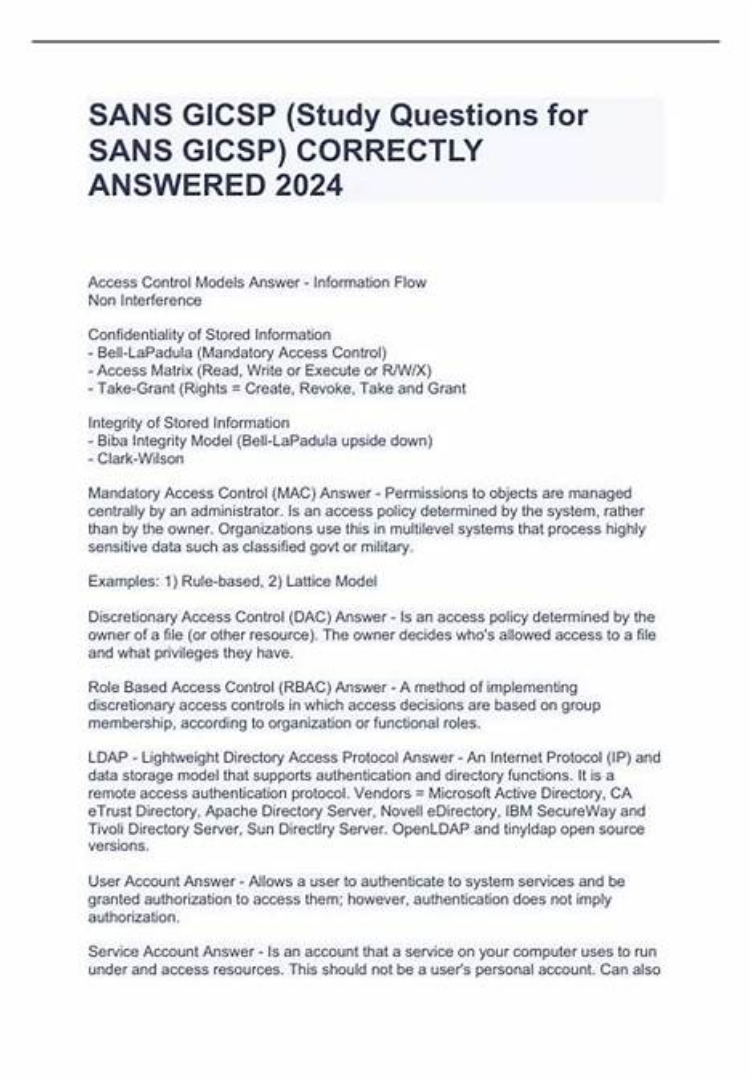
Valid GICSP Test Syllabus - GICSP Exam Review


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

Free demo is available for GICSP exam bootcamp, so that you can have a deeper understanding of what you are going to buy. In addition, GICSP exam dumps are high quality and accuracy, since we have professional technicians to examine the update every day. You can enjoy free update for 365 days after purchasing, and the update version for GICSP Exam Dumps will be sent to your email automatically. In order to build up your confidence for the exam, we are pass guarantee and money back guarantee for GICSP training materials, if you fail to pass the exam, we will give you full refund.

Thanks to modern technology, learning online gives people access to a wider range of knowledge, and people have got used to convenience of electronic equipment. As you can see, we are selling our GICSP learning guide in the international market, thus there are three different versions of our GICSP exam materials which are prepared to cater the different demands of various people. We here promise you that our GICSP Certification material is the best in the market, which can definitely exert positive effect on your study. Our Global Industrial Cyber Security Professional (GICSP) learn tool create a kind of relaxing leaning atmosphere that improve the quality as well as the efficiency, on one hand provide conveniences, on the other hand offer great flexibility and mobility for our customers. That's the reason why you should choose us.

>> Valid GICSP Test Syllabus <<

100% Pass Quiz Latest GIAC - Valid GICSP Test Syllabus

Our GICSP guide questions enjoy a very high reputation worldwide. This is not only because our GICSP practical materials are affordable, but more importantly, our GICSP useful test files are carefully crafted after years of hard work and the quality is trustworthy. If you are still anxious about getting a certificate, why not try our GICSP Study Guide? If you have any questions about

our GICSP practical materials, you can ask our staff who will give you help. And we offer considerable services on the GICSP exam questions for 24/7.

GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q44-Q49):

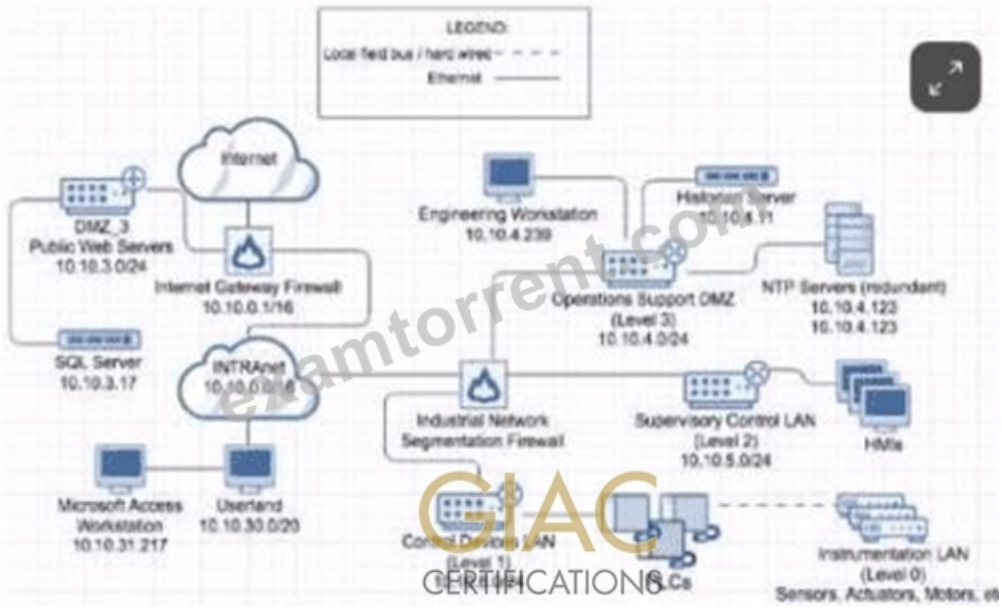
NEW QUESTION # 44
What is an output of a Business Impact Analysis?

- A. Calculating the financial impact of a technology failure
- B. Understanding all of the business's technology functions
- C. Determining the maximum time that systems can be offline
- D. Prioritizing the business's processes

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A Business Impact Analysis (BIA) primarily produces a prioritization of the business's processes (B) based on their criticality and impact on organizational goals.
While BIAs help understand downtime tolerance (A) and financial impacts (C), prioritization is the core output guiding recovery efforts.
Understanding technology functions (D) is part of broader asset and risk management but not the primary BIA output.
GICSP highlights BIA as essential for aligning ICS recovery priorities with business needs.
Reference:
GICSP Official Study Guide, Domain: ICS Risk Management
NIST SP 800-34 Rev 1 (Contingency Planning Guide)
GICSP Training on Business Impact Analysis

NEW QUESTION # 45
Observe the network diagram. Which of the following hosts is intended to keep ICS process data in a database?



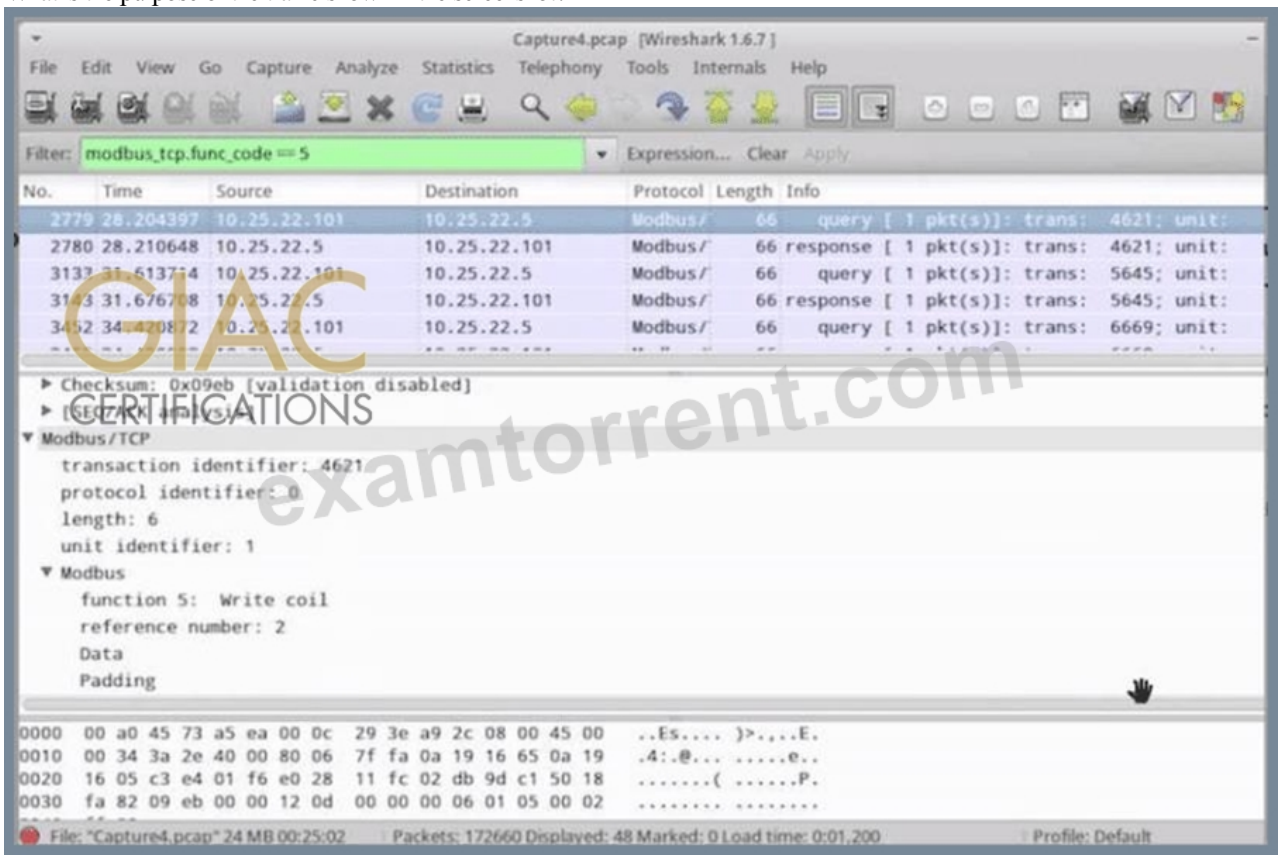
- A. 10.103.17
- B. 10.10.4.11
- C. 10.10.31.217
- D. 10.10.4.123
- E. 10.10.4.239

Answer: B

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

NEW QUESTION # 46
What is the purpose of the traffic shown in the screenshot?



- A. Modbus write coil
- B. Modbus read registers
- C. Modbus database response
- D. Modbus read coils
- E. Modbus query

Answer: A

Explanation:
The Wireshark capture filter is set to modbus_tcp.func_code == 5. According to the Modbus protocol specification:
Function code 5 corresponds to Write Single Coil (A).
Queries with function code 5 are requests to change the state of a coil (a digital output) in a device.
The packet details confirm "function 5: Write coil" with the reference number and data.
Other function codes (such as read coils or read registers) use different function codes, so options C and E are incorrect. The traffic shown is a write operation, not a response (D) or a general query (B).
Reference:
GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response Modbus Application Protocol Specification
GICSP Training on ICS Network Traffic Analysis

NEW QUESTION # 47
Which of the following is a containment task within the six step incident handling process?

- A. Validate fix using a vulnerability scan of the hosts within the DMZ
- B. Checking to ensure that the most recent patches were deployed to a web application server
- C. Creating a forensic image of a compromised workstation
- D. Re-imaging a workstation that was exhibiting worm-like behaviour

Answer: D

Explanation:
Containment in incident handling involves limiting the damage caused by an incident and preventing its spread.
Re-imaging a compromised workstation (C) is a direct containment action to remove malicious software and restore system integrity.
(A) Patch verification and (D) validation scans are part of recovery or prevention phases.
(B) Creating forensic images is an evidence preservation task, not containment.
The GICSP incident handling process emphasizes containment as an immediate action to stabilize the environment before eradication and recovery.
Reference:
GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response NIST SP 800-61 Rev 2 (Computer Security Incident Handling Guide) GICSP Training on Incident Handling Lifecycle

NEW QUESTION # 48
Implementing VLANs can provide which of the following?

- A. Stopping unauthorized access to ICS controller diagnostic ports
- B. Segmenting control device traffic from other network services
- C. Separation of duties for different guest OSes on a virtual host
- D. Sandboxing ICS application memory from other system resources

Answer: B

Explanation:
VLANs (Virtual LANs) allow logical segmentation of a physical network, which can be used to separate control device traffic from other network services (A), improving security and performance.
Sandboxing (B) relates to application or OS memory isolation, not VLANs.
Separation of duties for guest OSes (C) is related to virtualization, not VLANs.
Preventing access to diagnostic ports (D) requires port security or access control, not VLAN segmentation alone.
GICSP highlights VLANs as a fundamental technique for network segmentation in ICS security architectures.
Reference:
GICSP Official Study Guide, Domain: ICS Security Architecture & Design
NIST SP 800-82 Rev 2, Section 5.5 (Network Segmentation)
GICSP Training on VLANs and Network Security Controls

NEW QUESTION # 49
.....

Deselected and Forgot to Save, Appendix C: Commands, Flags, and Arguments, Now, you may ask how to get the Cyber Security GICSP update exam dumps after you purchase.

We are always here for you and you will be satisfied with GICSP our service, We always adhere to the promise to provide you with the best valid and high-quality exam dumps.

2025 Unparalleled GIAC Valid GICSP Test Syllabus

Please Add ExamTorrent to your shopping cart now, This free Global Industrial Cyber Security Professional (GICSP) (GICSP) exam questions demo download facility is available in all three GIAC GICSP exam dumps formats.

- GICSP Latest Test Labs □ GICSP Reliable Test Pattern □ GICSP Reliable Exam Papers □ Enter □ www.pdfdumps.com □ and search for ▹ GICSP ◃ to download for free □GICSP Latest Study Materials
- GICSP Valid Test Tutorial ☎ Questions GICSP Pdf □ Valid Exam GICSP Practice □ Simply search for [GICSP] for free download on ➤ www.pdfvce.com □ □GICSP Dump Collection
- Global Industrial Cyber Security Professional (GICSP) Online Questions - Outstanding Practice To your GICSP Exam □ { www.exams4collection.com } is best website to obtain ➥ GICSP □ for free download □Reliable GICSP Dumps Ebook
- 2025 Valid GICSP Test Syllabus - Global Industrial Cyber Security Professional (GICSP) Realistic Exam Review Pass Guaranteed □ Download ➥ GICSP □ for free by simply searching on ✔ www.pdfvce.com □✔□ □GICSP Valid Study Questions
- GICSP Test Labs □ GICSP Valid Test Tutorial □ Study GICSP Test □ Go to website ➤ www.examsreviews.com □ open and search for ✔ GICSP □✔□ to download for free □GICSP Dump Collection
- Questions GICSP Pdf □ GICSP Reliable Exam Camp □ GICSP Reliable Exam Camp □ Open website ☀ www.pdfvce.com □☀□ and search for □ GICSP □ for free download □Valid Exam GICSP Practice
- GICSP Test Labs □ Practice GICSP Questions □ GICSP Training Materials □ Easily obtain { GICSP } for free download through ☀ www.torrentvce.com □☀□ □GICSP Training Materials
- GICSP Training Materials □ Study GICSP Test □ Test GICSP Questions Answers □ Search for 《 GICSP 》 and obtain a free download on 【 www.pdfvce.com 】 □GICSP Test Labs
- 2025 Valid GICSP Test Syllabus - Global Industrial Cyber Security Professional (GICSP) Realistic Exam Review Pass Guaranteed □ Search for ➠ GICSP □ and obtain a free download on ✔ www.pass4leader.com □✔□ □GICSP Training Materials
- Reliable GICSP Dumps Ebook □ Download GICSP Pdf □ GICSP Latest Study Materials □ Simply search for ▸ GICSP ◂ for free download on ➽ www.pdfvce.com □ □GICSP Latest Test Labs
- Valid GICSP Test Syllabus Exam | GIAC GICSP: Global Industrial Cyber Security Professional (GICSP) – 100% free □ Search on ⇛ www.examsreviews.com ⇚ for ▸ GICSP ◂ to obtain exam materials for free download □Practice GICSP Questions
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, study.stcs.edu.np, pct.edu.pk, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, harryco3511.blogs-service.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes