Free CompTIA SY0-701 Practice Questions

Q1: A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

A. Accept

B. Transfer

C. Mitigate

D. Avoid

Correct Answer: B

Answer(s): B

Q2: Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

A. Risk tolerance

B. Risk transfer

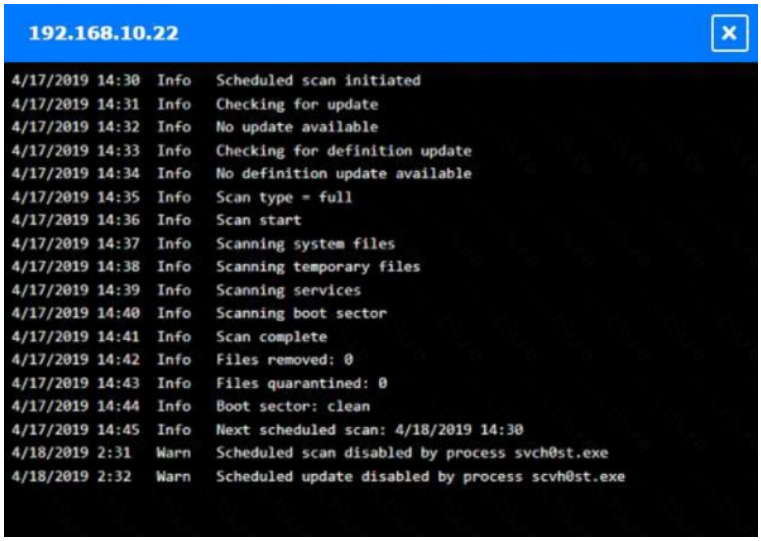
C. Risk register

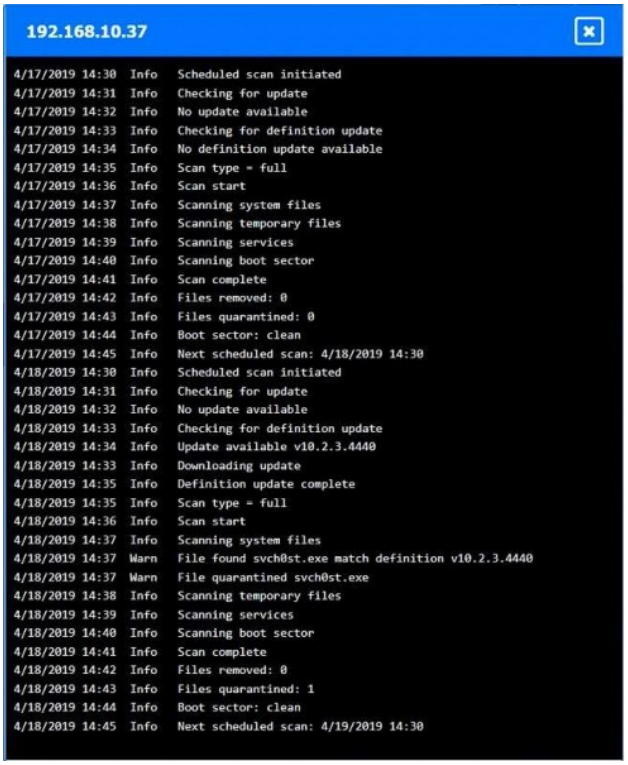
D. Risk analysis

Correct Answer: C

Answer(s): C

Q3: HOTSPOT (Drag and Drop is not supported) You are a security administrator investigating a potential infection on a network. INSTRUCTIONS Click on each host and firewall. Review all logs to determine which host originated the infection and then identify if each remaining host is clean or infected. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button. Hot Area:





192.168.10.41

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

Firewall

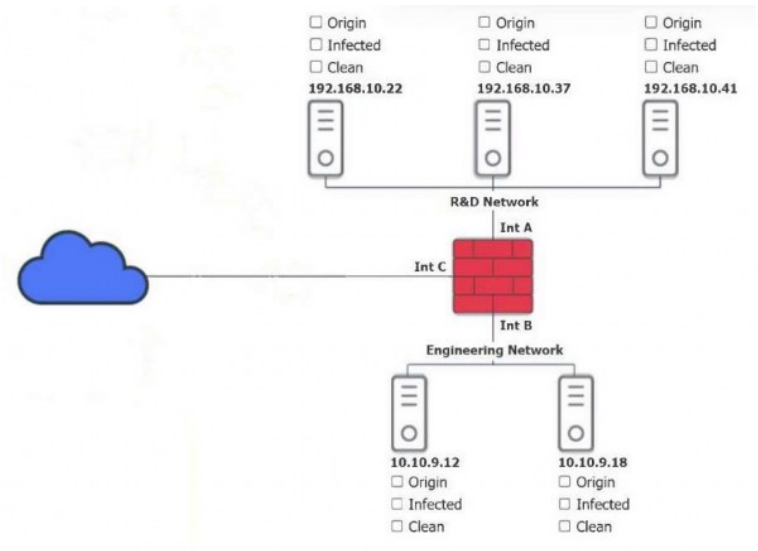
Timestamp	Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019 16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019 16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019 16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504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

10.10.9.12

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

10.10.9.18

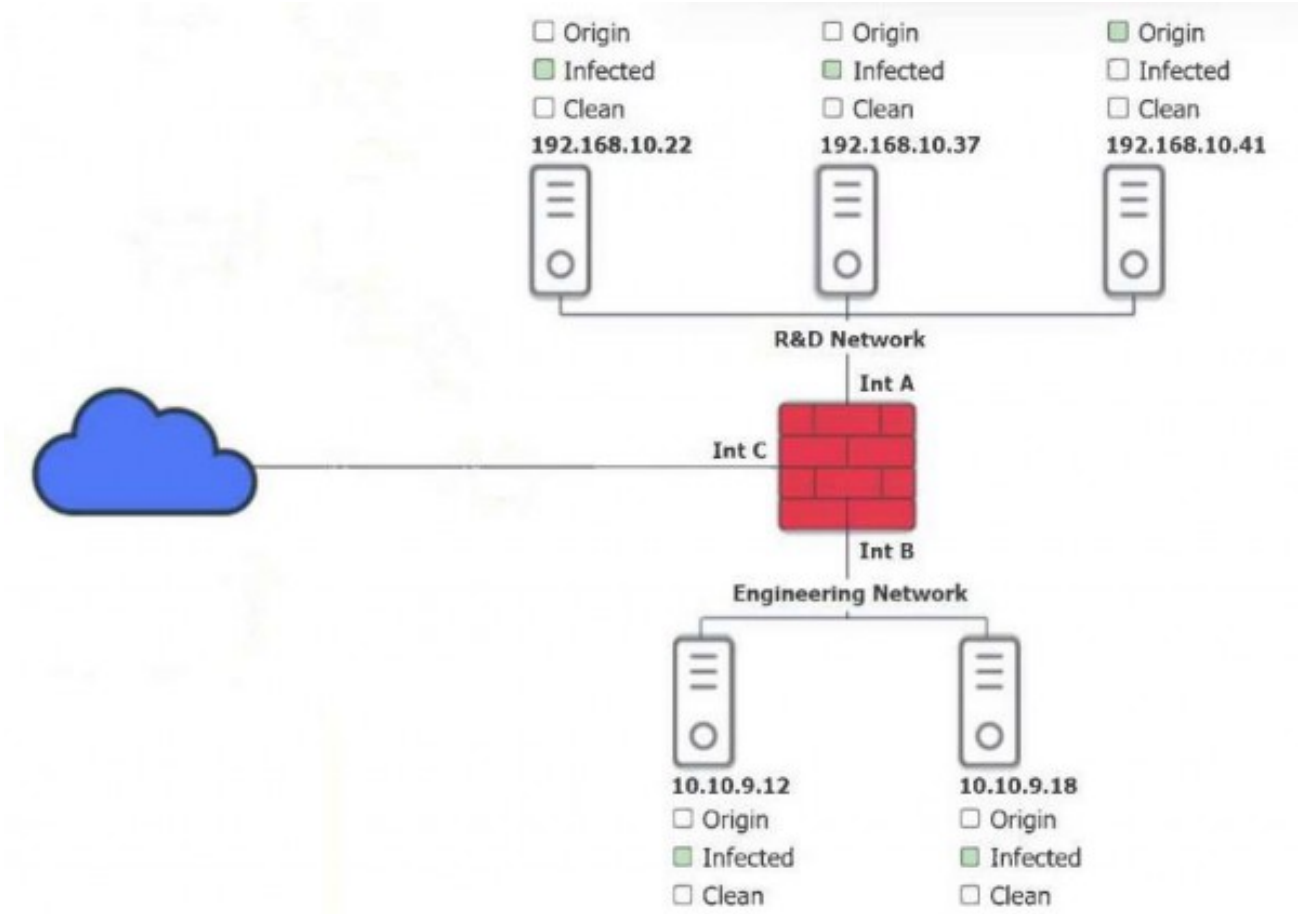
```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019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



A. See Explanation section for answer.

Correct Answer: A

Answer(s): A



Q4: A systems administrator notices that the research and development department is not using the company VPN when accessing various company-related services and systems. Which of the following scenarios describes this activity?

A. Espionage

B. Data exfiltration

C. Nation-state attack

D. Shadow IT

Correct Answer: D

Answer(s): D

Q5: 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

Correct Answer: A

Answer(s): A

Q6: Which of the following agreement types defines the time frame in which a vendor needs to respond?

A. SOW

B. SLA

C. MOA

D. MOU

Correct Answer: B

Answer(s): B

Q7: 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

Correct Answer: B

Answer(s): B

Q8: To improve the security at a data center, a security administrator implements a CCTV system and posts several signs about the possibility of being filmed. Which of the following best describe these types of controls? (Choose two.)

Answer(s): B,F

Q9: Which of the following examples would be best mitigated by input sanitization?

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

B. nmap - 10.11.1.130

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

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

Correct Answer: A

Answer(s): A

Q10: 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

Correct Answer: C

Answer(s): C

Q11: After conducting a vulnerability scan, a systems administrator notices that one of the identified vulnerabilities is not present on the systems that were scanned. Which of the following describes this example?

A. False positive

B. False negative

C. True positive

D. True negative

Correct Answer: A

Answer(s): A

Q12: A recent penetration test identified that an attacker could flood the MAC address table of network switches. Which of the following would best mitigate this type of attack?

A. Load balancer

B. Port security

C. IPS

D. NGFW

Correct Answer: B

Answer(s): B

Q13: A user would like to install software and features that are not available with a smartphone's default software. Which of the following would allow the user to install unauthorized software and enable new features?

A. SQLi

B. Cross-site scripting

C. Jailbreaking

D. Side loading

Correct Answer: C

Answer(s): C

Q14: Which of the following phases of an incident response involves generating reports?

A. Recovery

B. Preparation

C. Lessons learned

D. Containment

Correct Answer: C

Answer(s): C

Q15: Which of the following methods would most likely be used to identify legacy systems?

A. Bug bounty program

B. Vulnerability scan

C. Package monitoring

D. Dynamic analysis

Correct Answer: B

Answer(s): B

Q16: Employees located off-site must have access to company resources in order to complete their assigned tasks. These employees utilize a solution that allows remote access without interception concerns. Which of the following best describes this solution?

A. Proxy server

B. NGFW

C. VPN

D. Security zone

Correct Answer: C

Answer(s): C

Q17: 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

Correct Answer: B

Answer(s): B

Q18: 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

Correct Answer: D

Answer(s): D

Q19: 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

Correct Answer: B

Answer(s): B

Q20: An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Choose two.)

Answer(s): A,C

Q21: 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

Correct Answer: C

Answer(s): C

Q22: Which of the following security concepts is accomplished with the installation of a RADIUS server?

A. CIA

B. AAA

C. ACL

D. PEM

Correct Answer: B

Answer(s): B

Q23: 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

Correct Answer: D

Answer(s): D

Q24: 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

Correct Answer: B

Answer(s): B

Q25: 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.

Correct Answer: C

Answer(s): C

Q26: Which of the following teams is best suited to determine whether a company has systems that can be exploited by a potential, identified vulnerability?

A. Purple team

B. Blue team

C. Red team

D. White team

Correct Answer: C

Answer(s): C

Q27: 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

Correct Answer: A

Answer(s): A

Q28: Which of the following methods can be used to detect attackers who have successfully infiltrated a network? (Choose two.)

Answer(s): C,E

Q29: 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

Correct Answer: A

Answer(s): A

Q30: An organization completed a project to deploy SSO across all business applications last year. Recently, the finance department selected a new cloud-based accounting software vendor. Which of the following should most likely be configured during the new software deployment?

A. RADIUS

B. SAML

C. EAP

D. OpenID

Correct Answer: B

Answer(s): B

Q31: 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

Correct Answer: D

Answer(s): D

Q32: A network engineer deployed a redundant switch stack to increase system availability. However, the budget can only cover the cost of one ISP connection. Which of the following best describes the potential risk factor?

A. The equipment MTBF is unknown.

B. The ISP has no SLA.

C. An RPO has not been determined.

D. There is a single point of failure.

Correct Answer: D

Answer(s): D

Q33: 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.)

Answer(s): E,F

Q34: 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

Correct Answer: B

Answer(s): B

Q35: 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

Correct Answer: A

Answer(s): A

Q36: 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

Correct Answer: B

Answer(s): B

Q37: 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

Correct Answer: B

Answer(s): B

Q38: 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.)

Answer(s): A,F

Q39: A user downloaded software from an online forum. After the user installed the software, the security team observed external network traffic connecting to the user's computer on an uncommon port. Which of the following is the most likely explanation of this unauthorized connection?

A. The software had a hidden keylogger.

B. The software was ransomware.

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

D. The software contained a backdoor.

Correct Answer: D

Answer(s): D

Q40: A utility company is designing a new platform that will host all the virtual machines used by business applications. The requirements include: A starting baseline of 50% memory utilization Storage scalability Single circuit failure resilience Which of the following best meets all of these requirements?

A. Connecting dual PDUs to redundant power supplies

B. Transitioning the platform to an IaaS provider

C. Configuring network load balancing for multiple paths

D. Deploying multiple large NAS devices for each host

Correct Answer: B

Answer(s): B

Q41: Which of the following best describes a use case for a DNS sinkhole?

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

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

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

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

Correct Answer: C

Answer(s): C

Q42: 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

Correct Answer: B

Answer(s): B

Q43: 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

Correct Answer: D

Answer(s): D

Q44: During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?

A. Whaling

B. Credential harvesting

C. Prepending

D. Dumpster diving

Correct Answer: D

Answer(s): D

Q45: 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

Correct Answer: A

Answer(s): A

Q46: 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

Correct Answer: B

Answer(s): B

Q47: 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

Correct Answer: B

Answer(s): B

Q48: A hosting provider needs to prove that its security controls have been in place over the last six months and have sufficiently protected customer data. Which of the following would provide the best proof that the hosting provider has met the requirements?

A. NIST CSF

B. SOC 2 Type 2 report

C. CIS Top 20 compliance reports

D. Vulnerability report

Correct Answer: B

Answer(s): B

Q49: 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

Correct Answer: C

Answer(s): C

Q50: Which of the following is considered a preventive control?

A. Configuration auditing

B. Log correlation

C. Incident alerts

D. Segregation of duties

Correct Answer: D

Answer(s): D

Q51: A systems administrator notices that a testing system is down. While investigating, the systems administrator finds that the servers are online and accessible from any device on the server network. The administrator reviews the following information from the monitoring system: Which of the following is the most likely cause of the outage?

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

A. Denial of service

B. ARP poisoning

C. Jamming

D. Kerberoasting

Correct Answer: A

Answer(s): A

Q52: 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.

Correct Answer: D

Answer(s): D

Q53: 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

Correct Answer: A

Answer(s): A

Q54: 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

Correct Answer: C

Answer(s): C

Q55: Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

A. Code repositories

B. Dark web

C. Threat feeds

D. State actors

E. Vulnerability databases

Correct Answer: A

Answer(s): A

Q56: Which of the following is the best reason an organization should enforce a data classification policy to help protect its most sensitive information?

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

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

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

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

Correct Answer: C

Answer(s): C

Q57: 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

Correct Answer: A

Answer(s): A

Q58: 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

Correct Answer: A

Answer(s): A

Q59: An architect has a request to increase the speed of data transfer using JSON requests externally. Currently, the organization uses SFTP to transfer data files. Which of the following will most likely meet the requirements?

A. A website-hosted solution

B. Cloud shared storage

C. A secure email solution

D. Microservices using API

Correct Answer: D

Answer(s): D

Q60: 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

Correct Answer: A

Answer(s): A

Q61: An administrator is installing an LDAP browser tool in order to view objects in the corporate LDAP directory. Secure connections to the LDAP server are required. When the browser connects to the server, certificate errors are being displayed, and then the connection is terminated. Which of the following is the most likely solution?

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

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

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

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

Correct Answer: B

Answer(s): B

Q62: Which of the following is the most important security concern when using legacy systems to provide production service?

A. Instability

B. Lack of vendor support

C. Loss of availability

D. Use of insecure protocols

Correct Answer: B

Answer(s): B

Q63: 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.

Correct Answer: B

Answer(s): B

Q64: 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

Correct Answer: C

Answer(s): C

Q65: 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

Correct Answer: A

Answer(s): A

Q66: An auditor discovered multiple insecure ports on some servers. Other servers were found to have legacy protocols enabled. Which of the following tools did the auditor use to discover these issues?

A. Nessus

B. curl

C. Wireshark

D. netcat

Correct Answer: A

Answer(s): A

Q67: A security analyst received a tip that sensitive proprietary information was leaked to the public. The analyst is reviewing the PCAP and notices traffic between an internal server and an external host that includes the following: ... 12:47:22.327233 PPPoE [ses 0x8122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41), length 331) 10.5.1.1 > 52.165.16.154: IP6 (hlim E3, next- header TCP (6) paylcad length: 271) 2001:67c:2158:a019::ace.53104 > 2001:0:5ef5:79fd:380c:dddd:a601:24fa.13788: Flags [P.], cksum 0xd7ee (correct), seq 97:348, ack 102, win 16444, length 251 ... Which of the following was most likely used to exfiltrate the data?

A. Encapsulation

B. MAC address spoofing

C. Steganography

D. Broken encryption

E. Sniffing via on-path position

Correct Answer: A

Answer(s): A

Q68: A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?

A. Serverless architecture

B. Thin clients

C. Private cloud

D. Virtual machines

Correct Answer: A

Answer(s): A

Q69: A security administrator is performing an audit on a stand-alone UNIX server, and the following message is immediately displayed: (Error 13): /etc/shadow: Permission denied. Which of the following best describes the type of tool that is being used?

A. Pass-the-hash monitor

B. File integrity monitor

C. Forensic analysis

D. Password cracker

Correct Answer: D

Answer(s): D

Q70: A security administrator needs to create firewall rules for the following protocols: RTP, SIP, H.323. and SRTP. Which of the following does this rule set support?

A. RTOS

B. VoIP

C. SoC

D. HVAC

Correct Answer: B

Answer(s): B

Q71: 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

Correct Answer: A

Answer(s): A

Q72: 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

Correct Answer: B

Answer(s): B

Q73: 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

Correct Answer: A

Answer(s): A

Q74: A company hired an external consultant to assist with required system upgrades to a critical business application. A systems administrator needs to secure the consultant's access without sharing passwords to critical systems. Which of the following solutions should most likely be utilized?

A. TACACS+

B. SAML

C. An SSO platform

D. Role-based access control

E. PAM software

Correct Answer: E

Answer(s): E

Q75: 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.

Correct Answer: C

Answer(s): C

Q76: Which of the following data roles is responsible for identifying risks and appropriate access to data?

A. Owner

B. Custodian

C. Steward

D. Controller

Correct Answer: A

Answer(s): A

Q77: Which of the following physical controls can be used to both detect and deter? (Choose two.)

Answer(s): A,D

Q78: A multinational bank hosts several servers in its data center. These servers run a business-critical application used by customers to access their account information. Which of the following should the bank use to ensure accessibility during peak usage times?

A. Load balancer

B. Cloud backups

C. Geographic dispersal

D. Disk multipathing

Correct Answer: A

Answer(s): A

Q79: The author of a software package is concerned about bad actors repackaging and inserting malware into the software. The software download is hosted on a website, and the author exclusively controls the website's contents. Which of the following techniques would best ensure the software's integrity?

A. Input validation

B. Code signing

C. Secure cookies

D. Fuzzing

Correct Answer: B

Answer(s): B

Q80: 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

Correct Answer: A

Answer(s): A

Q81: A security analyst recently read a report about a flaw in several of the organization's printer models that causes credentials to be sent over the network in cleartext, regardless of the encryption settings. Which of the following would be best to use to validate this finding?

A. Wireshark

B. netcat

C. Nessus

D. Nmap

Correct Answer: A

Answer(s): A

Q82: A development team is launching a new public-facing web product. The Chief Information Security Officer has asked that the product be protected from attackers who use malformed or invalid inputs to destabilize the system. Which of the following practices should the development team implement?

A. Fuzzing

B. Continuous deployment

C. Static code analysis

D. Manual peer review

Correct Answer: A

Answer(s): A

Q83: 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

Correct Answer: D

Answer(s): D

Q84: Which of the following is best to use when determining the severity of a vulnerability?

A. CVE

B. OSINT

C. SOAR

D. CVSS

Correct Answer: D

Answer(s): D

Q85: An organization experienced a security breach that allowed an attacker to send fraudulent wire transfers from a hardened PC exclusively to the attacker's bank through remote connections. A security analyst is creating a timeline of events and has found a different PC on the network containing malware. Upon reviewing the command history, the analyst finds the following: PS>.\mimikatz.exe "sekurlsa::pth /user:localadmin /domain:corp-domain.com /ntlm:B4B9B02E1F29A3CF193EAB28C8D617D3F327 Which of the following best describes how the attacker gained access to the hardened PC?

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

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

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

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

Correct Answer: B

Answer(s): B

Q86: Which of the following is the best resource to consult for information on the most common application exploitation methods?

A. OWASP

B. STIX

C. OVAL

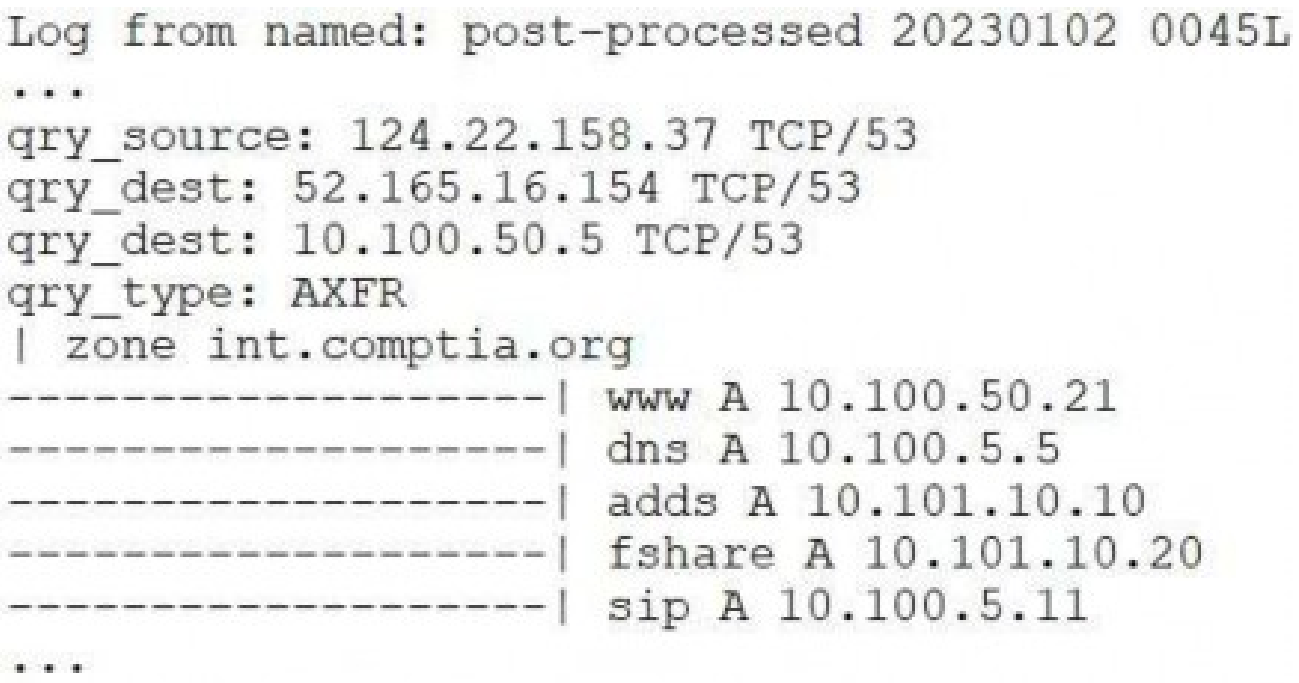
D. Threat intelligence feed

E. Common Vulnerabilities and Exposures

Correct Answer: A

Answer(s): A

Q87: A security analyst is reviewing the logs on an organization's DNS server and notices the following unusual snippet: Which of the following attack techniques was most likely used?



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

B. Bypassing the organization's DNS sinkholing

C. Footprinting the internal network

D. Attempting to achieve initial access to the DNS server

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

Correct Answer: C

Answer(s): C

Q88: 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.)

Answer(s): B,D

Q89: 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.)

Answer(s): A,E

Q90: A systems administrator would like to create a point-in-time backup of a virtual machine. Which of the following should the administrator use?

A. Replication

B. Simulation

C. Snapshot

D. Containerization

Correct Answer: C

Answer(s): C

Q91: 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

Correct Answer: B

Answer(s): B

Q92: Which of the following is a common data removal option for companies that want to wipe sensitive data from hard drives in a repeatable manner but allow the hard drives to be reused?

A. Sanitization

B. Formatting

C. Degaussing

D. Defragmentation

Correct Answer: A

Answer(s): A

Q93: 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

Correct Answer: D

Answer(s): D

Q94: A security officer is implementing a security awareness program and has placed security-themed posters around the building and assigned online user training. Which of the following will the security officer most likely implement?

A. Password policy

B. Access badges

C. Phishing campaign

D. Risk assessment

Correct Answer: C

Answer(s): C

Q95: 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

Correct Answer: D

Answer(s): D

Q96: 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.

Correct Answer: A

Answer(s): A

Q97: 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

Correct Answer: D

Answer(s): D

Q98: 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

Correct Answer: A

Answer(s): A

Explanation:

Reference: https://www.strongdm.com/what-is/agentless-monitoring

---

Q99: 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

Correct Answer: B

Answer(s): B

Q100: Which of the following agreement types is used to limit external discussions?

A. BPA

B. NDA

C. SLA

D. MSA

Correct Answer: B

Answer(s): B

Q101: 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

Correct Answer: D

Answer(s): D

Q102: Which of the following is used to conceal credit card information in a database log file?

A. Tokenization

B. Masking

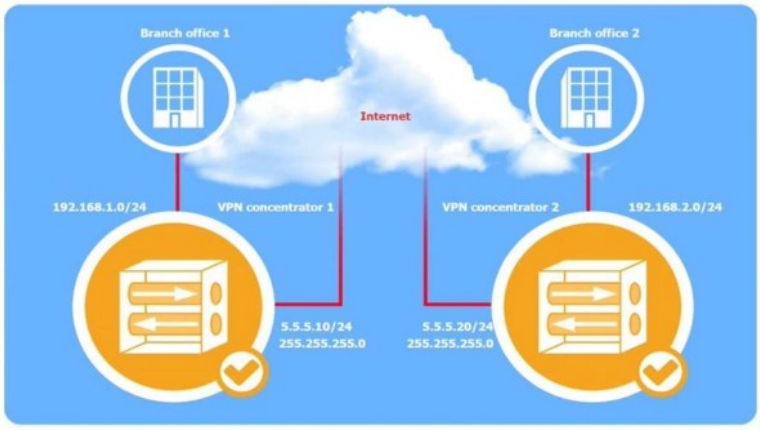
C. Hashing

D. Obfuscation

Correct Answer: B

Answer(s): B

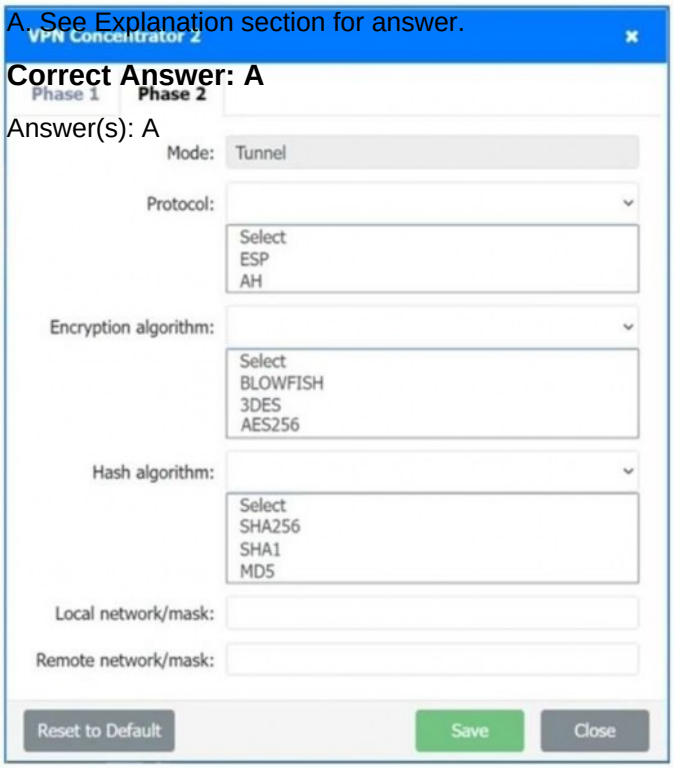
Q103: SIMULATION A systems administrator is configuring a site-to-site VPN between two branch offices. Some of the settings have already been configured correctly. The systems administrator has been provided the following requirements as part of completing the configuration: Most secure algorithms should be selected All traffic should be encrypted over the VPN A secret password will be used to authenticate the two VPN concentrators INSTRUCTIONS Click on the two VPN Concentrators to configure the appropriate settings. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

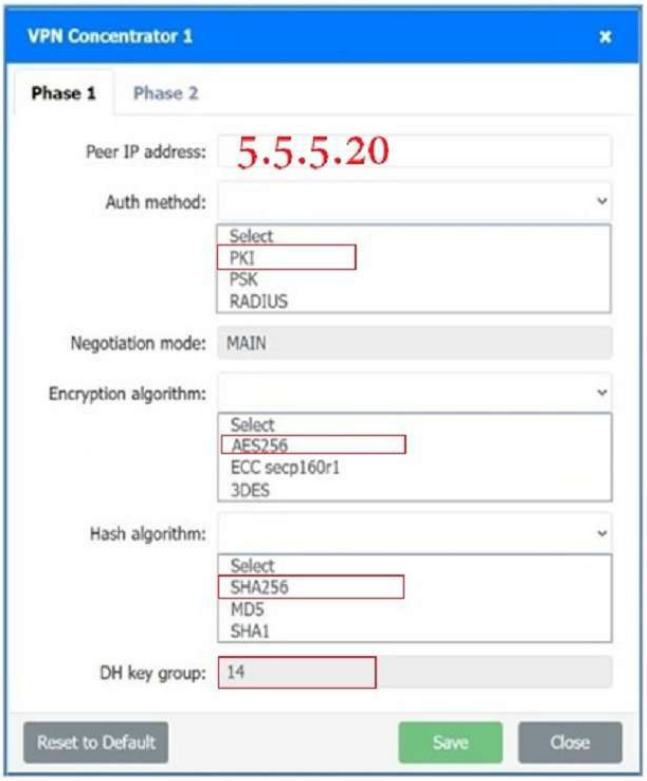


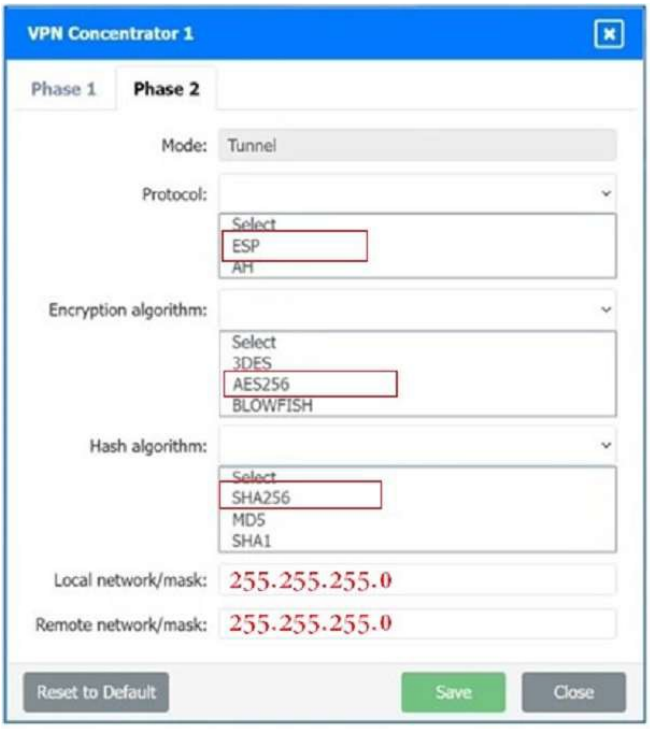
A. See Explanation section for answer.

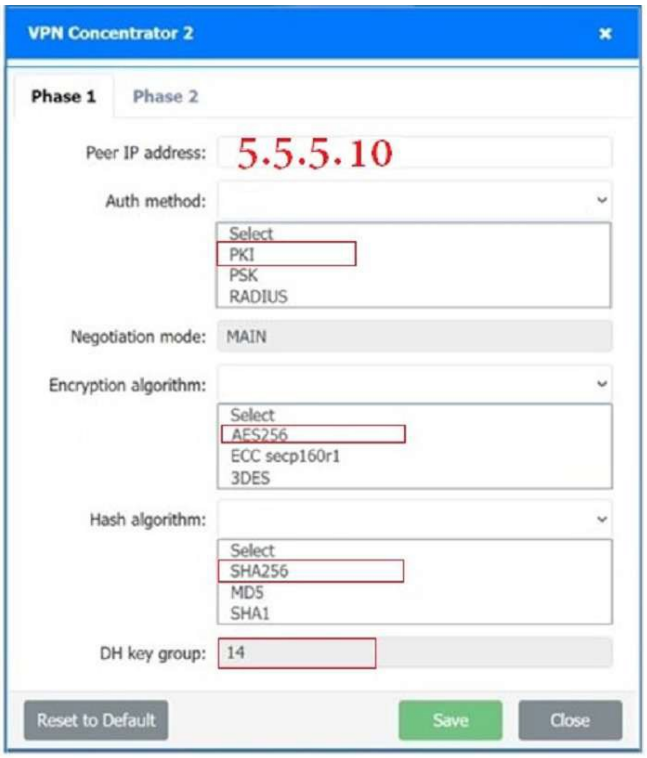
Correct Answer: A

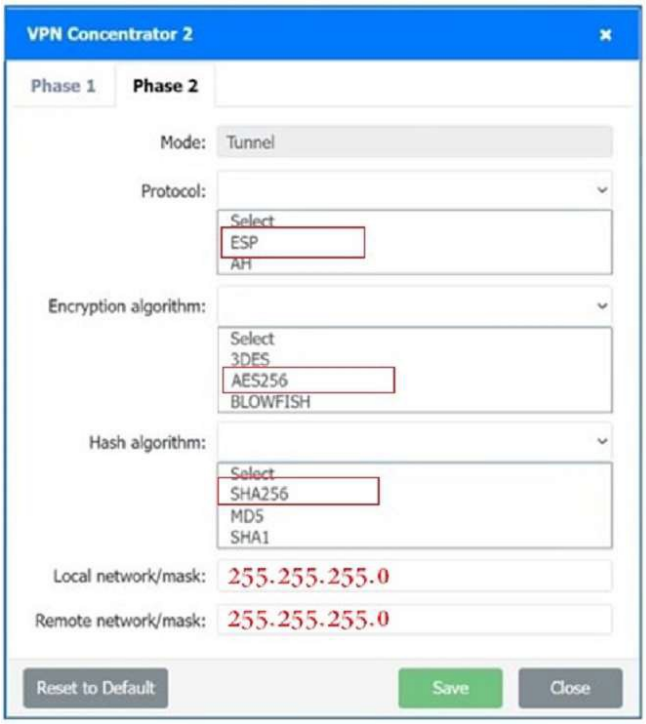
Answer(s): A




VPN Concentrator 1
Phase 1
Phase 2
Peer IP address:
5.5.5.20
Auth method:
Select
PKI
PSK
RADIUS
Negotiation mode:
MAIN
Encryption algorithm:
Select
AES256
ECC secp160r1
3DES
Hash algorithm:
Select
SHA256
MD5
SHA1
DH key group:
14
Reset to Default
Save
Close


VPN Concentrator 1
Phase 1
Phase 2
Mode:
Tunnel
Protocol:
Select
ESP
AH
Encryption algorithm:
Select
3DES
AES256
BLOWFISH
Hash algorithm:
Select
SHA256
MD5
SHA1
Local network/mask:
255.255.255.0
Remote network/mask:
255.255.255.0
Reset to Default
Save
Close


VPN Concentrator 2
Phase 1
Phase 2
Peer IP address:
5.5.5.10
Auth method:
Select
PKI
PSK
RADIUS
Negotiation mode:
MAIN
Encryption algorithm:
Select
AES256
ECC secp160r1
3DES
Hash algorithm:
Select
SHA256
MD5
SHA1
DH key group:
14
Reset to Default
Save
Close


VPN Concentrator 2
Phase 1
Phase 2
Mode:
Tunnel
Protocol:
Select
ESP
AH
Encryption algorithm:
Select
3DES
AES256
BLOWFISH
Hash algorithm:
Select
SHA256
MD5
SHA1
Local network/mask:
255.255.255.0
Remote network/mask:
255.255.255.0
Reset to Default
Save
Close

Q104: 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

Correct Answer: C

Answer(s): C

Q105: 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

Correct Answer: D

Answer(s): D

Q106: Which of the following control types is AUP an example of?

A. Physical

B. Managerial

C. Technical

D. Operational

Correct Answer: D

Answer(s): D

Q107: 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.

Correct Answer: D

Answer(s): D

Q108: A company's online shopping website became unusable shortly after midnight on

January 30, 2023. When a security analyst reviewed the database server, the analyst noticed the following code used for backing up data: Which of the following should the analyst do next?

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

A. Check for recently terminated DBAs.

B. Review WAF logs for evidence of command injection.

C. Scan the database server for malware.

D. Search the web server for ransomware notes.

Correct Answer: B

Answer(s): B

Q109: 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

Correct Answer: D

Answer(s): D

Q110: Which of the following would be the most appropriate way to protect data in transit?

A. SHA-256

B. SSL3.0

C. TLS 1.3

D. AES-256

Correct Answer: C

Answer(s): C

Q111: 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

Correct Answer: A

Answer(s): A

Q112: 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

Correct Answer: A

Answer(s): A

Explanation:

Organized crime groups are primarily motivated by financial gain. Ransomware attacks are a popular tool for these groups because they can encrypt a victim's data and demand a ransom payment (often in cryptocurrency) to restore access. This form of attack can yield a high financial return if victims choose to pay.

Q113: 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

Correct Answer: D

Answer(s): D

Explanation:

A maintenance window is a pre-scheduled period when system or network changes, updates, or repairs are performed. By using a designated maintenance window, a systems administrator can minimize disruption to the organization's operations, as this window is typically chosen during a time when network usage is lower, reducing the impact on users.

Q114: The security team has been asked to only enable host A (10.2.2.7) and host B (10.3.9.9) to the new isolated network segment (10.9.8.14) that provides access to legacy devices. Access from all other hosts should be blocked. Which of the following entries would need to be added on the firewall?

Permit 10.2.2.0/24 to 10.9.8.14/27	Deny 0.0.0.0/0 to 10.9.8.14/27
Permit 10.3.9.0/24 to 10.9.8.14/27	Permit 10.2.2.0/24 to 10.9.8.14/27
Deny 0.0.0.0/0 to 10.9.8.14/27	Permit 10.3.9.0/24 to 10.9.8.14/27

Permit 10.2.2.7/32 to 10.9.8.14/27	Permit 10.2.2.7/32 to 10.9.8.14/27
Permit 10.3.9.9/32 to 10.9.8.14/27	Permit 10.3.9.0/24 to 10.9.8.14/27
Deny 0.0.0.0/0 to 10.9.8.14/27	Deny 10.9.8.14/27 to 0.0.0.0/0

A.

B.

C.

D.

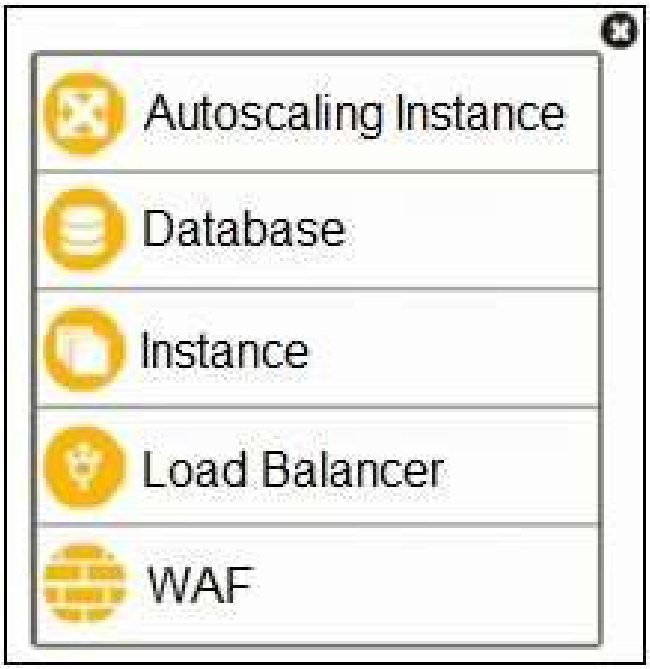
Correct Answer: C

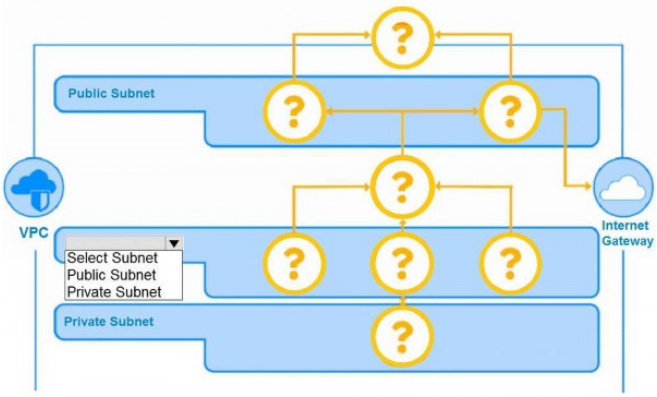
Answer(s): C

Explanation:

Permit 10.2.2.7/32 to 10.9.8.14/27: This rule allows host A (10.2.2.7) specific access to the isolated network (10.9.8.14/27). Permit 10.3.9.9/32 to 10.9.8.14/27: This rule allows host B (10.3.9.9) specific access to the isolated network (10.9.8.14/27). Deny 0.0.0.0/0 to 10.9.8.14/27: This rule blocks access from all other IPs to the isolated network (10.9.8.14/27).

Q115: SIMULATION A security analyst is creating the first draft of a network diagram for the company's new customer-facing payment application that will be hosted by a third-party cloud service provider. INSTRUCTIONS Click the ? to select the appropriate icons to create a secure, redundant web application. Then use the dropdown menu to select the appropriate subnet type. Every space in the diagram must be filled. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Autoscaling Instance
Database
Instance
Load Balancer
WAF


Public Subnet
VPC
Internet Gateway
Select Subnet
Public Subnet
Private Subnet
Private Subnet

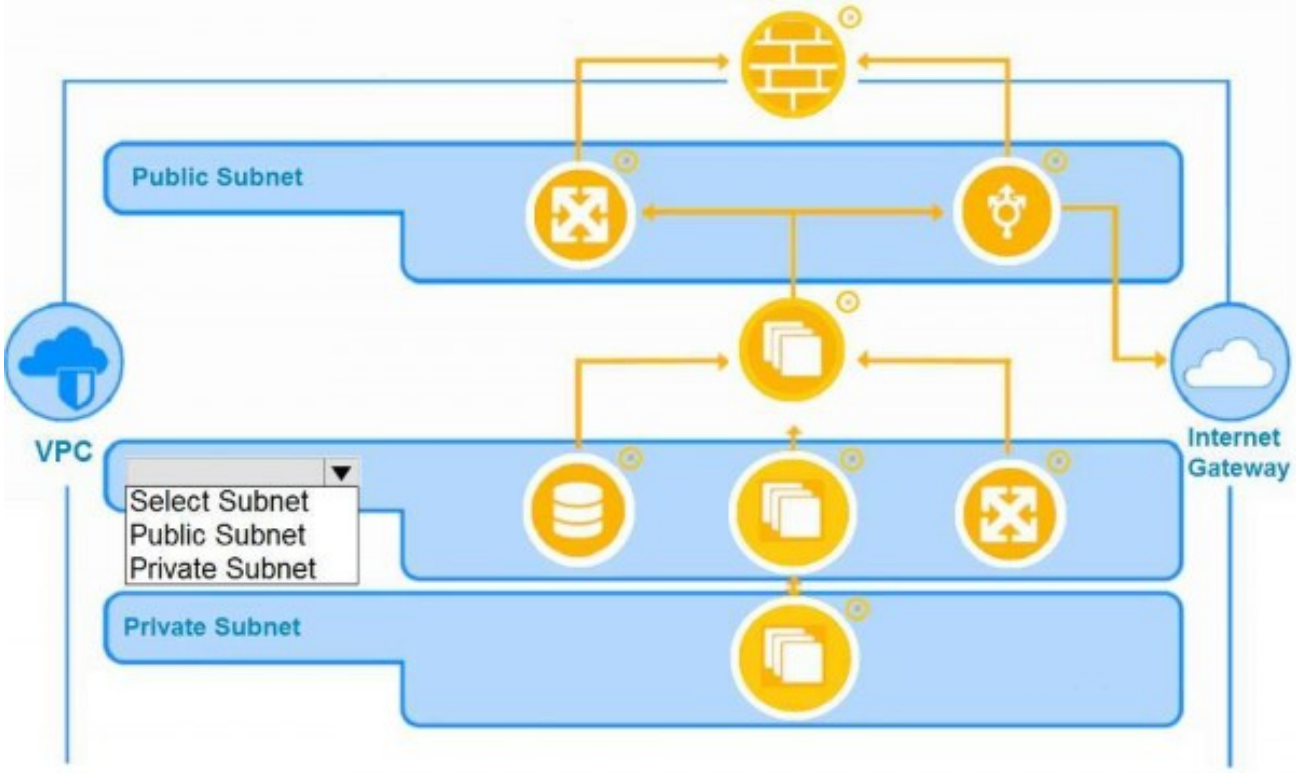
A. See Explanation section for answer.

Correct Answer: A

Answer(s): A

Explanation:

The diagram should be filled in the way shown below. WAF (Web Application Firewall) at the top to handle incoming traffic from the Internet Gateway. Load Balancer for distributing traffic between instances. Instances for handling the application workloads, ensuring multiple instances for redundancy. Autoscaling Instance to adjust the number of instances based on demand dynamically. In the middle of the diagram, you should select Private Subnet in the dropdown menu. This choice is appropriate because the elements in the lower section, especially the Database instances, are part of the private subnet. Placing databases in a private subnet adds an additional layer of security, as it prevents direct internet access to sensitive data. The private subnet is also typically used for backend resources that don't need to be exposed publicly.



Q116: A systems administrator needs to ensure the secure communication of sensitive data within the organization's private cloud. Which of the following is the best choice for the administrator to implement?

A. IPSec

B. SHA-1

C. RSA

D. TGT

Correct Answer: A

Answer(s): A

Explanation:

IPSec (Internet Protocol Security) is a suite of protocols designed to secure IP communications by authenticating and encrypting each IP packet in a communication session. It is widely used for securing data transfer in networks, including private clouds, by providing confidentiality, integrity, and authenticity of data.

Q117: Which of the following should an internal auditor check for first when conducting an audit of the organization's risk management program?

A. Policies and procedures

B. Asset management

C. Vulnerability assessment

D. Business impact analysis

Correct Answer: A

Answer(s): A

Explanation:

Policies and procedures form the foundation of an organization's risk management program. They establish the framework and guidelines for managing risks across the organization, including roles, responsibilities, and the approach for identifying, assessing, and mitigating risks. Without well-defined policies and procedures, it would be challenging to assess other areas of risk management effectively, as they are all built upon these foundational documents. Asset management, vulnerability assessment, and business impact analysis are critical components of a risk management program, but they should follow a review of policies and procedures. These documents set the standards and processes that the organization uses to manage assets, assess vulnerabilities, and conduct impact analyses.

Q118: Which of the following activities are associated with vulnerability management? (Choose two.)

Answer(s): A,B

Explanation:

Reporting involves documenting and communicating the findings of vulnerability scans and assessments. This allows stakeholders to be informed about existing vulnerabilities and track remediation efforts. Prioritization is the process of ranking vulnerabilities based on their severity, impact, and exploitability, helping the organization address the most critical vulnerabilities first.

Q119: An administrator wants to perform a risk assessment without using proprietary company information. Which of the following methods should the administrator use to gather information?

A. Network scanning

B. Penetration testing

C. Open-source intelligence

D. Configuration auditing

Correct Answer: C

Answer(s): C

Explanation:

Open-source intelligence (OSINT) involves collecting information from publicly available sources, such as websites, social media, news articles, and other publicly accessible databases. OSINT allows an administrator to gather valuable information about potential risks without using any proprietary or internal company information.

Q120: A systems administrator is concerned about vulnerabilities within cloud computing instances. Which of the following is most important for the administrator to consider when architecting a cloud computing environment?

A. SQL injection

B. TOC/TOU

C. VM escape

D. Tokenization

E. Password spraying

Correct Answer: C

Answer(s): C

Explanation:

In cloud computing, virtual machines (VMs) share physical resources. VM escape is a critical vulnerability where an attacker could break out of a virtualized environment and access the host system or other VMs running on the same physical hardware. This would pose a significant security risk, as it could allow attackers to compromise the entire cloud infrastructure.

Q121: 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

Correct Answer: C

Answer(s): C

Explanation:

Tokenization replaces sensitive data, like credit card information, with a unique identifier (token) that has no exploitable value outside of a specific context. This approach is widely used to secure payment card information and reduces the risk of exposure in case of a breach, as the actual credit card data is not stored in the database.

Q122: Which of the following is a benefit of vendor diversity?

A. Patch availability

B. Zero-day resiliency

C. Secure configuration guide applicability

D. Load balancing

Correct Answer: B

Answer(s): B

Explanation:

Vendor diversity can help mitigate the impact of zero-day vulnerabilities. By using multiple vendors for similar services or components, organizations reduce the likelihood that a single vulnerability affecting one vendor's products will compromise the entire system. This diversity creates resilience against attacks exploiting unknown vulnerabilities in any single vendor's software.

Q123: 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

Correct Answer: A

Answer(s): A

Explanation:

Application logs will contain records of activities within the billing system, including transactions, actions taken by users, and any anomalies. This is the most direct source of evidence for tracing fraudulent activity within the specific application, such as issuing unauthorized checks.

Q124: 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

Correct Answer: D

Answer(s): D

Explanation:

Containers package applications with only the necessary components and dependencies, which reduces the footprint of the operating system components in each instance. This approach minimizes the number of OS patches required, as each container runs only essential services instead of a full OS environment, making it easier to isolate and update application dependencies without affecting the host or requiring frequent OS-level patches.

Q125: 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

Correct Answer: A

Answer(s): A

Explanation:

In a BIA, estimating the recovery time of systems, also known as the Recovery Time Objective (RTO), is crucial. The BIA process focuses on identifying critical systems, understanding the impact of their unavailability, and

determining acceptable downtime. This helps in planning for recovery times, resource allocation, and continuity strategies.

Q126: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q127: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q128: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q129: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q130: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q131: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q132: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q133: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q134: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q135: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q136: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations,

especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q137: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q138: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q139: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q140: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q141: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q142: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q143: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q144: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q145: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q146: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q147: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to

monitor and detect suspicious activity by insiders attempting unauthorized access.

Q148: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q149: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q150: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q151: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q152: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q153: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q154: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q155: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q156: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q157: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q158: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing

monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q159: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q160: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q161: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q162: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q163: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q164: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q165: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q166: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q167: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q168: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q169: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q170: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q171: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q172: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q173: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q174: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q175: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q176: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q177: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q178: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q179: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q180: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q181: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q182: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q183: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q184: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q185: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q186: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q187: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q188: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q189: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q190: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q191: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q192: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q193: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q194: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q195: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q196: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q197: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q198: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q199: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the

risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q200: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q201: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q202: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q203: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q204: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q205: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q206: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q207: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q208: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q209: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q210: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO

to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q211: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q212: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q213: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q214: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q215: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q216: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q217: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q218: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q219: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q220: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q221: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations,

especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q222: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q223: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q224: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q225: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q226: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q227: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q228: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q229: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q230: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q231: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q232: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to

monitor and detect suspicious activity by insiders attempting unauthorized access.

Q233: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q234: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q235: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q236: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q237: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q238: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q239: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q240: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q241: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q242: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q243: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing

monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q244: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q245: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q246: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q247: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q248: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q249: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q250: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q251: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q252: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q253: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q254: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q255: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q256: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q257: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q258: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q259: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q260: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q261: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q262: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q263: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q264: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q265: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q266: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q267: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q268: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q269: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q270: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q271: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q272: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q273: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q274: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q275: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q276: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q277: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q278: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q279: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q280: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q281: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q282: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q283: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q284: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the

risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q285: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q286: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q287: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q288: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q289: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q290: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q291: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q292: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q293: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q294: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q295: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO

to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q296: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q297: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q298: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q299: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q300: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q301: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q302: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q303: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q304: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q305: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q306: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations,

especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q307: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q308: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q309: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q310: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q311: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q312: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q313: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q314: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q315: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q316: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q317: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to

monitor and detect suspicious activity by insiders attempting unauthorized access.

Q318: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q319: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q320: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q321: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q322: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q323: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q324: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q325: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q326: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q327: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q328: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing

monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q329: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q330: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q331: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q332: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q333: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q334: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q335: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q336: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q337: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q338: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q339: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q340: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q341: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q342: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q343: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q344: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q345: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q346: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q347: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q348: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q349: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q350: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q351: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q352: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q353: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q354: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q355: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q356: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q357: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q358: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q359: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q360: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q361: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q362: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q363: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q364: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q365: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q366: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q367: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q368: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q369: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the

risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q370: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q371: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q372: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q373: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q374: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q375: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q376: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q377: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q378: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q379: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q380: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO

to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q381: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q382: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q383: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q384: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q385: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q386: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q387: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q388: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q389: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q390: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q391: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations,

especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q392: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q393: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q394: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q395: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q396: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q397: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q398: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q399: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q400: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q401: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q402: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to

monitor and detect suspicious activity by insiders attempting unauthorized access.

Q403: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q404: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q405: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q406: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q407: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q408: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q409: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q410: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q411: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q412: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q413: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing

monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q414: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q415: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q416: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q417: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q418: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q419: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q420: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q421: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q422: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q423: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q424: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q425: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q426: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q427: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q428: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q429: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q430: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.

Q431: 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

Correct Answer: A

Answer(s): A

Explanation:

During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

Q432: Which of the following techniques would attract the attention of a malicious attacker in an insider threat scenario?

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

B. Setting weak passwords in /etc/shadow

C. Scheduling vulnerable jobs in /etc/crontab

D. Adding a fake account to /etc/passwd

Correct Answer: A

Answer(s): A

Explanation:

A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

Q433: 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

Correct Answer: A

Answer(s): A

Explanation:

Insider threats pose a significant risk to intellectual property, as insiders often have access to sensitive information and may attempt to misuse it. Training employees to recognize signs of insider threats, along with implementing monitoring and reporting protocols, helps protect intellectual property from theft or unauthorized disclosure by employees or other trusted individuals within the organization.

Q434: 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

Correct Answer: C

Answer(s): C

Explanation:

An on-premises architecture provides the highest level of control over data security, as the organization manages its own hardware, software, and network infrastructure directly. This setup enables the organization to implement strict access controls, customize security measures according to regulatory requirements, and avoid some of the risks associated with data transmission and storage in cloud environments, particularly for sensitive or proprietary information.

Q435: 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

Correct Answer: B

Answer(s): B

Explanation:

A data inventory provides a comprehensive overview of what data the organization holds, where it is stored, and its sensitivity. This information is crucial for assessing the potential impact of a data breach, as it allows the DPO to identify which data would be affected and the associated risks. Additionally, it aids in compliance with data protection regulations by ensuring that sensitive data is adequately managed and protected.
