but has discovered there are no controls defined to evaluate third-party risk or hardware source authenticity. The compliance officer wants to gain some level of assurance on a recurring basis regarding the implementation of controls by third parties. Which of the following would BEST satisfy the objectives defined by the compliance officer? (Choose two.)

A. Executing vendor compliance assessments against the organization's security controls
B. Executing NDAs prior to sharing critical data with third parties
C. Soliciting third-party audit reports on an annual basis
D. Maintaining and reviewing the organizational risk assessment on a quarterly basis
E. Completing a business impact assessment for all critical service providers
F. Utilizing DLP capabilities at both the endpoint and perimeter levels

Correct Answer: AC

QUESTION 16
A security analyst is reviewing the following DNS logs as part of security-monitoring activities:

```
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www.company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfcbfaerwfj.com 32.56.32.122
FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53
FROM 192.168.1.93 AAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www.comptia.org 122.10.31.87
```

Which of the following MOST likely occurred?

A. The attack used an algorithm to generate command and control information dynamically.
B. The attack used encryption to obfuscate the payload and bypass detection by an IDS.
C. The attack caused an internal host to connect to a command and control server.
D. The attack attempted to contact www.google.com to verify Internet connectivity.

Correct Answer: A

QUESTION 17
An organization wants to move non-essential services into a cloud computing environment. Management has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work BEST to attain the desired outcome?

A. Duplicate all services in another instance and load balance between the instances.
B. Establish a hot site with active replication to another region within the same cloud provider.
C. Set up a warm disaster recovery site with the same cloud provider in a different region
D. Configure the systems with a cold site at another cloud provider that can be used for failover.

Correct Answer: C
QUESTION 18
A security analyst has received reports of very slow, intermittent access to a public-facing

corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -1
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0   0   0.0.0.0:22      172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0   0   127.0.0.1:631   0.0.0.0:*     LISTEN      1214/cupsd
tcp 0   0   0.0.0.0:443     0.0.0.0:*     LISTEN      1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

A. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.
B. Examine the server logs for further indicators of compromise of a web application.
C. Run kill -9 1325 to bring the load average down so the server is usable again.
D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

Correct Answer: B

QUESTION 19
An analyst needs to provide a recommendation that will allow a custom-developed application to have full access to the system's processors and peripherals but still be contained securely from other applications that will be developed. Which of the following is the BEST technology for the analyst to recommend?

A. Software-based drive encryption
B. Hardware security module
C. Unified Extensible Firmware Interface
D. Trusted execution environment

Correct Answer: D

QUESTION 20
A security analyst receives an alert from the SIEM about a possible attack happening on the network. The analyst opens the alert and sees the IP address of the suspected server as 192.168.54.66, which is part of the network 192 168 54 0/24. The analyst then pulls all the command history logs from that server and sees the following:

```
$ route -n
$ ifconfig -a
$ ping 192.168.54.1
$ tcpdump 192.168.54.80 -nnS
$ hping -s 192.168.54.80 -c 3
```

Which of the following activities is MOST likely happening on the server?

A. A MITM attack
B. Enumeration
C. Fuzzing
D. A vulnerability scan

Correct Answer: A

QUESTION 21
When reviewing a compromised authentication server, a security analyst discovers the following hidden file:

```
root@ldap1:~# cat .pass.txt
jsmith:Welcome123:18073:0:99999:7:::
mjones4:Welcome123:18073:0:99999:7:::
egreen1:Welcome123:18073:0:99999:7:::
rbarger:Welcome123:18073:0:99999:7:::
mhemme14:Welcome123:18073:0:99999:7:::
mgill:Welcome123:18073:0:99999:7:::
cyoung1:Welcome123:18073:0:99999:7:::
gkiepper3:Welcome123:18073:0:99999:7:::
```

Further analysis shows these users never logged in to the server. Which of the following types of attacks was used to obtain the file and what should the analyst recommend to prevent this type of attack from reoccurring?

A. A rogue LDAP server is installed on the system and is connecting passwords. The analyst should recommend wiping and reinstalling the server.
B. A password spraying attack was used to compromise the passwords. The analyst should recommend that all users receive a unique password.
C. A rainbow tables attack was used to compromise the accounts. The analyst should recommend that future password hashes contains a salt.
D. A phishing attack was used to compromise the account. The analyst should recommend users install endpoint protection to disable phishing links.

Correct Answer: B

QUESTION 22
Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

A. Use a UEFI boot password.
B. Implement a self-encrypted disk.
C. Configure filesystem encryption
D. Enable Secure Boot using TPM

Correct Answer: C

QUESTION 23

A company's blocklist has outgrown the current technologies in place. The ACLS are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures. Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

A. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed.
B. Implement a host-file based solution that will use a list of all domains to deny for all machines on the network
C. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs and IPS signatures.
D. Review the current blocklist and prioritize it based on the level of threat severity. Add the domains with the highest severity to the blocklist and remove the lower-severity threats from it.

Correct Answer: A

QUESTION 24
While analyzing logs from a WAF, a cybersecurity analyst finds the following:

```
"GET /form.php?id=463225%2b%2575%256e%2569%256f%256e%2b%2573%2574%2box3133333731,1223,1224&name=&state=IL"
```

Which of the following BEST describes what the analyst has found?

A. This is an encrypted GET HTTP request
B. A packet is being used to bypass the WAF
C. This is an encrypted packet
D. This is an encoded WAF bypass

Correct Answer: D

QUESTION 25
A security analyst reviews SIEM logs and discovers the following error event:

```
ERROR Event ID 4
The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server DEASVRR45. The target name used was GC/PDC1DC.Domain57/Administrator. This indicates that the
target server failed to decrypt the ticket provided by the client. Check if there are identically named server accounts in these two domains, or use the fully-
qualified name to identify the server.
```

Which of the following environments does the analyst need to examine to continue troubleshooting the event?

A. Proxy server
B. SQL server
C. Windows domain controller
D. WAF appliance
E. DNS server

Correct Answer: E

QUESTION 26

A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:

A. proprietary and timely
B. proprietary and accurate
C. relevant and deep
D. relevant and accurate

Correct Answer: D

QUESTION 27
A cybersecurity analyst is contributing to a team hunt on an organization's endpoints. Which of the following should the analyst do FIRST?

A. Write detection logic.
B. Establish a hypothesis.
C. Profile the threat actors and activities.
D. Perform a process analysis.

Correct Answer: C

QUESTION 28
During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website. Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

A. An IPS signature modification for the specific IP addresses
B. An IDS signature modification for the specific IP addresses
C. A firewall rule that will block port 80 traffic
D. A firewall rule that will block traffic from the specific IP addresses

Correct Answer: D

QUESTION 29
Which of the following types of policies is used to regulate data storage on the network?

A. Password
B. Acceptable use
C. Account management
D. Retention

Correct Answer: D

QUESTION 30
A security analyst for a large financial institution is creating a threat model for a specific threat