QUESTION 121
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization $1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised. Which of the following is the value of this risk?

A. $75.000
B. $300.000
C. $1.425 million
D. $1.5 million

Correct Answer: A

QUESTION 122
A company wants to ensure confidential data from its storage media files is sanitized so the drives cannot oe reused. Which of the following is the BEST approach?

A. Degaussing
B. Shreoding
C. Formatting
D. Encrypting

Correct Answer: B

QUESTION 123
In web application scanning, static analysis refers to scanning:

A. the system for vulnerabilities before installing the application.
B. the compiled code of the application to detect possible issues.
C. an application that is installed and active on a system.
D. an application that is installed on a system that is assigned a static IP.

Correct Answer: A

QUESTION 124
A hybrid control is one that:

A. is implemented differently on individual systems
B. is implemented at the enterprise and system levels
C. has operational and technical components
D. authenticates using passwords and hardware tokens

Correct Answer: B

QUESTION 125
Which of the following incident response components can identify who is the llaison between multiple lines of business and the pubic?

A. Red-team analysis
B. Escalation process and procedures
C. Triage and analysis
D. Communications plan

Correct Answer: C

QUESTION 126
A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

A. Configure DLP to reject all changes to the files without pre-authorization. Monitor the files for unauthorized changes.
B. Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes.
C. Place a legal hold on the files. Require authorized users to abide by a strict time context access policy. Monitor the files for unauthorized changes.
D. Use Wireshark to scan all traffic to and from the directory. Monitor the files for unauthorized changes.

Correct Answer: AC

QUESTION 127
A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further in investigation?

A. Data carving
B. Timeline construction
C. File cloning
D. Reverse engineering

Correct Answer: C

QUESTION 128
Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?

A. Security regression testing
B. Stress testing
C. Static analysis testing
D. Dynamic analysis testing
E. User acceptance testing

Correct Answer: B

QUESTION 129
Bootloader malware was recently discovered on several company workstations. All the workstations run Windows and are current models with UEFI capability. Which of the following UEFI settings is the MOST likely cause of the infections?

A. Compatibility mode
B. Secure boot mode
C. Native mode
D. Fast boot mode

Correct Answer: A

QUESTION 130
A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet. Which of the following solutions would meet this requirement?

A. Establish a hosted SSO.
B. Implement a CASB.
C. Virtualize the server.
D. Air gap the server.

Correct Answer: D

QUESTION 131
An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC. Which of the following is the BEST approach for supply chain assessment when selecting a vendor?

A. Gather information from providers, including datacenter specifications and copies of audit reports.
B. Identify SLA requirements for monitoring and logging.
C. Consult with senior management for recommendations.
D. Perform a proof of concept to identify possible solutions.

Correct Answer: A

QUESTION 132
The Cruel Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organza lion. Which of the following actions would work BEST to prevent against this type of attack?

A. Turn on full behavioral analysis to avert an infection
B. Implement an EDR mail module that will rewrite and analyze email links.
C. Reconfigure the EDR solution to perform real-time scanning of all files
D. Ensure EDR signatures are updated every day to avert infection.
E. Modify the EDR solution to use heuristic analysis techniques for malware.

Correct Answer: B
Explanation:
If you're concerned about spear phishing and other advanced threats that may impact your organization, a next-gen EDR endpoint protection platform offers a lot of advantages over

traditional antivirus.

QUESTION 133
A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

```
A. alert udp any any ---> root any ---> 21
B. alert tcp any any ---> any 21 (content:"root")
C. alert tcp any any ---> any root 21
D. alert tcp any any ---> any root (content:"ftp")
```

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: B

QUESTION 134
A security analyst is providing a risk assessment for a medical device that will be installed on the corporate network. During the assessment, the analyst discovers the device has an embedded operating system that will be at the end of its life in two years. Due to the criticality of the device, the security committee makes a risk-based policy decision to review and enforce the vendor upgrade before the end of life is reached. Which of the following risk actions has the security committee taken?

A. Risk exception
B. Risk avoidance
C. Risk tolerance
D. Risk acceptance

Correct Answer: D

QUESTION 135
A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities. The type of vulnerability that should be disseminated FIRST is one that:

A. enables remote code execution that is being exploited in the wild.
B. enables data leakage but is not known to be in the environment
C. enables lateral movement and was reported as a proof of concept
D. affected the organization in the past but was probably contained and eradicated

Correct Answer: C

QUESTION 136

A small organization has proprietary software that is used internally. The system has not been wen maintained and cannot be updated with the rest or the environment. Which of the following is the BEST solution?

A. virtualize the system and decommission the physical machine.
B. Remove it from the network and require air gapping.
C. Implement privileged access management for identity access.
D. Implement MFA on the specific system.

Correct Answer: B

QUESTION 137
During an investigation, an incident responder intends to recover multiple pieces of digital media. Before removing the media, the responder should initiate:

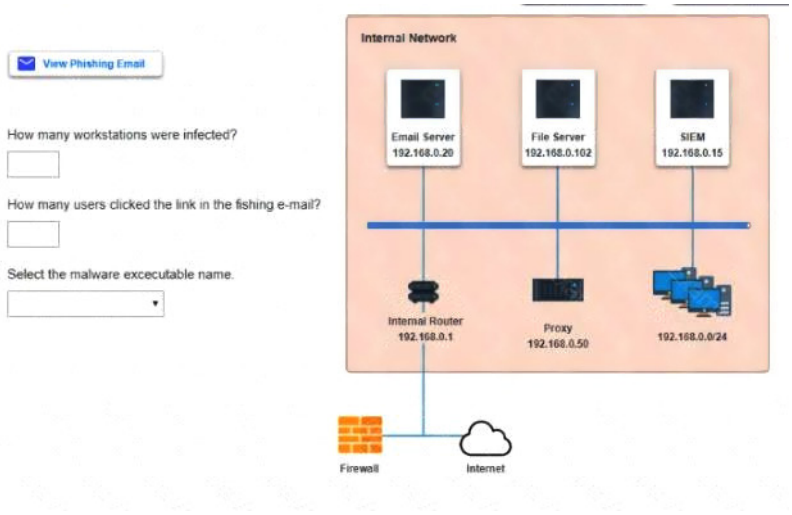
A. malware scans.
B. secure communications.
C. chain of custody forms.
D. decryption tools.

Correct Answer: C

QUESTION 138
Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

INSTRUCTIONS
Review the information provided and determine the following:

1. How many employees clicked on the link in the phishing email?
2. On how many workstations was the malware installed?
3. What is the executable file name or the malware?



Correct Answer: see the explanation.