QUESTION 854
A security analyst is examining threats with the following code function:

```
var httpLibraryUri = 'https://examplesite.com/httpEnhanced.js';
var jsLoadHttpPlugin = XMLHttpRequest.open("GET", httpLibraryUri, true);
eval (jsLoadHttpPlugin);

httpEnahnced.createserver (function(request, response) {
     response.writeHead(403, {'Content-Type'; 'type-plain'});
     response.end('Unauthorized');
}).listen(8443);
```

Which of the following threats should the security analyst report?

A. POST should be used instead of GET when making requests.
B. Root privileges are needed for the service to bind to the privileged port 8443.
C. The website allows unauthorized access to sensitive resources.
D. The web server allows insecure cookie storage.
E. There is unsafe execution of third-party JavaScript code.

Answer: E

QUESTION 855
A security team wants to keep up with emerging threats more efficiently by automating NIDS signature development and deployment. Which of the following approaches would BEST support this objective?

A. Use open-source intelligence sources to gather current information on adversary networks/systems
B. Subscribe to a commercial service provider that publishes IOCs.
C. Monitor cyberthreat newsgroups and translate articles into IDS/IPS rulesets.
D. Configure NIDS to operate inline and use a DNS whitelist.

Answer: B

QUESTION 856
A newly hired employee is trying to complete online training. When the employee logs on to the third-party service for training using known-good credentials through a SAML-based mechanism, an error message appears regarding the account. Which of the following is MOST likely occurring?

A. The third-party service does not support special characters in passwords.

B. The new employee's user account is not listed properly by the IdP.
C. The service provider is not verifying the user account exists in the directory.
D. The user agent string is not listing the correct information.

Answer: D

QUESTION 857
A product owner is working with a security engineer to improve the security surrounding certificate revocation, which is important for the clients using a web application. The organization is currently using a CRL configuration to manage revocation, but it is looking for a solution that addresses the reporting delays associated with CRLs. The security engineer recommends OCSP, but the product owner is concerned about the overhead associated with its use. Which of the following would the security engineer MOST likely suggest to address the product owner's concerns?

A. Key escrow can be used on the WAF
B. S/MIME can be used in lieu of OCSP
C. Stapling should be used with OCSP
D. The organization should use wildcard certificates.

Answer: C

QUESTION 858
A security analyst is investigating an alert arising from an impossible travel pattern. Within the span of 30 minutes, the email system saw successful authentication from two IP addresses, which geolocate more than 500mi (805km) away from each other. Before locking the account, which of the following actions should the analyst take?

A. Verify email server NTP synchronization status
B. Validate GeoIP data source
C. Review VPN authentication logs
D. Verify the user's recent travel activities

Answer: C

QUESTION 859
Company A is establishing a contractual relationship with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights. Which of the following documents will MOST likely contain these elements?

A. Company A-B SLA v2.docx
B. Company A OLA v1b.docx
C. Company A MSA v3.docx
D. Company A MOU v1.docx
E. Company A-B NDA v0.3.docx

Answer: C

QUESTION 860
A cloud architect is moving a distributed system to an external cloud environment. The company must be able to:
- Administer the server software at OS and application levels.
- Show the data being stored is physically separated from other tenants.
- Provide remote connectivity for MSSPs.

Which of the following configurations and architectures would BEST support these requirements?

A. Private PaaS
B. Single-tenancy IaaS
C. Hybrid SaaS

D. Multitenancy DBaaS

Answer: A

QUESTION 861
After multiple availability issues, a systems administrator is reviewing the following metrics from the web server farm, which is configured to serve the company's e-commerce site:

Service	Current active connections
Web01	321
Web02	1002
Web03	90
Web04	762
Web05	5672

To reduce the availability risk, the company should implement a new:

A. log correlation and aggregation system
B. load balancer algorithm
C. web application firewall
D. web server to the farm

Answer: B

QUESTION 862
A company's human resources department recently had its own shadow IT department spin up multiple VM guests on one host, each hosting a mixture of differently labeled data types (confidential and restricted) on the same guest. Which of the following cloud and virtualization considerations would BEST address the issue presented in this scenario?

A. Vulnerabilities associated with a single platform hosting multiple data types on VMs should have been considered.
B. Vulnerabilities associated with maintaining and patching multiple hypervisors.
C. Type 1 vs. Type 2 hypervisor approaches should have been considered.
D. Vulnerabilities associated with shared hosting services provided by the IT department should have been considered.

Answer: A

QUESTION 863
A legacy SCADA system is in place in a manufacturing facility to ensure proper facility operations. Recent industry reports made available to the security team state similar legacy systems are being used as part of an attack chain in the same industry market. Due to the age of these devices, security control options are limited. Which of the following would BEST provide continuous monitoring for these threats?

A. Full packet captures and log analysis
B. Passive vulnerability scanners
C. Red-team threat hunting
D. Network-based intrusion detection systems

Answer: D

QUESTION 864
A line-of-business manager has decided, in conjunction with the IT and legal departments, that outsourcing a specific

function to a third-party vendor would be the best course of action for the business to increase efficiency and profit. Which of the following should the Chief Security Officer (CSO) perform before signing off on the third-party vendor?

A. Supply chain audit
B. Vulnerability assessment
C. Penetration test
D. Application code review
E. Risk assessment

Answer: E

QUESTION 865
An organization uses an internal, web-based chat service that is served by an Apache HTTP daemon. A vulnerability scanner has identified this service is susceptible to a POODLE attack. Which of the following strings within the server's virtual-host configuration block is at fault and needs to be changed?

A. `AccessFileName /var/http/.acl`
B. `SSLProtocol -all +SSLv3`
C. `AllowEncodeSlashes on`
D. `SSLCertificateFile /var/certs/home.pem`
E. `AllowOverride Nonfatal=All AuthConfig`

Answer: A

QUESTION 866
The latest security scan of a web application reported multiple high vulnerabilities in session management. Which of the following is the BEST way to mitigate the issue?

A. Prohibiting session hijacking of cookies
B. Using secure cookie storage and transmission
C. Performing state management on the server
D. Using secure and HttpOnly settings on cookies

Answer: D

QUESTION 867
Which of the following is the primary cybersecurity-related difference between the goals of a risk assessment and a business impact analysis?

A. Broad spectrum threat analysis
B. Adherenece to quantitative vs. qualitative methods
C. A focus on current state without regard to cost
D. Measurements of ALE vs.SLE and downtime

Answer: A

QUESTION 868
A security manager is creating an incident response plan for an organization. Executive management wants to designate a specific group of personnel to respond to incidents and an additional group to perform more proactive threat detection before an active incident occurs. Which of the following groups must be formed to satisfy these requirements? (Choose two.)

A. CRM
B. Threat hunters
C. Governance board

D. CIRT
E. Risk committee
F. Business analysts

Answer: BD

QUESTION 869
A security analyst is testing a server and finds the following in the output of a vulnerability scan:

```
PORT STATE SERVICE
139/tcp open netbios-ssn
Host script results:
| samba-vuln-cve-2018-1264:
| SAMBA remote heap overflow
| State: VULNERABLE
| Risk factor: HIGH CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
| Description:
| Samba versions 4.1.3 and all versions previous to this are affected by
| a vulnerability that allows remote code execution as the "root" user
| from an anonymous connection.
|
|_Disclosure date: 2018-03-15
```

Which of the following will the security analyst most likely use NEXT to explore this further?

A. Exploitation framework
B. Reverse engineering tools
C. Vulnerability scanner
D. Visualization tool

Answer: A

QUESTION 870
A company's design team is increasingly concerned about intellectual property theft. Members of the team often travel to suppliers' offices where they collaborate and share access to their sensitive data. Which of the following should be implemented?

A. Apply MDM and enforce full disk encryption on all design team laptops.
B. Allow access to sensitive data only through a multifactor-authenticated VDI environment.
C. Require all sensitive files be saved only on company fileshares, accessible only through multifactor-authenticated VPN.
D. Store all sensitive data on geographically restricted, public-facing SFTP servers authenticated using TOTP.

Answer: D

QUESTION 871
The Chief Information Security Officer (CISO) developed a robust plan to address both internal and external vulnerabilities due to an increase in ransomware attacks on the network. However, the number of successful attacks continues to increase. Which of the following is the MOST likely failure?

A. The company did not blacklist suspected websites properly.
B. The threat model was not vetted properly.
C. The IDS/IPS were not updated with the latest malware signatures.
D. The organization did not conduct a business impact analysis.

Answer: B

QUESTION 872
While reviewing wire transfer procedures, the Chief Information Security Officer (CISO) of a bank discovers a flaw in the policy that can potentially allow for some wire transfers to occur without the account owner's consent. The CISO recommends a compensating control, which is implemented immediately by operational staff, although there is still some risk posed to the bank. Which of the following BEST describes the CISO's new concerns about wire transfer fraud?

A. Residual risk
B. Mitigated risk
C. Inherent risk
D. Accepted risk

Answer: B

QUESTION 873
A security analyst is reviewing the security of a company's public-facing servers. After some research, the analyst discovers the following on a public pastebin website.

```
try {
 //Class.forName ("com.mysql.jdbc.Driver").newInstance();
 Connection cn = DriverManager.getConnection
("jdbc:mysql://mysql.company.com", "root", "QYOGHgasd842");
 PreparedStatement pst = cn.prepateStatement ("INSERT INTO newdata
VALUES (ID, name, account)");
 pst.executeUpdate ();
} catch (SQLException e) {
 System.out.println ("Error " + e);
}
```

Which of the following should the analyst do NEXT?

A. Review the system logs.
B. Scan *.company.com for vulnerabilities.
C. Begin a root cause analysis.
D. Change the password to the MySQL database.

Answer: B

QUESTION 874
A recent incident revealed a log entry was modified after its original creation. Which of the following technologies would BEST ensure end user systems are able to defend against future incidents?

A. Use an offline archival server.
B. Deploy MFA for access to services.
C. Implement a blockchain scheme.
D. Employ a behavioral HIDS on end user devices.

Answer: A

QUESTION 875
An organization's email filter is an ineffective control, and as a result, employees have been constantly receiving phishing emails. As part of a security incident investigation, a security analyst identifies the following:
1. An employee was working remotely when the security alert was triggered.
2. An employee visited a number of uncategorized Internet sites.

3. A .doc file was downloaded.
4. A number of files were uploaded to an unknown collaboration site.

Which of the following would provide the security analyst with more data to identify the root cause of the issue and protect the organization's information during future incidents?

A. EDR and DLP
B. DAM and MFA
C. HIPS and application whitelisting
D. FIM and antivirus

Answer: D

QUESTION 876

To reduce costs, an organization, has decided it will no longer support corporate phones. All employees must use a BYOD device to access the company's collaboration services, which are cloud hosted. To simplify device management, the end user computing department does not want to deploy agents to the devices. The Chief Information Security Officer (CISO) has identified the following requirements to support access to the service:

1. Only the current and N-1 operating systems are supported.
2. The devices cannot be jail broken.
3. Access is limited through the cloud forward proxy.
4. No company unstructured data is downloaded to local storage.
5. Strong authentication controls are implemented.
6. Any cached organization data is protected.

Which of the following controls must be implemented to meet these requirements?

A. Secure storage, 2FA, and an iris scan
B. MAM, geofencing, and MFA
C. VPN, device management, and OTP
D. MDM, context-aware management, and a PIN

Answer: B

QUESTION 877

A security analyst is reviewing the following event:

Packet#1:
Fragment offset = 0
Packet length = 820
More fragment bit = 1
Data = 800

Packet#2:
Fragment offset = 800
Packet length = 620
More fragment bit = 0
Data = 600

The packet appears to contain a malicious payload that is being delivered to the endpoint through the gateway firewall. Which of the following should the company implement to reduce the risk of similar attacks in the future?

A. NIPS
B. HIDS
C. Antivirus
D. SIEM

Answer: A

.