

➤ **Vendor: CompTIA**

➤ **Exam Code: CS0-002**

➤ **Exam Name: CompTIA CSA+ Certification Exam**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [Dec./2020](#))**

**[Visit Braindump2go and Download Full Version CS0-002 Exam Dumps](#)**

**QUESTION 531**

An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment. One of the primary concerns is exfiltration of data by malicious insiders. Which of the following controls is the MOST appropriate to mitigate risks?

- A. Data deduplication
- B. OS fingerprinting
- C. Digital watermarking
- D. Data loss prevention

**Answer: D**

**QUESTION 532**

A security analyst has discovered that developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

- A. Create a security rule that blocks Internet access in the development VPC
- B. Place a jumpbox in between the developers' workstations and the development VPC
- C. Remove the administrator's profile from the developer user group in identity and access management
- D. Create an alert that is triggered when a developer installs an application on a server

**Answer: A**

**QUESTION 533**

An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested in a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?

- A. TPM
- B. eFuse
- C. FPGA
- D. HSM
- E. UEFI

**Answer: A**

**QUESTION 534**

[CS0-002 Exam Dumps](#) [CS0-002 Exam Questions](#) [CS0-002 PDF Dumps](#) [CS0-002 VCE Dumps](#)

<https://www.braindump2go.com/cs0-002.html>

An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?

- A. Root-cause analysis
- B. Active response
- C. Advanced antivirus
- D. Information-sharing community
- E. Threat hunting

**Answer: E**

**QUESTION 535**

An analyst is investigating an anomalous event reported by the SOC. After reviewing the system logs, the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?

- A. Patching logs
- B. Threat feed
- C. Backup logs
- D. Change requests
- E. Data classification matrix

**Answer: E**

**QUESTION 536**

A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Big Data sets. Exploitation of the vulnerability could cost the organization \$1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised. Which of the following is the value of this risk?

- A. \$75,000
- B. \$300,000
- C. \$1.425 million
- D. \$1.5 million

**Answer: A**

**QUESTION 537**

A security analyst is investigating a system compromise. The analyst verifies the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely exploited?

- A. Insider threat
- B. Buffer overflow
- C. Advanced persistent threat
- D. Zero day

**Answer: D**

**QUESTION 538**

An organization developed a comprehensive incident response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

- A. A simulated breach scenario involving the incident response team

- B. Completion of annual information security awareness training by all employees
- C. Tabletop activities involving business continuity team members
- D. Completion of lessons-learned documentation by the computer security incident response team
- E. External and internal penetration testing by a third party

**Answer: A**

**QUESTION 539**

A cybersecurity analyst is responding to an incident. The company's leadership team wants to attribute the incident to an attack group. Which of the following models would BEST apply to the situation?

- A. Intelligence cycle
- B. Diamond Model of Intrusion Analysis
- C. Kill chain
- D. MITRE ATT&CK

**Answer: B**

**QUESTION 540**

Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

- A. Use a UEFI boot password
- B. Implement a self-encrypted disk
- C. Configure filesystem encryption
- D. Enable Secure Boot using TPM

**Answer: C**

**QUESTION 541**

A security analyst implemented a solution that would analyze the attacks that the organization's firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command:

```
$ sudo nc -l -v -e maildaemon.py 25 > caplog.txt
```

Which of the following solutions did the analyst implement?

- A. Log collector
- B. Crontab mail script
- C. Sinkhole
- D. Honeypot

**Answer: A**

**QUESTION 542**

Which of the following will allow different cloud instances to share various types of data with a minimal amount of complexity?

- A. Reverse engineering
- B. Application log collectors
- C. Workflow orchestration
- D. API integration
- E. Scripting

**Answer: D**