Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?
A. A full inventory of all hardware and software
B. Documentation of system classifications
C. A list of system owners and their departments
D. Third-party risk assessment documentation
Answer: A

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. The reporting mechanisms for ethics violations
C. Threat vectors based on the industry in which the organization operates
D. Secure software development training for all personnel
E. Cadence and duration of training events
F. Retraining requirements for individuals who fail phishing simulations
Answer: CE

Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?
A. Integrity
B. Availability
C. Confidentiality
D. Non-repudiation
Answer: C

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

Which of the following security control types does an acceptable use policy best represent?
A. Detective
B. Compensating
C. Corrective
D. Preventive
Answer: D

A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?
A. MSA
B. SLA
C. BPA
D. SOW
Answer: D

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?
A. Air gap the system.
B. Move the system to a different network segment.
C. Create a change control request.
D. Apply the patch to the system.
Answer: C

Which of the following describes the reason root cause analysis should be conducted as part of incident response?
A. To gather IoCs for the investigation
B. To discover which systems have been affected
C. To eradicate any trace of malware on the network
D. To prevent future incidents of the same nature
Answer: D

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

A. Testing input validation on the user input fields
B. Performing code signing on company-developed software
C. Performing static code analysis on the software
D. Ensuring secure cookies are use
Answer: B

Which of the following allows for the attribution of messages to individuals?
A. Adaptive identity
B. Non-repudiation
C. Authentication
D. Access logs
Answer: B

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?
A. Place posters around the office to raise awareness of common phishing activities.
B. Implement email security filters to prevent phishing emails from being delivered
C. Update the EDR policies to block automatic execution of downloaded programs.
D. Create additional training for users to recognize the signs of phishing attempts.
Answer: C

A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?
A. Corrective
B. Preventive
C. Detective
D. Deterrent
Answer: C

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?
A. VM escape
B. SQL injection
C. Buffer overflow
D. Race condition
Answer: C

A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?
A. Set the maximum data retention policy.
B. Securely store the documents on an air-gapped network.
C. Review the documents' data classification policy.
D. Conduct a tabletop exercise with the team.
Answer: D

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. Provisioning resources
B. Disabling access
C. Reviewing change approvals
D. Escalating permission requests
Answer: B

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. Air gap
B. Jump server
C. Logical segmentation
D. Virtualization
Answer: A

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

C. Spyware
D. Ransomware
Answer: D

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).
A. The device has been moved from a production environment to a test environment.
B. The device is configured to use cleartext passwords.
C. The device is moved to an isolated segment on the enterprise network.
D. The device is moved to a different location in the enterprise.
E. The device's encryption level cannot meet organizational standards.
F. The device is unable to receive authorized updates.
Answer: EF

An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?
A. Compromise
B. Retention
C. Analysis
D. Transfer
E. Inventory
Answer: B

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?
A. Preparation
B. Recovery
C. Lessons learned
D. Analysis
Answer: A

Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?
A. Impersonation
B. Disinformation
C. Watering-hole
D. Smishing
Answer: C

After a recent ransomware attack on a company's system, an administrator reviewed the log files.
Which of the following control types did the administrator use?
A. Compensating
B. Detective
C. Preventive
D. Corrective
Answer: B

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. Logging all NetFlow traffic into a SIEM
B. Deploying network traffic sensors on the same subnet as the servers
C. Logging endpoint and OS-specific security logs
D. Enabling full packet capture for traffic entering and exiting the servers
Answer: D

Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?
A. Code scanning for vulnerabilities
B. Open-source component usage
C. Quality assurance testing
D. Peer review and approval
Answer: D

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

C. Baseline
D. Policy enforcement
Answer: B

After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?
A. Group Policy
B. Content filtering
C. Data loss prevention
D. Access control lists
Answer: D

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?
A. Impact analysis
B. Scheduled downtime
C. Backout plan
D. Change management boards
Answer: B

Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?
A. Configure all systems to log scheduled tasks.
B. Collect and monitor all traffic exiting the network.
C. Block traffic based on known malicious signatures.
D. Install endpoint management software on all systems.
Answer: D

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. Masking
C. Data classification
D. Permission restrictions
Answer: A

An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?
A. Segmentation
B. Isolation
C. Patching
D. Encryption
Answer: A

Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included. Which of the following best describes how the controls should be set up?
A. Remote access points should fail closed.
B. Logging controls should fail open.
C. Safety controls should fail open.
D. Logical security controls should fail closed.
Answer: C

Which of the following can best protect against an employee inadvertently installing malware on a company system?
A. Host-based firewall
B. System isolation
C. Least privilege
D. Application allow list
Answer: D

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS severs, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?
A. Concurrent session usage
B. Secure DNS cryptographic downgrade
C. On-path resource consumption
D. Reflected denial of service

Answer: D

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. Federation
B. Identity proofing
C. Password complexity
D. Default password changes
E. Password manager
F. Open authentication

Answer: AC

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

A. NGFW
B. WAF
C. TLS
D. SD-WAN

Answer: B

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

A. Smishing
B. Disinformation
C. Impersonating
D. Whaling

Answer: C

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

A. Data in use
B. Data in transit
C. Geographic restrictions
D. Data sovereignty

Answer: B

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

A. Validate the code signature.
B. Execute the code in a sandbox.
C. Search the executable for ASCII strings.
D. Generate a hash of the files.

Answer: A

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

A. Exception
B. Segmentation
C. Risk transfer
D. Compensating controls

Answer: D

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

A. A thorough analysis of the supply chain
B. A legally enforceable corporate acquisition policy
C. A right to audit clause in vendor contracts and SOWs
D. An in-depth penetration test of all suppliers and vendors

Answer: A

A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?
A. Active
B. Passive
C. Defensive
D. Offensive
Answer: A

Which of the following is required for an organization to properly manage its restore process in the event of system failure?
A. IRP
B. DRP
C. RPO
D. SDLC
Answer: B

1. An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources.
Which of the following would be the best solution?
A. RDP server
B. Jump server
C. Proxy server
D. Hypervisor
Answer: B

1. A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered.
Which of the following best describes the program the company is setting up?
A. Open-source intelligence
B. Bug bounty
C. Red team
D. Penetration testing
Answer: B

1. Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data.
Which of the following is the type of data these employees are most likely to use in day-to-day work activities?
A. Encrypted
B. Intellectual property
C. Critical
D. Data in transit
Answer: B

1. A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work.
Which of the following is the best option?
A. Send out periodic security reminders.
B. Update the content of new hire documentation.
C. Modify the content of recurring training.
D. Implement a phishing campaign
Answer: C

1. Which of the following are the most likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Choose two).
A. Certificate mismatch
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software
Answer: DE

1. A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows https://www.organization.com is pointing to 151.191.122.115.
Which of the following is occurring?

A. DoS attack
B. ARP poisoning
C. DNS spoofing
D. NXDOMAIN attack
Answer: C

1. A certificate vendor notified a company that recently invalidated certificates may need to be updated.
Which of the following mechanisms should a security administrator use to determine whether the certificates installed on the company's machines need to be updated?
A. SCEP
B. OCSP
C. CSR
D. CRL
Answer: D

1. In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password.
Which of the following best describes this technique?
A. Key stretching
B. Tokenization
C. Data masking
D. Salting
Answer: D

1. A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?
A. Attribute-based
B. Time of day
C. Role-based
D. Least privilege
Answer: D

1. Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?
A. IDS
B. ACL
C. EDR
D. NAC
Answer: C

1. A business received a small grant to migrate its infrastructure to an off-premises solution. Which of the following should be considered first?
A. Security of cloud providers
B. Cost of implementation
C. Ability of engineers
D. Security of architecture
Answer: D

1. A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?
A. A worm is propagating across the network.
B. Data is being exfiltrated.
C. A logic bomb is deleting data.
D. Ransomware is encrypting files.
Answer: B

1. A company is working with a vendor to perform a penetration test.
Which of the following includes an estimate about the number of hours required to complete the engagement?
A. SOW
B. BPA
C. SLA
D. NDA
Answer: A

1. A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports. Which of the following vulnerabilities has likely been exploited in this software?
A. Memory injection
B. Race condition
C. Side loading
D. SQL injection
Answer: A

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

A. Bollards
B. Access badge
C. Motion sensor
D. Video surveillance
Answer: B

1. A network administrator is working on a project to deploy a load balancer in the company's cloud environment.
Which of the following fundamental security requirements does this project fulfil?
A. Privacy
B. Integrity
C. Confidentiality
D. Availability
Answer: D

1. A technician is deploying a new security camera. Which of the following should the technician do?
A. Configure the correct VLAN.
B. Perform a vulnerability scan.
C. Disable unnecessary ports.
D. Conduct a site survey.
Answer: D

1. An organization experiences a cybersecurity incident involving a command-and-control server.
Which of the following logs should be analyzed to identify the impacted host? (Choose two.)
A. Application
B. Authentication
C. DHCP
D. Network
E. Firewall
F. Database
Answer: DE

1. Which of the following tasks is typically included in the BIA process?
A. Estimating the recovery time of systems
B. Identifying the communication strategy
C. Evaluating the risk management plan
D. Establishing the backup and recovery procedures
E. Developing the incident response plan
Answer: A

1. Which of the following most impacts an administrator's ability to address CVEs discovered on a server?
A. Rescanning requirements
B. Patch availability
C. Organizational impact
D. Risk tolerance
Answer: B

1. Which of the following describes effective change management procedures?
A. Approving the change after a successful deployment
B. Having a backout plan when a patch fails
C. Using a spreadsheet for tracking changes
D. Using an automatic change control bypass for security updates
Answer: B

1. The CIRT is reviewing an incident that involved a human resources recruiter exfiltrating sensitive company data. The CIRT found that the recruiter was able to use HTTP over port 53 to upload documents to a web server. Which of the following security infrastructure devices could have identified and blocked this activity?
A. WAF utilizing SSL decryption
B. NGFW utilizing application inspection
C. UTM utilizing a threat feed
D. SD-WAN utilizing IPSec
Answer: B

1. An organization would like to calculate the time needed to resolve a hardware issue with a server.
Which of the following risk management processes describes this example?
A. Recovery point objective
B. Mean time between failures
C. Recovery time objective
D. Mean time to repair
Answer: D

1. Which of the following describes the category of data that is most impacted when it is lost?
A. Confidential
B. Public
C. Private
D. Critical
Answer: D

1. 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
Answer: B

1. 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. Load balancing
B. Geographic disruption
C. Failover
D. Parallel processing
Answer: A

1. Which of the following is most likely to be deployed to obtain and analyze attacker activity and techniques?
A. Firewall
B. IDS
C. Honeypot
D. Layer 3 switch
Answer: C

1. 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

Answer: A

1. 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. Retention
B. Destruction
C. Inventory
D. Certification
Answer: A

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

A. Standardizing security incident reporting
B. Executing regular phishing campaigns
C. Implementing insider threat detection measures
D. Updating processes for sending wire transfers
Answer: D

1. Which of the following best describes configuring devices to log to an off-site location for possible future reference?
A. Log aggregation

B. DLP
C. Archiving
D. SCAP
Answer: A

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

B. Static
C. Gap
D. Impact
Answer: B

1. 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. DLP
B. FIM
C. IDS
D. EDR
Answer: A

1. A manager receives an email that contains a link to receive a refund. After hovering over the link, the manager notices that the domain's URL points to a suspicious link. Which of the following security practices helped the manager to identify the attack?
A. End user training
B. Policy review
C. URL scanning
D. Plain text email
Answer: A

1. 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. Role-based restrictions
B. Attribute-based restrictions
C. Mandatory restrictions
D. Time-of-day restrictions
Answer: D

1. An organization maintains intellectual property that it wants to protect. Which of the following concepts would be most beneficial to add to the company's security awareness training program?
A. Insider threat detection
B. Simulated threats
C. Phishing awareness
D. Business continuity planning
Answer: A

1. A company that is located in an area prone to hurricanes is developing a disaster recovery plan and looking at site considerations that allow the company to immediately continue operations. Which of the following is the best type of site for this company?
A. Cold
B. Tertiary
C. Warm
D. Hot
Answer: D

1. A company tested and validated the effectiveness of network security appliances within the corporate network. The IDS detected a high rate of SQL injection attacks against the company's servers, and the company's perimeter firewall is at capacity. Which of the following would be the best action to maintain security and reduce the traffic to the perimeter firewall?
A. Set the appliance to IPS mode and place it in front of the company firewall.
B. Convert the firewall to a WAF and use IPSec tunnels to increase throughput.
C. Set the firewall to fail open if it is overloaded with traffic and send alerts to the SIEM.
D. Configure the firewall to perform deep packet inspection and monitor TLS traffic.
Answer: A

1. Which of the following security controls is most likely being used when a critical legacy server is segmented into a private network?
A. Deterrent
B. Corrective
C. Compensating
D. Preventive
Answer: C

1. 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. Establish a security baseline.
B. Review security policies.
C. Adopt security benchmarks.
D. Perform a user ID revalidation.
Answer: B

1. A company is decommissioning its physical servers and replacing them with an architecture that will reduce the number of individual operating systems. Which of the following strategies should the company use to achieve this security requirement?
A. Microservices
B. Containerization
C. Virtualization
D. Infrastructure as code
Answer: B

1. An organization wants to ensure the integrity of compiled binaries in the production environment.
Which of the following security measures would best support this objective?
A. Input validation
B. Code signing
C. SQL injection
D. Static analysis
Answer: B

1. 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. Least privilege
D. Access control monitoring
Answer: C

1. Which of the following best describe a penetration test that resembles an actual external attach?
A. Known environment
B. Partially known environment
C. Bug bounty
D. Unknown environment
Answer: D

1. A security team created a document that details the order in which critical systems should be through back online after a major outage. Which of the following documents did the team create?
A. Communication plan
B. Incident response plan
C. Data retention policy
D. Disaster recovery plan
Answer: D

1. Which of the following best represents an application that does not have an on-premises requirement and is accessible from anywhere?
A. Pass
B. Hybrid cloud
C. Private cloud
D. IaaS
E. SaaS
Answer: E

1. A company is utilizing an offshore team to help support the finance department. The company wants to keep the data secure by keeping it on a company device but does not want to provide equipment to the offshore team. Which of the following should the company implement to meet this requirement?
A. VDI
B. MDM
C. VPN
D. VPC
Answer: A

1. An administrator is Investigating an incident and discovers several users' computers were Infected with malware after viewing files mat were shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins. Which of the following attacks Is most likely the cause of the malware?
A. Malicious flash drive
B. Remote access Trojan
C. Brute-forced password
D. Cryptojacking
Answer: D

1. Which of the following is an algorithm performed to verify that data has not been modified?
A. Hash
B. Code check
C. Encryption
D. Checksum
Answer: A

1. An employee recently resigned from a company. The employee was responsible for managing and supporting weekly batch jobs over the past five years. A few weeks after the employee resigned. one of the batch jobs talked and caused a major disruption. Which of the following would work best to prevent this type of incident from reoccurring?
A. Job rotation
B. Retention
C. Outsourcing
D. Separation of duties
Answer: A

1. A security manager is implementing MFA and patch management. Which of the following would best describe the control type and category? (Select two).
A. Physical
B. Managerial
C. Detective
D. Administrator
E. Preventative
F. Technical
Answer: EF

1. A network administrator deployed a DNS logging tool that togs suspicious websites that are visited and then sends a daily report based on various weighted metrics. Which of the following best describes the type of control the administrator put in place?
A. Preventive
B. Deterrent
C. Corrective
D. Detective
Answer: D

1. Which of the following is best used to detect fraud by assigning employees to different roles?
A. Least privilege
B. Mandatory vacation
C. Separation of duties

D. Job rotation
Answer: D

1. A systems administrate wants to implement a backup solution. the solution needs to allow recovery of the entire system, including the operating system, in case of a disaster. Which of the following backup types should the administrator consider?
A. Incremental
B. Storage area network
C. Differential
D. Image
Answer: D

1. A spoofed identity was detected for a digital certificate. Which of the following are the type of unidentified key and the certificate mat could be in use on the company domain?
A. Private key and root certificate
B. Public key and expired certificate
C. Private key and self-signed certificate
D. Public key and wildcard certificate
Answer: C

1. The Chief Information Security Officer wants to put security measures in place to protect PII. The organization needs to use its existing labeling and classification system to accomplish this goal.
Which of the following would most likely be configured to meet the requirements?
A. Tokenization
B. S/MIME
C. DLP
D. MFA
Answer: C

1. An analyst is reviewing an incident in which a user clicked on a link in a phishing email. Which of the following log sources would the analyst utilize to determine whether the connection was successful?
A. Network
B. System
C. Application
D. Authentication
Answer: A

1. Sine© a recent upgrade (o a WLAN infrastructure, several mobile users have been unable to access the internet from the lobby. The networking team performs a heat map survey of the building and finds several WAPs in the area. The WAPs are using similar frequencies with high power settings. Which of the following installation considerations should the security team evaluate next?
A. Channel overlap
B. Encryption type
C. New WLAN deployment
D. WAP placement
Answer: A

1. An employee in the accounting department receives an email containing a demand for payment tot services performed by a vendor However, the vendor is not in the vendor management database. Which of the following in this scenario an example of?
A. Pretexting
B. Impersonation
C. Ransomware
D. Invoice scam
Answer: D

1. A security analyst is assessing several company firewalls. Which of the following cools would the analyst most likely use to generate custom packets to use during the assessment?
A. hping
B. Wireshark
C. PowerShell
D. netstat
Answer: A

1. A new vulnerability enables a type of malware that allows the unauthorized movement of data from a system. Which of the following would detect this behavior?
A. Implementing encryption
B. Monitoring outbound traffic

C. Using default settings
D. Closing all open ports
Answer: B

1. Which of the following is the most effective way to protect an application server running software that is no longer supported from network threats?
A. Air gap
B. Barricade
C. Port security
D. Screen subnet
Answer: D

1. Which of the following is die most important security concern when using legacy systems to provide production service?
A. Instability
B. Lack of vendor support
C. Loss of availability
D. Use of insecure protocols
Answer: B

1. Cadets speaking a foreign language are using company phone numbers to make unsolicited phone calls lo a partner organization. A security analyst validates through phone system logs that the calls are occurring and the numbers are not being spoofed.
Which of the following is the most likely explanation?
A. The executive team is traveling internationally and trying to avoid roaming charges
B. The company's SIP server security settings are weak.
C. Disgruntled employees are making calls to the partner organization.
D. The service provider has assigned multiple companies the same numbers
Answer: B

1. An IT security team is concerned about the confidentiality of documents left unattended in MFPs.
Which of the following should the security team do to mitigate the situation?
A. Educate users about the importance of paper shredder devices.
B. Deploy an authentication factor that requires ln-person action before printing.
C. Install a software client m every computer authorized to use the MFPs.
D. Update the management software to utilize encryption.
Answer: B

1. During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers.
Which of the following describes an attack method that relates to printing centers?
A. Whaling
B. Credential harvesting
C. Prepending
D. Dumpster diving
Answer: D

1. A software developer would like to ensure. The source code cannot be reverse engineered or debugged. Which of the following should the developer consider?
A. Version control
B. Obfuscation toolkit
C. Code reuse
D. Continuous integration
E. Stored procedures
Answer: B

1. A website user is locked out of an account after clicking an email link and visiting a different website Web server logs show the user's password was changed, even though the user did not change the password. Which of the following is the most likely cause?
A. Cross-sue request forgery
B. Directory traversal
C. ARP poisoning
D. SQL injection
Answer: A

1. A security engineer is working to address the growing risks that shadow IT services are introducing to the organization. The organization has taken a cloud-first approach end does not have an on- premises IT infrastructure. Which of the following would best secure the organization?
A. Upgrading to a next-generation firewall

B. Deploying an appropriate in-line CASB solution
C. Conducting user training on software policies
D. Configuring double key encryption in SaaS platforms
Answer: B

1. A cybersecurity incident response team at a large company receives notification that malware is present on several corporate desktops No known Indicators of compromise have been found on the network. Which of the following should the team do first to secure the environment?
A. Contain the Impacted hosts
B. Add the malware to the application blocklist.
C. Segment the core database server.
D. Implement firewall rules to block outbound beaconing
Answer: A

1. Which of the following is a reason why a forensic specialist would create a plan to preserve data after an modem and prioritize the sequence for performing forensic analysis?
A. Order of volatility
B. Preservation of event logs
C. Chain of custody
D. Compliance with legal hold
Answer: A

1. A security analyst is creating base for the server team to follow when hardening new devices for deployment. Which of the following beet describes what the analyst is creating?
A. Change management procedure
B. Information security policy
C. Cybersecurity framework
D. Secure configuration guide
Answer: D

1. In which of the following scenarios is tokenization the best privacy technique 10 use?
A. Providing pseudo-anonymization tor social media user accounts
B. Serving as a second factor for authentication requests
C. Enabling established customers to safely store credit card Information
D. Masking personal information inside databases by segmenting data
Answer: C

1. Which of the following data roles is responsible for identifying risks and appropriate access to data?
A. Owner
B. Custodian
C. Steward
D. Controller
Answer: A

1. An external vendor recently visited a company's headquarters tor a presentation. Following the visit a member of the hosting team found a file that the external vendor left behind on a server. The file contained detailed architecture information and code snippets. Which of the following data types best describes this file?
A. Government
B. Public
C. Proprietary
D. Critical
Answer: C

1. Which of the following explains why an attacker cannot easily decrypt passwords using a rainbow table attack?
A. Digital signatures
B. Salting
C. Hashing
D. Perfect forward secrecy
Answer: B

1. A company is currently utilizing usernames and passwords, and it wants to integrate an MFA method that is seamless, can Integrate easily into a user's workflow, and can utilize employee- owned devices. Which of the following will meet these requirements?
A. Push notifications
B. Phone call
C. Smart card
D. Offline backup codes

Answer: A

1. A financial institution would like to store its customer data m the cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution Is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would best meet the requirement?
A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral
Answer: C

1. The Chief Information Security Officer of an organization needs to ensure recovery from ransomware would likely occur within the organization's agreed-upon RPOs end RTOs. Which of the following backup scenarios would best ensure recovery?
A. Hourly differential backups stored on a local SAN array
B. Dally full backups stored on premises in magnetic offline media
C. Daly differential backups maintained by a third-party cloud provider
D. Weekly full backups with daily incremental stored on a NAS drive
Answer: D

1. Which of the following best describe why a process would require a two-person integrity security control?
A. To Increase the chance that the activity will be completed in half of the time the process would take only one user to complete
B. To permit two users from another department to observe the activity that is being performed by an authorized user
C. To reduce the risk that the procedures are performed incorrectly or by an unauthorized user
D. To allow one person to perform the activity while being recorded on the CCTV camera
Answer: C

1. A company recently decided to allow employees to work remotely. The company wants to protect us data without using a VPN. Which of the following technologies should the company Implement?
A. Secure web gateway
B. Virtual private cloud end point
C. Deep packet Inspection
D. Next-gene ration firewall
Answer: A

1. In a rush to meet an end-of-year business goal, the IT department was told to implement a new business application. The security engineer reviews the attributes of the application and decides the time needed to perform due diligence is insufficient from a cybersecurity perspective. Which of the following best describes the security engineer's response?
A. Risk tolerance
B. Risk acceptance
C. Risk importance
D. Risk appetite
Answer: D

1. An organization has too many variations of a single operating system and needs to standardize the arrangement prior to pushing the system image to users. Which of the following should the organization implement first?
A. Standard naming convention
B. Mashing
C. Network diagrams
D. Baseline configuration
Answer: D

1. A growing company would like to enhance the ability of its security operations center to detect threats but reduce the amount of manual work required tor the security analysts. Which of the following would best enable the reduction in manual work?
A. SOAR
B. SIEM
C. MDM
D. DLP
Answer: A

1. A company implemented an MDM policy 10 mitigate risks after repealed instances of employees losing company-provided mobile phones. In several cases. The lost phones were used maliciously to perform social engineering attacks against other employees. Which of the following MDM features should be configured to best address this issue? (Select two).
A. Screen locks
B. Remote wipe

C. Full device encryption
D. Push notifications
E. Application management
F. Geolocation
Answer: BA

1. A security analyst needs to propose a remediation plan 'or each item in a risk register. The item with the highest priority requires employees to have separate logins for SaaS solutions and different password complexity requirements for each solution. Which of the following implementation plans will most likely resolve this security issue?
A. Creating a unified password complexity standard
B. Integrating each SaaS solution with the Identity provider
C. Securing access to each SaaS by using a single wildcard certificate
D. Configuring geofencing on each SaaS solution
Answer: B

1. Which of the following is the first step to take when creating an anomaly detection process?
A. Selecting events
B. Building a baseline
C. Selecting logging options
D. Creating an event log
Answer: B

1. Which of the following is the final step of the modem response process?
A. Lessons learned
B. Eradication
C. Containment
D. Recovery
Answer: A

1. While investigating a recent security breach an analyst finds that an attacker gained access by SOL infection through a company website. Which of the following should the analyst recommend to the website developers to prevent this from reoccurring?
A. Secure cookies
B. Input sanitization
C. Code signing
D. Blocklist
Answer: B

1. Which of the following environments utilizes a subset of customer data and is most likely to be used to assess the impacts of major system upgrades and demonstrate system features?
A. Development
B. Test
C. Production
D. Staging
Answer: D

1. An IT manager is putting together a documented plan describing how the organization will keep operating in the event of a global incident. Which of the following plans is the IT manager creating?
A. Business continuity
B. Physical security
C. Change management
D. Disaster recovery
Answer: A

1. Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?
A. SLA
B. MOU
C. MOA
D. BPA
Answer: A

1. Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?
A. Continuity of operations
B. Capacity planning
C. Tabletop exercise

D. Parallel processing
Answer: C

1. Which of the following methods would most likely be used to identify legacy systems?
A. Bug bounty program
B. Vulnerability scan
C. Package monitoring
D. Dynamic analysis
Answer: B

1. Client files can only be accessed by employees who need to know the information and have specified roles in the company. Which of the following best describes this security concept?
A. Availability
B. Confidentiality
C. Integrity
D. Non-repudiation
Answer: B

1. A user would like to install software and features that are not available with a smartphone's default software. Which of the following would allow the user to install unauthorized software and enable new features?
A. SOU
B. Cross-site scripting
C. Jailbreaking
D. Side loading
Answer: C

1. An administrator at a small business notices an increase in support calls from employees who receive a blocked page message after trying to navigate to a spoofed website. Which of the following should the administrator do?
A. Deploy multifactor authentication.
B. Decrease the level of the web filter settings
C. Implement security awareness training.
D. Update the acceptable use policy
Answer: C

1. Which of the following control types is AUP an example of?
A. Physical
B. Managerial
C. Technical
D. Operational
Answer: B

1. A security engineer is installing an IPS to block signature-based attacks in the environment. Which of the following modes will best accomplish this task?
A. Monitor
B. Sensor
C. Audit
D. Active
Answer: D

1. An organization wants to limit potential impact to its log-in database in the event of a breach. Which of the following options is the security team most likely to recommend?
A. Tokenization
B. Hashing
C. Obfuscation
D. Segmentation
Answer: B

1. A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network. Which of the following should be configured on the existing network infrastructure to best prevent this activity?
A. Port security
B. Web application firewall
C. Transport layer security
D. Virtual private network
Answer: A

1. During a penetration test, a vendor attempts to enter an unauthorized area using an access badge Which of the following types of tests does this represent?
A. Defensive
B. Passive
C. Offensive
D. Physical
Answer: D

1. Which of the following is a common, passive reconnaissance technique employed by penetration testers in the early phases of an engagement?
A. Open-source intelligence
B. Port scanning
C. Pivoting
D. Exploit validation
Answer: A

1. Which of the following should a security operations center use to improve its incident response procedure?
A. Playbooks
B. Frameworks
C. Baselines
D. Benchmarks
Answer: A

1. An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to email these files outside of the organization. Which of the following best describes the tool the administrator is using?
A. DLP
B. SNMP traps
C. SCAP
D. IPS
Answer: A

1. A security analyst is investigating a workstation that is suspected of outbound communication to a command-and-control server. During the investigation, the analyst discovered that logs on the endpoint were deleted. Which of the following logs would the analyst most likely look at next?
A. IPS
B. Firewall
C. ACL
D. Windows security
Answer: B

1. A security team is setting up a new environment for hosting the organization's on-premises software application as a cloud-based service. Which of the following should the team ensure is in place in order for the organization to follow security best practices?
A. Visualization and isolation of resources
B. Network segmentation
C. Data encryption
D. Strong authentication policies
Answer: A

1. Which of the following phases of an incident response involves generating reports?
A. Recovery
B. Preparation
C. Lessons learned
D. Containment
Answer: C

1. A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage. Which of the following recovery sites is the best option?
A. Hot
B. Cold
C. Warm
D. Geographically dispersed
Answer: C

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

A. Compliance reporting
B. GDPR
C. Due diligence
D. Attestation
Answer: C

1. A security analyst developed a script to automate a trivial and repeatable task. Which of the following best describes the benefits of ensuring other team members understand how the script works?
A. To reduce implementation cost
B. To identify complexity
C. To remediate technical debt
D. To prevent a single point of failure
Answer: D

1. 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. Full disk encryption
B. Network access control
C. File integrity monitoring
D. User behavior analytics
Answer: C

1. Employees located off-site must have access to company resources in order to complete their assigned tasks These employees utilize a solution that allows remote access without interception concerns. Which of the following best describes this solution?
A. Proxy server
B. NGFW
C. VPN
D. Security zone
Answer: C

1. The Chief Information Security Officer (CISO) at a large company would like to gain an understanding of how the company's security policies compare to the requirements imposed by external regulators.
Which of the following should the CISO use?
A. Penetration test
B. Internal audit
C. Attestation
D. External examination
Answer: D

1. A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system. Which of the following techniques would increase enterprise security?
A. Installing HIDS on the system
B. Placing the system in an isolated VLAN
C. Decommissioning the system
D. Encrypting the system's hard drive
Answer: B

1. An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in. so the security team wants to reduce the number of credentials each employee must maintain. Which of the following is the first step the security team should take?
A. Enable SAML
B. Create OAuth tokens.
C. Use password vaulting.
D. Select an IdP
Answer: D

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

1. Which of the following threat vectors is most commonly utilized by insider threat actors attempting data exfiltration?
A. Unidentified removable devices

B. Default network device credentials
C. Spear phishing emails
D. Impersonation of business units through typosquatting
Answer: A

1. A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company. Which of the following attack vectors is most likely being used?
A. Business email
B. Social engineering
C. Unsecured network
D. Default credentials
Answer: B

1. An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?
A. XDR
B. SPF
C. DLP
D. DMARC
Answer: C

1. An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch. Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?
A. Asset inventory
B. Network enumeration
C. Data certification
D. Procurement process
Answer: A

1. Which of the following security measures is required when using a cloud-based platform for IoT management?
A. Encrypted connection
B. Federated identity
C. Firewall
D. Single sign-on
Answer: A

1. Which of the following is a feature of a next-generation SIEM system?
A. Virus signatures
B. Automated response actions
C. Security agent deployment
D. Vulnerability scanning
Answer: B

1. A company allows customers to upload PDF documents to its public e-commerce website. Which of the following would a security analyst most likely recommend?
A. Utilizing attack signatures in an IDS
B. Enabling malware detection through a UTM
C. Limiting the affected servers with a load balancer
D. Blocking command injections via a WAF
Answer: B

1. After creating a contract for IT contractors, the human resources department changed several clauses. The contract has gone through three revisions. Which of the following processes should the human resources department follow to track revisions?
A. Version validation
B. Version changes
C. Version updates
D. Version control
Answer: D

1. A company is reviewing options to enforce user logins after several account takeovers. The following conditions must be met as part of the solution:
- Allow employees to work remotely or from assigned offices around the world.
- Provide a seamless login experience.
- Limit the amount of equipment required.

Which of the following best meets these conditions?
A. Trusted devices
B. Geotagging
C. Smart cards
D. Time-based logins
Answer: A

1. Which of the following methods can be used to detect attackers who have successfully infiltrated a network? (Choose two.)
A. Tokenization
B. CI/CD
C. Honeypots
D. Threat modeling
E. DNS sinkhole
F. Data obfuscation
Answer: CE

1. A company wants to ensure that the software it develops will not be tampered with after the final version is completed. Which of the following should the company most likely use?
A. Hashing
B. Encryption
C. Baselines
D. Tokenization
Answer: A

1. An organization completed a project to deploy SSO across all business applications last year. Recently, the finance department selected a new cloud-based accounting software vendor. Which of the following should most likely be configured during the new software deployment?
A. RADIUS
B. SAML
C. EAP
D. OpenID
Answer: B

1. A user, who is waiting for a flight at an airport, logs in to the airline website using the public Wi-Fi, ignores a security warning and purchases an upgraded seat. When the flight lands, the user finds unauthorized credit card charges. Which of the following attacks most likely occurred?
A. Replay attack
B. Memory leak
C. Buffer overflow attack
D. On-path attack
Answer: D

1. A network team segmented a critical, end-of-life server to a VLAN that can only be reached by specific devices but cannot be reached by the perimeter network. Which of the following best describe the controls the team implemented? (Choose two.)
A. Managerial
B. Physical
C. Corrective
D. Detective
E. Compensating
F. Technical
G. Deterrent
Answer: EF

1. A threat actor was able to use a username and password to log in to a stolen company mobile device. Which of the following provides the best solution to increase mobile data security on all employees' company mobile devices?
A. Application management
B. Full disk encryption
C. Remote wipe
D. Containerization
Answer: C

1. Which of the following best describes the risk present after controls and mitigating factors have been applied?
A. Residual
B. Avoided
C. Inherent
D. Operational

Answer: A

1. A software development team asked a security administrator to recommend techniques that should be used to reduce the chances of the software being reverse engineered. Which of the following should the security administrator recommend?
A. Digitally signing the software
B. Performing code obfuscation
C. Limiting the use of third-party libraries
D. Using compile flags
Answer: B

1. Easy-to-guess passwords led to an account compromise. The current password policy requires at least 12 alphanumeric characters, one uppercase character, one lowercase character, a password history of two passwords, a minimum password age of one day, and a maximum password age of 90 days. Which of the following would reduce the risk of this incident from happening again? (Choose two.)
A. Increasing the minimum password length to 14 characters.
B. Upgrading the password hashing algorithm from MD5 to SHA-512.
C. Increasing the maximum password age to 120 days.
D. Reducing the minimum password length to ten characters.
E. Reducing the minimum password age to zero days.
F. Including a requirement for at least one special character.
Answer: AF

1. A user downloaded software from an online forum. After the user installed the software, the security team observed external network traffic connecting to the user's computer on an uncommon port. Which of the following is the most likely explanation of this unauthorized connection?
A. The software had a hidden keylogger.
B. The software was ransomware.
C. The user's computer had a fileless virus.
D. The software contained a backdoor.
Answer: D

1. Which of the following most likely describes why a security engineer would configure all outbound emails to use S/MIME digital signatures?
A. To meet compliance standards
B. To increase delivery rates
C. To block phishing attacks
D. To ensure non-repudiation
Answer: D

1. Which of the following considerations is the most important regarding cryptography used in an IoT device?
A. Resource constraints
B. Available bandwidth
C. The use of block ciphers
D. The compatibility of the TLS version
Answer: A

1. A coffee shop owner wants to restrict internet access to only paying customers by prompting them for a receipt number. Which of the following is the best method to use given this requirement?
A. WPA3
B. Captive portal
C. PSK
D. IEEE 802.1X
Answer: B

1. While performing digital forensics, which of the following is considered the most volatile and should have the contents collected first?
A. Hard drive
B. RAM
C. SSD
D. Temporary files
Answer: B

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

D. IRP
Answer: A

1. Which of the following is considered a preventive control?
A. Configuration auditing
B. Log correlation
C. Incident alerts
D. Segregation of duties
Answer: D

1. A security team has been alerted to a flood of incoming emails that have various subject lines and are addressed to multiple email inboxes. Each email contains a URL shortener link that is redirecting to a dead domain. Which of the following is the best step for the security team to take?
A. Create a blocklist for all subject lines.
B. Send the dead domain to a DNS sinkhole.
C. Quarantine all emails received and notify all employees.
D. Block the URL shortener domain in the web proxy.
Answer: D

1. Which of the following is a common source of unintentional corporate credential leakage in cloud environments?
A. Code repositories
B. Dark web
C. Threat feeds
D. State actors
E. Vulnerability databases
Answer: A

1. A security administrator is hardening corporate systems and applying appropriate mitigations by consulting a real-world knowledge base for adversary behavior. Which of the following would be best for the administrator to reference?
A. MITRE ATT&CK
B. CSIRT
C. CVSS
D. SOAR
Answer: A

1. An architect has a request to increase the speed of data transfer using JSON requests externally. Currently, the organization uses SFTP to transfer data files. Which of the following will most likely meet the requirements?
A. A website-hosted solution
B. Cloud shared storage
C. A secure email solution
D. Microservices using API
Answer: D

1. Which of the following best describes a social engineering attack that uses a targeted electronic messaging campaign aimed at a Chief Executive Officer?
A. Whaling
B. Spear phishing
C. Impersonation
D. Identity fraud
Answer: A

1. During a penetration test, a flaw in the internal PKI was exploited to gain domain administrator rights using specially crafted certificates. Which of the following remediation tasks should be completed as part of the cleanup phase?
A. Updating the CRL
B. Patching the CA
C. Changing passwords
D. Implementing SOAR
Answer: A

1. A company wants to implement MFA. Which of the following enables the additional factor while using a smart card?
A. PIN
B. Hardware token
C. User ID
D. SMS
Answer: A

1. A company hired an external consultant to assist with required system upgrades to a critical business application. A systems administrator needs to secure the consultant's access without sharing passwords to critical systems. Which of the following solutions should most likely be utilized?
A. TACACS+
B. SAML
C. An SSO platform
D. Role-based access control
E. PAM software
Answer: E

1. A newly implemented wireless network is designed so that visitors can connect to the wireless network for business activities. The legal department is concerned that visitors might connect to the network and perform illicit activities. Which of me following should the security team implement to address this concern?
A. Configure a RADIUS server to manage device authentication.
B. Use 802.1X on all devices connecting to wireless.
C. Add a guest captive portal requiring visitors to accept terms and conditions.
D. Allow for new devices to be connected via WPS.
Answer: C

1. Which of the following physical controls can be used to both detect and deter? (Choose two.)
A. Lighting
B. Fencing
C. Signage
D. Sensor
E. Bollard
F. Lock
Answer: AD

1. A multinational bank hosts several servers in its data center. These servers run a business- critical application used by customers to access their account information. Which of the following should the bank use to ensure accessibility during peak usage times?
A. Load balancer
B. Cloud backups
C. Geographic dispersal
D. Disk multipathing
Answer: A

1. The author of a software package is concerned about bad actors repackaging and inserting malware into the software. The software download is hosted on a website, and the author exclusively controls the website's contents. Which of the following techniques would best ensure the software's integrity?
A. Input validation
B. Code signing
C. Secure cookies
D. Fuzzing
Answer: B

1. During an annual review of the system design, an engineer identified a few issues with the currently released design. Which of the following should be performed next according to best practices?
A. Risk management process
B. Product design process
C. Design review process
D. Change control process
Answer: D

1. A security analyst at an organization observed several user logins from outside the organization's network. The analyst determined that these logins were not performed by individuals within the organization. Which of the following recommendations would reduce the likelihood of future attacks? (Choose two.)
A. Disciplinary actions for users
B. Conditional access policies
C. More regular account audits
D. Implementation of additional authentication factors
E. Enforcement of content filtering policies
F. A review of user account permissions
Answer: BD

1. A security team is addressing a risk associated with the attack surface of the organization's web application over port 443. Currently, no advanced network security capabilities are in place. Which of the following would be best to set up? (Choose two.)
A. NIDS
B. Honeypot
C. Certificate revocation list
D. HIPS
E. WAF
F. SIEM
Answer: AE

1. A security administrator notices numerous unused, non-compliant desktops are connected to the network. Which of the following actions would the administrator most likely recommend to the management team?
A. Monitoring
B. Decommissioning
C. Patching
D. Isolating
Answer: B

1. Which of the following is a common data removal option for companies that want to wipe sensitive data from hard drives in a repeatable manner but allow the hard drives to be reused?
A. Sanitization
B. Formatting
C. Degaussing
D. Defragmentation
Answer: A

1. An organization wants to improve the company's security authentication method for remote employees. Given the following requirements:
- Must work across SaaS and internal network applications
- Must be device manufacturer agnostic
- Must have offline capabilities
Which of the following would be the most appropriate authentication method?
A. Username and password
B. Biometrics
C. SMS verification
D. Time-based tokens
Answer: D

1. A security officer is implementing a security awareness program and has placed security- themed posters around the building and assigned online user training. Which of the following will the security officer most likely implement?
A. Password policy
B. Access badges
C. Phishing campaign
D. Risk assessment
Answer: C

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

1. An organization requests a third-party full-spectrum analysis of its supply chain. Which of the following would the analysis team use to meet this requirement?
A. Vulnerability scanner
B. Penetration test
C. SCAP
D. Illumination tool
Answer: C

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

A. Agentless solution
B. Client-based soon
C. Open port
D. File-based solution
Answer: A

1. A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor. Which of the following processes is the analyst most likely conducting?
A. Internal audit
B. Penetration testing
C. Attestation
D. Due diligence
Answer: D

1. Which of the following is used to conceal credit card information in a database log file?
A. Tokenization
B. Masking
C. Hashing
D. Obfuscation
Answer: B

1. An organization recently started hosting a new service that customers access through a web portal. A security engineer needs to add to the existing security devices a new solution to protect this new service. Which of the following is the engineer most likely to deploy?
A. Layer 4 firewall
B. NGFW
C. WAF
D. UTM
Answer: C

1. Which of the following topics would most likely be included within an organization's SDLC?
A. Service-level agreements
B. Information security policy
C. Penetration testing methodology
D. Branch protection requirements
Answer: D

1. Which of the following activities should a systems administrator perform to quarantine a potentially infected system?
A. Move the device into an air-gapped environment.
B. Disable remote log-in through Group Policy.
C. Convert the device into a sandbox.
D. Remote wipe the device using the MDM platform.
Answer: A

1. Which of the following would be the best way to test resiliency in the event of a primary power failure?
A. Parallel processing
B. Tabletop exercise
C. Simulation testing
D. Production failover
Answer: D

1. A company is concerned about the theft of client data from decommissioned laptops. Which of the following is the most cost-effective method to decrease this risk?
A. Wiping
B. Recycling
C. Shredding
D. Deletion
Answer: A

1. Which of the following should be used to ensure an attacker is unable to read the contents of a mobile device's drive if the device is lost?
A. TPM
B. ECC
C. FDE
D. HSM
Answer: C

1. An organization plans to expand its operations internationally and needs to keep data at the new location secure. The organization wants to use the most secure architecture model possible. Which of the following models offers the highest level of security?
A. Cloud-based
B. Peer-to-peer
C. On-premises
D. Hybrid
Answer: A

1. The security team at a large global company needs to reduce the cost of storing data used for performing investigations. Which of the following types of data should have its retention length reduced?
A. Packet capture
B. Endpoint logs
C. OS security logs
D. Vulnerability scan
Answer: A

1. Which of the following is the primary purpose of a service that tracks log-ins and time spent using the service?
A. Availability
B. Accounting
C. Authentication
D. Authorization
Answer: B

1. Which of the following is a type of vulnerability that refers to the unauthorized installation of applications on a device through means other than the official application store?
A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading
Answer: D

1. Which of the following types of identification methods can be performed on a deployed application during runtime?
A. Dynamic analysis
B. Code review
C. Package monitoring
D. Bug bounty
Answer: A

1. Which of the following is the best way to provide secure remote access for employees while minimizing the exposure of a company's internal network?
A. VPN
B. LDAP
C. FTP
D. RADIUS
Answer: A

1. An administrator must replace an expired SSL certificate. Which of the following does the administrator need to create the new SSL certificate?
A. CSR
B. OCSP
C. Key
D. CRL
Answer: A

1. Which of the following strategies should an organization use to efficiently manage and analyze multiple types of logs?
A. Deploy a SIEM solution
B. Create custom scripts to aggregate and analyze logs
C. Implement EDR technology
D. Install a unified threat management appliance
Answer: A

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

C. Service-level agreement
D. Master service agreement
Answer: B

1. A penetration test has demonstrated that domain administrator accounts were vulnerable to pass- the-hash attacks. Which of the following would have been the best strategy to prevent the threat actor from using domain administrator accounts?
A. Audit each domain administrator account weekly for password compliance.
B. Implement a privileged access management solution.
C. Create IDS policies to monitor domain controller access.
D. Use Group Policy to enforce password expiration.
Answer: B

1. 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
Answer: A

1. A security professional discovers a folder containing an employee's personal information on the enterprise's shared drive. Which of the following best describes the data type the security professional should use to identify organizational policies and standards concerning the storage of employees' personal information?
A. Legal
B. Financial
C. Privacy
D. Intellectual property
Answer: C

1. An organization needs to monitor its users' activities to prevent insider threats. Which of the following solutions would help the organization achieve this goal?
A. Behavioral analytics
B. Access control lists
C. Identity and access management
D. Network intrusion detection system
Answer: A

1. A company wants to track modifications to the code used to build new virtual servers. Which of the following will the company most likely deploy?
A. Change management ticketing system
B. Behavioral analyzer
C. Collaboration platform
D. Version control tool
Answer: D

1. Company A jointly develops a product with Company B, which is located in a different country. Company A finds out that their intellectual property is being shared with unauthorized companies. Which of the following has been breached?
A. SLA
B. AUP
C. SOW
D. MOA
Answer: D

1. While a user reviews their email, a host gets infected by malware 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. Removable media and cables
C. Password management
D. Social engineering
Answer: B

1. Which of the following is the best way to validate the integrity and availability of a disaster recovery site?
A. Lead a simulated failover.
B. Conduct a tabletop exercise.
C. Periodically test the generators.

D. Develop requirements for database encryption.
Answer: A

1. While conducting a business continuity tabletop exercise, the security team becomes concerned by potential impacts if a generator fails during failover. Which of the following is the team most likely to consider in regard to risk management activities?
A. RPO
B. ARO
C. BIA
D. MTTR
Answer: D

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

1. Which of the following is the best way to prevent an unauthorized user from plugging a laptop into an employee's phone network port and then using tools to scan for database servers?
A. MAC filtering
B. Segmentation
C. Certification
D. Isolation
Answer: A

1. Which of the following describes the procedures a penetration tester must follow while conducting a test?
A. Rules of engagement
B. Rules of acceptance
C. Rules of understanding
D. Rules of execution
Answer: A

1. Which of the following is the stage in an investigation when forensic images are obtained?
A. Acquisition
B. Preservation
C. Reporting
D. E-discovery
Answer: A

1. A security analyst learns that an attack vector, used as part of a recent incident, was a well- known IoT device exploit. The analyst needs to review logs to identify the time of the initial exploit. Which of the following logs should the analyst review first?
A. Endpoint
B. Application
C. Firewall
D. NAC
Answer: C

1. A group of developers has a shared backup account to access the source code repository. Which of the following is the best way to secure the backup account if there is an SSO failure?
A. RAS
B. EAP
C. SAML
D. PAM
Answer: D

1. Which of the following threat actors would most likely deface the website of a high-profile music group?
A. Unskilled attacker
B. Organized crime
C. Nation-state
D. Insider threat
Answer: A

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

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

1. Which of the following should a company use to provide proof of external network security testing?
A. Business impact analysis
B. Supply chain analysis
C. Vulnerability assessment
D. Third-party attestation
Answer: D

1. Which of the following allows a systems administrator to tune permissions for a file?
A. Patching
B. Access control list
C. Configuration enforcement
D. Least privilege
Answer: B

1. Which of the following would a security administrator use to comply with a secure baseline during a patch update?
A. Information security policy
B. Service-level expectations
C. Standard operating procedure
D. Test result report
Answer: C

1. A company is aware of a given security risk related to a specific market segment. The business chooses not to accept responsibility and target their services to a different market segment. Which of the following describes this risk management strategy?
A. Exemption
B. Exception
C. Avoid
D. Transfer
Answer: C

1. A company wants to improve the availability of its application with a solution that requires minimal effort in the event a server needs to be replaced or added. Which of the following would be the best solution to meet these objectives?
A. Load balancing
B. Fault tolerance
C. Proxy servers
D. Replication
Answer: A

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

1. A security administrator is addressing an issue with a legacy system that communicates data using an unencrypted protocol to transfer sensitive data to a third party. No software updates that use an encrypted protocol are available, so a compensating control is needed. Which of the following are the most appropriate for the administrator to suggest? (Select two.)
A. Tokenization
B. Cryptographic downgrade
C. SSH tunneling
D. Segmentation
E. Patch installation
F. Data masking
Answer: CD

1. Which of the following should be used to ensure a device is inaccessible to a network- connected resource?
A. Disablement of unused services
B. Web application firewall
C. Host isolation

D. Network-based IDS
Answer: C

1. A security engineer at a large company needs to enhance IAM to ensure that employees can only access corporate systems during their shifts. Which of the following access controls should the security engineer implement?
A. Role-based
B. Time-of-day restrictions
C. Least privilege
D. Biometric authentication
Answer: B

1. Which of the following would be the greatest concern for a company that is aware of the consequences of non-compliance with government regulations?
A. Right to be forgotten
B. Sanctions
C. External compliance reporting
D. Attestation
Answer: B

1. An organization has a new regulatory requirement to implement corrective controls on a financial system. Which of the following is the most likely reason for the new requirement?
A. To defend against insider threats altering banking details
B. To ensure that errors are not passed to other systems
C. To allow for business insurance to be purchased
D. To prevent unauthorized changes to financial data
Answer: D

1. An organization has a new regulatory requirement to implement corrective controls on a financial system. Which of the following is the most likely reason for the new requirement?
A. To defend against insider threats altering banking details
B. To ensure that errors are not passed to other systems
C. To allow for business insurance to be purchased
D. To prevent unauthorized changes to financial data
Answer: D

1. Which of the following aspects of the data management life cycle is most directly impacted by local and international regulations?
A. Destruction
B. Certification
C. Retention
D. Sanitization
Answer: C

1. Which of the following would a systems administrator follow when upgrading the firmware of an organization's router?
A. Software development life cycle
B. Risk tolerance
C. Certificate signing request
D. Maintenance window
Answer: D

1. Which of the following should an internal auditor check for first when conducting an audit of the organization's risk management program?
A. Policies and procedures
B. Asset management
C. Vulnerability assessment
D. Business impact analysis
Answer: A

1. An administrator wants to perform a risk assessment without using proprietary company information. Which of the following methods should the administrator use to gather information?
A. Network scanning
B. Penetration testing
C. Open-source intelligence
D. Configuration auditing
Answer: C

1. A systems administrator is concerned about vulnerabilities within cloud computing instances. Which of the following is most important for the administrator to consider when architecting a cloud computing environment?
A. SQL injection
B. TOC/TOU
C. VM escape
D. Tokenization
E. Password spraying
Answer: C

1. A database administrator is updating the company's SQL database, which stores credit card information for pending purchases. Which of the following is the best method to secure the data against a potential breach?
A. Hashing
B. Obfuscation
C. Tokenization
D. Masking
Answer: C

1. An employee used a company's billing system to issue fraudulent checks. The administrator is looking for evidence of other occurrences of this activity. Which of the following should the administrator examine?
A. Application logs
B. Vulnerability scanner logs
C. IDS/IPS logs
D. Firewall logs
Answer: A

1. An organization is looking to optimize its environment and reduce the number of patches necessary for operating systems. Which of the following will best help to achieve this objective?
A. Microservices
B. Virtualization
C. Real-time operating system
D. Containers
Answer: D

1. Which of the following is the best way to securely store an encryption key for a data set in a manner that allows multiple entities to access the key when needed?
A. Public key infrastructure
B. Open public ledger
C. Public key encryption
D. Key escrow
Answer: D

1. The internal audit team determines a software application is no longer in scope for external reporting requirements. Which of the following will confirm management's perspective that the application is no longer applicable?
A. Data inventory and retention
B. Right to be forgotten
C. Due care and due diligence
D. Acknowledgement and attestation
Answer: D

1. Which of the following is an example of memory injection?
A. Two processes access the same variable, allowing one to cause a privilege escalation.
B. A process receives an unexpected amount of data, which causes malicious code to be executed.
C. Malicious code is copied to the allocated space of an already running process.
D. An executable is overwritten on the disk, and malicious code runs the next time it is executed.
Answer: C

1. Which of the following should a security administrator adhere to when setting up a new set of firewall rules?
A. Disaster recovery plan
B. Incident response procedure
C. Business continuity plan
D. Change management procedure
Answer: D

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

A. Length
B. Complexity
C. Least privilege
D. Something you have
E. Security keys
F. Biometrics
Answer: A B

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

1. 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. Business email compromise
B. Phishing
C. Brand impersonation
D. Pretexting
Answer: A

1. Which of the following activities should be performed first to compile a list of vulnerabilities in an environment?
A. Automated scanning
B. Penetration testing
C. Threat hunting
D. Log aggregation
E. Adversarial emulation
Answer: A

1. A company with a high-availability website is looking to harden its controls at any cost. The company wants to ensure that the site is secure by finding any possible issues. Which of the following would most likely achieve this goal?
A. Permission restrictions
B. Bug bounty program
C. Vulnerability scan
D. Reconnaissance
Answer: B

1. A security administrator needs to reduce the attack surface in the company's data centers. Which of the following should the security administrator do to complete this task?
A. Implement a honeynet.
B. Define Group Policy on the servers.
C. Configure the servers for high availability.
D. Upgrade end-of-support operating systems.
Answer: D

1. Which of the following considerations is the most important for an organization to evaluate as it establishes and maintains a data privacy program?
A. Reporting structure for the data privacy officer
B. Request process for data subject access
C. Role as controller or processor
D. Physical location of the company
Answer: C

1. A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks. Which of the following analysis elements did the company most likely use in making this decision?
A. IMTTR
B. RTO
C. ARO
D. MTBF
Answer: C

1. A company has yearly engagements with a service provider. The general terms and conditions are the same for all engagements. The company wants to simplify the process and revisit the general terms every three years. Which of the following documents would provide the best way to set the general terms?
A. MSA
B. NDA
C. MOU
D. SLA
Answer: A

1. A user needs to complete training at https://comptiatraining.com. After manually entering the URL, the user sees that the accessed website is noticeably different from the standard company website. Which of the following is the most likely explanation for the difference?
A. Cross-site scripting
B. Pretexting
C. Typosquatting
D. Vishing
Answer: C

1. A security analyst is prioritizing vulnerability scan results using a risk-based approach. Which of the following is the most efficient resource for the analyst to use?
A. Business impact analysis
B. Common Vulnerability Scoring System
C. Risk register
D. Exposure factor
Answer: B

1. Which of the following would be the best way to handle a critical business application that is running on a legacy server?
A. Segmentation
B. Isolation
C. Hardening
D. Decommissioning
Answer: C

1. An employee clicked a malicious link in an email and downloaded malware onto the company's computer network. The malicious program exfiltrated thousands of customer records. Which of the following should the company implement to prevent this in the future?
A. User awareness training
B. Network monitoring
C. Endpoint protection
D. Data loss prevention
Answer: A

1. A company is implementing a policy to allow employees to use their personal equipment for work. However, the company wants to ensure that only company-approved applications can be installed. Which of the following addresses this concern?
A. MDM
B. Containerization
C. DLP
D. FIM
Answer: A

1. An organization is developing a security program that conveys the responsibilities associated with the general operation of systems and software within the organization. Which of the following documents would most likely communicate these expectations?
A. Business continuity plan
B. Change management procedure
C. Acceptable use policy
D. Software development life cycle policy
Answer: D

1. A systems administrator works for a local hospital and needs to ensure patient data is protected and secure.
Which of the following data classifications should be used to secure patient data?
A. Private
B. Critical
C. Sensitive
D. Public
Answer: C

1. An organization is evaluating new regulatory requirements associated with the implementation of corrective controls on a group of interconnected financial systems. Which of the following is the most likely reason for the new requirement?
A. To defend against insider threats altering banking details
B. To ensure that errors are not passed to other systems
C. To allow for business insurance to be purchased
D. To prevent unauthorized changes to financial data
Answer: B

1. Which of the following phases of the incident response process attempts to minimize disruption?
A. Recovery
B. Containment
C. Preparation
D. Analysis
Answer: B

1. A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?
A. Processor
B. Custodian
C. Subject
D. Owner
Answer: C

1. A company has a website in a server cluster. One server is experiencing very high usage, while others are nearly unused. Which of the following should the company configure to help distribute traffic quickly?
A. Server multiprocessing
B. Warm site
C. Load balancer
D. Proxy server
Answer: C

1. 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. Social engineering
B. Situational awareness
C. Phishing
D. Acceptable use policy
Answer: B

1. A company is considering an expansion of access controls for an application that contractors and internal employees use to reduce costs. Which of the following risk elements should the implementation team understand before granting access to the application?
A. Threshold
B. Appetite
C. Avoidance
D. Register
Answer: B

1. An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?
A. Secured zones
B. Subject role
C. Adaptive identity
D. Threat scope reduction
Answer: D

1. Which of the following is the first step to secure a newly deployed server?
A. Close unnecessary service ports.
B. Update the current version of the software.
C. Add the device to the ACL.
D. Upgrade the OS version.
Answer: A

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

B. Risk identification
C. Risk treatment
D. Risk monitoring and review
Answer: B

1. A certificate authority needs to post information about expired certificates. Which of the following would accomplish this task?
A. TPM
B. CRL
C. PKI
D. CSR
Answer: B

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

1. During a SQL update of a database, a temporary field used as part of the update sequence was modified by an attacker before the update completed in order to allow access to the system. Which of the following best describes this type of vulnerability?
A. Race condition
B. Memory injection
C. Malicious update
D. Side loading
Answer: A

1. A vendor needs to remotely and securely transfer files from one server to another using the command line. Which of the following protocols should be Implemented to allow for this type of access? (Select two).
A. SSH
B. SNMP
C. RDP
D. S/MIME
E. SMTP
F. SFTP
Answer: AF

1. An administrator is installing an LDAP browser tool in order to view objects in the corporate LDAP directory. Secure connections to the LDAP server are required. When the browser connects to the server, certificate errors are being displayed, and then the connection is terminated. Which of the following is the most likely solution?
A. The administrator should allow SAN certificates in the browser configuration.
B. The administrator needs to install the server certificate into the local truststore.
C. The administrator should request that the secure LDAP port be opened to the server.
D. The administrator needs to increase the TLS version on the organization's RA.
Answer: B

1. A security investigation revealed that malicious software was installed on a server using a server administrator's credentials. During the investigation, the server administrator explained that Telnet was regularly used to log in. Which of the following most likely occurred?
A. A spraying attack was used to determine which credentials to use.
B. A packet capture tool was used to steal the password.
C. A remote-access Trojan was used to install the malware.
D. A dictionary attack was used to log in as the server administrator.
Answer: B

1. A user is requesting Telnet access to manage a remote development web server. Insecure protocols are not allowed for use within any environment. Which of the following should be configured to allow remote access to this server?
A. HTTPS
B. SNMPv3
C. SSH
D. RDP
E. SMTP
Answer: C

1. A security administrator is working to find a cost-effective solution to implement certificates for a large number of domains and subdomains owned by the company. Which of the following types of certificates should the administrator implement?
A. Wildcard
B. Client certificate
C. Self-signed
D. Code signing
Answer: A

1. An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?
A. Hardening
B. Employee monitoring
C. Configuration enforcement
D. Least privilege
Answer: D

1. A business received a small grant to migrate its infrastructure to an off-premises solution. Which of the following should be considered first?
A. Security of cloud providers
B. Cost of implementation
C. Ability of engineers
D. Security of architecture
Answer: D

1. A company tested and validated the effectiveness of network security appliances within the corporate network. The IDS detected a high rate of SQL injection attacks against the company's servers, and the company's perimeter firewall is at capacity. Which of the following would be the best action to maintain security and reduce the traffic to the perimeter firewall?
A. Set the appliance to IPS mode and place it in front of the company firewall.
B. Convert the firewall to a WAF and use IPSec tunnels to increase throughput.
C. Set the firewall to fail open if it is overloaded with traffic and send alerts to the SIEM.
D. Configure the firewall to perform deep packet inspection and monitor TLS traffic.
Answer: A

1. Which of the following describes effective change management procedures?
A. Approving the change after a successful deployment
B. Having a backout plan when a patch fails
C. Using a spreadsheet for tracking changes
D. Using an automatic change control bypass for security updates
Answer: B

1. An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group. Which of the following access controls is most likely causing the lack of access?
A. Role-based
B. Discretionary
C. Time of day
D. Least privilege
Answer: A

1. A company needs to keep the fewest records possible, meet compliance needs, and ensure destruction of records that are no longer needed.
Which of the following best describes the policy that meets these requirements?
A. Security policy
B. Classification policy
C. Retention policy
D. Access control policy
Answer: C

1. A company is experiencing a web services outage on the public network. The services are up and available but inaccessible. The network logs show a sudden increase in network traffic that is causing the outage. Which of the following attacks is the organization experiencing?
A. ARP poisoning
B. Brute force
C. Buffer overflow
D. DDoS
Answer: D

1. Which of the following threat actors is the most likely to be motivated by profit?
A. Hacktivist
B. Insider threat
C. Organized crime
D. Shadow IT
Answer: C

1. A systems administrator uses a key to encrypt a message being sent to a peer in a different branch office. The peer then uses the same key to decrypt the message. Which of the following describes this example?
A. Symmetric
B. Asymmetric
C. Hashing
D. Salting
Answer: A

1. An enterprise is working with a third party and needs to allow access between the internal networks of both parties for a secure file migration. The solution needs to ensure encryption is applied to all traffic that is traversing the networks. Which of the following solutions should most likely be implemented?
A. EAP
B. IPSec
C. SD-WAN
D. TLS
Answer: B

1. The Chief Information Security Officer (CISO) has determined the company is non- compliant with local data privacy regulations. The CISO needs to justify the budget request for more resources. Which of the following should the CISO present to the board as the direct consequence of non- compliance?
A. Fines
B. Reputational damage
C. Sanctions
D. Contractual implications
Answer: A

1. A Chief Information Security Officer would like to conduct frequent, detailed reviews of systems and procedures to track compliance objectives. Which of the following will be the best method to achieve this objective?
A. Third-party attestation
B. Penetration testing
C. Internal auditing
D. Vulnerability scans
Answer: C

1. Which of the following is a possible factor for MFA?
A. Something you exhibit
B. Something you have
C. Somewhere you are
D. Someone you know
Answer: B

1. An incident analyst finds several image files on a hard disk. The image files may contain geolocation coordinates. Which of the following best describes the type of information the analyst is trying to extract from the image files?
A. Log data
B. Metadata
C. Encrypted data
D. Sensitive data
Answer: B

1. A security administrator is working to secure company data on corporate laptops in case the laptops are stolen. Which of the following solutions should the administrator consider?
A. Disk encryption
B. Data loss prevention
C. Operating system hardening
D. Boot security
Answer: A

1. Which of the following is the best reason an organization should enforce a data classification policy to help protect its most sensitive information?
A. End users will be required to consider the classification of data that can be used in documents.
B. The policy will result in the creation of access levels for each level of classification.
C. The organization will have the ability to create security requirements based on classification levels.
D. Security analysts will be able to see the classification of data within a document before opening it.
Answer: C

1. An analyst is performing a vulnerability scan against the web servers exposed to the internet without a system account. Which of the following is most likely being performed?
A. Non-credentialed scan
B. Packet capture
C. Privilege escalation
D. System enumeration
E. Passive scan
Answer: A

1. Which of the following addresses individual rights such as the right to be informed, the right of access, and the right to be forgotten?
A. GDPR
B. PCI DSS
C. NIST
D. ISO
Answer: A

1. A third-party vendor is moving a particular application to the end-of-life stage at the end of the current year. Which of the following is the most critical risk if the company chooses to continue running the application?
A. Lack of security updates
B. Lack of new features
C. Lack of support
D. Lack of source code access
Answer: A

1. A systems administrator would like to create a point-in-time backup of a virtual machine. Which of the following should the administrator use?
A. Replication
B. Simulation
C. Snapshot
D. Containerization
Answer: C

1. A malicious update was distributed to a common software platform and disabled services at many organizations. Which of the following best describes this type of vulnerability?
A. DDoS attack
B. Rogue employee
C. Insider threat
D. Supply chain
Answer: D

1. Which of the following threat actors is the most likely to seek financial gain through the use of ransomware attacks?
A. Organized crime
B. Insider threat
C. Nation-state
D. Hacktivists
Answer: A

1. Which of the following activities are associated with vulnerability management? (Choose two.)
A. Reporting
B. Prioritization
C. Exploiting
D. Correlation
E. Containment
F. Tabletop exercise
Answer: AB

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

A. A disruption of business operations
B. Unauthorized access to the system
C. Reports of false positives
D. Finding security gaps in the system
Answer: A

1. Which of the following is the most relevant reason a DPO would develop a data inventory?
A. To manage data storage requirements better
B. To determine the impact in the event of a breach
C. To extend the length of time data can be retained
D. To automate the reduction of duplicated data
Answer: B

1. Which of the following cryptographic solutions protects data at rest?
A. Digital signatures
B. Full disk encryption
C. Private key
D. Steganography
Answer: B

1. Which of the following should an organization use to protect its environment from external attacks conducted by an unauthorized hacker?
A. ACL
B. IDS
C. HIDS
D. NIPS
Answer: D

1. Which of the following would enable a data center to remain operational through a multiday power outage?
A. Generator
B. Uninterruptible power supply
C. Replication
D. Parallel processing
Answer: A

1. For which of the following reasons would a systems administrator leverage a 3DES hash from an installer file that is posted on a vendor's website?
A. To test the integrity of the file
B. To validate the authenticity of the file
C. To activate the license for the file
D. To calculate the checksum of the file
Answer: A

1. Which of the following activities is included in the post-incident review phase?
A. Determining the root cause of the incident
B. Developing steps to mitigate the risks of the incident
C. Validating the accuracy of the evidence collected during the investigation
D. Reestablishing the compromised system's configuration and settings
Answer: A

1. 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
Answer: A

1. Which of the following is most likely to be used as a just-in-time reference document within a security operations center?
A. Change management policy
B. Risk profile
C. Playbook
D. SIEM profile
Answer: C

1. Executives at a company are concerned about employees accessing systems and information about sensitive company projects unrelated to the employees' normal job duties. Which of the following enterprise security capabilities will the security team most likely deploy to detect that activity?
A. UBA
B. EDR
C. NAC
D. DLP
Answer: A

1. Several customers want an organization to verify its security controls are operating effectively and have requested an independent opinion. Which of the following is the most efficient way to address these requests?
A. Hire a vendor to perform a penetration test
B. Perform an annual self-assessment.
C. Allow each client the right to audit
D. Provide a third-party attestation report
Answer: D

1. A university employee logged on to the academic server and attempted to guess the system administrators' log-in credentials. Which of the following security measures should the university have implemented to detect the employee's attempts to gain access to the administrators' accounts?
A. Two-factor authentication
B. Firewall
C. Intrusion prevention system
D. User activity logs
Answer: D

1. Which of the following consequences would a retail chain most likely face from customers in the event the retailer is non-compliant with PCI DSS?
A. Contractual impacts
B. Sanctions
C. Fines
D. Reputational damage
Answer: D

1. An administrator is installing an SSL certificate on a new system. During testing, errors indicate that the certificate is not trusted. The administrator has verified with the issuing CA and has validated the private key. Which of the following should the administrator check for next?
A. If the wildcard certificate is configured
B. If the certificate signing request is valid
C. If the root certificate is installed
D. If the public key is configured
Answer: C

1. An employee emailed a new systems administrator a malicious web link and convinced the administrator to change the email server's password. The employee used this access to remove the mailboxes of key personnel. Which of the following security awareness concepts would help prevent this threat in the future?
A. Recognizing phishing
B. Providing situational awareness training
C. Using password management
D. Reviewing email policies
Answer: A

1. A new security regulation was announced that will take effect in the coming year. A company must comply with it to remain in business. Which of the following activities should the company perform next?
A. Gap analysis
B. Policy review
C. Security procedure evaluation
D. Threat scope reduction
Answer: A

1. An accountant is transferring information to a bank over FTP. Which of the following mitigations should the accountant use to protect the confidentiality of the data?
A. Tokenization
B. Data masking
C. Encryption
D. Obfuscation

Answer: C

1. An organization has recently decided to implement SSO. The requirements are to leverage access tokens and focus on application authorization rather than user authentication. Which of the following solutions would the engineering team most likely configure?
A. LDAP
B. Federation
C. SAML
D. OAuth
Answer: D

1. Which of the following would most likely be used by attackers to perform credential harvesting?
A. Social engineering
B. Supply chain compromise
C. Third-party software
D. Rainbow table
Answer: A

1. A security engineer would like to enhance the use of automation and orchestration within the SIEM. Which of the following would be the primary benefit of this enhancement?
A. It increases complexity.
B. It removes technical debt.
C. It adds additional guard rails.
D. It acts as a workforce multiplier.
Answer: D

1. An organization issued new laptops to all employees and wants to provide web filtering both in and out of the office without configuring additional access to the network. Which of the following types of web filtering should a systems administrator configure?
A. Agent-based
B. Centralized proxy
C. URL scanning
D. Content categorization
Answer: A

1. Which of the following provides the best protection against unwanted or insecure communications to and from a device?
A. System hardening
B. Host-based firewall
C. Intrusion detection system
D. Anti-malware software
Answer: B

1. An employee who was working remotely lost a mobile device containing company data. Which of the following provides the best solution to prevent future data loss?
A. MDM
B. DLP
C. FDE
D. EDR
Answer: C

1. An IT administrator needs to ensure data retention standards are implemented on an enterprise application. Which of the following describes the administrator's role?
A. Processor
B. Custodian
C. Privacy officer
D. Owner
Answer: B

1. A company plans to secure its systems by:
- Preventing users from sending sensitive data over corporate email
- Restricting access to potentially harmful websites
Which of the following features should the company set up? (Choose two.)
A. DLP software
B. DNS filtering
C. File integrity monitoring
D. Stateful firewall
E. Guardrails

F. Antivirus signatures
Answer: AB

1. A company processes and stores sensitive data on its own systems. Which of the following steps should the company take first to ensure compliance with privacy regulations?
A. Implement access controls and encryption.
B. Develop and provide training on data protection policies.
C. Create incident response and disaster recovery plans.
D. Purchase and install security software.
Answer: A

1. Which of the following cryptographic methods is preferred for securing communications with limited computing resources?
A. Hashing algorithm
B. Public key infrastructure
C. Symmetric encryption
D. Elliptic curve cryptography
Answer: C

1. Which of the following definitions best describes the concept of log correlation?
A. Combining relevant logs from multiple sources into one location
B. Searching and processing data to identify patterns of malicious activity
C. Making a record of the events that occur in the system
D. Analyzing the log files of the system components
Answer: B

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

1. Which of the following allows an exploit to go undetected by the operating system?
A. Firmware vulnerabilities
B. Side loading
C. Memory injection
D. Encrypted payloads
Answer: A

1. A malicious insider from the marketing team alters records and transfers company funds to a personal account. Which of the following methods would be the best way to secure company records in the future?
A. Permission restrictions
B. Hashing
C. Input validation
D. Access control list
Answer: D

1. An organization is required to provide assurance that its controls are properly designed and operating effectively. Which of the following reports will best achieve the objective?
A. Red teaming
B. Penetration testing
C. Independent audit
D. Vulnerability assessment
Answer: C

1. A systems administrator successfully configures VPN access to a cloud environment. Which of the following capabilities should the administrator use to best facilitate remote administration?
A. A jump host in the shared services security zone
B. An SSH server within the corporate LAN
C. A reverse proxy on the firewall
D. An MDM solution with conditional access
Answer: A

1. An audit reveals that cardholder database logs are exposing account numbers inappropriately.
Which of the following mechanisms would help limit the impact of this error?
A. Segmentation
B. Hashing
C. Journaling
D. Masking
Answer: D

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

1. A penetration tester enters an office building at the same time as a group of employees despite not having an access badge. Which of the following attack types is the penetration tester performing?
A. Tailgating
B. Shoulder surfing
C. RFID cloning
D. Forgery
Answer: A

1. An organization needs to monitor its users' activities in order to prevent insider threats. Which of the following solutions would help the organization achieve this goal?
A. Behavioral analytics
B. Access control lists
C. Identity and access management
D. Network intrusion detection system
Answer: A

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

B. Whaling
C. Smishing
D. Vishing
Answer: D

1. A security analyst is reviewing logs to identify the destination of command-and-control traffic originating from a compromised device within the on-premises network. Which of the following is the best log to review?
A. IDS
B. Antivirus
C. Firewall
D. Application
Answer: C

1. When trying to access an internal website, an employee reports that a prompt displays, stating that the site is insecure. Which of the following certificate types is the site most likely using?
A. Wildcard
B. Root of trust
C. Third party
D. Self-signed
Answer: D

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

Answer: A

1. Which of the following organizational documents is most often used to establish and communicate expectations associated with integrity and ethical behavior within an organization?
A. AUP
B. SLA
C. EULA
D. MOA
Answer: A

1. Which of the following explains how to determine the global regulations that data is subject to regardless of the country where the data is stored?
A. Geographic dispersion
B. Data sovereignty
C. Geographic restrictions
D. Data segmentation
Answer: B

1. An organization's web servers host an online ordering system. The organization discovers that the servers are vulnerable to a malicious JavaScript injection, which could allow attackers to access customer payment information. Which of the following mitigation strategies would be most effective for preventing an attack on the organization's web servers? (Choose two.)
A. Regularly updating server software and patches
B. Implementing strong password policies
C. Encrypting sensitive data at rest and in transit
D. Utilizing a web-application firewall
E. Performing regular vulnerability scans
F. Removing payment information from the servers
Answer: AD

1. During a SQL update of a database, a temporary field that was created was replaced by an attacker in order to allow access to the system. Which of the following best describes this type of vulnerability?
A. Race condition
B. Memory injection
C. Malicious update
D. Side loading
Answer: A

1. Which of the following elements of digital forensics should a company use if it needs to ensure the integrity of evidence?
A. Preservation
B. E-discovery
C. Acquisition
D. Containment
Answer: A

1. A security analyst wants to better understand the behavior of users and devices in order to gain visibility into potential malicious activities. The analyst needs a control to detect when actions deviate from a common baseline. Which of the following should the analyst use?
A. Intrusion prevention system
B. Sandbox
C. Endpoint detection and response
D. Antivirus
Answer: C

1. A legal department must maintain a backup from all devices that have been shredded and recycled by a third party. Which of the following best describes this requirement?
A. Data retention
B. Certification
C. Sanitization
D. Destruction
Answer: A

1. Which of the following can be used to compromise a system that is running an RTOS?
A. Cross-site scripting
B. Memory injection
C. Replay attack
D. Ransomware

Answer: B

1. A security architect wants to prevent employees from receiving malicious attachments by email. Which of the following functions should the chosen solution do?
A. Apply IP address reputation data.
B. Tap and monitor the email feed.
C. Scan email traffic inline.
D. Check SPF records.
Answer: C

1. Which of the following activities is the first stage in the incident response process?
A. Detection
B. Declaration
C. Containment
D. Verification
Answer: A

1. Which of the following is the main consideration when a legacy system that is a critical part of a company's infrastructure cannot be replaced?
A. Resource provisioning
B. Cost
C. Single point of failure
D. Complexity
Answer: C

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

1. An organization is implementing a COPE mobile device management policy. Which of the following should the organization include in the COPE policy? (Choose two.)
A. Remote wiping of the device
B. Data encryption
C. Requiring passwords with eight characters
D. Data usage caps
E. Employee data ownership
F. Personal application store access
Answer: AB

1. 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. Enable network intrusion detection.
D. Apply patch management.
Answer: A

1. Which of the following techniques can be used to sanitize the data contained on a hard drive while allowing for the hard drive to be repurposed?
A. Degaussing
B. Drive shredder
C. Retention platform
D. Wipe tool
Answer: D

1. An attacker submits a request containing unexpected characters in an attempt to gain unauthorized access to information within the underlying systems. Which of the following best describes this attack?
A. Side loading
B. Target of evaluation
C. Resource reuse
D. SQL injection
Answer: D

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

1. A company discovered its data was advertised for sale on the dark web. During the initial investigation, the company determined the data was proprietary data. Which of the following is the next step the company should take?
A. Identify the attacker's entry methods.
B. Report the breach to the local authorities.
C. Notify the applicable parties of the breach.
D. Implement vulnerability scanning of the company's systems.
Answer: C

1. Which of the following would be the best solution to deploy a low-cost standby site that includes hardware and internet access?
A. Recovery site
B. Cold site
C. Hot site
D. Warm site
Answer: D

1. An organization needs to determine how many employees are accessing the building each day in order to configure the proper access controls. Which of the following control types best meets this requirement?
A. Detective
B. Preventive
C. Corrective
D. Directive
Answer: A

1. A security consultant is working with a client that wants to physically isolate its secure systems.
Which of the following best describes this architecture?
A. SDN
B. Air gapped
C. Containerized
D. Highly available
Answer: B

1. A company is in the process of migrating to cloud-based services. The company's IT department has limited resources for migration and ongoing support. Which of the following best meets the company's needs?
A. IPS
B. WAF
C. SASE
D. IAM
Answer: C

1. An employee clicks a malicious link in an email that appears to be from the company's Chief Executive Officer. The employee's computer is infected with ransomware that encrypts the company's files. Which of the following is the most effective way for the company to prevent similar incidents in the future?
A. Security awareness training
B. Database encryption
C. Segmentation
D. Reporting suspicious emails
Answer: A

1. Which of the following best describe the benefits of a microservices architecture when compared to a monolithic architecture? (Choose two.)
A. Easier debugging of the system
B. Reduced cost of ownership of the system
C. Improved scalability of the system
D. Increased compartmentalization of the system
E. Stronger authentication of the system

F. Reduced complexity of the system
Answer: CD

1. A user's workstation becomes unresponsive and displays a ransom note demanding payment to decrypt files. Before the attack, the user opened a resume they received in a message, browsed the company's website, and installed OS updates. Which of the following is the most likely vector of this attack?
A. Spear-phishing attachment
B. Watering hole
C. Infected website
D. Typo squatting
Answer: A

1. A penetration tester finds an unused Ethernet port during an on-site penetration test. Upon plugging a device into the unused port, the penetration tester notices that the machine is assigned an IP address, allowing the tester to enumerate the local network. Which of the following should an administrator implement in order to prevent this situation from happening in the future?
A. Port security
B. Transport Layer Security
C. Proxy server
D. Security zones
Answer: A

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

1. A company is concerned about theft of client data from decommissioned laptops. Which of the following is the most cost-effective method to decrease this risk?
A. Wiping
B. Recycling
C. Shredding
D. Deletion
Answer: A

1. A government official receives a blank envelope containing photos and a note instructing the official to wire a large sum of money by midnight to prevent the photos from being leaked on the internet. Which of the following best describes the threat actor's intent?
A. Organized crime
B. Philosophical beliefs
C. Espionage
D. Blackmail
Answer: D

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

1. A malicious actor conducted a brute-force attack on a company's web servers and eventually gained access to the company's customer information database. Which of the following is the most effective way to prevent similar attacks?
A. Regular patching of servers
B. Web application firewalls
C. Multifactor authentication
D. Enabling encryption of customer data
Answer: C

1. Due to a cyberattack, a company's IT systems were not operational for an extended period of time. The company wants to measure how quickly the systems must be restored in order to minimize business disruption. Which of the following would the company most likely use?
A. Recovery point objective
B. Risk appetite
C. Risk tolerance
D. Recovery time objective

E. Mean time between failure
Answer: D

1. Which of the following actors attacking an organization is the most likely to be motivated by personal beliefs?
A. Nation-state
B. Organized crime
C. Hacktivist
D. Insider threat
Answer: C

1. Which of the following should a security team use to document persistent vulnerabilities with related recommendations?
A. Audit report
B. Risk register
C. Compliance report
D. Penetration test
Answer: B

1. An organization purchased a critical business application containing sensitive data. The organization would like to ensure that the application is not exploited by common data exfiltration attacks. Which of the following approaches would best help to fulfill this requirement?
A. URL scanning
B. WAF
C. Reverse proxy
D. NAC
Answer: B

1. A company is performing a risk assessment on new software the company plans to use. Which of the following should the company assess during this process?
A. Software vulnerabilities
B. Cost-benefit analysis
C. Ongoing monitoring strategies
D. Network infrastructure compatibility
Answer: A

1. A malicious actor is trying to access sensitive financial information from a company's database by intercepting and reusing log-in credentials. Which of the following attacks is the malicious actor attempting?
A. SQL injection
B. On-path
C. Brute-force
D. Password spraying
Answer: B

1. A new employee accessed an unauthorized website. An investigation found that the employee violated the company's rules. Which of the following did the employee violate?
A. MOU
B. AUP
C. NDA
D. MOA
Answer: B

1. A systems administrator is reviewing the VPN logs and notices that during non-working hours a user is accessing the company file server and information is being transferred to a suspicious IP address. Which of the following threats is most likely occurring?
A. Typo squatting
B. Root or trust
C. Data exfiltration
D. Blackmail
Answer: C

1. A network engineer is increasing the overall security of network devices and needs to harden the devices. Which of the following will best accomplish this task?
A. Configuring centralized logging
B. Generating local administrator accounts
C. Replacing Telnet with SSH
D. Enabling HTTP administration
Answer: C

1. A company's accounting department receives an urgent payment message from the company's bank domain with instructions to wire transfer funds. The sender requests that the transfer be completed as soon as possible. Which of the following attacks is described?
A. Business email compromise
B. Vishing
C. Spear phishing
D. Impersonation
Answer: A

1. A company filed a complaint with its IT service provider after the company discovered the service provider's external audit team had access to some of the company's confidential information. Which of the following is the most likely reason the company filed the complaint?
A. The MOU had basic clauses from a template.
B. A SOW had not been agreed to by the client.
C. A WO had not been mutually approved.
D. A required NDA had not been signed.
Answer: D

1. An analyst is reviewing job postings to ensure sensitive company information is not being shared with the general public. Which of the following is the analyst most likely looking for?
A. Office addresses
B. Software versions
C. List of board members
D. Government identification numbers
Answer: B

1. An engineer has ensured that the switches are using the latest OS, the servers have the latest patches, and the endpoints' definitions are up to date. Which of the following will these actions most effectively prevent?
A. Zero-day attacks
B. Insider threats
C. End-of-life support
D. Known exploits
Answer: D

1. Which of the following is most likely a security concern when installing and using low-cost IoT devices in infrastructure environments?
A. Country of origin
B. Device responsiveness
C. Ease of deployment
D. Storage of data
Answer: D

1. A company captures log-in details and reviews them each week to identify conditions such as excessive log-in attempts and frequent lockouts. Which of the following should a security analyst recommend to improve security compliance monitoring?
A. Including the date and person who reviewed the information in a report
B. Adding automated alerting when anomalies occur
C. Requiring a statement each week that no exceptions were noted
D. Masking the username in a report to protect privacy
Answer: B

1. A security team is in the process of hardening the network against externally crafted malicious packets. Which of the following is the most secure method to protect the internal network?
A. Anti-malware solutions
B. Host-based firewalls
C. Intrusion prevention systems
D. Network access control
E. Network allow list
Answer: C

1. A company wants to add an MFA solution for all employees who access the corporate network remotely. Log-in requirements include something you know, are, and have. The company wants a solution that does not require purchasing third-party applications or specialized hardware. Which of the following MFA solutions would best meet the company's requirements?
A. Smart card with PIN and password
B. Security questions and a one-time passcode sent via email
C. Voice and fingerprint verification with an SMS one-time passcode
D. Mobile application-generated, one-time passcode with facial recognition
Answer: C

1. A company is using a legacy FTP server to transfer financial data to a third party. The legacy system does not support SFTP, so a compensating control is needed to protect the sensitive, financial data in transit. Which of the following would be the most appropriate for the company to use?
A. Telnet connection
B. SSH tunneling
C. Patch installation
D. Full disk encryption
Answer: B

1. A security manager wants to reduce the number of steps required to identify and contain basic threats. Which of the following will help achieve this goal?
A. SOAR
B. SIEM
C. DMARC
D. NIDS
Answer: A

1. The Chief Information Officer (CIO) asked a vendor to provide documentation detailing the specific objectives within the compliance framework that the vendor's services meet. The vendor provided a report and a signed letter stating that the services meet 17 of the 21 objectives. Which of the following did the vendor provide to the CIO?
A. Penetration test results
B. Self-assessment findings
C. Attestation of compliance
D. Third-party audit report
Answer: C

1. Which of the following describes the most effective way to address OS vulnerabilities after they are identified?
A. Endpoint protection
B. Removal of unnecessary software
C. Configuration enforcement
D. Patching
Answer: D

1. The management team reports that employees are missing features on company-provided tablets, which is causing productivity issues. The management team directs the IT team to resolve the issue within 48 hours. Which of the following would be the best solution for the IT team to leverage in this scenario?
A. EDR
B. COPE
C. MDM
D. FDE
Answer: C

1. An alert references attacks associated with a zero-day exploit. An analyst places a bastion host in the network to reduce the risk of the exploit. Which of the following types of controls is the analyst implementing?
A. Compensating
B. Detective
C. Operational
D. Physical
Answer: A

1. A security administrator is implementing encryption on all hard drives in an organization.
Which of the following security concepts is the administrator applying?
A. Integrity
B. Authentication
C. Zero Trust
D. Confidentiality
Answer: D

1. An administrator has configured a quarantine subnet for all guest devices that connect to the network. Which of the following would be best for the security team to perform before allowing access to corporate resources?
A. Device fingerprinting
B. Compliance attestation
C. Penetration test
D. Application vulnerability test
Answer: B

1. Which of the following testing techniques uses both defensive and offensive testing methodologies with developers to securely build key applications and software?
A. Blue
B. Yellow
C. Red
D. Green
Answer: B

1. An administrator wants to automate an account permissions update for a large number of accounts. Which of the following would best accomplish this task?
A. Security groups
B. Federation
C. User provisioning
D. Vertical scaling
Answer: C

1. Which of the following is the fastest and most cost-effective way to confirm a third-party supplier's compliance with security obligations?
A. Attestation report
B. Third-party audit
C. Vulnerability assessment
D. Penetration testing
Answer: A

1. Which of the following cryptographic solutions is used to hide the fact that communication is occurring?
A. Steganography
B. Data masking
C. Tokenization
D. Private key
Answer: A

1. Which of the following steps should be taken before mitigating a vulnerability in a production server?
A. Escalate the issue to the SDLC team.
B. Use the IR plan to evaluate the changes.
C. Perform a risk assessment to classify the vulnerability.
D. Refer to the change management policy.
Answer: D

1. A security engineer needs to quickly identify a signature from a known malicious file. Which of the following analysis methods would the security engineer most likely use?
A. Static
B. Sandbox
C. Network traffic
D. Package monitoring
Answer: A

1. 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. Typosquatting
B. Brand impersonation
C. On-path
D. Watering-hole
Answer: A

1. A growing organization, which hosts an externally accessible application, adds multiple virtual servers to improve application performance and decrease the resource usage on individual servers. Which of the following solutions is the organization most likely to employ to further increase performance and availability?
A. Load balancer
B. Jump server
C. Proxy server
D. SD-WAN
Answer: A

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

A. Impersonation
B. Replication
C. Phishing
D. Smishing
Answer: A

1. A company wants to ensure employees are allowed to copy files from a virtual desktop during the workday but are restricted during non-working hours. Which of the following security measures should the company set up?
A. Digital rights management
B. Role-based access control
C. Time-based access control
D. Network access control
Answer: C

1. Employees sign an agreement that restricts specific activities when leaving the company. Violating the agreement can result in legal consequences. Which of the following agreements does this best describe?
A. SLA
B. BPA
C. NDA
D. MOA
Answer: C

1. A systems administrator just purchased multiple network devices. Which of the following should the systems administrator perform to prevent attackers from accessing the devices by using publicly available information?
A. Install endpoint protection.
B. Disable ports/protocols.
C. Change default passwords.
D. Remove unnecessary software.
Answer: C

1. A CVE in a key back-end component of an application has been disclosed. The systems administrator is identifying all of the systems in the environment that are susceptible to this risk. Which of the following should the systems administrator perform?
A. Packet capture
B. Vulnerability scan
C. Metadata analysis
D. Automated reporting
Answer: B

1. Which of the following activities uses OSINT?
A. Social engineering testing
B. Data analysis of logs
C. Collecting evidence of malicious activity
D. Producing IOC for malicious artifacts
Answer: A

1. Which of the following is the act of proving to a customer that software developers are trained on secure coding?
A. Assurance
B. Contract
C. Due diligence
D. Attestation
Answer: D

1. An administrator is creating a secure method for a contractor to access a test environment. Which of the following would provide the contractor with the best access to the test environment?
A. Application server
B. Jump server
C. RDP server
D. Proxy server
Answer: B

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

D. Reputation
Answer: A

1. To which of the following security categories does an EDR solution belong?
A. Physical
B. Operational
C. Managerial
D. Technical
Answer: D

1. Which of the following describes the difference between encryption and hashing?
A. Encryption protects data in transit, while hashing protects data at rest.
B. Encryption replaces cleartext with ciphertext, while hashing calculates a checksum.
C. Encryption ensures data integrity, while hashing ensures data confidentiality.
D. Encryption uses a public-key exchange, while hashing uses a private key.
Answer: B

1. A Chief Information Security Officer (CISO) has developed information security policies that relate to the software development methodology. Which of the following would the CISO most likely include in the organization's documentation?
A. Peer review requirements
B. Multifactor authentication
C. Branch protection tests
D. Secrets management configurations
Answer: A

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

1. Which of the following is the best way to provide secure, remote access for employees while minimizing the exposure of a company's internal network?
A. VPN
B. LDAP
C. FTP
D. RADIUS
Answer: A

1. A company's gate access logs show multiple entries from an employee's ID badge within a two- minute period. Which of the following is this an example of?
A. RFID cloning
B. Side-channel attack
C. Shoulder surfing
D. Tailgating
Answer: A

1. A company evaluates several options that would allow employees to have remote access to the network. The security team wants to ensure the solution includes AAA to comply with internal security policies. Which of the following should the security team recommend?
A. IPSec with RADIUS
B. RDP connection with LDAPS
C. Web proxy for all remote traffic
D. Jump server with 802.1X
Answer: A

1. A Chief Information Security Officer (CISO) wants to:
- Prevent employees from downloading malicious content.
- Establish controls based on departments and users.
- Map internet access for business applications to specific service accounts.
- Restrict content based on categorization.
Which of the following should the CSO implement?
A. Web application firewall
B. Secure DNS server

C. Jump server
D. Next-generation firewall
Answer: D

1. Which of the following is an example of a treatment strategy for a continuous risk?
A. Email gateway to block phishing attempts
B. Background checks for new employees
C. Dual control requirements for wire transfers
D. Branch protection as part of the CI/CD pipeline
Answer: A

1. An organization wants to deploy software in a container environment to increase security.
Which of the following would limit the organization's ability to achieve this goal?
A. Regulatory compliance
B. Patch availability
C. Kernel version
D. Monolithic code
Answer: D

1. Prior to implementing a design change, the change must go through multiple steps to ensure that it does not cause any security issues.
Which of the following is most likely to be one of those steps?
A. Board review
B. Service restart
C. Backout planning
D. Maintenance
Answer: C

1. Which of the following are the first steps an analyst should perform when developing a heat map? (Choose two.)
A. Methodically walk around the office noting Wi-Fi signal strength.
B. Log in to each access point and check the settings.
C. Create or obtain a layout of the office.
D. Measure cable lengths between access points.
E. Review access logs to determine the most active devices.
F. Remove possible impediments to radio transmissions.
Answer: AC

1. Which of the following is used to improve security and overall functionality without losing critical application data?
A. Reformatting
B. Decommissioning
C. Patching
D. Encryption
Answer: C

1. An organization is preparing to export proprietary software to a customer. Which of the following would be the best way to prevent the loss of intellectual property?
A. Code signing
B. Obfuscation
C. Tokenization
D. Blockchain
Answer: B

1. In which of the following will unencrypted network traffic most likely be found?
A. SDN
B. IoT
C. VPN
D. SCADA
Answer: D

1. Which of the following is the best reason to perform a tabletop exercise?
A. To address audit findings
B. To collect remediation response times
C. To update the IRP
D. To calculate the ROI
Answer: C

1. Which of the following is a use of CVSS?
A. To determine the cost associated with patching systems
B. To identify unused ports and services that should be closed
C. To analyze code for defects that could be exploited
D. To prioritize the remediation of vulnerabilities
Answer: D

1. For an upcoming product launch, a company hires a marketing agency whose owner is a close relative of the Chief Executive Officer. Which of the following did the company violate?
A. Independent assessments
B. Supply chain analysis
C. Right-to-audit clause
D. Conflict of interest policy
Answer: D

1. An organization designs an inbound firewall with a fail-open configuration while implementing a website. Which of the following would the organization consider to be the highest priority?
A. Confidentiality
B. Non-repudiation
C. Availability
D. Integrity
Answer: C

1. An engineer needs to ensure that a script has not been modified before it is launched. Which of the following best provides this functionality?
A. Masking
B. Obfuscation
C. Hashing
D. Encryption
Answer: C

1. Which of the following is the most important element when defining effective security governance?
A. Discovering and documenting external considerations
B. Developing procedures for employee onboarding and offboarding
C. Assigning roles and responsibilities for owners, controllers, and custodians
D. Defining and monitoring change management procedures
Answer: C

1. While a school district is performing state testing, a security analyst notices all internet services are unavailable. The analyst discovers that ARP poisoning is occurring on the network and then terminates access for the host. Which of the following is most likely responsible for this malicious activity?
A. Unskilled attacker
B. Shadow IT
C. Insider threat
D. Nation-state
Answer: C

1. A new corporate policy requires all staff to use multifactor authentication to access company resources. Which of the following can be utilized to set up this form of identity and access management? (Choose two.)
A. Authentication tokens
B. Least privilege
C. Biometrics
D. LDAP
E. Password vaulting
F. SAML
Answer: AC

1. A help desk employee receives a call from someone impersonating the Chief Executive Officer. The caller asks for assistance with resetting a password. Which of the following best describes this event?
A. Vishing
B. Hacktivism
C. Blackmail
D. Misinformation
Answer: A

1. The number of tickets the help desk has been receiving has increased recently due to numerous false-positive phishing reports. Which of the following would be best to help to reduce the false positives?
A. Performing more phishing simulation campaigns
B. Improving security awareness training
C. Hiring more help desk staff
D. Implementing an incident reporting web page
Answer: B

1. A security report shows that during a two-week test period 80% of employees unwittingly disclosed their SSO credentials when accessing an external website. The organization purposely created the website to simulate a cost-free password complexity test. Which of the following would best help reduce the number of visits to similar websites in the future?
A. Block all outbound traffic from the intranet.
B. Introduce a campaign to recognize phishing attempts
C. Restrict internet access for the employees who disclosed credentials
D. Implement a deny list of websites
Answer: B

1. An organization that handles sensitive information wants to protect the information by using a reversible technology. Which of the following best satisfies this requirement?
A. Hardware security module
B. Hashing algorithm
C. Tokenization
D. Steganography
Answer: C

1. Which of the following actions best addresses a vulnerability found on a company's web server?
A. Patching
B. Segmentation
C. Decommissioning
D. Monitoring
Answer: A

1. A company is concerned about employees unintentionally introducing malware into the network. The company identified fifty employees who clicked on a link embedded in an email sent by the internal IT department. Which of the following should the company implement to best improve its security posture?
A. Social engineering training
B. SPF configuration
C. Simulated phishing campaign
D. Insider threat awareness
Answer: C

1. A penetration test identifies that an SMBv1 is enabled on multiple servers across an organization. The organization wants to remediate this vulnerability in the most efficient way possible. Which of the following should the organization use for this purpose?
A. GPO
B. ACL
C. SFTP
D. DLP
Answer: A

1. Which of the following best protects sensitive data in transit across a geographically dispersed infrastructure?
A. Encryption
B. Masking
C. Tokenization
D. Obfuscation
Answer: A

1. As part of new compliance audit requirements, multiple servers need to be segmented on different networks and should be reachable only from authorized internal systems. Which of the following would meet the requirements?
A. Configure firewall rules to block external access to Internal resources.
B. Set up a WAP to allow internal access from public networks.
C. Implement a new IPSec tunnel from internal resources.
D. Deploy an internal jump server to access resources.
Answer: A

1. Which of the following can be used to mitigate attacks from high-risk regions?

A. Obfuscation
B. Data sovereignty
C. IP geolocation
D. Encryption
Answer: C

1. The executive management team is mandating the company develop a disaster recovery plan. The cost must be kept to a minimum, and the money to fund additional internet connections is not available. Which of the following would be the best option?
A. Hot site
B. Cold site
C. Failover site
D. Warm site
Answer: B

1. The Chief Information Security Officer wants to discuss options for a disaster recovery site that allows the business to resume operations as quickly as possible. Which of the following solutions meets this requirement?
A. Hot site
B. Cold site
C. Geographic dispersion
D. Warm site
Answer: A

1. After failing an audit twice, an organization has been ordered by a government regulatory agency to pay fines.
Which of the following caused this action?
A. Non-compliance
B. Contract violations
C. Government sanctions
D. Rules of engagement
Answer: A

1. A company wants to ensure secure remote access to its internal network. The company has only one public IP and would like to avoid making any changes to the current network setup. Which of the following solutions would best accomplish this goal?
A. PAT
B. IPSec VPN
C. Perimeter network
D. Reverse proxy
Answer: B

1. A security administrator is reissuing a former employee's laptop. Which of the following is the best combination of data handling activities for the administrator to perform? (Select two).
A. Data retention
B. Certification
C. Tokenization
D. Classification
E. Sanitization
F. Enumeration
Answer: C E