Rely on ExamsReviews CAS-004 Practice Exam Software for Thorough Self-Assessment

P.S. Free & New CAS-004 dumps are available on Google Drive shared by ExamsReviews: https://drive.google.com/open?id=1beIaIFHf6kbqzltyqlpVxABOXOXOW35O

Thanks to modern technology, learning online gives people access to a wider range of knowledge, and people have got used to convenience of electronic equipment. As you can see, we are selling our CAS-004 learning guide in the international market, thus there are three different versions of our CAS-004 exam materials: PDF, Soft and APP versions. It is worth mentioning that, the simulation test of our CAS-004 Study Guide is available in our software version. With the simulation test, all of our customers will get accustomed to the CAS-004 exam easily, and pass the exam with confidence.

CompTIA CAS-004 (CompTIA Advanced Security Practitioner (CASP+)) Certification Exam is an advanced-level certification that demonstrates the ability to work with complex security solutions and provides validation of the skills and knowledge required to be an effective security practitioner. CAS-004 exam covers a wide range of security topics, and preparing for the exam requires a solid understanding of advanced-level security concepts and hands-on experience with security technologies. CompTIA Advanced Security Practitioner (CASP+) Exam certification is recognized globally and is highly valued by employers as it is a prerequisite for some advanced-level security certifications.

>> Online CAS-004 Test <<

Free PDF Quiz 2026 Efficient CompTIA Online CAS-004 Test

Do you want to get the CAS-004 exam braindumps as quickly as you finish paying, then choose the CAS-004 study material of us, we can do this for you. You can pass the exam only just need to spend about 48 to 72 hours in practicing. The CAS-004 exam braindumps of us is verified by experienced experts, therefore the quality and the accuracy of the CAS-004 Study Materials can be guaranteed, and we also pass guarantee and money back guarantee for your fail to pass the exam.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q239-Q244):

NEW QUESTION # 239

A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	56	2	$2000
June	721	598	120	2	$6000

Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	930	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

Which of the following meets the budget needs of the business?

- A. Filter GHI
- B. Filter XYZ
- C. Filter ABC
- D. Filter TUV

Answer: B

Explanation:
Filter XYZ is the best option that meets the budget needs of the business. Filter XYZ has an ALE of $1 million per year, which is lower than any other filter option. ALE stands for annualized loss expectancy, which is a measure of how much money a business can expect to lose due to a risk over a year. ALE is calculated by multiplying the annualized rate of occurrence (ARO) of an event by the single loss expectancy (SLE) of an event. ARO is how often an event is expected to occur in a year. SLE is how much money an event will cost each time it occurs. Therefore, ALE = ARO x SLE. Filter XYZ has an ARO of 0.1 and an SLE of $10 million, so ALE = 0.1 x $10 million = $1 million. Verified References: https://www.comptia.org /training/books/casp-cas-004-study-guide , https://www.techopedia.com/definition/24771/annualized-loss- expectancy-ale

NEW QUESTION # 240
A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	56	2	$2000
June	721	598	120	2	$6000

Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	930	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

Which of the following meets the budget needs of the business?

- A. Filter GHI
- B. Filter XYZ
- C. Filter ABC

- D. Filter TUV

Answer: B

Explanation:
Filter XYZ is the best option that meets the budget needs of the business. Filter XYZ has an ALE of $1 million per year, which is lower than any other filter option. ALE stands for annualized loss expectancy, which is a measure of how much money a business can expect to lose due to a risk over a year. ALE is calculated by multiplying the annualized rate of occurrence (ARO) of an event by the single loss expectancy (SLE) of an event. ARO is how often an event is expected to occur in a year. SLE is how much money an event will cost each time it occurs. Therefore, ALE = ARO x SLE. Filter XYZ has an ARO of 0.1 and an SLE of $10 million, so ALE = 0.1 x $10 million = $1 million. Verified References: https://www.comptia.org /training/books/casp-cas-004-study-guide , https://www.techopedia.com/definition/24771/annualized-loss- expectancy-ale

NEW QUESTION # 241
A company recently deployed a SIEM and began importing logs from a firewall, a file server, a domain controller a web server, and a laptop. A security analyst receives a series of SIEM alerts and prepares to respond. The following is the alert information:

Severity	Source device	Event info	Time (UTC)
Medium	abc-usa-fw01	RDP (3389) traffic from abc-admin-lp01 to abc-usa-fs1	1020:08
Low	abc-ger-dc1	Successful logon event for user jdoe on abc-usa-fs1	1020:34
Medium	abc-ger-fw01	RDP (3389) traffic from abc-usa-fs1 to abc-ger-fs1	1021:02
Low	abc-usa-fw01	SMB (445) traffic from abc-usa-fs1 to abc-web01	1020:51
Low	abc-usa-dc1	Successful logon event for user jdoe on abc-ger-fs1	1024:55
High	abc-usa-fw01	FTP (21) traffic from abc-ger-fs1 to abc-web01	1025:16
High	abc-web01	Successful logon event for user Administrator	1126:40

Which of the following should the security analyst do FIRST?

- A. Shut down the abc-usa-fsl server, a plaintext credential is being used
- B. Shut down abc-usa-fw01; the remote access VPN vulnerability is exploited
- C. Disable the jdoe account, it is likely compromised
- D. Disable Administrator on abc-uaa-fsl, the local account is compromised

Answer: C

Explanation:
Based on the SIEM alerts, the security analyst should first disable the jdoe account, as it is likely compromised by an attacker. The alerts show that the jdoe account successfully logged on to the abc-usa-fsl server, which is a file server, and then initiated SMB (445) traffic to the abc-web01 server, which is a web server. This indicates that the attacker may be trying to exfiltrate data from the file server to the web server. Disabling the jdoe account would help stop this unauthorized activity and prevent further damage.
Disabling Administrator on abc-usa-fsl, the local account is compromised, is not the first action to take, as it is not clear from the alerts if the local account is compromised or not. The alert shows that there was a successful logon event for Administrator on abc-usa-fsl, but it does not specify if it was a local or domain account, or if it was authorized or not. Moreover, disabling the local account would not stop the SMB traffic from jdoe to abc-web01.
Shutting down the abc-usa-fsl server, a plaintext credential is being used, is not the first action to take, as it is not clear from the alerts if a plaintext credential is being used or not. The alert shows that there was RDP (3389) traffic from abc-admin1-logon to abc-usa-fsl, but it does not specify if the credential was encrypted or not. Moreover, shutting down the file server would disrupt its normal operations and affect other users.
Shutting down abc-usa-fw01; the remote access VPN vulnerability is exploited, is not the first action to take, as it is not clear from the alerts if the remote access VPN vulnerability is exploited or not. The alert shows that there was FTP (21) traffic from abc-usa-

dcl to abc-web01, but it does not specify if it was related to the VPN or not. Moreover, shutting down the firewall would expose the network to other threats and affect other services. Reference: What is SIEM? | Microsoft Security, What is a SIEM Alert? | Cofense

NEW QUESTION # 242
A company suspects a web server may have been infiltrated by a rival corporation. The security engineer reviews the web server logs and finds the following:

The security engineer looks at the code with a developer, and they determine the log entry is created when the following line is run:

Which of the following is an appropriate security control the company should implement?

- A. Use server-side processing to avoid XSS vulnerabilities in path input.
- B. Restrict directory permission to read-only access.
- C. Separate the items in the system call to prevent command injection.
- D. Parameterize a query in the path variable to prevent SQL injection.

Answer: C

NEW QUESTION # 243
A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

- A. Implement the SDLC security guidelines.
- B. Track the library versions and monitor the CVE website for related vulnerabilities.
- C. Perform additional SAST/DAST on the open-source libraries.
- D. Perform unit testing of the open-source libraries.

Answer: B

Explanation:
Reference:https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/ Tracking the library versions and monitoring the CVE (Common Vulnerabilities and Exposures) website for related vulnerabilities is an activity that the organization should incorporate into the SDLC (software development life cycle) to ensure the security of the open-source libraries integrated into its software.
Tracking the library versions can help identify outdated or unsupported libraries that may contain vulnerabilities or bugs. Monitoring the CVE website can help discover publicly known vulnerabilities in the open-source libraries and their severity ratings. Performing additional SAST/DAST (static application security testing/dynamic application security testing) on the open-source libraries may not be feasible or effective for ensuring their security, as SAST/DAST are mainly focused on testing the source code or functionality of the software, not the libraries. Implementing the SDLC security guidelines is a general activity that the organization should follow for developing secure software, but it does not specifically address the security of the open-source libraries. Performing unit testing of the open-source libraries may not be feasible or effective for ensuring their security, as unit testing is mainly focused on testing the individual components or modules of the software, not thelibraries. Verified References:
https://www.comptia.org/blog/what-is-cvehttps://partners.comptia.org/docs/default-source/resources/casp-conten

NEW QUESTION # 244
.....

- Real CAS-004 Question □ Exam CAS-004 Quick Prep □ CAS-004 Exam Discount Voucher □ Search for ➥ CAS-004 □ and download exam materials for free through ▸ www.practicevce.com ◂ □CAS-004 Training For Exam
- Numerous Benefits of the CompTIA CAS-004 Exam Material □ Go to website [www.pdfvce.com] open and search for 「 CAS-004 」 to download for free □Official CAS-004 Study Guide
- Start Preparation With CompTIA CAS-004 Latest Dumps Today □ Download □ CAS-004 □ for free by simply searching on ☀ www.prepawayete.com □☀□ □CAS-004 Test Labs
- Free PDF Quiz Marvelous CompTIA - CAS-004 - Online CompTIA Advanced Security Practitioner (CASP+) Exam Test □ 【 www.pdfvce.com 】 is best website to obtain " CAS-004 " for free download □CAS-004 Latest Study Questions
- Start Preparation With CompTIA CAS-004 Latest Dumps Today □ Immediately open 《 www.troytecdumps.com 》 and search for [CAS-004] to obtain a free download □Reliable CAS-004 Exam Voucher
- Free PDF Quiz CompTIA - CAS-004 –High Pass-Rate Online Test □ Open ☀ www.pdfvce.com □☀□ and search for ✔ CAS-004 □✔□ to download exam materials for free □CAS-004 Training For Exam
- Exam CAS-004 Quick Prep □ Reliable CAS-004 Exam Question □ CAS-004 Test Labs □ Search for 「 CAS-004 」 on [www.prepawayexam.com] immediately to obtain a free download □Official CAS-004 Study Guide
- Pdf CAS-004 Torrent □ Pass CAS-004 Guaranteed □ Exam CAS-004 Quick Prep □ Easily obtain free download of □ CAS-004 □ by searching on ✔ www.pdfvce.com □✔□ □Real CAS-004 Question
- Free PDF Quiz CompTIA - CAS-004 –High Pass-Rate Online Test □ Search on ☀ www.vceengine.com □☀□ for 「 CAS-004 」 to obtain exam materials for free download □CAS-004 Training For Exam
- Free PDF Quiz Marvelous CompTIA - CAS-004 - Online CompTIA Advanced Security Practitioner (CASP+) Exam Test □ Easily obtain free download of □ CAS-004 □ by searching on ▹ www.pdfvce.com ◃ ↔CAS-004 Passleader Review
- Excellent Online CAS-004 Test - Leading Offer in Qualification Exams - Fast Download CompTIA CompTIA Advanced Security Practitioner (CASP+) Exam □ Open [www.vce4dumps.com] and search for □ CAS-004 □ to download exam materials for free □Reliable CAS-004 Exam Voucher
- 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, 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, writeablog.net, ofbiz.116.s1.nabble.com, zenwriting.net, www.stes.tyc.edu.tw, study.stcs.edu.np, archstudios-eg.com, Disposable vapes

DOWNLOAD the newest ExamsReviews CAS-004 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1beIaIFHf6kbqzltyqlpVxABOXOXOW35O