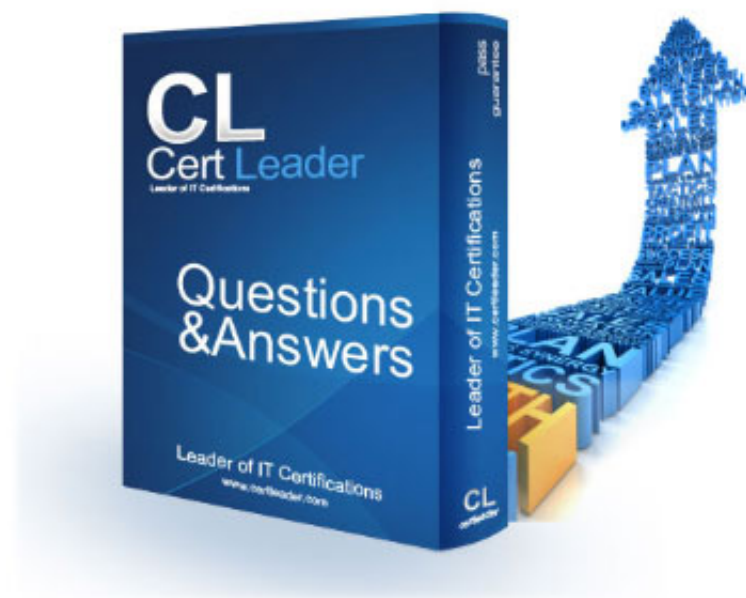


SY0-601 Dumps

CompTIA Security+ Exam

<https://www.certleader.com/SY0-601-dumps.html>



NEW QUESTION 1

Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

- A. Watering-hole attack
- B. Credential harvesting
- C. Hybrid warfare
- D. Pharming

Answer: A

NEW QUESTION 2

A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

Answer: D

NEW QUESTION 3

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- Check-in/checkout of credentials
- The ability to use but not know the password
- Automated password changes
- Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

Answer: D

NEW QUESTION 4

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 5

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 6

A security assessment determines DES and 3DES at still being used on recently deployed production servers. Which of the following did the assessment identify?

- A. Unsecre protocols
- B. Default settings
- C. Open permissions
- D. Weak encryption

Answer: D

NEW QUESTION 7

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 8

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 9

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 10

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 10

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 13

A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

- A. Segmentation
- B. Firewall whitelisting
- C. Containment
- D. isolation

Answer: A

NEW QUESTION 16

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 17

Which of the following relates 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 21

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 22

A malicious actor recently penetrated 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 25

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 29

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 30

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 32

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 37

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 38

The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the following would BEST address this security concern?

- A. install a smart meter on the staff WiFi.
- B. Place the environmental systems in the same DHCP scope as the staff WiFi.
- C. Implement Zigbee on the staff WiFi access points.
- D. Segment the staff WiFi network from the environmental systems network.

Answer: D

NEW QUESTION 40

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 42

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 44

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 45

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 50

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 53

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 54

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 59

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 63

Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
- B. DNS query logging
- C. Exact mail exchanger records in the DNS
- D. The addition of DNS conditional forwarders

Answer: C

NEW QUESTION 64

A worldwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

- A. Network location
- B. Impossible travel time
- C. Geolocation
- D. Geofencing

Answer: D

NEW QUESTION 69

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 73

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 74

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 78

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force
- D. Spraying

Answer: D

NEW QUESTION 82

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 84

A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.

An incident responder learns the following information:

- The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs.
- All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.
- Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

- A. HTTPS sessions are being downgraded to insecure cipher suites
- B. The SSL inspection proxy is feeding events to a compromised SIEM
- C. The payment providers are insecurely processing credit card charges
- D. The adversary has not yet established a presence on the guest WiFi network

Answer: C

NEW QUESTION 87

A company uses wireless for all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

- A. A BPDU guard
- B. WPA-EAP
- C. IP filtering
- D. A WIDS

Answer: B

NEW QUESTION 88

An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

- A. Date of birth
- B. Fingerprints
- C. PIN
- D. TPM

Answer: B

NEW QUESTION 89

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 90

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

- A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
- B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
- C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
- D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

NEW QUESTION 91

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

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.

NEW QUESTION 94

- A. An external security assessment
- B. A bug bounty program
- C. A tabletop exercise
- D. A red-team engagement

NEW QUESTION 96

- www.company.com (main website)
- contactus.company.com (for locating a nearby location)
- quotes.company.com (for requesting a price quote)

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

NEW QUESTION 98

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

NEW QUESTION 101

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@  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:cBqYjal6ToV3jEIJHUSKtjjVzignVd4Cz+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.

```

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

NEW QUESTION 105

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 107

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 111

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 112

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 116

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 121

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 125

An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering if the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?

- A. Disallow new hires from using mobile devices for six months
- B. Select four devices for the sales department to use in a CYOD model
- C. Implement BYOD for the sales department while leveraging the MDM
- D. Deploy mobile devices using the COPE methodology

Answer: C

NEW QUESTION 129

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 130

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 fulltape 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 133

The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

- A. A script kiddie
- B. Shadow IT
- C. Hacktivism
- D. White-hat

Answer: B

NEW QUESTION 137

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 140

A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

- A. SDP
- B. AAA
- C. IaaS
- D. MSSP
- E. Microservices

Answer: D

NEW QUESTION 142

Which of the following is the purpose of a risk register?

- A. To define the level of risk using probability and likelihood
- B. To register the risk with the required regulatory agencies
- C. To identify the risk, the risk owner, and the risk measures
- D. To formally log the type of risk mitigation strategy the organization is using

Answer: C

NEW QUESTION 143

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 148

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 152

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 156

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 158

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:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```

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 159

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 161

A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

- A. Automated information sharing
- B. Open-source intelligence
- C. The dark web
- D. Vulnerability databases

Answer: C

NEW QUESTION 164

A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

- A. Security information and event management
- B. A web application firewall
- C. A vulnerability scanner
- D. A next-generation firewall

Answer: A

NEW QUESTION 168

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 170

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 175

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 176

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 180

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 183

A security analyst is investigating an incident that was first reported as an issue connecting to network shares and the internet. While reviewing logs and tool output, the analyst sees the following:

IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?

- A. IP conflict
- B. Pass-the-hash
- C. MAC flooding
- D. Directory traversal
- E. ARP poisoning

Answer: E

NEW QUESTION 187

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 190

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 195

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 199

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 204

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 205

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 208

A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

- A. Recovery
- B. Identification
- C. Lessons learned
- D. Preparation

Answer: C

NEW QUESTION 213

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 218

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites. INSTRUCTIONS

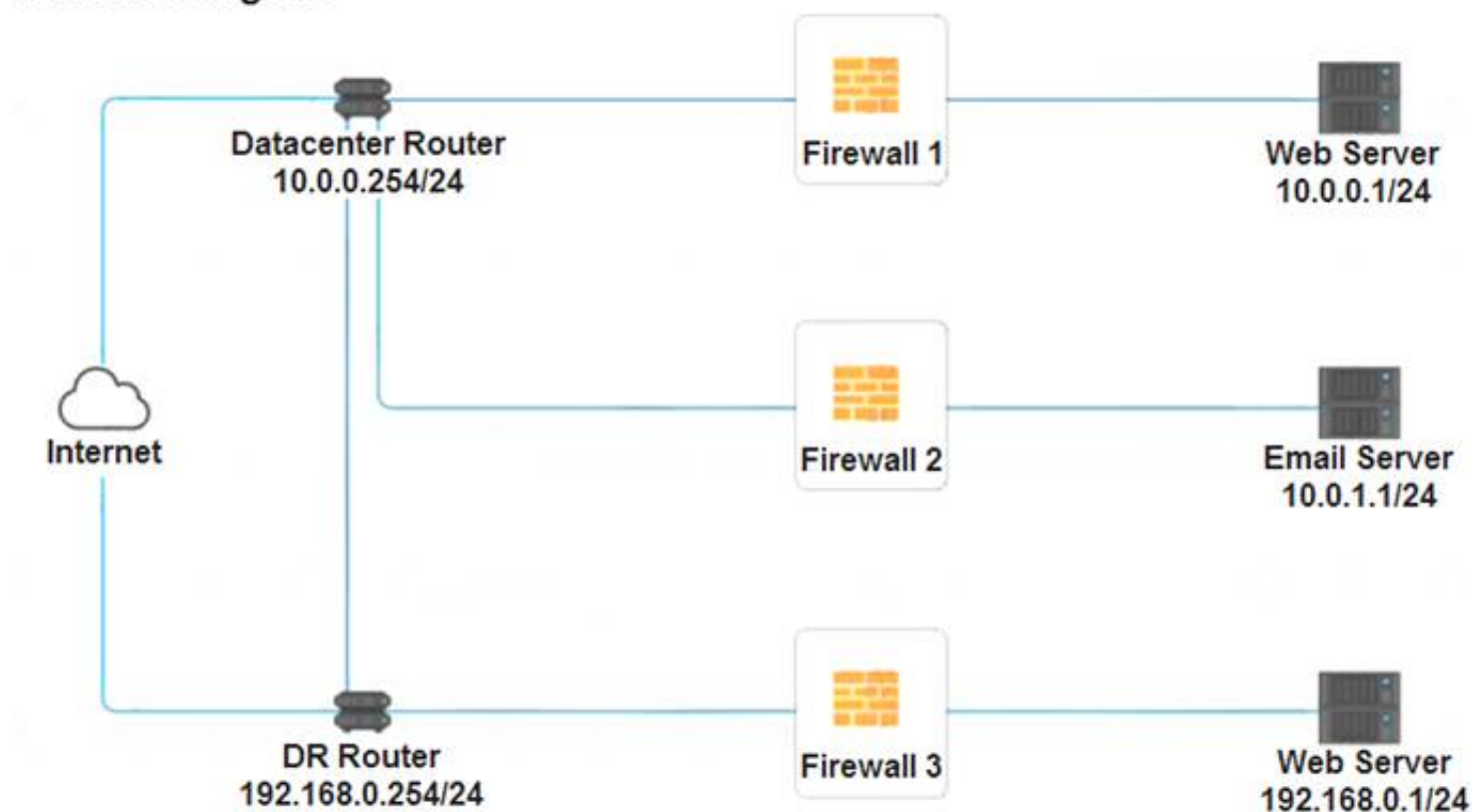
Click on each firewall to do the following:

- 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> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT DENY </div>
HTTPS Outbound	<div> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT DENY </div>
Management	<div> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT DENY </div>
HTTPS Inbound	<div> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT DENY </div>
HTTP Inbound	<div> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY DNS HTTP HTTPS TELNET SSH </div>	<div> <div></div> <div>▼</div> </div> <div> 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: 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

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

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

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

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 220

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 224

A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

- A. Verification
- B. Validation
- C. Normalization
- D. Staging

Answer: A

NEW QUESTION 225

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. Ofboarding

Answer: D

NEW QUESTION 230

A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?

- A. Checksums
- B. Watermarks
- C. Oder of volatility
- D. A log analysis
- E. A right-to-audit clause

Answer: D

NEW QUESTION 231

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 233

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 236

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 238

Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

- A. Alarms
- B. Signage
- C. Lighting
- D. Mantraps
- E. Fencing
- F. Sensors

Answer: DE

NEW QUESTION 243

A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

- A. Containerization
- B. Geofencing
- C. Full-disk encryption
- D. Remote wipe

Answer: C

NEW QUESTION 248

A security administrator needs to create a RAIS configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drives will fail simultaneously. Which of the following RAID configurations should the administration use?

- A. RA1D 0
- B. RAID1
- C. RAID 5
- D. RAID 10

Answer: C

NEW QUESTION 253

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 256

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 257

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 258

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 DIP 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 259

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 261

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 264

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device 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 268

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 271

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 273

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 274

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 277

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 282

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 286

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 288

A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

- A. Trusted Platform Module
- B. A host-based firewall
- C. A DLP solution
- D. Full disk encryption
- E. A VPN
- F. Antivirus software

Answer: AB

NEW QUESTION 292

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 293

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SY0-601 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SY0-601-dumps.html>