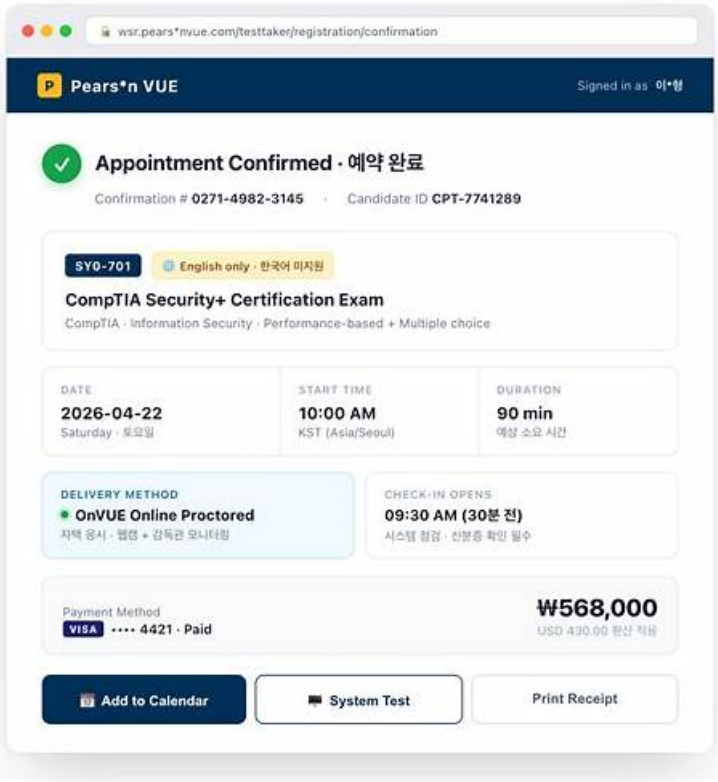
100%유효한SY0-701인증시험대비공부자료시험대비자료



DumpTOP SY0-701 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요: https://drive.google.com/open?id=13gX7redL-zjPTp8p_Uk0DXNB7VnNcFaG

CompTIA인증 SY0-701시험이 너무 어려워 보여서 오르지못할 산처럼 보이시나요? 그건DumpTOP의 CompTIA인증 SY0-701시험문제에 대비하여 제작한CompTIA인증 SY0-701덤프가 있다는 것을 모르고 있기때문입니다. CompTIA인증 SY0-701시험에 도전하고 싶으시다면 최강 시험패스율로 유명한DumpTOP의 CompTIA인증 SY0-701덤프로 시험공부를 해보세요.시간절약은 물론이고 가격도 착해서 간단한 시험패스에 딱 좋은 선택입니다.

CompTIA SY0-701 Exam Overview:

Certification Vendor:	CompTIA
Exam Name:	CompTIA Security+ Certification Exam
Exam Number:	SY0-701
Certificate Validity Period:	3 years
Exam Format:	Multiple-choice questions, Performance-based questions
Available Languages:	English, Japanese, Portuguese, Spanish
Exam Price:	$425 USD
Exam Duration:	90 minutes
Related Certifications:	CompTIA Network+ CompTIA CySA+ CompTIA PenTest+
Real Exam Qty:	Up to 90
Passing Score:	750 (scale 100–900)
Recommended Training:	CompTIA CertMaster Learn CompTIA Security+ Official Study Guide

Exam Registration:	Pearson VUE Test Registration CompTIA Official Registration
Sample Questions:	CompTIA SY0-701 Sample Questions
Exam Way:	Online proctored or in-person at authorized test centers
Pre Condition:	No mandatory prerequisites; recommended: CompTIA Network+ certification and 2 years of IT administration experience with security focus
Official Syllabus URL:	https://www.comptia.org/certifications/security

>> SY0-701인증시험대비 공부자료 <<

SY0-701시험대비 최신버전 공부자료, SY0-701덤프

지금21세기 IT업계가 주목 받고 있는 시대에 그 경쟁 또한 상상할만하죠, 당연히 it업계 중CompTIA SY0-701인증시험도 아주 인기가 많은 시험입니다. 응시자는 매일매일 많아지고 있으며, 패스하는 분들은 관련it업계에서 많은 지식과 내공을 지닌 분들뿐입니다.

CompTIA SY0-701 시험요강:

주제	소개
주제 1	• 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.
주제 2	• 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.
주제 3	• 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.
주제 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.
주제 5	• 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.

최신 CompTIA Security+ SY0-701 무료샘플문제 (Q257-Q262):

질문 # 257
An attacker defaces a company's website and refuses to relinquish control until the company removes specific harmful chemicals from its products. Which of the following best describes this type of threat actor?

- A. Unskilled attacker
- B. Organized crime
- C. Hacktivist
- D. Espionage

정답：C

설명:
A hacktivist uses cyberattacks, such as website defacement, to advance a political or social agenda. In this case, the attacker's demand to remove harmful chemicals reflects an ideological motive, characteristic of hacktivism.

질문 # 258
Which of the following is the most appropriate reason for a server technician to disable unused ports and services on an externally facing DNS server?

- A. To block ports not currently blocked by the network firewall
- B. To limit the attack surface area
- C. To conserve system memory
- D. To reduce the need for patching

정답: B

설명:
The best reason to disable unused ports and services is to limit the attack surface area. An externally facing DNS server is exposed to untrusted networks, so every unnecessary service, listener, protocol, or open port becomes another possible path for exploitation. Hardening the server by disabling unused services reduces opportunities for attackers to discover vulnerable software, abuse misconfigurations, or pivot into the environment. This does not remove the need for patching; all remaining software must still be maintained.
Blocking ports at the firewall is useful, but host-level hardening is still required because firewall rules can be misconfigured or bypassed internally. Conserving memory is not the security objective. Attack surface reduction is the correct rationale.

질문 # 259
A security analyst needs to harden access to a network. One of the requirements is to authenticate users with smart cards. Which of the following should the analyst enable to best meet this requirement?

- A. CHAP
- B. EAP-TLS
- C. PEAP
- D. MS-CHAPv2

정답: B

설명:
EAP-TLS is a strong and secure authentication method that involves the use of digital certificates, typically stored on smart cards, for user authentication. It requires the user to present a valid certificate, which is verified by the authentication server, providing a high level of security.

질문 # 260
While performing digital forensics, which of the following is considered the most volatile and should have the contents collected first?

- A. SSD
- B. RAM
- C. Hard drive
- D. Temporary files

정답: B

설명:
When the computer powers off, anything in the RAM is going to be lost. Therefore, collecting potential evidence out of the RAM is the first thing that should be done out of these options.

질문 # 261
A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should

the hosting provider consider first?

- A. Time zone differences in log correlation
- B. Impacts to existing contractual obligations
- C. Local data protection regulations
- D. Risks from hackers residing in other countries

정답：C

설명：
Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders.
Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States.
A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage.
Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269.
CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

질문 # 262
.....