

# CompTIA

## Exam Questions SY0-601

CompTIA Security+ Exam



#### NEW QUESTION 1

A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security. Which of the following controls will the analyst MOST likely recommend?

- A. MAC
- B. ACL
- C. BPDU
- D. ARP

**Answer:** A

#### NEW QUESTION 2

An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

- A. business continuity plan
- B. communications plan.
- C. disaster recovery plan.
- D. continuity of operations plan

**Answer:** C

#### NEW QUESTION 3

A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

- A. Something you know
- B. Something you have
- C. Somewhere you are
- D. Someone you are
- E. Something you are
- F. Something you can do

**Answer:** BE

#### NEW QUESTION 4

A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

- A. False rejection
- B. Cross-over error rate
- C. Efficacy rate
- D. Attestation

**Answer:** B

#### NEW QUESTION 5

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 6

A user contacts the help desk to report the following:

- Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
- The user was able to access the Internet but had trouble accessing the department share until the next day.
- The user is now getting notifications from the bank about unauthorized transactions. Which of the following attack vectors was MOST likely used in this scenario?

- A. Rogue access point
- B. Evil twin
- C. DNS poisoning
- D. ARP poisoning

**Answer:** A

#### NEW QUESTION 7

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 8

Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

- A. The data owner
- B. The data processor
- C. The data steward
- D. The data privacy officer.

**Answer:** C

#### NEW QUESTION 9

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 10

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 10

A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

- A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
- B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
- C. Deny unauthenticated users access to shared network folders.
- D. Verify computers are set to install monthly operating system, updates automatically.

**Answer:** A

#### NEW QUESTION 12

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 13

To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

- A. A password reuse policy
- B. Account lockout after three failed attempts
- C. Encrypted credentials in transit
- D. A geofencing policy based on login history

**Answer:** C

#### NEW QUESTION 15

A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

- A. Open the document on an air-gapped network
- B. View the document's metadata for origin clues
- C. Search for matching file hashes on malware websites
- D. Detonate the document in an analysis sandbox

**Answer: D**

#### NEW QUESTION 16

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

- A. Upgrade the bandwidth available into the datacenter
- B. Implement a hot-site failover location
- C. Switch to a complete SaaS offering to customers
- D. Implement a challenge response test on all end-user queries

**Answer: B**

#### NEW QUESTION 17

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 21

A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

- A. Create an OCSP
- B. Generate a CSR
- C. Create a CRL
- D. Generate a .pfx file

**Answer: B**

#### NEW QUESTION 25

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 28

An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

- A. Nmap
- B. cURL
- C. Netcat
- D. Wireshark

**Answer: D**

#### NEW QUESTION 30

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 34

A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

- A. Dual power supply
- B. Off-site backups
- C. Automatic OS upgrades
- D. NIC teaming
- E. Scheduled penetration testing
- F. Network-attached storage

**Answer:** AB

#### NEW QUESTION 35

A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

- A. Code signing
- B. Fuzzing
- C. Manual code review
- D. Dynamic code analysis

**Answer:** D

#### NEW QUESTION 39

A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

- A. DNS sinkholding
- B. DLP rules on the terminal
- C. An IP blacklist
- D. Application whitelisting

**Answer:** D

#### NEW QUESTION 44

Which of the following describes the ability of code to target a hypervisor from inside

- A. Fog computing
- B. VM escape
- C. Software-defined networking
- D. Image forgery
- E. Container breakout

**Answer:** B

#### NEW QUESTION 49

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 50

A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@  WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!  @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+lfhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

- A. MAC cloning
- B. Evil twin
- C. Man-in-the-middle
- D. ARP poisoning

**Answer: C**

#### NEW QUESTION 54

Which of the following algorithms has the SMALLEST key size?

- A. DES
- B. Twofish
- C. RSA
- D. AES

**Answer: B**

#### NEW QUESTION 55

Which of the following scenarios BEST describes a risk reduction technique?

- A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
- B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
- C. A security control objective cannot be met through a technical change, so the company changes as method of operation
- D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

**Answer: B**

#### NEW QUESTION 58

An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

- A. SED
- B. HSM
- C. DLP
- D. TPM

**Answer: A**

#### NEW QUESTION 62

A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

- A. A rainbow table attack
- B. A password-spraying attack
- C. A dictionary attack
- D. A keylogger attack

**Answer: C**

#### NEW QUESTION 63

A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

- A. Configuring signature-based antivirus to update every 30 minutes
- B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
- C. Implementing application execution in a sandbox for unknown software.
- D. Fuzzing new files for vulnerabilities if they are not digitally signed

**Answer: C**

#### NEW QUESTION 68

A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

- A. CASB
- B. SWG



- C. Containerization
- D. Automated failover

**Answer: C**

#### NEW QUESTION 70

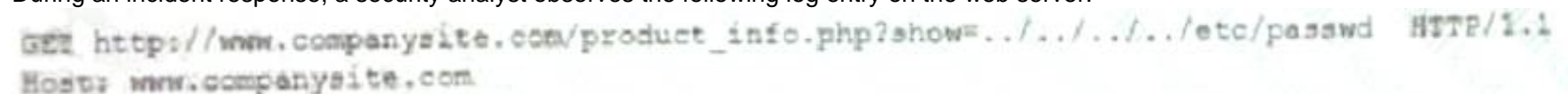
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load. Which of the following are the BEST options to accomplish this objective? (Select TWO)

- A. Load balancing
- B. Incremental backups
- C. UPS
- D. RAID
- E. Dual power supply
- F. NIC teaming

**Answer: AD**

#### NEW QUESTION 72

During an incident response, a security analyst observes the following log entry on the web server.



Which of the following BEST describes the type of attack the analyst is experiencing?

- A. SQL injection
- B. Cross-site scripting
- C. Pass-the-hash
- D. Directory traversal

**Answer: B**

#### NEW QUESTION 75

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	8025:2ad8: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 76

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 79

A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

- A. The GPS location
- B. When the file was deleted
- C. The total number of print jobs
- D. The number of copies made

**Answer: A**

**NEW QUESTION 84**

A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

- A. Developing an incident response plan
- B. Building a disaster recovery plan
- C. Conducting a tabletop exercise
- D. Running a simulation exercise

**Answer:** C

**NEW QUESTION 86**

A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

- A. OAuth
- B. SSO
- C. SAML
- D. PAP

**Answer:** C

**NEW QUESTION 89**

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:

```
CPU 0 percent busy, from 300 sec ago
 1 sec ave: 99 percent busy
 5 sec ave: 97 percent busy
 1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

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

**Answer:** D

**NEW QUESTION 91**

A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two- drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

- A. 1
- B. 5
- C. 6

**Answer:** B

**NEW QUESTION 94**

Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

- A. Investigation
- B. Containment
- C. Recovery
- D. Lessons learned

**Answer:** B

**NEW QUESTION 95**

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 100**

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 101

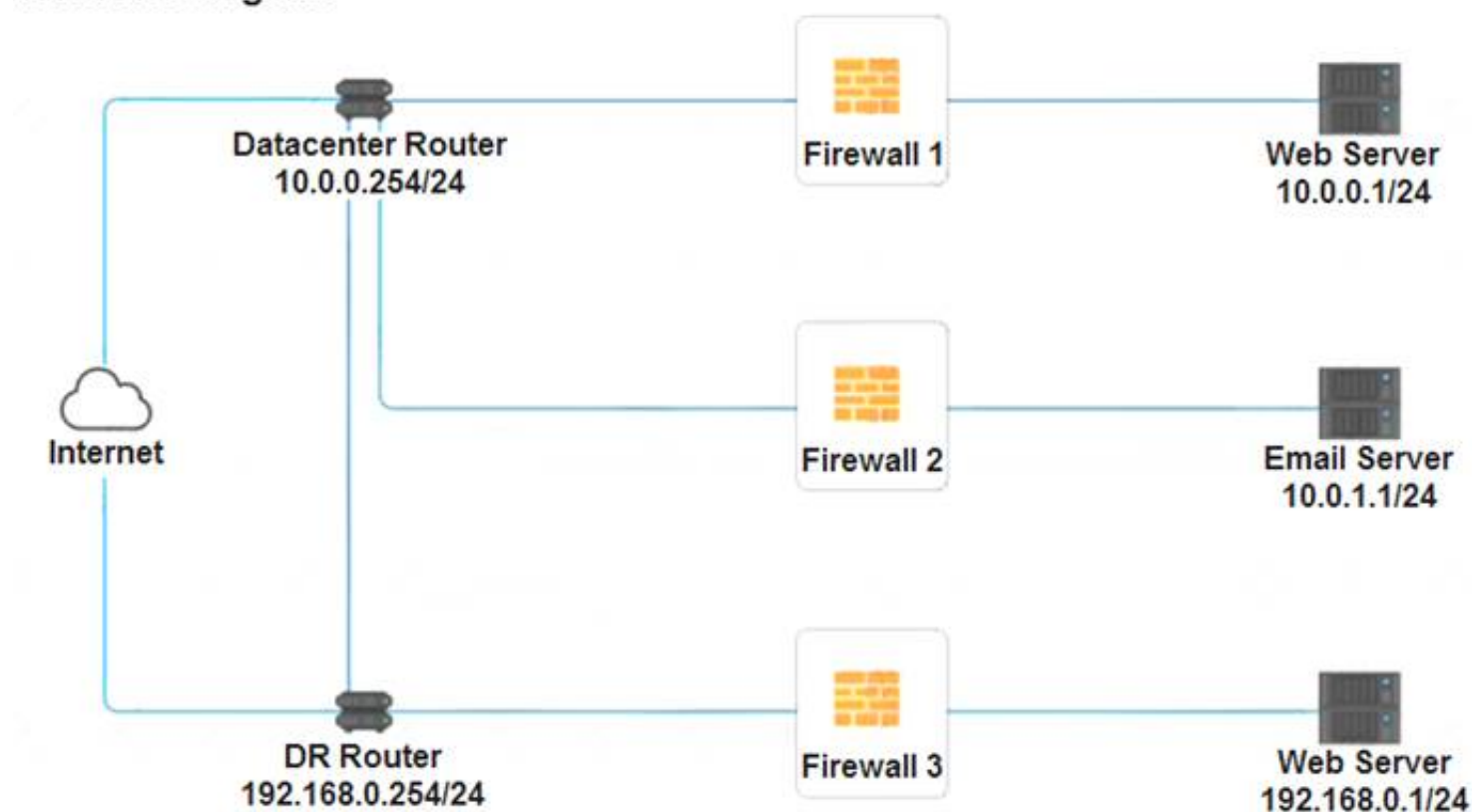
A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites. INSTRUCTIONS  
 Click on each firewall to do the following:

- > Deny cleartext web traffic.
- > Ensure secure management protocols are used.
- > Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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

#### Network Diagram



**Firewall 1**
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
Management	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>

Reset Answer
Save
Close

**Firewall 2**
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
Management	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>

Reset Answer
Save
Close



**Firewall 3**
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
Management	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px;">           PERMIT            DENY         </div>

Reset Answer
Save
Close

A.

**Answer:** A

**Explanation:**

See explanation below.

Explanation

Firewall 1:

Firewall 1					
Rule Name	Source	Destination	Service	Action	
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT	•
HTTPS Outbound	10.0.0.1/24	• ANY	• HTTPS	• PERMIT	•
Management	ANY	• 10.0.0.1/24	• SSH	• PERMIT	•
HTTPS Inbound	ANY	• 10.0.0.1/24	• HTTPS	• PERMIT	•
HTTP Inbound	ANY	• 10.0.0.1/24	• HTTP	• DENY	•
<div>Reset Answer</div> <div>Save</div> <div>Close</div>					

Firewall 1					
Rule Name	Source	Destination	Service	Action	
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT	•
HTTPS Outbound	10.0.0.1/24	• ANY	• HTTPS	• PERMIT	•
Management	ANY	• 10.0.0.1/24	• SSH	• PERMIT	•
HTTPS Inbound	ANY	• 10.0.0.1/24	• HTTPS	• PERMIT	•
HTTP Inbound	ANY	• 10.0.0.1/24	• HTTP	• DENY	•
<div>Reset Answer</div> <div>Save</div> <div>Close</div>					

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Firewall 2:

Firewall 2					
Rule Name	Source	Destination	Service	Action	
DNS Rule	10.0.1.1/24	• ANY	• DNS	• PERMIT	•
HTTPS Outbound	10.0.1.1/24	• ANY	• HTTPS	• PERMIT	•
Management	ANY	• 10.0.1.1/24	• DNS	• PERMIT	•
HTTPS Inbound	ANY	• 10.0.1.1/24	• HTTPS	• PERMIT	•
HTTP Inbound	ANY	• 10.0.1.1/24	• HTTP	• DENY	•
<div>Reset Answer</div> <div>Save</div> <div>Close</div>					

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	10.0.1.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 10.0.1.1/24	• DNS	• PERMIT
HTTPS Inbound	ANY	• 10.0.1.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 10.0.1.1/24	• HTTP	• DENY
<div>Reset AnswerSaveClose</div>				

Firewall 3:

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	192.168.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 192.168.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 192.168.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 192.168.0.1/24	• HTTP	• DENY
<div>Reset AnswerSaveClose</div>				

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	192.168.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 192.168.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 192.168.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 192.168.0.1/24	• HTTP	• DENY
<div>Reset AnswerSaveClose</div>				

DNS Rule – ANY --> ANY --> DNS --> PERMIT  
HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT  
Management – ANY --> ANY --> SSH --> PERMIT  
HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT  
HTTP Inbound – ANY --> ANY --> HTTP --> DENY

NEW QUESTION 106

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 109

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

**Answer:** AE

#### NEW QUESTION 111

The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in 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 pass 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 115

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 120

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 123

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 125

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.

visit - <https://www.surepassexam.com>

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 132

A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money than it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

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

**Answer:** C

#### NEW QUESTION 136

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 141

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 gets 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 142

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate devices using PKI. Which of the following should the administrator configure?

- A. A captive portal
- B. PSK
- C. 802.1X
- D. WPS

**Answer:** C

#### NEW QUESTION 147

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. Nmap
- B. Heat maps
- C. Network diagrams
- D. Wireshark

**Answer:** C

**NEW QUESTION 150**

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 155**

A forensics examiner is attempting to dump password cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

- A. The examiner does not have administrative privileges to the system
- B. The system must be taken offline before a snapshot can be created
- C. Checksum mismatches are invalidating the disk image
- D. The swap file needs to be unlocked before it can be accessed

**Answer:** A

**NEW QUESTION 160**

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 164**

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 169**

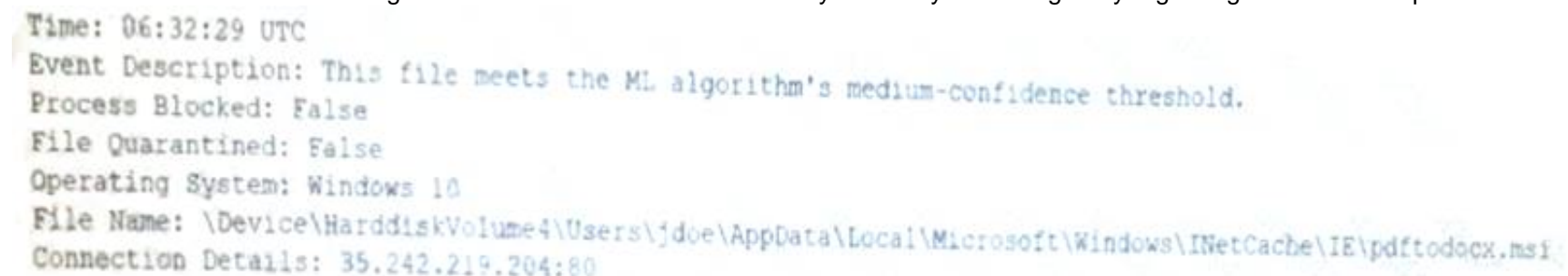
An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

- A. Screen locks
- B. Application management
- C. Geofencing
- D. Containerization

**Answer:** D

**NEW QUESTION 173**

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\pdftodocx.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 175**

.....



## 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](#)**