- **Vendor:** CompTIA
- **Exam Code:** SY0-601
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in July/2021)**

QUESTION 379
Entering a secure area requires passing through two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?

A. Cameras
B. Faraday cage
C. Access control vestibule
D. Sensors
E. Guards

Answer: C

QUESTION 380
The lessons-learned analysis from a recent incident reveals that an administrative office worker received a call from someone claiming to be from technical support. The caller convinced the office worker to visit a website, and then download and install a program masquerading as an antivirus package. The program was actually a backdoor that an attacker could later use to remote control the worker's PC. Which of the following would be BEST to help prevent this type of attack in the future?

A. Data loss prevention
B. Segmentation
C. Application whitelisting
D. Quarantine

Answer: C

QUESTION 381
A security administrator has noticed unusual activity occurring between different global instances and workloads and needs to identify the source of the unusual traffic. Which of the following log sources would be BEST to show the source of the unusual traffic?

A. HIDS
B. UEBA
C. CASB
D. VPC

Answer: C

QUESTION 382

A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The Oss are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery.
Which of the following resiliency techniques will provide these capabilities?

A. Redundancy
B. RAID 1+5
C. Virtual machines
D. Full backups

Answer: D

QUESTION 383
Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?

A. A right-to-audit clause allowing for annual security audits
B. Requirements for event logs to be kept for a minimum of 30 days
C. Integration of threat intelligence in the company's AV
D. A data-breach clause requiring disclosure of significant data loss

Answer: A

QUESTION 384
An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions.
Which of the following sources of information would BEST support this solution?

A. Web log files
B. Browser cache
C. DNS query logs
D. Antivirus

Answer: C

QUESTION 385
Which of the following represents a biometric FRR?

A. Authorized users being denied access
B. Users failing to enter the correct PIN
C. The denied and authorized numbers being equal
D. The number of unauthorized users being granted access

Answer: A

QUESTION 386
A web server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the following should the administrator implement to avoid disruption?

A. NIC teaming
B. High availability
C. Dual power supply
D. laaS

Answer: B

QUESTION 387
Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

A. OWASP
B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries

Answer: A

QUESTION 388
An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account.
Which of the following would be BEST to minimize this risk?

A. Require a complex, eight-character password that is updated every 90 days.
B. Perform only non-intrusive scans of workstations.
C. Use non-credentialed scans against high-risk servers.
D. Log and alert on unusual scanner account logon times.

Answer: D

QUESTION 389
The new Chief Executive Officer (CEO) of a large company has announced a partnership with a vendor that will provide multiple collaboration applications t make remote work easier. The company has a geographically dispersed staff located in numerous remote offices in different countries. The company's IT administrators are concerned about network traffic and load if all users simultaneously download the application.
Which of the following would work BEST to allow each geographic region to download the software without negatively impacting the corporate network?

A. Update the host IDS rules.
B. Enable application whitelisting.
C. Modify the corporate firewall rules.
D. Deploy all applications simultaneously.

Answer: B

QUESTION 390
A Chief Security Officer (CSO) was notified that a customer was able to access confidential internal company files on a commonly used file-sharing service. The file-sharing service is the same one used by company staff as one of its approved third-party applications. After further investigation, the security team determines the sharing of confidential files was accidental and not malicious. However, the CSO wants to implement changes to minimize this type of incident from reoccurring but does not want to impact existing business processes. Which of the following would BEST meet the CSO's objectives?

A. DLP
B. SWG
C. CASB
D. Virtual network segmentation
E. Container security

Answer: A

QUESTION 391
Which of the following is a reason why an organization would define an AUP?

A. To define the lowest level of privileges needed for access and use of the organization's resources
B. To define the set of rules and behaviors for users of the organization's IT systems
C. To define the intended partnership between two organizations
D. To define the availability and reliability characteristics between an IT provider and consumer

Answer: B

QUESTION 392
A security analyst needs to perform periodic vulnerably scans on production systems. Which of the following scan types would produce the BEST vulnerability scan report?

A. Port
B. Intrusive
C. Host discovery
D. Credentialed

Answer: D

QUESTION 393
To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain Which of the following is being used?

A. PFS
B. SPF
C. DMARC
D. DNSSEC

Answer: D

QUESTION 394
An.. that has a large number of mobile devices is exploring enhanced security controls to manage unauthorized access if a device is lost or stolen. Specifically, if mobile devices are more than 3mi (4 8km) from the building, the management team would like to have the security team alerted and server resources restricted on those devices. Which of the following controls should the organization implement?

A. Geofencing
B. Lockout
C. Near-field communication
D. GPS tagging

Answer: A

QUESTION 395
A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following:
- The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.
- One of the websites the manager used recently experienced a data breach.
- The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country

Which of the following attacks has MOST likely been used to compromise the manager's corporate account?

A. Remote access Trojan
B. Brute-force
C. Dictionary
D. Credential stuffing
E. Password spraying

Answer: D

QUESTION 396
An organization has implemented a two-step verification process to protect user access to data that 6 stored in the could Each employee now uses an email address of mobile number a code to access the data. Which of the following authentication methods did the organization implement?

A. Token key
B. Static code
C. Push notification
D. HOTP

Answer: A

QUESTION 397
A company Is concerned about is security after a red-team exercise. The report shows the team was able to reach the critical servers due to the SMB being exposed to the Internet and running NTLMV1, Which of the following BEST explains the findings?

A. Default settings on the servers
B. Unsecured administrator accounts
C. Open ports and services
D. Weak Data encryption

Answer: C

QUESTION 398
Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

A. Risk matrix
B. Risk tolerance
C. Risk register
D. Risk appetite

Answer: B

QUESTION 399
A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to Implement a high availability pair to:

A. decrease the mean ne between failures
B. remove the single point of failure
C. cut down the mean tine to repair
D. reduce the recovery time objective

Answer: B