free download on { www.pdfvce.com } □Exam GICSP Bible
- Quiz 2025 GICSP: Latest Global Industrial Cyber Security Professional (GICSP) Sample Questions Answers □ Search for ☀ GICSP □☀□ on （ www.getvalidtest.com ） immediately to obtain a free download □GICSP Guaranteed Questions Answers
- Quiz 2025 Newest GIAC GICSP: Global Industrial Cyber Security Professional (GICSP) Sample Questions Answers □ Search for ✔ GICSP □✔□ and obtain a free download on 「 www.pdfvce.com 」 □GICSP Valid Dumps Ebook
- GIAC GICSP PDF Questions-Shortcut To Success □ Search for □ GICSP □ and download it for free on ➡ www.vceengine.com □□□ website □GICSP Valid Study Plan
- GICSP Test Pattern □ Latest GICSP Study Plan □ Exam GICSP Bible □ Search on ➡ www.pdfvce.com □□□ for ➤ GICSP □ to obtain exam materials for free download □Training GICSP Pdf
- Pass Guaranteed GIAC - Accurate GICSP - Global Industrial Cyber Security Professional (GICSP) Sample Questions Answers □ Immediately open □ www.passcollection.com □ and search for 《 GICSP 》 to obtain a free download □ □Guaranteed GICSP Passing
- Pass Guaranteed GIAC - Accurate GICSP - Global Industrial Cyber Security Professional (GICSP) Sample Questions Answers □ Immediately open ➡ www.pdfvce.com □□□ and search for ⇛ GICSP ⇚ to obtain a free download □Valid Test GICSP Tips
- GICSP Valid Dumps Ebook □ Certification GICSP Torrent □ Guaranteed GICSP Passing □ Immediately open { www.torrentvalid.com } and search for □ GICSP □ to obtain a free download □GICSP Vce Test Simulator
- GIAC GICSP PDF Questions-Shortcut To Success □ Enter ➽ www.pdfvce.com □ and search for ➠ GICSP □ to download for free □GICSP Vce Test Simulator
- GICSP Vce Test Simulator □ Valid Test GICSP Tips □ Guaranteed GICSP Passing □ ⇛ www.pdfdumps.com ⇚ is best website to obtain ✔ GICSP □✔□ for free download □GICSP Valid Exam Registration
- shortcourses.russellcollege.edu.au, bacsihoangoanh.com, projectshines.com, www.stes.tyc.edu.tw, lmstaxmagic.com, a.lixy98.cn, learn.mikrajdigital.com, shortcourses.russellcollege.edu.au, demo.emshost.com, training.michalialtd.com, Disposable vapes