SY0-701 Praxisprüfung - SY0-701 Deutsche

Außerdem sind jetzt einige Teile dieser ExamFragen SY0-701 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1ImlP8Vn74xX0NgKrBwDx3_5HjlexY-gQ

Sorgen Sie noch darum, dass Sie keine autoritäre Lehrbücher über die CompTIA SY0-701 Prüfung finden können? Leute aus aller Welt möchten die CompTIA SY0-701 Zertifizierungsprüfung wählen. ExamFragen ist die einzigartige Webseite, die Ihnen hochwertige Schulungsunterlagen zur CompTIA SY0-701 Zertifizierung bietet. Wenn Sie noch besorgt sind, können Sie einen Teil der kostenlosen Zertifizierungsantworten herunterlagen, bevor Sie die SY0-701 Schulungsunterlagen von ExamFragen kaufen.

CompTIA SY0-701 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Security Architecture: Here, you'll learn about security implications across different architecture models, applying security principles to secure enterprise infrastructure in scenarios, and comparing data protection concepts and strategies. The topic also delves into the importance of resilience and recovery in security architecture.
Thema 2	• General Security Concepts: This topic covers various types of security controls, fundamental security concepts, the importance of change management processes in security, and the significance of using suitable cryptographic solutions.
Thema 3	• Security Operations: This topic delves into applying common security techniques to computing resources, addressing security implications of proper hardware, software, and data asset management, managing vulnerabilities effectively, and explaining security alerting and monitoring concepts. It also discusses enhancing enterprise capabilities for security, implementing identity and access management, and utilizing automation and orchestration for secure operations.
Thema 4	• Threats, Vulnerabilities, and Mitigations: In this topic, you'll find discussions comparing threat actors and motivations, explaining common threat vectors and attack surfaces, and outlining different types of vulnerabilities. Moreover, the topic focuses on analyzing indicators of malicious activity in scenarios and exploring mitigation techniques used to secure enterprises against threats.

Thema 5	• Security Program Management and Oversight: Finally, this topic discusses elements of effective security governance, the risk management process, third-party risk assessment, and management processes. Additionally, the topic focuses on security compliance requirements, types and purposes of audits and assessments, and implementing security awareness practices in various scenarios.

>> SY0-701 Praxisprüfung <<

SY0-701 Deutsche, SY0-701 Fragenpool

Möchten Sie wissen , woher unsere Konfidenz für CompTIA SY0-701 kommt? Lassen Sie mich erzählen. Zuerst, ExamFragen besitzt eine sehr erfahrene Gruppe, die Prüfungssoftware entwickelt. Zweitens, zahlose Kunden haben nach dem Benutzen unserer Produkte die CompTIA SY0-701 Prüfung bestanden. Die Zertifizierung der CompTIA SY0-701 wird weltweit anerkennt. Möchten Sie diese Zertifizierung besitzen? Mit Hilfe unserer CompTIA SY0-701 Prüfungssoftware können Sie auch unbelastet erwerben!

CompTIA Security+ Certification Exam SY0-701 Prüfungsfragen mit Lösungen (Q697-Q702):

697. Frage
A security analyst receives an alert from a corporate endpoint used by employees to issue visitor badges. The alert contains the following details:

Source Host	Destination Host	Port	Protocol	Action
FrontDesk1	DC01	445	TCP	Fail
FrontDesk1	DC02	445	TCP	Fail
FrontDesk1	File1	445	TCP	Connect
FrontDesk1	File2	445	TCP	Connect
FrontDesk1	FDesk2	445	TCP	Connect
FrontDesk1	Office1	445	TCP	Fail
FrontDesk1	Exchange1	445	TCP	Fail
FrontDesk1	Exchange2	445	TCP	Fail
FrontDesk1	Office3	445	TCP	Connect
FrontDesk1	Office4	445	TCP	Connect
FrontDesk1	ITSupport11	445	TCP	Connect

Which of the following best describes the indicator that triggered the alert?

- A. Brute-force attack
- B. Blocked content
- C. Account lockout
- D. Concurrent session usage

Antwort: A

Begründung:
Detailed Explanation:The activity described in the table, where multiple connection attempts are made on port 445 (used for SMB services), suggests a brute-force attack. The attacker likely used automated methods to guess credentials, causing multiple failures. Such attempts are a hallmark of brute-force attacks targeting shared resources. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Indicators of Malicious Activity".

698. Frage
A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

- A. A thorough analysis of the supply chain
- B. An in-depth penetration test of all suppliers and vendors
- C. A right to audit clause in vendor contracts and SOWs
- D. A legally enforceable corporate acquisition policy

Antwort: A

Begründung:
Counterfeit hardware is hardware that is built or modified without the authorization of the original equipment manufacturer (OEM). It can pose serious risks to network quality, performance, safety, and reliability12. Counterfeit hardware can also contain malicious components that can compromise the security of the network and the data that flows through it3. To address the risks associated with procuring counterfeit hardware, a company should conduct a thorough analysis of the supply chain, which is the network of entities involved in the production, distribution, and delivery of the hardware. By analyzing the supply chain, the company can verify the origin, authenticity, and integrity of the hardware, and identify any potential sources of counterfeit or tampered products. A thorough analysis of the supply chain can include the following steps:
* Establishing a trusted relationship with the OEM and authorized resellers
* Requesting documentation and certification of the hardware from the OEM or authorized resellers
* Inspecting the hardware for any signs of tampering, such as mismatched labels, serial numbers, or components
* Testing the hardware for functionality, performance, and security
* Implementing a tracking system to monitor the hardware throughout its lifecycle
* Reporting any suspicious or counterfeit hardware to the OEM and law enforcement agencies References = 1: Identify Counterfeit and Pirated Products - Cisco, 2: What Is Hardware Security? Definition, Threats, and Best Practices, 3: Beware of Counterfeit Network Equipment - TechNewsWorld, : Counterfeit Hardware: The Threat and How to Avoid It

699. Frage
An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

- A. Building a load-balanced VPN solution with redundant internet
- B. Purchasing a low-cost SD-WAN solution for VPN traffic
- C. Deploying a SASE solution to remote employees
- D. Using a cloud provider to create additional VPN concentrators

Antwort: C

Begründung:
SASE stands for Secure Access Service Edge. It is a cloud-based service that combines network and security functions into a single integrated solution. SASE can help reduce traffic on the VPN and internet circuit by providing secure and optimized access to the data center and cloud applications for remote employees. SASE can also monitor and enforce security policies on the remote employee internet traffic, regardless of their location or device. SASE can offer benefits such as lower costs, improved performance, scalability, and flexibility compared to traditional VPN solutions. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457-458 1

700. Frage
A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?

- A. Rescan the network.
- B. Submit a report.
- C. Conduct an audit.
- D. Initiate a penetration test.

Antwort: A

Begründung:
Explanation
After completing a vulnerability assessment and remediating the identified vulnerabilities, the next step is to rescan the network to verify that the vulnerabilities have been successfully fixed and no new vulnerabilities have been introduced. A vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network, system, or application that could be exploited by attackers. A vulnerability assessment typically involves using automated tools, such as scanners, to scan the network and generate a report of the findings. The report may include information such as the severity, impact, and remediation of the vulnerabilities. The operations team is responsible for applying the appropriate patches, updates, or configurations to address the vulnerabilities and reduce the risk to the network. A rescan is necessary to confirm that the remediation actions have been effective and that the network is secure.
Conducting an audit, initiating a penetration test, or submitting a report are not the next steps after completing a vulnerability assessment and remediating the vulnerabilities. An audit is a process of reviewing and verifying the compliance of the network with the established policies, standards, and regulations. An audit may be performed by internal or external auditors, and it may use the results of the vulnerability assessment as part of the evidence. However, an audit is not a mandatory step after a vulnerability assessment, and it does not validate the effectiveness of the remediation actions.
A penetration test is a process of simulating a real-world attack on the network to test the security defenses and identify any gaps or weaknesses. A penetration test may use the results of the vulnerability assessment as a starting point, but it goes beyond scanning and involves exploiting the vulnerabilities to gain access or cause damage. A penetration test may be performed after a vulnerability assessment, but only with the proper authorization, scope, and rules of engagement. A penetration test is not a substitute for a rescan, as it does not verify that the vulnerabilities have been fixed.
Submitting a report is a step that is done after the vulnerability assessment, but before the remediation. The report is a document that summarizes the findings and recommendations of the vulnerability assessment, and it is used to communicate the results to the stakeholders and the operations team. The report may also include a follow-up plan and a timeline for the remediation actions. However, submitting a report is not the final step after the remediation, as it does not confirm that the network is secure.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 372-375; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 0:00 - 8:00.

701. Frage
A systems administrator receives the following alert from a file integrity monitoring tool:
The hash of the cmd.exe file has changed.
The systems administrator checks the OS logs and notices that no patches were applied in the last two months.
Which of the following most likely occurred?

- A. A snapshot of the file system was taken.
- B. A rootkit was deployed.
- C. The end user changed the file permissions.
- D. A cryptographic collision was detected.

Antwort: B

Begründung:
Explanation
A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 147. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2, page 9.

702. Frage
.....

Die CompTIA SY0-701 Zertifizierungsprüfung ist eine sehr populäre Prüfung. Obwohl es sehr schwierig zu bestehen ist, können Sie diese Prüfung leichter bestehen, wenn Sie die richtige Methode finden. Und Wir ExamFragen sind Ihre beste Wahl. Mit der 100%-Hitrate Prüfungsunterlagen von ExamFragen können Sie alle Probleme in der CompTIA SY0-701 Zertifizierungsprüfung auslösen. Wenn Sie die Prüfungsfragen und Testantworten ernst lernen, gibt es keine Probleme für Sie. Und nach dem Kauf können Sie einjährigen kostlosen Aktualisierungsservice bekommen. (innerhalb einem Jahr) Sie können über die gewünschten CompTIA SY0-

701 Schulungsunterlagen beherrschen, wenn Sie auf jeden Fall die neueste Version bekommen. Probieren Sie sofort, bitte.

SY0-701 Deutsche: https://www.examfragen.de/SY0-701-pruefung-fragen.html

- Valid SY0-701 exam materials offer you accurate preparation dumps □ Erhalten Sie den kostenlosen Download von ➡ SY0-701 □□□ mühelos über 「 www.itzert.com 」 □SY0-701 Zertifizierungsantworten
- SY0-701 Testantworten ♣ SY0-701 Fragen Und Antworten □ SY0-701 Deutsch Prüfung □ Suchen Sie jetzt auf ✔ www.itzert.com □✔□ nach ➤ SY0-701 □ und laden Sie es kostenlos herunter □SY0-701 Testantworten
- SY0-701 Studienmaterialien: CompTIA Security+ Certification Exam - SY0-701 Zertifizierungstraining □ Suchen Sie jetzt auf ➤ www.itzert.com □ nach ➥ SY0-701 □ um den kostenlosen Download zu erhalten □SY0-701 Prüfung
- SY0-701 Testantworten □ SY0-701 Quizfragen Und Antworten □ SY0-701 Prüfung □ Erhalten Sie den kostenlosen Download von ➡ SY0-701 □□□ mühelos über ➥ www.itzert.com □ □SY0-701 Prüfungsfragen
- SY0-701 Schulungsangebot - SY0-701 Simulationsfragen - SY0-701 kostenlos downloden ☀ Suchen Sie einfach auf { www.it-pruefung.com } nach kostenloser Download von ➠ SY0-701 □ □SY0-701 Prüfungsfragen
- SY0-701 Exam □ SY0-701 Fragen Und Antworten □ SY0-701 Zertifizierungsfragen □ Suchen Sie auf ⇛ www.itzert.com ⇚ nach （ SY0-701 ） und erhalten Sie den kostenlosen Download mühelos □SY0-701 Demotesten
- SY0-701 Testking □ SY0-701 Online Tests □ SY0-701 Prüfung □ Sie müssen nur zu { www.examfragen.de } gehen um nach kostenloser Download von ➽ SY0-701 □ zu suchen □SY0-701 Zertifizierungsantworten
- SY0-701 Fragenkatalog □ SY0-701 Deutsch Prüfung □ SY0-701 Online Tests □ Suchen Sie einfach auf ⇛ www.itzert.com ⇚ nach kostenloser Download von ➠ SY0-701 □ □SY0-701 Quizfragen Und Antworten
- SY0-701 Übungsmaterialien - SY0-701 Lernführung: CompTIA Security+ Certification Exam - SY0-701 Lernguide □ Suchen Sie einfach auf □ www.echtefrage.top □ nach kostenloser Download von ▸ SY0-701 ◂ □SY0-701 Demotesten
- SY0-701 Übungsmaterialien - SY0-701 Lernführung: CompTIA Security+ Certification Exam - SY0-701 Lernguide Ⓜ Suchen Sie auf □ www.itzert.com □ nach kostenlosem Download von [SY0-701] □SY0-701 Deutsch Prüfung
- SY0-701 Examengine □ SY0-701 Quizfragen Und Antworten □ SY0-701 Fragenkatalog □ Öffnen Sie die Webseite ▹ www.deutschpruefung.com ◃ und suchen Sie nach kostenloser Download von ➠ SY0-701 □ □SY0-701 Prüfungen
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, visionskillacademy.com, owners111.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, Disposable vapes

Laden Sie die neuesten ExamFragen SY0-701 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1ImlP8Vn74xX0NgKrBwDx3_5HjlexY-gQ