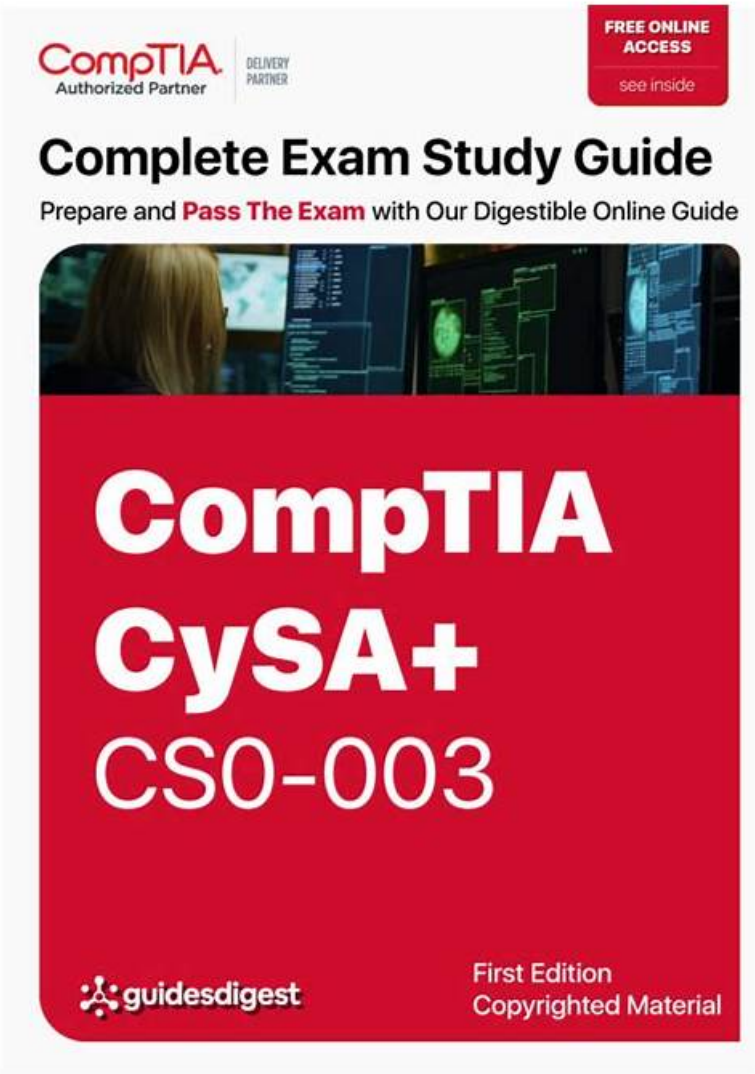
有効的CS0-003｜最高のCS0-003試験問題解説集試験｜試験の準備方法CompTIA Cybersecurity Analyst (CySA+) Certification Exam受験記対策



BONUS！！！ GoShiken CS0-003ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1szZrRMrkdfD6-EOB3mCakXNbsPDMk0kv

最も少ない時間とお金でCompTIA　CS0-003認定試験に高いポイントを取得したいですか。短時間で一度に本当の認定試験に高いポイントを取得したいなら、我々GoShikenのCompTIA　CS0-003日本語対策問題集は絶対にあなたへの最善なオプションです。このいいチャンスを把握して、GoShikenのCS0-003試験問題集の無料デモをダウンロードして勉強しましょう。

CompTIA CS0-003 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• セキュリティ運用:潜在的に悪意のあるアクティビティの指標の分析、悪意のあるアクティビティを判断するためのツールと技術の使用、脅威インテリジェンスと脅威ハンティングの概念の比較、セキュリティ運用における効率とプロセス改善の重要性の説明に重点を置いています。

トピック 2	• インシデント対応と管理: 攻撃手法のフレームワークを中心に、インシデント対応活動の実行、ライフ サイクルの準備段階とインシデント後の段階について説明します。
トピック 3	• 報告とコミュニケーション: このトピックでは、脆弱性管理とインシデント対応の報告とコミュニケーションの重要性について説明することに重点を置いています。
トピック 4	• 脆弱性管理: このトピックでは、脆弱性スキャン方法の実装、脆弱性評価ツールの出力の分析、脆弱性に優先順位を付けるためのデータ分析、問題を軽減するための管理の推奨について説明します。このトピックは、脆弱性への対応、処理、管理にも焦点を当てています。

CS0-003受験記対策 & CS0-003模擬体験

皆様はCS0-003試験を準備するとき、我々のサイトで最新の問題集を参考として練習することができます。そうしたら、CS0-003試験の復習の中で多くの時間を節約することができます。CompTIA試験は複雑ではなく、弊社の問題集でよく復習すれば簡単です。我々の問題集は受験生の合格を保証することができます。

CompTIA Cybersecurity Analyst (CySA+) Certification Exam 認定 CS0-003 試験問題 (Q284-Q289):

質問 # 284
Which of the following actions would an analyst most likely perform after an incident has been investigated?

- A. Tabletop exercise
- B. Incident response plan
- C. Risk assessment
- D. Root cause analysis

正解：A

解説：
A tabletop exercise is the most likely action that an analyst would perform after an incident has been investigated. A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and decision-makers of the organization. The purpose of a tabletop exercise is to evaluate the effectiveness of the incident response plan, identify the gaps and weaknesses in the plan, and improve the communication and coordination among the incident response team and other parties. A tabletop exercise can help the analyst to learn from the incident investigation, test the assumptions and recommendations made during the investigation, and enhance the preparedness and resilience of the organization for future incidents12. Risk assessment, root cause analysis, and incident response plan are all actions that an analyst would perform before or during an incident investigation, not after. Risk assessment is the process of identifying, analyzing, and evaluating the risks that may affect the organization. Root cause analysis is the method of finding the underlying or fundamental causes of an incident. Incident response plan is the document that defines the roles, responsibilities, procedures, and resources for responding to an incident345. References:
Tabletop Exercises: Six Scenarios to Help Prepare Your Cybersecurity Team, Tabletop Exercises for Incident Response - SANS Institute, Risk Assessment - NIST, Root Cause Analysis - OWASP, Incident Response Plan
| Ready.gov

質問 # 285
Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

- A. BIA
- B. MOU
- C. NDA
- D. SLA

正解：D

解説：
SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements. Official References:
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.comptia.org/certifications/cybersecurity-analyst
https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

質問 # 286
A security analyst needs to automate the incident response process for malware infections. When the following logs are generated, an alert email should automatically be sent within 30 minutes:
Which of the following is the best way for the analyst to automate alert generation?

- A. Create a custom rule on a SIEM
- B. Install a UEBA-capable antivirus
- C. Implement email protection with SPF
- D. Deploy a signature-based IDS

正解：A

解説：
A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A security analyst can create a custom rule on a SIEM system to automate the incident response process for malware infections. For example, the analyst can create a rule that triggers an alert email when the SIEM system detects logs that match the criteria of malware infection, such as process name, file name, file hash, etc. The alert email can be sent within 30 minutes or any other desired time frame. The other options are not suitable or sufficient for this purpose. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15;
https://www.sans.org/reading-room/whitepapers/analyst/security-information-event-management-siem-implementation-33969

質問 # 287
Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

- A. To verify the roles of the incident response team
- B. To perform tests against implemented security controls
- C. To provide recommendations for handling vulnerabilities
- D. TO provide metrics and test continuity controls

正解：D

解説：
The correct answer is A. To provide metrics and test continuity controls.
A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization.
A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues .
The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization's systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization's systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

質問 # 288
An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

- A. CIS Benchmarks
- B. PCI DSS
- C. ISO 27001
- D. OWASP Top Ten

正解：A

解説：
The best resource to ensure secure configuration of cloud infrastructure is
A) CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1
PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

質問 # 289
.....

id=1szZrRMrkdfD6-EOB3mCakXNbsPDMk0kv