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.pass4itsure.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 security architect recommends replacing the company\\'s monolithic software application with a containerized solution. Historically, secrets have been stored in the application\\'s configuration files. Which of the following changes should the security architect make in the new system?

A. Use a secrets management tool.

B. Save secrets in key escrow.

C. Store the secrets inside the Dockerfiles.

D. Run all Dockerfiles in a randomized namespace.

Correct Answer: A

QUESTION 2

Which of the following is MOST commonly found in a network SLA contract?

A. Price for extra services

B. Performance metrics

C. Service provider responsibility only

D. Limitation of liability

E. Confidentiality and non-disclosure

Correct Answer: B

QUESTION 3

A company was recently infected by malware. During the root cause analysis. the company determined that several users were installing their own applications. TO prevent further compromises, the company has decided it will only allow authorized applications to run on its systems. Which Of the following should the company implement?

A. Signing

B. Access control

C. HIPS

D. Permit listing

Correct Answer: D

QUESTION 4

A security analyst observes the following while looking through network traffic in a company\\'s cloud log:

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

Which of the following steps should the security analyst take FIRST?

A. Quarantine 10.0.5.52 and run a malware scan against the host.

B. Access 10.0.5.52 via EDR and identify processes that have network connections.

C. Isolate 10.0.50.6 via security groups.

D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Correct Answer: B

QUESTION 5

A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:

1.

Work at the application layer

2.

Send alerts on attacks from both privileged and malicious users

3.

Have a very low false positive

Which of the following should the architect recommend?

A. FIM

B. WAF

C. NIPS

D. DAM

E. UTM

Correct Answer: D