QUESTION 828
A software company tripled its workforce by hiring numerous early career developers out of college. The senior development team has a long-running history of secure coding, mostly through experience and extensive peer review, and recognizes it would be infeasible to train the new staff without halting development operations. Therefore, the company needs a strategy that will integrate training on secure code writing while reducing the impact to operations. Which of the following will BEST achieve this goal?

A. Give employees a book on the company coding standards.
B. Enroll new employees in a certification course on software assurance.
C. Roll out an automated testing and retesting framework.
D. Deploy static analysis and quality plug-ins into IDEs.

Answer: C

QUESTION 829
A security engineer has just been embedded in an agile development team to ensure security practices are maintained during frequent release cycles. A new web application includes an input form. Which of the following would work BEST to allow the security engineer to test how the application handles error conditions?

A. Running a dynamic analysis at form submission
B. Performing a static code analysis
C. Fuzzing possible input of the form
D. Conducting a runtime analysis of the code

Answer: C

QUESTION 830
The HVAC and fire suppression systems that were recently deployed at multiple locations are susceptible to a new vulnerability. A security engineer needs to ensure the vulnerability is not exploited. The devices are directly managed by a smart controller and do not need access to other parts of the network. Signatures are available to detect this vulnerability. Which of the following should be the FIRST step in completing the request?

A. Deploy a NAC solution that disables devices with unknown MACs.
B. Create a firewall policy with access to the smart controller from the internal network only.
C. Create a segmented subnet for all HVAC devices and the smart controller.
D. Create an IPS profile for the HVAC devices that includes the signatures.

Answer: C

QUESTION 831
An aircraft manufacturer is developing software that will perform automatic flight control (auto-pilot). Given the high safety criticality of the software, the developer can BEST prove software correctness to a requirement's specification by employing:

A. static code analyzers
B. formal methods
C. test harnesses
D. dynamic analysis methods

Answer: B

QUESTION 832
An application developer is including third-party backported security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, reports come in that a previously resolved vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

A. Peer review
B. Regression testing
C. User acceptance
D. Dynamic analysis

Answer: B

QUESTION 833
A forensic analyst must image the hard drive of a computer and store the image on a remote server. The analyst boots the computer with a live Linux distribution. Which of the following will allow the analyst to copy and transfer the file securely to the remote server?

A. `dd if=/dev/sda | sha256 | ssh -o username=user, password=mypass -p 2000 remote.server.com`
B. `dcfldd if=/dev/sda hash=sha256 sha256log=sha.log | cryptcat -k $key remote.server.com 2000`
C. `nc remote.server.com 5555 -e 'dcfldd if=/dev/sda of=./image.dd' | sha256 > sha256.log'`
D. `ssh -D 5555 user@remote.server.com; dd if=/dev/sda* | nc localhost 5555 'sha256 > sha.txt'`

Answer: D

QUESTION 834
A security engineer at a company is designing a system to mitigate recent setbacks caused by competitors that are beating the company to market with new products. Several of the products incorporate proprietary enhancements developed by the engineer's company. The network already includes a SIEM and a NIPS and requires 2FA for all user access. Which of the following systems should the engineer consider NEXT to mitigate the associated risks?

A. DLP
B. Mail gateway
C. Data flow enforcement
D. UTM

Answer: A

QUESTION 835

Which of the following risks does expanding business into a foreign country carry?

A. Data sovereignty laws could result in unexpected liability
B. Export controls might decrease software costs
C. Data ownership might revert to the regulatory entities in the new country
D. Some security tools might be monitored by legal authorities

Answer: C

QUESTION 836
An analyst is testing the security of a server and attempting to infiltrate the network. The analyst is able to obtain the following output after running some tools on the server:

```
Administrator:500 :AB42B4B22B87E3F1AAD3B435B51404EE:
71B0347EDC285C11DDFAE2B3D1EFD7C1:::
Guest:1003:NO PASSWORD*************:NO:::
HELPDESK:1002:NO
PASSWORD*************:964736C9179861DB2BEAC825C84F0B75:::
```

Which of the following will the analyst most likely do NEXT?

A. Use John the Ripper to attempt password recovery.
B. Log in with either of the administrator passwords shown.
C. Log in with the guest account since it has a blank password.
D. Use Medusa to perform an online attack of the HELPDESK account.

Answer: D

QUESTION 837
Following a recent disaster, a business activates its DRP. The business is operational again within 60 minutes. The business has multiple geographically dispersed locations that have similar equipment and operational capabilities. Which of the following strategies has the business implemented?

A. Cold site
B. Reciprocal agreement
C. Recovery point objective
D. Internal redundancy

Answer: C

QUESTION 838
A corporation with a BYOD policy is very concerned about issues that may arise from data ownership. The corporation is investigating a new MDM solution and has gathered the following requirements as part of the requirements-gathering phase:

- Each device must be issued a secure token of trust from the corporate PKI.
- All corporate applications and local data must be able to be deleted from a central console.
- Access to corporate data must be restricted on international travel.
- Devices must be on the latest OS version within three weeks of an OS release.

Which of the following should be features in the new MDM solution to meet these requirements? (Choose two.)

A. Application-based containerization
B. Enforced full-device encryption
C. Geofencing
D. Application allow listing

E. Biometric requirement to unlock device
F. Over-the-air update restriction

Answer: AC

QUESTION 839
A security engineer needs to implement controls that will prevent the theft of data by insiders who have valid credentials. Recent incidents were carried out with mobile and wearable devices that were used as transfer vectors. In response, USB data transfers are now tightly controlled and require executive authorization. Which of the following controls will further reduce the likelihood of another data theft?

A. Limit the ability to transfer data via Bluetooth connections.
B. Move the enterprise to a BYOD or COPE policy.
C. Deploy strong transit encryption across the enterprise.
D. Implement time-based restrictions on data transfers.

Answer: A

QUESTION 840
During an audit, an information security analyst discovers accounts that are still assigned to employees who no longer work for the company and new accounts that need to be verified against a list of authorized users. This type of auditing supports the development of:

A. information classification.
B. continuous monitoring.
C. employment and termination procedures.
D. least privilege.

Answer: C

QUESTION 841
A Chief Information Security Officer (CISO) wants to obtain data from other organizations in the same industry related to recent attacks against industry targets. A partner firm in the industry provides information that discloses the attack vector and the affected vulnerability that impacted other firms. The CISO then works with that firm's CERT to evaluate the organization for applicability associated with the intelligence provided. This activity is an example of:

A. an emerging threat feed
B. a risk analysis
C. a zero-day vulnerability
D. threat modeling
E. machine learning
F. Big Data

Answer: D

QUESTION 842
An organization has been the target of four phishing attacks in the last year. Each incident has cost the organization an average of $2,000. A security director researches additional anti-phishing solutions for the organization to deploy and submits the 42,000 messages received last year to each product to be analyzed.

Product	Emails scanned	Possible phishing emails scanned	Detected phishing emails	Blocked attachments	Yearly subscription
Product1	41,811	183	182	301	$10,000
Product2	41,427	180	178	287	$4,000
Product3	41,940	181	180	290	$7,000
Product4	41,688	185	185	315	$9,000
Product5	41,818	185	184	101	$5,500

Given the above information, which of the following products would be BEST to reduce risks and provide the highest total ROI?

A. Product1
B. Product2
C. Product3
D. Product4
E. Product5

Answer: B

QUESTION 843
Several corporate users returned from an international trip with compromised operating systems on their cellular devices. Additionally, intelligence reports confirm some international carriers are able to modify firmware unexpectedly even when the MDM policy is set to disable FOTA updates. Which of the following mitigations is operationally feasible and MOST likely to reduce the risk of firmware compromise by a carrier while traveling internationally?

A. Disable the ability to connect to third-party application stores.
B. Disable the smartphone's cellular radio and require the use of WiFi.
C. Enforce the use of an always-on SSL VPN with FIPS-validated encryption.
D. Issue device PKI certificates to ensure mutual authentication.

Answer: D

QUESTION 844
A developer implements the following code snippet:

```
catch (Exception e)
{
     if (log.isDebugEnabled())
     {
          log.debug ("Caught InvalidGSMException Exception --"
          + e.toString ());
     }
}
```

Which of the following vulnerabilities does this code snippet resolve?

A. SQL injection
B. Buffer overflow
C. Missing session limit
D. Information leakage

Answer: C

QUESTION 845

The Chief Information Security Officer (CISO) of a power generation facility is concerned about being able to detect missing security updates on the critical infrastructure in use at the facility. Most of this critical infrastructure consists of ICS and SCADA systems that are maintained by vendors, and the vendors have warned the CISO that proxying network traffic is likely to cause a DoS condition. Which of the following would be BEST to address the CISO's concerns while keeping the critical systems functional?

A. Configuring the existing SIEM to ingest all log files properly
B. Implementing a passive vulnerability scanning solution
C. Deploying a data diode for internal websites
D. Adding more frequent antivirus and anti-malware signature updates
E. Adjusting file access rules to use the concept of least privilege

Answer: C

QUESTION 846
Which of the following controls primarily detects abuse of privilege but does not prevent it?

A. Offboarding
B. Separation of duties
C. Least privilege
D. Job rotation

Answer: A

QUESTION 847
A company has a DLP system with the following capabilities:

- Text examination
- Optical character recognition
- File type validation
- Multilingual translation of key words and phrases
- Blocking of content encrypted with a known cipher
- Examination of all egress points

Despite the existing protections, a malicious insider was able to exfiltrate confidential information. DLP logs show the malicious insider transferred a number of JPEG files to an external host, but each of those files appears as negative for the presence of confidential information. Which of the following are the MOST likely explanations for this issue? (Choose two.)

A. Translating the confidential information from English into Farsi and then into French to avoid detection.
B. Scrambling the confidential information using a proprietary obfuscation scheme before sending the files via email.
C. Changing the extension of Word files containing confidential information to .jpg and uploading them to a file sharing site.
D. Printing the documents to TIFF images and attaching the files to outbound email messages.
E. Leveraging stenography to hide the information within the JPEG files
F. Placing the documents containing sensitive information into an AES-256 encrypted compressed archive files and using FTP to send them to an outside host

Answer: BE

QUESTION 848
A security analyst is responsible for the completion of a vulnerability assessment at a regional healthcare facility. The analyst reviews the following Nmap output:

```
nmap -v -p 445 --script=SMB-check-vulns --script-args=unsafe=1 192.168.1.10/24
```

Which of the following is MOST likely what the security analyst is reviewing?

A. An Nmap script to scan for unsafe servers on UDP 445
B. An Nmap script to run the SMB servers
C. An Nmap script to stop the SMB servers
D. An Nmap script to scan for vulnerable SMB servers

Answer: D

QUESTION 849
A developer is concerned about input validation for a newly created shopping-cart application, which will be released soon on a popular website. Customers were previously able to manipulate the shopping cart so they could receive multiple items while only paying for one item. This resulted in large losses. Which of the following would be the MOST efficient way to test the shopping cart and address the developer's concerns?

A. Log analysis
B. Dynamic analysis
C. Vulnerability assessment
D. Gray-box testing
E. Gray-box testing

Answer: E

QUESTION 850
A factory-floor system uses critical, legacy, and unsupported application software to enable factory operations. A latent vulnerability was recently exposed, which permitted attackers to send a specific string of characters followed by arbitrary code for execution. Patches are unavailable, as the manufacturer is no longer in business. Which of the following would be the BEST approach the company should take to mitigate the risk of this vulnerability and other latent vulnerability exploits? (Choose two.)

A. Configure a host-based firewall on the application server and restrict access to necessary ports and services.
B. Create a factory-floor enclave segregated from direct LAN/WAN reachability.
C. Implement a proxy that will sanitize input provided to the application.
D. Install server-side X.509 certificates and enable TLS 1.0 or later for client access.
E. Install network and host-based IDS, feeding logs to SIEM, and alerts to SOC operators.
F. Create a hunt team focused on the factory-floor operations.

Answer: BC

QUESTION 851
While standing up a proof-of-concept solution with a vendor, the following direction was given for connections to the different environments:

Test	10.10.24.38:443	www.vendordomain.com/testlogin
QA	10.10.24.38:443	www.vendordomain.com/qalogin
Production	10.10.24.38:443	www.vendordomain.com/prodlogin

Which of the following is being used to secure the three environments from overlap if all of them reside on separate servers in the same DMZ?

A. Separation of environments policy
B. Logical access controls
C. Segmentation of VLANs
D. Subnetting of cloud environments

Answer: C

QUESTION 852
A developer is writing a new mobile application that employees will use to connect to an Internet-facing sensitive system. The security team is concerned with MITM attacks against the encrypted application traffic aimed at intercepting and decrypting sensitive information from the server to the mobile client. Which of the following should the developer implement to address the security team's concerns? (Choose two.)

A. HSTS
B. TLS 1.3
C. OCSP
D. Certificate pinning
E. Key stretching

Answer: B

QUESTION 853
A company deploys a system to use device and user certificates for network authentication. Previously, the company only used separate certificates to send/receive encrypted email. Users have begun notifying the help desk because they cannot read encrypted email. Which of the following is the MOST likely cause of the issues?

A. The attestation service is not configured to accept the new certificates.
B. The device certificates have the S/MIME attribute selected.
C. The sending mail client is selecting the wrong public key to encrypt messages.
D. Multiple device certificates are associated with the same network port.

Answer: C\