A proposed network architecture requires systems to be separated from each other logically based on defined risk levels. Which of the following explains the reason why an architect would set up the network this way?

A. To complicate the network and frustrate a potential malicious attacker
B. To reduce the number of IP addresses that are used on the network
C. To reduce the attack surface of those systems by segmenting the network based on risk
D. To create a design that simplifies the supporting network

Correct Answer: C

QUESTION 157
Following a recent security breach, a company decides to investigate account usage to ensure privileged accounts are only being utilized during typical business hours. During the investigation, a security analyst determines an account was consistently utilized in the middle of the night. Which of the following actions should the analyst take NEXT?

A. Initiate the incident response plan.
B. Disable the privileged account
C. Report the discrepancy to human resources.
D. Review the activity with the user.

Correct Answer: D

QUESTION 158
A small marketing firm uses many SaaS applications that hold sensitive information. The firm has discovered terminated employees are retaining access to systems for many weeks after their end date. Which of the following would BEST resolve the issue of lingering access?

A. Configure federated authentication with SSO on cloud provider systems.
B. Perform weekly manual reviews on system access to uncover any issues.
C. Implement MFA on cloud-based systems.
D. Set up a privileged access management tool that can fully manage privileged account access.

Correct Answer: D

QUESTION 159
A company's modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

A. Quarantine the web server
B. Deploy virtual firewalls
C. Capture a forensic image of the memory and disk
D. Enable web server containerization

Correct Answer: B

QUESTION 160
An analyst has received a notification about potential malicious activity against a web server. The

analyst logs in to a central log collection server and runs the following command: "cat access.log.1 | grep "union". The output shown below appears:

```
<68.71.54.117> -- [31/Jan/2020:10:02:31 -0400] "Get
/cgi-bin/backend1.sh?id=%20union%20select%20192.168.60.50 HTTP/1.1"
```

Which of the following attacks has occurred on the server?

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

Correct Answer: C

QUESTION 161
Massivelog.log has grown to 40GB on a Windows server. At this size, local tools are unable to read the file, and it cannot be moved off the virtual server where it is located. Which of the following lines of PowerShell script will allow a user to extract the last 10.000 lines of the loq for review?

A. tail -10000 Massivelog.log > extract.txt
B. info tail n -10000 Massivelog.log | extract.txt;
C. get content `./Massivelog.log' -Last 10000 | extract.txt
D. get-content `./Massivelog.log' -Last 10000 > extract.txt;

Correct Answer: D

QUESTION 162
A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database. Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.
B. Remove the servers reported to have high and medium vulnerabilities.
C. Tag the computers with critical findings as a business risk acceptance.
D. Manually patch the computers on the network, as recommended on the CVE website.
E. Harden the hosts on the network, as recommended by the NIST framework.
F. Resolve the monthly job issues and test them before applying them to the production network.

Correct Answer: CE

QUESTION 163
A company wants to outsource a key human-resources application service to remote employees

as a SaaS-based cloud solution. The company's GREATEST concern should be the SaaS provider's:

A. DLP procedures.
B. logging and monitoring capabilities.
C. data protection capabilities.
D. SLA for system uptime.

Correct Answer: C

QUESTION 164
A computer hardware manufacturer developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?

A. Encryption
B. eFuse
C. Secure Enclave
D. Trusted execution

Correct Answer: C

QUESTION 165
An organization recently discovered some inconsistencies in the motherboards it received from a vendor. The organization's security team then provided guidance on how to ensure the authenticity of the motherboards it received from vendors. Which of the following would be the BEST recommendation for the security analyst to provide'?

A. The organization should evaluate current NDAs to ensure enforceability of legal actions.
B. The organization should maintain the relationship with the vendor and enforce vulnerability scans.
C. The organization should ensure all motherboards are equipped with a TPM.
D. The organization should use a certified, trusted vendor as part of the supply chain.

Correct Answer: D

QUESTION 166
During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the NEXT step the analyst should take?

A. Only allow whitelisted binaries to execute.
B. Run an antivirus against the binaries to check for malware.
C. Use file integrity monitoring to validate the digital signature.
D. Validate the binaries' hashes from a trusted source.

Correct Answer: B

QUESTION 167
For machine learning to be applied effectively toward security analysis automation, it requires.

A. relevant training data.
B. a threat feed API.
C. a multicore, multiprocessor system.
D. anomalous traffic signatures.

Correct Answer: A

QUESTION 168
A cybersecurity analyst is investigating a potential incident affecting multiple systems on a company's internal network. Although there is a negligible impact to performance, the following symptom present on each of the affected systems:

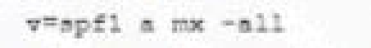
- Existence of a new and unexpected svchost exe process
- Persistent, outbound TCP/IP connections to an unknown external host with routine keep-alives transferred
- DNS query logs showing successful name resolution for an Internet-resident dynamic DNS domain

If this situation remains unresolved, which of the following will MOST likely occur?

A. The affected hosts may participate in a coordinated DDoS attack upon command
B. An adversary may leverage the affected hosts to reconfigure the company's router ACLs.
C. Key files on the affected hosts may become encrypted and require ransom payment for unlock.
D. The adversary may attempt to perform a man-in-the-middle attack.

Correct Answer: C

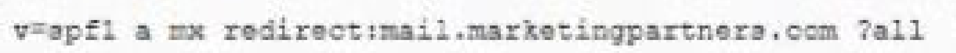
QUESTION 169
A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:



```
v=spf1 a mx -all
```

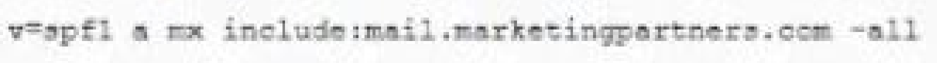
Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?

A.



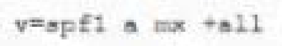
```
v=spf1 a mx redirect:mail.marketingpartners.com ?all
```

B.



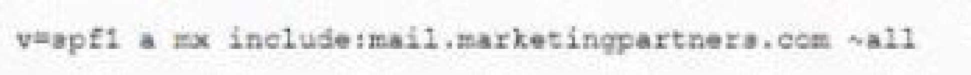
```
v=spf1 a mx include:mail.marketingpartners.com -all
```

C.



```
v=spf1 a mx +all
```

D.



```
v=spf1 a mx include:mail.marketingpartners.com ~all
```

Correct Answer: B
QUESTION 170
A security analyst has discovered suspicious traffic and determined a host is connecting to a known malicious website. The MOST appropriate action for the analyst to take would be lo

implement a change request to:

A. update the antivirus software
B. configure the firewall to block traffic to the domain
C. add the domain to the blacklist
D. create an IPS signature for the domain

Correct Answer: B

QUESTION 171
A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO), asking the employee to perform a wife transfer. Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

A. Implementing a sandboxing solution for viewing emails and attachments
B. Limiting email from the finance department to recipients on a pre-approved whitelist
C. Configuring email client settings to display all messages in plaintext when read
D. Adding a banner to incoming messages that identifies the messages as external

Correct Answer: D

QUESTION 172
A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur. They have asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the BEST way to achieve this goal?

A. Focus on incidents that may require law enforcement support.
B. Focus on common attack vectors first.
C. Focus on incidents that have a high chance of reputation harm.
D. Focus on incidents that affect critical systems.

Correct Answer: D

QUESTION 173
An organization's Chief Information Security Officer (CISO) has asked department leaders to coordinate on communication plans that can be enacted in response to different cybersecurity incident triggers. Which of the following is a benefit of having these communication plans?

A. They can help to prevent the inadvertent release of damaging information outside the organization.
B. They can quickly inform the public relations team to begin coordinating with the media as soon as a breach is detected.
C. They can help to keep the organization's senior leadership informed about the status of patching during the recovery phase.
D. They can help to limit the spread of worms by coordinating with help desk personnel earlier in the recovery phase.

Correct Answer: A