

CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam



NEW QUESTION 1

An organization has decided to host its web application and database in the cloud. Which of the following BEST describes the security concerns for this decision?

- A. Access to the organization's servers could be exposed to other cloud-provider clients
- B. The cloud vendor is a new attack vector within the supply chain
- C. Outsourcing the code development adds risk to the cloud provider
- D. Vendor support will cease when the hosting platforms reach EOL.

Answer: B

NEW QUESTION 2

In which of the following risk management strategies would cybersecurity insurance be used?

- A. Transference
- B. Avoidance
- C. Acceptance
- D. Mitigation

Answer: A

NEW QUESTION 3

An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: `ipconfig /flushdns`, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

- A. DNS cache poisoning
- B. Domain hijacking
- C. Distributed denial-of-service
- D. DNS tunneling

Answer: B

NEW QUESTION 4

A Chief Executive Officer (CEO) is dissatisfied with the level of service from the company's new service provider. The service provider is preventing the CEO from sending email from a work account to a personal account. Which of the following types of service providers is being used?

- A. Telecommunications service provider
- B. Cloud service provider
- C. Master managed service provider
- D. Managed security service provider

Answer: B

NEW QUESTION 5

Which of the following would MOST likely support the integrity of a voting machine?

- A. Asymmetric encryption
- B. Blockchain
- C. Transport Layer Security
- D. Perfect forward secrecy

Answer: D

NEW QUESTION 6

A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?

- A. Payment Card Industry Data Security Standard
- B. Cloud Security Alliance Best Practices
- C. ISO/IEC 27032 Cybersecurity Guidelines
- D. General Data Protection Regulation

Answer: A

NEW QUESTION 7

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen and later, enterprise data was found to have been compromised in a database. Which of the following was the MOST likely cause?

- A. Shadow IT
- B. Credential stuffing
- C. SQL injection

- D. Man-in-the-browser
- E. Bluejacking

Answer: A

NEW QUESTION 8

A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

- A. MSSP
- B. SOAR
- C. IaaS
- D. PaaS

Answer: B

NEW QUESTION 9

Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user's perspective against defined test cases? (Select TWO).

- A. Production
- B. Test
- C. Research and development
- D. PoC
- E. UAT
- F. SDLC

Answer: BE

NEW QUESTION 10

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?

- A. An incident response plan
- B. A communications plan
- C. A disaster recovery plan
- D. A business continuity plan

Answer: D

NEW QUESTION 10

A security analyst has been reading about a newly discovered cyber attack from a known threat actor. Which of the following would BEST support the analyst's review of the tactics, techniques, and protocols the threat actor was observed using in previous campaigns?

- A. Security research publications
- B. The MITRE ATT&CK framework
- C. The Diamond Model of Intrusion Analysis
- D. The Cyber Kill Chain

Answer: B

NEW QUESTION 13

Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

- A. An ARO
- B. An MOU
- C. An SLA
- D. A BPA

Answer: B

NEW QUESTION 18

A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?

- The solution must be inline in the network
- The solution must be able to block known malicious traffic
- The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

- A. HIDS
- B. NIDS
- C. HIPS
- D. NIPS

Answer: D

NEW QUESTION 23

A security analyst needs to be proactive in understanding the types of attacks that could potentially target the company's executives. Which of the following intelligence sources should the security analyst review?

- A. Vulnerability feeds
- B. Trusted automated exchange of indicator information
- C. Structured threat information expression
- D. Industry information-sharing and collaboration groups

Answer: D

NEW QUESTION 25

A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

- A. DAC
- B. ABAC
- C. SCAP
- D. SOAR

Answer: D

NEW QUESTION 28

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

NEW QUESTION 31

A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

- A. Continuous delivery
- B. Continuous integration
- C. Continuous validation
- D. Continuous monitoring

Answer: B

NEW QUESTION 32

A security analyst is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the analyst monitor?

- A. SFTP
- B. AS
- C. Tor
- D. IoC

Answer: C

NEW QUESTION 37

An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

- A. Incremental backups Monday through Friday at 6:00 p.m. and differential backups hourly
- B. Full backups Monday through Friday at 6:00 p.m. and incremental backups hourly
- C. Incremental backups Monday through Friday at 6:00 p.m. and full backups hourly
- D. Full backups Monday through Friday at 6:00 p.m. and differential backups hourly

Answer: A

NEW QUESTION 39

To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

- A. MaaS
- B. IaaS
- C. SaaS
- D. PaaS

Answer: D

NEW QUESTION 43

Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?

- A. An SLA
- B. An NDA
- C. ABPA
- D. An MOU

Answer: D

NEW QUESTION 44

Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

- A. DLP
- B. HIDS
- C. EDR
- D. NIPS

Answer: C

NEW QUESTION 47

A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

- A. perform attribution to specific APTs and nation-state actors.
- B. anonymize any PII that is observed within the IoC data.
- C. add metadata to track the utilization of threat intelligence reports.
- D. assist companies with impact assessments based on the observed data.

Answer: B

NEW QUESTION 52

A company is concerned about its 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

NEW QUESTION 53

An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

- A. The theft of portable electronic devices
- B. Geotagging in the metadata of images
- C. Bluesnarfing of mobile devices
- D. Data exfiltration over a mobile hotspot

Answer: D

NEW QUESTION 55

The security administrator has installed a new firewall which implements an implicit DENY policy by default.

INSTRUCTIONS:

Click on the firewall and configure it to allow ONLY the following communication.

* 1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.

* 2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port

* 3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.

Hot Area:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated with medium confidence

Graphical user interface Description automatically generated

Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443. Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22. Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.

References: Stewart,

James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 26, 44 http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION 57

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

NEW QUESTION 62

During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

- A. 1a
- B. chflags
- C. chmod
- D. leof
- E. setuid

Answer: D

NEW QUESTION 63

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

- A. It allows for the sharing of digital forensics data across organizations
- B. It provides insurance in case of a data breach
- C. It provides complimentary training and certification resources to IT security staff.
- D. It certifies the organization can work with foreign entities that require a security clearance
- E. It assures customers that the organization meets security standards

Answer: E

NEW QUESTION 68

A user recently attended an exposition and received some digital promotional materials. The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open. Which of the following is MOST likely the cause of the reported issue?

- A. There was a drive-by download of malware
- B. The user installed a cryptominer
- C. The OS was corrupted
- D. There was malicious code on the USB drive

Answer: D

NEW QUESTION 69

Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

- A. Unsecure protocols
- B. Use of penetration-testing utilities
- C. Weak passwords
- D. Included third-party libraries
- E. Vendors/supply chain
- F. Outdated anti-malware software

Answer: AD

NEW QUESTION 71

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned if servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139
- C. 143
- D. 161
- E. 443
- F. 445

Answer: BF

NEW QUESTION 72

Which of the following types of attacks is specific to the individual it targets?

- A. Whaling
- B. Pharming
- C. Smishing
- D. Credential harvesting

Answer: D

NEW QUESTION 77

A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

- A. logger
- B. Metasploit
- C. tcpdump
- D. netstat

Answer: D

NEW QUESTION 82

A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

- A. PCI DSS
- B. GDPR
- C. NIST
- D. ISO 31000

Answer: B

NEW QUESTION 83

A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

- A. FDE
- B. NIDS
- C. EDR

D. DLP

Answer: C

NEW QUESTION 88

A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:
Which of the following can the security analyst conclude?

- A. A replay attack is being conducted against the application.
- B. An injection attack is being conducted against a user authentication system.
- C. A service account password may have been changed, resulting in continuous failed logins within the application.
- D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Answer: C

NEW QUESTION 91

A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

- A. An external access point is engaging in an evil-twin attack.
- B. The signal on the WAP needs to be increased in that section of the building.
- C. The certificates have expired on the devices and need to be reinstalled.
- D. The users in that section of the building are on a VLAN that is being blocked by the firewall.

Answer: A

NEW QUESTION 93

Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

- A. The document is a honeypot and is meant to attract the attention of a cyberintruder.
- B. The document is a backup file if the system needs to be recovered.
- C. The document is a standard file that the OS needs to verify the login credentials.
- D. The document is a keylogger that stores all keystrokes should the account be compromised.

Answer: A

NEW QUESTION 95

A small business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the business network. Which of the following would BEST support the office's business needs? (Select TWO)

- A. Installing WAPs with strategic placement
- B. Configuring access using WPA3
- C. Installing a WIDS
- D. Enabling MAC filtering
- E. Changing the WiFi password every 30 days
- F. Reducing WiFi transmit power throughout the office

Answer: BD

NEW QUESTION 99

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

NEW QUESTION 100

Accompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?

- A. WPA3
- B. AES
- C. RADIUS
- D. WPS

Answer: D

NEW QUESTION 103

A retail company that is launching a new website to showcase the company's product line and other information for online shoppers registered the following URLs:

Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

- A. A self-signed certificate
- B. A root certificate
- C. A code-signing certificate
- D. A wildcard certificate
- E. An extended validation certificate

Answer: B

NEW QUESTION 104

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

NEW QUESTION 107

A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

- A. Discretionary
- B. Rule-based
- C. Role-based
- D. Mandatory

Answer: D

NEW QUESTION 112

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dnsenum
- D. logger

Answer: A

NEW QUESTION 117

An organization is having difficulty correlating events from its individual AV, EDR, DLP, SWG, WAF, MOM, HIPS, and CASB systems. Which of the following is the

BEST way to improve the situation?

- A. Remove expensive systems that generate few alerts.
- B. Modify the systems to alert only on critical issues.
- C. Utilize a SIEM to centralize logs and dashboards.
- D. Implement a new syslog/NetFlow appliance.

Answer: C

NEW QUESTION 119

A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

- A. Dual power supplies
- B. A UPS
- C. A generator
- D. APDU

Answer: B

NEW QUESTION 123

A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

- A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
- B. Restrict administrative privileges and patch all systems and applications.
- C. Rebuild all workstations and install new antivirus software
- D. Implement application whitelisting and perform user application hardening

Answer: A

NEW QUESTION 128

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

- A. Perform a site survey
- B. Deploy an FTK Imager
- C. Create a heat map
- D. Scan for rogue access points
- E. Upgrade the security protocols
- F. Install a captive portal

Answer: AC

NEW QUESTION 129

A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?

- A. A malicious USB was introduced by an unsuspecting employee.
- B. The ICS firmware was outdated
- C. A local machine has a RAT installed.
- D. The HVAC was connected to the maintenance vendor.

Answer: A

NEW QUESTION 133

A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

- A. Preventive
- B. Compensating
- C. Corrective
- D. Detective

Answer: D

NEW QUESTION 137

A financial institution would like to store its customer data as it could but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

- A. Asymmetric
- B. Symmetric
- C. Homeomorphic
- D. Ephemeral

Answer: B

NEW QUESTION 140

Which of the following describes the BEST approach for deploying application patches?

- A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
- B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
- C. Test the patches in a test environment apply them to the production systems and then apply them to a staging environment
- D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

Answer: A

NEW QUESTION 143

A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson's laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO's concern?

- A. Deploy an MDM solution.
- B. Implement managed FDE.
- C. Replace all hard drives with SEDs.
- D. Install DLP agents on each laptop.

Answer: B

NEW QUESTION 148

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

- A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.
- B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
- C. Malware trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox
- D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites

Answer: D

NEW QUESTION 149

An attacker is attempting to exploit users by creating a fake website with the URL www.validwebsite.com. The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

- A. Information elicitation
- B. Typo squatting
- C. Impersonation
- D. Watering-hole attack

Answer: D

NEW QUESTION 151

A network administrator at a large organization is reviewing methods to improve the security of the wired LAN. Any security improvement must be centrally managed and allow corporate-owned devices to have access to the intranet but limit others to Internet access only. Which of the following should the administrator recommend?

- A. 802.1X utilizing the current PKI infrastructure
- B. SSO to authenticate corporate users
- C. MAC address filtering with ACLs on the router
- D. PAM for user account management

Answer: A

NEW QUESTION 152

A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

- A. DNSSEC
- B. Reverse proxy
- C. VPN concentrator
- D. PKI
- E. Active Directory
- F. RADIUS

Answer: EF

NEW QUESTION 154

Which of the following would cause a Chief Information Security Officer (CISO) the MOST concern regarding newly installed Internet-accessible 4K surveillance cameras?

- A. An inability to monitor 100% of every facility could expose the company to unnecessary risk.
- B. The cameras could be compromised if not patched in a timely manner.

- C. Physical security at the facility may not protect the cameras from theft.
- D. Exported videos may take up excessive space on the file servers.

Answer: A

NEW QUESTION 159

A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

- A. Corrective
- B. Physical
- C. Detective
- D. Administrative

Answer: C

NEW QUESTION 160

In which of the following common use cases would steganography be employed?

- A. Obfuscation
- B. Integrity
- C. Non-repudiation
- D. Blockchain

Answer: A

NEW QUESTION 162

A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money. Which of the following types of attack is MOST likely being conducted?

- A. SQLi
- B. CSRF
- C. Session replay
- D. API

Answer: C

NEW QUESTION 166

Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?

- A. Data encryption
- B. Data masking
- C. Data deduplication
- D. Data minimization

Answer: B

NEW QUESTION 170

An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

- A. SLA
- B. BPA
- C. NDA
- D. MOU

Answer: A

NEW QUESTION 172

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

Which of the following is the router experiencing?

- A. DDoS attack
- B. Memory leak
- C. Buffer overflow
- D. Resource exhaustion

Answer: D

NEW QUESTION 173

A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

- A. Create a new acceptable use policy.
- B. Segment the network into trusted and untrusted zones.
- C. Enforce application whitelisting.
- D. Implement DLP at the network boundary.

Answer: C

NEW QUESTION 175

An attacker is attempting, to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:
Which of the following should the analyst recommend be enabled?

- A. Input validation
- B. Obfuscation
- C. Error handling
- D. Username lockout

Answer: B

NEW QUESTION 176

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII
- E. Configure the application to encrypt the PII

Answer: D

NEW QUESTION 180

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

NEW QUESTION 183

A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:
www.company.com (main website)
contactus.company.com (for locating a nearby location)
quotes.company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

- A. SAN
- B. Wildcard
- C. Extended validation
- D. Self-signed

Answer: B

NEW QUESTION 186

A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

- A. Nmapn
- B. Heat maps
- C. Network diagrams
- D. Wireshark

Answer: C

NEW QUESTION 190

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

- A. The system was configured with weak default security settings.
- B. The device uses weak encryption ciphers.

- C. The vendor has not supplied a patch for the appliance.
- D. The appliance requires administrative credentials for the assessment.

Answer: C

NEW QUESTION 193

A cybersecurity department purchased a new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

- A. Randomize the shared credentials
- B. Use only guest accounts to connect.
- C. Use SSH keys and remove generic passwords
- D. Remove all user accounts.

Answer: C

NEW QUESTION 198

Which of the following BEST explains the difference between a data owner and a data custodian?

- A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
- B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
- C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
- D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer: B

NEW QUESTION 202

A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

- A. Create consultant accounts for each region, each configured with push MFA notifications.
- B. Create one global administrator account and enforce Kerberos authentication
- C. Create different accounts for each region
- D. Limit their logon times, and alert on risky logins
- E. Create a guest account for each region
- F. Remember the last ten passwords, and block password reuse

Answer: C

NEW QUESTION 203

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

- A. A non-disclosure agreement
- B. Least privilege
- C. An acceptable use policy
- D. Offboarding

Answer: D

NEW QUESTION 207

Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth to be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

- A. Spear phishing
- B. Whaling
- C. Phishing
- D. Vishing

Answer: C

NEW QUESTION 210

A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

- A. Salting the magnetic strip information
- B. Encrypting the credit card information in transit.
- C. Hashing the credit card numbers upon entry.
- D. Tokenizing the credit cards in the database

Answer: C

NEW QUESTION 212

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

- A. Hping3 -s comptia.org -p 80
- B. Nc -1 -v comptia.org -p 80
- C. nmap comptia.org -p 80 -aV
- D. nslookup -port=80 comptia.org

Answer: C

NEW QUESTION 217

Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log in to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)

- A. COPE
- B. VDI
- C. GPS
- D. TOTP
- E. RFID
- F. BYOD

Answer: BE

NEW QUESTION 218

The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

- A. SSO would simplify username and password management, making it easier for hackers to guess accounts.
- B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
- C. SSO would reduce the password complexity for frontline staff.
- D. SSO would reduce the resilience and availability of system if the provider goes offline.

Answer: D

NEW QUESTION 219

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

Answer: C

NEW QUESTION 220

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

NEW QUESTION 224

A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

- A. Physical
- B. Detective
- C. Preventive
- D. Compensating

Answer: D

NEW QUESTION 225

A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

Which of the following will the forensics investigator MOST likely determine has occurred?

- A. SQL injection
- B. CSRF
- C. XSS

D. XSRF

Answer: B

NEW QUESTION 229

The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

- A. Security awareness training
- B. Frequency of NIDS updates
- C. Change control procedures
- D. EDR reporting cycle

Answer: A

NEW QUESTION 234

An organization's finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).

- A. Corrective
- B. Deterrent
- C. Preventive
- D. Mandatory vacations
- E. Job rotation
- F. Separation of duties

Answer: DE

NEW QUESTION 238

When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

- A. Acceptance
- B. Mitigation
- C. Avoidance
- D. Transference

Answer: D

NEW QUESTION 240

The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

- A. Updating the playbooks with better decision points
- B. Dividing the network into trusted and untrusted zones
- C. Providing additional end-user training on acceptable use
- D. Implementing manual quarantining of infected hosts

Answer: A

NEW QUESTION 245

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

NEW QUESTION 249

An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would BEST support the new office?

- A. Always On
- B. Remote access
- C. Site-to-site
- D. Full tunnel

Answer: C

NEW QUESTION 253

Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?

- A. Tabletop
- B. Parallel
- C. Full interruption
- D. Simulation

Answer: A

NEW QUESTION 258

A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

Which of the following BEST describes this kind of attack?

- A. Directory traversal
- B. SQL injection
- C. API
- D. Request forgery

Answer: D

NEW QUESTION 263

A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:

- * Employees must provide an alternate work location (i.e., a home address)
- * Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.

Which of the following BEST describes the MDM options the company is using?

- A. Geofencing, content management, remote wipe, containerization, and storage segmentation
- B. Content management, remote wipe, geolocation, context-aware authentication, and containerization
- C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
- D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

Answer: D

NEW QUESTION 267

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

- A. Least privilege
- B. Awareness training
- C. Separation of duties
- D. Mandatory vacation

Answer: C

NEW QUESTION 269

Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

- A. To provide data to quantify risk based on the organization's systems.
- B. To keep all software and hardware fully patched for known vulnerabilities
- C. To only allow approved, organization-owned devices onto the business network
- D. To standardize by selecting one laptop model for all users in the organization

Answer: A

NEW QUESTION 273

When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

- A. Tokenization
- B. Data masking
- C. Normalization
- D. Obfuscation

Answer: C

NEW QUESTION 275

A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

- A. A capture-the-flag competition
- B. A phishing simulation
- C. Physical security training
- D. Baste awareness training

Answer: B

NEW QUESTION 277

Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?

- A. Something you exhibit
- B. Something you can do
- C. Someone you know
- D. Somewhere you are

Answer: D

NEW QUESTION 282

Which of the following refers to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

Answer: A

NEW QUESTION 286

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

NEW QUESTION 289

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of \$10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

- A. Phishing
- B. Whaling
- C. Typo squatting
- D. Pharming

Answer: B

NEW QUESTION 290

A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:

- Mobile device OSs must be patched up to the latest release
- A screen lock must be enabled (passcode or biometric)
- Corporate data must be removed if the device is reported lost or stolen

Which of the following controls should the security engineer configure? (Select TWO)

- A. Containerization
- B. Storage segmentation
- C. Posturing
- D. Remote wipe

- E. Full-device encryption
- F. Geofencing

Answer: DE

NEW QUESTION 295

Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

- A. Red team
- B. White team
- C. Blue team
- D. Purple team

Answer: A

NEW QUESTION 296

A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN? (Select TWO).

- A. Due to foreign travel, the user's laptop was isolated from the network.
- B. The user's laptop was quarantined because it missed the latest patch update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.
- E. The laptop is still configured to connect to an international mobile network operator.
- F. The user is unable to authenticate because they are outside of the organization's mobile geofencing configuration.

Answer: AB

NEW QUESTION 297

A security engineer needs to implement the following requirements:

- All Layer 2 switches should leverage Active Directory for authentication.
- All Layer 2 switches should use local fallback authentication if Active Directory is offline.
- All Layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Select TWO).

- A. Implement RADIUS.
- B. Configure AAA on the switch with local login as secondary.
- C. Configure port security on the switch with the secondary login method.
- D. Implement TACACS+.
- E. Enable the local firewall on the Active Directory server.
- F. Implement a DHCP server.

Answer: AB

NEW QUESTION 301

After consulting with the Chief Risk Officer (CRO), a manager decides to acquire cybersecurity insurance for the company. Which of the following risk management strategies is the manager adopting?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transference
- D. Risk mitigation

Answer: C

NEW QUESTION 302

A company has limited storage available and online presence that cannot for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time in the event of a failure, while being mindful of the limited available storage space?

- A. Implement full tape backup every Sunday at 8:00 p.m. and perform nightly tape rotations.
- B. Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m.
- C. Implement nightly full backups every Sunday at 8:00 p.m.
- D. Implement full backups every Sunday at 8:00 p.m. and nightly differential backups at 8:00

Answer: B

NEW QUESTION 303

A security administrator needs to inspect in-transit files on the enterprise network to search for PII, credit card data, and classification words. Which of the following would be the BEST to use?

- A. IDS solution
- B. EDR solution
- C. HIPS software solution
- D. Network DLP solution

Answer: D

NEW QUESTION 306

Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

- A. Whaling
- B. Spam
- C. Invoice scam
- D. Pharming

Answer: A

NEW QUESTION 309

A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

- A. OSINT
- B. SIEM
- C. CVSS
- D. CVE

Answer: D

NEW QUESTION 313

The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

- A. Install a NIDS device at the boundary.
- B. Segment the network with firewalls.
- C. Update all antivirus signatures daily.
- D. Implement application blacklisting.

Answer: B

NEW QUESTION 317

An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes. Which of the following is the 60-minute expectation an example of:

- A. MTBF
- B. RPO
- C. MTTR
- D. RTO

Answer: D

NEW QUESTION 318

A bank detects fraudulent activity on user's account. The user confirms transactions completed yesterday on the bank's website at <https://www.company.com>. A security analyst then examines the user's

Internet usage logs and observes the following output: date; username; url;destinationport; responsecode

2020-03-01; userann; http://www.company.org/;80;302; userann: http://www.company.org/secure_login/;80;200

2020-03-01; userann: http://www.company.org/dashboard/;80;200

Which of the following has MOST likely occurred?

- A. Replay attack
- B. SQL injection
- C. SSL stripping
- D. Race conditions

Answer: A

NEW QUESTION 323

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

NEW QUESTION 328

A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

- A. AH
- B. ESP

- C. SRTP
- D. LDAP

Answer: B

NEW QUESTION 332

A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.

Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)

- A. DoS
- B. SSL stripping
- C. Memory leak
- D. Race condition
- E. Shimming
- F. Refactoring

Answer: AD

NEW QUESTION 337

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SY0-601 Practice Exam Features:

- * SY0-601 Questions and Answers Updated Frequently
- * SY0-601 Practice Questions Verified by Expert Senior Certified Staff
- * SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SY0-601 Practice Test Here](#)