- **Vendor: CompTIA**
- **Exam Code: CS0-002**
- **Exam Name: CompTIA CSA+ Certification Exam**
- **New Updated Questions from Braindump2go (Updated in Dec./2020)**

QUESTION 543
A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO), asking the employee to perform a wire transfer. Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

A. Implementing a sandboxing solution for viewing emails and attachments
B. Limiting email from the finance department to recipients on a pre-approved whitelist
C. Configuring email client settings to display all messages in plaintext when read
D. Adding a banner to incoming messages that identifies the messages as external

Answer: D

QUESTION 544
A security analyst wants to identify which vulnerabilities a potential attacker might initially exploit if the network is compromised. Which of the following would provide the BEST results?

A. Baseline configuration assessment
B. Uncredentialed scan
C. Network ping sweep
D. External penetration test

Answer: B

QUESTION 545
An analyst has been asked to provide feedback regarding the controls required by a revised regulatory framework. At this time, the analyst only needs to focus on the technical controls.
Which of the following should the analyst provide an assessment of?

A. Tokenization of sensitive data
B. Establishment of data classifications
C. Reporting on data retention and purging activities
D. Formal identification of data ownership
E. Execution of NDAs

Answer: A

QUESTION 546
A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level

of security. To BEST complete this task, the analyst should place the:

A. firewall behind the VPN server
B. VPN server parallel to the firewall
C. VPN server behind the firewall
D. VPN on the firewall

Answer: C

QUESTION 547
Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus, on company systems?

A. Code of conduct policy
B. Account management policy
C. Password policy
D. Acceptable use policy

Answer: D

QUESTION 548
As part of a review of incident response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?

A. Organizational policies
B. Vendor requirements and contracts
C. Service-level agreements
D. Legal requirements

Answer: D

QUESTION 549
A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a timely manner when an employee leaves the organization. To BEST resolve the issue, the organization should implement:

A. federated authentication
B. role-based access control
C. manual account reviews
D. multifactor authentication

Answer: A

QUESTION 550
A large software company wants to move its source control and deployment pipelines into a cloud- computing environment. Due to the nature of the business, management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

A. Establish an alternate site with active replication to other regions
B. Configure a duplicate environment in the same region and load balance between both instances
C. Set up every cloud component with duplicated copies and auto-scaling turned on
D. Create a duplicate copy on premises that can be used for failover in a disaster situation

Answer: A

QUESTION 551
A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities. The type of vulnerability that should be disseminated FIRST is one that:

A. enables remote code execution that is being exploited in the wild
B. enables data leakage but is not known to be in the environment
C. enables lateral movement and was reported as a proof of concept
D. affected the organization in the past but was probably contained and eradicated

Answer: A

QUESTION 552
A company's incident response team is handling a threat that was identified on the network. Security analysts have determined a web server is making multiple connections from TCP port 445 outbound to servers inside its subnet as well as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

A. Quarantine the web server
B. Deploy virtual firewalls
C. Capture a forensic image of the memory and disk
D. Enable web server containerization

Answer: A

QUESTION 553
During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation. Which of the following would cause the analyst to further review the incident?

A. BadReputationIp - - [2019-04-12 10:43Z] "GET /etc/passwd" 403 1023
B. BadReputationIp - - [2019-04-12 10:43Z] "GET /index.html?src=../.ssh/id_rsa" 401 17044
C. BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=/etc/passwd" 403 11056
D. BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=../../.ssh/id_rsa" 200 15036
E. BadReputationIp - - [2019-04-12 10:43Z] "GET /favicon.ico?src=../usr/share/ icons" 200 19064

Answer: E

QUESTION 554
A developer wrote a script to make names and other PII data unidentifiable before loading a database export into the testing system. Which of the following describes the type of control that is being used?

A. Data encoding
B. Data masking
C. Data loss prevention
D. Data classification

Answer: B