EXAMTOPICS

Topic 1 - Exam A

Question #1 *Topic 1*

Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

A. Hacktivist

B. Whistleblower

C. Organized crime Most Voted

D. Unskilled attacker

Correct Answer: *C*

Community vote distribution

C (76%) A (24%)

Question #2 *Topic 1*

Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching

B. Data masking

C. Steganography

D. Salting Most Voted

Correct Answer: *D*

Community vote distribution

D (88%) 12%

Question #3 *Topic 1*

An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a “page not found” error message. Which of the following types of social engineering attacks occurred?

A. Brand impersonation

B. Pretexting

C. Typosquatting

D. Phishing Most Voted

Correct Answer: *D*

Community vote distribution

D (91%) 6%

Question #4 *Topic 1*

An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53

B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53

D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53 Most Voted

Correct Answer: *D*

Community vote distribution

D (94%) 6%

Question #5 *Topic 1*

A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

A. SSO Most Voted

B. LEAP

C. MFA

D. PEAP

Correct Answer: *A*

Community vote distribution

A (100%)

Question #6 *Topic 1*

Which of the following scenarios describes a possible business email compromise attack?

A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.

B. Employees who open an email attachment receive messages demanding payment in order to access files.

C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account. Most Voted

D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Correct Answer: *C*

Community vote distribution

C (52%) A (39%) 8%

Question #7 *Topic 1*

A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the database servers?

A. Jump server Most Voted

B. RADIUS

C. HSM

D. Load balancer

Correct Answer: *A*

Community vote distribution

A (100%)

Question #8 *Topic 1*

An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?

A. NGFW

B. WAF Most Voted

C. TLS

D. SD-WAN

Correct Answer: *B*

Community vote distribution

B (78%) A (22%)

Question #9 *Topic 1*

An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A. Multifactor authentication Most Voted

B. Permissions assignment

C. Access management

D. Password complexity

Correct Answer: *A*

Community vote distribution

A (100%)

Question #10 *Topic 1*

An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

A. Typosquatting

B. Phishing

C. Impersonation Most Voted

D. Vishing

E. Smishing Most Voted

F. Misinformation

Correct Answer: *CE*

Community vote distribution

CE (88%) 12%

Question #11 *Topic 1*

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated: "I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."
Which of the following are the best responses to this situation? (Choose two).

A. Cancel current employee recognition gift cards.

B. Add a smishing exercise to the annual company training. Most Voted

C. Issue a general email warning to the company. Most Voted

D. Have the CEO change phone numbers.

E. Conduct a forensic investigation on the CEO's phone.

F. Implement mobile device management.

Correct Answer: *BC*

Community vote distribution

BC (92%) 8%

Question #12 *Topic 1*

A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

A. A thorough analysis of the supply chain Most Voted

B. A legally enforceable corporate acquisition policy

C. A right to audit clause in vendor contracts and SOWs

D. An in-depth penetration test of all suppliers and vendors

Correct Answer: *A*

Community vote distribution

A (78%) C (23%)

Question #13 *Topic 1*

Which of the following provides the details about the terms of a test with a third-party penetration tester?

A. Rules of engagement Most Voted

B. Supply chain analysis

C. Right to audit clause

D. Due diligence

Correct Answer: *A*

Community vote distribution

A (96%) 4%

Question #14 *Topic 1*

A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

A. Active Most Voted

B. Passive

C. Defensive

D. Offensive

Correct Answer: *A*

Community vote distribution

A (100%)

Question #15 *Topic 1*

Which of the following is required for an organization to properly manage its restore process in the event of system failure?

A. IRP

B. DRP Most Voted

C. RPO

D. SDLC

Correct Answer: *B*

Community vote distribution

B (96%) 4%

Question #16 *Topic 1*

Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

A. Jailbreaking

B. Memory injection

C. Resource reuse

D. Side loading Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #17 *Topic 1*

A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

A. Password spraying Most Voted

B. Account forgery

C. Pass-the-hash

D. Brute-force

Correct Answer: *A*

Community vote distribution

A (100%)

Question #18 *Topic 1*

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

A. Secured zones

B. Subject role Most Voted

C. Adaptive identity

D. Threat scope reduction

Correct Answer: *B*

Community vote distribution

B (38%) A (37%) D (17%) 8%

Question #19 *Topic 1*

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

A. RDP server

B. Jump server Most Voted

C. Proxy server

D. Hypervisor

Correct Answer: *B*

Community vote distribution

B (97%)

Question #20 *Topic 1*

A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

A. encryption=off

B. http:// Most Voted

C. www.*.com

D. :443

Correct Answer: *B*

Community vote distribution

B (100%)

Question #21 *Topic 1*

During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32

B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0 Most Voted

C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0

D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Correct Answer: *B*

Community vote distribution

B (100%)

Question #22 *Topic 1*

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

A. Implementing a bastion host Most Voted

B. Deploying a perimeter network

C. Installing a WAF

D. Utilizing single sign-on

Correct Answer: *A*

Community vote distribution

A (88%) 6%

Question #23 *Topic 1*

A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

A. Application

B. IPS/IDS

C. Network

D. Endpoint Most Voted

Correct Answer: *D*

Community vote distribution

D (83%) Other

Question #24 *Topic 1*

A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks.
SIEM alerts have not yet been configured. Which of the following best describes what the security analyst should do to identify this behavior?

A. Digital forensics

B. E-discovery

C. Incident response

D. Threat hunting Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #25 *Topic 1*

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

A. Accept

B. Transfer Most Voted

C. Mitigate

D. Avoid

Correct Answer: *B*

Community vote distribution

B (86%) 14%

Question #26 *Topic 1*

A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

A. Partition

B. Asymmetric

C. Full disk Most Voted

D. Database

Correct Answer: *C*

Community vote distribution

C (100%)

Question #27 *Topic 1*

Which of the following security control types does an acceptable use policy best represent?

A. Detective

B. Compensating

C. Corrective

D. Preventive Most Voted

Correct Answer: *D*

Community vote distribution

D (92%) 8%

Question #28 *Topic 1*

An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

A. Hardening

B. Employee monitoring

C. Configuration enforcement

D. Least privilege Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #29 *Topic 1*

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

A. Risk tolerance

B. Risk transfer

C. Risk register Most Voted

D. Risk analysis

Correct Answer: *C*

Community vote distribution

C (100%)

Question #30 *Topic 1*

Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

A. Disaster recovery plan

B. Incident response procedure

C. Business continuity plan

D. Change management procedure Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #31 *Topic 1*

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

A. Open-source intelligence

B. Bug bounty Most Voted

C. Red team

D. Penetration testing

Correct Answer: *B*

Community vote distribution

B (100%)

Question #32 *Topic 1*

Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

A. Insider

B. Unskilled attacker

C. Nation-state Most Voted

D. Hacktivist

Correct Answer: *C*

Community vote distribution

C (100%)

Question #33 *Topic 1*

Which of the following enables the use of an input field to run commands that can view or manipulate data?

A. Cross-site scripting

B. Side loading

C. Buffer overflow

D. SQL injection Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #34 *Topic 1*

Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

A. Encrypted

B. Intellectual property Most Voted

C. Critical

D. Data in transit

Correct Answer: *B*

Community vote distribution

B (89%) 11%

Question #35 *Topic 1*

A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

A. If a security incident occurs on the device, the correct employee can be notified. Most Voted

B. The security team will be able to send user awareness training to the appropriate device.

C. Users can be mapped to their devices when configuring software MFA tokens.

D. User-based firewall policies can be correctly targeted to the appropriate laptops.

E. When conducting penetration testing, the security team will be able to target the desired laptops.

F. Company data can be accounted for when the employee leaves the organization. Most Voted

Correct Answer: *AF*

Community vote distribution

AF (52%) AC (44%)

Question #36 *Topic 1*

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

A. Send out periodic security reminders.

B. Update the content of new hire documentation.

C. Modify the content of recurring training. Most Voted

D. Implement a phishing campaign.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #37 *Topic 1*

A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

A. Packet captures

B. Vulnerability scans

C. Metadata

D. Dashboard Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #38 *Topic 1*

A systems administrator receives the following alert from a file integrity monitoring tool:
The hash of the cmd.exe file has changed.
The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following most likely occurred?

A. The end user changed the file permissions.

B. A cryptographic collision was detected.

C. A snapshot of the file system was taken.

D. A rootkit was deployed. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #39 *Topic 1*

Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?

A. Client Most Voted

B. Third-party vendor

C. Cloud provider

D. DBA

Correct Answer: *A*

Community vote distribution

A (90%) 10%

Question #40 *Topic 1*

A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?

A. MSA

B. SLA

C. BPA

D. SOW Most Voted

Correct Answer: *D*

Community vote distribution

D (97%)

Question #41 *Topic 1*

A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

A. Secure cookies

B. Version control

C. Input validation Most Voted

D. Code signing

Correct Answer: *C*

Community vote distribution

C (100%)

Question #42 *Topic 1*

Which of the following must be considered when designing a high-availability network? (Choose two).

A. Ease of recovery Most Voted

B. Ability to patch

C. Physical isolation

D. Responsiveness Most Voted

E. Attack surface

F. Extensible authentication

Correct Answer: *AD*

Community vote distribution

AD (67%) AC (21%) 7%

Question #43 *Topic 1*

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

A. Air gap the system.

B. Move the system to a different network segment.

C. Create a change control request. Most Voted

D. Apply the patch to the system.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #44 *Topic 1*

Which of the following describes the reason root cause analysis should be conducted as part of incident response?

A. To gather IoCs for the investigation

B. To discover which systems have been affected

C. To eradicate any trace of malware on the network

D. To prevent future incidents of the same nature Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #45 *Topic 1*

Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?

A. Fines

B. Audit findings Most Voted

C. Sanctions

D. Reputation damage

Correct Answer: *B*

Community vote distribution

B (63%) A (31%) 3%

Question #46 *Topic 1*

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

A. Capacity planning Most Voted

B. Redundancy

C. Geographic dispersion

D. Tabletop exercise

Correct Answer: *A*

Community vote distribution

A (100%)

Question #47 *Topic 1*

A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

A. Data masking

B. Encryption

C. Geolocation policy Most Voted

D. Data sovereignty regulation

Correct Answer: *C*

Community vote distribution

C (100%)

Question #48 *Topic 1*

Which of the following is a hardware-specific vulnerability?

A. Firmware version Most Voted

B. Buffer overflow

C. SQL injection

D. Cross-site scripting

Correct Answer: *A*

Community vote distribution

A (100%)

Question #49 *Topic 1*

While troubleshooting a firewall configuration, a technician determines that a “deny any” policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.
Which of the following actions would prevent this issue?

A. Documenting the new policy in a change request and submitting the request to change management

B. Testing the policy in a non-production environment before enabling the policy in the production network Most Voted

C. Disabling any intrusion prevention signatures on the “deny any” policy prior to enabling the new policy

D. Including an “allow any” policy above the “deny any” policy

Correct Answer: *B*

Community vote distribution

B (71%) A (29%)

Question #50 *Topic 1*

An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days.
Which of the following types of sites is the best for this scenario?

A. Real-time recovery

B. Hot

C. Cold

D. Warm Most Voted

Correct Answer: *D*

Community vote distribution

D (76%) C (23%)

Question #51 *Topic 1*

A company requires hard drives to be securely wiped before sending decommissioned systems to recycling. Which of the following best describes this policy?

A. Enumeration

B. Sanitization Most Voted

C. Destruction

D. Inventory

Correct Answer: *B*

Community vote distribution

B (100%)

Question #52 *Topic 1*

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

A. Private

B. Critical

C. Sensitive Most Voted

D. Public

Correct Answer: *C*

Community vote distribution

C (100%)

Question #53 *Topic 1*

A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

A. Local data protection regulations Most Voted

B. Risks from hackers residing in other countries

C. Impacts to existing contractual obligations

D. Time zone differences in log correlation

Correct Answer: *A*

Community vote distribution

A (83%) C (17%)

Question #54 *Topic 1*

Which of the following would be the best way to block unknown programs from executing?

A. Access control list

B. Application allow list Most Voted

C. Host-based firewall

D. DLP solution

Correct Answer: *B*

Community vote distribution

B (100%)

Question #55 *Topic 1*

A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.
Which of the following teams will conduct this assessment activity?

A. White

B. Purple

C. Blue

D. Red Most Voted

Correct Answer: *D*

Community vote distribution

D (90%) 10%

Question #56 *Topic 1*

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

A. Testing input validation on the user input fields

B. Performing code signing on company-developed software Most Voted

C. Performing static code analysis on the software

D. Ensuring secure cookies are use

Correct Answer: *B*

Community vote distribution

B (100%)

Question #57 *Topic 1*

Which of the following can be used to identify potential attacker activities without affecting production servers?

A. Honeypot Most Voted

B. Video surveillance

C. Zero Trust

D. Geofencing

Correct Answer: *A*

Community vote distribution

A (100%)

Question #58 *Topic 1*

During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

A. Analysis Most Voted

B. Lessons learned

C. Detection

D. Containment

Correct Answer: *A*

Community vote distribution

A (81%) B (19%)

Question #59 *Topic 1*

A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?

A. Conduct an audit.

B. Initiate a penetration test.

C. Rescan the network. Most Voted

D. Submit a report.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #60 *Topic 1*

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.
Which of the following best describes the user's activity?

A. Penetration testing

B. Phishing campaign

C. External audit

D. Insider threat Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #61 *Topic 1*

Which of the following allows for the attribution of messages to individuals?

A. Adaptive identity

B. Non-repudiation Most Voted

C. Authentication

D. Access logs

Correct Answer: *B*

Community vote distribution

B (95%) 5%

Question #62 *Topic 1*

Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

A. Automation Most Voted

B. Compliance checklist

C. Attestation

D. Manual audit

Correct Answer: *A*

Community vote distribution

A (90%) 10%

Question #63 *Topic 1*

Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

A. SCAP

B. NetFlow

C. Antivirus

D. DLP Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #64 *Topic 1*

An organization recently updated its security policy to include the following statement:
Regular expressions are included in source code to remove special characters such as $, |, ;. &, `, and ? from variables set by forms in a web application.
Which of the following best explains the security technique the organization adopted by making this addition to the policy?

A. Identify embedded keys

B. Code debugging

C. Input validation Most Voted

D. Static code analysis

Correct Answer: *C*

Community vote distribution

C (100%)

Question #65 *Topic 1*

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

A. Place posters around the office to raise awareness of common phishing activities.

B. Implement email security filters to prevent phishing emails from being delivered.

C. Update the EDR policies to block automatic execution of downloaded programs. Most Voted

D. Create additional training for users to recognize the signs of phishing attempts.

Correct Answer: *C*

Community vote distribution

C (82%) Other

Question #66 *Topic 1*

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

A. Compensating control Most Voted

B. Network segmentation

C. Transfer of risk

D. SNMP traps

Correct Answer: *A*

Community vote distribution

A (92%) 8%

Question #67 *Topic 1*

The management team notices that new accounts that are set up manually do not always have correct access or permissions.
Which of the following automation techniques should a systems administrator use to streamline account creation?

A. Guard rail script

B. Ticketing workflow

C. Escalation script

D. User provisioning script Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #68 *Topic 1*

A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?

A. Corrective

B. Preventive

C. Detective Most Voted

D. Deterrent

Correct Answer: *C*

Community vote distribution

C (100%)

Question #69 *Topic 1*

A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

A. Serverless framework Most Voted

B. Type 1 hypervisor

C. SD-WAN

D. SDN

Correct Answer: *A*

Community vote distribution

A (100%)

Question #70 *Topic 1*

A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

A. Tuning Most Voted

B. Aggregating

C. Quarantining

D. Archiving

Correct Answer: *A*

Community vote distribution

A (100%)

Question #71 *Topic 1*

A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

A. The user jsmith's account has been locked out.

B. A keylogger is installed on jsmith's workstation.

C. An attacker is attempting to brute force jsmith's account. Most Voted

D. Ransomware has been deployed in the domain.

Correct Answer: *C*

Community vote distribution

C (59%) B (41%)

Question #72 *Topic 1*

A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

A. Clustering servers

B. Geographic dispersion Most Voted

C. Load balancers

D. Off-site backups

Correct Answer: *B*

Community vote distribution

B (94%) 6%

Question #73 *Topic 1*

Which of the following is a primary security concern for a company setting up a BYOD program?

A. End of life

B. Buffer overflow

C. VM escape

D. Jailbreaking Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #74 *Topic 1*

A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks.
Which of the following analysis elements did the company most likely use in making this decision?

A. MTTR

B. RTO

C. ARO Most Voted

D. MTBF

Correct Answer: *C*

Community vote distribution

C (100%)

Question #75 *Topic 1*

Which of the following is the most likely to be included as an element of communication in a security awareness program?

A. Reporting phishing attempts or other suspicious activities Most Voted

B. Detecting insider threats using anomalous behavior recognition

C. Verifying information when modifying wire transfer data

D. Performing social engineering as part of third-party penetration testing

Correct Answer: *A*

Community vote distribution

A (100%)

Question #76 *Topic 1*

HOTSPOT -

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS -

Not all attacks and remediation actions will be used.

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

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

Correct Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Virus	Patch vulnerable systems
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Implement 2FA using push notification
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Conduct a code review

Question #77 *Topic 1*

HOTSPOT -

You are a security administrator investigating a potential infection on a network.

INSTRUCTIONS -

Click on each host and firewall. Review all logs to determine which host originated the infection and then identify if each remaining host is clean or infected.

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

192.168.10.22

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31   Warn   Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32   Warn   Scheduled update disabled by process scvh0st.exe
```

192.168.10.37

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Info   Update available v10.2.3.4440
4/18/2019 14:33  Info   Downloading update
4/18/2019 14:35  Info   Definition update complete
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37  Warn   File quarantined svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 1
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```

192.168.10.41

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 0
4/18/2019 14:43  Warn   File quarantine file
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```

Firewall

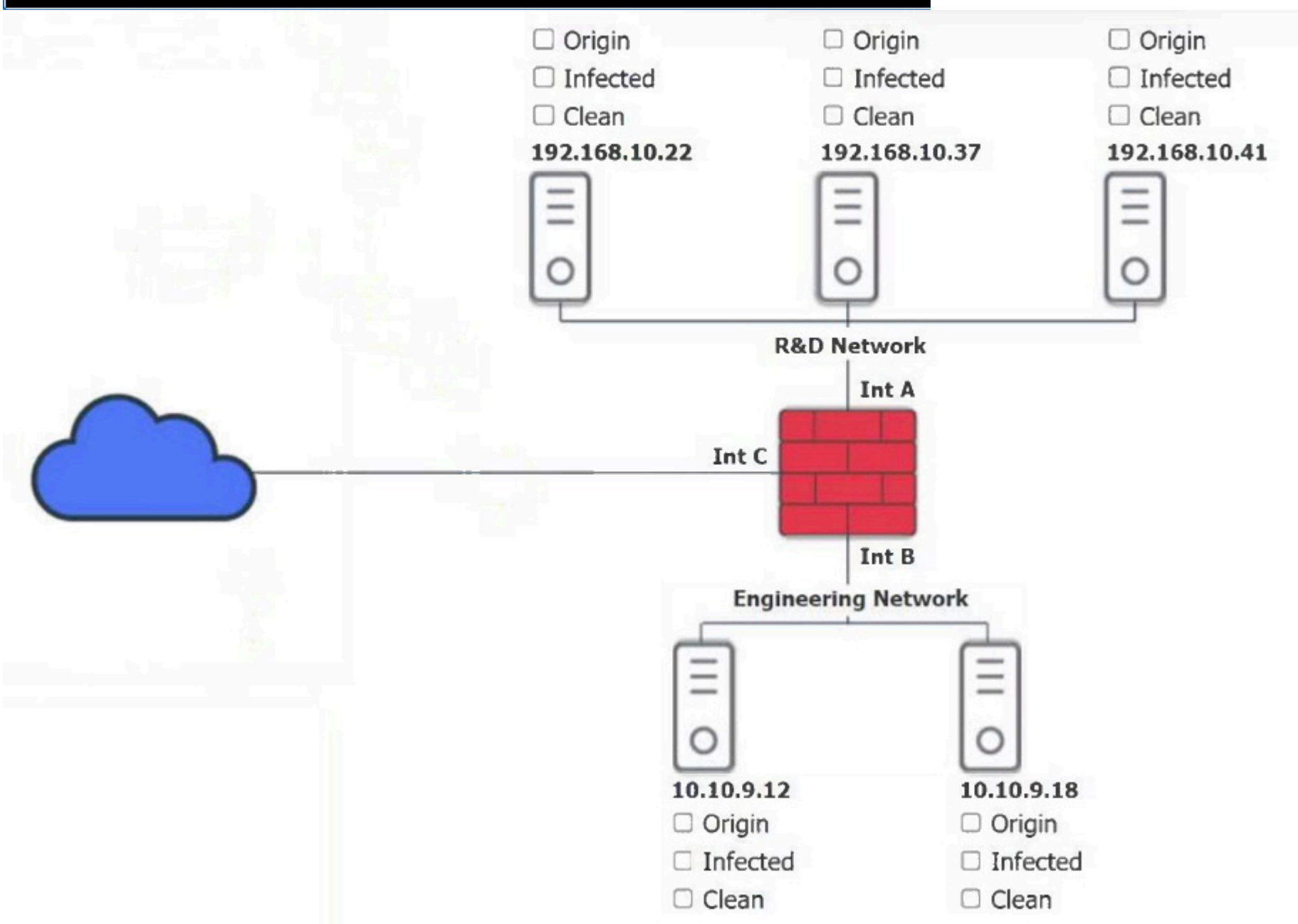
Timestamp	Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019 16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019 16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019 16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019 16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019 16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019 16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019 16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019 23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019 23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019 23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019 2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019 2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019 2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019 2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019 2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019 2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019 2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019 13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019 13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019 13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019 13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019 13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019 13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019 14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019 14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

10.10.9.12

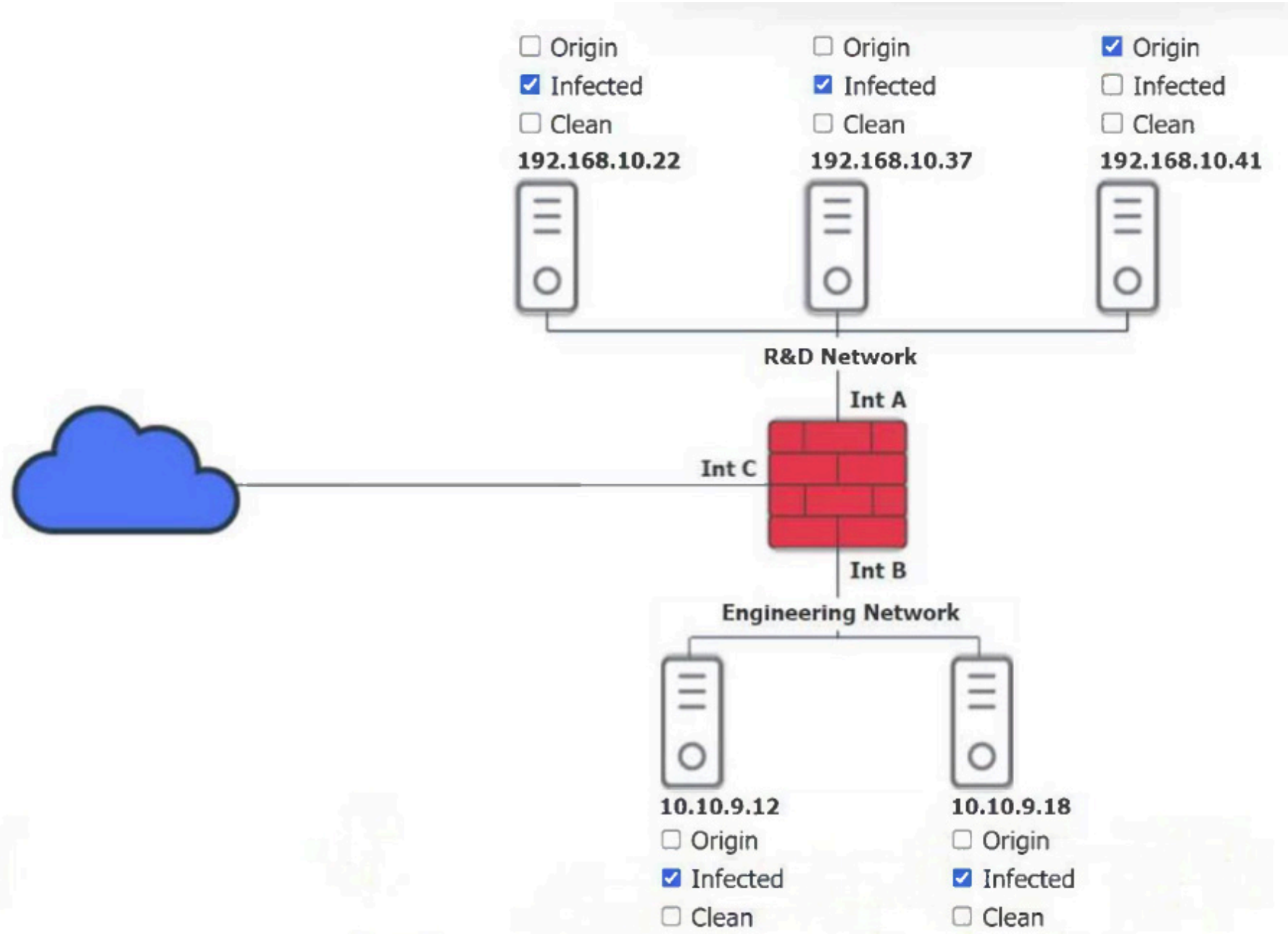
```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Info   Update available v10.2.3.4440
4/18/2019 14:33  Info   Downloading update
4/18/2019 14:35  Info   Definition update complete
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37  Warn   File quarantined svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 1
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```

10.10.9.18

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 0
4/18/2019 14:43  Warn   File quarantine file
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```



Correct Answer:



Question #78 *Topic 1*

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

A. Preparation Most Voted

B. Recovery

C. Lessons learned

D. Analysis

Correct Answer: *A*

Community vote distribution

A (74%) C (26%)

Question #79 *Topic 1*

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

A. Console access

B. Routing protocols

C. VLANs

D. Web-based administration Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #80 *Topic 1*

A security administrator needs a method to secure data in an environment that includes some form of checks so track any changes. Which of the following should the administrator set up to achieve this goal?

A. SPF

B. GPO

C. NAC

D. FIM Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #81 *Topic 1*

An administrator is reviewing a single server's security logs and discovers the following:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	09/16/2022 11:13:05 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:07 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:09 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:11 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:13 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:15 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:17 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:19 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:21 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:23 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:25 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:27 AM	Microsoft Windows security	4625	Logon

Which of the following best describes the action captured in this log file?

A. Brute-force attack Most Voted

B. Privilege escalation

C. Failed password audit

D. Forgotten password by the user

Correct Answer: *A*

Community vote distribution

A (100%)

Question #82 *Topic 1*

A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Choose two.)

A. Key escrow Most Voted

B. TPM presence Most Voted

C. Digital signatures

D. Data tokenization

E. Public key management

F. Certificate authority linking

Correct Answer: *AB*

Community vote distribution

AB (100%)

Question #83 *Topic 1*

A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

A. Changing the remote desktop port to a non-standard number

B. Setting up a VPN and placing the jump server inside the firewall Most Voted

C. Using a proxy for web connections from the remote desktop server

D. Connecting the remote server to the domain and increasing the password length

Correct Answer: *B*

Community vote distribution

B (100%)

Question #84 *Topic 1*

An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

A. ACL

B. DLP

C. IDS

D. IPS Most Voted

Correct Answer: *D*

Community vote distribution

D (97%)

Question #85 *Topic 1*

Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included. Which of the following best describes how the controls should be set up?

A. Remote access points should fail closed.

B. Logging controls should fail open.

C. Safety controls should fail open. Most Voted

D. Logical security controls should fail closed.

Correct Answer: *C*

Community vote distribution

C (89%) 11%

Question #86 *Topic 1*

Which of the following would be best suited for constantly changing environments?

A. RTOS

B. Containers Most Voted

C. Embedded systems

D. SCADA

Correct Answer: *B*

Community vote distribution

B (100%)

Question #87 *Topic 1*

Which of the following incident response activities ensures evidence is properly handled?

A. E-discovery

B. Chain of custody Most Voted

C. Legal hold

D. Preservation

Correct Answer: *B*

Community vote distribution

B (96%) 4%

Question #88 *Topic 1*

An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions to use a new account. Which of the following would most likely prevent this activity in the future?

A. Standardizing security incident reporting

B. Executing regular phishing campaigns

C. Implementing insider threat detection measures

D. Updating processes for sending wire transfers Most Voted

Correct Answer: *D*

Community vote distribution

D (83%) B (17%)

Question #89 *Topic 1*

A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

A. Off-the-shelf software

B. Orchestration Most Voted

C. Baseline

D. Policy enforcement

Correct Answer: *B*

Community vote distribution

B (100%)

Question #90 *Topic 1*

A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?

A. Processor

B. Custodian

C. Subject Most Voted

D. Owner

Correct Answer: *C*

Community vote distribution

C (90%) 10%

Question #91 *Topic 1*

Which of the following describes the maximum allowance of accepted risk?

A. Risk indicator

B. Risk level

C. Risk score

D. Risk threshold Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #92 *Topic 1*

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A. A worm is propagating across the network.

B. Data is being exfiltrated. Most Voted

C. A logic bomb is deleting data.

D. Ransomware is encrypting files.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #93 *Topic 1*

A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?

A. Default credentials

B. Non-segmented network

C. Supply chain vendor Most Voted

D. Vulnerable software

Correct Answer: *C*

Community vote distribution

C (38%) D (33%) B (29%)

Question #94 *Topic 1*

A systems administrator is working on a solution with the following requirements:

• Provide a secure zone.

• Enforce a company-wide access control policy.

• Reduce the scope of threats.

Which of the following is the systems administrator setting up?

A. Zero Trust Most Voted

B. AAA

C. Non-repudiation

D. CIA

Correct Answer: *A*

Community vote distribution

A (100%)

Question #95 *Topic 1*

Which of the following involves an attempt to take advantage of database misconfigurations?

A. Buffer overflow

B. SQL injection Most Voted

C. VM escape

D. Memory injection

Correct Answer: *B*

Community vote distribution

B (100%)

Question #96 *Topic 1*

Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP Most Voted

B. CSR

C. CA

D. CRC

Correct Answer: *A*

Community vote distribution

A (68%) C (32%)

Question #97 *Topic 1*

One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?

A. Virtualization

B. Firmware Most Voted

C. Application

D. Operating system

Correct Answer: *B*

Community vote distribution

B (100%)

Question #98 *Topic 1*

Which of the following is used to quantitatively measure the criticality of a vulnerability?

A. CVE

B. CVSS Most Voted

C. CIA

D. CERT

Correct Answer: *B*

Community vote distribution

B (100%)

Question #99 *Topic 1*

Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

A. Configure all systems to log scheduled tasks.

B. Collect and monitor all traffic exiting the network.

C. Block traffic based on known malicious signatures.

D. Install endpoint management software on all systems Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #100 *Topic 1*

An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

A. Data in use

B. Data in transit Most Voted

C. Geographic restrictions

D. Data sovereignty

Correct Answer: *B*

Community vote distribution

B (100%)

Question #101 *Topic 1*

After reviewing the following vulnerability scanning report:

```
Server:192.168.14.6
Service: Telnet
Port: 23 Protocol: TCP
Status: Open Severity: High
Vulnerability: Use of an insecure network protocol
```

A security analyst performs the following test:

```
nmap -p 23 192.168.14.6 --script telnet-encryption

PORT     STATE SERVICE REASON
23/tcp   open  telnet  syn-ack
|  telnet encryption:
|_ Telnet server supports encryption
```

Which of the following would the security analyst conclude for this reported vulnerability?

A. It is a false positive. Most Voted

B. A rescan is required.

C. It is considered noise.

D. Compensating controls exist.

Correct Answer: *A*

Community vote distribution

A (56%) D (43%)

Question #102 *Topic 1*

An organization disabled unneeded services and placed a firewall in front of a business-critical legacy system. Which of the following best describes the actions taken by the organization?

A. Exception

B. Segmentation

C. Risk transfer

D. Compensating controls Most Voted

Correct Answer: *D*

Community vote distribution

D (96%) 4%

Question #103 *Topic 1*

A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

A. EAP

B. DHCP

C. IPSec Most Voted

D. NAT

Correct Answer: *C*

Community vote distribution

C (100%)

Question #104 *Topic 1*

Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

A. Software as a service

B. Infrastructure as code Most Voted

C. Internet of Things

D. Software-defined networking

Correct Answer: *B*

Community vote distribution

B (100%)

Question #105 *Topic 1*

After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

A. Insider threat

B. Email phishing

C. Social engineering Most Voted

D. Executive whaling

Correct Answer: *C*

Community vote distribution

C (84%) D (16%)

Question #106 *Topic 1*

A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data. Which of the following should the administrator do first?

A. Block access to cloud storage websites.

B. Create a rule to block outgoing email attachments.

C. Apply classifications to the data. Most Voted

D. Remove all user permissions from shares on the file server.

Correct Answer: *C*

Community vote distribution

C (86%) 14%

Question #107 *Topic 1*

An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

A. Compromise

B. Retention Most Voted

C. Analysis

D. Transfer

E. Inventory

Correct Answer: *B*

Community vote distribution

B (100%)

Question #108 *Topic 1*

A company is working with a vendor to perform a penetration test. Which of the following includes an estimate about the number of hours required to complete the engagement?

A. SOW Most Voted

B. BPA

C. SLA

D. NDA

Correct Answer: *A*

Community vote distribution

A (100%)

Question #109 *Topic 1*

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

A. Insider threat

B. Hacktivist

C. Nation-state

D. Organized crime Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #110 *Topic 1*

Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

A. Code scanning for vulnerabilities

B. Open-source component usage

C. Quality assurance testing

D. Peer review and approval Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #111 *Topic 1*

Which of the following can best protect against an employee inadvertently installing malware on a company system?

A. Host-based firewall

B. System isolation

C. Least privilege

D. Application allow list Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #112 *Topic 1*

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting

B. Buffer overflow

C. Jailbreaking Most Voted

D. Side loading

Correct Answer: *C*

Community vote distribution

C (100%)

Question #113 *Topic 1*

Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Choose two.)

A. Fencing

B. Video surveillance

C. Badge access Most Voted

D. Access control vestibule Most Voted

E. Sign-in sheet

F. Sensor

Correct Answer: *CD*

Community vote distribution

CD (80%) AC (20%)

Question #114 *Topic 1*

An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

A. Segmentation Most Voted

B. Isolation

C. Patching

D. Encryption

Correct Answer: *A*

Community vote distribution

A (93%) 7%

Question #115 *Topic 1*

Which of the following is the most common data loss path for an air-gapped network?

A. Bastion host

B. Unsecured Bluetooth

C. Unpatched OS

D. Removable devices Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #116 *Topic 1*

Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

A. Impersonation

B. Disinformation

C. Watering-hole Most Voted

D. Smishing

Correct Answer: *C*

Community vote distribution

C (100%)

Question #117 *Topic 1*

An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

A. Deploying a SASE solution to remote employees Most Voted

B. Building a load-balanced VPN solution with redundant internet

C. Purchasing a low-cost SD-WAN solution for VPN traffic

D. Using a cloud provider to create additional VPN concentrators

Correct Answer: *A*

Community vote distribution

A (100%)

Question #118 *Topic 1*

Which of the following is the best reason to complete an audit in a banking environment?

A. Regulatory requirement Most Voted

B. Organizational change

C. Self-assessment requirement

D. Service-level requirement

Correct Answer: *A*

Community vote distribution

A (100%)

Question #119 *Topic 1*

Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

A. Integrity

B. Availability

C. Confidentiality Most Voted

D. Non-repudiation

Correct Answer: *C*

Community vote distribution

C (100%)

Question #120 *Topic 1*

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Choose two.)

A. The device has been moved from a production environment to a test environment.

B. The device is configured to use cleartext passwords.

C. The device is moved to an isolated segment on the enterprise network.

D. The device is moved to a different location in the enterprise.

E. The device's encryption level cannot meet organizational standards. Most Voted

F. The device is unable to receive authorized updates. Most Voted

Correct Answer: *EF*

Community vote distribution

EF (75%) BE (25%)

Question #121 *Topic 1*

A company is required to perform a risk assessment on an annual basis. Which of the following types of risk assessments does this requirement describe?

A. Continuous

B. Ad hoc

C. Recurring Most Voted

D. One time

Correct Answer: *C*

Community vote distribution

C (100%)

Question #122 *Topic 1*

After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

A. Compensating

B. Detective Most Voted

C. Preventive

D. Corrective

Correct Answer: *B*

Community vote distribution

B (100%)

Question #123 *Topic 1*

Which of the following exercises should an organization use to improve its incident response process?

A. Tabletop Most Voted

B. Replication

C. Failover

D. Recovery

Correct Answer: *A*

Community vote distribution

A (100%)

Question #124 *Topic 1*

Which of the following best ensures minimal downtime and data loss for organizations with critical computing equipment located in earthquake-prone areas?

A. Generators and UPS

B. Off-site replication Most Voted

C. Redundant cold sites

D. High availability networking

Correct Answer: *B*

Community vote distribution

B (100%)

Question #125 *Topic 1*

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

A. Insurance

B. Patching

C. Segmentation Most Voted

D. Replacement

Correct Answer: *C*

Community vote distribution

C (95%) 3%

Question #126 *Topic 1*

After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?

A. Group Policy

B. Content filtering

C. Data loss prevention

D. Access control lists Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #127 *Topic 1*

A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

A. MOA

B. SOW

C. MOU

D. SLA Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #128 *Topic 1*

A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

A. Certification Most Voted

B. Inventory list

C. Classification

D. Proof of ownership

Correct Answer: *A*

Community vote distribution

A (100%)

Question #129 *Topic 1*

A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup data. Which of the following should the company consider?

A. Geographic dispersion

B. Platform diversity

C. Hot site

D. Load balancing

Correct Answer: *A*

Community vote distribution

A (100%)

Question #130 *Topic 1*

A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

A. Obtain the file's SHA-256 hash.

B. Use hexdump on the file's contents.

C. Check endpoint logs.

D. Query the file's metadata. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #131 *Topic 1*

Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

A. Red

B. Blue

C. Purple Most Voted

D. Yellow

Correct Answer: *C*

Community vote distribution

C (100%)

Question #132 *Topic 1*

A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

A. Patch availability Most Voted

B. Product software compatibility

C. Ease of recovery

D. Cost of replacement

Correct Answer: *A*

Community vote distribution

A (100%)

Question #133 *Topic 1*

Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

A. A full inventory of all hardware and software Most Voted

B. Documentation of system classifications

C. A list of system owners and their departments

D. Third-party risk assessment documentation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #134 *Topic 1*

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

A. Impact analysis

B. Scheduled downtime Most Voted

C. Backout plan

D. Change management boards

Correct Answer: *B*

Community vote distribution

B (100%)

Question #135 *Topic 1*

A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

A. Hashing

B. Tokenization

C. Encryption Most Voted

D. Segmentation

Correct Answer: *C*

Community vote distribution

C (91%) 9%

Question #136 *Topic 1*

A legacy device is being decommissioned and is no longer receiving updates or patches. Which of the following describes this scenario?

A. End of business

B. End of testing

C. End of support

D. End of life Most Voted

Correct Answer: *D*

Community vote distribution

D (52%) C (48%)

Question #137 *Topic 1*

A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

A. Encryption at rest Most Voted

B. Masking

C. Data classification

D. Permission restrictions

Correct Answer: *A*

Community vote distribution

A (100%)

Question #138 *Topic 1*

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS severs, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

A. Concurrent session usage

B. Secure DNS cryptographic downgrade

C. On-path resource consumption

D. Reflected denial of service Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #139 *Topic 1*

A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

A. RBAC Most Voted

B. ACL

C. SAML

D. GPO

Correct Answer: *A*

Community vote distribution

A (100%)

Question #140 *Topic 1*

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Choose two.)

A. Federation Most Voted

B. Identity proofing

C. Password complexity Most Voted

D. Default password changes

E. Password manager

F. Open authentication

Correct Answer: *AC*

Community vote distribution

AC (100%)

Question #141 *Topic 1*

Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

A. SIEM Most Voted

B. DLP

C. IDS

D. SNMP

Correct Answer: *A*

Community vote distribution

A (100%)

Question #142 *Topic 1*

A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:

Something you know -

Something you have -

Something you are -

Which of the following would accomplish the manager's goal?

A. Domain name, PKI, GeoIP lookup

B. VPN IP address, company ID, facial structure

C. Password, authentication token, thumbprint Most Voted

D. Company URL, TLS certificate, home address

Correct Answer: *C*

Community vote distribution

C (100%)

Question #143 *Topic 1*

Which of the following would be the best way to handle a critical business application that is running on a legacy server?

A. Segmentation Most Voted

B. Isolation

C. Hardening

D. Decommissioning

Correct Answer: *A*

Community vote distribution

A (44%) B (40%) Other

Question #144 *Topic 1*

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

A. VM escape

B. SQL injection

C. Buffer overflow Most Voted

D. Race condition

Correct Answer: *C*

Community vote distribution

C (100%)

Question #145 *Topic 1*

After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

A. Retain the emails between the security team and affected customers for 30 days.

B. Retain any communications related to the security breach until further notice. Most Voted

C. Retain any communications between security members during the breach response.

D. Retain all emails from the company to affected customers for an indefinite period of time.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #146 *Topic 1*

Which of the following describes the process of concealing code or text inside a graphical image?

A. Symmetric encryption

B. Hashing

C. Data masking

D. Steganography Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #147 *Topic 1*

An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

A. Vishing

B. Smishing Most Voted

C. Pretexting

D. Phishing

Correct Answer: *B*

Community vote distribution

B (100%)

Question #148 *Topic 1*

Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?

A. Mitigate Most Voted

B. Accept

C. Transfer

D. Avoid

Correct Answer: *A*

Community vote distribution

A (100%)

Question #149 *Topic 1*

Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule. Which of the following best describes this form of security control?

A. Physical Most Voted

B. Managerial

C. Technical

D. Operational

Correct Answer: *A*

Community vote distribution

A (100%)

Question #150 *Topic 1*

The local administrator account for a company's VPN appliance was unexpectedly used to log in to the remote management interface. Which of the following would have most likely prevented this from happening?

A. Using least privilege

B. Changing the default password Most Voted

C. Assigning individual user IDs

D. Reviewing logs more frequently

Correct Answer: *B*

Community vote distribution

B (63%) A (21%) C (16%)

Question #151 *Topic 1*

Which of the following is the best way to secure an on-site data center against intrusion from an insider?

A. Bollards

B. Access badge Most Voted

C. Motion sensor

D. Video surveillance

Correct Answer: *B*

Community vote distribution

B (100%)

Question #152 *Topic 1*

An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group. Which of the following access controls is most likely causing the lack of access?

A. Role-based Most Voted

B. Discretionary

C. Time of day

D. Least privilege

Correct Answer: *A*

Community vote distribution

A (100%)

Question #153 *Topic 1*

Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Choose two.)

A. Channels by which the organization communicates with customers

B. The reporting mechanisms for ethics violations

C. Threat vectors based on the industry in which the organization operates Most Voted

D. Secure software development training for all personnel

E. Cadence and duration of training events Most Voted

F. Retraining requirements for individuals who fail phishing simulations

Correct Answer: *CE*

Community vote distribution

CE (100%)

Question #154 *Topic 1*

A network administrator is working on a project to deploy a load balancer in the company's cloud environment. Which of the following fundamental security requirements does this project fulfil?

A. Privacy

B. Integrity

C. Confidentiality

D. Availability Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #155 *Topic 1*

A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

A. Deploying PowerShell scripts

B. Pushing GPO update Most Voted

C. Enabling PAP

D. Updating EDR profiles

Correct Answer: *B*

Community vote distribution

B (100%)

Question #156 *Topic 1*

Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

A. ARO

B. RTO

C. RPO

D. ALE Most Voted

E. SLE

Correct Answer: *D*

Community vote distribution

D (100%)

Question #157 *Topic 1*

In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

A. Key stretching

B. Tokenization

C. Data masking

D. Salting Most Voted

Correct Answer: *D*

Community vote distribution

D (71%) A (29%)

Question #158 *Topic 1*

A technician is deploying a new security camera. Which of the following should the technician do?

A. Configure the correct VLAN.

B. Perform a vulnerability scan.

C. Disable unnecessary ports.

D. Conduct a site survey. Most Voted

Correct Answer: *D*

Community vote distribution

D (87%) 10%

Question #159 *Topic 1*

A company is experiencing a web services outage on the public network. The services are up and available but inaccessible. The network logs show a sudden increase in network traffic that is causing the outage. Which of the following attacks is the organization experiencing?

A. ARP poisoning

B. Brute force

C. Buffer overflow

D. DDoS Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #160 *Topic 1*

Which of the following threat actors is the most likely to be motivated by profit?

A. Hacktivist

B. Insider threat

C. Organized crime Most Voted

D. Shadow IT

Correct Answer: *C*

Community vote distribution

C (100%)

Question #161 *Topic 1*

An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Choose two.)

A. Application

B. Authentication

C. DHCP

D. Network Most Voted

E. Firewall Most Voted

F. Database

Correct Answer: *DE*

Community vote distribution

DE (81%) Other

Question #162 *Topic 1*

During a penetration test, a vendor attempts to enter an unauthorized area using an access badge. Which of the following types of tests does this represent?

A. Defensive

B. Passive

C. Offensive

D. Physical Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #163 *Topic 1*

A systems administrator uses a key to encrypt a message being sent to a peer in a different branch office. The peer then uses the same key to decrypt the message. Which of the following describes this example?

A. Symmetric Most Voted

B. Asymmetric

C. Hashing

D. Salting

Correct Answer: *A*

Community vote distribution

A (85%) C (15%)

Question #164 *Topic 1*

A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network. Which of the following should be configured on the existing network infrastructure to best prevent this activity?

A. Port security Most Voted

B. Web application firewall

C. Transport layer security

D. Virtual private network

Correct Answer: *A*

Community vote distribution

A (83%) C (17%)

Question #165 *Topic 1*

A security administrator is reissuing a former employee's laptop. Which of the following is the best combination of data handling activities for the administrator to perform? (Choose two.)

A. Data retention

B. Certification Most Voted

C. Destruction

D. Classification

E. Sanitization Most Voted

F. Enumeration

Correct Answer: *BE*

Community vote distribution

BE (46%) AE (39%) Other

Question #166 *Topic 1*

A systems administrator would like to deploy a change to a production system. Which of the following must the administrator submit to demonstrate that the system can be restored to a working state in the event of a performance issue?

A. Backout plan Most Voted

B. Impact analysis

C. Test procedure

D. Approval procedure

Correct Answer: *A*

Community vote distribution

A (100%)

Question #167 *Topic 1*

A company is redesigning its infrastructure and wants to reduce the number of physical servers in use. Which of the following architectures is best suited for this goal?

A. Serverless

B. Segmentation

C. Virtualization Most Voted

D. Microservices

Correct Answer: *C*

Community vote distribution

C (100%)

Question #168 *Topic 1*

A bank set up a new server that contains customers' PII. Which of the following should the bank use to make sure the sensitive data is not modified?

A. Full disk encryption

B. Network access control

C. File integrity monitoring Most Voted

D. User behavior analytics

Correct Answer: *C*

Community vote distribution

C (100%)

Question #169 *Topic 1*

Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked. Which of the following changes would allow users to access the site?

A. Creating a firewall rule to allow HTTPS traffic

B. Configuring the IPS to allow shopping

C. Tuning the DLP rule that detects credit card data

D. Updating the categorization in the content filter Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #170 *Topic 1*

Which of the following most impacts an administrator's ability to address CVEs discovered on a server?

A. Rescanning requirements

B. Patch availability Most Voted

C. Organizational impact

D. Risk tolerance

Correct Answer: *B*

Community vote distribution

B (100%)

Question #171 *Topic 1*

Which of the following describes effective change management procedures?

A. Approving the change after a successful deployment

B. Having a backout plan when a patch fails Most Voted

C. Using a spreadsheet for tracking changes

D. Using an automatic change control bypass for security updates

Correct Answer: *B*

Community vote distribution

B (100%)

Question #172 *Topic 1*

The CIRT is reviewing an incident that involved a human resources recruiter exfiltrating sensitive company data. The CIRT found that the recruiter was able to use HTTP over port 53 to upload documents to a web server. Which of the following security infrastructure devices could have identified and blocked this activity?

A. WAF utilizing SSL decryption

B. NGFW utilizing application inspection Most Voted

C. UTM utilizing a threat feed

D. SD-WAN utilizing IPSec

Correct Answer: *B*

Community vote distribution

B (100%)

Question #173 *Topic 1*

An enterprise is working with a third party and needs to allow access between the internal networks of both parties for a secure file migration. The solution needs to ensure encryption is applied to all traffic that is traversing the networks. Which of the following solutions should most likely be implemented?

A. EAP

B. IPSec Most Voted

C. SD-WAN

D. TLS

Correct Answer: *B*

Community vote distribution

B (100%)

Question #174 *Topic 1*

An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to email these files outside of the organization. Which of the following best describes the tool the administrator is using?

A. DLP Most Voted

B. SNMP traps

C. SCAP

D. IPS

Correct Answer: *A*

Community vote distribution

A (100%)

Question #175 *Topic 1*

A software developer released a new application and is distributing application files via the developer's website. Which of the following should the developer post on the website to allow users to verify the integrity of the downloaded files?

A. Hashes Most Voted

B. Certificates

C. Algorithms

D. Salting

Correct Answer: *A*

Community vote distribution

A (100%)

Question #176 *Topic 1*

An organization wants to limit potential impact to its log-in database in the event of a breach. Which of the following options is the security team most likely to recommend?

A. Tokenization

B. Hashing Most Voted

C. Obfuscation

D. Segmentation

Correct Answer: *B*

Community vote distribution

B (68%) D (21%) 12%

Question #177 *Topic 1*

An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?

A. Virus

B. Trojan

C. Spyware

D. Ransomware Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #178 *Topic 1*

A systems administrator is advised that an external web server is not functioning property. The administrator reviews the following firewall logs containing traffic going to the web server:

```
Date       |     Time     |   SourceIP   |SPort|Flag| DestIP | DPort
2023-01-25 01:45:09.102 98.123.45.100 4560 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 95.123.45.101 3361 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 99.123.45.102 3662 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 89.123.45.103 5663 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 98.123.45.104 4064 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 80.123.45.105 4365 SYN 100.50.20.7 443
```

Which of the following attacks is likely occurring?

A. DDoS Most Voted

B. Directory traversal

C. Brute-force

D. HTTPS downgrade

Correct Answer: *A*

Community vote distribution

A (100%)

Question #179 *Topic 1*

An organization would like to calculate the time needed to resolve a hardware issue with a server. Which of the following risk management processes describes this example?

A. Recovery point objective

B. Mean time between failures

C. Recovery time objective

D. Mean time to repair Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #180 *Topic 1*

A security engineer is installing an IPS to block signature-based attacks in the environment.

Which of the following modes will best accomplish this task?

A. Monitor

B. Sensor

C. Audit

D. Active Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #181 *Topic 1*

An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?

A. XDR

B. SPF

C. DLP Most Voted

D. DMARC

Correct Answer: *C*

Community vote distribution

C (67%) D (33%)

Question #182 *Topic 1*

Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

A. IDS

B. ACL

C. EDR Most Voted

D. NAC

Correct Answer: *C*

Community vote distribution

C (100%)

Question #183 *Topic 1*

Client files can only be accessed by employees who need to know the information and have specified roles in the company. Which of the following best describes this security concept?

A. Availability

B. Confidentiality Most Voted

C. Integrity

D. Non-repudiation

Correct Answer: *B*

Community vote distribution

B (100%)

Question #184 *Topic 1*

Which of the following describes the category of data that is most impacted when it is lost?

A. Confidential

B. Public

C. Private

D. Critical Most Voted

Correct Answer: *D*

Community vote distribution

D (60%) A (40%)

Question #185 *Topic 1*

A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company. Which of the following attack vectors is most likely being used?

A. Business email

B. Social engineering Most Voted

C. Unsecured network

D. Default credentials

Correct Answer: *B*

Community vote distribution

B (55%) A (45%)

Question #186 *Topic 1*

Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?

A. SLA Most Voted

B. MOU

C. MOA

D. BPA

Correct Answer: *A*

Community vote distribution

A (64%) B (36%)

Question #187 *Topic 1*

A company that is located in an area prone to hurricanes is developing a disaster recovery plan and looking at site considerations that allow the company to immediately continue operations. Which of the following is the best type of site for this company?

A. Cold

B. Tertiary

C. Warm

D. Hot Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #188 *Topic 1*

Which of the following security controls is most likely being used when a critical legacy server is segmented into a private network?

A. Deterrent

B. Corrective

C. Compensating Most Voted

D. Preventive

Correct Answer: *C*

Community vote distribution

C (59%) D (41%)

Question #189 *Topic 1*

Which of the following best describes the practice of researching laws and regulations related to information security operations within a specific industry?

A. Compliance reporting

B. GDPR

C. Due diligence Most Voted

D. Attestation

Correct Answer: *C*

Community vote distribution

C (100%)

Question #190 *Topic 1*

Which of the following considerations is the most important for an organization to evaluate as it establishes and maintains a data privacy program?

A. Reporting structure for the data privacy officer

B. Request process for data subject access

C. Role as controller or processor Most Voted

D. Physical location of the company

Correct Answer: *C*

Community vote distribution

C (83%) B (17%)

Question #191 *Topic 1*

A security analyst is investigating a workstation that is suspected of outbound communication to a command-and-control server. During the investigation, the analyst discovered that logs on the endpoint were deleted. Which of the following logs would the analyst most likely look at next?

A. IPS

B. Firewall Most Voted

C. ACL

D. Windows security

Correct Answer: *B*

Community vote distribution

B (100%)

Question #192 *Topic 1*

An IT manager is putting together a documented plan describing how the organization will keep operating in the event of a global incident. Which of the following plans is the IT manager creating?

A. Business continuity Most Voted

B. Physical security

C. Change management

D. Disaster recovery

Correct Answer: *A*

Community vote distribution

A (100%)

Question #193 *Topic 1*

A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage. Which of the following recovery sites is the best option?

A. Hot

B. Cold

C. Warm Most Voted

D. Geographically dispersed

Correct Answer: *C*

Community vote distribution

C (100%)

Question #194 *Topic 1*

A security team is setting up a new environment for hosting the organization's on-premises software application as a cloud-based service. Which of the following should the team ensure is in place in order for the organization to follow security best practices?

A. Virtualization and isolation of resources Most Voted

B. Network segmentation

C. Data encryption

D. Strong authentication policies

Correct Answer: *A*

Community vote distribution

A (65%) C (29%) 6%

Question #195 *Topic 1*

A manager receives an email that contains a link to receive a refund. After hovering over the link, the manager notices that the domain's URL points to a suspicious link. Which of the following security practices helped the manager to identify the attack?

A. End user training Most Voted

B. Policy review

C. URL scanning

D. Plain text email

Correct Answer: *A*

Community vote distribution

A (83%) C (17%)

Question #196 *Topic 1*

A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?

A. Validate the code signature. Most Voted

B. Execute the code in a sandbox.

C. Search the executable for ASCII strings.

D. Generate a hash of the files.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #197 *Topic 1*

A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system. Which of the following techniques would increase enterprise security?

A. Installing HIDS on the system

B. Placing the system in an isolated VLAN Most Voted

C. Decommissioning the system

D. Encrypting the system's hard drive

Correct Answer: *B*

Community vote distribution

B (61%) C (39%)

Question #198 *Topic 1*

The Chief Information Security Officer (CISO) at a large company would like to gain an understanding of how the company's security policies compare to the requirements imposed by external regulators. Which of the following should the CISO use?

A. Penetration test

B. Internal audit Most Voted

C. Attestation

D. External examination

Correct Answer: *B*

Community vote distribution

B (63%) D (38%)

Question #199 *Topic 1*

A systems administrator notices that the research and development department is not using the company VPN when accessing various company-related services and systems. Which of the following scenarios describes this activity?

A. Espionage

B. Data exfiltration

C. Nation-state attack

D. Shadow IT Most Voted

Correct Answer: *D*

Community vote distribution

D (85%) B (15%)

Question #200 *Topic 1*

The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

A. Shadow IT Most Voted

B. Insider threat

C. Data exfiltration

D. Service disruption

Correct Answer: *A*

Community vote distribution

A (100%)

Question #201 *Topic 1*

Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

A. To track the status of patching installations Most Voted

B. To find shadow IT cloud deployments

C. To continuously the monitor hardware inventory

D. To hunt for active attackers in the network

Correct Answer: *A*

Community vote distribution

A (100%)

Question #202 *Topic 1*

Which of the following is classified as high availability in a cloud environment?

A. Access broker

B. Cloud HSM

C. WAF

D. Load balancer Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #203 *Topic 1*

Which of the following security measures is required when using a cloud-based platform for IoT management?

A. Encrypted connection Most Voted

B. Federated identity

C. Firewall

D. Single sign-on

Correct Answer: *A*

Community vote distribution

A (100%)

Question #204 *Topic 1*

Which of the following threat vectors is most commonly utilized by insider threat actors attempting data exfiltration?

A. Unidentified removable devices Most Voted

B. Default network device credentials

C. Spear phishing emails

D. Impersonation of business units through typosquatting

Correct Answer: *A*

Community vote distribution

A (100%)

Question #205 *Topic 1*

Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

A. Encryption

B. Hashing

C. Masking Most Voted

D. Tokenization

Correct Answer: *C*

Community vote distribution

C (88%) 13%

Question #206 *Topic 1*

The Chief Information Security Officer (CISO) has determined the company is non-compliant with local data privacy regulations. The CISO needs to justify the budget request for more resources. Which of the following should the CISO present to the board as the direct consequence of non-compliance?

A. Fines Most Voted

B. Reputational damage

C. Sanctions

D. Contractual implications

Correct Answer: *A*

Community vote distribution

A (87%) 13%

Question #207 *Topic 1*

Which of the following alert types is the most likely to be ignored over time?

A. True positive

B. True negative

C. False positive Most Voted

D. False negative

Correct Answer: *C*

Community vote distribution

C (100%)

Question #208 *Topic 1*

A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports. Which of the following vulnerabilities has likely been exploited in this software?

A. Memory injection

B. Race condition

C. Side loading

D. SQL injection

Correct Answer: *A*

Community vote distribution

A (75%) C (25%)

Question #209 *Topic 1*

An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch. Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?

A. Asset inventory Most Voted

B. Network enumeration

C. Data certification

D. Procurement process

Correct Answer: *A*

Community vote distribution

A (100%)

Question #210 *Topic 1*

Which of the following should a security operations center use to improve its incident response procedure?

A. Playbooks Most Voted

B. Frameworks

C. Baselines

D. Benchmarks

Correct Answer: *A*

Community vote distribution

A (100%)

Question #211 *Topic 1*

Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?

A. Continuity of operations

B. Capacity planning

C. Tabletop exercise Most Voted

D. Parallel processing

Correct Answer: *C*

Community vote distribution

C (100%)

Question #212 *Topic 1*

A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies. Which of the following is the most important consideration during development?

A. Scalability

B. Availability Most Voted

C. Cost

D. Ease of deployment

Correct Answer: *B*

Community vote distribution

B (86%) 14%

Question #213 *Topic 1*

Which of the following agreement types defines the time frame in which a vendor needs to respond?

A. SOW

B. SLA Most Voted

C. MOA

D. MOU

Correct Answer: *B*

Community vote distribution

B (100%)

Question #214 *Topic 1*

Which of the following is a feature of a next-generation SIEM system?

A. Virus signatures

B. Automated response actions Most Voted

C. Security agent deployment

D. Vulnerability scanning

Correct Answer: *B*

Community vote distribution

B (100%)

Question #215 *Topic 1*

To improve the security at a data center, a security administrator implements a CCTV system and posts several signs about the possibility of being filmed. Which of the following best describe these types of controls? (Choose two.)

A. Preventive

B. Deterrent Most Voted

C. Corrective

D. Directive

E. Compensating

F. Detective Most Voted

Correct Answer: *BF*

Community vote distribution

BF (78%) BD (22%)

Question #216 *Topic 1*

Which of the following examples would be best mitigated by input sanitization?

A. `<script>alert("Warning!");</script>` Most Voted

B. nmap - 10.11.1.130

C. Email message: "Click this link to get your free gift card."

D. Browser message: "Your connection is not private."

Correct Answer: *A*

Community vote distribution

A (100%)

Question #217 *Topic 1*

An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

A. Smishing

B. Disinformation

C. Impersonating Most Voted

D. Whaling

Correct Answer: *C*

Community vote distribution

C (94%) 6%

Question #218 *Topic 1*

After conducting a vulnerability scan, a systems administrator notices that one of the identified vulnerabilities is not present on the systems that were scanned. Which of the following describes this example?

A. False positive Most Voted

B. False negative

C. True positive

D. True negative

Correct Answer: *A*

Community vote distribution

A (53%) B (47%)

Question #219 *Topic 1*

A recent penetration test identified that an attacker could flood the MAC address table of network switches. Which of the following would best mitigate this type of attack?

A. Load balancer

B. Port security

C. IPS

D. NGFW

Correct Answer: *B*

Question #220 *Topic 1*

A user would like to install software and features that are not available with a smartphone's default software. Which of the following would allow the user to install unauthorized software and enable new features?

A. SQLi

B. Cross-site scripting

C. Jailbreaking Most Voted

D. Side loading

Correct Answer: *C*

Community vote distribution

C (94%) 6%

Question #221 *Topic 1*

Which of the following phases of an incident response involves generating reports?

A. Recovery

B. Preparation

C. Lessons learned Most Voted

D. Containment

Correct Answer: *C*

Community vote distribution

C (100%)

Question #222 *Topic 1*

Which of the following methods would most likely be used to identify legacy systems?

A. Bug bounty program

B. Vulnerability scan

C. Package monitoring

D. Dynamic analysis

Correct Answer: *B*

Community vote distribution

B (100%)

Question #223 *Topic 1*

Employees located off-site must have access to company resources in order to complete their assigned tasks. These employees utilize a solution that allows remote access without interception concerns. Which of the following best describes this solution?

A. Proxy server

B. NGFW

C. VPN

D. Security zone

Correct Answer: *C*

Question #224 *Topic 1*

A company allows customers to upload PDF documents to its public e-commerce website. Which of the following would a security analyst most likely recommend?

A. Utilizing attack signatures in an IDS

B. Enabling malware detection through a UTM Most Voted

C. Limiting the affected servers with a load balancer

D. Blocking command injections via a WAF

Correct Answer: *B*

Community vote distribution

B (100%)

Question #225 *Topic 1*

A security analyst developed a script to automate a trivial and repeatable task. Which of the following best describes the benefits of ensuring other team members understand how the script works?

A. To reduce implementation cost

B. To identify complexity

C. To remediate technical debt

D. To prevent a single point of failure Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #226 *Topic 1*

A company is decommissioning its physical servers and replacing them with an architecture that will reduce the number of individual operating systems. Which of the following strategies should the company use to achieve this security requirement?

A. Microservices

B. Containerization Most Voted

C. Virtualization

D. Infrastructure as code

Correct Answer: *B*

Community vote distribution

B (61%) C (35%)

Question #227 *Topic 1*

An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Choose two.)

A. Disable default accounts. Most Voted

B. Add the server to the asset inventory.

C. Remove unnecessary services. Most Voted

D. Document default passwords.

E. Send server logs to the SIEM.

F. Join the server to the corporate domain.

Correct Answer: *AC*

Community vote distribution

AC (100%)

Question #228 *Topic 1*

A Chief Information Security Officer would like to conduct frequent, detailed reviews of systems and procedures to track compliance objectives. Which of the following will be the best method to achieve this objective?

A. Third-party attestation

B. Penetration testing

C. Internal auditing Most Voted

D. Vulnerability scans

Correct Answer: *C*

Community vote distribution

C (100%)

Question #229 *Topic 1*

Which of the following security concepts is accomplished with the installation of a RADIUS server?

A. CIA

B. AAA Most Voted

C. ACL

D. PEM

Correct Answer: *B*

Community vote distribution

B (100%)

Question #230 *Topic 1*

After creating a contract for IT contractors, the human resources department changed several clauses. The contract has gone through three revisions. Which of the following processes should the human resources department follow to track revisions?

A. Version validation

B. Version changes

C. Version updates

D. Version control Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #231 *Topic 1*

The executive management team is mandating the company develop a disaster recovery plan. The cost must be kept to a minimum, and the money to fund additional internet connections is not available. Which of the following would be the best option?

A. Hot site

B. Cold site Most Voted

C. Failover site

D. Warm site

Correct Answer: *B*

Community vote distribution

B (100%)

Question #232 *Topic 1*

An administrator at a small business notices an increase in support calls from employees who receive a blocked page message after trying to navigate to a spoofed website. Which of the following should the administrator do?

A. Deploy multifactor authentication.

B. Decrease the level of the web filter settings.

C. Implement security awareness training. Most Voted

D. Update the acceptable use policy.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #233 *Topic 1*

Which of the following teams is best suited to determine whether a company has systems that can be exploited by a potential, identified vulnerability?

A. Purple team

B. Blue team

C. Red team Most Voted

D. White team

Correct Answer: *C*

Community vote distribution

C (57%) B (40%)

Question #234 *Topic 1*

A company is reviewing options to enforce user logins after several account takeovers. The following conditions must be met as part of the solution:

• Allow employees to work remotely or from assigned offices around the world.
• Provide a seamless login experience.
• Limit the amount of equipment required.

Which of the following best meets these conditions?

A. Trusted devices Most Voted

B. Geotagging

C. Smart cards

D. Time-based logins

Correct Answer: *A*

Community vote distribution

A (100%)

Question #235 *Topic 1*

Which of the following methods can be used to detect attackers who have successfully infiltrated a network? (Choose two.)

A. Tokenization

B. CI/CD

C. Honeypots Most Voted

D. Threat modeling

E. DNS sinkhole Most Voted

F. Data obfuscation

Correct Answer: *CE*

Community vote distribution

CE (100%)

Question #236 *Topic 1*

A company wants to ensure that the software it develops will not be tampered with after the final version is completed. Which of the following should the company most likely use?

A. Hashing Most Voted

B. Encryption

C. Baselines

D. Tokenization

Correct Answer: *A*

Community vote distribution

A (75%) C (25%)

Question #237 *Topic 1*

An organization completed a project to deploy SSO across all business applications last year. Recently, the finance department selected a new cloud-based accounting software vendor. Which of the following should most likely be configured during the new software deployment?

A. RADIUS

B. SAML

C. EAP

D. OpenID

Correct Answer: *B*

Community vote distribution

B (100%)

Question #238 *Topic 1*

A user, who is waiting for a flight at an airport, logs in to the airline website using the public Wi-Fi, ignores a security warning and purchases an upgraded seat. When the flight lands, the user finds unauthorized credit card charges. Which of the following attacks most likely occurred?

A. Replay attack

B. Memory leak

C. Buffer overflow attack

D. On-path attack Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #239 *Topic 1*

A network engineer deployed a redundant switch stack to increase system availability. However, the budget can only cover the cost of one ISP connection. Which of the following best describes the potential risk factor?

A. The equipment MTBF is unknown.

B. The ISP has no SLA.

C. An RPO has not been determined.

D. There is a single point of failure. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #240 *Topic 1*

A network team segmented a critical, end-of-life server to a VLAN that can only be reached by specific devices but cannot be reached by the perimeter network. Which of the following best describe the controls the team implemented? (Choose two.)

A. Managerial

B. Physical

C. Corrective

D. Detective

E. Compensating Most Voted

F. Technical Most Voted

G. Deterrent

Correct Answer: *EF*

Community vote distribution

EF (86%) 14%

Question #241 *Topic 1*

A threat actor was able to use a username and password to log in to a stolen company mobile device. Which of the following provides the best solution to increase mobile data security on all employees' company mobile devices?

A. Application management

B. Full disk encryption

C. Remote wipe Most Voted

D. Containerization

Correct Answer: *C*

Community vote distribution

C (52%) B (37%) 11%

Question #242 *Topic 1*

Which of the following best describes the risk present after controls and mitigating factors have been applied?

A. Residual Most Voted

B. Avoided

C. Inherent

D. Operational

Correct Answer: *A*

Community vote distribution

A (100%)

Question #243 *Topic 1*

A software development team asked a security administrator to recommend techniques that should be used to reduce the chances of the software being reverse engineered. Which of the following should the security administrator recommend?

A. Digitally signing the software

B. Performing code obfuscation Most Voted

C. Limiting the use of third-party libraries

D. Using compile flags

Correct Answer: *B*

Community vote distribution

B (100%)

Question #244 *Topic 1*

Which of the following is a possible factor for MFA?

A. Something you exhibit

B. Something you have Most Voted

C. Somewhere you are

D. Someone you know

Correct Answer: *B*

Community vote distribution

B (100%)

Question #245 *Topic 1*

Easy-to-guess passwords led to an account compromise. The current password policy requires at least 12 alphanumeric characters, one uppercase character, one lowercase character, a password history of two passwords, a minimum password age of one day, and a maximum password age of 90 days. Which of the following would reduce the risk of this incident from happening again? (Choose two.)

A. Increasing the minimum password length to 14 characters. Most Voted

B. Upgrading the password hashing algorithm from MD5 to SHA-512.

C. Increasing the maximum password age to 120 days.

D. Reducing the minimum password length to ten characters.

E. Reducing the minimum password age to zero days.

F. Including a requirement for at least one special character. Most Voted

Correct Answer: *AF*

Community vote distribution

AF (85%) Other

Question #246 *Topic 1*

A user downloaded software from an online forum. After the user installed the software, the security team observed external network traffic connecting to the user's computer on an uncommon port. Which of the following is the most likely explanation of this unauthorized connection?

A. The software had a hidden keylogger.

B. The software was ransomware.

C. The user's computer had a fileless virus.

D. The software contained a backdoor.

Correct Answer: *D*

Community vote distribution

D (100%)

Question #247 *Topic 1*

A utility company is designing a new platform that will host all the virtual machines used by business applications. The requirements include:

- A starting baseline of 50% memory utilization
- Storage scalability
- Single circuit failure resilience

Which of the following best meets all of these requirements?

A. Connecting dual PDUs to redundant power supplies

B. Transitioning the platform to an IaaS provider Most Voted

C. Configuring network load balancing for multiple paths

D. Deploying multiple large NAS devices for each host

Correct Answer: *B*

Community vote distribution

B (100%)

Question #248 *Topic 1*

Which of the following best describes a use case for a DNS sinkhole?

A. Attackers can see a DNS sinkhole as a highly valuable resource to identify a company's domain structure.

B. A DNS sinkhole can be used to draw employees away from known-good websites to malicious ones owned by the attacker.

C. A DNS sinkhole can be used to capture traffic to known-malicious domains used by attackers.

D. A DNS sinkhole can be set up to attract potential attackers away from a company's network resources.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #249 *Topic 1*

An incident analyst finds several image files on a hard disk. The image files may contain geolocation coordinates. Which of the following best describes the type of information the analyst is trying to extract from the image files?

A. Log data

B. Metadata Most Voted

C. Encrypted data

D. Sensitive data

Correct Answer: *B*

Community vote distribution

B (100%)

Question #250 *Topic 1*

Which of the following most likely describes why a security engineer would configure all outbound emails to use S/MIME digital signatures?

A. To meet compliance standards

B. To increase delivery rates

C. To block phishing attacks

D. To ensure non-repudiation Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #251 *Topic 1*

During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?

A. Whaling

B. Credential harvesting

C. Prepending

D. Dumpster diving

Correct Answer: *D*

Question #252 *Topic 1*

Which of the following considerations is the most important regarding cryptography used in an IoT device?

A. Resource constraints Most Voted

B. Available bandwidth

C. The use of block ciphers

D. The compatibility of the TLS version

Correct Answer: *A*

Community vote distribution

A (82%) C (18%)

Question #253 *Topic 1*

A coffee shop owner wants to restrict internet access to only paying customers by prompting them for a receipt number. Which of the following is the best method to use given this requirement?

A. WPA3

B. Captive portal Most Voted

C. PSK

D. IEEE 802.1X

Correct Answer: *B*

Community vote distribution

B (100%)

Question #254 *Topic 1*

While performing digital forensics, which of the following is considered the most volatile and should have the contents collected first?

A. Hard drive

B. RAM Most Voted

C. SSD

D. Temporary files

Correct Answer: *B*

Community vote distribution

B (100%)

Question #255 *Topic 1*

A hosting provider needs to prove that its security controls have been in place over the last six months and have sufficiently protected customer data. Which of the following would provide the best proof that the hosting provider has met the requirements?

A. NIST CSF

B. SOC 2 Type 2 report Most Voted

C. CIS Top 20 compliance reports

D. Vulnerability report

Correct Answer: *B*

Community vote distribution

B (100%)

Question #256 *Topic 1*

A city municipality lost its primary data center when a tornado hit the facility. Which of the following should the city staff use immediately after the disaster to handle essential public services?

A. BCP

B. Communication plan

C. DRP Most Voted

D. IRP

Correct Answer: *C*

Community vote distribution

C (67%) A (33%)

Question #257 *Topic 1*

Which of the following is considered a preventive control?

A. Configuration auditing

B. Log correlation

C. Incident alerts

D. Segregation of duties Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #258 *Topic 1*

A systems administrator notices that a testing system is down. While investigating, the systems administrator finds that the servers are online and accessible from any device on the server network. The administrator reviews the following information from the monitoring system:

Server name	IP	Traffic sent	Traffic received	Status
File01	10.12.14.13	2654812	23185	Up
DC01	10.12.15.2	168741	65481	Up
Test01	10.25.1.3	14872	654123168	Down
Test02	10.25.1.4	16941	651321685	Down
DC02	10.12.15.3	32145	32158	Up
Finance01	10.18.1.14	12374	6548	Up

Which of the following is the most likely cause of the outage?

A. Denial of service Most Voted

B. ARP poisoning

C. Jamming

D. Kerberoasting

Correct Answer: *A*

Community vote distribution

A (100%)

Question #259 *Topic 1*

A security team has been alerted to a flood of incoming emails that have various subject lines and are addressed to multiple email inboxes. Each email contains a URL shortener link that is redirecting to a dead domain. Which of the following is the best step for the security team to take?

A. Create a blocklist for all subject lines.

B. Send the dead domain to a DNS sinkhole.

C. Quarantine all emails received and notify all employees.

D. Block the URL shortener domain in the web proxy. Most Voted

Correct Answer: *D*

Community vote distribution

D (46%) B (46%) 8%

Question #260 *Topic 1*

A security administrator is working to secure company data on corporate laptops in case the laptops are stolen. Which of the following solutions should the administrator consider?

A. Disk encryption Most Voted

B. Data loss prevention

C. Operating system hardening

D. Boot security

Correct Answer: *A*

Community vote distribution

A (100%)

Question #261 *Topic 1*

A company needs to keep the fewest records possible, meet compliance needs, and ensure destruction of records that are no longer needed. Which of the following best describes the policy that meets these requirements?

A. Security policy

B. Classification policy

C. Retention policy Most Voted

D. Access control policy

Correct Answer: *C*

Community vote distribution

C (100%)

Question #262 *Topic 1*

Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

A. Code repositories

B. Dark web

C. Threat feeds

D. State actors

E. Vulnerability databases

Correct Answer: *A*

Community vote distribution

A (100%)

Question #263 *Topic 1*

Which of the following is the best reason an organization should enforce a data classification policy to help protect its most sensitive information?

A. End users will be required to consider the classification of data that can be used in documents.

B. The policy will result in the creation of access levels for each level of classification.

C. The organization will have the ability to create security requirements based on classification levels.

D. Security analysts will be able to see the classification of data within a document before opening it.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #264 *Topic 1*

An analyst is performing a vulnerability scan against the web servers exposed to the internet without a system account. Which of the following is most likely being performed?

A. Non-credentialed scan Most Voted

B. Packet capture

C. Privilege escalation

D. System enumeration

E. Passive scan

Correct Answer: *A*

Community vote distribution

A (100%)

Question #265 *Topic 1*

A security administrator is hardening corporate systems and applying appropriate mitigations by consulting a real-world knowledge base for adversary behavior. Which of the following would be best for the administrator to reference?

A. MITRE ATT&CK Most Voted

B. CSIRT

C. CVSS

D. SOAR

Correct Answer: *A*

Community vote distribution

A (100%)

Question #266 *Topic 1*

An architect has a request to increase the speed of data transfer using JSON requests externally. Currently, the organization uses SFTP to transfer data files. Which of the following will most likely meet the requirements?

A. A website-hosted solution

B. Cloud shared storage

C. A secure email solution

D. Microservices using API

Correct Answer: *D*

Community vote distribution

D (100%)

Question #267 *Topic 1*

Which of the following addresses individual rights such as the right to be informed, the right of access, and the right to be forgotten?

A. GDPR Most Voted

B. PCI DSS

C. NIST

D. ISO

Correct Answer: *A*

Community vote distribution

A (100%)

Question #268 *Topic 1*

An administrator is installing an LDAP browser tool in order to view objects in the corporate LDAP directory. Secure connections to the LDAP server are required. When the browser connects to the server, certificate errors are being displayed, and then the connection is terminated. Which of the following is the most likely solution?

A. The administrator should allow SAN certificates in the browser configuration.

B. The administrator needs to install the server certificate into the local truststore.

C. The administrator should request that the secure LDAP port be opened to the server.

D. The administrator needs to increase the TLS version on the organization's RA.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #269 *Topic 1*

Which of the following is the most important security concern when using legacy systems to provide production service?

A. Instability

B. Lack of vendor support Most Voted

C. Loss of availability

D. Use of insecure protocols

Correct Answer: *B*

Community vote distribution

B (56%) D (41%)

Question #270 *Topic 1*

A security investigation revealed that malicious software was installed on a server using a server administrator's credentials. During the investigation, the server administrator explained that Telnet was regularly used to log in. Which of the following most likely occurred?

A. A spraying attack was used to determine which credentials to use.

B. A packet capture tool was used to steal the password. Most Voted

C. A remote-access Trojan was used to install the malware.

D. A dictionary attack was used to log in as the server administrator.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #271 *Topic 1*

A user is requesting Telnet access to manage a remote development web server. Insecure protocols are not allowed for use within any environment. Which of the following should be configured to allow remote access to this server?

A. HTTPS

B. SNMPv3

C. SSH Most Voted

D. RDP

E. SMTP

Correct Answer: *C*

Community vote distribution

C (100%)

Question #272 *Topic 1*

A security administrator is working to find a cost-effective solution to implement certificates for a large number of domains and subdomains owned by the company. Which of the following types of certificates should the administrator implement?

A. Wildcard Most Voted

B. Client certificate

C. Self-signed

D. Code signing

Correct Answer: *A*

Community vote distribution

A (86%) 14%

Question #273 *Topic 1*

An auditor discovered multiple insecure ports on some servers. Other servers were found to have legacy protocols enabled. Which of the following tools did the auditor use to discover these issues?

A. Nessus Most Voted

B. curl

C. Wireshark

D. netcat

Correct Answer: *A*

Community vote distribution

A (100%)

Question #274 *Topic 1*

A security analyst received a tip that sensitive proprietary information was leaked to the public. The analyst is reviewing the PCAP and notices traffic between an internal server and an external host that includes the following:

...
12:47:22.327233 PPPoE [ses 0x8122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41), length 331) 10.5.1.1 > 52.165.16.154: IP6 (hlim E3, next-header TCP (6) paylcad length: 271) 2001:67c:2158:a019::ace.53104 > 2001:0:5ef5:79fd:380c:dddd:a601:24fa.13788: Flags [P.], cksum 0xd7ee (correct), seq 97:348, ack 102, win 16444, length 251
...

Which of the following was most likely used to exfiltrate the data?

A. Encapsulation Most Voted

B. MAC address spoofing

C. Steganography

D. Broken encryption

E. Sniffing via on-path position

Correct Answer: *A*

Community vote distribution

A (100%)

Question #275 *Topic 1*

A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?

A. Serverless architecture Most Voted

B. Thin clients

C. Private cloud

D. Virtual machines

Correct Answer: *A*

Community vote distribution

A (100%)

Question #276 *Topic 1*

A security administrator is performing an audit on a stand-alone UNIX server, and the following message is immediately displayed:

(Error 13): /etc/shadow: Permission denied.

Which of the following best describes the type of tool that is being used?

A. Pass-the-hash monitor

B. File integrity monitor

C. Forensic analysis

D. Password cracker Most Voted

Correct Answer: *D*

Community vote distribution

D (56%) B (44%)

Question #277 *Topic 1*

A security administrator needs to create firewall rules for the following protocols: RTP, SIP, H.323. and SRTP. Which of the following does this rule set support?

A. RTOS

B. VoIP Most Voted

C. SoC

D. HVAC

Correct Answer: *B*

Community vote distribution

B (100%)

Question #278 *Topic 1*

Which of the following best describes a social engineering attack that uses a targeted electronic messaging campaign aimed at a Chief Executive Officer?

A. Whaling Most Voted

B. Spear phishing

C. Impersonation

D. Identity fraud

Correct Answer: *A*

Community vote distribution

A (100%)

Question #279 *Topic 1*

During a penetration test, a flaw in the internal PKI was exploited to gain domain administrator rights using specially crafted certificates. Which of the following remediation tasks should be completed as part of the cleanup phase?

A. Updating the CRL

B. Patching the CA Most Voted

C. Changing passwords

D. Implementing SOAR

Correct Answer: *B*

Community vote distribution

B (55%) A (45%)

Question #280 *Topic 1*

A company wants to implement MFA. Which of the following enables the additional factor while using a smart card?

A. PIN Most Voted

B. Hardware token

C. User ID

D. SMS

Correct Answer: *A*

Community vote distribution

A (100%)

Question #281 *Topic 1*

A company hired an external consultant to assist with required system upgrades to a critical business application. A systems administrator needs to secure the consultant's access without sharing passwords to critical systems. Which of the following solutions should most likely be utilized?

A. TACACS+

B. SAML

C. An SSO platform

D. Role-based access control

E. PAM software

Correct Answer: *E*

Community vote distribution

E (100%)

Question #282 *Topic 1*

A newly implemented wireless network is designed so that visitors can connect to the wireless network for business activities. The legal department is concerned that visitors might connect to the network and perform illicit activities. Which of me following should the security team implement to address this concern?

A. Configure a RADIUS server to manage device authentication.

B. Use 802.1X on all devices connecting to wireless.

C. Add a guest captive portal requiring visitors to accept terms and conditions. Most Voted

D. Allow for new devices to be connected via WPS.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #283 *Topic 1*

Which of the following data roles is responsible for identifying risks and appropriate access to data?

A. Owner Most Voted

B. Custodian

C. Steward

D. Controller

Correct Answer: *A*

Community vote distribution

A (67%) C (27%) 7%

Question #284 *Topic 1*

Which of the following physical controls can be used to both detect and deter? (Choose two.)

A. Lighting Most Voted

B. Fencing

C. Signage

D. Sensor Most Voted

E. Bollard

F. Lock

Correct Answer: *AD*

Community vote distribution

AD (93%) 7%

Question #285 *Topic 1*

A multinational bank hosts several servers in its data center. These servers run a business-critical application used by customers to access their account information. Which of the following should the bank use to ensure accessibility during peak usage times?

A. Load balancer

B. Cloud backups

C. Geographic dispersal

D. Disk multipathing

Correct Answer: *A*

Question #286 *Topic 1*

The author of a software package is concerned about bad actors repackaging and inserting malware into the software. The software download is hosted on a website, and the author exclusively controls the website's contents. Which of the following techniques would best ensure the software's integrity?

A. Input validation

B. Code signing

C. Secure cookies

D. Fuzzing

Correct Answer: *B*

Question #287 *Topic 1*

A third-party vendor is moving a particular application to the end-of-life stage at the end of the current year. Which of the following is the most critical risk if the company chooses to continue running the application?

A. Lack of security updates Most Voted

B. Lack of new features

C. Lack of support

D. Lack of source code access

Correct Answer: *A*

Community vote distribution

A (100%)

Question #288 *Topic 1*

A security analyst recently read a report about a flaw in several of the organization's printer models that causes credentials to be sent over the network in cleartext, regardless of the encryption settings. Which of the following would be best to use to validate this finding?

A. Wireshark

B. netcat

C. Nessus

D. Nmap

Correct Answer: *A*

Community vote distribution

A (100%)

Question #289 *Topic 1*

A development team is launching a new public-facing web product. The Chief Information Security Officer has asked that the product be protected from attackers who use malformed or invalid inputs to destabilize the system. Which of the following practices should the development team implement?

A. Fuzzing Most Voted

B. Continuous deployment

C. Static code analysis

D. Manual peer review

Correct Answer: *A*

Community vote distribution

A (88%) 13%

Question #290 *Topic 1*

During an annual review of the system design, an engineer identified a few issues with the currently released design. Which of the following should be performed next according to best practices?

A. Risk management process

B. Product design process

C. Design review process

D. Change control process Most Voted

Correct Answer: *D*

Community vote distribution

D (56%) C (38%) 6%

Question #291 *Topic 1*

Which of the following is best to use when determining the severity of a vulnerability?

A. CVE

B. OSINT

C. SOAR

D. CVSS Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #292 *Topic 1*

An organization experienced a security breach that allowed an attacker to send fraudulent wire transfers from a hardened PC exclusively to the attacker's bank through remote connections. A security analyst is creating a timeline of events and has found a different PC on the network containing malware. Upon reviewing the command history, the analyst finds the following:

PS>.\mimikatz.exe "sekurlsa::pth /user:localadmin /domain:corp-domain.com /ntlm:B4B9B02E1F29A3CF193EAB28C8D617D3F327

Which of the following best describes how the attacker gained access to the hardened PC?

A. The attacker created fileless malware that was hosted by the banking platform.

B. The attacker performed a pass-the-hash attack using a shared support account. Most Voted

C. The attacker utilized living-off-the-land binaries to evade endpoint detection and response software.

D. The attacker socially engineered the accountant into performing bad transfers.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #293 *Topic 1*

Which of the following is the best resource to consult for information on the most common application exploitation methods?

A. OWASP Most Voted

B. STIX

C. OVAL

D. Threat intelligence feed

E. Common Vulnerabilities and Exposures

Correct Answer: *A*

Community vote distribution

A (67%) E (33%)

Question #294 *Topic 1*

A security analyst is reviewing the logs on an organization's DNS server and notices the following unusual snippet:

```
Log from named: post-processed 20230102 0045L
...
qry_source: 124.22.158.37 TCP/53
qry_dest: 52.165.16.154 TCP/53
qry_dest: 10.100.50.5 TCP/53
qry_type: AXFR
| zone int.comptia.org
-------------------| www A 10.100.50.21
-------------------| dns A 10.100.5.5
-------------------| adds A 10.101.10.10
-------------------| fshare A 10.101.10.20
-------------------| sip A 10.100.5.11
...
```

Which of the following attack techniques was most likely used?

A. Determining the organization's ISP-assigned address space

B. Bypassing the organization's DNS sinkholing

C. Footprinting the internal network Most Voted

D. Attempting to achieve initial access to the DNS server

E. Exfiltrating data from fshare.int.complia.org

Correct Answer: *C*

Community vote distribution

C (100%)

Question #295 *Topic 1*

A security analyst at an organization observed several user logins from outside the organization's network. The analyst determined that these logins were not performed by individuals within the organization. Which of the following recommendations would reduce the likelihood of future attacks? (Choose two.)

A. Disciplinary actions for users

B. Conditional access policies Most Voted

C. More regular account audits

D. Implementation of additional authentication factors Most Voted

E. Enforcement of content filtering policies

F. A review of user account permissions

Correct Answer: *BD*

Community vote distribution

BD (100%)

Question #296 *Topic 1*

A security team is addressing a risk associated with the attack surface of the organization's web application over port 443. Currently, no advanced network security capabilities are in place. Which of the following would be best to set up? (Choose two.)

A. NIDS Most Voted

B. Honeypot

C. Certificate revocation list

D. HIPS

E. WAF Most Voted

F. SIEM

Correct Answer: *AE*

Community vote distribution

AE (52%) DE (31%) EF (17%)

Question #297 *Topic 1*

A systems administrator would like to create a point-in-time backup of a virtual machine. Which of the following should the administrator use?

A. Replication

B. Simulation

C. Snapshot

D. Containerization

Correct Answer: *C*

Question #298 *Topic 1*

A security administrator notices numerous unused, non-compliant desktops are connected to the network. Which of the following actions would the administrator most likely recommend to the management team?

A. Monitoring

B. Decommissioning Most Voted

C. Patching

D. Isolating

Correct Answer: *B*

Community vote distribution

B (88%) 13%

Question #299 *Topic 1*

Which of the following is a common data removal option for companies that want to wipe sensitive data from hard drives in a repeatable manner but allow the hard drives to be reused?

A. Sanitization

B. Formatting

C. Degaussing

D. Defragmentation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #300 *Topic 1*

An organization wants to improve the company's security authentication method for remote employees. Given the following requirements:

- Must work across SaaS and internal network applications
- Must be device manufacturer agnostic
- Must have offline capabilities

Which of the following would be the most appropriate authentication method?

A. Username and password

B. Biometrics

C. SMS verification

D. Time-based tokens Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #301 *Topic 1*

A security officer is implementing a security awareness program and has placed security-themed posters around the building and assigned online user training. Which of the following will the security officer most likely implement?

A. Password policy

B. Access badges

C. Phishing campaign

D. Risk assessment

Correct Answer: *C*

Community vote distribution

C (100%)

Question #302 *Topic 1*

A malicious update was distributed to a common software platform and disabled services at many organizations. Which of the following best describes this type of vulnerability?

A. DDoS attack

B. Rogue employee

C. Insider threat

D. Supply chain Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #303 *Topic 1*

A company web server is initiating outbound traffic to a low-reputation, public IP on non-standard pat. The web server is used to present an unauthenticated page to clients who upload images the company. An analyst notices a suspicious process running on the server hat was not created by the company development team. Which of the following is the most likely explanation for his security incident?

A. A web shell has been deployed to the server through the page. Most Voted

B. A vulnerability has been exploited to deploy a worm to the server.

C. Malicious insiders are using the server to mine cryptocurrency.

D. Attackers have deployed a rootkit Trojan to the server over an exposed RDP port.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #304 *Topic 1*

An organization requests a third-party full-spectrum analysis of its supply chain. Which of the following would the analysis team use to meet this requirement?

A. Vulnerability scanner

B. Penetration test

C. SCAP

D. Illumination tool Most Voted

Correct Answer: *D*

Community vote distribution

D (63%) C (27%) 10%

Question #305 *Topic 1*

A systems administrator deployed a monitoring solution that does not require installation on the endpoints that the solution is monitoring. Which of the following is described in this scenario?

A. Agentless solution Most Voted

B. Client-based soon

C. Open port

D. File-based solution

Correct Answer: *A*

Community vote distribution

A (100%)

Question #306 *Topic 1*

A security analyst is reviewing the source code of an application in order to identify misconfigurations and vulnerabilities. Which of the following kinds of analysis best describes this review?

A. Dynamic

B. Static Most Voted

C. Gap

D. Impact

Correct Answer: *B*

Community vote distribution

B (100%)

Question #307 *Topic 1*

Which of the following agreement types is used to limit external discussions?

A. BPA

B. NDA Most Voted

C. SLA

D. MSA

Correct Answer: *B*

Community vote distribution

B (100%)

Question #308 *Topic 1*

A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor. Which of the following processes is the analyst most likely conducting?

A. Internal audit

B. Penetration testing

C. Attestation

D. Due diligence Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #309 *Topic 1*

Which of the following is used to conceal credit card information in a database log file?

A. Tokenization

B. Masking Most Voted

C. Hashing

D. Obfuscation

Correct Answer: *B*

Community vote distribution

B (70%) A (30%)

Question #310 *Topic 1*

SIMULATION

-

A systems administrator is configuring a site-to-site VPN between two branch offices. Some of the settings have already been configured correctly. The systems administrator has been provided the following requirements as part of completing the configuration:

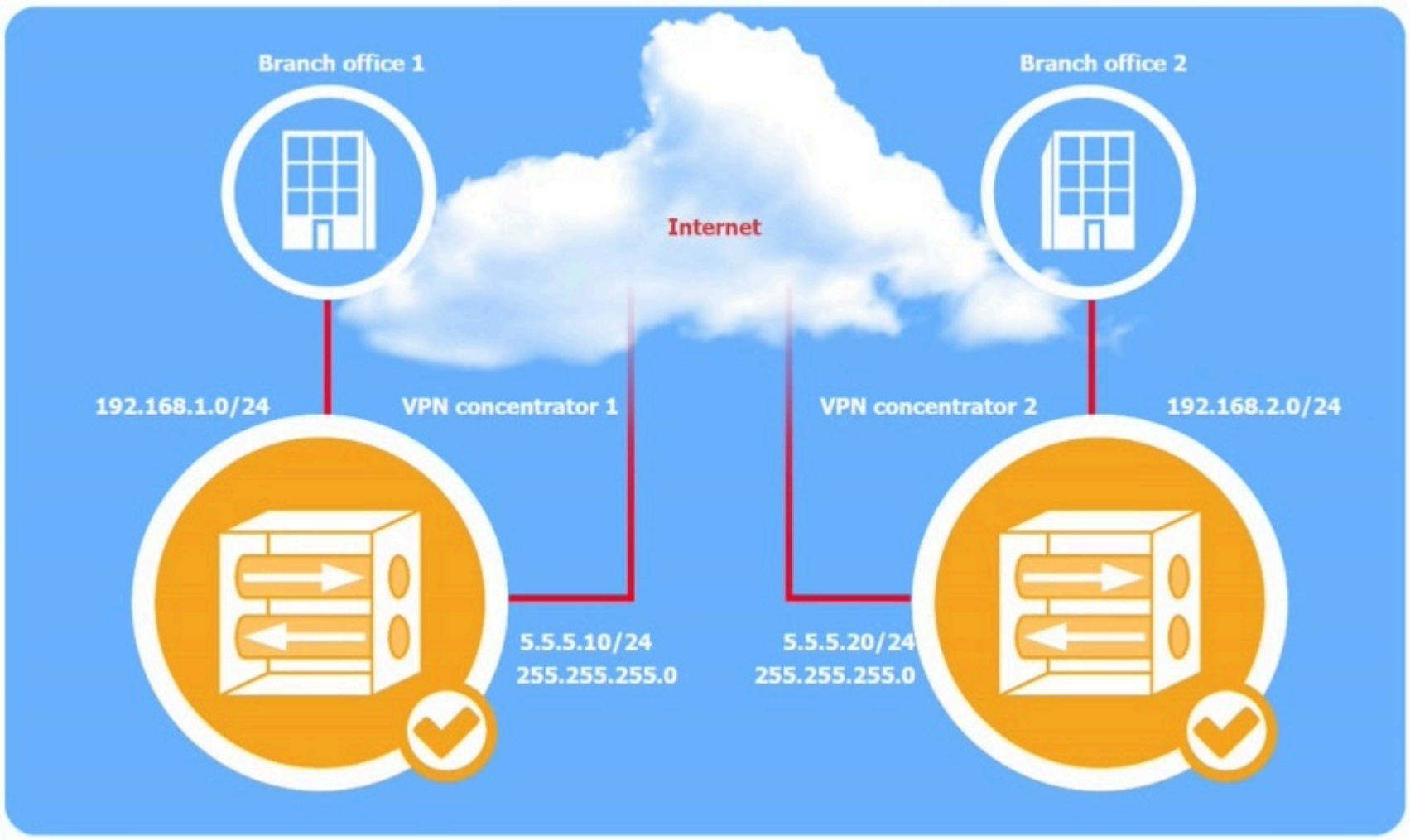
• Most secure algorithms should be selected
• All traffic should be encrypted over the VPN
• A secret password will be used to authenticate the two VPN concentrators

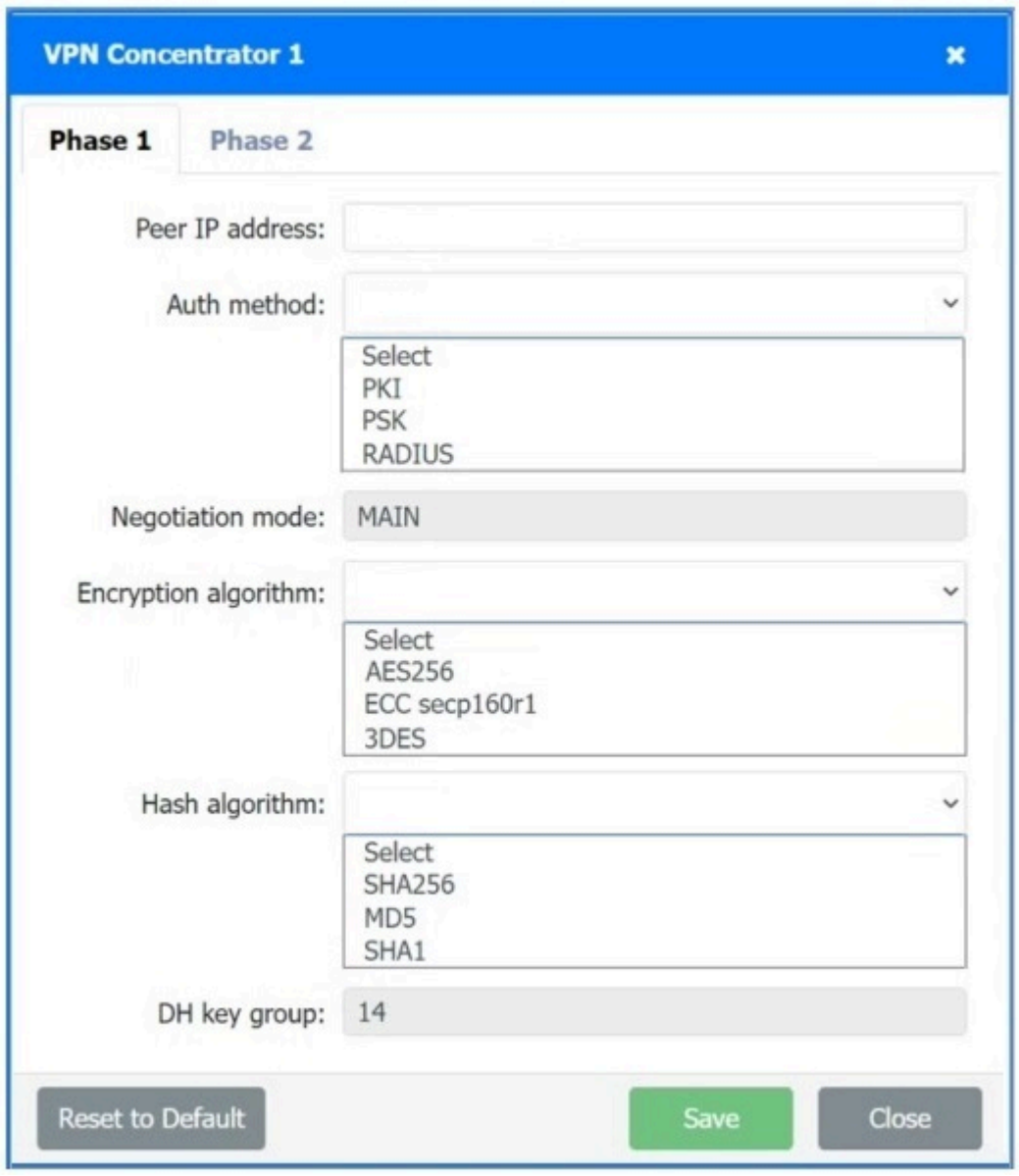
INSTRUCTIONS

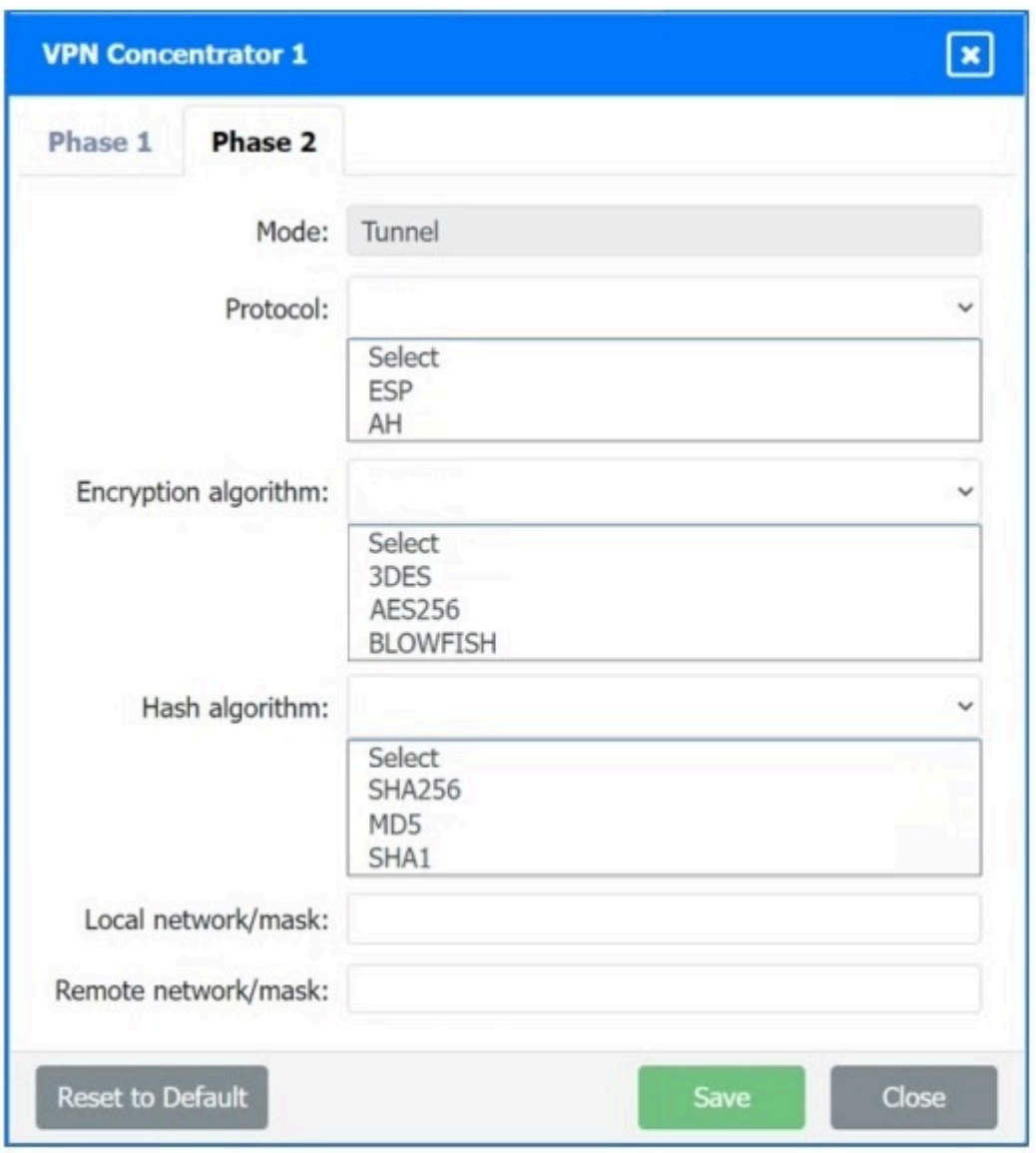
-

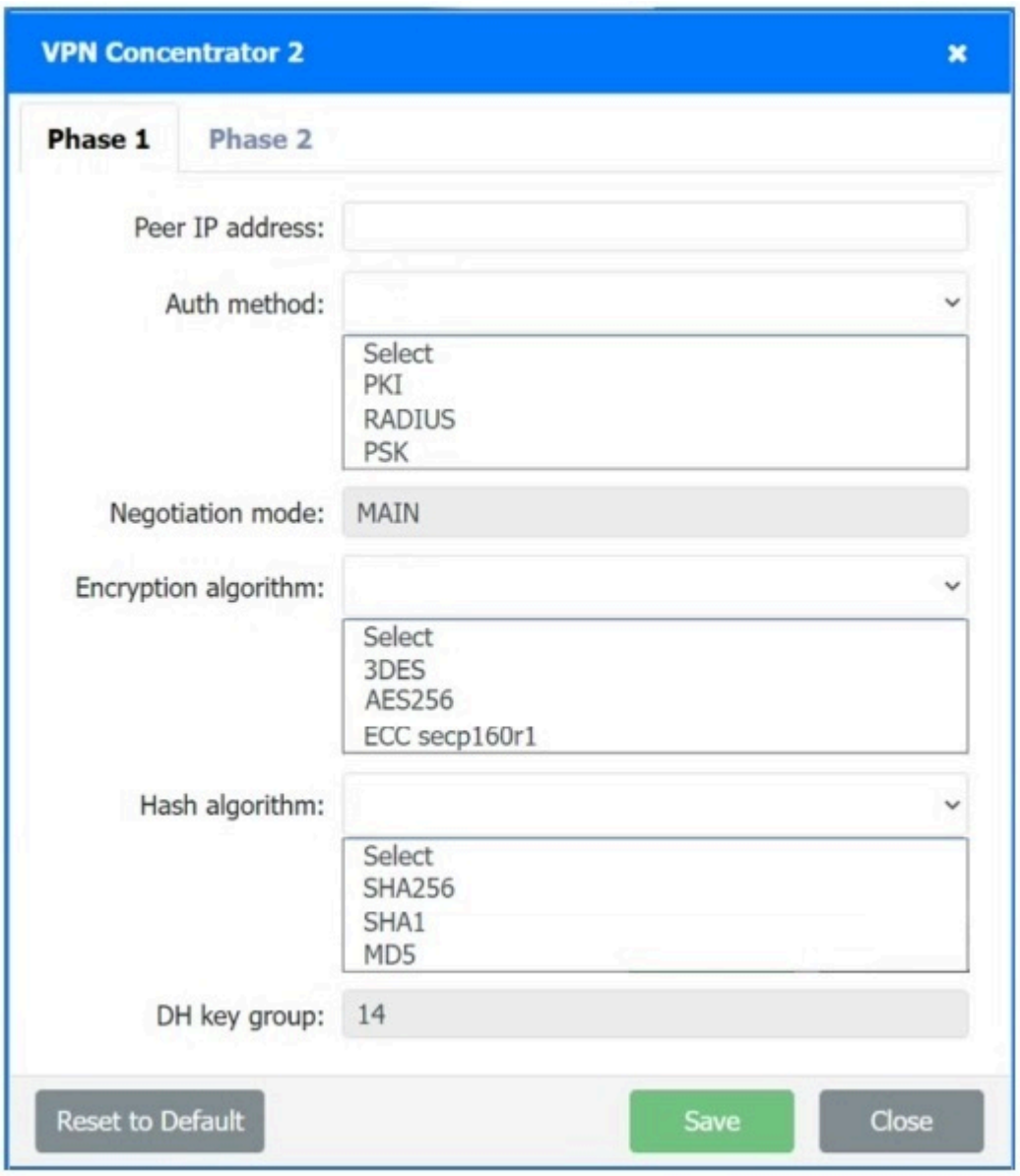
Click on the two VPN Concentrators to configure the appropriate settings.

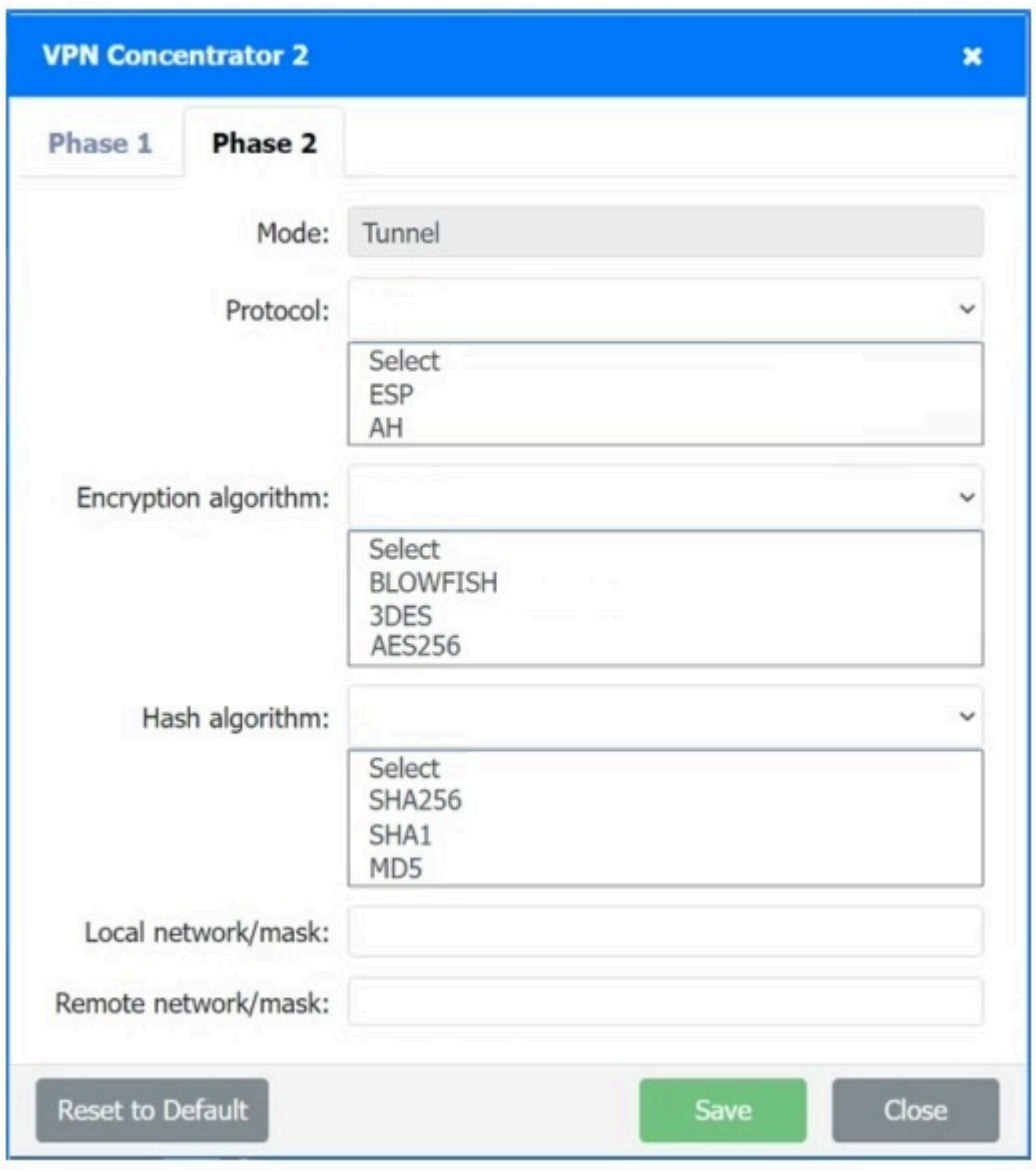
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

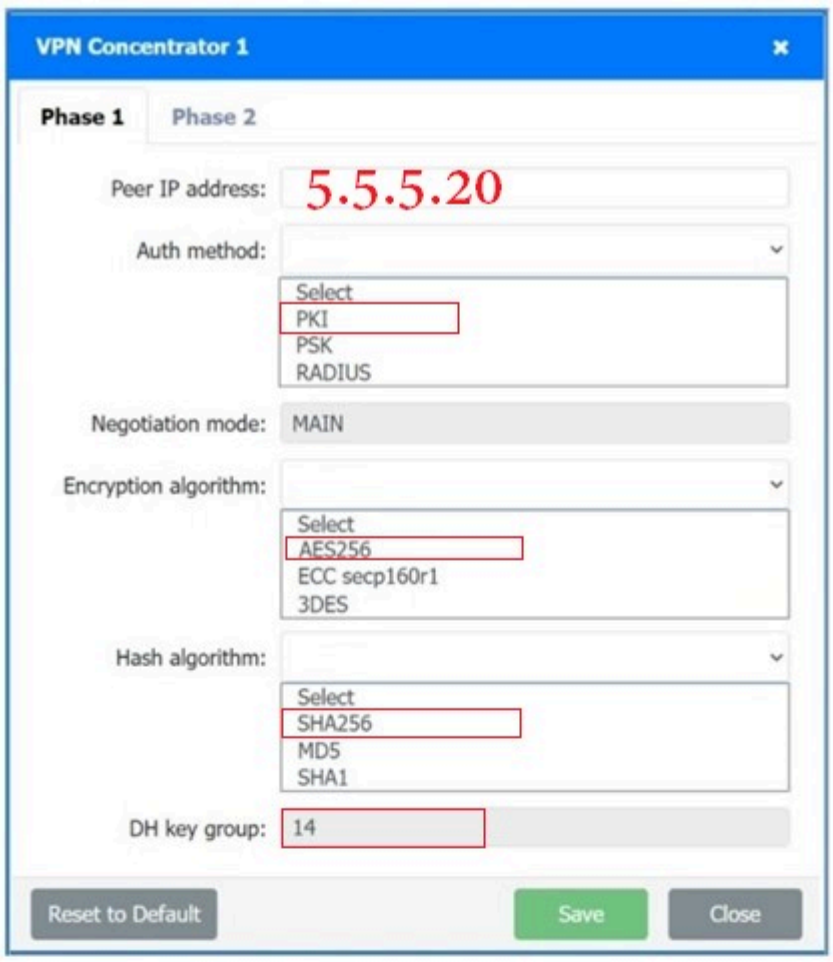


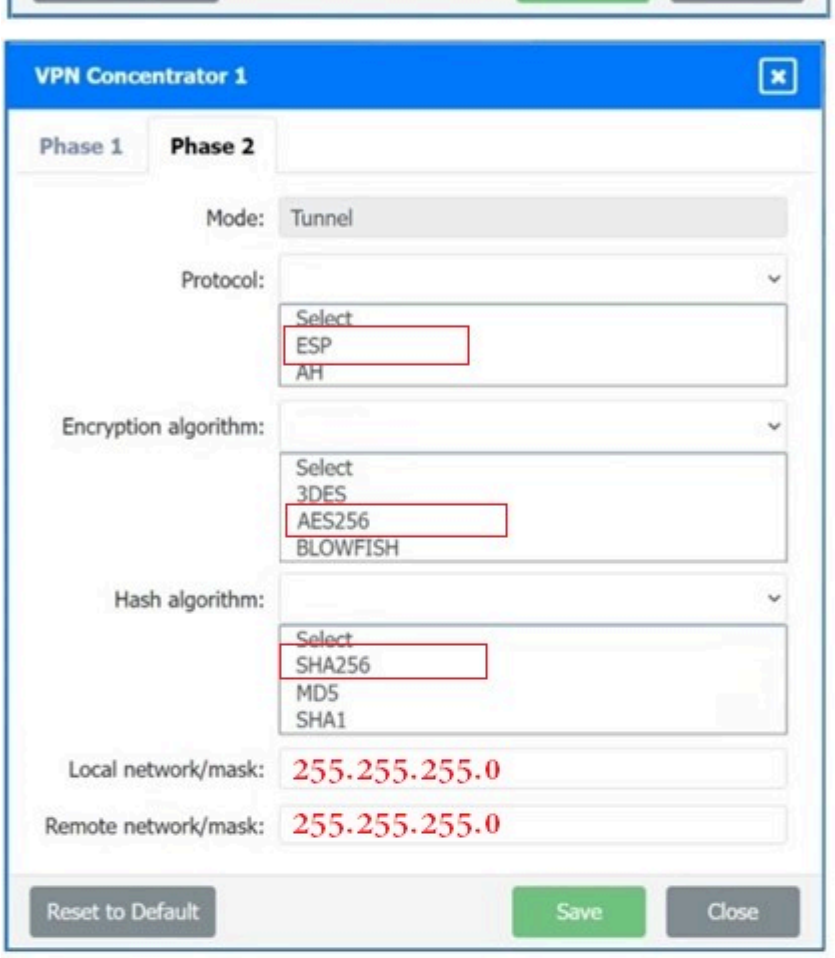

VPN Concentrator 1
Phase 1
Phase 2
Peer IP address:
Auth method:
Select
PKI
PSK
RADIUS
Negotiation mode:
MAIN
Encryption algorithm:
Select
AES256
ECC secp160r1
3DES
Hash algorithm:
Select
SHA256
MD5
SHA1
DH key group:
14
Reset to Default
Save
Close


VPN Concentrator 1
Phase 1
Phase 2
Mode:
Tunnel
Protocol:
Select
ESP
AH
Encryption algorithm:
Select
3DES
AES256
BLOWFISH
Hash algorithm:
Select
SHA256
MD5
SHA1
Local network/mask:
Remote network/mask:
Reset to Default
Save
Close

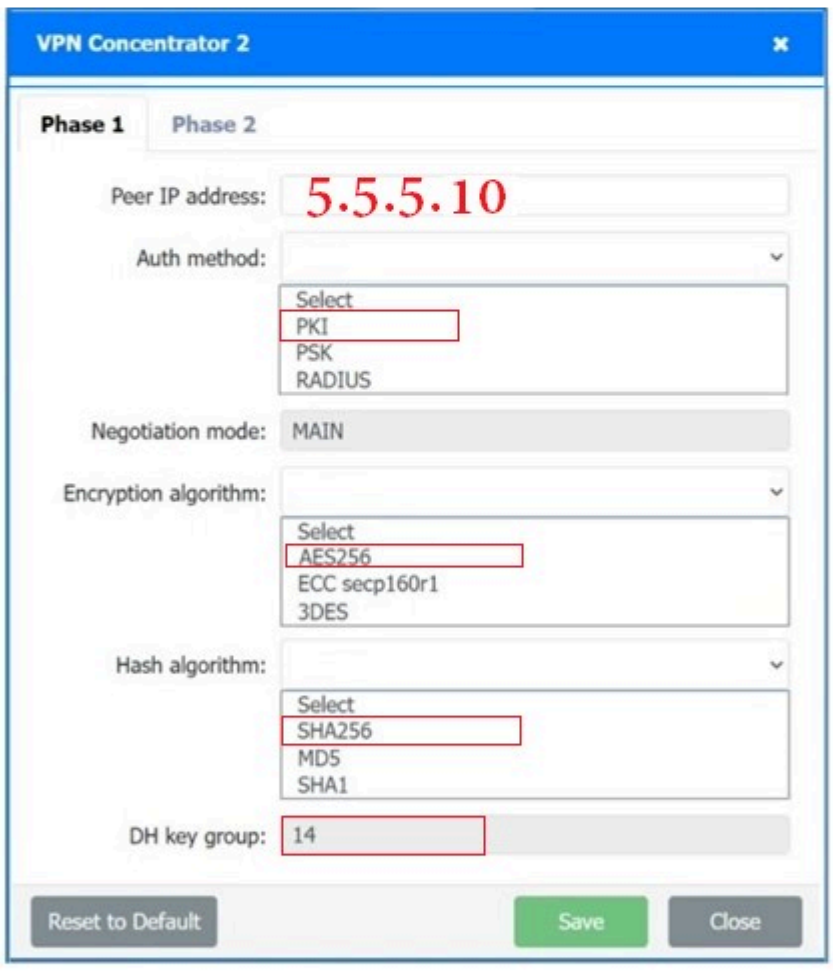

VPN Concentrator 2
Phase 1
Phase 2
Peer IP address:
Auth method:
Select
PKI
RADIUS
PSK
Negotiation mode:
MAIN
Encryption algorithm:
Select
3DES
AES256
ECC secp160r1
Hash algorithm:
Select
SHA256
SHA1
MD5
DH key group:
14
Reset to Default
Save
Close

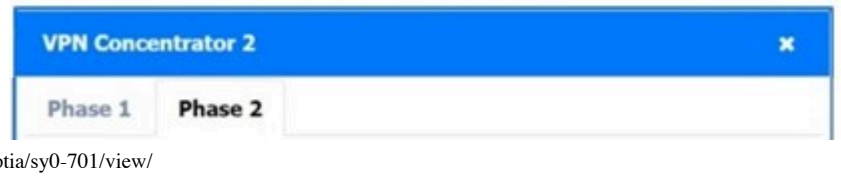

VPN Concentrator 2
Phase 1
Phase 2
Mode:
Tunnel
Protocol:
Select
ESP
AH
Encryption algorithm:
Select
BLOWFISH
3DES
AES256
Hash algorithm:
Select
SHA256
SHA1
MD5
Local network/mask:
Remote network/mask:
Reset to Default
Save
Close

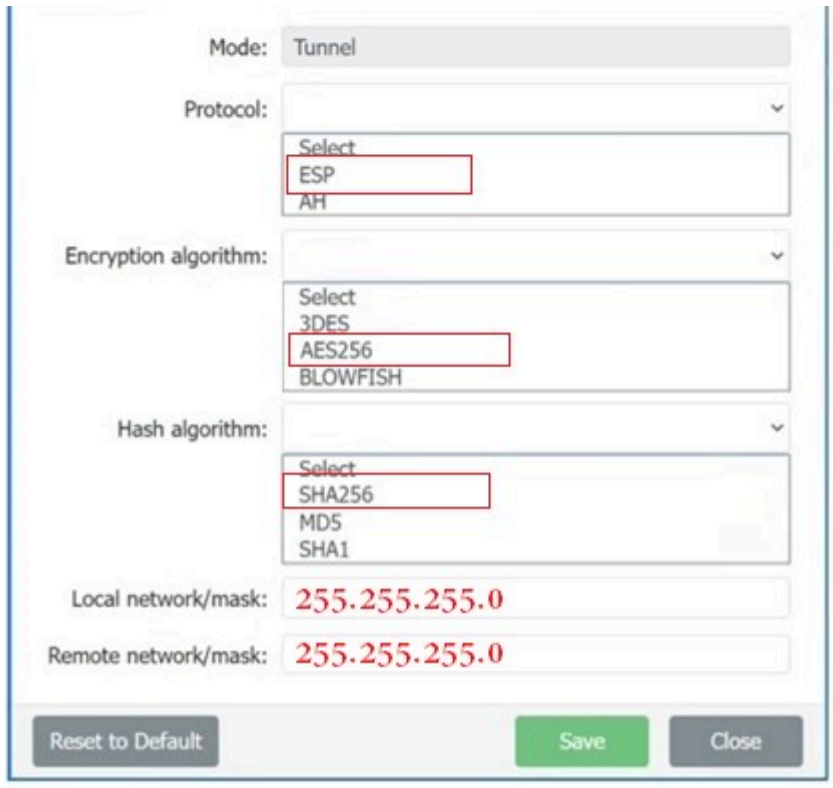




Correct Answer:







Question #311 *Topic 1*

An organization recently started hosting a new service that customers access through a web portal. A security engineer needs to add to the existing security devices a new solution to protect this new service. Which of the following is the engineer most likely to deploy?

A. Layer 4 firewall

B. NGFW

C. WAF Most Voted

D. UTM

Correct Answer: *C*

Community vote distribution

C (100%)

Question #312 *Topic 1*

Which of the following topics would most likely be included within an organization's SDLC?

A. Service-level agreements

B. Information security policy

C. Penetration testing methodology

D. Branch protection requirements Most Voted

Correct Answer: *D*

Community vote distribution

D (38%) C (38%) B (25%)

Question #313 *Topic 1*

Which of the following control types is AUP an example of?

A. Physical

B. Managerial Most Voted

C. Technical

D. Operational

Correct Answer: *B*

Community vote distribution

B (66%) D (34%)

Question #314 *Topic 1*

An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in, so the security team wants to reduce the number of credentials each employee must maintain. Which of the following is the first step the security team should take?

A. Enable SAML.

B. Create OAuth tokens.

C. Use password vaulting.

D. Select an IdP. Most Voted

Correct Answer: *D*

Community vote distribution

D (86%) 14%

Question #315 *Topic 1*

A company's online shopping website became unusable shortly after midnight on January 30, 2023. When a security analyst reviewed the database server, the analyst noticed the following code used for backing up data:

```
IF DATE() = "01/30/2023" THEN BEGIN
  DROP DATABASE WebShopOnline;
END
```

Which of the following should the analyst do next?

A. Check for recently terminated DBAs. Most Voted

B. Review WAF logs for evidence of command injection.

C. Scan the database server for malware.

D. Search the web server for ransomware notes.

Correct Answer: *A*

Community vote distribution

A (54%) B (46%)

Question #316 *Topic 1*

Which of the following would be the best way to test resiliency in the event of a primary power failure?

A. Parallel processing

B. Tabletop exercise

C. Simulation testing

D. Production failover Most Voted

Correct Answer: *D*

Community vote distribution

D (73%) A (18%) 9%

Question #317 *Topic 1*

Which of the following would be the most appropriate way to protect data in transit?

A. SHA-256

B. SSL3.0

C. TLS 1.3 Most Voted

D. AES-256

Correct Answer: *C*

Community vote distribution

C (100%)

Question #318 *Topic 1*

Which of the following is a common, passive reconnaissance technique employed by penetration testers in the early phases of an engagement?

A. Open-source intelligence Most Voted

B. Port scanning

C. Pivoting

D. Exploit validation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #319 *Topic 1*

Which of the following threat actors is the most likely to seek financial gain through the use of ransomware attacks?

A. Organized crime Most Voted

B. Insider threat

C. Nation-state

D. Hacktivists

Correct Answer: *A*

Community vote distribution

A (100%)

Question #320 *Topic 1*

Which of the following would a systems administrator follow when upgrading the firmware of an organization's router?

A. Software development life cycle

B. Risk tolerance

C. Certificate signing request

D. Maintenance window Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #321 *Topic 1*

The security team has been asked to only enable host A (10.2.2.7) and host B (10.3.9.9) to the new isolated network segment (10.9.8.14) that provides access to legacy devices.
Access from all other hosts should be blocked. Which of the following entries would need to be added on the firewall?

A.
```
Permit 10.2.2.0/24 to 10.9.8.14/27
Permit 10.3.9.0/24 to 10.9.8.14/27
Deny 0.0.0.0/0 to 10.9.8.14/27
```

B.
```
Deny 0.0.0.0/0 to 10.9.8.14/27
Permit 10.2.2.0/24 to 10.9.8.14/27
Permit 10.3.9.0/24 to 10.9.8.14/27
```

C.
```
Permit 10.2.2.7/32 to 10.9.8.14/27
Permit 10.3.9.9/32 to 10.9.8.14/27
Deny 0.0.0.0/0 to 10.9.8.14/27
```
Most Voted

D.
```
Permit 10.2.2.7/32 to 10.9.8.14/27
Permit 10.3.9.0/24 to 10.9.8.14/27
Deny 10.9.8.14/27 to 0.0.0.0/0
```

Correct Answer: *C*

Community vote distribution

C (100%)

Question #322 *Topic 1*

SIMULATION

-

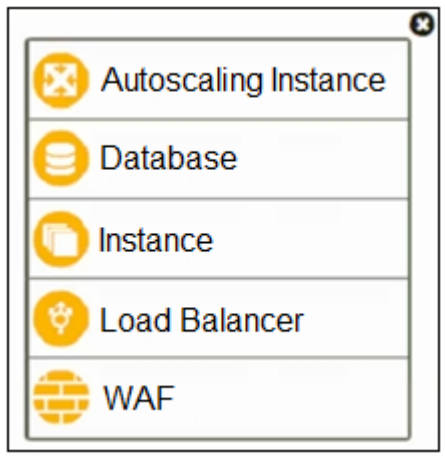
A security analyst is creating the first draft of a network diagram for the company's new customer-facing payment application that will be hosted by a third-party cloud service provider.

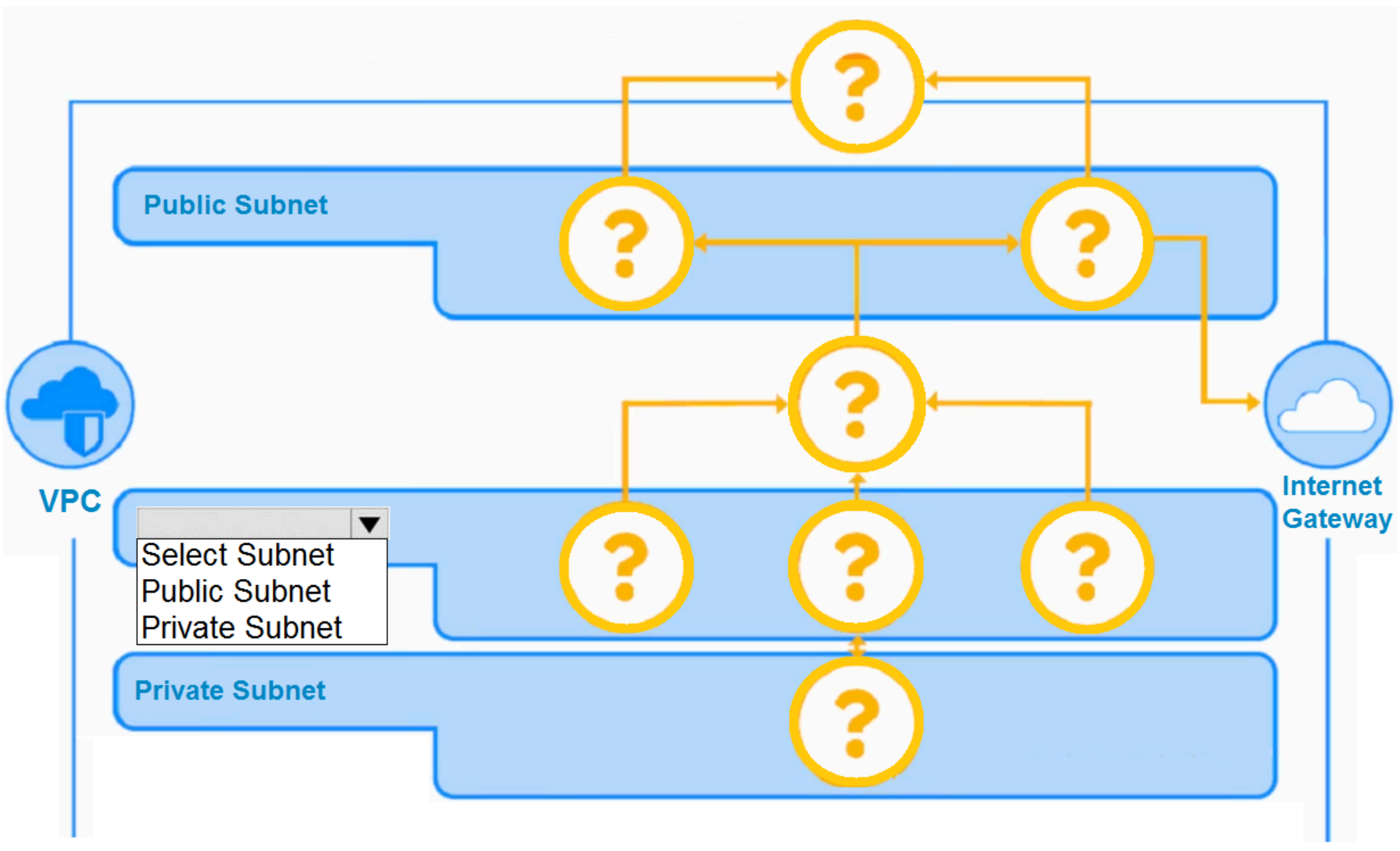
INSTRUCTIONS

-

Click the ? to select the appropriate icons to create a secure, redundant web application. Then use the dropdown menu to select the appropriate subnet type. Every space in the diagram must be filled.

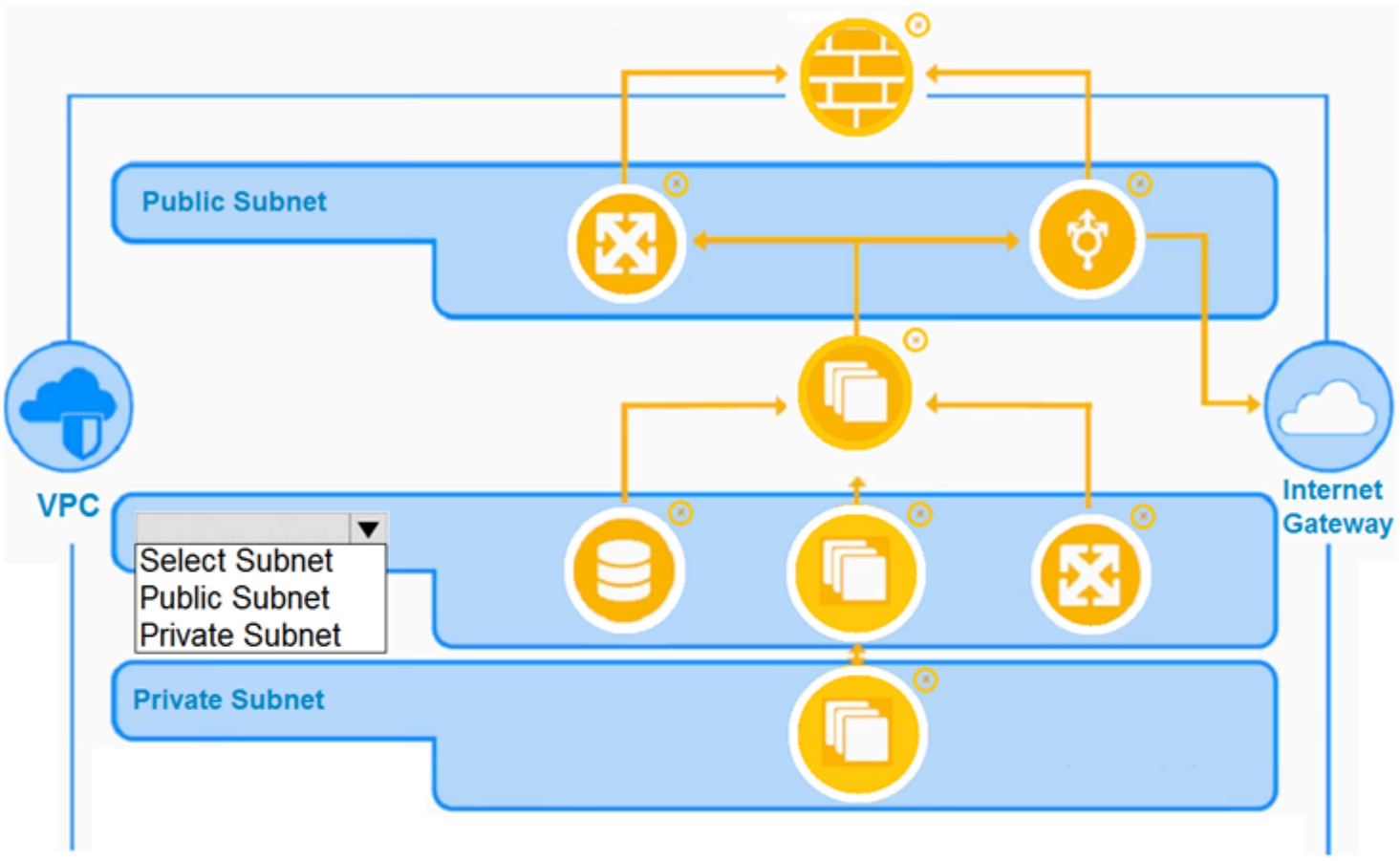
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Correct Answer:

The diagram should be filled in the way shown below.



WAF (Web Application Firewall) at the top to handle incoming traffic from the Internet Gateway.
Load Balancer for distributing traffic between instances.
Instances for handling the application workloads, ensuring multiple instances for redundancy.
Autoscaling Instance to adjust the number of instances based on demand dynamically.

In the middle of the diagram, you should select **Private Subnet** in the dropdown menu.

This choice is appropriate because the elements in the lower section, especially the **Database** instances, are part of the private subnet. Placing databases in a private subnet adds an additional layer of security, as it prevents direct internet access to sensitive data. The private subnet is also typically used for backend resources that don't need to be exposed publicly.

Question #323 *Topic 1*

A systems administrator needs to ensure the secure communication of sensitive data within the organization's private cloud. Which of the following is the best choice for the administrator to implement?

A. IPSec Most Voted

B. SHA-1

C. RSA

D. TGT

Correct Answer: *A*

Community vote distribution

A (100%)

Question #324 *Topic 1*

Which of the following should an internal auditor check for first when conducting an audit of the organization's risk management program?

A. Policies and procedures

B. Asset management

C. Vulnerability assessment

D. Business impact analysis

Correct Answer: *A*

Question #325 *Topic 1*

Which of the following activities are associated with vulnerability management? (Choose two.)

A. Reporting Most Voted

B. Prioritization Most Voted

C. Exploiting

D. Correlation

E. Containment

F. Tabletop exercise

Correct Answer: *AB*

Community vote distribution

AB (87%) 7%

Question #326 *Topic 1*

An administrator wants to perform a risk assessment without using proprietary company information. Which of the following methods should the administrator use to gather information?

A. Network scanning

B. Penetration testing

C. Open-source intelligence

D. Configuration auditing

Correct Answer: *C*

Question #327 *Topic 1*

A systems administrator is concerned about vulnerabilities within cloud computing instances. Which of the following is most important for the administrator to consider when architecting a cloud computing environment?

A. SQL injection

B. TOC/TOU

C. VM escape

D. Tokenization

E. Password spraying

Correct Answer: *C*

Question #328 *Topic 1*

A database administrator is updating the company's SQL database, which stores credit card information for pending purchases. Which of the following is the best method to secure the data against a potential breach?

A. Hashing

B. Obfuscation

C. Tokenization Most Voted

D. Masking

Correct Answer: *C*

Community vote distribution

C (65%) D (35%)

Question #329 *Topic 1*

Which of the following is a benefit of vendor diversity?

A. Patch availability

B. Zero-day resiliency

C. Secure configuration guide applicability

D. Load balancing

Correct Answer: *B*

Community vote distribution

B (100%)

Question #330 *Topic 1*

An employee used a company's billing system to issue fraudulent checks. The administrator is looking for evidence of other occurrences of this activity. Which of the following should the administrator examine?

A. Application logs Most Voted

B. Vulnerability scanner logs

C. IDS/IPS logs

D. Firewall logs

Correct Answer: *A*

Community vote distribution

A (100%)

Question #331 *Topic 1*

An organization is looking to optimize its environment and reduce the number of patches necessary for operating systems. Which of the following will best help to achieve this objective?

A. Microservices

B. Virtualization

C. Real-time operating system

D. Containers Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #332 *Topic 1*

Which of the following tasks is typically included in the BIA process?

A. Estimating the recovery time of systems Most Voted

B. Identifying the communication strategy

C. Evaluating the risk management plan

D. Establishing the backup and recovery procedures

E. Developing the incident response plan

Correct Answer: *A*

Community vote distribution

A (100%)

Question #333 *Topic 1*

Which of the following is a risk of conducting a vulnerability assessment?

A. A disruption of business operations Most Voted

B. Unauthorized access to the system

C. Reports of false positives

D. Finding security gaps in the system

Correct Answer: *A*

Community vote distribution

A (67%) C (33%)

Question #334 *Topic 1*

Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

A. Creating a false text file in /docs/salaries Most Voted

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: *A*

Community vote distribution

A (77%) B (23%)

Question #335 *Topic 1*

An organization maintains intellectual property that it wants to protect. Which of the following concepts would be most beneficial to add to the company's security awareness training program?

A. Insider threat detection Most Voted

B. Simulated threats

C. Phishing awareness

D. Business continuity planning

Correct Answer: *A*

Community vote distribution

A (83%) D (17%)

Question #336 *Topic 1*

An organization plans to expand its operations internationally and needs to keep data at the new location secure. The organization wants to use the most secure architecture model possible. Which of the following models offers the highest level of security?

A. Cloud-based

B. Peer-to-peer

C. On-premises Most Voted

D. Hybrid

Correct Answer: *C*

Community vote distribution

C (70%) D (20%) 10%

Question #337 *Topic 1*

Which of the following is the most relevant reason a DPO would develop a data inventory?

A. To manage data storage requirements better

B. To determine the impact in the event of a breach Most Voted

C. To extend the length of time data can be retained

D. To automate the reduction of duplicated data

Correct Answer: *B*

Community vote distribution

B (100%)

Question #338 *Topic 1*

Which of the following cryptographic solutions protects data at rest?

A. Digital signatures

B. Full disk encryption Most Voted

C. Private key

D. Steganography

Correct Answer: *B*

Community vote distribution

B (100%)

Question #339 *Topic 1*

Which of the following should an organization use to protect its environment from external attacks conducted by an unauthorized hacker?

A. ACL

B. IDS

C. HIDS

D. NIPS Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #340 *Topic 1*

Which of the following would enable a data center to remain operational through a multiday power outage?

A. Generator Most Voted

B. Uninterruptible power supply

C. Replication

D. Parallel processing

Correct Answer: *A*

Community vote distribution

A (100%)

Question #341 *Topic 1*

A company installed cameras and added signs to alert visitors that they are being recorded. Which of the following controls did the company implement? (Choose two.)

A. Directive

B. Deterrent Most Voted

C. Preventive

D. Detective Most Voted

E. Corrective

F. Technical

Correct Answer: *BD*

Community vote distribution

BD (100%)

Question #342 *Topic 1*

Which of the following is the best way to securely store an encryption key for a data set in a manner that allows multiple entities to access the key when needed?

A. Public key infrastructure

B. Open public ledger

C. Public key encryption

D. Key escrow Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #343 *Topic 1*

For which of the following reasons would a systems administrator leverage a 3DES hash from an installer file that is posted on a vendor's website?

A. To test the integrity of the file Most Voted

B. To validate the authenticity of the file

C. To activate the license for the file

D. To calculate the checksum of the file

Correct Answer: *A*

Community vote distribution

A (100%)

Question #344 *Topic 1*

A company is redesigning its infrastructure and wants to reduce the number of physical servers in use. Which of the following architectures is best suited for this goal?

A. Isolation

B. Segmentation

C. Virtualization Most Voted

D. Redundancy

Correct Answer: *C*

Community vote distribution

C (100%)

Question #345 *Topic 1*

Which of the following security concepts is being followed when implementing a product that offers protection against DDoS attacks?

A. Availability Most Voted

B. Non-repudiation

C. Integrity

D. Confidentiality

Correct Answer: *A*

Community vote distribution

A (100%)

Question #346 *Topic 1*

A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?

A. Set the maximum data retention policy.

B. Securely store the documents on an air-gapped network.

C. Review the documents' data classification policy.

D. Conduct a tabletop exercise with the team. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #347 *Topic 1*

After failing an audit twice, an organization has been ordered by a government regulatory agency to pay fines. Which of the following causes this action?

A. Non-compliance

B. Contract violations

C. Government sanctions

D. Rules of engagement

Correct Answer: *A*

Community vote distribution

A (100%)

Question #348 *Topic 1*

A company is developing a critical system for the government and storing project information on a fileshare. Which of the following describes how this data will most likely be classified? (Choose two.)

A. Private

B. Confidential Most Voted

C. Public

D. Operational

E. Urgent

F. Restricted Most Voted

Correct Answer: *BF*

Community vote distribution

BF (100%)

Question #349 *Topic 1*

Which of the following activities is included in the post-incident review phase?

A. Determining the root cause of the incident Most Voted

B. Developing steps to mitigate the risks of the incident

C. Validating the accuracy of the evidence collected during the investigation

D. Reestablishing the compromised system's configuration and settings

Correct Answer: *A*

Community vote distribution

A (100%)

Question #350 *Topic 1*

Which of the following attacks exploits a potential vulnerability as a result of using weak cryptographic algorithms?

A. Password cracking Most Voted

B. On-path

C. Digital signing

D. Side-channel

Correct Answer: *A*

Community vote distribution

A (65%) B (35%)

Question #351 *Topic 1*

Which of the following is a preventive physical security control?

A. Video surveillance system

B. Bollards Most Voted

C. Alarm system

D. Motion sensors

Correct Answer: *B*

Community vote distribution

B (86%) 14%

Question #352 *Topic 1*

Which of the following is most likely to be used as a just-in-time reference document within a security operations center?

A. Change management policy

B. Risk profile

C. Playbook

D. SIEM profile

Correct Answer: *C*

Question #353 *Topic 1*

A security engineer configured a remote access VPN. The remote access VPN allows end users to connect to the network by using an agent that is installed on the endpoint, which establishes an encrypted tunnel. Which of the following protocols did the engineer most likely implement?

A. GRE

B. IPSec Most Voted

C. SD-WAN

D. EAP

Correct Answer: *B*

Community vote distribution

B (100%)

Question #354 *Topic 1*

Executives at a company are concerned about employees accessing systems and information about sensitive company projects unrelated to the employees' normal job duties. Which of the following enterprise security capabilities will the security team most likely deploy to detect that activity?

A. UBA Most Voted

B. EDR

C. NAC

D. DLP

Correct Answer: *A*

Community vote distribution

A (100%)

Question #355 *Topic 1*

Several customers want an organization to verify its security controls are operating effectively and have requested an independent opinion. Which of the following is the most efficient way to address these requests?

A. Hire a vendor to perform a penetration test

B. Perform an annual self-assessment.

C. Allow each client the right to audit

D. Provide a third-party attestation report Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #356 *Topic 1*

A university employee logged on to the academic server and attempted to guess the system administrators' log-in credentials. Which of the following security measures should the university have implemented to detect the employee's attempts to gain access to the administrators' accounts?

A. Two-factor authentication

B. Firewall

C. Intrusion prevention system

D. User activity logs Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #357 *Topic 1*

Which of the following consequences would a retail chain most likely face from customers in the event the retailer is non-compliant with PCI DSS?

A. Contractual impacts

B. Sanctions

C. Fines

D. Reputational damage Most Voted

Correct Answer: *D*

Community vote distribution

D (89%) 11%

Question #358 *Topic 1*

A security analyst is reviewing logs and discovers the following:

```
149.32.228.10 - - [28/Jan/2023:16:32:45 -0300] "GET / HTTP/1.0"
User-Agent: ${/bin/sh/ id} 200 397
```

Which of the following should be used to best mitigate this type of attack?

A. Input sanitization Most Voted

B. Secure cookies

C. Static code analysis

D. Sandboxing

Correct Answer: *A*

Community vote distribution

A (100%)

Question #359 *Topic 1*

An administrator is installing an SSL certificate on a new system. During testing, errors indicate that the certificate is not trusted. The administrator has verified with the issuing CA and has validated the private key. Which of the following should the administrator check for next?

A. If the wildcard certificate is configured

B. If the certificate signing request is valid

C. If the root certificate is installed Most Voted

D. If the public key is configured

Correct Answer: *C*

Community vote distribution

C (100%)

Question #360 *Topic 1*

An employee emailed a new systems administrator a malicious web link and convinced the administrator to change the email server's password. The employee used this access to remove the mailboxes of key personnel. Which of the following security awareness concepts would help prevent this threat in the future?

A. Recognizing phishing Most Voted

B. Providing situational awareness training

C. Using password management

D. Reviewing email policies

Correct Answer: *A*

Community vote distribution

A (86%) 14%

Question #361 *Topic 1*

Which of the following strategies should an organization use to efficiently manage and analyze multiple types of logs?

A. Deploy a SIEM solution Most Voted

B. Create custom scripts to aggregate and analyze logs.

C. Implement EDR technology.

D. Install a unified threat management appliance.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #362 *Topic 1*

A new security regulation was announced that will take effect in the coming year. A company must comply with it to remain in business. Which of the following activities should the company perform next?

A. Gap analysis Most Voted

B. Policy review

C. Security procedure evaluation

D. Threat scope reduction

Correct Answer: *A*

Community vote distribution

A (100%)

Question #363 *Topic 1*

An accountant is transferring information to a bank over FTP. Which of the following mitigations should the accountant use to protect the confidentiality of the data?

A. Tokenization

B. Data masking

C. Encryption Most Voted

D. Obfuscation

Correct Answer: *C*

Community vote distribution

C (100%)

Question #364 *Topic 1*

An organization has recently decided to implement SSO. The requirements are to leverage access tokens and focus on application authorization rather than user authentication. Which of the following solutions would the engineering team most likely configure?

A. LDAP

B. Federation

C. SAML

D. OAuth Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #365 *Topic 1*

Which of the following would most likely be used by attackers to perform credential harvesting?

A. Social engineering Most Voted

B. Supply chain compromise

C. Third-party software

D. Rainbow table

Correct Answer: *A*

Community vote distribution

A (89%) 11%

Question #366 *Topic 1*

A security engineer would like to enhance the use of automation and orchestration within the SIEM. Which of the following would be the primary benefit of this enhancement?

A. It increases complexity.

B. It removes technical debt.

C. It adds additional guard rails.

D. It acts as a workforce multiplier. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #367 *Topic 1*

A systems administrator receives an alert that a company's internal file server is very slow and is only working intermittently. The systems administrator reviews the server management software and finds the following information about the server:

```
ServerName | #Connections | CPU%   |  MEM%  |  Read/s   |  Writes/s
FileSev01  |       12     | 99.6%  |   97%  |  50KB/s   |  100KB/s
```

Which of the following indicators most likely triggered this alert?

A. Concurrent session usage

B. Network saturation

C. Account lockout

D. Resource consumption

Correct Answer: *D*

Community vote distribution

D (100%)

Question #368 *Topic 1*

Which of the following data states applies to data that is being actively processed by a database server?

A. In use Most Voted

B. At rest

C. In transit

D. Being hashed

Correct Answer: *A*

Community vote distribution

A (100%)

Question #369 *Topic 1*

Which of the following architectures is most suitable to provide redundancy for critical business processes?

A. Network-enabled

B. Server-side

C. Cloud-native Most Voted

D. Multitenant

Correct Answer: *C*

Community vote distribution

C (71%) D (29%)

Question #370 *Topic 1*

After a security incident, a systems administrator asks the company to buy a NAC platform. Which of the following attack surfaces is the systems administrator trying to protect?

A. Bluetooth

B. Wired Most Voted

C. NFC

D. SCADA

Correct Answer: *B*

Community vote distribution

B (100%)

Question #371 *Topic 1*

While reviewing logs, a security administrator identifies the following code:

```
<script>function (send_info)</script>
```

Which of the following best describes the vulnerability being exploited?

A. XSS Most Voted

B. SQLi

C. DDoS

D. CSRF

Correct Answer: *A*

Community vote distribution

A (82%) B (18%)

Question #372 *Topic 1*

An organization issued new laptops to all employees and wants to provide web filtering both in and out of the office without configuring additional access to the network. Which of the following types of web filtering should a systems administrator configure?

A. Agent-based Most Voted

B. Centralized proxy

C. URL scanning

D. Content categorization

Correct Answer: *A*

Community vote distribution

A (100%)

Question #373 *Topic 1*

Which of the following should be used to aggregate log data in order to create alerts and detect anomalous activity?

A. SIEM

B. WAF

C. Network taps

D. IDS

Correct Answer: *A*

Community vote distribution

A (100%)

Question #374 *Topic 1*

Which of the following provides the best protection against unwanted or insecure communications to and from a device?

A. System hardening

B. Host-based firewall Most Voted

C. Intrusion detection system

D. Anti-malware software

Correct Answer: *B*

Community vote distribution

B (100%)

Question #375 *Topic 1*

Which of the following is the primary purpose of a service that tracks log-ins and time spent using the service?

A. Availability

B. Accounting Most Voted

C. Authentication

D. Authorization

Correct Answer: *B*

Community vote distribution

B (100%)

Question #376 *Topic 1*

An employee who was working remotely lost a mobile device containing company data. Which of the following provides the best solution to prevent future data loss?

A. MDM Most Voted

B. DLP

C. FDE

D. EDR

Correct Answer: *A*

Community vote distribution

A (52%) C (48%)

Question #377 *Topic 1*

An IT administrator needs to ensure data retention standards are implemented on an enterprise application. Which of the following describes the administrator's role?

A. Processor

B. Custodian Most Voted

C. Privacy officer

D. Owner

Correct Answer: *B*

Community vote distribution

B (100%)

Question #378 Topic 1

A company plans to secure its systems by:

• Preventing users from sending sensitive data over corporate email
• Restricting access to potentially harmful websites

Which of the following features should the company set up? (Choose two.)

A. DLP software Most Voted
B. DNS filtering Most Voted
C. File integrity monitoring
D. Stateful firewall
E. Guardrails
F. Antivirus signatures

Correct Answer: *AB*

Community vote distribution

AB (100%)

Question #379 Topic 1

A company processes and stores sensitive data on its own systems. Which of the following steps should the company take first to ensure compliance with privacy regulations?

A. Implement access controls and encryption. Most Voted
B. Develop and provide training on data protection policies.
C. Create incident response and disaster recovery plans.
D. Purchase and install security software.

Correct Answer: *A*

Community vote distribution

A (67%) B (33%)

Question #380 Topic 1

Which of the following cryptographic methods is preferred for securing communications with limited computing resources?

A. Hashing algorithm
B. Public key infrastructure
C. Symmetric encryption Most Voted
D. Elliptic curve cryptography

Correct Answer: *C*

Community vote distribution

C (63%) D (38%)

Question #381 *Topic 1*

A network administrator wants to ensure that network traffic is highly secure while in transit.

Which of the following actions best describes the actions the network administrator should take?

A. Ensure that NAC is enforced on all network segments, and confirm that firewalls have updated policies to block unauthorized traffic.

B. Ensure only TLS and other encrypted protocols are selected for use on the network, and only permit authorized traffic via secure protocols. Most Voted

C. Configure the perimeter IPS to block inbound HTTPS directory traversal traffic, and verify that signatures are updated on a daily basis.

D. Ensure the EDR software monitors for unauthorized applications that could be used by threat actors, and configure alerts for the security team.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #382 *Topic 1*

Which of the following definitions best describes the concept of log correlation?

A. Combining relevant logs from multiple sources into one location

B. Searching and processing data to identify patterns of malicious activity Most Voted

C. Making a record of the events that occur in the system

D. Analyzing the log files of the system components

Correct Answer: *B*

Community vote distribution

B (71%) A (29%)

Question #383 *Topic 1*

An enterprise security team is researching a new security architecture to better protect the company's networks and applications against the latest cyberthreats. The company has a fully remote workforce. The solution should be highly redundant and enable users to connect to a VPN with an integrated, software-based firewall. Which of the following solutions meets these requirements?

A. IPS

B. SIEM

C. SASE

D. CASB

Correct Answer: *C*

Community vote distribution

C (100%)

Question #384 *Topic 1*

Which of the following is the best way to validate the integrity and availability of a disaster recovery site?

A. Lead a simulated failover. Most Voted

B. Conduct a tabletop exercise.

C. Periodically test the generators.

D. Develop requirements for database encryption.

Correct Answer: *A*

Community vote distribution

A (83%) B (17%)

Question #385 *Topic 1*

Which of the following allows an exploit to go undetected by the operating system?

A. Firmware vulnerabilities

B. Side loading

C. Memory injection Most Voted

D. Encrypted payloads

Correct Answer: *C*

Community vote distribution

C (58%) A (38%) 4%

Question #386 *Topic 1*

A malicious insider from the marketing team alters records and transfers company funds to a personal account. Which of the following methods would be the best way to secure company records in the future?

A. Permission restrictions Most Voted

B. Hashing

C. Input validation

D. Access control list

Correct Answer: *A*

Community vote distribution

A (100%)

Question #387 *Topic 1*

An organization is required to provide assurance that its controls are properly designed and operating effectively. Which of the following reports will best achieve the objective?

A. Red teaming

B. Penetration testing

C. Independent audit Most Voted

D. Vulnerability assessment

Correct Answer: *C*

Community vote distribution

C (100%)

Question #388 *Topic 1*

A systems administrator successfully configures VPN access to a cloud environment. Which of the following capabilities should the administrator use to best facilitate remote administration?

A. A jump host in the shared services security zone Most Voted

B. An SSH server within the corporate LAN

C. A reverse proxy on the firewall

D. An MDM solution with conditional access

Correct Answer: *A*

Community vote distribution

A (100%)

Question #389 *Topic 1*

Which of the following best describes the concept of information being stored outside of its country of origin while still being subject to the laws and requirements of the country of origin?

A. Data sovereignty Most Voted

B. Geolocation

C. Intellectual property

D. Geographic restrictions

Correct Answer: *A*

Community vote distribution

A (100%)

Question #390 *Topic 1*

An audit reveals that cardholder database logs are exposing account numbers inappropriately. Which of the following mechanisms would help limit the impact of this error?

A. Segmentation

B. Hashing

C. Journaling

D. Masking Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #391 *Topic 1*

A security analyst attempts to start a company's database server. When the server starts, the analyst receives an error message indicating the database server did not pass authentication. After reviewing and testing the system, the analyst receives confirmation that the server has been compromised and that attackers have redirected all outgoing database traffic to a server under their control. Which of the following MITRE ATT&CK techniques did the attacker most likely use to redirect database traffic?

A. Browser extension

B. Process injection

C. Valid accounts Most Voted

D. Escape to host

Correct Answer: *C*

Community vote distribution

C (37%) D (34%) B (29%)

Question #392 *Topic 1*

A penetration tester enters an office building at the same time as a group of employees despite not having an access badge. Which of the following attack types is the penetration tester performing?

A. Tailgating Most Voted

B. Shoulder surfing

C. RFID cloning

D. Forgery

Correct Answer: *A*

Community vote distribution

A (100%)

Question #393 *Topic 1*

Which of the following enables the ability to receive a consolidated report from different devices on the network?

A. IPS

B. DLP

C. SIEM Most Voted

D. Firewall

Correct Answer: *C*

Community vote distribution

C (100%)

Question #394 *Topic 1*

Which of the following should an organization focus on the most when making decisions about vulnerability prioritization?

A. Exposure factor

B. CVSS Most Voted

C. CVE

D. Industry impact

Correct Answer: *B*

Community vote distribution

B (64%) A (36%)

Question #395 *Topic 1*

An organization needs to monitor its users' activities in order to prevent insider threats. Which of the following solutions would help the organization achieve this goal?

A. Behavioral analytics Most Voted

B. Access control lists

C. Identity and access management

D. Network intrusion detection system

Correct Answer: *A*

Community vote distribution

A (100%)

Question #396 *Topic 1*

A customer of a large company receives a phone call from someone claiming to work for the company and asking for the customer's credit card information. The customer sees the caller ID is the same as the company's main phone number. Which of the following attacks is the customer most likely a target of?

A. Phishing

B. Whaling

C. Smishing

D. Vishing Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #397 *Topic 1*

A security analyst is reviewing logs to identify the destination of command-and-control traffic originating from a compromised device within the on-premises network. Which of the following is the best log to review?

A. IDS

B. Antivirus

C. Firewall Most Voted

D. Application

Correct Answer: *C*

Community vote distribution

C (100%)

Question #398 *Topic 1*

When trying to access an internal website, an employee reports that a prompt displays, stating that the site is insecure. Which of the following certificate types is the site most likely using?

A. Wildcard

B. Root of trust

C. Third-party

D. Self-signed

Correct Answer: *D*

Community vote distribution

D (100%)

Question #399 *Topic 1*

Which of the following would most likely be deployed to obtain and analyze attacker activity and techniques?

A. Firewall

B. IDS

C. Honeypot

D. Layer 3 switch

Correct Answer: *C*

Community vote distribution

C (100%)

Question #400 *Topic 1*

Which of the following objectives is best achieved by a tabletop exercise?

A. Familiarizing participants with the incident response process

B. Deciding red and blue team rules of engagement

C. Quickly determining the impact of an actual security breach

D. Conducting multiple security investigations in parallel

Correct Answer: *A*

Community vote distribution

A (100%)

Question #401 *Topic 1*

The private key for a website was stolen, and a new certificate has been issued. Which of the following needs to be updated next?

A. SCEP

B. CRL Most Voted

C. OCSP

D. CSR

Correct Answer: *B*

Community vote distribution

B (92%) 8%

Question #402 *Topic 1*

Which of the following organizational documents is most often used to establish and communicate expectations associated with integrity and ethical behavior within an organization?

A. AUP Most Voted

B. SLA

C. EULA

D. MOA

Correct Answer: *A*

Community vote distribution

A (100%)

Question #403 *Topic 1*

Which of the following explains how to determine the global regulations that data is subject to regardless of the country where the data is stored?

A. Geographic dispersion

B. Data sovereignty

C. Geographic restrictions

D. Data segmentation

Correct Answer: *B*

Community vote distribution

B (100%)

Question #404 *Topic 1*

An organization's web servers host an online ordering system. The organization discovers that the servers are vulnerable to a malicious JavaScript injection, which could allow attackers to access customer payment information. Which of the following mitigation strategies would be most effective for preventing an attack on the organization's web servers? (Choose two.)

A. Regularly updating server software and patches Most Voted

B. Implementing strong password policies

C. Encrypting sensitive data at rest and in transit

D. Utilizing a web-application firewall Most Voted

E. Performing regular vulnerability scans

F. Removing payment information from the servers

Correct Answer: *AD*

Community vote distribution

AD (89%) 11%

Question #405 *Topic 1*

Which of the following tools is best for logging and monitoring in a cloud environment?

A. IPS

B. FIM

C. NAC

D. SIEM

Correct Answer: *D*

Community vote distribution

D (100%)

Question #406 *Topic 1*

During a SQL update of a database, a temporary field that was created was replaced by an attacker in order to allow access to the system. Which of the following best describes this type of vulnerability?

A. Race condition

B. Memory injection

C. Malicious update Most Voted

D. Side loading

Correct Answer: *C*

Community vote distribution

C (58%) A (42%)

Question #407 *Topic 1*

A group of developers has a shared backup account to access the source code repository. Which of the following is best way to secure the backup account if there is an SSO failure?

A. RAS

B. EAP

C. SAML

D. PAM Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #408 *Topic 1*

Which of the following elements of digital forensics should a company use if it needs to ensure the integrity of evidence?

A. Preservation Most Voted

B. E-discovery

C. Acquisition

D. Containment

Correct Answer: *A*

Community vote distribution

A (100%)

Question #409 *Topic 1*

A company suffered a critical incident where 30GB of data was exfiltrated from the corporate network. Which of the following actions is the most efficient way to identify where the system data was exfiltrated from and what location the attacker sent the data to?

A. Analyze firewall and network logs for large amounts of outbound traffic to external IP addresses or domains. Most Voted

B. Analyze IPS and IDS logs to find the IP addresses used by the attacker for reconnaissance scans.

C. Analyze endpoint and application logs to see whether file-sharing programs were running on the company systems.

D. Analyze external vulnerability scans and automated reports to identify the systems the attacker could have exploited a remote code vulnerability.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #410 *Topic 1*

Which of the following describes the procedures a penetration tester must follow while conducting a test?

A. Rules of engagement

B. Rules of acceptance

C. Rules of understanding

D. Rules of execution

Correct Answer: *A*

Community vote distribution

A (100%)

Question #411 *Topic 1*

A security analyst wants to better understand the behavior of users and devices in order to gain visibility into potential malicious activities. The analyst needs a control to detect when actions deviate from a common baseline. Which of the following should the analyst use?

A. Intrusion prevention system

B. Sandbox

C. Endpoint detection and response Most Voted

D. Antivirus

Correct Answer: *C*

Community vote distribution

C (100%)

Question #412 *Topic 1*

A legal department must maintain a backup from all devices that have been shredded and recycled by a third party. Which of the following best describes this requirement?

A. Data retention Most Voted

B. Certification

C. Sanitization

D. Destruction

Correct Answer: *A*

Community vote distribution

A (71%) B (29%)

Question #413 *Topic 1*

Which of the following can be used to compromise a system that is running an RTOS?

A. Cross-site scripting

B. Memory injection Most Voted

C. Replay attack

D. Ransomware

Correct Answer: *B*

Community vote distribution

B (100%)

Question #414 *Topic 1*

Which of the following threat actors would most likely deface the website of a high-profile music group?

A. Unskilled attacker Most Voted

B. Organized crime

C. Nation-state

D. Insider threat

Correct Answer: *A*

Community vote distribution

A (90%) 10%

Question #415 *Topic 1*

A security architect wants to prevent employees from receiving malicious attachments by email. Which of the following functions should the chosen solution do?

A. Apply IP address reputation data.

B. Tap and monitor the email feed.

C. Scan email traffic inline. Most Voted

D. Check SPF records.

Correct Answer: *C*

Community vote distribution

C (69%) D (31%)

Question #416 *Topic 1*

Which of the following activities is the first stage in the incident response process?

A. Detection Most Voted

B. Declaration

C. Containment

D. Verification

Correct Answer: *A*

Community vote distribution

A (100%)

Question #417 *Topic 1*

Which of the following is the main consideration when a legacy system that is a critical part of a company's infrastructure cannot be replaced?

A. Resource provisioning

B. Cost

C. Single point of failure Most Voted

D. Complexity

Correct Answer: *C*

Community vote distribution

C (100%)

Question #418 *Topic 1*

Which of the following is a compensating control for providing user access to a high-risk website?

A. Enabling threat prevention features on the firewall Most Voted

B. Configuring a SIEM tool to capture all web traffic

C. Setting firewall rules to allow traffic from any port to that destination

D. Blocking that website on the endpoint protection software

Correct Answer: *A*

Community vote distribution

A (88%) 13%

Question #419 *Topic 1*

An organization is implementing a COPE mobile device management policy. Which of the following should the organization include in the COPE policy? (Choose two.)

A. Remote wiping of the device

B. Data encryption

C. Requiring passwords with eight characters

D. Data usage caps

E. Employee data ownership

F. Personal application store access

Correct Answer: *AB*

Community vote distribution

AB (100%)

Question #420 *Topic 1*

A security administrator observed the following in a web server log while investigating an incident:

"GET ../../../../etc/passwd"

Which of the following attacks did the security administrator most likely see?

A. Privilege escalation

B. Credential replay

C. Brute force

D. Directory traversal Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #421 *Topic 1*

An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device. Which of the following best describes this kind of penetration test?

A. Partially known environment

B. Unknown environment

C. Integrated

D. Known environment

Correct Answer: *A*

Community vote distribution

A (100%)

Question #422 *Topic 1*

Which of the following should a security team do first before a new web server goes live?

A. Harden the virtual host. Most Voted

B. Create WAF rules.

C. Enable network intrusion detection.

D. Apply patch management.

Correct Answer: *A*

Community vote distribution

A (57%) D (43%)

Question #423 *Topic 1*

Which of the following techniques can be used to sanitize the data contained on a hard drive while allowing for the hard drive to be repurposed?

A. Degaussing

B. Drive shredder

C. Retention platform

D. Wipe tool Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #424 *Topic 1*

An attacker submits a request containing unexpected characters in an attempt to gain unauthorized access to information within the underlying systems. Which of the following best describes this attack?

A. Side loading

B. Target of evaluation

C. Resource reuse

D. SQL injection Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #425 *Topic 1*

A security analyst has determined that a security breach would have a financial impact of $15,000 and is expected to occur twice within a three-year period. Which of the following is the ALE for this risk?

A. $7,500

B. $10,000 Most Voted

C. $15,000

D. $30,000

Correct Answer: *B*

Community vote distribution

B (100%)

Question #426 *Topic 1*

A systems administrator discovers a system that is no longer receiving support from the vendor. However, this system and its environment are critical to running the business, cannot be modified, and must stay online. Which of the following risk treatments is the most appropriate in this situation?

A. Reject

B. Accept Most Voted

C. Transfer

D. Avoid

Correct Answer: *B*

Community vote distribution

B (70%) C (30%)

Question #427 *Topic 1*

A company discovered its data was advertised for sale on the dark web. During the initial investigation, the company determined the data was proprietary data. Which of the following is the next step the company should take?

A. Identify the attacker's entry methods.

B. Report the breach to the local authorities.

C. Notify the applicable parties of the breach. Most Voted

D. Implement vulnerability scanning of the company's systems.

Correct Answer: *C*

Community vote distribution

C (64%) B (32%) 5%

Question #428 *Topic 1*

Which of the following would be the best solution to deploy a low-cost standby site that includes hardware and internet access?

A. Recovery site

B. Cold site

C. Hot site

D. Warm site Most Voted

Correct Answer: *D*

Community vote distribution

D (53%) B (44%)

Question #429 *Topic 1*

An organization needs to determine how many employees are accessing the building each day in order to configure the proper access controls. Which of the following control types best meets this requirement?

A. Detective Most Voted

B. Preventive

C. Corrective

D. Directive

Correct Answer: *A*

Community vote distribution

A (83%) B (17%)

Question #430 *Topic 1*

An organization wants to implement a secure solution for remote users. The users handle sensitive PHI on a regular basis and need to access an internally developed corporate application. Which of the following best meet the organization's security requirements? (Choose two.)

A. Local administrative password

B. Perimeter network

C. Jump server

D. WAF

E. MFA Most Voted

F. VPN Most Voted

Correct Answer: *EF*

Community vote distribution

EF (40%) CF (33%) CE (27%)

Question #431 *Topic 1*

A security officer is implementing a security awareness program and is placing security-themed posters around the building and is assigning online user training. Which of the following would the security officer most likely implement?

A. Password policy

B. Access badges

C. Phishing campaign Most Voted

D. Risk assessment

Correct Answer: *C*

Community vote distribution

C (100%)

Question #432 *Topic 1*

A security consultant is working with a client that wants to physically isolate its secure systems. Which of the following best describes this architecture?

A. SDN

B. Air gapped

C. Containerized

D. Highly available

Correct Answer: *B*

Community vote distribution

B (100%)

Question #433 *Topic 1*

A company is in the process of migrating to cloud-based services. The company's IT department has limited resources for migration and ongoing support. Which of the following best meets the company's needs?

A. IPS

B. WAF

C. SASE Most Voted

D. IAM

Correct Answer: *C*

Community vote distribution

C (100%)

Question #434 *Topic 1*

An employee clicks a malicious link in an email that appears to be from the company's Chief Executive Officer. The employee's computer is infected with ransomware that encrypts the company's files. Which of the following is the most effective way for the company to prevent similar incidents in the future?

A. Security awareness training

B. Database encryption

C. Segmentation

D. Reporting suspicious emails

Correct Answer: *A*

Community vote distribution

A (100%)

Question #435 *Topic 1*

Which of the following types of vulnerabilities is primarily caused by improper use and management of cryptographic certificates?

A. Misconfiguration

B. Resource reuse

C. Insecure key storage Most Voted

D. Weak cipher suites

Correct Answer: *C*

Community vote distribution

C (55%) A (41%) 5%

Question #436 *Topic 1*

Which of the following best describe the benefits of a microservices architecture when compared to a monolithic architecture? (Choose two.)

A. Easier debugging of the system

B. Reduced cost of ownership of the system

C. Improved scalability of the system Most Voted

D. Increased compartmentalization of the system Most Voted

E. Stronger authentication of the system

F. Reduced complexity of the system

Correct Answer: *CD*

Community vote distribution

CD (60%) AC (40%)

Question #437 *Topic 1*

A user's workstation becomes unresponsive and displays a ransom note demanding payment to decrypt files. Before the attack, the user opened a resume they received in a message, browsed the company's website, and installed OS updates. Which of the following is the most likely vector of this attack?

A. Spear-phishing attachment Most Voted

B. Watering hole

C. Infected website

D. Typosquatting

Correct Answer: *A*

Community vote distribution

A (83%) B (17%)

Question #438 *Topic 1*

A penetration tester finds an unused Ethernet port during an on-site penetration test. Upon plugging a device into the unused port, the penetration tester notices that the machine is assigned an IP address, allowing the tester to enumerate the local network. Which of the following should an administrator implement in order to prevent this situation from happening in the future?

A. Port security Most Voted

B. Transport Layer Security

C. Proxy server

D. Security zones

Correct Answer: *A*

Community vote distribution

A (100%)

Question #439 *Topic 1*

Which of the following should be used to ensure an attacker is unable to read the contents of a mobile device's drive if the device is lost?

A. TPM

B. ECC

C. FDE

D. HSM

Correct Answer: *C*

Question #440 *Topic 1*

A security administrator documented the following records during an assessment of network services:

Record	Type	Address	TTL
@	A	192.168.1.1	14400
WWW	CNAME	192.168.1.1	14400

Two weeks later, the administrator performed a log review and noticed the records were changed as follows:

Record	Type	Address	TTL
@	A	233.123.123.23	14400
WWW	CNAME	233.123.123.23	14400

When consulting the service owner, the administrator validated that the new address was not part of the company network. Which of the following was the company most likely experiencing?

A. DDoS attack

B. DNS poisoning Most Voted

C. Ransomware compromise

D. Spyware infection

Correct Answer: *B*

Community vote distribution

B (71%) A (29%)

Question #441 *Topic 1*

Which of the following is the primary reason why false negatives on a vulnerability scan should be a concern?

A. The system has vulnerabilities that are not being detected. Most Voted

B. The time to remediate vulnerabilities that do not exist is excessive.

C. Vulnerabilities with a lower severity will be prioritized over critical vulnerabilities.

D. The system has vulnerabilities, and a patch has not yet been released.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #442 *Topic 1*

A company is concerned about theft of client data from decommissioned laptops. Which of the following is the most cost-effective method to decrease this risk?

A. Wiping Most Voted

B. Recycling

C. Shredding

D. Deletion

Correct Answer: *A*

Community vote distribution

A (80%) C (20%)

Question #443 *Topic 1*

A company that has a large IT operation is looking to better control, standardize, and lower the time required to build new servers. Which of the following architectures will best achieve the company's objectives?

A. IoT

B. IaC Most Voted

C. IaaS

D. ICS

Correct Answer: *B*

Community vote distribution

B (100%)

Question #444 *Topic 1*

A government official receives a blank envelope containing photos and a note instructing the official to wire a large sum of money by midnight to prevent the photos from being leaked on the internet. Which of the following best describes the threat actor's intent?

A. Organized crime

B. Philosophical beliefs

C. Espionage

D. Blackmail

Correct Answer: *D*

Community vote distribution

D (100%)

Question #445 *Topic 1*

Which of the following is the best security reason for closing service ports that are not needed?

A. To mitigate risks associated with unencrypted traffic

B. To eliminate false positives from a vulnerability scan

C. To reduce a system's attack surface Most Voted

D. To improve a system's resource utilization

Correct Answer: *C*

Community vote distribution

C (100%)

Question #446 *Topic 1*

Which of the following would a security administrator use to comply with a secure baseline during a patch update?

A. Information security policy

B. Service-level expectations

C. Standard operating procedure Most Voted

D. Test result report

Correct Answer: *C*

Community vote distribution

C (100%)

Question #447 *Topic 1*

A malicious actor conducted a brute-force attack on a company's web servers and eventually gained access to the company's customer information database. Which of the following is the most effective way to prevent similar attacks?

A. Regular patching of servers

B. Web application firewalls

C. Multifactor authentication Most Voted

D. Enabling encryption of customer data

Correct Answer: *C*

Community vote distribution

C (87%) 13%

Question #448 *Topic 1*

Which of the following options will provide the lowest RTO and RPO for a database?

A. Snapshots

B. On-site backups

C. Journaling

D. Hot site Most Voted

Correct Answer: *D*

Community vote distribution

D (57%) C (43%)

Question #449 *Topic 1*

Which of the following is a possible consequence of a VM escape?

A. Malicious instructions can be inserted into memory and give the attacker elevated permissions.

B. An attacker can access the hypervisor and compromise other VMs. Most Voted

C. Unencrypted data can be read by a user who is in a separate environment.

D. Users can install software that is not on the manufacturer's approved list.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #450 *Topic 1*

A security team at a large, global company needs to reduce the cost of storing data used for performing investigations. Which of the following types of data should have its retention length reduced?

A. Packet capture Most Voted

B. Endpoint logs

C. OS security logs

D. Vulnerability scan

Correct Answer: *A*

Community vote distribution

A (88%) 13%

Question #451 *Topic 1*

Which of the following is a type of vulnerability that involves inserting scripts into web-based applications in order to take control of the client's web browser?

A. SQL injection

B. Cross-site scripting Most Voted

C. Zero-day exploit

D. On-path attack

Correct Answer: *B*

Community vote distribution

B (100%)

Question #452 *Topic 1*

While investigating a possible incident, a security analyst discovers the following:

```
67.118.34.157 - - [28/Jul/2022:10:26:59 -0300] "GET /query.php?q=wireless%20headphones / HTTP/1.0" 200 12737
132.18.222.103 - - [28/Jul/2022:10:27:10 -0300] "GET /query.php?q=123'';INSERT INTO users VALUES('temp','pass123')# /
HTTP/1.0" 200 935
12.45.101.121 - - [28/Jul/2022:10:27:22 -0300] "GET /query.php?q=mp3%20players / HTTP/1.0" 200 14650
```

Which of the following should the analyst do first?

A. Implement a WAF.

B. Disable the query.php script.

C. Block brute-force attempts on temporary users.

D. Check the users table for new accounts. Most Voted

Correct Answer: *D*

Community vote distribution

D (75%) B (25%)

Question #453 *Topic 1*

Due to a cyberattack, a company's IT systems were not operational for an extended period of time. The company wants to measure how quickly the systems must be restored in order to minimize business disruption. Which of the following would the company most likely use?

A. Recovery point objective

B. Risk appetite

C. Risk tolerance

D. Recovery time objective Most Voted

E. Mean time between failure

Correct Answer: *D*

Community vote distribution

D (100%)

Question #454 *Topic 1*

Which of the following actors attacking an organization is the most likely to be motivated by personal beliefs?

A. Nation-state

B. Organized crime

C. Hacktivist

D. Insider threat

Correct Answer: *C*

Community vote distribution

C (100%)

Question #455 *Topic 1*

Which of the following should a security team use to document persistent vulnerabilities with related recommendations?

A. Audit report

B. Risk register Most Voted

C. Compliance report

D. Penetration test

Correct Answer: *B*

Community vote distribution

B (100%)

Question #456 *Topic 1*

An organization purchased a critical business application containing sensitive data. The organization would like to ensure that the application is not exploited by common data exfiltration attacks. Which of the following approaches would best help to fulfill this requirement?

A. URL scanning

B. WAF Most Voted

C. Reverse proxy

D. NAC

Correct Answer: *B*

Community vote distribution

B (81%) D (19%)

Question #457 *Topic 1*

A company wants to improve the availability of its application with a solution that requires minimal effort in the event a server needs to be replaced or added. Which of the following would be the best solution to meet these objectives?

A. Load balancing Most Voted

B. Fault tolerance

C. Proxy servers

D. Replication

Correct Answer: *A*

Community vote distribution

A (67%) D (33%)

Question #458 *Topic 1*

A company is performing a risk assessment on new software the company plans to use. Which of the following should the company assess during this process?

A. Software vulnerabilities Most Voted

B. Cost-benefit analysis

C. Ongoing monitoring strategies

D. Network infrastructure compatibility

Correct Answer: *A*

Community vote distribution

A (100%)

Question #459 *Topic 1*

A malicious actor is trying to access sensitive financial information from a company's database by intercepting and reusing log-in credentials. Which of the following attacks is the malicious actor attempting?

A. SQL injection

B. On-path Most Voted

C. Brute-force

D. Password spraying

Correct Answer: *B*

Community vote distribution

B (88%) 13%

Question #460 *Topic 1*

A new employee accessed an unauthorized website. An investigation found that the employee violated the company's rules. Which of the following did the employee violate?

A. MOU

B. AUP Most Voted

C. NDA

D. MOA

Correct Answer: *B*

Community vote distribution

B (100%)

Question #461 *Topic 1*

A systems administrator is reviewing the VPN logs and notices that during non-working hours a user is accessing the company file server and information is being transferred to a suspicious IP address. Which of the following threats is most likely occurring?

A. Typosquatting

B. Root or trust

C. Data exfiltration Most Voted

D. Blackmail

Correct Answer: *C*

Community vote distribution

C (100%)

Question #462 *Topic 1*

HOTSPOT

-

A security architect is tasked with designing a highly resilient, business-critical application. The application SLA is 99.999%.

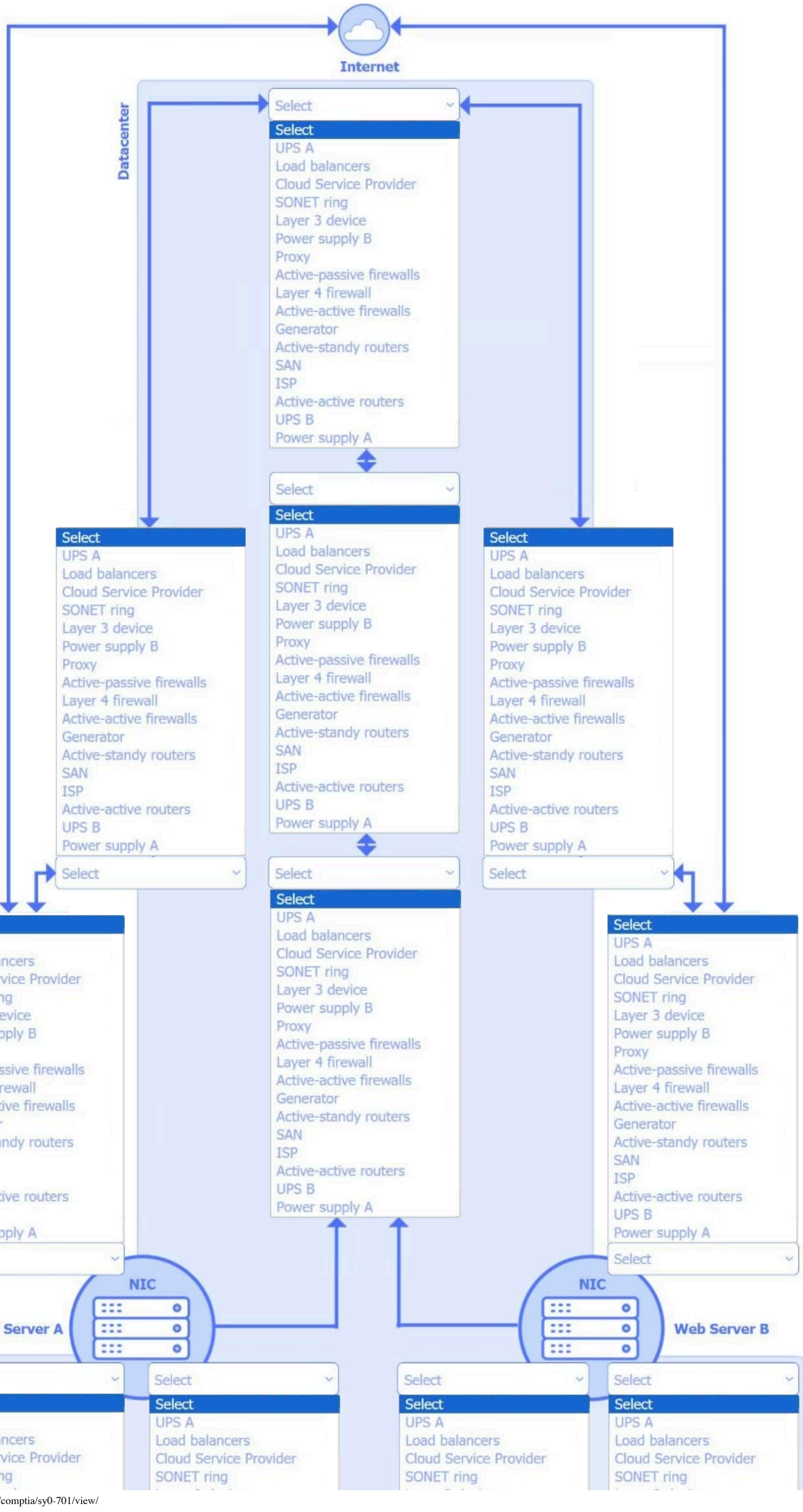
INSTRUCTIONS

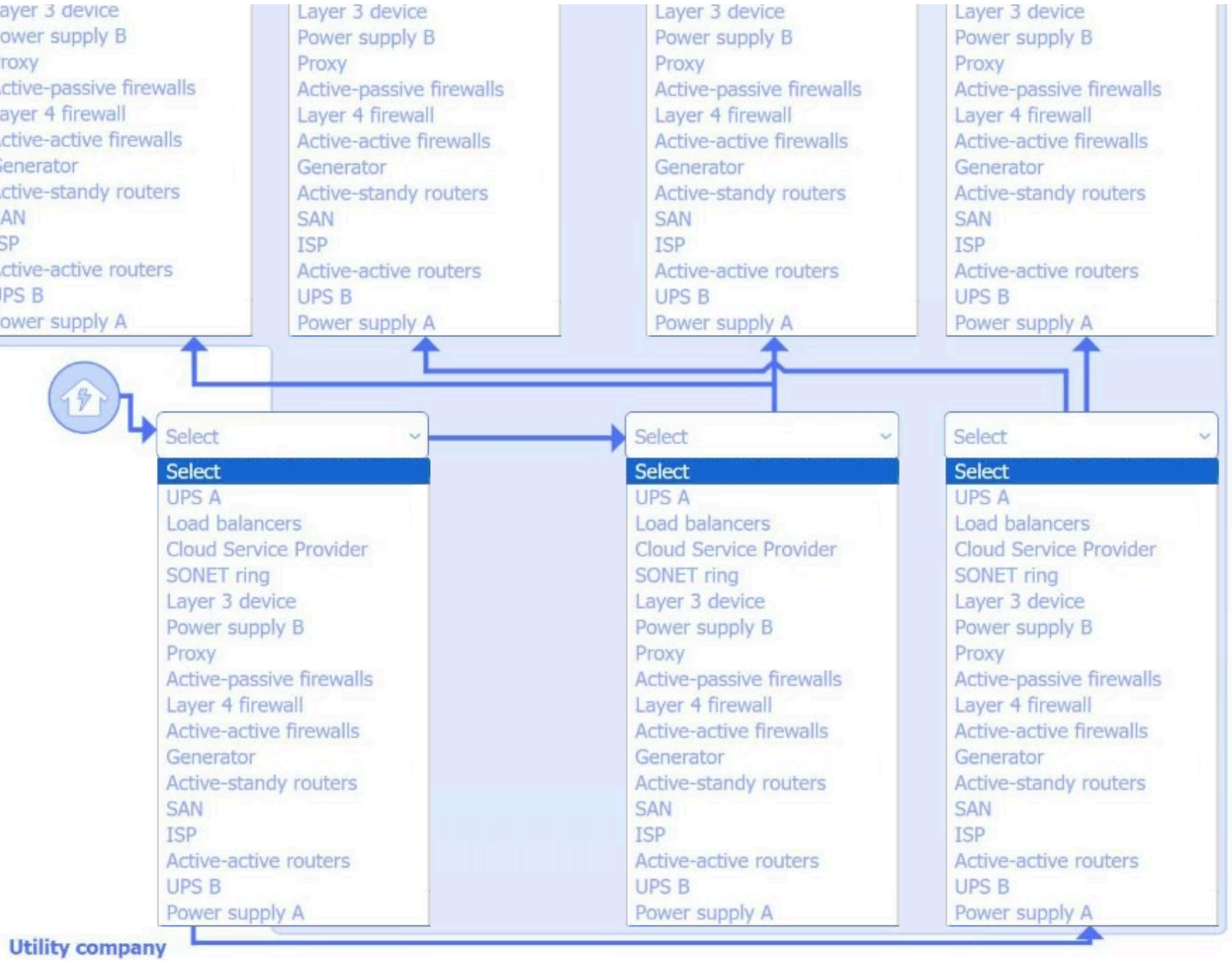
-

Select the network, power, and server components for the appropriate locations to achieve application resiliency.

A component should be selected for each location, and components may be selected more than once.

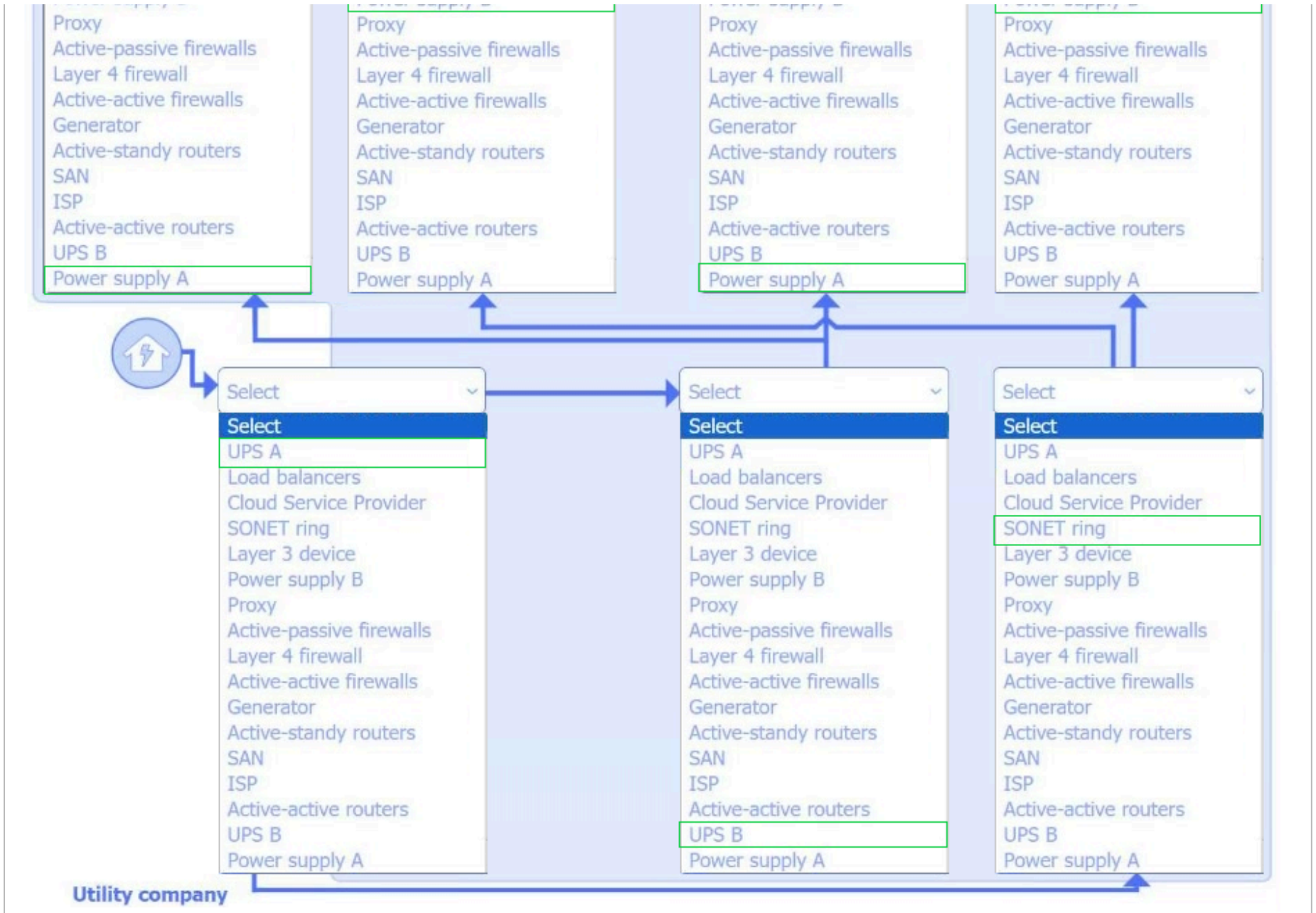
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Internet
Datacenter
Select
UPS A
Load balancers
Cloud Service Provider
SONET ring
Layer 3 device
Power supply B
Proxy
Active-passive firewalls
Layer 4 firewall
Active-active firewalls
Generator
Active-standy routers
SAN
ISP
Active-active routers
UPS B
Power supply A
NIC
Web Server A
Web Server B



Correct Answer:


Internet
Datacenter
Select
UPS A
Load balancers
Cloud Service Provider
SONET ring
Layer 3 device
Power supply B
Proxy
Active-passive firewalls
Layer 4 firewall
Active-active firewalls
Generator
Active-standy routers
SAN
ISP
Active-active routers
UPS B
Power supply A
NIC
Web Server A
Web Server B



Question #463 *Topic 1*

A company discovers suspicious transactions that were entered into the company's database and attached to a user account that was created as a trap for malicious activity. Which of the following is the user account an example of?

A. Honeytoken Most Voted

B. Honeynet

C. Honeypot

D. Honeyfile

Correct Answer: *A*

Community vote distribution

A (100%)

Question #464 *Topic 1*

A network engineer is increasing the overall security of network devices and needs to harden the devices. Which of the following will best accomplish this task?

A. Configuring centralized logging

B. Generating local administrator accounts

C. Replacing Telnet with SSH Most Voted

D. Enabling HTTP administration

Correct Answer: *C*

Community vote distribution

C (100%)

Question #465 *Topic 1*

A company's accounting department receives an urgent payment message from the company's bank domain with instructions to wire transfer funds. The sender requests that the transfer be completed as soon as possible. Which of the following attacks is described?

A. Business email compromise Most Voted

B. Vishing

C. Spear phishing

D. Impersonation

Correct Answer: *A*

Community vote distribution

A (89%) 11%

Question #466 *Topic 1*

A company filed a complaint with its IT service provider after the company discovered the service provider's external audit team had access to some of the company's confidential information. Which of the following is the most likely reason the company filed the complaint?

A. The MOU had basic clauses from a template.

B. A SOW had not been agreed to by the client.

C. A WO had not been mutually approved.

D. A required NDA had not been signed.

Correct Answer: *D*

Community vote distribution

D (100%)

Question #467 *Topic 1*

Which of the following aspects of the data management life cycle is most directly impacted by local and international regulations?

A. Destruction

B. Certification

C. Retention Most Voted

D. Sanitization

Correct Answer: *C*

Community vote distribution

C (100%)

Question #468 *Topic 1*

An analyst is reviewing job postings to ensure sensitive company information is not being shared with the general public. Which of the following is the analyst most likely looking for?

A. Office addresses

B. Software versions Most Voted

C. List of board members

D. Government identification numbers

Correct Answer: *B*

Community vote distribution

B (64%) D (36%)

Question #469 *Topic 1*

An engineer has ensured that the switches are using the latest OS, the servers have the latest patches, and the endpoints' definitions are up to date. Which of the following will these actions most effectively prevent?

A. Zero-day attacks

B. Insider threats

C. End-of-life support

D. Known exploits Most Voted

Correct Answer: *D*

Community vote distribution

D (91%) 9%

Question #470 *Topic 1*

Which of the following is most likely a security concern when installing and using low-cost IoT devices in infrastructure environments?

A. Country of origin

B. Device responsiveness

C. Ease of deployment

D. Storage of data Most Voted

Correct Answer: *D*

Community vote distribution

D (70%) A (30%)

Question #471 *Topic 1*

A company captures log-in details and reviews them each week to identify conditions such as excessive log-in attempts and frequent lockouts. Which of the following should a security analyst recommend to improve security compliance monitoring?

A. Including the date and person who reviewed the information in a report

B. Adding automated alerting when anomalies occur

C. Requiring a statement each week that no exceptions were noted

D. Masking the username in a report to protect privacy

Correct Answer: *B*

Community vote distribution

B (100%)

Question #472 *Topic 1*

A security team is in the process of hardening the network against externally crafted malicious packets. Which of the following is the most secure method to protect the internal network?

A. Anti-malware solutions

B. Host-based firewalls

C. Intrusion prevention systems Most Voted

D. Network access control

E. Network allow list

Correct Answer: *C*

Community vote distribution

C (75%) E (25%)

Question #473 *Topic 1*

Which of the following is the best way to prevent an unauthorized user from plugging a laptop into an employee's phone network port and then using tools to scan for database servers?

A. MAC filtering Most Voted

B. Segmentation

C. Certification

D. Isolation

Correct Answer: *A*

Community vote distribution

A (50%) C (31%) B (19%)

Question #474 *Topic 1*

Which of the following should a systems administrator use to decrease the company's hardware attack surface?

A. Replication

B. Isolation

C. Centralization

D. Virtualization Most Voted

Correct Answer: *D*

Community vote distribution

D (64%) B (36%)

Question #475 *Topic 1*

A company wants to add an MFA solution for all employees who access the corporate network remotely. Log-in requirements include something you know, are, and have. The company wants a solution that does not require purchasing third-party applications or specialized hardware. Which of the following MFA solutions would best meet the company's requirements?

A. Smart card with PIN and password

B. Security questions and a one-time passcode sent via email

C. Voice and fingerprint verification with an SMS one-time passcode

D. Mobile application-generated, one-time passcode with facial recognition Most Voted

Correct Answer: *D*

Community vote distribution

D (59%) C (37%) 4%

Question #476 *Topic 1*

A company is using a legacy FTP server to transfer financial data to a third party. The legacy system does not support SFTP, so a compensating control is needed to protect the sensitive, financial data in transit. Which of the following would be the most appropriate for the company to use?

A. Telnet connection

B. SSH tunneling

C. Patch installation

D. Full disk encryption

Correct Answer: *B*

Community vote distribution

B (100%)

Question #477 *Topic 1*

A security manager wants to reduce the number of steps required to identify and contain basic threats. Which of the following will help achieve this goal?

A. SOAR

B. SIEM

C. DMARC

D. NIDS

Correct Answer: *A*

Community vote distribution

A (100%)

Question #478 *Topic 1*

The Chief Information Officer (CIO) asked a vendor to provide documentation detailing the specific objectives within the compliance framework that the vendor's services meet. The vendor provided a report and a signed letter stating that the services meet 17 of the 21 objectives. Which of the following did the vendor provide to the CIO?

A. Penetration test results

B. Self-assessment findings

C. Attestation of compliance

D. Third-party audit report

Correct Answer: *C*

Community vote distribution

C (100%)

Question #479 *Topic 1*

Which of the following describes the most effective way to address OS vulnerabilities after they are identified?

A. Endpoint protection

B. Removal of unnecessary software

C. Configuration enforcement

D. Patching

Correct Answer: *D*

Community vote distribution

D (100%)

Question #480 *Topic 1*

The management team reports that employees are missing features on company-provided tablets, which is causing productivity issues. The management team directs the IT team to resolve the issue within 48 hours. Which of the following would be the best solution for the IT team to leverage in this scenario?

A. EDR

B. COPE

C. MDM

D. FDE

Correct Answer: *C*

Community vote distribution

C (100%)

Question #481 *Topic 1*

A company is implementing a policy to allow employees to use their personal equipment for work. However, the company wants to ensure that only company-approved applications can be installed. Which of the following addresses this concern?

A. MDM Most Voted

B. Containerization

C. DLP

D. FIM

Correct Answer: *A*

Community vote distribution

A (55%) B (45%)

Question #482 *Topic 1*

An alert references attacks associated with a zero-day exploit. An analyst places a bastion host in the network to reduce the risk of the exploit. Which of the following types of controls is the analyst implementing?

A. Compensating

B. Detective

C. Operational

D. Physical

Correct Answer: *A*

Community vote distribution

A (100%)

Question #483 *Topic 1*

A penetration test has demonstrated that domain administrator accounts were vulnerable to pass-the-hash attacks. Which of the following would have been the best strategy to prevent the threat actor from using domain administrator accounts?

A. Audit each domain administrator account weekly for password compliance.

B. Implement a privileged access management solution.

C. Create IDS policies to monitor domain controller access.

D. Use Group Policy to enforce password expiration.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #484 *Topic 1*

Which of the following is an example of memory injection?

A. Two processes access the same variable, allowing one to cause a privilege escalation.

B. A process receives an unexpected amount of data, which causes malicious code to be executed.

C. Malicious code is copied to the allocated space of an already running process.

D. An executable is overwritten on the disk, and malicious code runs the next time it is executed.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #485 *Topic 1*

A security administrator is implementing encryption on all hard drives in an organization. Which of the following security concepts is the administrator applying?

A. Integrity

B. Authentication

C. Zero Trust

D. Confidentiality Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #486 *Topic 1*

An administrator has configured a quarantine subnet for all guest devices that connect to the network. Which of the following would be best for the security team to perform before allowing access to corporate resources?

A. Device fingerprinting

B. Compliance attestation Most Voted

C. Penetration test

D. Application vulnerability test

Correct Answer: *B*

Community vote distribution

B (80%) A (20%)

Question #487 *Topic 1*

A customer has a contract with a CSP and wants to identify which controls should be implemented in the IaaS enclave. Which of the following is most likely to contain this information?

A. Statement of work

B. Responsibility matrix Most Voted

C. Service-level agreement

D. Master service agreement

Correct Answer: *B*

Community vote distribution

B (67%) C (33%)

Question #488 *Topic 1*

A Chief Information Security Officer is developing procedures to guide detective and corrective activities associated with common threats, including phishing, social engineering, and business email compromise. Which of the following documents would be most relevant to revise as part of this process?

A. SDLC

B. IRP

C. BCP

D. AUP

Correct Answer: *B*

Community vote distribution

B (100%)

Question #489 *Topic 1*

Which of the following testing techniques uses both defensive and offensive testing methodologies with developers to securely build key applications and software?

A. Blue

B. Yellow Most Voted

C. Red

D. Green

Correct Answer: *B*

Community vote distribution

B (86%) 14%

Question #490 *Topic 1*

An administrator wants to automate an account permissions update for a large number of accounts. Which of the following would best accomplish this task?

A. Security groups

B. Federation

C. User provisioning Most Voted

D. Vertical scaling

Correct Answer: *C*

Community vote distribution

C (100%)

Question #491 *Topic 1*

Which of the following is the fastest and most cost-effective way to confirm a third-party supplier's compliance with security obligations?

A. Attestation report

B. Third-party audit

C. Vulnerability assessment

D. Penetration testing

Correct Answer: *A*

Community vote distribution

A (100%)

Question #492 *Topic 1*

Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach that would affect offshore offices. Which of the following is this an example of?

A. Tabletop exercise

B. Penetration test

C. Geographic dispersion

D. Incident response

Correct Answer: *A*

Community vote distribution

A (100%)

Question #493 *Topic 1*

Which of the following is an example of a data protection strategy that uses tokenization?

A. Encrypting databases containing sensitive data

B. Replacing sensitive data with surrogate values

C. Removing sensitive data from production systems

D. Hashing sensitive data in critical systems

Correct Answer: *B*

Community vote distribution

B (100%)

Question #494 *Topic 1*

Which of the following is a type of vulnerability that refers to the unauthorized installation of applications on a device through means other than the official application store?

A. Cross-site scripting

B. Buffer overflow

C. Jailbreaking

D. Side loading Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #495 *Topic 1*

Which of the following types of identification methods can be performed on a deployed application during runtime?

A. Dynamic analysis Most Voted

B. Code review

C. Package monitoring

D. Bug bounty

Correct Answer: *A*

Community vote distribution

A (100%)

Question #496 *Topic 1*

Which of the following cryptographic solutions is used to hide the fact that communication is occurring?

A. Steganography

B. Data masking

C. Tokenization

D. Private key

Correct Answer: *A*

Community vote distribution

A (100%)

Question #497 *Topic 1*

Which of the following steps should be taken before mitigating a vulnerability in a production server?

A. Escalate the issue to the SDLC team.

B. Use the IR plan to evaluate the changes.

C. Perform a risk assessment to classify the vulnerability. Most Voted

D. Refer to the change management policy.

Correct Answer: *C*

Community vote distribution

C (56%) D (44%)

Question #498 *Topic 1*

A security engineer needs to quickly identify a signature from a known malicious file. Which of the following analysis methods would the security engineer most likely use?

A. Static

B. Sandbox

C. Network traffic

D. Package monitoring

Correct Answer: *A*

Community vote distribution

A (100%)

Question #499 *Topic 1*

Which of the following should a company use to provide proof of external network security testing?

A. Business impact analysis

B. Supply chain analysis

C. Vulnerability assessment

D. Third-party attestation

Correct Answer: *D*

Community vote distribution

D (100%)

Question #500 *Topic 1*

A security administrator is addressing an issue with a legacy system that communicates data using an unencrypted protocol to transfer sensitive data to a third party. No software updates that use an encrypted protocol are available, so a compensating control is needed. Which of the following are the most appropriate for the administrator to suggest? (Choose two.)

A. Tokenization

B. Cryptographic downgrade

C. SSH tunneling Most Voted

D. Segmentation Most Voted

E. Patch installation

F. Data masking

Correct Answer: *CD*

Community vote distribution

CD (83%) AD (17%)

Question #501 *Topic 1*

Which of the following steps in the risk management process involves establishing the scope and potential risks involved with a project?

A. Risk assessment

B. Risk identification Most Voted

C. Risk treatment

D. Risk monitoring and review

Correct Answer: *B*

Community vote distribution

B (83%) A (17%)

Question #502 *Topic 1*

A company's website is www.company.com. Attackers purchased the domain www.c0mpany.com. Which of the following types of attacks describes this example?

A. Typosquatting Most Voted

B. Brand impersonation

C. On-path

D. Watering-hole

Correct Answer: *A*

Community vote distribution

A (86%) 14%

Question #503 *Topic 1*

Which of the following allows a systems administrator to tune permissions for a file?

A. Patching

B. Access control list Most Voted

C. Configuration enforcement

D. Least privilege

Correct Answer: *B*

Community vote distribution

B (100%)

Question #504 *Topic 1*

Which of the following would be the greatest concern for a company that is aware of the consequences of non-compliance with government regulations?

A. Right to be forgotten

B. Sanctions

C. External compliance reporting

D. Attestation

Correct Answer: *B*

Community vote distribution

B (100%)

Question #505 *Topic 1*

Which of the following security concepts is accomplished when granting access after an individual has logged into a computer network?

A. Authorization Most Voted

B. Identification

C. Non-repudiation

D. Authentication

Correct Answer: *A*

Community vote distribution

A (86%) 14%

Question #506 *Topic 1*

A growing organization, which hosts an externally accessible application, adds multiple virtual servers to improve application performance and decrease the resource usage on individual servers. Which of the following solutions is the organization most likely to employ to further increase performance and availability?

A. Load balancer Most Voted

B. Jump server

C. Proxy server

D. SD-WAN

Correct Answer: *A*

Community vote distribution

A (100%)

Question #507 *Topic 1*

A systems administrator is concerned users are accessing emails through a duplicate site that is not run by the company. Which of the following is used in this scenario?

A. Impersonation Most Voted

B. Replication

C. Phishing

D. Smishing

Correct Answer: *A*

Community vote distribution

A (54%) C (46%)

Question #508 *Topic 1*

A security engineer at a large company needs to enhance IAM in order to ensure that employees can only access corporate systems during their shifts. Which of the following access controls should the security engineer implement?

A. Role-based

B. Time-of-day restrictions Most Voted

C. Least privilege

D. Biometric authentication

Correct Answer: *B*

Community vote distribution

B (100%)

Question #509 *Topic 1*

A company wants to ensure employees are allowed to copy files from a virtual desktop during the workday but are restricted during non-working hours. Which of the following security measures should the company set up?

A. Digital rights management

B. Role-based access control

C. Time-based access control

D. Network access control

Correct Answer: *C*

Community vote distribution

C (100%)

Question #510 *Topic 1*

Employees sign an agreement that restricts specific activities when leaving the company. Violating the agreement can result in legal consequences. Which of the following agreements does this best describe?

A. SLA

B. BPA

C. NDA

D. MOA

Correct Answer: *C*

Community vote distribution

C (100%)

Question #511 *Topic 1*

A systems administrator just purchased multiple network devices. Which of the following should the systems administrator perform to prevent attackers from accessing the devices by using publicly available information?

A. Install endpoint protection.

B. Disable ports/protocols.

C. Change default passwords.

D. Remove unnecessary software.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #512 *Topic 1*

A CVE in a key back-end component of an application has been disclosed. The systems administrator is identifying all of the systems in the environment that are susceptible to this risk. Which of the following should the systems administrator perform?

A. Packet capture

B. Vulnerability scan

C. Metadata analysis

D. Automated reporting

Correct Answer: *B*

Community vote distribution

B (100%)

Question #513 *Topic 1*

Which of the following activities uses OSINT?

A. Social engineering testing

B. Data analysis of logs

C. Collecting evidence of malicious activity

D. Producing IOC for malicious artifacts

Correct Answer: *A*

Community vote distribution

A (75%) C (25%)

Question #514 *Topic 1*

Which of the following are the best security controls for controlling on-premises access? (Choose two.)

A. Swipe card

B. Picture ID

C. Phone authentication application

D. Biometric scanner

E. Camera

F. Memorable question

Correct Answer: *AD*

Community vote distribution

AD (100%)

Question #515 *Topic 1*

A company is considering an expansion of access controls for an application that contractors and internal employees use to reduce costs. Which of the following risk elements should the implementation team understand before granting access to the application?

A. Threshold

B. Appetite

C. Avoidance

D. Register

Correct Answer: *B*

Community vote distribution

B (100%)

Question #516 *Topic 1*

Which of the following is the act of proving to a customer that software developers are trained on secure coding?

A. Assurance

B. Contract

C. Due diligence

D. Attestation Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #517 *Topic 1*

An administrator is creating a secure method for a contractor to access a test environment. Which of the following would provide the contractor with the best access to the test environment?

A. Application server

B. Jump server

C. RDP server

D. Proxy server

Correct Answer: *B*

Community vote distribution

B (100%)

Question #518 *Topic 1*

A security analyst notices unusual behavior on the network. The IDS on the network was not able to detect the activities. Which of the following should the security analyst use to help the IDS detect such attacks in the future?

A. Signatures

B. Trends

C. Honeypot

D. Reputation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #519 *Topic 1*

To which of the following security categories does an EDR solution belong?

A. Physical

B. Operational

C. Managerial

D. Technical

Correct Answer: *D*

Community vote distribution

D (100%)

Question #520 *Topic 1*

A company relies on open-source software libraries to build the software used by its customers. Which of the following vulnerability types would be the most difficult to remediate due to the company's reliance on open-source libraries?

A. Buffer overflow

B. SQL injection

C. Cross-site scripting

D. Zero-day

Correct Answer: *D*

Community vote distribution

D (100%)

Question #521 *Topic 1*

An organization has a new regulatory requirement to implement corrective controls on a financial system. Which of the following is the most likely reason for the new requirement?

A. To defend against insider threats altering banking details

B. To ensure that errors are not passed to other systems Most Voted

C. To allow for business insurance to be purchased

D. To prevent unauthorized changes to financial data

Correct Answer: *B*

Community vote distribution

B (75%) D (25%)

Question #522 *Topic 1*

Which of the following is the stage in an investigating when forensic images are obtained?

A. Acquisition

B. Preservation

C. Reporting

D. E-discovery

Correct Answer: *A*

Community vote distribution

A (100%)

Question #523 *Topic 1*

Which of the following describes the difference between encryption and hashing?

A. Encryption protects data in transit, while hashing protects data at rest.

B. Encryption replaces cleartext with ciphertext, while hashing calculates a checksum.

C. Encryption ensures data integrity, while hashing ensures data confidentiality.

D. Encryption uses a public-key exchange, while hashing uses a private key.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #524 *Topic 1*

A security report shows that during a two-week test period, 80% of employees unwittingly disclosed their SSO credentials when accessing an external website. The organization purposely created the website to simulate a cost-free password complexity test. Which of the following would best help reduce the number of visits to similar websites in the future?

A. Block all outbound traffic from the intranet.

B. Introduce a campaign to recognize phishing attempts. Most Voted

C. Restrict internet access for the employees who disclosed credentials.

D. Implement a deny list of websites.

Correct Answer: *B*

Community vote distribution

B (67%) D (33%)

Question #525 *Topic 1*

A Chief Information Security Officer (CISO) has developed information security policies that relate to the software development methodology. Which of the following would the CISO most likely include in the organization's documentation?

A. Peer review requirements

B. Multifactor authentication

C. Branch protection tests

D. Secrets management configurations

Correct Answer: *A*

Community vote distribution

A (100%)

Question #526 *Topic 1*

An organization is developing a security program that conveys the responsibilities associated with the general operation of systems and software within the organization. Which of the following documents would most likely communicate these expectations?

A. Business continuity plan

B. Change management procedure

C. Acceptable use policy

D. Software development life cycle policy

Correct Answer: *C*

Community vote distribution

C (100%)

Question #527 *Topic 1*

A security analyst created a fake account and saved the password in a non-readily accessible directory in a spreadsheet. An alert was also configured to notify the security team if the spreadsheet is opened. Which of the following best describes the deception method being deployed?

A. Honeypot

B. Honeyfile

C. Honeytoken Most Voted

D. Honeynet

Correct Answer: *C*

Community vote distribution

C (56%) B (44%)

Question #528 *Topic 1*

Which of the following is the best way to provide secure, remote access for employees while minimizing the exposure of a company's internal network?

A. VPN

B. LDAP

C. FTP

D. RADIUS

Correct Answer: *A*

Community vote distribution

A (100%)

Question #529 *Topic 1*

A company wants to track modifications to the code that is used to build new virtual servers. Which of the following will the company most likely deploy?

A. Change management ticketing system

B. Behavioral analyzer

C. Collaboration platform

D. Version control tool Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #530 *Topic 1*

Which of the following documents details how to accomplish a technical security task?

A. Standard

B. Policy

C. Guideline

D. Procedure

Correct Answer: *D*

Community vote distribution

D (100%)

Question #531 *Topic 1*

While conducting a business continuity tabletop exercise, the security team becomes concerned by potential impact if a generator was to develop a fault during failover. Which of the following is the team most likely to consider in regard to risk management activities?

A. RPO

B. ARO

C. BIA Most Voted

D. MTTR

Correct Answer: *C*

Community vote distribution

C (86%) 14%

Question #532 *Topic 1*

Which of the following is prevented by proper data sanitization?

A. Hackers' ability to obtain data from used hard drives

B. Devices reaching end-of-life and losing support

C. Disclosure of sensitive data through incorrect classification

D. Incorrect inventory data leading to a laptop shortage

Correct Answer: *A*

Community vote distribution

A (100%)

Question #533 *Topic 1*

A certificate authority needs to post information about expired certificates. Which of the following would accomplish this task?

A. TPM

B. CRL

C. PKI

D. CSR

Correct Answer: *B*

Community vote distribution

B (100%)

Question #534 *Topic 1*

Which of the following can best contribute to prioritizing patch applications?

A. CVSS

B. SCAP

C. OSINT

D. CVE

Correct Answer: *A*

Community vote distribution

A (100%)

Question #535 *Topic 1*

A systems administrator creates a script that validates OS version, patch levels, and installed applications when users log in. Which of the following examples best describes the purpose of this script?

A. Resource scaling

B. Policy enumeration

C. Baseline enforcement

D. Guard rails implementation

Correct Answer: *C*

Community vote distribution

C (100%)

Question #536 *Topic 1*

A security analyst learns that an attack vector, which was used as a part of a recent incident, was a well-known IoT device exploit. The analyst needs to review logs to identify the time of initial exploit. Which of the following logs should the analyst review first?

A. Endpoint

B. Application

C. Firewall

D. NAC

Correct Answer: *C*

Community vote distribution

C (60%) A (40%)

Question #537 *Topic 1*

A company's gate access logs show multiple entries from an employee's ID badge within a two-minute period. Which of the following is this an example of?

A. RFID cloning Most Voted

B. Side-channel attack

C. Shoulder surfing

D. Tailgating

Correct Answer: *A*

Community vote distribution

A (80%) D (20%)

Question #538 *Topic 1*

Which of the following most accurately describes the order in which a security engineer should implement secure baselines?

A. Deploy, maintain, establish

B. Establish, maintain, deploy

C. Establish, deploy, maintain

D. Deploy, establish, maintain

Correct Answer: *C*

Community vote distribution

C (100%)

Question #539 *Topic 1*

A SOC analyst establishes a remote control session on an end user's machine and discovers the following in a file:

gmail.com[ENT]my.name@gmail.com[ENT]NoOneCanGuessThis123! [ENT]Hello Susan, it was great to see you the other day! Let's plan a followup[BACKSPACE]follow-up meeting soon. Here is the link to register. [RTN][CTRL]c [CTRL]v [RTN]after[BACKSPACE]After you register give me a call on my cellphone.

Which of the following actions should the SOC analyst perform first?

A. Advise the user to change passwords. Most Voted

B. Reimage the end user's machine.

C. Check the policy on personal email at work.

D. Check host firewall logs.

Correct Answer: *A*

Community vote distribution

A (64%) B (36%)

Question #540 *Topic 1*

Which of the following is a reason environmental variables are a concern when reviewing potential system vulnerabilities?

A. The contents of environmental variables could affect the scope and impact of an exploited vulnerability.

B. In-memory environmental variable values can be overwritten and used by attackers to insert malicious code.

C. Environmental variables define cryptographic standards for the system and could create vulnerabilities if deprecated algorithms are used.

D. Environmental variables will determine when updates are run and could mitigate the likelihood of vulnerability exploitation.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #541 *Topic 1*

A company evaluates several options that would allow employees to have remote access to the network. The security team wants to ensure the solution includes AAA to comply with internal security policies. Which of the following should the security team recommend?

A. IPSec with RADIUS

B. RDP connection with LDAPS

C. Web proxy for all remote traffic

D. Jump server with 802.1X

Correct Answer: *A*

Community vote distribution

A (100%)

Question #542 *Topic 1*

An administrator must replace an expired SSL certificate. Which of the following does the administrator need to create the new SSL certificate?

A. CSR

B. OCSP

C. Key

D. CRL

Correct Answer: *A*

Community vote distribution

A (100%)

Question #543 *Topic 1*

A systems administrator receives a text message from an unknown number claiming to be the Chief Executive Officer of the company. The message states an emergency situation requires a password reset. Which of the following threat vectors is being used?

A. Typosquatting

B. Smishing

C. Pretexting

D. Impersonation

Correct Answer: *B*

Community vote distribution

B (100%)

Question #544 *Topic 1*

A Chief Information Security Officer (CISO) wants to:

• Prevent employees from downloading malicious content.
• Establish controls based on departments and users.
• Map internet access for business applications to specific service accounts.
• Restrict content based on categorization.

Which of the following should the CSO implement?

A. Web application firewall

B. Secure DNS server

C. Jump server

D. Next-generation firewall

Correct Answer: *D*

Community vote distribution

D (100%)

Question #545 *Topic 1*

A company is aware of a given security risk related to a specific market segment. The business chooses not to accept responsibility and target their services to a different market segment. Which of the following describes this risk management strategy?

A. Exemption

B. Exception

C. Avoid

D. Transfer

Correct Answer: *C*

Community vote distribution

C (100%)

Question #546 *Topic 1*

A security analyst needs to improve the company's authentication policy following a password audit. Which of the following should be included in the policy? (Choose two.)

A. Length Most Voted

B. Complexity

C. Least privilege

D. Something you have

E. Security keys

F. Biometrics

Correct Answer: *A*

Community vote distribution

A (67%) B (33%)

Question #547 *Topic 1*

Which of the following is an example of a treatment strategy for a continuous risk?

A. Email gateway to block phishing attempts Most Voted

B. Background checks for new employees

C. Dual control requirements for wire transfers

D. Branch protection as part of the CI/CD pipeline

Correct Answer: *A*

Community vote distribution

A (57%) D (43%)

Question #548 *Topic 1*

An organization wants to deploy software in a container environment to increase security. Which of the following would limit the organization's ability to achieve this goal?

A. Regulatory compliance

B. Patch availability

C. Kernel version

D. Monolithic code

Correct Answer: *D*

Community vote distribution

D (100%)

Question #549 *Topic 1*

Prior to implementing a design change, the change must go through multiple steps to ensure that it does not cause any security issues. Which of the following is most likely to be one of those steps?

A. Board review

B. Service restart

C. Backout planning

D. Maintenance

Correct Answer: *C*

Community vote distribution

C (100%)

Question #550 *Topic 1*

The internal audit team determines a software application is no longer in scope for external reporting requirements. Which of the following will confirm that the application is no longer applicable?

A. Data inventory and retention

B. Right to be forgotten

C. Due care and due diligence

D. Acknowledgement and attestation Most Voted

Correct Answer: *D*

Community vote distribution

D (67%) A (33%)

Question #551 *Topic 1*

Which of the following are the first steps an analyst should perform when developing a heat map? (Choose two.)

A. Methodically walk around the office noting Wi-Fi signal strength.

B. Log in to each access point and check the settings.

C. Create or obtain a layout of the office.

D. Measure cable lengths between access points.

E. Review access logs to determine the most active devices.

F. Remove possible impediments to radio transmissions.

Correct Answer: *AC*

Community vote distribution

AC (67%) BC (33%)

Question #552 *Topic 1*

Which of the following is used to improve security and overall functionality without losing critical application data?

A. Reformatting

B. Decommissioning

C. Patching

D. Encryption

Correct Answer: *C*

Community vote distribution

C (100%)

Question #553 *Topic 1*

An organization is preparing to export proprietary software to a customer. Which of the following would be the best way to prevent the loss of intellectual property?

A. Code signing

B. Obfuscation

C. Tokenization

D. Blockchain

Correct Answer: *B*

Community vote distribution

B (100%)

Question #554 *Topic 1*

After a series of account compromises and credential misuse, a company hires a security manager to develop a security program. Which of the following steps should the security manager take first to increase security awareness?

A. Evaluate tools that identify risky behavior and distribute reports on the findings. Most Voted

B. Send quarterly newsletters that explain the importance of password management.

C. Develop phishing campaigns and notify the management team of any successes.

D. Update policies and handbooks to ensure all employees are informed of the new procedures.

Correct Answer: *A*

Community vote distribution

A (50%) D (38%) 13%

Question #555 *Topic 1*

Which of the following should be used to ensure a device is inaccessible to a network-connected resource?

A. Disablement of unused services

B. Web application firewall

C. Host isolation

D. Network-based IDS

Correct Answer: *C*

Community vote distribution

C (100%)

Question #556 *Topic 1*

In which of the following will unencrypted network traffic most likely be found?

A. SDN

B. IoT Most Voted

C. VPN

D. SCADA

Correct Answer: *B*

Community vote distribution

B (100%)

Question #557 *Topic 1*

Which of the following is the best reason to perform a tabletop exercise?

A. To address audit findings

B. To collect remediation response times

C. To update the IRP

D. To calculate the ROI

Correct Answer: *C*

Community vote distribution

C (100%)

Question #558 *Topic 1*

Which of the following is a use of CVSS?

A. To determine the cost associated with patching systems

B. To identify unused ports and services that should be closed

C. To analyze code for defects that could be exploited

D. To prioritize the remediation of vulnerabilities

Correct Answer: *D*

Community vote distribution

D (100%)

Question #559 *Topic 1*

For an upcoming product launch, a company hires a marketing agency whose owner is a close relative of the Chief Executive Officer. Which of the following did the company violate?

A. Independent assessments

B. Supply chain analysis

C. Right-to-audit clause

D. Conflict of interest policy

Correct Answer: *D*

Community vote distribution

D (100%)

Question #560 *Topic 1*

An organization designs an inbound firewall with a fail-open configuration while implementing a website. Which of the following would the organization consider to be the highest priority?

A. Confidentiality

B. Non-repudiation

C. Availability

D. Integrity

Correct Answer: *C*

Community vote distribution

C (100%)

Question #561 *Topic 1*

An engineer needs to ensure that a script has not been modified before it is launched. Which of the following best provides this functionality?

A. Masking

B. Obfuscation

C. Hashing

D. Encryption

Correct Answer: *C*

Community vote distribution

C (100%)

Question #562 *Topic 1*

Which of the following is the most important element when defining effective security governance?

A. Discovering and documenting external considerations

B. Developing procedures for employee onboarding and offboarding

C. Assigning roles and responsibilities for owners, controllers, and custodians

D. Defining and monitoring change management procedures

Correct Answer: *C*

Community vote distribution

C (100%)

Question #563 *Topic 1*

A contractor is required to visually inspect the motherboards of all new servers that are purchased to determine whether the servers were tampered with. Which of the following risks is the contractor attempting to mitigate?

A. Embedded rootkit

B. Supply chain

C. Firmware failure

D. RFID keylogger

Correct Answer: *B*

Community vote distribution

B (100%)

Question #564 *Topic 1*

Which of the following could potentially be introduced at the time of side loading?

A. User impersonation

B. Rootkit

C. On-path attack

D. Buffer overflow

Correct Answer: *B*

Community vote distribution

B (100%)

Question #565 *Topic 1*

While a school district is performing state testing, a security analyst notices all internet services are unavailable. The analyst discovers that ARP poisoning is occurring on the network and then terminates access for the host. Which of the following is most likely responsible for this malicious activity?

A. Unskilled attacker

B. Shadow IT

C. Insider threat

D. Nation-state

Correct Answer: *C*

Community vote distribution

C (100%)

Question #566 *Topic 1*

A user needs to complete training at https://comptiatraining.com. After manually entering the URL, the user sees that the accessed website is noticeably different from the standard company website. Which of the following is the most likely explanation for the difference?

A. Cross-site scripting

B. Pretexting

C. Typosquatting

D. Vishing

Correct Answer: *C*

Community vote distribution

C (100%)

Question #567 *Topic 1*

A company has yearly engagements with a service provider. The general terms and conditions are the same for all engagements. The company wants to simplify the process and revisit the general terms every three years. Which of the following documents would provide the best way to set the general terms?

A. MSA

B. NDA

C. MOU

D. SLA

Correct Answer: *A*

Community vote distribution

A (100%)

Question #568 *Topic 1*

While updating the security awareness training, a security analyst wants to address issues created if vendors' email accounts are compromised. Which of the following recommendations should the security analyst include in the training?

A. Refrain from clicking on images included in emails from new vendors

B. Delete emails from unknown service provider partners.

C. Require that invoices be sent as attachments

D. Be alert to unexpected requests from familiar email addresses

Correct Answer: *D*

Community vote distribution

D (100%)

Question #569 *Topic 1*

A new corporate policy requires all staff to use multifactor authentication to access company resources. Which of the following can be utilized to set up this form of identity and access management? (Choose two.)

A. Authentication tokens

B. Least privilege

C. Biometrics

D. LDAP

E. Password vaulting

F. SAML

Correct Answer: *AC*

Community vote distribution

AC (100%)

Question #570 *Topic 1*

A help desk employee receives a call from someone impersonating the Chief Executive Officer. The caller asks for assistance with resetting a password. Which of the following best describes this event?

A. Vishing

B. Hacktivism

C. Blackmail

D. Misinformation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #571 *Topic 1*

The number of tickets the help desk has been receiving has increased recently due to numerous false-positive phishing reports. Which of the following would be best to help to reduce the false positives?

A. Performing more phishing simulation campaigns

B. Improving security awareness training

C. Hiring more help desk staff

D. Implementing an incident reporting web page

Correct Answer: *B*

Community vote distribution

B (100%)

Question #572 *Topic 1*

An organization that handles sensitive information wants to protect the information by using a reversible technology. Which of the following best satisfies this requirement?

A. Hardware security module

B. Hashing algorithm

C. Tokenization

D. Steganography

Correct Answer: *C*

Community vote distribution

C (100%)

Question #573 *Topic 1*

A systems administrator needs to encrypt all data on employee laptops. Which of the following encryption levels should be implemented?

A. Volume

B. Partition

C. Full disk

D. File

Correct Answer: *C*

Community vote distribution

C (100%)

Question #574 *Topic 1*

Which of the following actions best addresses a vulnerability found on a company's web server?

A. Patching

B. Segmentation

C. Decommissioning

D. Monitoring

Correct Answer: *A*

Community vote distribution

A (100%)

Question #575 *Topic 1*

A company is changing its mobile device policy. The company has the following requirements:

- Company-owned devices
- Ability to harden the devices
- Reduced security risk
- Compatibility with company resources

Which of the following would best meet these requirements?

A. BYOD

B. CYOD

C. COPE

D. COBO Most Voted

Correct Answer: *D*

Community vote distribution

D (85%) C (15%)

Question #576 *Topic 1*

A company is concerned about employees unintentionally introducing malware into the network. The company identified fifty employees who clicked on a link embedded in an email sent by the internal IT department. Which of the following should the company implement to best improve its security posture?

A. Social engineering training Most Voted

B. SPF configuration

C. Simulated phishing campaign

D. Insider threat awareness

Correct Answer: *A*

Community vote distribution

A (73%) C (18%) 9%

Question #577 *Topic 1*

A penetration test identifies that an SMBv1 is enabled on multiple servers across an organization. The organization wants to remediate this vulnerability in the most efficient way possible. Which of the following should the organization use for this purpose?

A. GPO Most Voted

B. ACL

C. SFTP

D. DLP

Correct Answer: *A*

Community vote distribution

A (100%)

Question #578 *Topic 1*

Which of the following best protects sensitive data in transit across a geographically dispersed infrastructure?

A. Encryption

B. Masking

C. Tokenization

D. Obfuscation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #579 *Topic 1*

As part of new compliance audit requirements, multiple servers need to be segmented on different networks and should be reachable only from authorized internal systems. Which of the following would meet the requirements?

A. Configure firewall rules to block external access to Internal resources.

B. Set up a WAP to allow internal access from public networks.

C. Implement a new IPSec tunnel from internal resources.

D. Deploy an internal jump server to access resources. Most Voted

Correct Answer: *D*

Community vote distribution

D (71%) A (29%)

Question #580 *Topic 1*

Which of the following activities should be performed first to compile a list of vulnerabilities in an environment?

A. Automated scanning

B. Penetration testing

C. Threat hunting

D. Log aggregation

E. Adversarial emulation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #581 *Topic 1*

Which of the following can be used to mitigate attacks from high-risk regions?

A. Obfuscation

B. Data sovereignty

C. IP geolocation

D. Encryption

Correct Answer: *C*

Community vote distribution

C (100%)