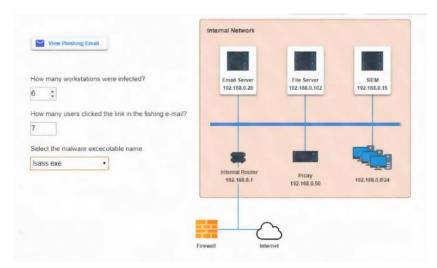**Explanation:**
Select the following answer as per diagram below.

QUESTION 139
A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

A. detection and prevention capabilities to improve.
B. which systems were exploited more frequently.
C. possible evidence that is missing during forensic analysis.
D. which analysts require more training.
E. the time spent by analysts on each of the incidents.

Correct Answer: A

QUESTION 140
After examine a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

A. Header analysis
B. File carving
C. Metadata analysis
D. Data recovery

Correct Answer: B

QUESTION 141
The Chief information Officer of a large cloud software vendor reports that many employees are falling victim to phishing emails because they appear to come from other employees. Which of the following would BEST prevent this issue

A. Induce digital signatures on messages originating within the company.

B.   Require users authenticate to the SMTP server
C.   Implement DKIM to perform authentication that will prevent this Issue.
D.   Set up an email analysis solution that looks for known malicious links within the email.

Correct Answer: A

QUESTION 142
A security analyst reviews a recent network capture and notices encrypted inbound traffic on TCP port 465 was coming into the company's network from a database server. Which of the following will the security analyst MOST likely identify as the reason for the traffic on this port?

A.   The server is receiving a secure connection using the new TLS 1.3 standard
B.   Someone has configured an unauthorized SMTP application over SSL
C.   The traffic is common static data that Windows servers send to Microsoft
D.   A connection from the database to the web front end is communicating on the port

Correct Answer: B

QUESTION 143
Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

A.   Human resources
B.   Public relations
C.   Marketing
D.   Internal network operations center

Correct Answer: B

QUESTION 144
An incident response team is responding to a breach of multiple systems that contain PII and PHI. Disclosing the incident to external entities should be based on:

A.   the responder's discretion
B.   the public relations policy
C.   the communication plan
D.   senior management's guidance

Correct Answer: A

QUESTION 145
An organization is focused on restructuring its data governance programs and an analyst has been tasked with surveying sensitive data within the organization. Which of the following is the MOST accurate method for the security analyst to complete this assignment?

A.   Perform an enterprise-wide discovery scan.
B.   Consult with an internal data custodian.
C.   Review enterprise-wide asset Inventory.
D.   Create a survey and distribute it to data owners.

Correct Answer: D

QUESTION 146
A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?

A.   Implement UEM on an systems and deploy security software.
B.   Implement DLP on all workstations and block company data from being sent outside the company
C.   Implement a CASB and prevent certain types of data from being downloaded to a workstation
D.   Implement centralized monitoring and logging for an company systems.

Correct Answer: C

QUESTION 147
A security analyst is researching ways to improve the security of a company's email system to mitigate emails that are impersonating company executives. Which of the following would be BEST for the analyst to configure to achieve this objective?

A.   A TXT record on the name server for SPF
B.   DNSSEC keys to secure replication
C.   Domain Keys identified Man
D.   A sandbox to check incoming mad

Correct Answer: B

QUESTION 148
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

Antivirus is installed on the remote host:

Installation path: C:\Program Files\AVProduct\Win32\

Product Engine: 14.12.101

Engine Version: 3.5.71

Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.

The engine version is out of date. The oldest supported version from the vendor is 4.2.11.

The analyst uses the vendor's website to confirm the oldest supported version is correct.

Which of the following BEST describes the situation?

A.   This is a false positive, and the scanning plugin needs to be updated by the vendor.
B.   This is a true negative, and the new computers have the correct version of the software.
C.   This is a true positive, and the new computers were imaged with an old version of the software.

D. This is a false negative, and the new computers need to be updated by the desktop team.

Correct Answer: C

QUESTION 149
A security analyst needs to perform a search for connections with a suspicious IP on the network traffic. The company collects full packet captures at the Internet gateway and retains them for one week. Which of the following will enable the analyst to obtain the BEST results?

A. tcpdump -n -r internet.pcap host <suspicious ip>
B. strings internet.pcap | grep <suspicious ip>
C. grep -a <suspicious ip> internet.pcap
D. npcapd internet.pcap | grep <suspicious ip>

Correct Answer: A

QUESTION 150
A SIEM analyst receives an alert containing the following URL:

http://companywebsite.com/displayPicture?filename=../../../etc/passwd

Which of the following BEST describes the attack?

A. Password spraying
B. Buffer overflow
C. insecure object access
D. Directory traversal

Correct Answer: D

QUESTION 151
A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?

A. Motion detection
B. Perimeter fencing
C. Monitored security cameras
D. Badged entry

Correct Answer: A

QUESTION 152
A security analyst is reviewing the following web server log:

GET %2f..%2f..%2f..%2f..%2f..%2f..%2f../etc/passwd

Which of the following BEST describes the issue?

A. Directory traversal exploit
B. Cross-site scripting
C. SQL injection
D. Cross-site request forgery

Correct Answer: A

QUESTION 153
A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-m-the-middle attack .The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices. Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?

A. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network,
B. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router.
C. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network
D. Conduct a wireless survey to determine if the wireless strength needs to be reduced.

Correct Answer: A

QUESTION 154
A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats. Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

A. Development of a hypothesis as part of threat hunting
B. Log correlation, monitoring, and automated reporting through a SIEM platform
C. Continuous compliance monitoring using SCAP dashboards
D. Quarterly vulnerability scanning using credentialed scans

Correct Answer: A

QUESTION 155
The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:

A. web servers on private networks
B. HVAC control systems
C. smartphones
D. firewalls and UTM devices

Correct Answer: B

QUESTION 156