Item 16 of 620 (Exam B,Q1)

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? (Select two).

A.Typosquatting
B.Smishing
C.Impersonation
D.Misinformation
E.Vishing
F.Phishing

Item 17 of 620 (Exam B,Q2)

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.IDS
B.IPS
C.ACL
D.DIP

Item 18 of 620 (Exam B,Q3)

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.Firmware
B.Virtualization
C.Application
D.Operating system

Item 19 of 620 (Exam B,Q4)

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

A.Inventory list
B.Certification
C.Proof of ownership
D.Classification

Item 20 of 620 (Exam B,Q5)

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.Adaptive identity
B.Threat scope reduction
C.Subject role
D.Secured zones

Item 21 of 620 (Exam B,Q6)

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

A.Removable devices
B.Bastion host
C.Unsecured Bluetooth
D.Unpatched OS

Item 22 of 620 (Exam B,Q7)

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.Performing code signing on company-developed software

B.Ensuring secure cookies are used

C.Performing static code analysis on the software

D.Testing input validation on the user input fields

Item 23 of 620 (Exam B,Q8)

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

C.Software-defined networking

D.Internet of Things

Item 24 of 620 (Exam B, Q9)

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 folowing best describes how the controls should be set up?

A.Safety controls should fail open.

B.Remote access points should fail closed.

C.Logical security controls should fail closed.

D.Logging controls should fail open.

Item 25 of 620 (Exam B,Q10)

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.Redundancy

B.Capacity planning

C.Tabletop exercise

D.Geographic dispersion

Item 26 of 620 (Exam B,Q11)

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.RADIUS

B.HSM

C.Jump server

D.Load balancer

Item 27 of 620 (Exam B,Q12)

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 folowing types of sites is the best for this scenario?

A.Hot

B.Warm

C.Cold

D.Real-time recovery

Item 28 of 620 (Exam B,Q13)

Which of the following roles,according to the shared responsibility model,is responsible for securing the company's database in an laaS model for a cloud environment?
A.Cloud provider
B.DBA
C.Third-party vendor
D.Client

Item 29 of 620 (Exam B,Q14)
Which of the following is a hardware-specific vulnerability?
A.Buffer overflow
B.SQL injection
C.Cross-site scripting
D.Firmware version

Item 30 of 620 (Exam B,Q15)
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.Use hexdump on the file's contents
B.Query the file's metadata.
C.Check endpoint logs.
D.Obtain the file's SHA-256 hash.

Item 31 of 620 (Exam B,Q16)
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 sovereignty regulation
B.Geolocation policy
C.Data masking
D.Encryption

Item 32 of 620 (Exam B,Q17)
A security analyst is scanning 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.Using a proxy for web connections from the remote desktop server
C.Setting up a VPN and placing the jump server inside the firewall
D.Connecting the remote server to the domain and increasing the password length

Item 33 of 620 (Exam B,Q18)
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.Employee monitoring
B.Hardening
C.Configuration enforcement
D.Least privilege

Item 34 of 620 (Exam B,Q19)

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.Watering-hole
C.Smishing
D.Disinformation

Item 35 of 620 (Exam B,Q20)
Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?
A.Yellow
B.Red
C.Purple
D.Blue

Item 36 of 620 (Exam B,Q21)
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.Modify the content of recurring training.
B.Send out periodic security reminders.
C.Update the content of new hire documentation.
D.Implement a phishing campaign.

Item 37 of 620 (Exam B,Q22)
Which of the following security concepts should an e-commerce organization apply for protection against erroneous purchases?
A.Confidentiality
B.Privacy
C.Availability
D.Integrity

Item 38 of 620 (Exam B,Q23)
A security administrator would like to protect data on employees'laptops.Which of the folowing encryption techniques should the security administrator use?
A.Database
B.Full disk
C.Partition
D.Asymmetric

Item 39 of 620(Exam B,Q24)
Which of the following describes the reason root cause analysis should be conducted as part of incident response?
A.To eradicate any trace of malware on the network
B.To gather loCs for the investigation
C.To discover which systems have been affected
D.To prevent future incidents of the same nature

Item 40 of 620 (Exam B,Q25)
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? (Select two).
A.Open authentication
B.Identity proofing
C.Password manager
D.Password complexity
E.Federation
F.Default password changes

Item 41 of 620 (Exam B,Q26)
Which of the following must be considered when designing a high-availability network?(Select two).
A.Ability to patch
B.Ease of recovery
C.Responsiveness
D.Attack surface
E.Physical isolation
F.Extensible authentication

Item 42 of 620 (Exam B,Q27)
A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.Which of the following teams wil conduct this assessment activity?
A.White
B.Purple
C.Red
D.Blue

Item 43 of 620 (Exam B,Q28)
A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?
A.Mitigate
B.Avoid
C.Accept
D.Transfer

Item 44 of 620 (Exam B,Q29)
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.Inventory
C.Destruction
D.Sanitization

Item 45 of 620 (Exam B,Q30)
Which of the following is used to quantitatively measure the criticality of a vulnerability?
A.CIA
B.CVE
C.CERT
D.CVSS

Item 46 of 620 (Exam B,Q31)

Which of the following would be the best way to block unknown programs from executing?
A.Application allow list
B.DLP solution
C.Access control list
D.Host-based firewall

Item 47 of 620 (Exam B,Q32)
Which of the following incident response activities ensures evidence is properly handled?
A.Chain of custody
B.Legal hold
C.Preservation
D.E-discovery

Item 48 of 620 (Exam B,Q33)
While troubleshooting a firewal 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.Testing the policy in a non-production environment before enabling the policy in the production network
B.Documenting the new policy in a change request and submitting the request to change management
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

Item 49 of 620 (Exam B,Q34)
Which of the following scenarios describes a possible business email compromise attack?
A.Employees who open an email attachment receive messages demanding payment in order to access files.
B.A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
C.An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.
D.An employee receives a gift card request in an email that has an executive's name in the display field of the email.

Item 50 of 620 (Exam B,Q35)
An organization disabled unneeded services and placed a firewallin front of a businesscritical legacy system.Which of the following best describes the actions taken by the organization?
A.Risk transfer
B.Exception
C.Compensating controls
D.Segmentation

Item 51 of 620 (Exam B,Q36)
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.Isolation
B.Encryption
C.Patching
D.Segmentation

Item 52 of 620 (Exam B,Q37)

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.Password complexity
B.Permissions assignment
C.Multifactor authentication
D.Access management

Item 53 of 620 (Exam B,Q38)
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
B.SNMP traps
C.Network segmentation
D.Transfer of risk

Item 54 of 620(Exam B,Q39)
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.A rootkit was deployed.
B.A cryptographic collision was detected.
C.A snapshot of the file system was taken.
D.The end user changed the file permissions

Item 55 of 620 (Exam B,Q40)
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
B.Data classification
C.Permission restrictions
D.Masking

Item 56 of 620(Exam B,Q41)
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 ClO's report?
CA.Insider threat
B.Nation-state
C.Organized crime
D.Hacktivist

Item 57 of 620 (Exam B,Q42)
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.ARO
B.RIO
C.MTTR

D.MTBF

Item 58 of 620 (Exam B,Q43)
Which of the following should a security administrator adhere to when setting up a new set of firewall rules?
A.Incident response procedure
B.Disaster recovery plan
C.Business continuity plan
D.Change management procedure

Item 59 of 620 (Exam B,Q44)
A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes.Which of the following shouldthe administrator set up to achieve this goal?
A.NAC
B.SPF
C.GPO
D.FIM

Item 60 of 620 (Exam B,Q45)
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.Web-based administration
B.VLANS
C.Console access
D.Routing protocols

ltem 61 of 620 (Exam B,Q46)
Which of the following is a primary security concern for a company setting up a BYOD program?
A.Jailbreaking
B.Buffer overflow
C.End of life
D.VM escape

Item 62 of 620 (Exam B,Q47)
Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?
A.Jailbreaking
B.Memory injection
C.Side loading
D.Resource reuse

Item 63 of 620 (Exam B,Q48)
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.Create additional training for users to recognize the signs of phishing attempts.
C.Update the EDR policies to block automatic execution of downloaded programs.
D.Implement email security filters to prevent phishing emails from being delivered.

Item 64 of 620 (Exam B,Q49)

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.Version control
B.Code signing
C.Input validation
D.Secure cookies

Item 65 of 620 (Exam B,Q50)

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.Detection
B.Analysis
C.Containment
D.Lessons learned

Item 66 of 620 (Exam B,Q51)

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.BPA
B.MSA
C.SLA
D.SOW

Item 67 of 620 (Exam B,Q52)

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.Rescan the network.
C.Initiate a penetration test.
D.Submit a report.

Item 68 of 620 (Exam B,Q53)

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.Salting
D.Steganography

Item 69 of 620 (Exam B,Q54)

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.User provisioning script
C.Escalation script
D.Ticketing workflow

Item 70 of 620 (Exam B,Q55)

Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?
A.Audit findings
B.Sanctions
C.Reputation damage
D.Fines

Item 71 of 620 (Exam B,Q56)
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
B.Attestation
C.Manual audit
D.Compliance checklist

Item 72 of 620 (Exam B,Q57)
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 alow users to access the site?
A.Configuring the IPs to allow shopping
B.Creating a firewall rule to allow HTTPS traffic
C.Tuning the DLP rule that detects credit card data
D.Updating the categorization in the content filter

Item 73 of 620 (Exam B,Q58)
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.An in-depth penetration test of all suppliers and vendors
B.A thorough analysis of the supply chain
C.A legally enforceable corporate acquisition policy
D.A right to audit clause in vendor contracts and sows

Item 74 of 620(Exam B,Q59)
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.Bug bounty
B.Penetration testing
C.Red team
D.Open-source intelligence

Item 75 of 620 (Exam B,Q60)
Which of the following is the most likely to be included as an element of communication in a security awareness program?
A.Detecting insider threats using anomalous behavior recognition
B.Verifying information when modifying wire transfer data
C.Performing social engineering as part of third-party penetration testing
D.Reporting phishing attempts or other suspicious activities

Item 76 of 620 (Exam B,Q61)
A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

A.Load balancers
B.Geographic dispersion
C.Clustering servers
D.Off-site backups

Item 77 of 620 (Exam B,Q62)
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.Unskilled attacker
B.Organized crime
C.Whistleblower
D.Hacktivist

Item 78 of 620 (Exam B,Q63)
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?(Select two).
A.Sanitization
B.Certification
C.Classification
D.Enumeration
E.Data retention
F.Destruction

Item 79 of 620 (Exam B,Q64)
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.One time
B.Ad hoc
C.Continuous
D.Recurring

Item 80 of 620 (Exam B,Q65)
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? (Select two).
A.Cancel current employee recognition gift cards.
B.Add a smishing exercise to the annual company training.
C.Conduct a forensic investigation on the CEO's phone.
D.Have the CEO change phone numbers.
E.Implement mobile device management.
F.Issue a general email warning to the company.

Item 81 of 620 (Exam B,Q66)
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

Item 82 of 620 (Exam B,Q67)
Which of the following allows for the attribution of messages to individuals?
A.Authentication
B.Non-repudiation
C.Access logs
D.Adaptive identity

Item 83 of 620 (Exam B,Q68)
Which of the following is classified as high availability in a cloud environment?
A.Access broker
B.Load balancer
C.Cloud HSM
D.WAF

Item 84 of 620 (Exam B,Q69)
A company needs to provide administrative access to internal resources while minimizing the traffic alowed through the security boundary. Which of the following methods is most secure?
A.Installing a WAF
B.Utilizing single sign-on
C.Deploying a perimeter network
D.Implementing a bastion host

Item 85 of 620 (Exam B,Q70)
Which of the following is required for an organization to properly manage its restore process in the event of system failure?
A.DRP
B.SDLC
C.IRP
D.RPO

Item 86 of 620 (Exam B,Q71)
Which of the following threat actors is the most likely to be motivated by profit?
A.Shadow IT
B.Hacktivist
C.Organized crime
D.Insider threat

Item 87 of 620(Exam B,Q72)
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 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
B.Access list outbound permit 0.0.0.0/o 0.0.0.0/0 port 53
Access list outbound deny 10.50.10.25/32 0.0.0.070 port 53
C.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
D.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

Item 88 of 620 (Exam B,Q73)

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.http://
B.encryption=off
C.:443
D.www.*.com

Item 89 of 620 (Exam B,Q74)

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? (Select two).

A.When conducting penetration testing, the security team will be able to target the desired laptops.
B.If a security incident occurs on the device,the correct employee can be notified.
C.Company data can be accounted for when the employee leaves the organization.
D.User-based firewall policies can be correctly targeted to the appropriate laptops.
E. The security team will be able to send user awareness training to the appropriate device.
F.Users can be mapped to their devices when configuring software MFA tokens.

Item 90 of 620 (Exam B,Q75)

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.Dashboard
B.Packet captures
C.Vulnerability scans
D.Metadata

Item 91 of 620 (Exam B,Q76)

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

A.DLP
B.SCAP
C.Antivirus
D.NetFlow

Item 92 of 620 (Exam B,Q77)

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.Endpoint
D.Network

Item 93 of 620 (Exam B,Q78)

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.Critical

C.Intellectual property
D.Data in transit

Item 94 of 620 (Exam B,Q79)
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.PEAP
B.LEAP
C.SSO
D.MFA

Item 95 of 620 (Exam B,Q80)
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.Quarantining
B.Aggregating
C.Archiving
D.Tuning

Item 96 of 620 (Exam B,Q81)
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.TLS
B.SD-WAN
C.WAF
D.NGFW

Item 97 of 620 (Exam B,Q82)
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 $, I , ;, &, '; 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.Input validation
B.Identify embedded keys
C.Code debugging
D.Static code analysis

Item 98 of 620 (Exam B,Q83)
Which of the following is the most likely to be used to document risks,responsible parties,and thresholds?
A.Risk transfer
B.Risk analysis
C.Risk tolerance
D.Risk register

Item 99 of 620 (Exam B,Q84)
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.Defensive

B.Offensive
C.Passive
D.Active

Item 100 of 620 (Exam B,Q85)
Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other counties?
A.Hacktivist
B.Unskilled attacker
C.Insider
D.Nation-state

Item 101 of 620 (Exam B,Q86)
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.Sensitive
B.Critical
C.Public
D.Private

Item 102 of 620 (Exam B,Q87)
A systems administrator is looking for a low-cost application-hosting solution that is cloudbased.Which of the following meets these requirements?
A.SDN
B.Serverless framework
C.SD-WAN
D.Type 1 hypervisor

Item 103 of 620 (Exam B,Q88)
Which of the following enables the use of an input field to run commands that can view or manipulate data?
A.Buffer overflow
B.Side loading
C.SQL injection
D.Cross-site scripting

Item 104 of 620 (Exam B,Q89)
Which of the following security control types does an acceptable use policy best represent?
A.Compensating
B.Preventive
C.Corrective
D.Detective

Item 105 of 620 (Exam B,Q90)
Which of the following can be used to identify potential attacker activities without affecting production servers?
A.Honeypot
B.Geofencing
C.Video surveillance
D.Zero Trust

Item 106 of 620 (Exam B,Q91)

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.Detective
B.Preventive
C.Deterrent
D.Corrective

Item 107 of 620 (Exam B,Q92)
A technician needs to apply a high-priority patch to a production system.Which of the following steps should be taken first?
A.Move the system to a different network segment.
B.Air gap the system.
C.Create a change control request
D.Apply the patch to the system.

Item 108 of 620 (Exam B,Q93)
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
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

Item 109 of 620 (Exam B,Q94)
A security analyst reviews domain activity logs and notices the following:
UserID jamith,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) ehich of the following is the best explanation for what the security analyst has discovered?
A.An attacker is attempting to brute force jsmith's account.
B.A keylogger is installed on jsmith's workstation.
C.The user jsmith's account has been locked out.
D.Ransomware has been deployed in the domain.

Item 110 of 620 (Exam B,Q95)
A security analyst is reviewing the following logs:

[10:00:00 AM] Login rejected -username administrator-password Spring2023

(1000:01 AM) Login relected-usemame isneith password soring

[10:00:02 AM] Login rejected -username cpolk-pasaword spring2023 [10:00:03 AMj Login rejected-username fmartin-password spring2023

Which of the following attacks is most likely occurring?
A.Pass-the-hash
B.Brute-force
C.Password spraying
D.Account forgery

Item 111 of 620 (Exam B,Q96)

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.Impacts to existing contractual obligations
B.Risks from hackers residing in other countries
C.Time zone differences in log correlation
D.Local data protection regulations

Item 112 of 620 (Exam B,Q97)
Which of the folowing would be best suited for constantly changing environments?
A.RTOS
B.Containers
C.SCADA
D.Embedded systems

Item 113 of 620(Exam B,Q98)
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.Confidentiality
B.Availability
C.Non-repudiation
D.Integrity

Item 114 of 620 (Exam B,Q99)
Which of the following is used to validate a certificate when it is presented to a user?
A.CSR
B.OCSP
C.CA
D.CRC

Item 115 of 620 (Exam B,Q100)
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.On-path resource consumption
B.Secure DNS cryptographic downgrade
C.Concurrent session usage
D.Reflected denial of service

Item 115 of 620 (Exam B,Q100)
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.On-path resource consumption
B.Secure DNS cryptographic downgrade
C.Concurrent session usage
D.Reflected denial f service

Item 116 of 620 (Exam B,Q101)

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.Apply classifications to the data.
C.Remove all user permissions from shares on the file server.
D.Create a rule to block outgoing email attachments.

Item 117 of 620 (Exam B,Q102)
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.Content filtering
B.Data loss prevention
C.Access control lists
D.Group Policy

Item 118 of 620 (Exam B,Q103)
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 list of system owners and their departments
B.Documentation of system classifications
C.A full inventory of all hardware and software
D.Third-party risk assessment documentation

Item 119 of 620 (Exam B,Q104)
A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set in up in order to mitigate the threat posed by the suspicious activity?
A.Application allow list
B.Access control list
C.Web application firewall
D.Host-based firewall

Item 120 of 620 (Exam B,Q105)
Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program?(Select two).
A.Channels by which the organization communicates with customers
B.Cadence and duration of training events
C.The reporting mechanisms for ethics violations
D.Retraining requirements for individuals who fail phishing simulations
E.Secure software development training for all personnel
F.Threat vectors based on the industry in which the organization operates

Item 121 of 620 (Exam B,Q106)
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.Vulnerable software
B.Supply chain vendor
C.Non-segmented network
D.Default credentials

Item 122 of 620 (Exam B,Q107)

Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Select two).
A.Video surveillance
B.Sign-in sheet
C.Sensor
D.Fencing
E.Access control vestibule
F.Badge access

Item 123 of 620 (Exam B,Q108)

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.Owner
C.Subject
D.Custodian

Item 124 of 620 (Exam B,Q109)
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.DHCP
B.NAT
C.IPSec
D.EAP

Item 125 of 620 (Exam B,Q110)
Which of the following exercises should an organization use to improve its incident response process?
A.Replication
B.Tabletop
C.Failover
D.Recovery

Item 126 of 620 (Exam B,Q111)
A newly identified network access vulnerability has been found in the OS of legacy loT devices. Which of the following would best mitigate this vulnerability quickly?
A.Insurance
B.Segmentation
C.Patching
D.Replacement

Item 127 of 620 (Exam B,Q112)
Which of the following is the best reason to complete an audit in a banking environment?
A.Self-assessment requirement
B.Regulatory requirement
C.Organizational change
D.Service-level requirement

Item 128 of 620(Exam B,Q113)

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.Preventive
C.Detective
D.Corrective

Item 129 of 620 (Exam B,Q114)
Which of the following can best protect against an employee inadvertently installing malware on a company system?
A.System isolation
B.Least privilege
C.Host-based firewall
D.Application allow list

Item 130 of 620 (Exam B,Q115)
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
B.Product software compatibility
C.Ease of recovery
D.Cost of replacement

Item 131 of 620 (Exam B,Q116)
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.Policy enforcement
B.Baselinex
C.Off-the-shelf software
D.Orchestration

Item 132 of 620 (Exam B,Q117)
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.Change management boards
C.Scheduled downtime
D.Backout plan

Item 133 of 620 (Exam B,Q118)
Which of the following methods would most likely be used to identify legacy systems?
A.Bug bounty program
B.Vulnerability scan
C.Dynamic analysis
D.Package monitoring

Item 134 of 620 (Exam B,Q119)
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 folowing should the company consider?

A.Platform diversity
B.Geographic dispersion
C.Load balancing
D.Hot site

Item 135 of 62 (Exam B,Q120)
Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?
A.Preparation
B.Lessons learned
C.Recovery
D.Analysis

Item 136 of 620 (Exam B,Q121)
Which of the following are cases in which an engineer should recommend the decommissioning of a network device?(Select two).
A.The device's encryption level cannot meet organizational standards.
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 unable to receive authorized updates.
E.The device is moved to a different location in the enterprise.
F.The device has been moved from a production environment to a test environment.

Item 137 of 620 (Exam B,Q122)
A legacy device is being decommissioned and is no longer receiving updates or patches.Which of the following describes this scenario?
A.End of testing
B.End of life
C.End of business
D.End of support

Item 138 of 620 (Exam B,Q123)
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.Inventory
B.Retention
C.Analysis
D.Compromise
E.Transfer

Item 139 of 620 (Exam B,Q124)
Which of the following involves an attempt to take advantage of database misconfigurations?
A.SQL injection
B.VM escape
C.Buffer overflow
D.Memory injection

Item 140 of 620 (Exam B,Q125)
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.Peer review and approval
D.Quality assurance testing

Item 141 of 620 (Exam B,Q126)
A systems administrator is working on a solution with the following requirements:
1. Provide a secure zone.
2. Enforce a company-wide access control policy. 3 Reduce the scope of threats.
Which of the following is the systems administrator setting up?
A.CIA
B.AAA
C.Non-repudiation
D.Zero Trust

Item 142 of 620 (Exam B,Q127)
A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the folowing documents includes the information the service provider should return to the client?
A.MOA
B.SLA
C.SOW
D.MOU

Item 143 of 620 (Exam B,Q128)
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.Building a load-balanced VPN solution with redundant internet
B.Deploying a SASE solution to remote employees
C.Purchasing a low-cost SD-WAN solution for VPN traffic
D.Using a cloud provider to create additional VPN concentrators

Item 144 of 620 (Exam B,Q129)
A company must ensure sensitive data at rest is rendered unreadable. Which of the following wil the company most likely use?
A.Tokenization
B.Segmentation
C.Encryption
D.Hashing

Item 145 of 620 (Exam B,Q130)
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 folowing vulnerabilties is the organization addressing?
A.Jailbreaking
B.Cross-site scripting
C.Side loading
D.Buffer overflow

Item 146 of 620 (Exam B,Q131)
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.SNMP

B.SIEM
C.DLP
D.IDS

Item 147 of 620 (Exam B,Q132)
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.NDA
B.SLA
C.BPA
D.SOW

Item 148 of 620 (Exam B,Q133)
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.GPO
B.SAML
C.RBAC
D.ACL

Item 149 of 620 (Exam B,Q134)
A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over to short periods of time during nonbusiness hours.Which of the following is most likely occurring?
A.A logic bomb is deleting data
B.Data is being exfiltrated.
C.A worm is propagating across the network.
D.Ransomware is encrypting files.

Item 150 of 620 (Exam B,Q135)
A security engineer is implementing FDE for all plops in an organization.Which of the following are the most important for the engineer to consider as part of the planning process?(Select two). A.Digital signatures
B.Data tokenization
C.Key escrow
D.Certificate authority linking
E.Public key management
F.TPM presence

Item 151 of 620 (Exam B,Q136)
Which of the folowing actions could a security engineer take to ensure workstations and servers are property monitored for unauthorized changes and software?
A.Configure all systems to log scheduled tasks.
B.Collect and monitor all traffic exiting the network.
C.Install endpoint management software on all systems.
D.Block traffic based on known malicious signatures.

Item 152 of 620 (Exam B,Q137)
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: msp 23 192-160.14.6aceipt cezhecjenoryption
PORT BTATE SERVICE REASON

/ eoaryplaye-aok

JTelnet server supports encryption
Which of the following would the security analyst conclude for this reported vulnerability?
A.It is a false positive.
B.A rescan is required.
C.Compensating controls exist.
D.It is considered noise.

Item 153 of 620 (Exam B,Q138)
Which of the following describes the maximum allowance of accepted risk?
A.Risk score
B.Risk indicator
C.Risk threshold
D.Risk level

ltem 154 of 620(Exam B,Q139)
Which of the following IS the most common data loss path for an air-gapped network?
A.Removable devices
B.Bastion host
C.Unpatched OS
D.Unsecured Bluetooth

Item 155 of 620 (Exam B,Q140)
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.Email phishing
B.Executive whaling
C.Social engineering
D.Insider threat

Item 156 of 620 (Exam B,Q141)
A security analyst discovers a web shell on one of the company's public web servers.Which of the following would have helped the company discover this issue automatically?
A.IDS
B.FIM
C.WAF
D.DLP

ltem 157 of 620 (Exam B,Q142)
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.Hashing
B.Symmetric
C.Salting

D.Asymmetric

Item 158 of 620(Exam B,Q143)

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.Warm

C.Geographically dispersed

D.Cold

Item 159 of 620 (Exam B,Q144)

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 foilowing best describes the tool the administrator is using?

A.SCAP

B.SNMP traps

C.DLP

D.IPS

Item 160 of 620 (Exam B,Q145)

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.Execute the code in a sandbox.

B.Generate a hash of the files.

C.Search the executable for ASCII strings.

D.Validate the code signature.

Item 161 of 620 (Exam B,Q146)

A security analyst inspects the following log: html H77P/1. Q822E/110

200 9080

00100

Which of the following was attempted?

A.Command injection

B.Buffer overflow

C.Directory traversal

D.Privilege escalation

Item 162 of 620 (Exam B,Q147)

Mal grant to migrate its infrastructure to an off-premises solution. Which of the following should be considered first?

A.Ability of engineers

B.Security of architecture

C.Cost of implementation

D.Security of cloud providers

Item 163 of 620 (Exam B,Q148)

Employees who work remotely have reported network speed issues. A help desk technician asked an employee to look up the public P address on a designated website, and it matched the data cntr ad

Which of the following types of tunnels is most likely being used for this VPN connection?

A.Layer 2 tunnel

B.IPSec tunnel
C.Full tunnel
D.Split tunnel

Item 164 of 620 (Exam B,Q149)
A company's security policy states that only the production servers should have bidirectional internet access Which of the following needs to be configured to comply with this policy?
A.MDM server
B.Firewall rule
C.DLP policy
D.URL filter

Item 165 of 620(Exam B,Q150)
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.EAP
C.SAML
D.OpenID

Item 166 of 620 (Exam B,Q151)
During a wireless network scan at a data center,the IT security team discovered Wi-Fi signals broadcasting from an unknown device. Which of the following best describes the cause of the incident?
A.Domain hijacking
B.Rogue access point
C.Jamming
D.On-path attack

Item 167 of 620 (Exam B,Q152)
In order to save on expenses, Company A and Company B agree to host each other's compute and storage disaster recovery sites at their primary data centers. The two data centers are about a mile apart, and they each have their own power source.When necessary,one company will escort the other company to its data center.Which of the following is the greatest risk with this arrangement?
A.The data center sites are not geographically dispersed.
B.A redundant power source for disaster recovery is lacking.
C.The physical security resources are shared.
D.In an emergency,escorted access may not be timely enough.

Item 168 of 620 (Exam B,Q153)
An administrator is reviewing a single server's security logs and discovers the following:
Keywords Date and Time Source
Event ID Task Category
- - -
02022
Agdie
Miaronot
Legen
Pailure
211123:05 AM
Windows aecurity

Audit
09/16/2022
Microsor
4625 Logon
Failut 東 O11:13:07
Windove aecuzity
Audie
09/16/2022
Microsoft
4625
Logon
Fatlure
49213:09 AK
Windows Secusicy
Audie
09/16/2022 Miorosof
4625
Logon
Paituse
31:13:11 AM
Windows seeurity
Audie
09/16/2022
CMLCro2016)
4625
Legon
Falluze
11:13:13 AM
Windows security
Audit
09/16/2022
Microsoft
4625
Logon
Failure 1013:15 AM windows security udir309/16/2022 Micxonoft
4625
Eogon
Wa12dze
12:13:17 AM
Windoss security
Addie
09/16/2022
Microssto
4625 Logen
Fatlun 型
11:13:19 AM
Windowa security
Audie
09/16/2022
Microsoft
4625

Logon
Fallure 10:13:21 AM
wilyiovs serurity
Audit309/3672022 Microsoto
4625
Oggen
EAi1ure
20:13:23 AM/ Windows sepurity
Audie
09/16/2022
4625
Logen
8312030650T
Falluze
11:13:25 AM
Addie
09/16/2022
MIcrosott
4625
Logon
Failure
13:27 AM
Windows security
Which of the following best describes the action captured in this log file?
A.Forgotten password by the user
B.Brute-force attack
C.Failed password audit
D.Privilege escalation

Item 169 of 620 (Exam B,Q154)
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? (Select two).
A.TPM presence
B.Data tokenization
C.Certificate authority linking
D.Digital signatures
E.Key escrow
F.Public key management

Item 170 of 620 (Exam B,Q155)
An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of.ryxk.Which of the following types of infections is present on the systems?
A.Spyware
B.Mirus
C.Trolan
D.Ransomware

Item 171 of 620 (Exam B,Q156)
Which of the following phases of an incident response involves generating reports?
A.Preparation
B.Containment
C.Lessons learned

D.Recovery

Item 172 of 620 (Exam B,Q157)
A systems administrator would like to set up a system that will make it difficult or impossible to deny that someone has performed an action.which of the following is the administrator trying t accomplish? A.Adaptive ldentity
B.Deception and disruption
C.Non-repudiation
D.Security zones

Item 173 of 620 (Exam B,Q158)
When decommissioning physical hardware that contains Pll, a financial institution requires that a third-party recycling company wipe and destroy the hard drives,and document the process.Which of the following best describes this procedure?
A.Sanitization
B.Data retention
C.Certification
D.Destruction

Item 174 of 620 (Exam B,Q159)
Which of the following is considered a preventive control?
A.Log correlation
B.Configuration auditing
C.Incident alerts
D.Segregation of duties

Item 175 of 620 (Exam B,Q160)
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.Passive
B.Defensive
C.Physical
D.Offensive

Item 176 of 620 (Exam B,Q161)
An organization wants to ensure the integrity of compiled binaries in the production environment.Which of the folowing security measures would best support this objective?
A.Static analysis
B.SQL injection
C.Code signing
D.Input validation

Item 177 of 620 (Exam B,Q162)
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.Confidentiality
C.Integrity
D.Availability

Item 178 of 620 (Exam B,Q163)

A Chief Information Security Officer wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigations if an attack occurs. The company uses SSL decryption to allow traffic monitoring.Which of the following strategies would best accomplish this goal?
A.Enabling full packet capture for traffic entering and exiting the servers
B.Deploying network traffic sensors on the same subnet as the servers
C.Logging endpoint and OS-specific security logs
D.Logging all NetFlow traffic into a SIEM

Item 179 of 620 (Exam B,Q164)
Which of the following alert types is the most likely to be ignored over time?
A.True positive
B.False negative
C.True negative
D.False positive

Item 180 of 620 (Exam B,Q165)
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 wil most likely be classified?(Select two). A.Urgent
B.Public
C.Restricted
D.Operational
E.Private
F.Confidential

Item 181 of 620(Exam B,Q166)
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.SLE
B.RTO
C.ALE
D.RPO
E.ARO

Item 182 of 620 (Exam B,Q167)
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.Integrated
B.Partially known environment
C.Unknown environment
D.Known environment

Item 183 of 620 (Exam B,Q168)
A bank set up a new server that contains customers' Pll. Which of the following should the bank use to make sure the sensitive data is not modified?
A.User behavior analytics
B.File integrity monitoring
C.Network access control
D.Full disk encryption

Item 184 of 620 (Exam B,Q169)

An organization is leveraging a VPN between its headquarters and a branch location.Which of the folowing is the VPN protecting?
A.Geographic restrictions
B.Data sovereignty
C.Data in use
D.Data in transit

Item 185 of 620 (Exam B,Q170)
A security analyst is investigating an alert that was produced by endpoint protection software. The analyst determines this event was a false positive triggered by an employee who attempted to download a file.
Which of the following is the most likely reason the download was blocked?
A.A misconfiguration in the endpoint protection software
B.A zero-day vulnerability in the file
C.A supply chain attack on the endpoint protection vendor
D.Incorrect file permissions

Item 186 of 620 (Exam B,Q171)
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.Salting
B.Certificates
C.Algorithms
D.Hashes

Item 187 of 620 (Exam B,Q172)
Which of the following steps is performed with the goal of improving the incident response process?
A.Containment
B.Detection
C.Recovery
D.Lessons learned

Item 188 of 620 (Exam B,Q173)
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 prevent a single point of failure
B.To identify complexity
C.To reduce implementation cost
D.To remediate technical debt

Item 189 of 620 (Exam B,Q174)
Which of the following best ensures minimal downtime and data loss for organizations with critical computing equipment located in earthquake-prone areas?
A.High availability networking
B.Generators and UPS
C.Redundant cold sites
D.Off-site replication

Item 190 of 620 (Exam B,Q175)
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.Jump server

B.Proxy server
C.RDP server
D.Hypervisor

Item 191 of 620 (Exam B,Q176)
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
B.Managerial
C.Operational
D.Technical

Item 192 of 620 (Exam B,Q177)
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.Attestation
C.Internal audit
D.External examination

Item 193 of 620 (Exam B,Q178)
A systems administrator is advised that an external web server is not functioning properly.The administrator reviews the following firewall logs containing traffic going to the web server:
3043 1 413490 1501313198014105og
23-01-25 01+35)09.102 98.123.45.100-4540
23.45.101/1101787540010-20:7
Which of the following attacks is likely occurring?
A.Brute-force
B.Directory traversal
C.DDoS
D.HTTPS downgrade

Item 194 of 620 (Exam B,Q179)
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.Procurement process
B.Asset inventory
C.Network enumeration
D.Data certification

Item 195 of 620 (Exam B,Q180)
A company would like to provide employees with computers that do not have access to the internet in order to prevent information from being leaked to an online forum.Which of the following would be best for the systems administrator to implement?
A.Jump server
B.Virtualization
C.Air gap
D.Logical segmentation

Item 196 of 620(Exam B,Q181)

Which of the following provides the details about the terms of a test with a third-party penetration tester?
A.Supply chain analysis
B.Right to audit clause
C.Rules of engagement
D.Due diligence

Item 197 of 620 (Exam B,Q182)
An administrator is creating a server that cannot be shared with any other organizations. The administrator also wants to ensure that the company retains control over the infrastructure.Which of the following cloud architectures should the administrator choose?
A.Private
B.Public
C.Hybrid
D.Community

Item 198 of 620 (Exam B,Q183)
An administrator discovers that some files on a database server were recently encrypted.The administrator sees from the security logs that the data was last accessed by a domain user.Which of the following best describes the type of attack that occurred?
A.Insider threat
B.Watering-hole
C.Social engineering
D.Unauthorized attacker

Item 199 of 620 (Exam B,Q184)
A security engineer needs to configure an NGFW to minimize the impact of the increasing number of various traffic types during attacks.Which of the following types of rules is the engineer the most likely to configure?
A.Agent-based
B.Behavioral-based
C.URL-based
D.Signature-based

Item 200 of 620 (Exam B,Q185)
A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:
1 Something you know
2 Something you have
3.Something you are
Which of the following would accomplish the manager's goal?
A.Domain name,PKI,GeolP lookup
B.Password,authentication token,thumbprint
C.VPN IP address,company ID,facial structure
D.Company URL,TLS certificate,home address

Item 201 of 620 (Exam B,Q186)
Which of the following provides the details about the terms of a test with a third-party penetration tester?
A.Due diligence
B.Supply chain analysis
C.Right to audit clause
D.Rules of engagement

Item 202 of 620 (Exam B,Q187)

An administrator is creating a server that cannot be shared with any other organizations.The administrator also wants to ensure that the company retains control over the infrastructure.Which of the folowing cloud architectures should the administrator choose?
A.Private
B.Public
C.Hybrid
D.Community

Item 203 of 620 (Exam B,Q188)
An administrator discovers that some files on a database server were recently encrypted.The administrator sees from the security logs that the data was last accessed by a domain user.which of the following best describes the type of attack that occurred?
A.Social engineering
B.Insider threat
C.Unauthorized attacker
D.Watering-hole

Item 204 of 620 (Exam B,Q189)
A network manager wants to protect the company's VPN by implementing multifactor authentication that uses 1 Something you know
2 Something you have
3. Something you are
Which of the following would accomplish the manager's goal?
A.Domain name,PKI,GeolP lookup
B.VPN IP address,company ID,facial structure
C.Password,authentication token,thumbprint
D.Company URL,TLS certificate,home address

Item 205 of 620 (Exam B,Q190)
A security engineer needs to configure an NGFW to minimize the impact of the increasing number of various traffic types uring attacks.Which of the following types of rules is the engineer the most likely to configure?
A.Behavioral-based
B.Signature-based
C.URL-based
D.Agent-based

Item 206 of 620 (Exam B,Q191)
A systems administrator is changing the password policy within an enterprise environment and wants this update implemented I on all systems as quickly as possible.Which of the following operating system security measures will the administrator most likely use?
A.Enabling PAP
B.Updating EDR profiles
C.Deploying PowerShell scripts
D.Pushing GPO update

Item 207 of 620 (Exam B,Q192)
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.Tertiary
B.Warm
C.Cold

D.Hot

Item 208 of 620(Exam B,Q193)
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.Default credentials
B.Business email
C.Social engineering
D.Unsecured network

Item 209 of 620 (Exam B,Q194)
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 descnibe?
A.Vishing
B.Smishing
C.Pretexting
D.Phishing

Item 210 of 620(Exam B,Q195)
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.Gap
B.Static
C.Impact
D.Dynamic

Item 211 of 620(Exam B,Q196)
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.NGFW
B.Load balancer
C.Port security
D.IPS

Item 212 of 620 (Exam B,Q197)
In order to strengthen a password and prevent a hacker from cracking it,a randlom string of 36 characters was added to the password. Which of the following best describes this technique?
A.Salting
B.Data masking
C.Key stretching
D.Tokenization

Item 213 of 620 (Exam B,Q198)
Which of the following is the best way to secure an on-site data center against intrusion from an insider?
A.Access badge
B.Motion sensor
C.Video surveillance
D.Bollards

Item 214 of 620 (Exam B,Q199)
A company hired a security manager from outside the organization to lead security operations.Which of the following actions should the security manager perform first in this new role?
A.Perform a user ID revalidation.
B.Review security policies.
C.Establish a security baseline
D.Adopt security benchmarks.

Item 215 of 620 (Exam B,Q200)
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.Transport layer security
B.Port security
C.Web application firewall
D.Virtual private network

Item 216 of 620 (Exam B,Q201)
A security analyst is investigating an application server and discovers that software on the server is behaving abnormally.The software normally runs batch jobslocally 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.Race condition
B.Side loading
C.Memory injection
D.SQL injection

Item 217 of 620 (Exam B,Q202)
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
B.True negative
C.True positive
D.False negative

Item 218 of 620 (Exam B,Q203)
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?
(Select two).
A.Key escrow
B.TPM presence
C.Data tokenization
D.Digital signatures
E.Public key management
F.Certificate authority linking

Item 219 of 620 (Exam B,Q204)
Users at a company reported that one of the company's VPN tunnels was not functioning.Security analysts discovered that traffic to the VPN tunnel was being redirected to a malicious IP address to caplure log-in credentials.Whlch of the fcllowing security measures should have been the first step in preventing this attack?
A.Patching the VPN servers to the latest version
B.Enabling MFA for DNS admin accounts

C.Using honeypots to detect network attacks
D.Deploying updates to VPN agents sooner

Item 220 of 620 (Exam B,Q205)
Which of the following threat vectors is most commonly utilized by insider threat actors alternating data exfiltration?
A.Spear phishing emails
B.Unidentified removable evices
C.Impersonation of business units through typo squatting
D.Default network device credentials

Item 221 of 620 (Exam B,Q206)
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.Database
C.Full disk
D.Asymmetric

Item 222 of 620 (Exam B,Q207)
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.Availability
B.Ease of deployment
C.Scalability
D.Cost

Item 223 of 620 (Exam B,Q208)
Which of the following should a systems administrator set up to increase the resilience of an application by splitting the traffic between two identical sites?
A.Geographic disruption
B.Parallel processing
C.Failover
D.Load balancing

Item 224 of 620 (Exam B,Q209)
A security manager crested 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.Review the docurnents' data classification policy.
B.Set the maximum data retention policy.
C.Securely store the documents on an air-gapped network.
D.Conduct a tabletop exercise with the team.

Item 225 of 620 (Exam B,Q210)
Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?
A.Escalating permission requests
B.Provisioning resources
C.Disabling access
D.Reviewing change approvals

Item 226 of 620(Exam B,Q211)
A technician is deploying a new security camera.Which of the following should the technician do?

A.Disable unnecessary ports.
B.Conduct a site survey.
C.Perform a vulnerability scan.
D.Configure the correct VLAN.

Item 227 of 620(Exam B,Q212)
Which of the following should a security operations center use to improve its incident response procedure?
A.Frameworks
B.Playbooks
C.Baselines
D.Benchmarks

Item 228 of 620 (Exam B,Q213)
Which of the following control types should be used to identify an unauthorized log-in to the network?
A.Detective
B.Directive
C.Corrective
D.Preventive

Item 229 of 620 (Exam B,Q214)
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.External audit
C.Insider threat
D.Phishing campaign

Item 230 of 620 (Exam B,Q215)
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?(Select two).
A.Corrective
B.Directive
C.Deterrent
D.Preventive
E.Compensating
F.Detective

Item 231 of 620 (Exam B,Q216)
A company recognizes that most employees own smartphones and do not want to carry a Separate company phone to access work-related emails.The company would like to set up a program that allows employees to install special software on personal phones in order to access company email. Which of the following is the company setting up?
A.SCAP
B.RTOS
C.BYOD
D.COPE

Item 232 of 620 (Exam B,Q217)
An organization is required to maintain financial data records for three years and customer data for five years.Which of the following data management policies should the organization implement?
A.Certification

B.Inventory
C.Retention
D.Destruction

Item 233 of 620 (Exam B,Q218)
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.Side loading
B.Jailbreaking
C.Cross-site scripting
D.SQLI

Item 234 of 620(Exam B,Q219)
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.Connecting the remote server to the domain and increasing the password length
B.Setting up a VPN and placing the jump server inside the firewall
C.Using a proxy for web connections from the reote desktop server
D.Changing the remote desktop port to a non-standard number

Item 235 of 620 (Exam B,Q220)
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.Executing regular phishing campaigns
B.Implementing insider threat detection measures
C.Updating processes for sending wire transfers
D.Standardizing security incident reporting

Item 236 of 620 (Exam B,Q221)
A security administrator is configuring fileshares.The administrator removed the default permissions and added permissions for only users who will need to access the fileshares as part of their job duties.Which of the following best describes why the administrator performed these actions?
A.Encryption standard compliance
B.Data replication requirements
C.Access control monitoring
D.Least privilege

Item 237 of 620 (Exam B,Q222)
Which of the following would most likely be used by attackers to perform credential harvesting?
A.Social engineering
B.Rainbow table
C.Third-party software
D.Supply chain compromise

Item 238 of 620 (Exam B,Q223)
Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?
A.Buffer overflow
B.VM escape
C.SQL injection
D.Race condition

Item 239 of 620(Exam B,Q224)
A security administrator identifies an application that is storing data using MD5. Which of the following best identifies the vulnerability likely present in the application?
A.Malicious update
B.Zero day
C.Cryptographic
D.Side loading

Item 240 of 620 (Exam B,Q225)
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.SCADA
C.NFC
D.Wired

Item 241 of 620 (Exam B,Q226)
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.Mean time to repair
B.Recovery time objective
C.Mean time between failures
D.Recovery point objective

Item 242 of 620 (Exam B,Q227)
An organization is required to maintain financial data records for three years and customer data for five years.Which of the folowing data management policies should the organization implement?
A.Inventory
B.Retention
C.Certification
D.Destruction

Item 243 of 620 (Exam B,Q228)
A cyber operations team informs a security analyst about a new tactic maliciousactors are using to compromise networks.SIM alerts have not yet been configured. Which of the following best describes what the security analyst should do to identify this behavior?
A.Threat hunting
B.Digital forensics
C.Incident response
D.E-discovery

Item 244 of 620 (Exam B,Q229)
Which of the following best describes configuring devices to log to an off-site location for possible future reference?
A.Log aggregation
B.Archiving
C.SCAP
D.DLP

Item 245 of 620 (Exam B,Q230)

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
B.Approval procedure
C.Test procedure
D.Impact analysis

Item 246 of 620 (Exam B,Q231)
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.Data exfiltration
B.Shadow IT
C.Nation-state attack
D.Espionage

Item 247 of 620 (Exam B,Q232)
Which of the following would be the best way to handle a critical business application that is running on a legacy server?
A.Hardening
B.Decommissioning
C.Segmentation
D.Isolation

Item 248 of 620 (Exam B,Q233)
A systems administrator receivers 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:
BerverName Conpections CUEH)| Pead/o writee/
E11e5eV01
12019906901 50k3/g1 10088/3
Which of the following indicators most likely triggered this alert?
A.Network saturation
B.Resource consumption
C.Account lockout
D.Concurrent session usage

Item 249 of 620 (Exam B,Q234)
Which of the following security concepts is accomplished with the installation of a RADIUS server?
A.AAA
B.ACL
C.CIA
D.PEM

Item 250 of 620 (Exam B,Q235)
Which of the following would be used to detect an employee who is emailing a customer list to a personal account before leaving the company?
A.EDR
B.FIM
C.DLP
D.IDS

Item 251 of 620(Exam B,Q236)
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.TGT
B.IPSec
C.RSA
D.SHA-1

Item 252 of 620 (Exam B,Q237)
During a recent breach, employee credentials were compromised when a service desk employee issued an MFA bypass code to an attacker who called and posed as an employee.Which of the following should be used to prevent this type of incident in the future?
A.Biometrics
B.Hardware token MFA
C.Least privilege
D.Identity proofing

Item 253 of 620 (Exam B,Q238)
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.Conduct a tabletop exercise with the team.
C.Review the documents' data classification policy.
D.Securely store the documents on an air-gapped network.

Item 254 of 620 (Exam B,Q239)
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.lllumination tool

ltem 255 of 620 (Exam B,Q240)
Which of the following security controls is most likely being used when a critical legacy server is segmented into a private network?
A.Preventive
B.Compensating
C.Deterrent
D.Corrective

Item 256 of 620 (Exam B,Q241)
After performing an assessment,an analyst wants to provide a risk rating for the findings. Which of the following concepts should most likely be considered when calculating the ratings?
A.Owners and thresholds
B.Impact and likelihood
C.Appetite and tolerance
D.Probability and exposure factor

Item 257 of 620 (Exam B,Q242)

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
B.Certificates
C.Salting
D.Algorithms

Item 258 of 620 (Exam B,Q243)
Which of the following describes the category of data that is most impacted when it is lost?
A.Private
B.Critical
C.Public
D.Confidential

Item 259 of 620 (Exam B,Q244)
Which of the following activities is included in the post-incident review phase?
A.Reestablishing the compromised system's configuration and settings
B.Developing steps to mitigate the risks of the incident
C.Validating the accuracy of the evidence collected during the investigation
D.Determining the root cause of the incident

Item 260 of 620 (Exam B,Q245)
An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Select two).
A.Disable default accounts.
B.Join the server to the corporate domain.
C.Send server logs to the SIEM.
D.Remove unnecessary services
E.Document default passwords.
F.Add the server to the asset inventory

Item 261 of 620 (Exam B,Q246)
Which of the following agreement types defines the time frame in which a vendor needs to respond?
A.MOA
B.SLA
C.MOU
D.SOW

Item 262 of 620 (Exam B,Q247)
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.URL scanning
B.Policy review
C.End user training
D.Plain text email

Item 263 of 620 (Exam B,Q248)
Which of the following penetration testing teams is focused only on trying to compromise an organization using an attacker's tactics?
A.Red

B.Blue
C.White
D.Purple

Item 264 of 620(Exam B,Q249)
Which of the following most impacts an administrator's ability to address CVEs discovered on a server? A.Risk tolerance
B.Patch availability
C.Organizational impact
D.Rescanning requirements

Item 265 of 620(Exam B,Q250)
Which of the following would most likely mitigate the impact of an extended power outage on a company's environment?
A.SOAR
B.UPS
C.Hot site
D.Snapshots

Item 266 of 620 (Exam B,Q251)
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
C.SD-WAN utilizing IPSec
D.UTM utilizing a threat feed

Item 267 of 620 (Exam B,Q252)
A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware,which laid dormant for multiple weeks,across the network.Which of the following would have mitigated the spread?
A.UAT
B.IDS
C.IPS
D.WAF

Item 268 of 620 (Exam B,Q253)
A company is decommissioning its physical servers and replacing them with an architecture that wil reduce the number of individual operating systems.Which of the following strategies should the company use to achieve this security requirement?
A.Virtualization
B.Microservices
C.Infrastructure as code
D.Containerization

Item 269 of 620 (Exam B,Q254)
Which of the following risks can be mitigated by HTTP headers?
A.SSL
B.DoSJ
C.XSS
D.SQLi

Item 270 of 620 (Exam B,Q255)
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.Simulated threats
B.Phishing awareness
C.Insider threat detection
D.Business continuity planning

Item 271 of 620 (Exam B,Q256)
An IT technician receives notification that users are unable to connect to network resources at the company's remote site. The remote site is located in a multitenant office building. The company uses an 802.11 enterprise network for Wi-Fi connections. The IT technician arrives at the remote site and observes an open Wi-Fi SSID that is identical to the company's official SSID. Which of the following best describes this type of attack?
A.User credential replay
B.Resource inaccessibility
C.On-path rogue access point
D.Application forgery

Item 272 of 620 (Exam B,Q257)
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.$10,000
B.$30,000
C.$7,500
D.$15,000

Item 273 of 620 (Exam B,Q258)
Which of the following metrics is used to quantify the severity of a vulnerability according to the cvss?(Select two).
A.Probability of impact
B.Environmental score
C.Temporal score
D.Exploitability
E.Remediation effort
F.Confidence level

Item 274 of 620 (Exam B,Q259)
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.Insider threat
B.DDoS attack
C.Supply chain
D.Rogue employee

Item 275 of 620 (Exam B,Q260)
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 control
B.Version changes
C.Version updates
D.Version validation

Item 276 of 620 (Exam B,Q261)
The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?
A.Data exfiltration
B.Shadow IT
C.Service disruption
D.Insider threat

Item 277 of 620 (Exam B,Q262)
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.Provide a third-party attestation report.
B.to Hire a vendor to perform a penetration test.
C.Perform an annual self-assessment.
D.Allow each client the right to audit.

Item 278 of 620 (Exam B,Q263)
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 folowing best describes this type of vulnerability?
A.Race condition
B.Malicious update
C.Side loading
D.Memory injection

Item 279 of 620 (Exam B,Q264)
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.Segmentation
B.Tokenization
C.Hashing
D.Obfuscation

Item 280 of 620 (Exam B,Q265)
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.Windows security
C.ACL
D.Firewall

Item 281 of 620 (Exam B,Q266)
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.Placing the system in an isolated VLAN
B.Decommissioning the system
C.Instaling HIDS on the system
D.Encrypting the system's hard drive

Item 282 of 620 (Exam B,Q267)

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.VPN
B.NGFW
C.Security zone
D.Proxy server

Item 283 of 620 (Exam B,Q268)
Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?
A.Tabletop exercise
B.Capacity planning
C.Continuity of operations
D.Parallel processing

Item 284 of 620 (Exam B,Q269)
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.Non-repudiation
B.Integrity
C.Avallability
D.Confidentiality

Item 285 of 620(Exam B,Q270)
Which of the following is the incident response process phase in which the goals to prevent future security incidents?
A.Eradication
B.Containment
C.Recovery
D.Collection of evidence
E.Lessons learned

Item 286 of 620 (Exam B,Q271)
Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?
A.To continuously the monitor hardware inventory
B.To hunt for active attackers in the network
C.To find shadow IT cloud deployments
D.To track the status of patching installations

Item 287 of 620 (Exam B,Q272)
Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?
A.EDR
B.IDS
C.ACL
D.NAC

Item 288 of 620 (Exam B,Q273)
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.Attestation
C.GDPR
D.Due diligence

Item 289 of 620 (Exam B,Q274)
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 wil most likely be required to take?
A.Retain the emails between the security team and affected customers for 30 days.
B.Retain all emails from the company to affected customers for an indefinite period of time.
C.Retain any communications related to the security breach until further notice.
D.Retain any communications between security members during the breach response.

Item 290 of 620 (Exam B,Q275)
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.Masking
B.Tokenization
C.Encryption
D.Hashing

Item 291 of 620(Exam B,Q276)
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.DLP
B.DMARC
C.XDR
D.SPF

Item 292 of 620 (Exam B,Q277)
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

Item 293 of 620 (Exam B,Q278)
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.Real-time operating system
B.Virtualization
C.Virtualization
D.Microservices

Item 294 of 620 (Exam B,Q279)
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
B.Change management

C.Disaster recovery
D.Physical security

Item 295 of 620 (Exam B,Q280)
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.Active
B.Audit
C.Monitor
D.Sensor

Item 296 of 620 (Exam B,Q281)
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.Implement security awareness training.
B.Deploy muitifactor authentication.
C.Update the acceptable use policy
D.Decrease the level of the web filter settings.

Item 297 of 620(Exam B,Q282)
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.Vishing
C.Impersonating
D.Phishing

Item 298 of 620 (Exam B,Q283)
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? (Select two).
A.Network
B.System
C.Authentication
D.Application
E.Error
F.Firewall

Item 299 of 620 (Exam B,Q284)
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.Masking
C.Obfuscation
D.Tokenization

Item 300 of 620 (Exam B,Q285)
Which of the following considerations is the most important for an organization to evaluate as it establishes and maintains a data privacy program?
A.Role as controller or processor
B.Request process for data subject access
C.Reporting structure for the data privacy officer
D.Physical location of the company

Item 301 of 620 (Exam B,Q286)
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
B.MOA
C.MOU
D.BPA

Item 302 of 620 (Exam B,Q287)
Which of the following should a security team do first before a new web server goes live?
A.Harden the virtual host.
B.Create WAF rules.
C.Apply patch management.
D.Enable network intrusion detection.

Item 303 of 620(Exam B,Q288)
Which of the following is a risk of conducting a vulnerability assessment?
A.Finding security gaps in the system
B.Unauthorized access to the system
C.Reports of false positives
D.A disruption of business operations

Item 304 of 620 (Exam B,Q289)
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.Contractual implications
B.Fines
C.Sanctions
D.Reputational damage

Item 305 of 620 (Exam B,Q290)
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? (Select two).
A.Certificate revocation list
B.WAF
C.Honeypot
D.NIDS
E.HIPS
F.SIEM

Item 306 of 620 (Exam B,Q291)
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.EAP
C.SD-WAN
D.IPSec

Item 307 of 620 (Exam B,Q292)
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.Report the breach to the local authorities.
B.Implement vulnerability scanning of the company's systems.
C.Notify the applicable parties of the breach.
D.Identify the attacker's entry methods.

Item 308 of 620 (Exam B,Q293)
An organization with multiple geographic locations has invested in various internet circuits at each location, including MPLS,4G/5G,broadband,and dial-up. An architect is configuring a solution that wil allow locations to function consistently and leverage links based on specific criteria.Which of the following is the best solution for the architect to configure?
A.UTM
B.SASE
C.VPN
D.SD-WAN

Item 309 of 620 (Exam B,Q294)
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.Due diligence
B.Attestation
C.Penetration testing
D.Internal audit

Item 310 of 620 (Exam B,Q295)
Which of the following describes effective change management procedures?
A.Approving the change after a successful deployment
B.Using an automatic change control bypass fosecurity updates
C.Having a backout plan when a patch fails
D.Using a ticket system for tracking changes

Item 311 of 620 (Exam B,Q296)
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.UTM
B.NGFW
C.WAF
D.Layer 4 firewall

Item 312 of 620 (Exam B,Q297)
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.Least privilege
B.Time of day
C.Role-based

D.Discretionary

Item 313 of 620 (Exam B,Q298)
A legal department must maintain a backup from all devices that have been shredded and recycled boy a third party.Which of the folowing best describes this requirement?
A.Destruction
B.Data retention
C.Certification
D.Sanitization

Item 314 of 620 (Exam B,Q299)
Which of the following hardening techniques should be done to newly purchased devices to reduce attack surfac
A.Using configuration enforcement
B.Removing unnecessary software
C.Implementing a host-based firewall
D.Installing endpoint protection

Item 315 of 620(Exam B,Q300)
Which of the following topics would most likely be included within an organization's SDLC?
A.Penetration testing methodology
B.Service-level agreements
C.Information security policy
D.Branch protection requirements

Item 316 of 620 (Exam B,Q301)
A security researcher just disclosed a critical vulnerability.Prior to the disclosure of the vulnerability, the vendor was not aware that it was present in the product. Which of the following describes this type of vulnerability?
A.Race condition
B.Zero-day
C.Logic bomb
D.Time-of-check

Item 317 of 620 (Exam B,Q302)
Which of the folowing organizational documents is most often used to establish and communicate expectations associated with integrity and ethical behavior within an organization?
A.MOA
B.EULA
C.SLA
D.AUP

Item 318 of 620 (Exam B,Q303)
Which of the following is used to conceal credit card information in a database log file?
A.Hashing
B.Masking
C.Obfuscation
D.Tokenization

Item 319 of 620 (Exam B,Q304)
A systems administrator is reviewing a recent environment intrusion. Which of the following logs is the first place the administrator should look to find evidence of the intrusion using network-based indicators of compromise?
A.IPS/IDS

B.CASB
C.Application
D.Endpoint

Item 320 of 620 (Exam B,Q305)
A security architect wants to prevent employees from receiving malicious attachments by email.
Which of the following functions should the chosen solution do?
A.Scan email traffic inline.
B.Apply IP address reputation data.
C.Check SPF records.
D.Tap and monitor the email feed.

Item 321 of 620 (Exam B,Q306)
Which of the following would be the best solution to deploy a low-cost standby site that includes hardware and internet access?
A.Cold site
B.Hot site
C.Recovery site
D.Warm site

Item 322 of 620 (Exam B,Q307)
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.0 :012 10183
Deny 10.9.8.14/27 to 0.0.0.0/0 B.
Permit 10.2.2.0/24 to 10.9.8.14/27
B.Permit 10.3.9.0/24 to 10.9.8.14/27 Deny 9-9-0.0/0 50
C. 10.9.8.14/27 mie 10:2 2.7/32 0 1003.8.14/27
Pezmi: 1013.9.9/32 to 10.9.8.14/27
Deny 0.0.0.0/0 to 10.9.8.14/27
D. Deny 0.0.0.0/0 to 10.9.6.14/27
Permit 10.2.2.0/24 to 10.9.8.14/27
Permit 10.3.9.0/24 to 10.9.8.14/27

Item 317 of 620 (Exam B,Q302)
Which of the folowing organizational documents is most often used to establish and communicate expectations associated with integrity and ethical behavior within an organization?
A.MOA
B.EULA
C.SLA
D.AUP

Item 318 of 620 (Exam B,Q303)
Which of the following is used to conceal credit card information in a database log file?
A.Hashing
B.Masking
C.Obfuscation
D.Tokenization

Item 319 of 620 (Exam B,Q304)

A systems administrator is reviewing a recent environment intrusion. Which of the following logs is the first place the administrator should look to find evidence of the intrusion using network-based indicators of compromise?
A.IPS/IDS
B.CASB
C.Application
D.Endpoint

Item 320 of 620 (Exam B,Q305)
A security architect wants to prevent employees from receiving malicious attachments by email.
Which of the following functions should the chosen solution do?
A.Scan email traffic inline.
B.Apply IP address reputation data.
C.Check SPF records.
D.Tap and monitor the email feed.

Item 321 of 620 (Exam B,Q306)
Which of the following would be the best solution to deploy a low-cost standby site that includes hardware and internet access?
A.Cold site
B.Hot site
C.Recovery site
D.Warm site

Item 322 of 620 (Exam B,Q307)
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.0 :012 10183
Deny 10.9.8.14/27 to 0.0.0.0/0 B.
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 9-9-0.0/0 50
C. 10.9.8.14/27 mie 10:2 2.7/32 0 1003.8.14/27 Pezmi: 1013.9.9/32 to 10.9.8.14/27
Deny 0.0.0.0/0 to 10.9.8.14/27
D. Deny 0.0.0.0/0 to 10.9.6.14/27
Permit 10.2.2.0/24 to 10.9.8.14/27
Permit 10.3.9.0/24 to 10.9.8.14/27

Item 328 of 620 (Exam B,Q313)
Which of the following control types is AUP an example of?
A.Technical
B.Physical
C.Managerial
D.Operational

Item 329 of 620 (Exam B,Q314)
An employee used a company's biling 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.Firewall logs
B.Application logs
C.IDS/IPS logs
D.Vulnerability scanner logs

Item 330 of 620 (Exam B,Q315)
Which of the following is 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 encryption
B.Open public ledger
C.Public key infrastructure
D.Key escrow

Item 331 of 620 (Exam B,Q316)
Asystems 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.Nation-state attack
B.Espionage
C.Data exfiltration
D.Shadow IT

Item 332 of 620 (Exam B,Q317)
Which of the following should an organization use to protect its environment from external attacks conducted by an unauthorized hacker?
A.HIDS
B.NIPS
C.ACL
D.IDS

Item 333 of 620 (Exam B,Q318)
Which of the following is a compensating control for providing user access to a high-risk website?
A.Blocking that website on the endpoint protection software
B.Setting firewall rules to allow traffic from any port to that destination
C.Enabling threat prevention features on the firewall
D.Configuring a SIEM tool to capture all web traffic

Item 334 of 620 (Exam B,Q319)
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.Highly available
C.Air-gapped
D.Containerized

Item 335 of 620 (Exam B,Q320)
Whichof the following threat actors would most likely deface the website of a high-profile music group?
A.Unskilled attacker
B.Nation-state
C.Organized crime
D.Insider threat

Item 336 of 620 (Exam B,Q321)
A company has a website with a huge database.The company wants to ensure that a DR site could be brought online quickly in the event of a failover, and end users would miss no more than 30 minutes of data.

Which of the following should the company do to meet these objectives? A.Store the nightly full backups at the DR site.
B.Build a content caching system at the DR site.
C.Implement real-time replication for the DR site.
D.Increase the network bandwidth to the DR site

Item 337 of 620 (Exam B,Q322)
An employee who was working remotely lost a mobile device containing company da Which of the following provides the best solution to prevent future data loss?
A.DLP
B.FDE
C.EDR
D.MDM

Item 338 of 620 (Exam B,Q323)
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 will the engineer team most likely configure?
A.Federation
B.SAML
C.LDAP
D.OAuth

Item 339 of 620 (Exam B,Q324)
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 Which of the following should the analyst do next? A.Search the web server for ransomware notes.
B.Scan the database server for malware.
C.Review WAF logs for evidence of command injection.
D.Check for recently terminated DBAs.

Item 340 of 620 (Exam B,Q325)
Which of the following best describes a hacktivist's motivation?
A.Financial gain
B.Surveillance of individuals
C.Espionage of state secrets
D.Political influence

Item 341 of 620 (Exam B,Q326)
Which of the following data states applies to data that is being actively processed by a database server?
A.At rest
B.In use
C.Being hashed
D.In transit

Item 342 of 620 (Exam B,Q327)
Which of the following would be the most appropriate way to protect data in transit?
A.AES-256
B.TLS 1.3
C.SHA-256
D.SSL 3.0

Item 343 of 620 (Exam B,Q328)
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
C.Privacy officer
D.Owner

Item 344 of 620(Exam B,Q329)
Which of the following are activities that should be completed during the containment phase of the incident response process? (Select two).
A.Analyzing the incident
B.Restoring the system
C.Removing the malicious threat
D.ldentifying the threat actor
E.Developing a recovery plan
F.Notifying stakeholders

lItem 345 of 620(Exam B,Q330)
A penetration tester, who did not have an access badge, managed to follow a group of employees through multiple badged-access doors and into the data center without being stopped.The tester mentions this finding during the after-action review with the Chief Information Security Officer (CISO). Which of the following issues should the CISO address as a result of this finding?
A.Role-based access
B.Insider threat
C.Shoulder surfing
D.Social engineering

Item 346 of 620 (Exam B,Q331)
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 target of?
A.Vishing
B.Smishing
C.Phishing
D.Whaling

Item 347 of 620(Exam B,Q332)
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 s in place in order for the organization to follow security best practices?
A.Network segmentation
B.Virtualization and isolation of resources
C.Strong authentication policies
D.Data encryption

Item 348 of 620 (Exam B,Q333)
For which of the a following reasons would a systems administrator leverage a 3DES hash from an installer file that is posted on a vendor's website?
A.To activate the license for the file
B.To validate the authenticity of the file
C.To calculate the checksum of the file

D.To test the integrity of the file

Item 349 of 620 (Exam B,Q334)
While surveilling a facility, a penetration tester notices that a particular employee tends to place their access badge in their jacket pocket when leaving the facility.Which of the following can the penetration tester use to gain access to the facility based on the employee's actions?
A.Logic bomb
B.On-path attack
C.Brute force
D.RFID cloning

Item 350 of 620 (Exam B,Q335)
A security analyst is investigating an incident in which a workstation was redirecting to malicious websites. The analyst suspects that the hosts file was modifed to include mapping to malicious URLs.Which of the following logs should the analyst use to confirm that the file was modified?
A.Application
B.Firewall
C.IDS
D.Endpoint

Item 351 of 620 (Exam B,Q336)
Which of the following is a benefit of vendor diversity?
A.Patch availability
B.Zero-day resiliency
C.Load balancing
D.Secure configuration guide applicability

Item 352 of 620 (Exam B,Q337)
A company is aware of a given security risk and chooses not to accept responsibility.Which of the following describes this risk management strategy?
A.Transfer
B.Exemption
C.Avoid
D.Exception

Item 353 of 620 (Exam B,Q338)
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 negative
B.True negative
C.True positive
D.False positive

Item 354 of 620 (Exam B,Q339)
The security team of placeholder.com advises the organization to buy several new web domains,including placeholdes.com,placeholders.com,and placeholdez.com.Which of the following attack vectors is the security team trying to prevent?
A.Typosquatting
B.Watering hole
C.Vishing
D.Pretexting

Item 355 of 62 (Exam B,Q340)

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

Item 356 of 620 (Exam B,Q341)
Which of the following tasks is typically included in the BIA process?
A.Evaluating the risk management plan
B.Developing the incident response plan
C.Identifying the communication strategy
D.Establishing the backup and recovery procedures
E.Estimating the recovery time of systems

Item 357 of 620 (Exam B,Q342)
A security administrator observed the following in a web server log while investigating an incident:

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

Which of the following attacks did the security administrator most likely see?
DA.Credential replay
B.Privilege escalation
C.Brute force
D.Directory traversal

Item 358 of 620 (Exam B,Q343)
Which of the following tools is best for logging and monitoring in a cloud environment?
A.NAC
B.AIPS
C.SIEM
D.FIM

Item 359 of 620 (Exam B,Q344)
Which of the following security measures is required when using a cloud-based platform for loT management?
A.Encrypted connection
B.Firewall
C.Single sign-on
D.Federated identity

Item 360 of 620 (Exam B,Q345)
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?(Select two).
A.Authentication
B.Database
C.Network
D.Firewall
E.Application
F.DHCP

Item 361 of 620 (Exam B,Q346)
Which of the following security measures is required when using a cloud-based platform for loT management?
A.Firewall

B.Single sign-on
C.Encrypted connection
D.Federated identity
Item 362 of 620 (Exam B,Q347)
Which of the following cryptographic solutions protects data at rest?
A.Full disk encryption
B.Steganography
C.Private key
D.Digital signatures

Item 363 of 620 (Exam B,Q348)
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.Simulation
B.Replication
C.Snapshot
D.Containerization

Item 364 of 620 (Exam B,Q349)
A systems administrator is working on a defense-in-depth strategy and needs to restrict activity from employees after hours.Which of the following should the systems administrator implement? A.Time-of-day restrictions
B.Mandatory restrictions
C.Role-based restrictions
D.Attribute-based restrictions

Item 365 of 620 (Exam B,Q350)
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
C.Isolating
D.Patching

Item 366 of 620 (Exam B,Q351)
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.Redundancy
B.Isolation
C.Virtualization
D.Segmentation

Item 367 of 620 (Exam B,Q352)
A company web server is initiating outbound traffic to a low-reputation, public IP on a nonstandard port. The web server is used to present an unauthenticated page to clients who upload images to the company.An analyst notices a suspicious process running on the server that was not created by the company development team Which of the following is the most likely explanation for this security incident?
A.A web shell has been deployed to the server through the page.
B.Malicious insiders are using the server to mine cryptocurrency.
C.Attackers have deployed a rootkit Trojan to the server over an exposed RDP port.
D.A vulnerability has been exploited to deploy a worm to the server.

Item 368 of 620 (Exam B,Q353)

Which of the following should an analyst consider when performing a business impact analysis?(Select two).
A.ARO
B.RPO
C.SLA
D.ALE
E.SLE
F.RTO

Item 369 of 620 (Exam B,Q354)
After falling an audit twice, an organization has been ordered by a movement regulatory agency to pay fines.Which of the following caused this action?
A.Contract violations
B.Government sanctions
C.Rules of engagement
D.Non-compliance

Item 370 of 620 (Exam B,Q355)
While reviewing incoming tickets, a security analyst notices that endpoint protection is out of date on a number of systems. Which of the following should the analyst confirm has been updated prior to marking the issue as resolved?
A.OS version
B.Sensor version
C.Firmware version
D.Engine version

Item 371 of 620 (Exam B,Q356)
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.Root of trust
B.Self-signed
C.Wildcard
D.Third-party

Item 372 of 620 (Exam B,Q357)
A user,who wants to watch a movie during a break at work, connects to a network switch using an Ethenet cable from a personal laptop. Which of the following security principles should be applied to best secure the company's infrastructure and prevent recurrence of this issue?
A.802.1Q
B.WAF
C.VPN
D.802.1X

Item 373 of 620(Exam B,Q358)
Which of the following methods to secure data provides the best protection for data at rest?
A.Encryption
B.Hashing
C.Obfuscation
D.Segmentation

Item 374 of 620 (Exam B,Q359)
Which of the following agreement types is used to limit external discussions?
A.MSA

B.BPA
C.SLA
D.NDA

Item 375 of 620 (Exam B,Q360)
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.Warm
C.Cold
D.Geographically dispersed

Item 376 of 620 (Exam B,Q361)
The Chief Information Security Officer (CISO) wants to add a section to the security training that details social engineering attacks against the company via telephone systems. Which of the following best describes the security topic the CISO wishes to address?
A.Smishing
B.Pretexting
C.Impersonation
D.Vishing

Item 377 of 620 (Exam B,Q362)
Which of the following examples would be best mitigated by input sanitization?
A.<script>alert("Warning!");</script>
B.Browser message:"Your connection is not private."
C.Email message:"Click this link to get your free gift card."
D.map-10.11.1.130

Item 378 of 620 (Exam B,Q363)
Which of the following threat actors is the most likely to seek financial gain through the use of ransomware attacks?
A.Insider threat
B.Nation-state
C.Hacktivists
D.Organized crime

Item 379 of 620 (Exam B,Q364)
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.Changing the default password
B.Assigning individual user IDs
C.Using least privilege
D.Reviewing logs more frequently

Item 380 of 620 (Exam B,Q365)
A security analyst is reviewing logs and discovers the following.
149.34.228.10--[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
B.Secure cookies
C.Static code analysis
D.Sandboxing

Item 381 of 620 (Exam B,Q366)
Which of the following is an important security feature that helps protect sensitive data when consolidating to a centralized architecture model?
A.Improved scalability
B.High availability
C.Network segmentation
D.Global access

Item 382 of 620 (Exam B,Q367)
Which of the following is a benefit of launching a bug bounty program? (Select two).
A.Reduced cost of managing the program
B.Increased security awareness for the workforce
C.Reduction in the number of zero-day vulnerabilities
D.Improved reputation for the organization
E.Quicker discovery of vulnerabilities
F.Improved patch management process

Item 383 of 620 (Exam B,Q368)
A university employee logged on to the academic server and attempted to guess the system administrators' log-in credentials.Which of the folowing security measures should the university have implemented to detect the employee's attempts to gain access to the administrators' accounts?
A.Firewall
B.User activity logs
C.Two-factor authentication
D.Intrusion prevention system

Item 384 of 620 (Exam B,Q369)
Which of the following would be the best way to test resiliency in the event of a primary power failure?
A.Tabletop exercise
B.Parallel processing
C.Simulation testing
D.Production failover

Item 385 of 620 (Exam B,Q370)
Which of the following techniques is used to assess the effectiveness of security controls that are designed to protect a system from unauthorized access?
A.Penetration test
B.Vulnerability scan
C.Risk assessment
D.Internal audit review

Item 386 of 620 (Exam B,Q371)
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.Avoid
B.Reject
C.Transfer
D.Accept

Item 387 of 620(Exam B,Q372)

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.Using password management
B.Providing situational awareness training
C.Reviewing email policies
D.Recognizing phishing

Item 388 of 620 (Exam B,Q373)
Which of the following activities are associated with vulnerability management?(Select two).
A.Prioritization
B.Containment
C.Reporting
D.Exploiting
E.Tabletop exercise
F.Correlation

Item 389 of 620 (Exam B,Q374)
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 adds additional guard rails
C.It removes technical debt.
D.It acts as a workforce multiplier.

Item 390 of 620 (Exam B,Q375)
A Chief Information Security Officer would like to conduct frequent,detailed reviews of systems and procedures to track compliance objectives. Which of the following is the best method to achieve this objective?
A.Penetration testing
B.Internal auditing
C.Third party attestation
D.Vulnerability scans

Item 391 of 620 (Exam B,Q376)
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.Access badges
B.Risk assessment
C.Password policy
D.Phishing campaign

Item 392 of 620 (Exam B,Q377)
Which of the following would most likely be deployed to obtain and analyze attacker activity and techniques?
A.Laver 3 switch
B.Firewall
C.Honeypot
D.IDS

Item 393 of 620 (Exam B,Q378)
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.Antivirus

B.Firewall
C.Application
D.IDS

Item 394 of 620 (Exam B,Q379)
Which of the following should an internal auditor check for first when conducting an audit of the organization's risk management program?
A.Business impact analysis
B.Policies and procedures
C.Vulnerability assessment
D.Asset management

Item 395 of 620 (Exam B,Q380)
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.Reputational damage
D.Fines

Item 396 of 620 (Exam B,Q381)
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.EDR
B.NAC
C.DIP
D.UBA

Item 397 of 620 (Exam B,Q382)
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.Sandbox
B.Endpoint detection and response
C.Antivirus
D.Intrusion prevention system

Item 398 of 620 (Exam B,Q383)
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.Select an ldP.
C.Create Auth tokens.
D.Use password vaulting

Item 399 of 620 (Exam B,Q384)
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 folowingbest meets the company's needs?
A.IPS
B.IAM

C.WAF
D.SASE

Item 400 of 620 (Exam B,Q385)
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.CRL
B.SCEP
C.CSR
D.OCSP

Item 401 of 620 (Exam B,Q386)
Which of the following can be used to compromise a system that is running an RTOS?
A.Memory injection
B.Replay attack
C.Ransomware
D.Cross site scripting

Item 402 of 620 (Exam B,Q387)
Which of the following is the best security reason for closing service ports that are not needed?
A.To eliminate false positives from a vulnerability scan
B.To reduce a system's attack surface
C.To improve a system's resource utilization
D.To mitigate risks associated with unencrypted traffic

Item 403 of 620 (Exam B,Q388)
Which of the following objectives is best achieved by a tabletop exercise?
A.Deciding red and blue team rules of engagement
B.Conducting multiple security investigations in parallel
C.Familiarizing participants with the incident response process
D.Quickly determining the impact of an actual security breach

Item 404 of 620 (Exam B,Q389)
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.Data sovereignty
B.Data segmentation
C.Geographic restrictions
D.Geographic dispersion

Item 405 of 620 (Exam B,Q390)
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
D.Complexity

Item 406 of 620 (Exam B,Q391)
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.SOL injection
B.VM escape
C.Password spraying
D.Tokenization E.TOC/TOU

Item 407 of 620 (Exam B,Q392)
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.Penetration testing
B.Network scanning
C.Configuration auditing
D.Open-source intelligence

Item 408 of 620 (Exam B,Q393)
The executive management tear 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.Warm site
C.Cold site
D.Failover site

Item 409 of 620 (Exam B,Q394)
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
B.Replication
C.Smishing
D.Phishing

Item 410 of 620 (Exam B,Q395)
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.SQL injection
B.Resource reuse
C.Target of evaluation
D.Side loading

Item 411 of 620 (Exam B,Q396)
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

Item 412 of 620(Exam B,Q397)
An administrator is installing an sol 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 root certificate is installed
B.If the wildcard certificate is configured
C.If the public key is configured

D.If the certificate signing request is valid

Item 413 of 620 (Exam B,Q398)
A company handles sensitive data and needs to securely transfer it to other organizations using a digital medium. Which of the following should the company implement to best ensure a secure data transfer?
A.Hashing
B.Obfuscation
C.Masking
D.Encryption

Item 414 of 620 (Exam B,Q399)
Which of the following should a company use to provide proof of external network security testing?
A.Vulnerability assessment
B.Supply chain analysis
C.Third-party attestation
D.Business impact analysis

Item 415 of 620 (Exam B,Q400)
A company plans to secure its systems by:
1 Preventing users from sending sensitive data over corporate email
2 Restricting access to potentially harmful websites
Which of the following features should the company set up?(Select two).
A.DNS filtering
B.DLP software
C.Guardrails
D.Antivirus signatures
E.File integrity monitoring
F.Stateful firewall

Item 416 of 620 (Exam B,Q401)
Which of the following most accurately describes the order in which a security engineer should implement secure baselines?
A.Establish,deploy,maintain
B.Establish,maintain, deploy
C.Deploy,maintain,establish
D.Deploy,establish,maintain

Item 417 of 620 (Exam B,Q402)
Which of the following would a systems administrator follow when upgrading the firmware of an organization's router?
A.Software development life cycle
B.Certificate signing request
C.Risk tolerance
D.Maintenance window

Item 418 of 620 (Exam B,Q403)
Which of the following activities is the first stage in the incident response process?
A.Detection
B.Verification
C.Containment
D.Declaration

Item 419 of 620 (Exam B,Q404)
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.Security procedure evaluation
B.Gap analysis
C.Policy review
D.Threat scope reduction

Item 420 of 620 (Exam B,Q405)
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.Network access control
B.Time-based access control
C.Digital rights management
D.Role-based access control

Item 421 of 620 (Exam B,Q406)
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.IDS
D.Network taps

Item 422 of 620 (Exam B,Q407)
Which of the following would enable a data center to remain operational through a multiday power outage?
A.Parallel processing
B.Uninterruptible power supply
C.Replication
D.Generator

Item 423 of 620 (Exam B,Q408)
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.EAP B.RAS
C.PAM
D.SAML

Item 424 of 620 (Exam B,Q409)
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.Transport Layer Security
B.Security zones
C.Proxy server
D.Port security

Item 425 of 620 (Exam B,Q410)
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.
B.Create incident response and disaster recovery plans.
C.Purchase and install security software.

D.Develop and provide training on data protection policies.

Item 426 of 620 (Exam B,Q411)
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.Vishing
B.Spear phishing
C.Impersonation
D.Business email compromise

Item 427 of 620 (Exam B,Q412)
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.Restrict internet access for the employees who disclosed credentials.
B.Block all outbound traffic from the intranet.
C.Introduce a campaign to recognize phishing attempts
D.Implement a deny list of websites.

Item 428 of 620 (Exam B,Q413)
Which of the following is a preventive physical security control?
A.Alarm system
B.Video surveillance system
C.Bollards
D.Motion sensors

Item 429 of 620 (Exam B,Q414)
Which of the following architectures is most suitable to provide redundancy for critical business processes?
A.Multitenant
B.Cloud-native
C.Network-enabled
D.Server-side

Item 430 of 620 (Exam B,Q415)
Which of the following security concepts is being followed when implementing a product that offers protection against DDoS attacks?
A.Confidentiality
B.Integrity
C.Availability
D.Non-repudiation

Item 431 of 620 (Exam B,Q416)
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.Centralized proxy
B.URL scanning
CC.Content categorization
D.Agent-based

Item 432 of 620 (Exam B,Q417)
A company installed cameras and added signs to alert visitors that they are being recorded. Which of the following controls did the company implement? (Select two).
A.Corrective
B.Technical
C.Detective
D.Directive
E.Deterrent
F.Preventive

Item 433 of 620 (Exam B,Q418)
Which of the following is a feature of a next-generation SIEM system?
A.Automated response actions
B.Vulnerability scanning
C.Security agent deployment
D.Virus signatures

Item 434 of 620 (Exam B,Q419)
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.Encryption
B.Data masking
C.Tokenization
D.Obfuscation

Item 435 of 620 (Exam B,Q420)
Which of the following allows an exploit to go undetected by the operating system?
A.Side loading
B.Firmware vulnerabilities
C.Encrypted payloads
D.Memory injection

Item 436 of 620 (Exam B,Q421)
A security analyst learms that an attack vector,which was used as a part of a recent incident,was a well-known loT 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.Firewall
B.Application
C.Endpoint
D.NAC

Item 437 of 620 (Exam B,Q422)
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.Warm site
B.Cold site
C.Failover site
D.Hot site

Item 438 of 620(Exam B,Q423)

While reviewing logs, a security admiistrator identifies the following code: <

script>function(send_info)</script>

Which of the following best describes the vulnerability being exploited?
A.CSRF B.DDoS
C.XSS
D.SQLi

Item 439 of 620 (Exam B,Q424)
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.Escape to host
C.Valid accounts
D.Process injection

Item 440 of 620 (Exam B,Q425)
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.Attestation of compliance
C.Self-assessment findings
D.Third-party audit report

Item 441 of 620 (Exam B,Q426)
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 public key is configured
C.If the certificate signing request is valid
D.If the root certificate is installed

Item 442 of 620(Exam B,Q427)
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.Preventive
B.Detective
C.Directive
D.Corrective

Item 443 of 620 (Exam B,Q428)
Which of the following is the primary reason why false negatives on a vulnerability scan should be a concern?
A.The system has vulnerabilities,and a patch has not yet been released
B.The system has vulnerabilities that are not being detected
C.Vulnerabilities with a lower severity will be prioritized over critical vulnerabilities
D. The time to remediate vulnerabilities that do not exist is excessive

Item 444 of 620 (Exam B,Q429)
A vendor salesperson is a personal friend of a company's Chief Financial Officer (CFO).The company recently made a large purchase from the vendor,which was directly approved by the CFO.Which of the following best describes this situation?
A.Contractual impact
B.Conflict of interest
C.Reputational damage
D.Due diligence
E.Rules of engagement

Item 445 of 620 (Exam B,Q430)
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.Sanitization
B.Certification
C.Data retention
D.Destruction

Item 446 of 620 (Exam B,Q431)
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? (Select two).
A.Performing regular vulnerability scans
B.Encrypting sensitive data at rest and in transit
C.Implementing strong password policies
D.Regularly updating server software and patches
E.Removing payment information from the servers
F.Utilizing a web-application firewall

Item 447 of 620 (Exam B,Q432)
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.LDAP
B.FTP
C.RADIUS
D.VPN

Item 448 of 620 (Exam B,Q433)
Which of the following is the primary purpose of a service that tracks log-ins and time spent using the service?
A.Availability
B.Authentication
C.Accounting
D.Authorization

Item 449 of 620 (Exam B,Q434)
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.SASE
B.CASB

C.IPS
D.SIEM

Item 450 of 620 (Exam B,Q435)
Which of the following cryptographic solutions is used to hide the fact that communication is occurring? A.Data masking
B.Steganography
C.Tokenization
D.Private key

Item 451 of 620 (Exam B,Q436)
Which of the following elements of digital forensics should a company use if it needs to ensure the integrity of evidence?
A.E-discovery
B.Preservation
C.Acquisition
D.Containment

Item 452 of 620 (Exam B,Q437)
Which of the following allows a systems administrator to tune permissions for a file?
A.Least privilege
B.Access control list
C.Patching
D.Configuration enforcement

Item 453 of 620 (Exam B,Q438)
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? (Select two).
A.SSH tunneling
B.Segmentation
C.Data masking
D.Patch installation
E.Cryptographic downgrade
F.Tokenization

Item 454 of 620 (Exam B,Q439)
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.Sanctions
B.Right to be forgotten
C.External compliance reporting
D.Attestation

Item 455 of 620 (Exam B,Q440)
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.Unencrypted data can be read by a user who is in a separate environment
C.Users can install software that is not on the manufacturer's approved list.
D.An attacker can access the hypervisor and compromise other VMs.

Item 456 of 620 (Exam B,Q441)
Which of the following objectives is clustering most likely to achieve?
A.Balancing load
B.Increasing performance
C.Facilitating backups
D.Creating hot sites

Item 457 of 620 (Exam B,Q442)
An organization wants to donate its aging network hardware.Which of the following should the organization perform to prevent any network details from leaking?
A.Sanitization
B.Data retention
C.Certification
D.Destruction
Answer:A

Item 458 of 620 (Exam B,Q443)
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.Risk appetite
B.Mean time between failure
C.Recovery point objective
D.Risk tolerance
E.Recovery time objective

Item 459 of 620 (Exam B,Q444)
A security engineer proposes a Layer 7 firewall solution. Which of the following best describes the capabilities that the security engineer must meet?
A.Perform application inspection and block unwanted traffic.
B.Protect cloud-based workloads and ensure data integrity.
C.Maintain a stateful traffic table and reduce network utilization.
D.Monitor host-based network activity and respond to alerts.

Item 460 of 620 (Exam B,Q445)
A penetration tester examined the security posture of a company.The tester completed the following:
1.Checked the locks on perimeter doors
2 Located blind spots on security cameras
3 Attempted to open secured server rack doors
Which of the following describes the type of test the penetration tester most likely conducted?
A.Defensive
B.Offensive
C.Physical
D.Compliance

Item 461 of 620 (Exam B,Q446)
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.Network access control
B.Host-based firewalls
C.Network allow list
D.Anti-malware solutions

E.Intrusion prevention systems

Item 462 of 620(Exam B,Q447)
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
B.Deletion
C.Recycling
D.Shredding

Item 463 of 620 (Exam B,Q448)
Which of the following should an organization focus on the most when making decisions about vulnerability prioritization?
A.CVSS
B.Industry impact
C.CVE
D.Exposure factor

Item 464 of 620 (Exam B,Q449)
Which of the following provides the best protection against unwanted or insecure communications to and from a device?
A.Intrusion detection system
B.Host-based firewall
C.System hardening
D.Anti-malware software

Item 465 of 620 (Exam B,Q450)
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.Virtualization
B.Microservices
C.Containers
D.Real-time operating system

Item 466 of 620 (Exam B,Q451)
Which of the following best describe the benefits of a microservices architecture when compared to a monolithic architecture?(Select two.) A.Easier debugging of the system
B.Stronger authentication of the system
C.Reduced cost of ownership of the system
D.Increased compartmentalization of the system
E.Reduced complexity of the system
F.Improved scalability of the system

Item 467 of 620 (Exam B,Q452)
A company recently set up a system for employees to access their files remotely. However, the IT team has noticed that some employees are using personal devices to access the system.Which of the following security techniques could help mitigate the risk of unauthorized connections?
A.ACL
B.2FA
C.IPS
D.SIEM

Item 468 of 620 (Exam B,Q453)

Which of the following types of vulnerabilities is primarily caused by improper use and management of cryptographic certificates?
A.Resource reuse
B.Weak cipher suites
C.Misconfiguration
D.Insecure key storage

Item 469 of 620 (Exam B,Q454)
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.Phishing campaign
C.Risk assessment
D.Access badges

Item 470 of 620(Exam B,Q455)
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.Least privilege
B.Role-based
C.Biometric authentication
D.Time-of-day restrictions

Item 471 of 620 (Exam B,Q456)
Which of the following cryptographic solutions is used to hide the fact that communication is occurring?
A.Steganography
B.Tokenization
C.Data masking
D.Private key

Item 472 of 620 (Exam B,Q457)
Which of the following should be considered before implementing a SIEM tool?(Select two).
A.Integration of the SIEM with other systems
B.Installation of the SIEM infrastructure
C.Types of data the tool can ingest
D.Automation of the alerts
E.Prioritization of the information
F.Amount of data the tool can process

Item 473 of 620 (Exam B,Q458)
Which of the following activities uses OSINT?
A.Collecting evidence of malicious activity
B.Producing IOC for malicious artifacts
C.Social engineering testing
D.Data analysis of logs

Item 474 of 620 (Exam B,Q459)
Which of the following strategies should an organization use to efficiently manage and analyze multiple types of logs?
A.Deploy a SIEM solution.

B.Install a unified threat management appliance.
C.Implement EDR technology.
D.Create custom scripts to aggregate and analyze logs.

Item 475 of 620 (Exam B,Q460)
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.Access control lists
B.Identity and access management
C.Network intrusion detection system
D.Behavioral analytics

Item 476 of 620 (Exam B,Q461)
An administrator must replace an expired SSL certificate.Which of the following does the administrator need to create the new SSL certificate?
A.CRL
B.OCSP
C.Key
D.CSR

Item 477 of 620 (Exam B,Q462)
A company discovers that an employee was paid by a competitor to save internal business files to a thumb drive and deliver it to the competitor. Which of the following is most likely the employee's motivation?
A.Blackmail
B.Revenge
C.Data exfiltration
D.Financial gain

Item 478 of 620 (Exam B,Q463)
Which of the following would best prevent a vehicle from crashing into a data center?
A.Bollards
B.Fencing
C.Video camera
D.Body of water

Item 479 of 620 (Exam B,Q464)
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.Failover site
B.Warm site
C.Hot site
D.Cold site

Item 480 of 620 (Exam B,Q465)
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 allow for business insurance to be purchased
C.To ensure that errors are not passed to other systems
D.To prevent unauthorized changes to financial data

Item 481 of 620 (Exam B,Q466)
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
C.Green
D.Red

Item 482 of 620 (Exam B,Q467)
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 extend the length of time data can be retained
C.To automate the reduction of duplicated data
D.To determine the impact in the event of a breach

Item 483 of 620(Exam B,Q468)
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.Containerization
B.FIM
C.MDM
D.DLP

Item 484 of 620 (Exam B,Q469)
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.ICS
B.laaS
C.laC
D.loT

Item 485 of 620 (Exam B,Q470)
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.A WO had not been mutually approved.
B.A SOW had not been agreed to by the client.
C.The MOU had basic clauses from a template.
D.A required NDA had not been signed.

Item 486 of 620 (Exam B,Q471)
Which of the following aspects of the data management life cycle is most directly impacted by local and international regulations?
A.Sanitization
B.Destruction
C.Certification
D.Retention

Item 487 of 620 (Exam B,Q472)
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.Espionage
B.Blackmail
C.Organized crime
D.Philosophical beliefs

Item 488 of 620 (Exam B,Q473)
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? (Select two).
A.WAF
B.MFA
C.Local administrative password
D.Perimeter network
E.Jump server
F.VPN

Item 489 of 620 (Exam B,Q474)
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.An MDM solution with conditional access
B.A jump host in the shared services security zone
C.An SSH server within the corporate LAN
D.A reverse proxy on the firewall

Item 490 of 620 (Exam B,Q475)
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.Change management procedure
B.Acceptable use policy
C.Business continuity plan
D.Software development life cycle policy

Item 491 of 620 (Exam B,Q476)
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.Incident response
B.Penetration test
C.Geographic dispersion
D.Tabletop exercise

Item 492 of 620 (Exam B,Q477)
Which of the following types of identification methods can be performed on a deployed application during runtime?
A.Code review
B.Bug bounty
C.Dynamic analysis
D.Package monitoring

Item 493 of 620 (Exam B,Q478)

A company sets up strict access controls for sensitive data. Employees in different departments have different levels of access,and managers must approve all requests. Which of the following describes this type of access control?
A.Mandatory
B.Attribute-based
C.Role-based
D.Discretionary

Item 494 of 620 (Exam B,Q479)
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.Accept
B.Transfer
C.Avoid
D.Reject

Item 495 of 620 (Exam B,Q480)
A company is increasing its security standards and wants to monitor and record authorized access.Which of the folowing should the company implement to best meet these requirements?
A.CCTV
B.Gate guards
C.Smart cards
D.Fencing

Item 496 of 620 (Exam B,Q481)
A systems administrator needs to update systems without disrupting operations.Which of the following should the systems administrator and company leadership agree upon?
A.Backout plan
B.Impact analysis
C.Maintenance window
D.Standard operating procedure
Answer:C

Item 497 of 620 (Exam B,Q482)
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.Hybrid
B.Cloud-based
C.Peer-to-peer
D.On-premises

Item 498 of 620 (Exam B,Q483)
In an effort to reduce costs, a company is implementing a strategy that gives employees access to internal company resources,including email,from personal devices.Which of the following strategies is the company implementing?
A.COPE
B.CYOD
C.BYOD
D.MDM

Item 499 of 620(Exam B,Q484)
A customer has a contract with a CSP and wants to identify which controls should be implemented in the laaS enclave.Which of the following is most likely to contain this information?
A.Responsibility matrix
B.Service-level agreement
C.Statement of work
D.Master service agreement

Item 500 of 620 (Exam B,Q485)
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.Reporting suspicious emails
D.Segmentation

Item 501 of 620 (Exam B,Q486)
Which of the following aspects of the data management life cycle is most directly impacted by local and international regulations?
A.Certification
B.Retention
C.Sanitization
D.Destruction

Item 502 of 620 (Exam B,Q487)
Which of the following options will provide the lowest TO and RPO for a database?
A.On-site backups
B.Snapshots
C.Journaling
D.Hot site

Item 503 of 620 (Exam B,Q488)
Which of the following actors attacking an organization is the most likely to be motivated by personal beliefs?
A.Hacktivist
B.Nation-state
C.Organized crime
D.Insider threat

Item 504 of 620 (Exam B,Q489)
Which of the following should a security team use to document persistent vulnerabilities with related recommendations?
A.Compliance report
B.Audit report
C.Penetration test
D.Risk register

Item 505 of 620 (Exam B,Q490)
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.Enabling HTTP administration
B.Generating local administrator accounts

C.Replacing Telnet with SSH
D.Configuring centralized logging

Item 506 of 620 (Exam B,Q491)
Which of the following describes the procedures a penetration tester must follow while conducting a test?
A.Rules of execution
B.Rules of engagement
C.Rules of acceptance
D.Rules of understanding

Item 507 of 620 (Exam B,Q492)
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:
3000/
Which of the following indicators most likely triggered this alert?
A.Concurrent session usage
B.Network saturation
C.Account lockout
D.Resource consumption

Item 508 of 620 (Exam B,Q493)
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.Watering hole
B.Typosquatting
C.Spear-phishing attachment
D.Infected website

Item 509 of 620 (Exam B,Q494)
A user is receiving an account is locked out" error message when trying to log in to a laptop.
Authentication logs reveal the following messages:
110:00:00 AMI Login rejecced-usernameyjsmith-pasaword Monday
110:00:01 00 100im rejectad-usernace zonach-pasnvord Mondayz
110:00:01 A41CLoodn rejected -/usernaze jsslth-pasavord Monday3
110:00:02 AM) Login rejectedusernaneanith-passvord Monday4
AI0:00:03 AM Login rejected usernane jmith-pasmvord
Which of the following attacks is currently occurring?
A.Directory traversal
B.Brute-force
C.DDoS
D.Privilege escalation

Item 510 of 620 (Exam B,Q495)
Which of the following attacks exploits a potential vulnerability as a result of using weak cryptographic algorithms?
A.Password cracking
B.On-path
C.Digital signing
D.Side-channel

Item 511 of 620(Exam B,Q496)
Which of the following is prevented by proper data sanitization?
A.Devices reaching end-of-life and losing support
B.Disclosure of sensitive data through incorrect classification
C.Hackers' ability to obtain data from used hard drives
D.Incorrect inventory data leading to a laptop shortage

Item 512 of 620 (Exam B,Q497)
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.Access control list
B.Permission restrictions
C.Hashing
D.Input validation

Item 513 of 620 (Exam B,Q498)
Which of the following is most likely to be used as a just-in-time reference document within a security operations center?
A.Risk profile
B.Playbook
C.SIEM profile
D.Change management policy

Item 514 of 620 (Exam B,Q499)
Which of the following can be used to compromise a system that is running an RTOS?
A.Memory injection
B.Cross-site scripting
C.Replay attack
D.Ransomware

Item 515 of 620 (Exam B,Q500)
A nation-state attacker gains access to the email accounts of several journalists by compromising a website that the journalists frequently use. Which of the following types of attacks describes this example?
A.On-path
B.Brand impersonation
C.Typosquatting
D.Watering-hole

Item 516 of 620 (Exam B,Q501)
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.Known exploits
C.Insider threats
D.End-of-life support

Item 517 of 620 (Exam B,Q502)
An organization has decided that devices connected to on-premises networks must meet specific requirements related to OS patch level, antivirus version, and device types before being able to access internal resources.Which of the following solutions will the organization most likely implement?
A.XDR
B.DMARC

C.EDR
D.NAC

Item 518 of 620(Exam B,Q503)
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 egard to risk management activities?
A.RPO
B.MTTR
C.BIA
D.ARO

Item 519 of 620 (Exam B,Q504)
Which of the following analysis methods allows an organization to measure the exposure factor associated with organizational assets?
A.Trend-based
B.Quantitative
C.User-driven
D.Heuristic

Item 520 of 620 (Exam B,Q505)
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.Requiring a statement each week that no exceptions were noted
B.Including the date and person who reviewed the information in a report
C.Adding automated alerting when anomalies occur
D.Masking the username in a report to protect privacy

Item 521 of 620 (Exam B,Q506)
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.FDE
C.ECC
D.HSM

Item 522 of 620 (Exam B,Q507)
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.Security questions and a one-time passcode sent via email
B.Smart card with PIN and password
C.Voice and fingerprint verification with an SMS one-time passcode
D.Mobile application-generated,one-time passcode with facial recognition

Item 523 of 620(Exam B,Q508)
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.Web application firewalls

B.Multifactor authentication
C.Enabling encryption of customer data
D.Regular patching of servers

Item 524 of 620 (Exam B,Q509)
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.Journaling
C.Masking
D.Hashing

Item 525 of 620 (Exam B,Q510)
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.NIDS
D.DMARC

Item 526 of 620 (Exam B,Q511)
Which of the following steps should be taken before mitigating a vulnerability in a production server?
A.Refer to the change management policy.
B.Perform a risk assessment to classify the vulnerability.
C.Use the IR plan to evaluate the changes.
D.Escalate the issue to the SDLC team.

Item 527 of 620(Exam B,Q512)
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.WAF
B.Reverse proxy
C.NAC
D.URL scanning
Item 528 of 620 (Exam B,Q513)
While a user reviews their email, a host gets infected by malware that came from an external hard drive plugged into the host. The malware steals all the user's credentials stored in the browser. Which of the following training topics should the user review to prevent this situation from reoccurring?
A.Operational security
B.Social engineering
C.Removable media and cables
D.Password management

Item 529 of 620 (Exam B,Q514)
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.AUP
B.BCP
C.IRP
D.SDLC

Item 530 of 620 (Exam B,Q515)
Which of the following should a systems administrator use to decrease the company's hardware attack surface?
A.Virtualization
B.Isolation
C.Centralization
D.Replication

Item 531 of 620 (Exam B,Q516)
A security administrator is implementing encryption on all hard drives in an organization. Which of the following security concepts is the administrator applying?
A.Confidentiality
B.Authentication
C.Zero Trust
D.Integrity

Item 532 of 620 (Exam B,Q517)
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.On-path attack
B.Cross-site scripting
C.Zero-day exploit
D.SQL injection

Item 533 of 620 (Exam B,Q518)
A certificate authority needs to post information about expired certificates.Which of the following would accomplish this task?
A.PKI
B.CRL
C.TPM
D.CSR

Item 534 of 620 (Exam B,Q519)
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.Side loading
B.Cross-site scripting
C.Buffer overflow
D.Jailbreaking

Item 535 of 620 (Exam B,Q520)
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.Password spraying
B.On-path
C.SQL injection
D.Brute-force

Item 536 of 620 (Exam B,Q521)
Which of the following actions best addresses a vulnerability found on a company's web server?
A.Monitoring
B.Decommissioning
C.Patching

D.Segmentation

Item 537 of 620 (Exam B,Q522)
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.Government identification numbers
B.Software versions
C.List of board members
D.Office addresses

Item 538 of 620 (Exam B,Q523)
Which of the following describes the most effective way to address OS vulnerabilities after they are identified?
A.Patching
B.Removal of unnecessary software
C.Endpoint protection
D.Configuration enforcement

Item 539 of 620 (Exam B,Q524)
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.User provisioning
B.Security groups
C.Vertical scaling
D.Federation

Item 540 of 620 (Exam B,Q525)
Which of the following enables the ability to receive a consolidated report from different devices on the network?
A.IPS
B.Firewall
C.SIEM
D.DLP

Item 541 of 620 (Exam B,Q526)
Which of the following is an example of a data protection strategy that uses tokenization?
A.Removing sensitive data from production systems
B.Replacing sensitive data with surrogate values
C.Hashing sensitive data in critical systems
D.Encrypting databases containing sensitive data

ltem 542 of 620 (Exam B,Q527)
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.Sandboxo
B.Package monitoring
C.Static
D.Network traffic

Item 543 of 620 (Exam B,Q528)
A penetration test has demonstrated that domain administrator accounts were vulnerable to passthe-hash attacks.Which of the following would have been the best strategy to prevent the threat actor from using domain administrator accounts?

A.Use Group Policy to enforce password expiration B.Create IDS policies to monitor domain controller access
C.Implement a privileged access management solution.
D.Audit each domain administrator account weekly for password compliance

Item 544 of 620 (Exam B,Q529)
Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?
A.Adding a fake account to /etc/passwd
B.Creating a false text file in /docs/salaries
C.Setting weak passwords in /etc/shadow
D.Scheduling vulnerable jobs in /etc/crontab

Item 545 of 620 (Exam B,Q530)
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.Vulnerability scan
B.Endpoint logs
C.Packet capture
D.OS security logs

Item 546 of 620 (Exam B,Q531)
Which of the following is a use of CVSS?
A.To determine the cost associated with patching systems
B.To analyze code for defects that could be exploited
C.To identify unused ports and services that should be closed
D.To prioritize the remediation of vulnerabilities

Item 547 of 620 (Exam B,Q532)
Which of the following activities should be performed first to compile a list of vulnerabilities in an environment? A.Penetration testing
B.Threat hunting
C.Log aggregation
D.Adversarial emulation
E.Automated scanning

Item 548 of 620(Exam B,Q533)
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 alowing access to corporate resources?
A.Compliance attestation
B.Application vulnerability test
C.Penetration test
D.Device fingerprinting

Item 549 of 620 (Exam B,Q534)
Which of the following is the greatest advantage that network segmentation provides?
A.Decreased resource utilization
B.Security zones
C.End-to-end encryption
D.Enhanced endpoint protection
E.Configuration enforcement

Item 550 of 620 (Exam B,Q535)

When used with an access control vestibule,which of the following would provide the best prevention against tailgating?
A.CCTV
B.Access card
C.PIN
D.Security guard

Item 551 of 620 (Exam B,Q536)

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.Enabling encryption of customer data
C.Multifactor authentication
D.Web application firewalls
Item 552 of 620 (Exam B,Q537)
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

Item 553 of 620 (Exam B,Q538)
Which of the following enables the ability to receive a consolidated report from different devices on the network?
A.Firewall
B.SIEM
C.IPS
D.DLP

Item 554 of 620 (Exam B,Q539)
A systems administrator needs to encrypt all data on employee laptops. Which of the following encryption levels should be implemented?
A.File
B.Full disk
C.Volume
D.Partition

Item 555 of 620 (Exam B,Q540)
A penetration test reveals that users can easily access internal VLANs from the company's guest Wi-Fi. Which of the following security principles would help remediate this vulnerability?
A.Proxy server
B.802.1X authentication
C.VLAN ACLs
D.TLS

Item 556 of 620 (Exam B,Q541)
A company processes and stores sensitive data on its own systems.Which of the folowing steps should the company take first to ensure compliance with privacy regulations? A.Implement access controls and encryption.

B.Create incident response and disaster recovery plans.
C.Identify and understand relevant data protection requirements.
D.Purchase and install security software.

Item 557 of 620(Exam B,Q542)
The physical security team at a company receives reports that employees are not displaying their badges. The team also observes employees tailgating at controlled entrances. Which of the following topics will the security team most likely emphasize in upcoming security training?
A.Phishing
B.Social engineering
C.Acceptable use policy
D.Situational awareness

Item 558 of 620 (Exam B,Q543)
A user attempts to send an invoice to a customer. When the user follows up with the customer to see if the invoice was received, the customer informs the user that it went to the spam folder. The management team has asked the systems administrator to implement measures to reduce the likelihood of this happening again.Which of the following should the systems administrator implement?
A.DMARC
B.SPF
C.DNSSEC
D.XDR

Item 559 of 620 (Exam B,Q544)
A new employee accessed an unauthorized website.An investigation found that the empioyee violated the company's rules.Which of the following did the employee violate?
A.MOA
B.NDA
C.MOU
D.AUP

Item 560 of 620 (Exam B,Q545)
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.COPE
B.FDE
C.MDM
D.EDR

Item 561 of 620(Exam B,Q546)
Which of the following are examples of operational controls that would be appropriate to implement in an environment where financial processing activities occur?(Select two).
A.Key escrow
B.Dual control
C.Mandatory vacations
D.Access badge readers
E.Tokenization
F.Biometrics

Item 562 of 620 (Exam B,Q547)
Which of the following options will provide the lowest RTO and RPO for a database? A.Journaling

B.Snapshots
C.On-site backups
D.Hot site

Item 563 of 620 (Exam B,Q548)
Which of the following best protects sensitive data in transit across a geographically dispersed infrastructure?
A.Tokenization
B.Masking
C.Obfuscation
D.Encryption

Item 564 of 620 (Exam B,Q549)
A company's gate access logs show multiple entries from an employee's 1D badge within a twominute period. Which of the following is this an example of?
A.Side-channel attack
B.Tailgating
C.RFID cloning
D.Shoulder surfing

Item 565 of 620 (Exam B,Q550)
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.RFID keylogger
C.Firmware failure
D.Supply chain

Item 566 of 620 (Exam B,Q551)
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.Implement a new IPsec tunnel from internal resources.
B.Set up a WAP to allow internal access from public networks
C.Deploy an internal jump server to access resources
D.Configure firewall rules to block external access to internal resources.

Item 567 of 620(Exam B,Q552)
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.Due care and due diligence
C.Acknowledgement and attestation
D.Right to be forgotten

Item 568 of 620(Exam B,Q553)
Which of the following is the stage in an investigation when forensic images are obtained?
A.Reporting
B.Acquisition
C.E-discovery
D.Preservation

Item 569 of 620 (Exam B,Q554)

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.Replication
B.Load balancing
C.Proxy servers
D.Fault tolerance

Item 570 of 620 (Exam B,Q555)
Which of the following is the best way to validate the integrity and availability of a disaster recovery site?
A.Conduct a tabletop exercise
B.Develop requirements for database encryption.
C.Periodically test the generators:
D.Lead a simulated failover.

Item 571 of 620 (Exam B,Q556)
Which of the following would a security administrator use to comply with a secure baseline during a patch update?
A.Information security policy
B.Standard operating procedure
C.Service-level expectations
D.Test result report

Item 572 of 620 (Exam B,Q557)
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.RDP server
B.Jump server
C.Proxy server
D.Application server

Item 573 of 620 (Exam B,Q558)
A company's website is www.company.com.Attackers purchased the domain www.company.com Which of the following types of attacks describes this example?
A.Brand impersonation
B.On-path
C.Watering-hole
D.Typosquatting

Item 574 of 620 (Exam B,Q559)
Which of the following threat vectors would a user be vulnerable to when using a smartphone to scan a two-dimensional matrix barcode?
A.Quashing
B.Phishing
C.Smishing
D.Vishing

Item 575 of 620 (Exam B,Q560)
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?(Select two).

A.Cryptographic downgrade
B.Segmentation
C.Data masking
D.Tokenization
E.SSH tunneling
F.Patch installation

Item 576 of 620 (Exam B,Q561)
Which of the following security concepts is accomplished when granting access after an individual has logged into a computer network?
A.Authorization
B.Identification
C.Non-repudiation
D.Authentication

Item 577 of 620 (Exam B,Q562)
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

Item 578 of 620 (Exam B,Q563)
A company just received a notification about an exploit that has no current patch or fix. Which of the following describes this scenario?
A.On-path attack
B.Replay attack
C.Zero-day vulnerability
D.VM escape

Item 579 of 620 (Exam B,Q564)
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.Cross-site scripting
B.Buffer overflow
C.SQL injection
D.Zero-day

Item 580 of 620 (Exam B,Q565)
A Chief Information Security offcer (CISO)has developed information security policies that relate to the software development methodology.Which of the folowing 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

Item 581 of 620 (Exam B,Q566)
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

Item 582 of 620 (Exam B,Q567)
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
B.Intellectual property
C.Geolocation
D.Geographic restrictions

Item 583 of 620(Exam B,Q568)
A company plans to secure its systems by:
1.Preventing users from sending sensitive data over corporate email
2.Restricting access to potentially harmful websites
Which of the following features should the company set up?(Select two)
A.Stateful firewall
B.DNS filtering
C.Guardrails
D.Antivirus signatures
E.File integrity monitoring
F.DLP software

Item 584 of 620 (Exam B,Q569)
Which of the following are the best security controls for controlling on-premises access?(Select two) A.Picture ID
B.Phone authentication application
C.Camera
D.Biometric scanner
E.Swipe card
F.Memorable question

Item 585 of 620 (Exam B,Q570)
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,andconfirm that firewalls have updated policies to block unauthorized traffio.
B.Ensure only TLS and other encrypted protocols are selected for use on the network, and only permit authorized traffic via secure protocols.
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

Item 586 of 620 (Exam B,Q571)
While investigating a possible incident, a security analyst discovers the following:
Which of the following should the analyst do first?
A.Check the users table for new accounts.
B.Block brute-force attempts on temporary users.
C.Disable the guezy.php script.
D.implement a WAF.

Item 587 of 620 (Exam B,Q572)
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.Vulnerability assessment
B.Red teaming
C.Independent audit
D.Penetration testing

Item 588 of 620 (Exam B,Q573)
Which of the following best protects sensitive data in transit across a geographically dispersed infrastructure?
A.Tokenization
B.Encryption
C.Obfuscation
D.Masking

Item 589 of 620 (Exam B,Q574)
A company's gate access logs show multiple entries from an employee's 1D badge within a twominute period.Which of the following is this an example of?
A.Shoulder surfing
B.Tailgating
C.RFID cloning
D.Side-channel attack

Item 590 of 620(Exam B,Q575)
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.Firmware failure
C.RFID keylogger
D.Supply chain

Item 591 of 620(Exam B,Q576)
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.Implement a new IPsec tunnel from internal resources.
B.Configure firewall rules to block external access to internal resources.
C.Deploy an internal jump server to access resources
D.Set up a WAP to allow internal access from public networks

Item 592 of 620 (Exam B,Q577)
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.Due care and due diligence
C.Right to be forgotten
D.Acknowledgement and attestation

Item 593 of 620 (Exam B,Q578)
Which of the following is the stage in an investigation when forensic images are obtained? A.Preservation
B.E-discovery

C.Reporting
D.Acquisition

Item 594 of 620 (Exam B,Q579)
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
B.Fault tolerance
C.Proxy servers
D.Replication

Item 595 of 620 (Exam B,Q580)
Which of the following is the best way to validate the integrity and availability of a disaster recovery site?
A.Lead a simulated failover.
B.Conduct a tabletop exercise
C.Periodically test the generators:
D.Develop requirements for database encryption.

Item 596 of 620 (Exam B,Q581)
Which of the following would a security administrator use to comply with a secure baseline during a patch update?
A.Test result report
B.Service-level expectations
C.Information security policy
D.Standard operating procedure

Item 597 of 620 (Exam B,Q582)
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.Proxy server
B.Jump server
C.RDP server
D.Application server

Item 598 of 620 (Exam B,Q583)
A company's website is www.company.com.Attackers purchased the domain www.company.com Which of the following types of attacks describes this example?
A.Watering-hole
B.Brand impersonation
C.On-path
D.Typosquatting

Item 599 of 620 (Exam B,Q584) Hise Amunier
Which of the following threat vectors would a user be vulnerable to when using a smartphone to scan a two-dimensional matrix barcode?
A.Quashing
B.Smishing
C.Vishing
D.Phishing

Item 600 of 620 (Exam B,Q585) Hide Anuner
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? (Select two).
A.Tokenization
B.Data masking
C.Segmentation
D.SSH tunneling
E.Patch installation
F.Cryptographic downgrade

Item 601 of 620 (Exam B,Q586)
Which of the following security concepts is accomplished when granting access after an individual has logged into a computer network?
A.Authentication
B.Authorization
C.Identification
D.Non-repudiation

Item 602 of 620 (Exam B,Q587) Hise Ataser
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.Jump server with 802.1x
B.IPSec with RADIUS
C.Web proxy for all remote traffic
D.RDP connection with LDAPS

Item 603 of 620 (Exam B,Q588)
A company just received a notification about an exploit that has no current patch or fix. Which of the following describes this scenario?
A.Replay attack
B.On-path attack
C.Zero-day vulnerability
D.VM escape
Item 604 of 620 (Exam B,Q589)
A company relies on open-source software libraries to build the software used byits 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.Cross-site scripting
B.SQL Injection
C.Buffer overflow
D.Zero-day

Item 605 of 620 (Exam B,Q590) Hie Arswer
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.Branch protection tests

C.Secrets management configurations
D.Multifactor authentication

Item 606 of 620 (Exam B,Q591)
Which of the following is used to improve security and overall functionality without losing critical application data?

A.Encryption
B.Reformatting
C.Patching
D.Decom missionin

Item 607 of 620(Exam B,Q592)
Which of the following best describes the concept of information being stored outsideof its country of origin while still being subject to the laws and requirements of the country of origin?

A.Data sovereignty
B.Intellectual property
C.Geolocation
D.Geographic restrictions

Item 608 of 620(Exam B,Q593)
A company plans to secure its systems by:
1.Preventing users from sending sensitive data over corporate email
2 Restricting access to potentially harmful websites
Which of the following features should the company set up? (Select two)
A.File integrity monitoring
B.DNS filtering
C.Guardrails
D.DLP software
E.Stateful firewall
F.Antivirus signatures

Item 609 of 620 (Exam B,Q594)
Which of the following are the best security controls for controlling on-premises access? (Select two)
A.Memorable question
B.Picture ID
C.Swipe card
D.Camera
E.Phone authentication application
F.Biometric scanner
Item 610 of 620 (Exam B,Q595)
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.
C.Ensure the EDR software monitors for unauthorized applications that could be used by threat actors,and configure alerts for the.security team

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

ltem 611 of 620 (Exam B,Q596)
While investigating a possible incident, a security analyst discovers the following:
Which of the following should the analyst do first? A.implement a WAF.
B.Block brute-force attempts on temporary users.
C.Disable the guezy.php script.
D.Check the users table for new accounts.

Item 612 of 620 (Exam B,Q597)
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.Penetration testing
B.Vulnerability assessment
C.Independent audit
D.Red teaming

Item 613 of 620 (Exam B,Q598)
Which of the following best describes the benefit of deploying multiple redundant web servers? A.integrity
B.Non-repudiation
C.Confidentiality
D.High availabilityh

Item 614 of 620 (Exam B,Q599)
A user needs to complete training at https:/lcomptiatraining.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.Pretexting
B.Vishing
C.Cross-site scnpting
D.Typosquatting

Item 615 of 620 (Exam B,Q600)
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.MOA
D.NDA

Item 616 of 620 (Exam B,Q601) Hie Arower
An unexpected and out-of-character email message from a Chief Executive Officer's corporate account asked an employee to provide financial information and to change the recipient's contact number. Which of the following attack vectors is most likely being used?
A.Brand impersonation
B.Business email compromise
C.Phishing
D.Pretexting

Item 617 of 620 (Exam B,Q602) Hide Arswer

ACVE 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.Automated reporting
B.Packet capture
C.Vuinerability scan
D.Metadata analysis

Item 618 of 620 (Exam B,Q603)
Which of the following would most likely be a hacktivist's motive?
A.Revenge
B.Financial gain
C.Espionage
D.Philosophical beliefs
Item 619 of 620 (Exam B,Q604)
An employee receives a text message from an unrecognized number claiming to be the Chief Executive Officer and asking the employee to purchase gift cards. Which of the following types of attacks describes this example?
A.Phishing
B.Disinformation
C.Impersonation
D.Watering-hole

Item 620 of 620 (Exam B,Q605)
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.Pretexting
B.Smishing
C.Impersonation
D.Typosquatting