QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

CompTIA

CAS-003

CompTIA Advanced Security Practitioner (CASP)

QUESTION: 273
A company sales manager received a memo from the company's financial department which stated that the company would not be putting its software products through the same security testing as previous years to reduce the research and development cost by 20 percent for the upcoming year. The memo also stated that the marketing material and service level agreement for each product would remain unchanged. The sales manager has reviewed the sales goals for the upcoming year and identified an increased target across the software products that will be affected by the financial department's change. All software products will continue to go through new development in the coming year. Which of the following should the sales manager do to ensure the company stays out of trouble?

A. Discuss the issue with the software product's user groups
B. Consult the company's legal department on practices and law
C. Contact senior finance management and provide background information
D. Seek industry outreach for software practices and law

Answer: B
To ensure that the company stays out of trouble, the sales manager should enquire about the legal ramifications of the change by consulting with the company's legal department, particularly as the marketing material is not being amended.
Incorrect Answers:
A: The software product's user groups would not have insight on the legal ramifications of the change by the company, and they might not have knowledge of the service-level agreements or any contracts that the company has with other customers.
C: The sales manager does not have additional background information to provide.
D: Legal information pertaining to internal operations should be obtained from the company's legal department.

QUESTION: 274
A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

A. Purchase new hardware to keep the malware isolated.
B. Develop a policy to outline what will be required in the secure lab.
C. Construct a series of VMs to host the malware environment.
D. Create a proposal and present it to management for approval.

Answer: D
Before we can create a solution, we need to motivate why the solution needs to be created and plan the best implementation with in the company's business operations. We therefore need to create a proposal that explains the intended implementation and allows for the company to budget for it.
Incorrect Answers:
A: Purchasing of equipment cannot take place before approval for the purchases have been obtained. B: A proposal, rather than a policy, of what will be required in the secure lab needs to be created. A policy is a document that outlines person responsible and the standards that must be upheld to meet minimum corporate governance requirements.
C: Virtual machines (VMs) allows for multiple operating systems to run simultaneously on a single host. However, viruses, worms, and malware also have the potential to migrate from one virtual machine to another and to the host machine.

References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 96, 219, 232, 371

QUESTION: 275
A company has issued a new mobile device policy permitting BYOD and company-issued devices. The company-issued device has a managed middleware client that restricts the applications allowed on company devices and provides those that are approved. The middleware client provides configuration standardization for both company owned and BYOD to secure data and communication to the device according to industry best practices. The policy states that, "BYOD clients must meet the company's infrastructure requirements to permit a connection." The company also issues a memorandum separate from the policy, which provides instructions for the purchase, installation, and use of the middleware client on BYOD. Which of the following is being described?

A. Asset management
B. IT governance
C. Change management
D. Transference of risk

Answer: B
It governance is aimed at managing information security risks. It entails educating users about risk and implementing policies and procedures to reduce risk.
Incorrect Answers:
A: Asset management is the process of organizing, t racking, and supporting the assets of a company. However, bring your own device (BYOD) entail the use of personal devices, which are not company assets.
C: Change management is the process of managing changes to the system and programs to ensure that changes occur in an ordered process. It should minimize the risk of unauthorized changes and help reverse any unauthorized change.
D: Transference of risk is the process of having a third party carry the risk for a company, through insurance, for example.

References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 80-81, 133-134, 209-210, 218, 231-233

QUESTION: 276
A security engineer on a large enterprise network needs to schedule maintenance within a fixed window of time. A total outage period of four hours is permitted for servers. Workstations can undergo maintenance from 8:00 pm to 6:00 am daily. Which of the following can specify parameters for the maintenance work? (Select TWO).

A. Managed security service
B. Memorandum of understanding
C. Quality of service
D. Network service provider
E. Operating level agreement

Answer: B, E
B: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. It must be signed by a re presentative from each organization that has the legal authority to sign and are typically secured, as they are considered confidential.
E: An operating level agreement (O LA) defines the responsibilities of each partner's internal support group and what group and resources are used to meet the specified goal. It is used in conjunction with service level agreements (SLAs).
Incorrect Answers:
A: A managed security service (MSS) is a network security service that has been outsourced to a service provider, such as an Internet Service Provider (ISP). In the earlier days of the Internet, ISPs would sell customers a firewall appliance, as customer premises equipment (CPE), and for an additional fee would manage the customer-owned firewall over a dial-up connection.
C: Quality of service (QoS) is a mechanism that is designed to give priority to different applications, users, or data to provide a specific level of performance. It is often used in networks to prioritize certain types of network traffic.
D: A network service provider (NSP) provides bandwidth or network access via direct

Internet backbone access to the Internet and usually access to its network access points (NAPs). They are sometimes referred to as backbone providers or internet providers.

References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 237, 362
https://en.wikipedia.org/wiki/Managed_security_service
https://en.wikipedia.org/wiki/Network_service_provider

QUESTION: 277
An organization has decided to reduce labor costs by outsourcing back office processing of credit applications to a provider located in another country. Data sovereignty and privacy concerns raised by the security team resulted in the third-party provider only accessing and processing the data via remote desktop sessions. To facilitate communications and improve productivity, staff at the third party has been provided with corporate email accounts that are only accessible via the remote desktop sessions. Email forwarding is blocked and staff at the third party can only communicate with staff within the organization. Which of the following additional controls should be implemented to prevent data loss? (Select THREE).

A. Implement hashing of data in transit
B. Session recording and capture
C. Disable cross session cut and paste
D. Monitor approved credit accounts
E. User access audit reviews
F. Source IP whitelisting

Answer: C, E, F
Data sovereignty is a legal concern where the data is governed by the laws of the country in which the data resides. In this scenario the company does not want the data to fall under the law of the country of the organization to whom back office process has be outsourced to. Therefore we must ensure that data can only be accessed on local servers and no copies are held on computers of the outsource partner. It is important therefore to prevent cut and paste operations.
Privacy concerns can be addressed by ensuring the unauthorized users do not have access to the data. This can be accomplished though user access auditing, which needs to be reviewed on an ongoing basis; and source IP whitelisting, which is a list of IP addresses that are explicitly allowed access to the system.
Incorrect Answers:
A: Hashing is used to ensure data integrity. In other words, it ensures that the data has not been altered and is in its true, original state. This does not address data sovereignty and privacy concerns. B: Session recording and capture would represent an additional potential threat for privacy concerns should an unauthorized user access the recorded session data.
D: The monitoring of approved credit accounts is a processing issue. It is not related to data sovereignty or privacy concerns.

References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17-19, 204, 247

QUESTION: 278
A company has received the contract to begin developing a new suite of software tools to replace an aging collaboration solution. The original collaboration solution has been in place for nine years, contains over a million lines of code, and took over two years to develop originally. The SDLC has been broken up into eight primary stages, with each stage requiring an in-depth risk analysis before moving on to the next phase. Which of the following software development methods is MOST applicable?

A. Spiral model
B. Incremental model
C. Waterfall model
D. Agile model

Answer: C
The waterfall model is a sequential software development processes, in which progress is seen as flowing steadily downwards through identified phases.
Incorrect Answers:
A: The spiral model is a risk-driven process model generator for software projects. Based on the unique risk patterns of a given project, the spiral model guides a team to adopt elements of one or more process models, such as incremental, waterfall, or evolutionary prototyping.
B: The incremental model is used to develop a system through repeated cycles (iterative) and in smaller portions at a time (incremental), allowing software developers to take advantage of what was learned during development of earlier parts or versions of the system. Learning comes from both the development and use of the system, where possible key steps in the process start with a simple implementation of a subset of the software requirements and iteratively enhance the evolving versions until the full system is implemented. At each iteration, design modifications are made and new functional capabilities are added.
D: In the agile software development model, teams of programmers and business experts work closely together, using an iterative approach.

References:
https://en.wikipedia.org/wiki/Waterfall_model
https://en.wikipedia.org/wiki/Spiral_model
https://en.wikipedia.org/wiki/Iterative_and_incremental_development BOOK p. 371

QUESTION: 279
An attacker attempts to create a DoS event against the VoIP system of a company. The attacker uses a tool to flood the network with a large number of SIP INVITE traffic. Which of the following would be LEAST likely to thwart such an attack?

A. Install IDS/IPS systems on the network
B. Force all SIP communication to be encrypted
C. Create separate VLANs for voice and data traffic
D. Implement QoS parameters on the switches

Answer: D
Quality of service (QoS) is a mechanism that is designed to give priority to different applications, users, or data to provide a specific level of performance. It is often used in networks to prioritize certain types of network traffic. It is not designed to block traffic, per se, but to give certain types of traffic a lower or higher priority than others. This is least likely to counter a denial of service (DoS) attack.
Incorrect Answers:
A: Denial of Service (DoS) attacks web-based attacks that exploit flaws in the operating system, applications, services, or protocols. These attacks can be mitigated by means of firewalls, routers, and intrusion detection systems (IDSs) that detect DoS traffic, disabling echo replies on external systems, disabling broadcast features on border systems, blocking spoofed packets on the network, and proper patch management.
B: VoIP makes use of Session Initiation Protocol (SIP) and the attack is making use of SIP INVITE requests to initiate VoIP calls. Forcing SIP communication to be encrypted would reduce SIP INVITE requests.
C: Using virtual local area networks (VLANs), to segregate data traffic from voice traffic can drastically reduce the potential for attacks that utilize automated tools.

References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 135-138, 355-356, 357, 362,

QUESTION: 280
The helpdesk department desires to roll out a remote support application for internal use on all company computers. This tool should allow remote desktop sharing, system log gathering, chat, hardware logging, inventory management, and remote registry access. The risk management team has been asked to review vendor responses to the RFQ. Which of the following questions is the MOST important?

A. What are the protections against MITM?
B. What accountability is built into the remote support application?
C. What encryption standards are used in tracking database?
D. What snapshot or “undo” features are present in the application?
E. What encryption standards are used in remote desktop and file transfer functionality?

Answer: B
Incorrect Answers:
A: Man-in-the-Middle (MiTM) attacks are carried out when an attacker places himself between the sender and the receiver in the communication path, where they can intercept and modify the communication. However, the risk of a MITM is slim whereas the support staff WILL be accessing personal information.
C: Database encryption to prevent unauthorized access could be important (depending

on other security controls in place). However, the risk of an unauthorized database access is slim whereas the support staff WILL be accessing personal information.
D: What snapshot or “undo” features are present in the application is a relatively unimportant question. The application may have no snapshot or “undo” features. Accounting for data access is more important than the risk of support user wanting to undo a mistake.
E: Encryption to prevent against MITM or packet sniffing attacks is important. However, the risk of such attacks is slim whereas the support staff WILL be accessing personal information. This makes the accountability question more important.

References:

https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp