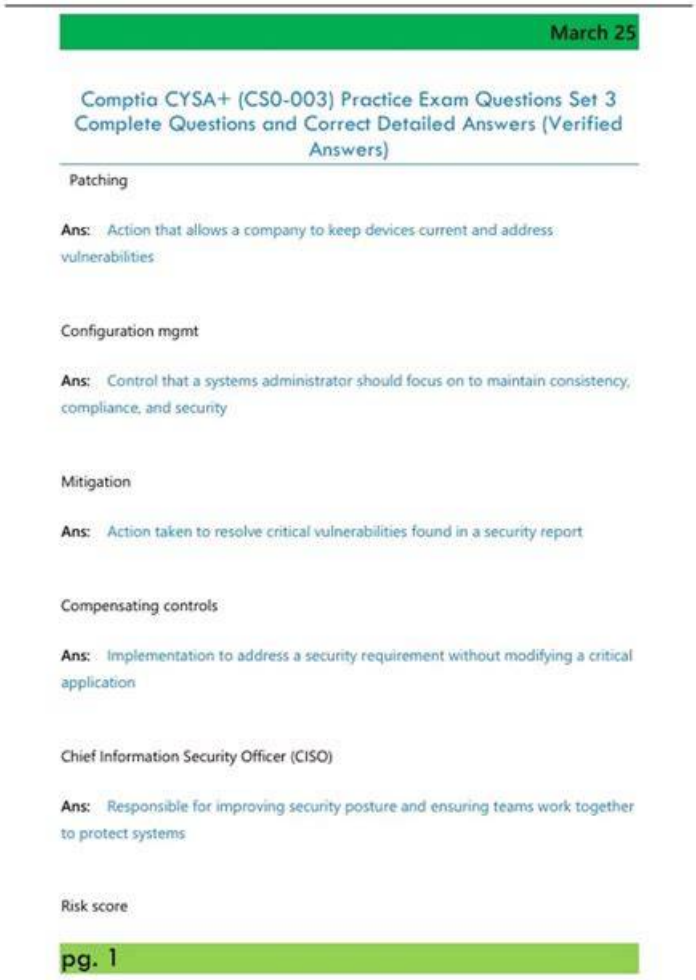
Exam CS0-003 Fee - CS0-003 Verified Answers


March 25

Comptia CYSA+ (CS0-003) Practice Exam Questions Set 3 Complete Questions and Correct Detailed Answers (Verified Answers)

Patching

Ans: Action that allows a company to keep devices current and address vulnerabilities

Configuration mgmt

Ans: Control that a systems administrator should focus on to maintain consistency, compliance, and security

Mitigation

Ans: Action taken to resolve critical vulnerabilities found in a security report

Compensating controls

Ans: Implementation to address a security requirement without modifying a critical application

Chief Information Security Officer (CISO)

Ans: Responsible for improving security posture and ensuring teams work together to protect systems

Risk score

pg. 1

BONUS!!! Download part of TorrentVCE CS0-003 dumps for free: https://drive.google.com/open?id=1lubQ1Kzi13pEZ6wrjS2jbDK3B0gMAXpU

This CS0-003 exam prep material has been prepared under the expert surveillance of 90,000 highly experienced IT professionals worldwide. This updated and highly reliable TorrentVCE product consists of 3 prep formats: CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003) dumps PDF, desktop practice exam software, and browser-based mock exam. Each format specializes in a specific study style and offers unique benefits, each of which is crucial to good CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003) exam preparation. The specs of each CompTIA CS0-003 exam questions format are listed below, you may select any of them as per your requirements.

CompTIA CS0-003 Exam Syllabus Topics:

Section	Weight	Objectives

Topic 1: Security Operations	30%	- Security Monitoring • 1. Data sources for security monitoring • 2. SOAR (Security Orchestration, Automation, and Response) • 3. Security event collection and correlation • 4. SIEM (Security Information and Event Management) • 5. Log types and log analysis - Security Posture Assessment • 1. Penetration testing fundamentals • 2. Vulnerability scanning and analysis • 3. Configuration management - Intrusion Detection/Prevention • 1. Host-based IDS/IPS • 2. Indicator identification • 3. Network-based IDS/IPS
Topic 2: Threat and Attack Analysis	20%	- Threat Intelligence • 1. Indicators of compromise (IOC) • 2. Threat intelligence frameworks (MITRE ATT&CK, STIX/TAXII) • 3. Threat intelligence types and sources • 4. Threat actor identification - Threat Analysis Process • 1. Anomaly detection • 2. Traffic and activity analysis • 3. Behavioral analysis
Topic 3: Vulnerability Management	30%	- Vulnerability Response and Remediation • 1. Remediation workflow • 2. Exception handling • 3. Risk acceptance and mitigation strategies - Vulnerability Validation • 1. Vulnerability scanning validation • 2. Penetration testing verification - Vulnerability Identification • 1. Asset inventory and prioritization • 2. False positive/negative analysis • 3. Vulnerability scanning tools

Topic 4: Incident Response	20%	- Incident Response Process • 1. Preparation and detection • 2. Containment, eradication, and recovery • 3. Lessons learned and post-incident activities - Incident Response Techniques • 1. Malware incident response • 2. Unauthorized access incident response • 3. Denial of service incident response - Digital Forensics • 1. Forensic imaging • 2. Chain of custody • 3. Evidence collection and preservation
Topic 5: Reporting and Communication	0%	- Communication Strategies • 1. Stakeholder communication • 2. Risk management communication - Metrics and Reporting • 1. Security maturity models • 2. Key metrics development • 3. Security reporting • 4. MTTR (Mean Time to Respond/Detect)

CS0-003 Verified Answers | CS0-003 Real Dumps Free

We guarantee that this study material will prove enough to prepare successfully for the CS0-003 examination. If you prepare with our CompTIA Cybersecurity Analyst (CySA+) Certification Exam CS0-003 actual dumps, we ensure that you will become capable to crack the CompTIA CS0-003 test within a few days. This has helped hundreds of CompTIA CS0-003 Exam candidates. Applicants who have used our CompTIA CS0-003 valid dumps are now certified. If you also want to pass the test on your first sitting, use our CompTIA CS0-003 updated dumps.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q419-Q424):

NEW QUESTION # 419
After updating the email client to the latest patch, only about 15% of the workforce is able to use email.
Windows 10 users do not experience issues, but Windows 11 users have constant issues. Which of the following did the change management team fail to do?

- A. Implementation
- B. Rollback
- C. Validation
- D. Testing

Answer: D

Explanation:
Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users.
Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.

References: 7 Reasons Why Change Management Strategies Fail and How to Avoid Them, CompTIA CySA+ CS0-003 Certification Study Guide

NEW QUESTION # 420
A digital forensics investigator works from duplicate images to preserve the integrity of the original evidence. Which of the following types of media are most volatile and should be preserved? (Select two).

- A. Swap volume
- B. Registry file
- C. Memory cache
- D. Temporary filesystems
- E. Packet decoding
- F. SSD storage

Answer: A,C

Explanation:
Memory cache and swap volume are types of media that are most volatile and should be preserved during a digital forensics investigation. Volatile media are those that store data temporarily and lose their contents when the power is turned off or interrupted. Memory cache is a small and fast memory that stores frequently used data or instructions for faster access by the processor. Swap volume is a part of the hard disk that is used as an extension of the memory when the memory is full or low .

NEW QUESTION # 421
An analyst receives alerts that state the following traffic was identified on the perimeter network firewall:

Source	Destination	IP reputation	Bytes sent	Bytes received	Action
192.168.1.14	172.16.2.8	low	64	0	allow
192.168.1.14	172.16.2.8	low	64	0	allow
192.168.0.4	172.16.2.8	low	512	512	allow
192.168.1.14	172.16.2.8	low	1512	960	allow
192.168.1.58	172.16.2.8	low	1985	354	allow
192.168.1.14	172.16.2.8	low	512	758	allow
192.168.1.58	172.16.2.8	low	64	0	allow
192.168.0.4	172.16.2.8	low	64	168468	allow
192.168.1.14	172.16.2.8	low	1289	154	allow

Which of the following best describes the indicator of compromise that triggered the alerts?

- A. Bandwidth saturation
- B. Anomalous activity
- C. Denial of service
- D. Cryptomining

Answer: D

Explanation:
The given firewall logs indicatehigh outbound traffic with low IP reputation, sustained over time, which is a strongindicator of cryptomining activity.
* Option A (Anomalous activity)is a general term but does not specifywhythe activity is suspicious.
* Option B (Bandwidth saturation)occurs when network traffic is overwhelming, but cryptomining typicallyuses CPU/GPU powerrather than overwhelming bandwidth.
* Option D (Denial of service - DoS)would result incontinuous large requests, but cryptomining generatesconsistent, high-bandwidth outbound trafficrather than bursts of large requests.
Thus,C is the correct answer, as cryptomininggenerates unusual outbound network activity from internal hosts to mining pools.

NEW QUESTION # 422
A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

- A. vote.4p
- B. sweet.bike
- C. nessie.explosion
- D. great.skills

Answer: C

Explanation:
nessie.explosion should be prioritized for remediation, as it has the highest CVSSv3.1 exploitability score of 8.6. The exploitability score is a sub-score of the CVSSv3.1 base score, which reflects the ease and technical means by which the vulnerability can be exploited. The exploitability score is calculated based on four metrics: Attack Vector, Attack Complexity, Privileges Required, and User Interaction. The higher the exploitability score, the more likely and feasible the vulnerability is to be exploited by an attacker12. nessie.
explosion has the highest exploitability score because it has the lowest values for all four metrics: Network (AV:N), Low (AC:L), None (PR:N), and None (UI:N). This means that the vulnerability can be exploited remotely over the network, without requiring any user interaction or privileges, and with low complexity.
Therefore, nessie.explosion poses the greatest threat to the end user workstations, and should be remediated first. vote.4p, sweet.bike, and great.skills have lower exploitability scores because they have higher values for some of the metrics, such as Adjacent Network (AV:A), High (AC:H), Low (PR:L), or Required (UI:R). This means that the vulnerabilities are more difficult or less likely to be exploited, as they require physical proximity, user involvement, or some privileges34. References: CVSS v3.1 Specification Document - FIRST, NVD - CVSS v3 Calculator, CVSS v3.1 User Guide - FIRST, CVSS v3.1 Examples - FIRST

NEW QUESTION # 423
The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

Which of the following vulnerabilities should the analyst be most concerned about, knowing that end users frequently click on malicious links sent via email?

- A. Vulnerability C
- B. Vulnerability A

- C. Vulnerability B
- D. Vulnerability D

Answer: C

Explanation:
Vulnerability B is the vulnerability that the analyst should be most concerned about, knowing that end users frequently click on malicious links sent via email. Vulnerability B is a remote code execution vulnerability in Microsoft Outlook that allows an attacker to run arbitrary code on the target system by sending a specially crafted email message. This vulnerability is very dangerous, as it does not require any user interaction or attachment opening to trigger the exploit. The attacker only needs to send an email to the victim's Outlook account, and the code will execute automatically when Outlook connectsto the Exchange server. This vulnerability has a high severity rating of 9.8 out of 10, and it affects all supported versions of Outlook.
Therefore, the analyst should prioritize patching this vulnerability as soon as possible to prevent potential compromise of the workstations.

NEW QUESTION # 424
.....

If you are finding a study material to prepare your exam, our material will end your search. Our CS0-003 exam torrent has a high quality that you can't expect. I think our CS0-003 prep torrent will help you save much time, and you will have more free time to do what you like to do. I can guarantee that you will have no regrets about using our CS0-003 Test Braindumps When the time for action arrives, stop thinking and go in, try our CS0-003 exam torrent, you will find our products will be a very good choice for you to pass your exam and get you certificate in a short time.

id=1lubQ1Kzi13pEZ6wrjS2jbDK3B0gMAXpU