Regualer SY0-701 Update - SY0-701 Test Simulator Fee

In this era, everything is on the rise. Do not you want to break you own? Double your salary, which is not impossible. Through the CompTIA SY0-701 Exam, you will get what you want. ITExamSimulator will provide you with the best training materials, and make you pass the exam and get the certification. It's a marvel that the pass rate can achieve 100%. This is indeed true, no doubt, do not consider, act now.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 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.
Topic 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.
Topic 4	• 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.

Topic 5	• 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.

Free PDF CompTIA - High Pass-Rate SY0-701 - Regualer CompTIA Security+ Certification Exam Update

Life will always face a lot of choices. When we choose to work, we will also be selected by the job in reverse. And today, in an era of fierce competition, how can we occupy a place in a market where talent is saturated? The answer is a certificate. What the certificate main? All kinds of the test CompTIA certification, prove you through all kinds of qualification certificate, it is not hard to find, more and more people are willing to invest time and effort on the SY0-701 Study Materials, because get the test SY0-701 certification is not an easy thing, so, a lot of people are looking for an efficient learning method. And here, fortunately, you have found the SY0-701 study materials, a learning platform that can bring you unexpected experiences.

CompTIA Security+ Certification Exam Sample Questions (Q280-Q285):

NEW QUESTION # 280
An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

- A. Compromise
- B. Retention
- C. Inventory
- D. Analysis
- E. Transfer

Answer: B

Explanation:
A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security.
References
* CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211
* CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832

NEW QUESTION # 281
Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

- A. Resource reuse
- B. Jailbreaking
- C. Memory injection
- D. Side loading

Answer: D

Explanation:
Explanation
Side loading is the process of installing software outside of a manufacturer's approved software repository.
This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices. References = Sideloading - CompTIA

NEW QUESTION # 282

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

- A. Recovery
- B. Preparation
- C. Analysis
- D. Lessons learned

Answer: B

Explanation:
Explanation
Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the impact and duration of the incident.
Some of the activities that a security analyst performs during the preparation phase are:
Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor.
Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.
Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.
Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.
Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.
Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.
Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.
References:
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section
6.4: Secure Systems Design, p. 279-280
CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.5: Given a scenario, implement secure network architecture concepts, Sub-objective:
Incident response, p. 16

NEW QUESTION # 283

A security team purchases a tool for cloud security posture management. The team is quickly overwhelmed by the number of misconfigurations the tool detects. Which of the following should the security team configure to establish secure baselines for cloud resource usage?

- A. Guardrails
- B. XDR
- C. CASB
- D. IAM

Answer: A

Explanation:
Guardrails define and enforce organization-specific policies and secure configuration baselines in cloud environments, automatically detecting and preventing deviations from approved settings.

NEW QUESTION # 284

After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

- A. Corrective
- B. Detective
- C. Compensating
- D. Preventive

Answer: B

Explanation:
Explanation
Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network. They can help to discover the source, scope, and impact of an attack, and provide evidence for further analysis or investigation. Detective controls include log files, security audits, intrusion detection systems, network monitoring tools, and antivirus software. In this case, the administrator used log files as a detective control to review the ransomware attack on the company's system. Log files are records of events and activities that occur on a system or network, such as user actions, system errors, network traffic, and security alerts. They can provide valuable information for troubleshooting, auditing, and forensics.
References:
Security+ (Plus) Certification | CompTIA IT Certifications, under "About the exam", bullet point 3:
"Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance."
CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: "Detective controls are designed to identify and monitor any malicious activity or anomalies on a system or network." Control Types - CompTIA Security+ SY0-401: 2.1 - Professor Messer IT ..., under "Detective Controls": "Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network."

NEW QUESTION # 285

......

Services like quick downloading within five minutes, convenient and safe payment channels made for your convenience. Even newbies will be tricky about this process. Unlike product from stores, quick browse of our SY0-701 practice materials can give you the professional impression wholly. So, they are both efficient in practicing and downloading process. By the way, we also have free demo of SY0-701 practice materials as freebies for your reference to make your purchase more effective.

Braindumps SY0-701 Ppt

- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, learn.csisafety.com.au, www.stes.tyc.edu.tw, www.divephotoguide.com, 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, www.stes.tyc.edu.tw, myspace.com, curs.myclip.ro, 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

DOWNLOAD the newest ITExamSimulator SY0-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1AQyofgV1yszZQiLA5r2pw6dFEAQnyx5g