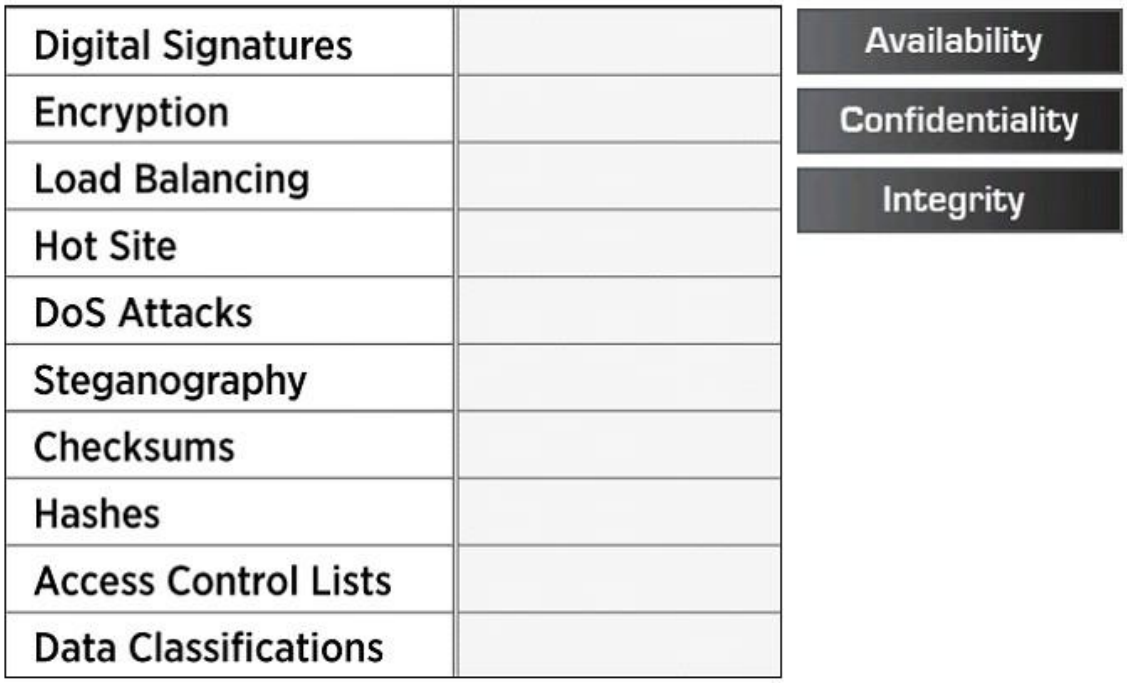
Vendor: CompTIA

Exam Code: CAS-002

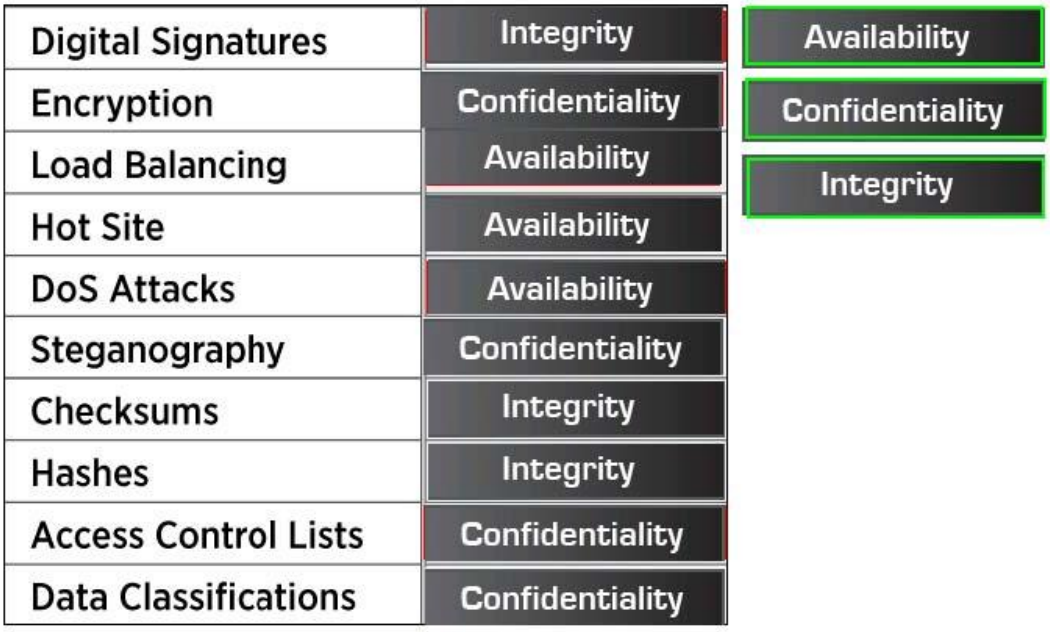
Exam Name: CompTIA Advanced Security Practitioner

Version: DEMO

QUESTION 1
Drag and Drop Question
Drag and Drop the following information types on to the appropriate CIA category



Answer:



QUESTION 2
A telecommunication company has recently upgraded their teleconference systems to multicast.

Additionally, the security team has instituted a new policy which requires VPN to access the company's video conference. All parties must be issued a VPN account and must connect to the company's VPN concentrator to participate in the remote meetings.
Which of the following settings will increase bandwidth utilization on the VPN concentrator during the remote meetings?

A. IPSec transport mode is enabled
B. ICMP is disabled
C. Split tunneling is disabled
D. NAT-traversal is enabled

Answer: C

QUESTION 3
Several critical servers are unresponsive after an update was installed. Other computers that have not yet received the same update are operational, but are vulnerable to certain buffer overflow attacks. The security administrator is required to ensure all systems have the latest updates while minimizing any downtime.
Which of the following is the BEST risk mitigation strategy to use to ensure a system is properly updated and operational?

A. Distributed patch management system where all systems in production are patched as updates are released.
B. Central patch management system where all systems in production are patched by automatic updates as they are released.
C. Central patch management system where all updates are tested in a lab environment after being installed on a live production system.
D. Distributed patch management system where all updates are tested in a lab environment prior to being installed on a live production system.

Answer: D

QUESTION 4
Which of the following is true about an unauthenticated SAMLv2 transaction?

A. The browser asks the SP for a resource.
The SP provides the browser with an XHTML format.
The browser asks the IdP to validate the user, and then provides the XHTML back to the SP for access.
B. The browser asks the IdP for a resource.
The IdP provides the browser with an XHTML format.
The browser asks the SP to validate the user, and then provides the XHTML to the IdP for access.
C. The browser asks the IdP to validate the user.
The IdP sends an XHTML form to the SP and a cookie to the browser.
The browser asks for a resource to the SP, which verifies the cookie and XHTML format for access.
D. The browser asks the SP to validate the user.
The SP sends an XHTML form to the IdP.
The IdP provides the XHTML form back to the SP, and then the browser asks the SP for a resource.

Answer: A

QUESTION 5
The internal auditor at Company ABC has completed the annual audit of the company's financial system. The audit report indicates that the accounts receivable department has not followed proper record disposal procedures during a COOP/BCP tabletop exercise involving manual processing of financial transactions.
Which of the following should be the Information Security Officer's (ISO's) recommendation? (Select TWO).

A. Wait for the external audit results
B. Perform another COOP exercise
C. Implement mandatory training
D. Destroy the financial transactions
E. Review company procedures

Answer: CE

QUESTION 6
A system designer needs to factor in CIA requirements for a new SAN.
Which of the CIA requirements is BEST met by multipathing?

A. Confidentiality
B. Authentication
C. Integrity
D. Availability

Answer: D

QUESTION 7
The Chief Information Officer (CIO) comes to the security manager and asks what can be done to reduce the potential of sensitive data being emailed out of the company.
Which of the following is an active security measure to protect against this threat?

A. Require a digital signature on all outgoing emails.
B. Sanitize outgoing content.
C. Implement a data classification policy.
D. Implement a SPAM filter.

Answer: B

QUESTION 8
Which of the following BEST defines the term e-discovery?

A. A product that provides IT-specific governance, risk management, and compliance.
B. A form of reconnaissance used by penetration testers to discover listening hosts.
C. A synonymous term for computer emergency response and incident handling.
D. A process of producing electronically stored information for use as evidence.

Answer: D

QUESTION 9
A data breach occurred which impacted the HR and payroll system. It is believed that an attack from within the organization resulted in the data breach.
Which of the following should be performed FIRST after the data breach occurred?

A. Assess system status
B. Restore from backup tapes
C. Conduct a business impact analysis
D. Review NIDS logs

Answer: A

QUESTION 10
Employees have recently requested remote access to corporate email and shared drives. Remote access has never been offered; however, the need to improve productivity and rapidly responding to customer demands means staff now requires remote access.
Which of the following controls will BEST protect the corporate network?

A. Develop a security policy that defines remote access requirements. Perform regular audits of user accounts and reviews of system logs.
B. Secure remote access systems to ensure shared drives are read only and access is provided through a SSL portal. Perform regular audits of user accounts and reviews of system logs.
C. Plan and develop security policies based on the assumption that external environments have active hostile threats.
D. Implement a DLP program to log data accessed by users connecting via remote access. Regularly perform user revalidation.

Answer: C

QUESTION 11
Driven mainly by cost, many companies outsource computing jobs which require a large amount of processor cycles over a short duration to cloud providers.
This allows the company to avoid a large investment in computing resources which will only be used for a short time.
Assuming the provisioned resources are dedicated to a single company, which of the following is the MAIN vulnerability associated with on-demand provisioning?

A. Traces of proprietary data which can remain on the virtual machine and be exploited
B. Remnants of network data from prior customers on the physical servers during a compute job
C. Exposure of proprietary data when in-transit to the cloud provider through IPSec tunnels
D. Failure of the de-provisioning mechanism resulting in excessive charges for the resources

Answer: A

QUESTION 12
A company contracts with a third party to develop a new web application to process credit cards. Which of the following assessments will give the company the GREATEST level of assurance for the web application?

A. Social Engineering
B. Penetration Test
C. Vulnerability Assessment
D. Code Review

Answer: D

QUESTION 13
A security audit has uncovered that some of the encryption keys used to secure the company B2B financial transactions with its partners may be too weak. The security administrator needs to implement a process to ensure that financial transactions will not be compromised if a weak encryption key is found. Which of the following should the security administrator implement?

A. Entropy should be enabled on all SSLv2 transactions.
B. AES256-CBC should be implemented for all encrypted data.
C. PFS should be implemented on all VPN tunnels.
D. PFS should be implemented on all SSH connections.

Answer: C

QUESTION 14
Company Z is merging with Company A to expand its global presence and consumer base. This purchase includes several offices in different countries. To maintain strict internal security and compliance requirements, all employee activity may be monitored and reviewed.
Which of the following would be the MOST likely cause for a change in this practice?

A. The excessive time it will take to merge the company's information systems.
B. Countries may have different legal or regulatory requirements.
C. Company A might not have adequate staffing to conduct these reviews.
D. The companies must consolidate security policies during the merger.

Answer: B

QUESTION 15
A business is currently in the process of upgrading its network infrastructure to accommodate a personnel growth of over fifty percent within the next six months. All preliminary planning has been completed and a risk assessment plan is being adopted to decide which security controls to put in place throughout each phase.
Which of the following risk responses is MOST likely being considered if the business is creating an SLA with a third party?

A. Accepting risk
B. Mitigating risk
C. Identifying risk
D. Transferring risk

Answer: D

QUESTION 16
Which of the following must be taken into consideration for e-discovery purposes when a legal case is first presented to a company?

A. Data ownership on all files
B. Data size on physical disks
C. Data retention policies on only file servers
D. Data recovery and storage

Answer: D

QUESTION 17
Based on the results of a recent audit, a company rolled out a standard computer image in an effort to provide consistent security configurations across all computers. Which of the following controls provides the GREATEST level of certainty that unauthorized changes are not occurring?

A. Schedule weekly vulnerability assessments
B. Implement continuous log monitoring
C. Scan computers weekly against the baseline
D. Require monthly reports showing compliance with configuration and updates

Answer: C

QUESTION 18
A new project initiative involves replacing a legacy core HR system, and is expected to touch many major operational systems in the company. A security administrator is engaged in the project to provide security consulting advice. In addition, there are database, network, application, HR, and transformation management consultants engaged on the project as well. The administrator has established the security requirements.
Which of the following is the NEXT logical step?

A. Document the security requirements in an email and move on to the next most urgent task.
B. Organize for a requirements workshop with the non-technical project members, being the HR and transformation management consultants.
C. Communicate the security requirements with all stakeholders for discussion and buy-in.
D. Organize for a requirements workshop with the technical project members, being the database, network, and application consultants.

Answer: C

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**