QUESTION 677
A company uses AD and RADIUS to authenticate VPN and WiFi connections.
The Chief Information Security Officer (CISO) initiates a project to extend a third-party MFA solution to VPN. During the pilot phase, VPN users successfully get an MFA challenge, however they also get the challenge when connecting to WiFi which is not desirable.
Which of the following BEST explains why users are getting the MFA challenge when using WiFi?

A. In the RADIUS server, the proxy rule has not specified the NAS-Port-Type attribute that should be matched
B. In the firewall, in the AAA configuration the IP address of the third-party MFA solution needs to be set as a secondary RADIUS server
C. In the third-party MFA solution authentication properties need to be configured to recognize WiFi authentication requests
D. In the WiFi configuration authentication needs to be changed to WPA2 Enterprise using EAP-TLS to support the configuration

Answer: A

QUESTION 678
A PaaS provider deployed a new product using a DevOps methodology.
Because DevOps is used to support both development and production assets inherent separation of duties is limited.
To ensure compliance with security frameworks that require a specific set of controls relating to separation of duties the organization must design and implement an appropriate compensating control.
Which of the following would be MOST suitable in this scenario?

A. Configuration of increased levels of logging, monitoring and alerting on production access
B. Configuration of MFA and context-based login restrictions for all DevOps personnel
C. Development of standard code libraries and usage of the WS-security module on all web servers
D. Implementation of peer review, static code analysis and web application penetration testing against the staging environment

Answer: A

QUESTION 679
A red team is able to connect a laptop with penetration testing tools directly into an open network port.
The team then is able to take advantage of a vulnerability on the domain controller to create and promote a new enterprise administrator.
Which of the following technologies would MOST likely eliminate this attack vector m the future?

A. Monitor for anomalous creations of privileged domain accounts
B. Install a NIPS with rules appropriate to drop most exploit traffic

C. Ensure the domain controller has the latest security patches
D. Implement 802.1X with certificate-based authentication

Answer: C

QUESTION 680
Confidential information related to ApplicationA. Application B and Project X appears to have been leaked to a competitor.
After consulting with the legal team, the IR team is advised to take immediate action to preserve evidence for possible litigation and criminal charges.
While reviewing the rights and group ownership of the data involved in the breach, the IR team inspects the following distribution group access lists:

```
Group Name: product-updates-application-a
Members: administrator, app-support, dev-ops, jdoe, jsmith, mpeters

Group Name: pending-bug-fixes-application-a
Members: administrator, app-support, dev-ops, jsmith, jdoe, mpeters, rwilliams

Group Name: inflight-updates-application-b
Members: app-support, dev-ops, jdoe, nbrown, jsmith

Group Name: PoC-project-x
Members: dev-support, product-mgt, jsmith, nbrown, rwilliams
```

Which of the following actions should the IR team take FIRST?

A. Remove all members from the distribution groups immediately
B. Place the mailbox for jsmith on legal hold
C. Implement a proxy server on the network to inspect all outbound SMTP traffic for the DevOps group
D. Install DLP software on all developer laptops to prevent data from leaving the network.

Answer: A

QUESTION 681
A secure facility has a server room that currently is controlled by a simple lock and key. and several administrators have copies of the key.
To maintain regulatory compliance, a second lock, which is controlled by an application on the administrators' smartphones, is purchased and installed.
The application has various authentication methods that can be used.
The criteria for choosing the most appropriate method are:
- It cannot be invasive to the end user
- It must be utilized as a second factor.
- Information sharing must be avoided
- It must have a low false acceptance rate
Which of the following BEST meets the criteria?

A. Facial recognition
B. Swipe pattern
C. Fingerprint scanning
D. Complex passcode
E. Token card

Answer: C

QUESTION 682
A security engineer is helping the web developers assess a new corporate web application
The application will be Internet facing so the engineer makes the following recommendation:

In an htaccess file or the site config add:
or add to the location block:

```
HeadereditSet_Cookie ^(.*)$ $1;HttpOnly;Secure
```

Which of the following is the security engineer trying to accomplish via cookies? (Select TWO)

A. Ensure session IDs are generated dynamically with each cookie request
B. Prevent cookies from being transmitted to other domain names
C. Create a temporary space on the user's drive root for ephemeral cookie storage
D. Enforce the use of plain text HTTP transmission with secure local cookie storage
E. Add a sequence ID to the cookie session ID while in transit to prevent CSRF.
F. Allow cookie creation or updates only over TLS connections

Answer: AD

QUESTION 683
A company is the victim of a phishing and spear-phishing campaign.
Users are Clicking on website links that look like common bank sites and entering their credentials accidentally.
A security engineer decides to use a layered defense to prevent the phishing or lessen its impact.
Which of the following should the security engineer implement? (Select TWO)

A. Spam filter
B. Host intrusion prevention
C. Client certificates
D. Content filter
E. Log monitoring
F. Data loss prevention

Answer: AE

QUESTION 684
A company is purchasing an application that will be used to manage all IT assets as well as provide an incident and problem management solution for IT activity.
The company narrows the search to two products. Application A and Application B; which meet all of its requirements.
Application A is the most cost-effective product, but it is also the riskiest so the company purchases Application B.
Which of the following types of strategies did the company use when determining risk appetite?

A. Mitigation
B. Acceptance
C. Avoidance
D. Transfer

Answer: B

QUESTION 685
An internal penetration tester finds a legacy application that takes measurement input made in a text box and outputs a specific string of text related to industry requirements.
There is no documentation about how this application works, and the source code has been lost.
Which of the following would BEST allow the penetration tester to determine the input and output relationship?

A. Running an automated fuzzer
B. Constructing a known cipher text attack
C. Attempting SQL injection commands
D. Performing a full packet capture
E. Using the application in a malware sandbox

Answer: A

QUESTION 686
A security analyst is reviewing weekly email reports and finds an average of 1.000 emails received daily from the internal security alert email address.
Which of the following should be implemented?

A. Tuning the networking monitoring service
B. Separation of duties for systems administrators
C. Machine learning algorithms
D. DoS attack prevention

Answer: B

QUESTION 687
An engineer needs to provide access to company resources for several offshore contractors.
The contractors require:
- Access to a number of applications, including internal websites
- Access to database data and the ability to manipulate it
- The ability to log into Linux and Windows servers remotely
Which of the following remote access technologies are the BEST choices to provide all of this access securely? (Choose two.)

A. VTC
B. VRRP
C. VLAN
D. VDI
E. VPN
F. Telnet

Answer: DE

QUESTION 688
An application development company implements object reuse to reduce life-cycle costs for the company and its clients.
Despite the overall cost savings, which of the following BEST describes a security risk to customers inherent within this model?

A. Configurations of applications will affect multiple products.
B. Reverse engineering of applications will lead to intellectual property loss
C. Software patch deployment will occur less often
D. Homogeneous vulnerabilities will occur across multiple products

Answer: D

QUESTION 689
A company recently experienced a period of rapid growth, and it now needs to move to a more scalable cloud-based solution.
Historically, salespeople have maintained separate systems for information on competing customers to prevent the inadvertent disclosure of one customer's information to another customer.
Which of the following would be the BEST method to provide secure data separation?

A. Use a CRM tool to separate data stores
B. Migrate to a single-tenancy cloud infrastructure
C. Employ network segmentation to provide isolation among salespeople
D. Implement an open-source public cloud CRM

Answer: C

QUESTION 690
A company is in the process of re-architecting its sensitive system infrastructure to take advantage of on-demand computing through a public cloud provider.
The system to be migrated is sensitive with respect to latency availability, and integrity.
The infrastructure team agreed to the following
- Application and middleware servers will migrate to the cloud"; Database servers will remain on-site
- Data backup wilt be stored in the cloud
Which of the following solutions would ensure system and security requirements are met?

A. Implement a direct connection from the company to the cloud provider
B. Use a cloud orchestration tool and implement appropriate change control processes
C. Implement a standby database on the cloud using a CASB for data-at-rest security
D. Use multizone geographic distribution with satellite relays

Answer: A

QUESTION 691
An enterprise solution requires a central monitoring platform to address the growing networks of various departments and agencies that connect to the network.
The current vendor products are not adequate due to the growing number of heterogeneous devices.
Which of the following is the primary concern?

A. Scalability
B. Usability
C. Accountability
D. Performance

Answer: A

QUESTION 692
The SOC has noticed an unusual volume of traffic coming from an open WiFi guest network that appears correlated with a broader network slowdown.
The network team is unavailable to capture traffic but logs from network services are available
- No users have authenticated recently through the guest network's captive portal
- DDoS mitigation systems are not alerting
- DNS resolver logs show some very long domain names
Which of the following is the BEST step for a security analyst to take next?

A. Block all outbound traffic from the guest network at the border firewall
B. Verify the passphrase on the guest network has not been changed.
C. Search antivirus logs for evidence of a compromised company device
D. Review access pent fogs to identify potential zombie services

Answer: A