

Exam Questions SY0-601

CompTIA Security+ Exam

<https://www.2passeasy.com/dumps/SY0-601/>



NEW QUESTION 1

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 2

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 3

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

- A. Bug bounty
- B. Black-box
- C. Gray-box
- D. White-box

Answer: A

NEW QUESTION 4

A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

- A. A firewall
- B. A device pin
- C. A USB data blocker
- D. Biometrics

Answer: C

NEW QUESTION 5

A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123
```

```
user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

- A. Rainbow table
- B. Brute-force
- C. Password-spraying
- D. Dictionary

Answer: C

NEW QUESTION 6

A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF

- C. Configure WIPS on the APs
- D. Install a captive portal

Answer: D

NEW QUESTION 7

A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

- A. Security
- B. Application
- C. Dump
- D. Syslog

Answer: C

NEW QUESTION 8

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?

- 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 path update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.

Answer: A

NEW QUESTION 9

Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

- A. The employee's physical access card was cloned.
- B. The employee is colluding with human resources
- C. The employee's biometrics were harvested
- D. A criminal used lock picking tools to open the door.

Answer: A

NEW QUESTION 10

Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

- A. SIEM
- B. CASB
- C. UTM
- D. DLP

Answer: D

NEW QUESTION 10

A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

- A. Man-in-the-middle
- B. Spear-phishing
- C. Evil twin
- D. DNS poisoning

Answer: D

NEW QUESTION 15

A symmetric encryption algorithm is BEST suited for:

- A. key-exchange scalability.
- B. protecting large amounts of data.
- C. providing hashing capabilities,
- D. implementing non-repudiation.

Answer: D

NEW QUESTION 18

A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an item, the password for the wireless network is printed on the receipt so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

- A. WPA-EAP
- B. WEP-TKIP
- C. WPA-PSK
- D. WPS-PIN

Answer: A

NEW QUESTION 23

A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

- A. PCI DSS
- B. ISO 22301
- C. ISO 27001
- D. NIST CSF

Answer: A

NEW QUESTION 27

Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continues to evade detection. Which of the following should administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

Answer: C

NEW QUESTION 29

A network administrator would like to configure a site-to-site VPN utilizing iPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions Which of the following should the administrator use when configuring the VPN?

- A. AH
- B. EDR
- C. ESP
- D. DNSSEC

Answer: C

NEW QUESTION 34

A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?

- A. Role-based access control
- B. Discretionary access control
- C. Mandatory access control
- D. Attribute-based access control

Answer: B

NEW QUESTION 37

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 40

A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

* Protection from power outages

* Always-available connectivity In case of an outage

The owner has decided to implement battery backups for the computer equipment Which of the following would BEST fulfill the owner's second need?

- A. Lease a point-to-point circuit to provide dedicated access.
- B. Connect the business router to its own dedicated UPS.
- C. Purchase services from a cloud provider for high availability
- D. Replace the business's wired network with a wireless network.

Answer: C

NEW QUESTION 44

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO).

- A. Full-device encryption
- B. Network usage rules
- C. Geofencing
- D. Containerization
- E. Application whitelisting
- F. Remote control

Answer: AB

NEW QUESTION 48

A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

- A. The scan results show open ports, protocols, and services exposed on the target host
- B. The scan enumerated software versions of installed programs
- C. The scan produced a list of vulnerabilities on the target host
- D. The scan identified expired SSL certificates

Answer: B

NEW QUESTION 52

A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this task?

- A. Netcat
- B. Netstat
- C. Nmap
- D. Nessus

Answer: B

NEW QUESTION 57

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 62

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 63

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 66

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 69

An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

- A. Order of volatility
- B. Data recovery
- C. Chain of custody
- D. Non-repudiation

Answer: C

NEW QUESTION 72

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 73

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 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 77

A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

- A. Loss of proprietary information
- B. Damage to the company's reputation
- C. Social engineering
- D. Credential exposure

Answer: C

NEW QUESTION 82

The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

- A. data controller.
- B. data owner
- C. data custodian.
- D. data processor

Answer: D

NEW QUESTION 84

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 87

A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa;b6a3:1212	Dynamic	GE0/5
1	2025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

- A. MAC Flooding
- B. DNS poisoning
- C. MAC cloning
- D. ARP poisoning

Answer: A

NEW QUESTION 91

After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

- A. Multifactor authentication
- B. Something you can do
- C. Biometric
- D. Two-factor authentication

Answer: D

NEW QUESTION 94

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 98

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 103

A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sample.url.sampleurl.com/malicious-dns-redirect
```

- A. Option A
- B. Option B

- C. Option C
- D. Option D

Answer: B

NEW QUESTION 108

Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

- A. DDoS
- B. Man-in-the-middle
- C. MAC flooding
- D. Domain hijacking

Answer: A

NEW QUESTION 110

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: D

NEW QUESTION 115

A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

- A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
- B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
- C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
- D. Refrain from completing a forensic analysts of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

Answer: D

NEW QUESTION 117

A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

- A. IPSec
- B. Always On
- C. Split tunneling
- D. L2TP

Answer: B

NEW QUESTION 119

Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?

- A. Footprinting
- B. White-box testing
- C. A drone/UAV
- D. Pivoting

Answer: A

NEW QUESTION 124

A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:

`http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us`

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

`http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us` Which of the following application attacks is being tested?

- A. Pass-the-hash
- B. Session replay
- C. Object deference
- D. Cross-site request forgery

Answer: B

NEW QUESTION 125

Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

- A. Testing security systems and processes regularly
- B. Installing and maintaining a web proxy to protect cardholder data
- C. Assigning a unique ID to each person with computer access
- D. Encrypting transmission of cardholder data across private networks
- E. Benchmarking security awareness training for contractors
- F. Using vendor-supplied default passwords for system passwords

Answer: BD

NEW QUESTION 127

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 128

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 129

Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

- A. Cross-site scripting
- B. Data exfiltration
- C. Poor system logging
- D. Weak encryption
- E. SQL injection
- F. Server-side request forgery

Answer: DF

NEW QUESTION 130

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: A

NEW QUESTION 131

A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

- A. An air gap
- B. A Faraday cage
- C. A shielded cable
- D. A demilitarized zone

Answer: A

NEW QUESTION 135

An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:

```
Hello everyone,  
I am having the same problem with my server. Can you help me?  
  
<script type="text/javascript" src=http://website.com/user.js>  
Onload=sqlexec();  
</script>  
  
Thank you,  
  
Joe
```

Which of the following BEST describes the attack that was attempted against the forum readers?

- A. SOU attack
- B. DLL attack
- C. XSS attack
- D. API attack

Answer: C

NEW QUESTION 140

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 141

An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?

- A. Document the collection and require a sign-off when possession changes.
- B. Lock the device in a safe or other secure location to prevent theft or alteration.
- C. Place the device in a Faraday cage to prevent corruption of the data.
- D. Record the collection in a blockchain-protected public ledger.

Answer: A

NEW QUESTION 142

A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

- A. SIEM
- B. DLP
- C. CASB
- D. SWG

Answer: C

NEW QUESTION 147

A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

```

Commands
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
    
```

```

SSH Client
?
    
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

Commands
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
    
```

```

SSH Client
ssh root@server
scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys
ssh -i ~/.ssh/id_rsa user@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
chmod 777 ~/.ssh/authorized_keys
chmod 644 ~/.ssh/id_rsa
    
```

NEW QUESTION 149

Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function properly. Which of the following should the security administrator consider implementing to address this issue?

- A. Application code signing
- B. Application whitelisting
- C. Data loss prevention
- D. Web application firewalls

Answer: B

NEW QUESTION 150

While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

- A. A RAT was installed and is transferring additional exploit tools.
- B. The workstations are beaconing to a command-and-control server.
- C. A logic bomb was executed and is responsible for the data transfers.
- D. A fireless virus is spreading in the local network environment.

Answer: A

NEW QUESTION 151

A database administrator needs to ensure all passwords are stored in a secure manner, so the administrator adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

- A. Predictability
- B. Key stretching
- C. Salting
- D. Hashing

Answer: C

NEW QUESTION 153

An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?

- A. NGFW
- B. Pagefile
- C. NetFlow
- D. RAM

Answer: C

NEW QUESTION 156

A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?

- A. The S/MIME plug-in is not enabled.
- B. The SLL certificate has expired.
- C. Secure IMAP was not implemented
- D. POP3S is not supported.

Answer: A

NEW QUESTION 160

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

- A. Session replay
- B. Evil twin
- C. Bluejacking
- D. ARP poisoning

Answer: B

NEW QUESTION 163

An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate datacenter that houses confidential information. There is a firewall at the Internet border followed by a DLP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?

- A. The DLP appliance should be integrated into a NGFW.
- B. Split-tunnel connections can negatively impact the DLP appliance's performance
- C. Encrypted VPN traffic will not be inspected when entering or leaving the network
- D. Adding two hops in the VPN tunnel may slow down remote connections

Answer: C

NEW QUESTION 165

Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

- A. The data protection officer
- B. The data processor
- C. The data owner
- D. The data controller

Answer: C

NEW QUESTION 167

A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plain text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

- A. Create DLP controls that prevent documents from leaving the network
- B. Implement salting and hashing
- C. Configure the web content filter to block access to the forum.
- D. Increase password complexity requirements

Answer: A

NEW QUESTION 170

A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

- A. Monitoring large data transfer transactions in the firewall logs
- B. Developing mandatory training to educate employees about the removable media policy
- C. Implementing a group policy to block user access to system files
- D. Blocking removable-media devices and write capabilities using a host-based security tool

Answer: D

NEW QUESTION 171

A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization's network. Which of the following will the analyst MOST likely use to accomplish the objective?

- A. A table exercise
- B. NST CSF
- C. MTRE ATT\$CK
- D. OWASP

Answer: A

NEW QUESTION 173

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File level encryption
- E. USB blocker
- F. MFA

Answer: BE

NEW QUESTION 177

An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:

```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdfdocx.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

- A. The end user purchased and installed a PUP from a web browser
- B. A bot on the computer is brute forcing passwords against a website
- C. A hacker is attempting to exfiltrate sensitive data
- D. Ransomware is communicating with a command-and-control server.

Answer: A

NEW QUESTION 181

Which of the following ISO standards is certified for privacy?

- A. ISO 9001
- B. ISO 27002
- C. ISO 27701
- D. ISO 31000

Answer: C

NEW QUESTION 184

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-601 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-601 Product From:

<https://www.2passeasy.com/dumps/SY0-601/>

Money Back Guarantee

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