CAS-004 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

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	55	2	$2000
June	721	598	120	6	$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 ABC

B. Filter XYZ

C. Filter GHI

D. Filter TUV

Correct Answer: C

QUESTION 2

The email administrator must reduce the number of phishing emails by utilizing more appropriate security controls. The following configurations already are in place:

1.

Keyword blocking based on word lists

2.

URL rewnting and protection

3.

Stopping executable files from messages

Which of the following is the BEST configuration change for the administrator to make?

A. Configure more robust word lists for blocking suspicious emails

B. Configure appropriate regular expression rules per suspicious email received

C. Configure Bayesian filtering to block suspicious inbound email

D. Configure the mail gateway to strip any attachments.

Correct Answer: B

Reference: https://www ibm.com/docs/en/rsoa-and-rD/36?tODic=Darsing-extension-customization

QUESTION 3

A security compliance requirement states that specific environments that handle sensitive data must be protected by need-to-know restrictions and can only connect to authorized endpoints. The requirement also states that a DLP solution

within the environment must be used to control the data from leaving the environment.

Which of the following should be implemented for privileged users so they can support the environment from their workstations while remaining compliant?

A. NAC to control authorized endpoints

B. FIM on the servers storing the data

C. A jump box in the screened subnet

D. A general VPN solution to the primary network

Correct Answer: C

QUESTION 4

Which of the following BEST describe the importance of maintaining chain of custody in forensic evidence collection? (Choose two.)

A. It increases the likelihood that evidence will be deemed admissible in court.

B. It authenticates personnel who come in contact with evidence after collection.

C. It ensures confidentiality and the need-to-know basis of forensically acquired evidence.

D. It attests to how recently evidence was collected by recording date/time attributes.

E. It provides automated attestation for the integrity of the collected evidence.

F. It ensures the integrity of the collected evidence.

Correct Answer: AF

QUESTION 5

A SaaS startup is maturing its DevSecOps program and wants to identify weaknesses earlier in the development process in order to reduce the average time to identify serverless application vulnerabilities and the costs associated with remediation. The startup began its early security testing efforts with DAST to cover public-facing application components and recently implemented a bug bounty program. Which of the following will BEST accomplish the company\\'s objectives?

A. RASP

B. SAST

C. WAF

D. CMS

Correct Answer: B

to identify bug at the early stage of the SDLC