A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

A. FDE
B. NIDS
C. EDR
D. DLP

Correct Answer: C

QUESTION 155
A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

A. Security information and event management
B. A web application firewall
C. A vulnerability scanner
D. A next-generation firewall

Correct Answer: A

QUESTION 156
A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical
B. Detective
C. Preventive
D. Compensating

Correct Answer: D

QUESTION 157
A company was recently breached Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

A. Log enrichment
B. Log aggregation
C. Log parser
D. Log collector

Correct Answer: D

QUESTION 158
After consulting with the Chief Risk Officer (CRO). a manager decides to acquire cybersecurity insurance for the company. Which of the following risk management strategies is the manager adopting?

A. Risk acceptance
B. Risk avoidance
C. Risk transference
D. Risk mitigation

Correct Answer: C

QUESTION 159
A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

A. Recovery
B. Identification
C. Lessons learned
D. Preparation

Correct Answer: C

QUESTION 160
A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?

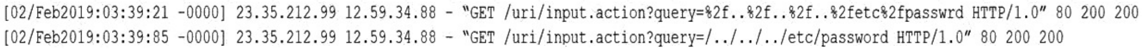
- The solution must be inline in the network
- The solution must be able to block known malicious traffic
- The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

A. HIDS
B. NIDS
C. HIPS
D. NIPS

Correct Answer: D

QUESTION 161
A security analyst sees the following log output while reviewing web logs:



```
[02/Feb2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpasswrd HTTP/1.0" 80 200 200
[02/Feb2019:03:39:85 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=/../../../etc/password HTTP/1.0" 80 200 200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

A. Secure cookies
B. Input validation
C. Code signing
D. Stored procedures

Correct Answer: B

QUESTION 162
Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

A. An ARO
B. An MOU
C. An SLA
D. A BPA

Correct Answer: C
Explanation:
Most SLA include a monetary penalty if the vendor is unable to meet the agreed-upon expectations

QUESTION 163
A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

A. MTBF
B. RPO
C. RTO
D. MTTR

Correct Answer: C

QUESTION 164
An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

A. Screen locks
B. Application management
C. Geofencing
D. Containerization

Correct Answer: C

QUESTION 165
A company is designing the layout of a new datacenter so it will have an optimal environmental temperature. Which of the following must be included? (Select TWO)

A. An air gap
B. A cold aisle
C. Removable doors
D. A hot aisle
E. An IoT thermostat
F. A humidity monitor

Correct Answer: BD
Explanation:

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/secure-areas/

QUESTION 166
A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

A. AH
B. ESP
C. SRTP
D. LDAP

Correct Answer: B

QUESTION 167
A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

- Protection from power outages
- Always-available connectivity In case of an outage

The owner has decided to implement battery backups for the computer equipment Which of the following would BEST fulfill the owner's second need?

A. Lease a point-to-point circuit to provide dedicated access.
B. Connect the business router to its own dedicated UPS.
C. Purchase services from a cloud provider for high availability
D. Replace the business's wired network with a wireless network.

Correct Answer: C

QUESTION 168
A security administrator currently spends a large amount of time on common security tasks, such aa report generation, phishing investigations, and user provisioning and deprovisioning This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

A. DAC
B. ABAC
C. SCAP
D. SOAR

Correct Answer: D

QUESTION 169
An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?

A. Information elicitation
B. Typo squatting
C. Impersonation
D. Watering-hole attack

Correct Answer: D

QUESTION 170
An organization has decided to host its web application and database in the cloud. Which of the following BEST describes the security concerns for this decision?

A. Access to the organization's servers could be exposed to other cloud-provider clients
B. The cloud vendor is a new attack vector within the supply chain
C. Outsourcing the code development adds risk to the cloud provider
D. Vendor support will cease when the hosting platforms reach EOL.

Correct Answer: B
Explanation:
Supply chain attacks piggyback legitimate processes to gain uninhibited access into a business's ecosystem. This attack begins with infiltrating a vendor's security defences. This process is usually much simpler than attacking a victim directly due to the unfortunate myopic cybersecurity practices of many vendors.

https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/#:~:text=That%20insidious%20and%20increasingly%20common,piece%20of%20software%20or%20hardware.
https://resources.infosecinstitute.com/topic/cloud-computing-attacks-vectors-and-counter-measures/

QUESTION 171
A company recently experienced an attack in which a malicious actor was able to exfiltrate data by cracking stolen passwords, using a rainbow table the sensitive data. Which of the following should a security engineer do to prevent such an attack in the future?

A. Use password hashing.
B. Enforce password complexity.
C. Implement password salting.
D. Disable password reuse.

Correct Answer: D

QUESTION 172
A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string. Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head