

Realistic GIAC Reliable GICSP Exam Bootcamp Quiz



The TestBraindump guarantees their customers that if they have prepared with Global Industrial Cyber Security Professional (GICSP) (GICSP) practice test, they can pass the Global Industrial Cyber Security Professional (GICSP) (GICSP) certification easily. If the applicants fail to do it, they can claim their payment back according to the terms and conditions. Many candidates have prepared from the actual GIAC GICSP Practice Questions and rated them as the best to study for the examination and pass it in a single try with the best score. The GIAC GICSP practice material of TestBraindump came into existence after consultation with many professionals and getting their positive reviews.

For a long time, our company is insisting on giving back to our customers. Also, we have benefited from such good behavior. Our GICSP exam prep has gained wide popularity among candidates. Every worker in our company sticks to their jobs all the time. No one complain about the complexity of their jobs. Our researchers and experts are working hard to develop the newest version GICSP Study Materials. So please rest assured that we are offering you the most latest GICSP learning questions.

>> **Reliable GICSP Exam Bootcamp** <<

First-class GICSP Exam Dumps supply you high-quality Practice Materials - TestBraindump

Our GICSP study materials boost the self-learning and self-evaluation functions so as to let the clients understand their learning results and learning process, then find the weak links to improve them. Through the self-learning function the learners can choose the learning methods by themselves and choose the contents which they think are important. Through the self-evaluation function the learners can evaluate their mastery degree of our GICSP Study Materials and their learning process. The two functions can help the learners adjust their learning arrangements and schedules to efficiently prepare the exam.

GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q35-Q40):

NEW QUESTION # 35

Which of the following is a team of incident responders that often coordinate with organizations and law enforcement to reduce risks and advise on security threats?

- A. CVE
- B. CVSS
- **C. CERT**
- D. COBIT

Answer: C

Explanation:

CERT (Computer Emergency Response Team) (C) is a designated group of cybersecurity experts who provide incident response, threat intelligence, and coordination with organizations and law enforcement to manage and reduce cybersecurity risks.

CVE (A) is a list of publicly disclosed vulnerabilities.

COBIT (B) is a framework for IT governance and management.

CVSS (D) is a scoring system for vulnerabilities.

GICSP highlights CERTs as critical entities in incident handling and collaborative cyber defense.

Reference:

GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response CERT Coordination Center (Carnegie Mellon University) GICSP Training on Incident Response and Coordination

NEW QUESTION # 36

Implementing VLANs can provide which of the following?

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

Answer: D

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 # 37

What is a benefit of MECM over WSUS?

- A. Minimal system resource use
- B. Lower operating and product cost
- C. Lower configuration and management overhead
- **D. Hardware and software inventory control**

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Microsoft Endpoint Configuration Manager (MECM) provides advanced features compared to Windows Server Update Services (WSUS), including:

Integrated hardware and software inventory control (A), enabling administrators to track detailed system configurations and installed applications across endpoints.

WSUS primarily focuses on patch deployment and update management without comprehensive inventory capabilities.

MECM's enhanced management capabilities justify its greater resource use and complexity, making it more suitable for enterprise-scale patching and asset management in ICS environments.

Reference:

GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response Microsoft MECM vs WSUS Feature Comparison (Referenced in GICSP Training) GICSP Training on Patch and Configuration Management

NEW QUESTION # 38

Which of the following is typically performed during the Recovery phase of incident response?

- **A. Patching and configuring systems to meet established secure configuration standards.**
- B. Making a forensic image of the system(s) involved in the incident.
- C. Updating the organization's security policies to prevent future breaches.

- D. Finding the root cause or vector used by the attacker to gain entry and maintain access.

Answer: A

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 # 39

Martin is writing a document that describes in general terms how to secure embedded operating systems. The document includes issues that are specific to embedded devices vs desktop and laptop operating systems.

However, it does not call out specific flavors and versions of embedded operating systems. Which type of document is Martin writing?

- **A. Guideline**
- B. Policy
- C. Procedure
- D. Standard

Answer: A

Explanation:

A Guideline (A) provides general recommendations and best practices without mandatory requirements or detailed instructions.

Procedures (B) are step-by-step instructions for specific tasks.

Standards (C) specify mandatory requirements, often with measurable criteria.

Policies (D) establish high-level organizational directives and rules.

Martin's document provides general, non-mandatory advice applicable broadly, fitting the definition of a guideline.

Reference:

GICSP Official Study Guide, Domain: ICS Security Governance & Compliance NIST SP 800-53 Rev 5 (Security Control Documentation Types) GICSP Training on Security Documentation and Governance

NEW QUESTION # 40

.....

The GIAC GICSP questions certificates are the most sought-after qualifications for those looking to further their careers in the business. To get the GIAC GICSP exam questions credential, candidates must pass the GIAC GICSP exam. But what should you do if you want to pass the GIAC Global Industrial Cyber Security Professional (GICSP) exam questions the first time? Fortunately, TestBraindump provides its users with the most recent and accurate GIAC GICSP Questions to assist them in preparing for their real GICSP exam. Our GIAC GICSP exam dumps and answers have been verified by GIAC certified professionals in the area.

Latest GICSP Exam Papers: <https://www.testbraindump.com/GICSP-exam-prep.html>

Why do we have confidence that every user can pass exam with our GICSP dumps PDF, GIAC Reliable GICSP Exam Bootcamp More importantly, the demo from our company is free for all people, Convenience, Exam GICSP is just a piece of cake if you have prepared for the exam with the help of it's exceptional study material, Secure System By TestBraindump Latest GICSP Exam Papers: We maintain the privacy of your data and provide the software at discounted rates.

Learning to use AV Foundation is the key Certification GICSP Torrent to building the next generation of media applications for Mac OS X and iOS, Active Directory Domain Services Primer, Why do we have confidence that every user can pass exam with our GICSP Dumps PDF?

Clearing Exam isnt Difficult with Real GIAC GICSP Questions

More importantly, the demo from our company is free for all people, Convenience, Exam GICSP is just a piece of cake if you have prepared for the exam with the help of it's exceptional study material.

Secure System By TestBraindump: We maintain GICSP the privacy of your data and provide the software at discounted rates.

- [illegible]