

GIAC GICSP Exam Fee - GICSP Pdf Demo Download



GICSP exam study material have a 99% pass rate. What does this mean? As long as you purchase GICSP exam simulating and you are able to persist in your studies, you can basically pass the exam. This passing rate is not what we say out of thin air. This is the value we obtained from analyzing all the users' exam results. It can be said that choosing GICSP study engine is your first step to pass the exam. If your job is very busy and there is not much time to specialize, and you are very eager to get a certificate to prove yourself, it is very important to choose our GICSP Exam simulating. I know that the 99% pass rate of GICSP exam must have attracted you. Do not hesitate anymore. You will never regret buying GICSP study engine!

Do you have registered for the GIAC GICSP exam and are worried about GIAC GICSP exam preparation? Try GIAC GICSP PDF Questions and practice tests which help you prepare the whole course in less duration. The GIAC GICSP practice test material gives you a clear idea to prepare for the GIAC GICSP Exam and saves you preparation time. An GICSP exam is a time-based exam, and the candidate must be fast enough to solve the problems in a limited time.

>> **GIAC GICSP Exam Fee** <<

GICSP Pdf Demo Download & GICSP Instant Discount

It can be said that all the content of the GICSP study materials are from the experts in the field of masterpieces, and these are understandable and easy to remember, so users do not have to spend a lot of time to remember and learn. It takes only a little practice on a daily basis to get the desired results. Especially in the face of some difficult problems, the user does not need to worry too much, just learn the GICSP Study Materials provide questions and answers, you can simply pass the exam. This is a wise choice, and in the near future, after using our GICSP training materials, you will realize your dream of a promotion and a raise, because your pay is worth the rewards.

GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q27-Q32):

NEW QUESTION # 27

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

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

Answer: B

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 # 28

A brewer uses a local HMI to communicate with a controller that opens a pump to move the work from the boil kettle to the fermenter. What level of the Purdue model would the controller be considered?

- A. Level 4
- **B. Level 1**
- C. Level 3
- D. Level 2
- E. Level 0

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The Purdue Enterprise Reference Architecture (PERA) model, commonly used in ICS security frameworks like GICSP, segments industrial control systems into hierarchical levels that correspond to the function and control of devices:

Level 0: Physical process (sensors and actuators directly interacting with the process) Level 1: Basic control level (controllers such as PLCs or DCS controllers that execute control logic and command actuators) Level 2: Supervisory control (HMIs, SCADA supervisory systems that interface with controllers) Level 3: Operations management (Manufacturing Execution Systems, batch control, production scheduling) Level 4: Enterprise level (business systems, ERP, corporate IT) In this scenario, the controller opening the pump is a device executing control logic directly on the process, placing it at Level 1. The local HMI used to communicate with the controller is at Level 2, supervising and providing operator interface.

This classification is foundational in GICSP's ICS Fundamentals and Architecture domain, which emphasizes clear understanding of network segmentation and device role for security zoning.

Reference:

GICSP Official Study Guide, Domain: ICS Fundamentals & Architecture

Purdue Model description in IEC 62443 and NIST SP 800-82

GICSP Training materials on Purdue Model and Network Segmentation

NEW QUESTION # 29

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

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

Answer: D

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 # 30

What is a benefit of log aggregation?

- **A. Assists in analysis of log data from multiple sources**
- B. Simplifies initial setup of logging in the environment
- C. Reduces system load on logging devices
- D. Eliminates the need for baselining normal log activity

Answer: A

Explanation:

Log aggregation involves collecting log data from multiple devices and systems into a centralized repository.

This provides a holistic view of the environment and enables security teams to correlate events across disparate sources. The key benefit of log aggregation is that it:

Assists in analysis of log data from multiple sources (D) by providing a unified platform for searching, filtering, and correlating events, enabling quicker detection of security incidents and comprehensive forensic investigations.

While log aggregation can help improve management, it does not simplify initial setup (A), nor does it inherently reduce system load (B) because devices still generate logs locally. It also does not eliminate the need for baselining normal activity (C), which remains essential for detecting anomalies.

GICSP stresses centralized logging as a critical component of effective ICS security monitoring and incident response.

Reference:

GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response NIST SP 800-92 (Guide to Computer Security Log Management) GICSP Training Materials on Security Monitoring and Incident Analysis

NEW QUESTION # 31

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. 10.10.4.239
- D. 10.10.4.123
- E. 10.10.31.217

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 # 32

.....

As you know, today's society is changing very fast. We also need new knowledge to fill in as we learn. And our GICSP learning prep can suit you most in this need for you will get the according certification as well as the latest information. GICSP Exam simulation is selected by many experts and constantly supplements and adjust our questions and answers. When you use our GICSP study materials, you can find the information you need at any time.

GICSP Pdf Demo Download: <https://www.vceprep.com/GICSP-latest-vce-prep.html>

GIAC GICSP Exam Fee The selection of Q&As format has multiple advantages for the exam takers, Using VCEPrep GICSP Pdf Demo Download exam dumps, you will achieve success, And our online test engine and the windows software of the GICSP guide

- [illegible]