CompTIA.SY0-601.v2023-04-27.q438

Exam Code:	SY0-601
Exam Name:	CompTIA Security+ Exam
Certification Provider:	CompTIA
Free Question Number:	438
Version:	v2023-04-27
# of views:	3188
# of Questions views:	4380
https://www.freepdfdumps.com/CompTIA.SY0-601.v2023-04-27.q438.html	

NEW QUESTION: 1
As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?
A. TAXII
B. STIX
C. TLP
D. TTP
Answer: (SHOW ANSWER)

NEW QUESTION: 2
A security analyst is reviewing application logs to determine the source of a breach and locates the following log:
Which Of the following has been observed?
A. API attack
B. XSS
C. SQLI
D. DLL Injection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
An organization is having difficulty correlating events from its individual AV, EDR. DLP. SWG, WAF, MDM. HIPS. and CASB systems. Which of the following Is the BEST way to improve the situation?
A. Utilize a SIEM to centralize logs and dashboards.
B. Remove expensive systems that generate few alerts,
C. implement a new syslog/NetFlow appliance.

D. Modify the systems to alert only on critical issues.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?
A. FAR
B. CER
C. Cost
D. FRR
E. Difficulty of use
Answer: (SHOW ANSWER)

NEW QUESTION: 5
A security architect is designing the new outbound internet for a small company. The company would like all 50 users to share the same single Internet connection. In addition, users will not be permitted to use social media sites or external email services while at work. Which of the following should be included in this design to satisfy these requirements? (Select TWO).
A. DLP
B. MAC filtering
C. NAT
D. VPN
E. Content filler
F. WAF
Answer: C,D (LEAVE A REPLY)
NAT (Network Address Translation) is a technology that allows multiple devices to share a single IP address, allowing them to access the internet while still maintaining security and privacy. VPN (Virtual Private Network) is a technology that creates a secure, encrypted tunnel between two or more devices, allowing users to access the internet and other network resources securely and privately. Additionally, VPNs can also be used to restrict access to certain websites and services, such as social media sites and external email services.

NEW QUESTION: 6
An organization wants to enable built-in FDE on all laptops Which of the following should the organization ensure is Installed on all laptops?
A. TPM
B. CA
C. SAML
D. CRL
Answer: A (LEAVE A REPLY)

The organization should ensure that a Trusted Platform Module (TPM) is installed on all laptops in order to enable built-in Full Disk Encryption (FDE). TPM is a hardware-based security chip that stores encryption keys and helps to protect data from malicious attacks. It is important to ensure that the TPM is properly configured and enabled in order to get the most out of FDE.

NEW QUESTION: 7
An employee's company account was used in a data breach Interviews with the employee revealed:
* The employee was able to avoid changing passwords by using a previous password again.
* The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.
Which of the following can be implemented to prevent these issues from reoccuring? (Select TWO)
A. Password complexity
B. Geofencing
C. Geographic dispersal
D. Password lockout
E. Geotagging
F. Password history
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 8
A security assessment determines DES and 3DES at still being used on recently deployed production servers. Which of the following did the assessment identify?
A. Weak encryption
B. Unsecme protocols
C. Default settings
D. Open permissions
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?
A. ARP poisoning
B. DNS poisoning
C. DDoS attack
D. MAC flooding
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10

The cost of removable media and the security risks of transporting data have become too great for a laboratory. The laboratory has decided to interconnect with partner laboratories to make data transfers easier and more secure.
The Chief Security Officer (CSO) has several concerns about proprietary data being exposed once the interconnections are established. Which of the following security features should the network administrator implement to prevent unwanted data exposure to users in partner laboratories?
A. VLAN zoning with a file-transfer server in an external-facing zone
B. VPN with full tunneling and NAS authenticating through the Active Directory
C. NAC that permits only data-transfer agents to move data between networks
D. DLP running on hosts to prevent file transfers between networks
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:
Which of the following is the MOST likely cause of the issue?
A. Ransomware is communicating with a command-and-control server
B. The end user purchased and installed a PUP from a web browser
C. A bot on the computer is brute forcing passwords against a website
D. A hacker is attempting to exfiltrate sensitive data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
Which of the following supplies non-repudiation during a forensics investigation?
A. Logging everyone in contact with evidence
B. Duplicating a drive with dd
C. Dumping volatile memory contents first
D. Using a SHA-2 signature of a drive image
E. Encrypting sensitive data
Answer: (SHOW ANSWER)

NEW QUESTION: 13
A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?
A. A non-disclosure agreement
B. An acceptable use policy
C. Least privilege

D. Ofboarding
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Which of the following is assured when a user signs an email using a private key?
A. Non-repudiation
B. Confidentiality
C. Availably
D. Authentication
Answer: A (LEAVE A REPLY)
Non Repudiation is your virtual John Hancock. It's a way of virtually stamping any data or document with "I am who I say I am". Only way to break this would be if the private key owners' private key became compromised. Which at that point you got bigger problems than Non Repudiation.

NEW QUESTION: 15
A penetration tester gains access to a network by exploiting a vulnerability on a public-facing web server. Which of the following techniques will the tester most likely perform NEXT?
A. Gather more Information about the target through passive reconnaissance.
B. Move laterally throughout the network to search for sensitive information.
C. Establish rules of engagement before proceeding.
D. Create a user account to maintain persistence.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?
A. WPS
B. 802.1X
C. PSK
D. A captive portal
Answer: (SHOW ANSWER)

NEW QUESTION: 17
A security administrator suspects an employee has been emailing proprietary information to a competitor.
Company policy requires the administrator to capture an exact copy of the employee's hard disk.
Which of the following should the administrator use?
A. logger
B. dd
C. dnsenum
D. chmod
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
Digital signatures use asymmetric encryption. This means the message is encrypted with:
A. the sender's private key and decrypted with the sender's public key
B. the sender's public key and decrypted with the sender's private key
C. the sender's private key and decrypted with the recipient's public key.
D. the sender's public key and decrypted with the recipient's private key
Answer: C (LEAVE A REPLY)

NEW QUESTION: 19
Which of the following is the GREATEST security concern when outsourcing code development to third-party contractors for an internet-facing application?
A. Elevated privileges
B. Unknown backdoor
C. Quality assurance
D. Intellectual property theft
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
After entering a username and password, and administrator must draw a gesture on a touch screen. Which of the following demonstrates what the administrator is providing?
A. Multifactor authentication
B. Two-factor authentication
C. Something you can do
D. Biometric
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21

Which of the following organizations sets frameworks and controls for optimal security configuration on systems?
A. GDPR
B. ISO
C. NIST
D. PCI DSS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
After a phishing scam for 9 user's credentals, the red team was able to craft a payload to deploy on @ server. The attack allowed the installaton of malicious software that intiates @ new remote session.
Which of the following types of attacks has occurred?
A. Privilege escalation
B. Directory traversal
C. Application programming interface
D. Session replay
Answer: (SHOW ANSWER)

NEW QUESTION: 23
An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?
A. Record the collection in a blockchain-protected public ledger
B. Document the collection and require a sign-off when possession changes.
C. Place the device in a Faraday cage to prevent corruption of the data.
D. Lock the device in a safe or other secure location to prevent theft or alteration.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
Which of the following BEST explains the difference between a data owner and a data custodian?
A. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
D. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25

Server administrator want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently acress a number of virtual servers. They also need to avoid potential denial-of-service situations caused by availiability. Which of the following should administrator configure to maximize system availability while efficiently utilizing available computing power?

A. High availability

B. Segmentation

C. Container security

D. Dynamic resource allocation

Answer: B (LEAVE A REPLY)

NEW QUESTION: 26

DURING A SECURITY ASSESSMENT. A SECURITY ANALYST FINDS A FILE WITH OVERLY PERMISSIVE PERMISSION. WICH OF THE FOLLOWING TOOL WILL ALLOW THE ANALYST TO REDUCE THR PERMISSONFOR THE EXIXTING USER AND GROUPS AND REMOVE THE SET-USER-ID BIT FROM THE FILE?

A. 1a

B. Leof

C. aeuid

D. Chmod

E. Chflaga

Answer: (SHOW ANSWER)

NEW QUESTION: 27

When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization

B. Obfuscation

C. Normalization

D. Data masking

Answer: C (LEAVE A REPLY)

NEW QUESTION: 28

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Certificate chaining

B. Key escrow

C. A self-signed certificate

D. An extended validation certificate

Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
Which of the following is a security best practice that ensures the integrity of aggregated log files within a SIEM?
A. Back up the aggregated log files at least two times a day or as stated by local regulatory requirements.
B. Write protect the aggregated log files and move them to an isolated server with limited access.
C. Set up hashing on the source log file servers that complies with local regulatory requirements,
D. Back up the source log files and archive them for at least six years or in accordance with local regulatory requirements.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
An organization is tuning SIEM rules based off of threat intelligence reports. Which of the following phases of the incident response process does this scenario represent?
A. Preparation
B. Lessons learned
C. Recovery
D. Eradication
Answer: (SHOW ANSWER)

NEW QUESTION: 31
After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?
A. The public ledger
B. The NetFlow data
C. A checksum
D. The event log
Answer: A (LEAVE A REPLY)
https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/

NEW QUESTION: 32

Which of the following would be indicative of a hidden audio file found inside of a piece of source code?

A. Steganography

B. Homomotphic encryption

C. Cipher surte

D. Blockchain

Answer: (SHOW ANSWER)

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).

NEW QUESTION: 33

An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

A. TLS

B. AH

C. PFS

D. ESP

Answer: (SHOW ANSWER)

NEW QUESTION: 34

Which of the following types of controls is a turnstile?

A. Physical

B. Detective

C. Corrective

D. Technical

Answer: A (LEAVE A REPLY)

https://en.wikipedia.org/wiki/Turnstile#:~:text=A%20turnstile%20(also%20called%20a,%2C%20a%20pass%2C%20or%20similar.

NEW QUESTION: 35

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO).

A. A warning banner

B. The vendor's name

C. The order of volatility

D. The provenance of the artifacts

E. The date time

F. A CRC32 checksum
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 36
A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?
A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
D. Refrain from completing a forensic analysts of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence
Answer: B (LEAVE A REPLY)
"To obtain a forensically sound image from nonvolatile storage, you need to ensure that nothing you do alters data or metadata (properties) on the source disk or file system. A write blocker assures this process by preventing any data on the disk or volume from being changed by filtering write commands at the driver and OS level. Data acquisition would normally proceed by attaching the target device to a forensics workstation or field capture device equipped with a write blocker."
For purposes of knowing, https://security.opentext.com/tableau/hardware/details/t8u write blockers like this are the most popular hardware blockers

NEW QUESTION: 37
The spread of misinformation sorrounding the outbreak of a bnovel virus on election day led to eligible voters chooseing not to take risk of goding to the polls. This is an exampla of:
A. Prepending
B. Intimidation.
C. A watering-hole attack.
D. An influence compain
E. Information elicitation.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
An enterprise to keep cryptpgraphic keys in a sade manner.Whihc of the fikkowug network appliances can achieve this goals?
A. DLP
B. CASB
C. HSM

D. TPM
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?
A. PaaS
B. SOAR
C. MSSP
D. IaaS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
Several universities are participating m a collaborative research project and need to share compute and storage resources Which of the following cloud deployment strategies would BEST meet this need?
A. Community
B. Private
C. Public
D. Hybrid
Answer: A (LEAVE A REPLY)
Community cloud storage is a variation of the private cloud storage model, which offers cloud solutions for specific businesses or communities. In this model, cloud storage providers offer their cloud architecture, software and other development tools to meet the requirements of the community. A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

NEW QUESTION: 41
An attacker has determined the best way to impact operations is to infiltrate third-party software vendors. Which of the following vectors is being exploited?
A. Cloud
B. Social engineering
C. Social media
D. Supply chain
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's

workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?
A. A fileless virus that is contained on a vCard that is attempting to execute an attack
B. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall
C. A worm that has propagated itself across the intranet, which was initiated by presentation media
D. A Trojan that has passed through and executed malicious code on the hosts
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?
A. Mitigation
B. Avoidance
C. Transference
D. Acceptance
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?
A. Mitigation
B. Avoidance
C. Transference
D. Acceptance
Answer: (SHOW ANSWER)

NEW QUESTION: 45
After reluming from a conference, a user's laptop has been operating slower than normal and overheating and the fans have been running constantly Dunng the diagnosis process, an unknown piece of hardware is found connected to the laptop's motherboard Which of the following attack vectors was exploited to install the hardware?
A. Supply chain
B. Direct access
C. Removable media
D. Spear phishing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46

An analyst Is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services. Given this output from Nmap:
Which of the following should the analyst recommend to disable?
A. 22/tcp
B. 443/tcp
C. 23/tcp
D. 21/tcp
Answer: (SHOW ANSWER)

NEW QUESTION: 47
A security monitoring company offers a service that alerts its customers if their credit cards have been stolen. Which of the following is the MOST likely source of this information?
A. PCI
B. TAXI
C. Social media
D. STIX
E. The dark web
Answer: (SHOW ANSWER)

NEW QUESTION: 48
The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?
A. Prevent data exposure queries.
B. Obfuscate the source code.
C. Limit the use of third-party libraries.
D. Submit the application to QA before releasing it.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?

A. Impersonation
B. Watering-hole attack
C. Type squatting
D. Information elicitation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 50
The website http://companywebsite.com requires users to provide personal information, including security question responses, for registration. Which of the following would MOST likely cause a data breach?
A. Missing patches
B. Unsecure protocol
C. Open permissions
D. Lack of input validation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
An organization is concerned that is hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?
A. Hping3 -s comptia, org -p 80
B. Nc -1 -v comptia, org -p 80
C. nmp comptia, org -p 80 -aV
D. nslookup -port=80 comtia.org
Answer: C (LEAVE A REPLY)
Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

NEW QUESTION: 52
After a WiFi scan of a local office was conducted, an unknown wireless signal was identified Upon investigation, an unknown Raspberry Pi device was found connected to an Ethernet port using a single connection. Which of the following BEST describes the purpose of this device?
A. Evil twin
B. Rogue access point
C. On-path attack
D. loT sensor
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53

An analyst is working onan email incident in which target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?
A. Utilize email content filtering.
B. Isolate the infected attachment.
C. Implement network segmentation.
D. Apply a DLP solution
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?
A. Update all antivirus signatures daily.
B. Implement application blacklisting
C. Segment the network with firewalls.
D. Install a NIDS device at the boundary.
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which of the following is an example of risk avoidance?
A. Not taking preventive measures to stop the theft of equipment
B. Not installing new software to prevent compatibility errors
C. Installing security updates directly in production to expedite vulnerability fixes
D. Buying insurance to prepare for financial loss associated with exploits
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?
A. Lessons learned
B. Preparation
C. Recovery
D. Identification
Answer: (SHOW ANSWER)

NEW QUESTION: 57
The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and

filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?

A. NGFW

B. Web-application firewall

C. Next-generation SWG

D. CASB

Answer: (SHOW ANSWER)

NEW QUESTION: 58

Which of the following would be used to find the MOST common web-application vulnerabilities?

A. MITRE ATT&CK

B. OWASP

C. SDLC

D. Cyber Kill Chain

Answer: B (LEAVE A REPLY)

NEW QUESTION: 59

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

A. MAC filtering

B. Guards

C. Bollards

D. Network access control

E. Zero trust segmentation

F. Access control vestibules

Answer: E,F (LEAVE A REPLY)

NEW QUESTION: 60

An enterpnse has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?

A. Gray-box

B. Bug bounty

C. Black-box

D. Red-leam

E. White-box

Answer: E (LEAVE A REPLY)

NEW QUESTION: 61

A security administrator needs to inspect in-transit files on the enterprise network to search for PII, credit card data, and classification words. Which of the following would be the BEST to use?
A. EDR solution
B. HIPS software solution
C. Network DLP solution
D. IDS solution
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?
A. MSSP
B. Public cloud
C. Hybrid cloud
D. Fog computing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 63
Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?
A. The employee's physical access card was cloned.
B. The employee's biometrics were harvested
C. A criminal used lock picking tools to open the door.
D. The employee is colluding with human resources
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?
A. Bug bounty

B. Penetration testing
C. Wardriving
D. Code review
Answer: B (LEAVE A REPLY)

NEW QUESTION: 65
Which of the following terms describes a broad range of information that is sensitive to a specific organization?
A. Top secret
B. Proprietary
C. Open-source
D. Public
Answer: (SHOW ANSWER)

NEW QUESTION: 66
A bank detects fraudulent activity on user's account. The user confirms transactions completed yesterday on the bank's website at https:/Awww.company.com. A security analyst then examines the user's Internet usage logs and observes the following output:
Which of the following has MOST likely occurred?
A. SQL injection
B. Race conditions
C. Replay attack
D. SSL stripping
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
A forensics investigator is examining a number of unauthorized payments the were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:
<a href-"https://www.company.com/payto.do?
routing=00001111&accc=22223334&amount-250">Click here to unsubscribe Which of the following will the forensics investigator MOST likely determine has occurred?
A. XSS
B. XSRF
C. CSRF
D. SQL injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 68

Due to unexpected circumstances, an IT company must vacate its main office, forcing all operations to alternate, off-site locations. Which of the following will the company MOST likely reference for guidance during this change?

A. The business continuity plan

B. The retention policy

C. The disaster recovery plan

D. The incident response plan

Answer: A (LEAVE A REPLY)

BCP is to empower an organization to keep crucial functions running during downtime. This, in turn, helps the organization respond quickly to an interruption, while creating resilient operational protocols.

NEW QUESTION: 69

Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

A. An MOU

B. An SLA

C. An ARO

D. A BPA

Answer: (SHOW ANSWER)

NEW QUESTION: 70

A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down. Which of the following should the architect implement on the server to achieve this goal?

A. RAID

B. UPS

C. NIC teaming

D. Load balancing

Answer: C (LEAVE A REPLY)

NIC Teaming is a feature that allows a server to be connected to multiple network switches, providing redundancy and increased network availability. If one of the switches goes down, the server will still be able to send and receive data through one of the other switches. To configure NIC Teaming in Windows Server, see Microsoft's documentation: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming. For more information on NIC Teaming and other network redundancy features, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION: 71

The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

A. Requiring all new, on-site visitors to configure their devices to use WPS

B. Creating a unique PSK for every visitor when they arrive at the reception area

C. Implementing a new SSID for every event hosted by the college that has visitors

D. Deploying a captive portal to capture visitors' MAC addresses and names

Answer: (SHOW ANSWER)

NEW QUESTION: 72

A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

* The devices will be used internationally by staff who travel extensively.
* Occasional personal use is acceptable due to the travel requirements.
* Users must be able to install and configure sanctioned programs and productivity suites.
* The devices must be encrypted
* The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

A. Configuring an always-on VPN

B. Requiring web traffic to pass through the on-premises content filter

C. Implementing application whitelisting

D. Setting the antivirus DAT update schedule to weekly

Answer: (SHOW ANSWER)

NEW QUESTION: 73

Which of the following represents a biometric FRR?

A. The number of unauthorized users being granted access

B. The denied and authorized numbers being equal

C. Authorized users being denied access

D. Users failing to enter the correct PIN

Answer: C (LEAVE A REPLY)

NEW QUESTION: 74

Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

A. Whaling

B. Spam

C. Invoice scam

D. Pharming

Answer: D (LEAVE A REPLY)
Pharming: Phishing attempt to trick a user to access a different or fake website (usually by modifying hosts file)

NEW QUESTION: 75
Which of the following uses SAML for authentication?
A. TOTP
B. Kerberos
C. Federation
D. HOTP
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?
A. HIDS
B. EDR
C. NIPS
D. DLP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
ir security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted file"sThe analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?
A. HIDS
B. TPM
C. NGFW
D. Allow list
Answer: B (LEAVE A REPLY)

NEW QUESTION: 78
A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has Just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?
A. Memory dumps
B. The application logs
C. The log retention policy
D. The syslog server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 79
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?
A. The SNMP logs
B. The web server logs
C. The DNS logs
D. The SIP traffic logs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
During an incident response process involving a laptop, a host was identified as the entry point for malware. The management team would like to have the laptop restored and given back to the user. The cybersecurity analyst would like to continue investigating the intrusion on the host. Which of the following would allow the analyst to continue the investigation and also return the laptop to the user as soon as possible?
A. dd
B. head
C. tcpdump
D. memdump
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
An attacker is attempting to harvest user credentials on a client's wedsite, A security analyst notices multiple attempts of rencom usemames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:
The username you entered does not exist.
Which of the following should the analyst recommend be enabled?
A. Obfuscation

B. Error handling
C. Input validation
D. Username lockout
Answer: A (LEAVE A REPLY)

NEW QUESTION: 82
n attack relies on an end user visiting a website the end user would typically visit; however, the site is compromised and uses vulnerabilities in the end user's browser to deploy malicious software. Which of the following types of attack does this describe?
A. Phishing
B. Whaling
C. Watering hole
D. Smishing
Answer: (SHOW ANSWER)

NEW QUESTION: 83
A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?
A. Role-based access control
B. Discretionary access control
C. Mandatory access control
D. Attribute-based access control
Answer: B (LEAVE A REPLY)
Discretionary access control (DAC) is a model of access control based on access being determined "by the owner" of the resource in question. The owner of the resource can decide who does and does not have access, and exactly what access they are allowed to have.

NEW QUESTION: 84
Which of the following would be the BEST way to analyze diskless malware that has infected a VDI?
A. Run a full on-demand scan of the root volume.
B. Take a memory snapshot of the running system.
C. Use NetFlow to identify command-and-control IPs.
D. Shut down the VDI and copy off the event logs.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 85
A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body

of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

A. Review the email event logs

B. Establish chain of custody.

C. Inspect the file metadata.

D. Reference the data retention policy.

Answer: (SHOW ANSWER)

NEW QUESTION: 86

An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

A. A watering-hole attack

B. Typo squatting

C. A spear-phishing attack

D. A phishing attack

Answer: A (LEAVE A REPLY)

NEW QUESTION: 87

Which of the following must be in place before implementing a BCP?

A. SLA

B. AUP

C. NDA

D. BIA

Answer: (SHOW ANSWER)

NEW QUESTION: 88

A security engineering installing A WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy

B. Load-balanced servers

C. A decryption certificate

D. A split-tunnel VPN

Answer: C (LEAVE A REPLY)

NEW QUESTION: 89

While reviewing the wireless router, a systems administrator of a small business determines someone is spoofing the MAC address of an authorized device.

Given the table below:

Which of the following should be the administrator's NEXT step to detect if there is a rague system without impacting availability?

A. Physically check each system.

B. Deny Internet access to the "UNKNOWN" hostname.
C. Conduct a ping sweep.
D. Apply MAC filtering.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
Which of the following would satisfy three-factor authentication requirements?
A. Password, PIN, and physical token
B. PIN, fingerprint scan, and ins scan
C. Password, fingerprint scan, and physical token
D. PIN, physical token, and ID card
Answer: (SHOW ANSWER)
Three-factor authentication combines three types of authentication methods: something you know (password), something you have (physical token), and something you are (fingerprint scan). Option C satisfies these requirements, as it uses a password (something you know), a physical token (something you have), and a fingerprint scan (something you are) for authentication.
Reference:
Note: There could be other options as well that could satisfy the three-factor authentication requirements as per the organization's security policies.

NEW QUESTION: 91
A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?
A. S/MIME
B. DLP
C. IMAP
D. HIDS
Answer: B (LEAVE A REPLY)
Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

NEW QUESTION: 92
An attacker replaces a digitally signed document with another version that foes unnoticed. Upon reviewing the document's contents, the author notices some additional verbaige that was not originally in the document but can't validate an integrity issue. Which of the following attacks was used?
A. Prepending
B. Cryptomalware
C. Collision
D. Phising
Answer: C (LEAVE A REPLY)

NEW QUESTION: 93
Whichppf the following will MOST likely cause machine-learning and AI-enabled systems to operate with unintended consequences?
A. Stored procedures
B. Code reuse
C. Data bias
D. Buffer overflows
Answer: (SHOW ANSWER)

NEW QUESTION: 94
A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and Is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?
A. AUPS
B. Dual power supplies
C. A generator
D. APDU
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:
Which of the following can the security analyst conclude?
A. A credentialed vulnerability scanner attack is testing several CVEs against the application.
B. A replay attack is being conducted against the application.

C. A service account password may have been changed, resulting in continuous failed logins within the application.
D. An injection attack is being conducted against a user authentication system.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 96
When planning to build a virtual environment, an administrator need to achieve the following,
* Establish polices in Limit who can create new VMs
* Allocate resources according to actual utilization'
* Require justification for requests outside of the standard requirements.
* Create standardized categories based on size and resource requirements Which of the following is the administrator MOST likely trying to do?
A. Implement IaaS replication
B. Avoid VM sprawl
C. Product against VM escape
D. Deploy a PaaS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
An n that has a large number of mobile devices is explonng enhanced secunty controls to manage unauthonzed access if a device is lost or stolen. Specifically, mobile devices are mor than dmi (4 8km) from the busding, the management team would like to have the secunty team alerted and server resources restricted on those devices. Which of the following controls should the organization implement?
A. Near-field communication
B. GPS tagging
C. Geofencing
D. Lockout
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
Which of the following environment utilizes dummy data and is MOST to be installed locally on a system that allows to be assessed directly and modified easily wit each build?
A. Production
B. Staging
C. Development
D. Test
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99

A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive All connections are being dropped by the firewall. Which of the following would be the BEST option to remove the rules?
A. # iptables -F
B. # iptables -t mangle -X
C. # iptables -P INPUT -j DROP
D. # iptables -Z
Answer: C (LEAVE A REPLY)

NEW QUESTION: 100
A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?
A. CASB
B. SWG
C. Containerization
D. Automated failover
Answer: C (LEAVE A REPLY)
Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

NEW QUESTION: 101
A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?
A. Man-in- the middle
B. Spear-phishing
C. Evil twin
D. DNS poising
Answer: (SHOW ANSWER)
DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).
https://en.wikipedia.org/wiki/DNS_spoofing

NEW QUESTION: 102

A SECURITY ANALYST NEEDS TO FIND REAL-TIME DATA ON THE LATEST MALWARE AND IoCs WHICH OF THE FOLLOWING BEST DESCRIBE THE SOLUTION THE ANALYST SHOULD PERSUE?

A. SECURITY NEWS ARTICLES

B. PEER-REVIEWED CONTENT

C. ADVISORIES AND BULLETINS

D. THREAT FEEDS

Answer: D (LEAVE A REPLY)

NEW QUESTION: 103

A secutlly analyst needs to perform periodic vulnerabilly scans on produclion ayalems Which of the following scan types would produce the BEST vulnerability scan report?

A. Port

B. Host discovery

C. Credentialed

D. Intrusive

Answer: C (LEAVE A REPLY)

NEW QUESTION: 104

Which of the following Is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

A. To provide data to quantify risk based on the organization's systems

B. To keep all software and hardware fully patched for known vulnerabilities

C. To only allow approved, organization-owned devices onto the business network

D. To standardize by selecting one laptop model for all users in the organization

Answer: A (LEAVE A REPLY)

An effective asset management policy helps an organization understand and manage the systems, hardware, and software it uses, and how they are used, including their vulnerabilities and risks. This information is crucial for accurately identifying and assessing risks to the organization, and making informed decisions about how to mitigate those risks. This is the best reason to maintain an effective asset management policy.

NEW QUESTION: 105

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head

B. Tcpdump

C. grep

D. rail
E. curl
F. openssi
G. dd
Answer: A,C (LEAVE A REPLY)
A - "analyst needs to review the first transactions quickly"
C - "search the entire series of requests for a particular string"

NEW QUESTION: 106
A security analyst wants to fingerpnnt a web server Which of the following tools will the security analyst MOST likely use to accomplish this task?
A. nmap -p1-65S35 192.168.0.10
B. dig 192.168.0.10
C. cur1 --htad http://192.168.0.10
D. ping 192.168.0.10
Answer: (SHOW ANSWER)
HTTP/1.1 301 Moved Permanently
Server: cloudflare
Date: Thu, 01 Sep 2022 22:36:50 GMT
Content-Type: text/html
Content-Length: 167
Connection: keep-alive
Location: https://1.1.1.1/
CF-RAY: 74417cb04d6b9a50-MFE

NEW QUESTION: 107
In which of the following risk management strategies would cybersecurity insurance be used?
A. Transference
B. Mitigation
C. Avoidance
D. Acceptance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack Which of the following options will mitigate this issue without compromising the number of outlets available?
A. Adding a new UPS dedicated to the rack
B. Installing a managed PDU
C. Using only a dual power supplies unit
D. Increasing power generator capacity
Answer: B (LEAVE A REPLY)
A managed Power Distribution Unit (PDU) allows you to monitor and control power outlets on the rack. This will allow the security team to identify which devices are drawing power and from which outlets, which can help to identify any unauthorized devices. Moreover, with a managed PDU, you can also control the power to outlets, turn off outlets that are not in use, and set up alerts if an outlet is overloaded. This will help to mitigate the issue of power consumption overloads without compromising the number of outlets available.

NEW QUESTION: 109
A security analyst is reviewing logs on a server and observes the following output:
Which of the following is the security analyst observing?
A. A keylogger attack
B. A rainbow table attack
C. A password-spraying attack
D. A dictionary attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
A user wanted to catch up on some work over the weekend but had issues logging in to the corporate network using a VPN. On Monday, the user opened a ticket for this issue but was able to log in successfully. Which of the following BEST describes the policy that is being implemented?
A. Time-based logins
B. Geofencing
C. Password history
D. Network location
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
A security analyst is designing the appropnate controls to limit unauthorized access to a physical site The analyst has a directive to utilize the lowest possible budget Which of the following would BEST meet the requirements?

A. Preventive controls
B. Compensating controls
C. Deterrent controls
D. Detective controls
Answer: C (LEAVE A REPLY)
Deterrent makes sense on further thought. The question just states unauthorized access. It doesn't state the intent of any unauthorized intruders. Deterrence is designed to reduce the occurrence of unintentional bystanders or unmotivated malicious agents from entering the site. Should the agent be motivated enough, a preventative measure is needed. But again, the question doesn't list intentions. Therefore this method works to limit the number of unauthorized visitors by weeding out everyone but the motivated, and the truly stupid.

NEW QUESTION: 112
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?
A. Investigation
B. Lessons learned
C. Recovery
D. Containment
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Which of the following stores data directly on devices with limited processing and storage capacity?
A. Hybrid cloud
B. Edge
C. Thin client
D. Containers
Answer: (SHOW ANSWER)

NEW QUESTION: 114
A news article states hackers have been selling access to IoT camera feeds. Which of the following is the Most likely reason for this issue?
A. Backdoors
B. Weak credentials
C. Lack of encryption
D. Outdated software
Answer: B (LEAVE A REPLY)

NEW QUESTION: 115

An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. Distributed denial-of-service
B. Domain hijacking
C. DNS tunneling
D. DNS cache poisoning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
A user is attempting to navigate to a website from inside the company network using a desktop. When the user types in the URL. https://www.site.com, the user is presented with a certificate mismatch warning from the browser. The user does not receive a warning when visiting http://www.anothersite.com. Which of the following describes this attack?

A. Domain hijacking
B. DNS poisoning
C. On-path
D. Evil twin
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which of the following can work as an authentication method and as an alerting mechanism for unauthorized access attempts?

A. Smart card
B. push notifications
C. HMAC-based, one-time password
D. Attestation service
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
A Chief Security Officer (CSO) is concerned that cloud-based services are not adequately protected from advanced threats and malware The CSO believes there is a high risk that a data breach could occur in the near future due to the lack of detective and preventive controls Which of the following should be implemented to BEST address the CSO's concerns? {Select TWO)

A. Segmentation
B. Encryption
C. Containerization
D. An NG-SWG

E. AWAF
F. ACASB
Answer: C,F (LEAVE A REPLY)

NEW QUESTION: 119
A security administrator has discovered that workstations on the LAN are becoming infected with malware. The cause of the infections appears to be users receiving phishing emails that are bypassing the current email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?
A. A jump server
B. HIDS
C. Awareness training
D. Forward proxy
E. IPS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120
The compliance team requires an annual recertification of privileged and non-privileged user access. However, multiple users who left the company six months ago still have access. Which of the following would have prevented this compliance violation?
A. Account audits
B. AUP
C. Password reuse
D. SSO
Answer: A (LEAVE A REPLY)
Account audits are periodic reviews of user accounts to ensure that they are being used appropriately and that access is being granted and revoked in accordance with the organization's policies and procedures. If the compliance team had been conducting regular account audits, they would have identified the users who left the company six months ago and ensured that their access was revoked in a timely manner. This would have prevented the compliance violation caused by these users still having access to the company's systems.
To prevent this compliance violation, the company should implement account audits. An account audit is a regular review of all user accounts to ensure that they are being used properly and that they are in compliance with the company's security policies. By conducting regular account audits, the company can identify inactive or unused accounts and remove access for those users. This will help to prevent compliance violations and ensure that only authorized users have access to the company's systems and data.

NEW QUESTION: 121

An organization maintains several environments in which patches are developed and tested before deployed to an operation status. Which of the following is the environment in which patches will be deployed just prior to being put into an operational status?

A. Development

B. Test

C. Production

D. Staging

Answer: D (LEAVE A REPLY)

The staging environment is an optional environment, but it is commonly used when an organization has multiple production environments. After passing testing, the system moves into staging, from where it can be deployed to the different production systems.

NEW QUESTION: 122

Which of the following actions would be recommended to improve an incident response process?

A. Train the team to identify the difference between events and incidents

B. Modify access so the IT team has full access to the compromised assets

C. Contact the authorities if a cybercrime is suspected

D. Restrict communication surrounding the response to the IT team

Answer: (SHOW ANSWER)

NEW QUESTION: 123

Several large orders of merchandise were recently purchased on an e-commerce company's website. The totals for each of the transactions were negative values, resulting in credits on the customers?

accounts. Which of the following should be implemented to prevent similar situations in the future?

A. Make sure transactions that are submitted within very short time periods are prevented from being processed.

B. Calculate all possible values to be added together and ensure the use of the proper integer in the code.

C. Configure the web application firewall to look for and block session replay attacks.

D. Ensure input validation is in place to prevent the use of invalid characters and values.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 124
A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?
A. Run a vulnerability scan.
B. Disable unneeded services.
C. Encrypt all disks.
D. Install the latest security patches.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 125
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the real data?
A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization
Answer: B (LEAVE A REPLY)
https://ktechproducts.com/Data-mask#:~:text=Data%20Masking%20is%20a%20method%20of%20creating%20a,partial%20data%20based%20on%20the%20user%E2%80%99s%20security%20permissions.
The main reason for applying masking to a data field is to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data. However, the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. It is more common to have masking applied to data that is represented outside of a corporate production system. In other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles https://en.wikipedia.org/wiki/Data_masking

NEW QUESTION: 126
A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following BEST describes these systems?
A. Neural networks
B. DNS sinkholes
C. Virtual machines
D. Hafieypots
Answer: (SHOW ANSWER)

NEW QUESTION: 127

During a recent security assessment, a vulnerability was found in a common OS, The OS vendor was unaware of the issue and promised to release a patch within next quarter, Which of the following BEST describes this type of vulnerability?

A. Supply chain

B. Weak configuration

C. Legacy operating system

D. Zero day

Answer: D (LEAVE A REPLY)

NEW QUESTION: 128

Which of the following conditions impacts data sovereignty?

A. Rights management

B. Healthcare data

C. Criminal investigations

D. Intemational operations

Answer: D (LEAVE A REPLY)

NEW QUESTION: 129

A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

A. SAML

B. PAP

C. OAuth

D. SSO

Answer: (SHOW ANSWER)

NEW QUESTION: 130

A security administrator is seeking a solution to prevent unauthorized access to the internal network. Which of the following security solutions should the administrator choose?

A. MAC filtering

B. Anti-malware

C. Translation gateway

D. VPN

Answer: D (LEAVE A REPLY)

A VPN (virtual private network) is a secure tunnel used to encrypt traffic and prevent unauthorized access to the internal network. It is a secure way to extend a private network across public networks, such as the Internet, and can be used to allow remote users to securely access resources on the internal network. Additionally, a VPN can be used to prevent malicious traffic from entering the internal network.

NEW QUESTION: 131

An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise. Which of the following will accomplish this goal?
A. IPS.
B. FIM
C. FTP
D. Antivirus
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears.
The task list shows the following results
Which of the following is MOST likely the issue?
A. RAT
B. Spyware
C. PUP
D. Keylogger
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
Which of the following would MOST likely support the integrity of a voting machine?
A. Blockchain
B. Transport Layer Security
C. Asymmetric encryption
D. Perfect forward secrecy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 134
The Chief Information Security Officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer dat a. Which of the following would be BEST for the third-party vendor to provide to the CISO?
A. GDPR compliance attestation
B. Cloud Security Alliance materials
C. SOC 2 Type 2 report
D. NIST RMF workbooks
Answer: (SHOW ANSWER)
https://www.itgovernance.co.uk/soc-reporting

NEW QUESTION: 135
Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?

A. Full interruption
B. Parallel
C. Simulation
D. Tabletop
Answer: (SHOW ANSWER)

NEW QUESTION: 136
A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?
A. Ephemeral
B. Homomorphic
C. Symmetric
D. Asymmetric
Answer: (SHOW ANSWER)

NEW QUESTION: 137
The Chief Information Secunty Officer (CISO) requested a report on potential areas of improvement following a security incident. Which of the following incident response processes is the CISO requesting?
A. Detection
B. Root cause analysis
C. Lessons learned
D. Containment
E. Preparation
Answer: (SHOW ANSWER)

NEW QUESTION: 138
A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability

of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

A. iPSec

B. Always On

C. L2TP

D. Split tunneling

Answer: (SHOW ANSWER)

NEW QUESTION: 139

A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

A. Configure HIPS

B. Utilize a WAF

C. Implement input validations

D. Deploy MFA

Answer: D (LEAVE A REPLY)

NEW QUESTION: 140

A Chief Security Officer is looking for a solution that can reduce the occurrence of customers receiving errors from back-end infrastructure when systems go offline unexpectedly. The security architect would like the solution to help maintain session persistence. Which of the following would BEST meet the requirements?

A. Reverse proxy

B. Forward proxy

C. Load balancer

D. NIC teaming

Answer: D (LEAVE A REPLY)

NEW QUESTION: 141

A Chief Information Security Officer (CISO) is evaluating (he dangers involved in deploying a new ERP system tor the company. The CISO categorizes the system, selects the controls mat apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system Which of the following is the CISO using to evaluate Hie environment for this new ERP system?

A. CIS Critical Security Controls

B. NIST Risk Management Framevtoik

C. ISO 27002

D. The Diamond Model of Intrusion Analysis

Answer: (SHOW ANSWER)

NEW QUESTION: 142

After a recent security breach a security analyst reports that several admimstratrve usemames and passwords are being sent via cieartext across the network to access network devices over prot 23 Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configunng network devices?

A. SSH
B. Telnet
C. SNMPv3
D. SFTP
E. FTP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 143
Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?

A. Privileged access management
B. RADIUS
C. Attribute-based access control
D. SSO
Answer: A (LEAVE A REPLY)

NEW QUESTION: 144
A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and Chin a. Payments for services are managed bya third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?

A. ISO/IEC 27032 Cybersecurity Guidelines
B. Payment Card Industry Data Security Standard
C. Cloud Security Alliance Best Practices
D. General Data Protection Regulation
Answer: (SHOW ANSWER)

NEW QUESTION: 145
Which of the following describes the ability of code to target a hypervisor from inside

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

Answer: B (LEAVE A REPLY)
Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor. https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%20an,VMs)%20running%20on%20that%20host.

NEW QUESTION: 146
An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would BEST maintain high-quality video conferencing while minimizing latency when connected to the VPN?
A. Utilizing split tunneling so only traffic for corporate resources is encrypted
B. Using geographic diversity to have VPN terminators closer to end users
C. Purchasing higher-bandwidth connections to meet the increased demand
D. Configuring QoS properly on the VPN accelerators
Answer: D (LEAVE A REPLY)

NEW QUESTION: 147
A financial nstitution wauid like to stare its customer data in a coud but still allaw the data ta he accessed and manipulated while encrypted. Doing so would prevent the claud servine provider from heing adle ta decipher the data due ta its sensitivity. The financial institutan is not concernec about computational averheads and slow speeds, Which of the follawing cryotographic techniques would BEST meet the requirement?
A. Homeomorphic
B. Asymmatric
C. Symmetric
D. Ephemeral
Answer: (SHOW ANSWER)

NEW QUESTION: 148
A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?
A. The incident response process
B. The Cyber Kill Chain e
C. The MITRE CVE database
D. The Diamond Mode! of Intrusion Analysis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 149

A Chief Security Officer is looking for a solution that can provide increased scalability and flexibility for back-end infrastructure, allowing it to be updated and modified without disruption to services. The security architect would like the solution selected to reduce the back-end server resources and has highlighted that session persistence is not important for the applications running on the back-end servers. Which of the following would BEST meet the requirements?
A. Reverse proxy
B. Automated patch management
C. Snapshots
D. NIC teaming
Answer: (SHOW ANSWER)
A reverse proxy would be the best solution for increased scalability and flexibility for back-end infrastructure.

NEW QUESTION: 150
A administrator needs to allow mobele BYOD devices to access network resources, As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practces for authentication and infrastructure security? (Select TWO)
A. Use a captive portal for user authentication
B. Implement SSO and allow communication to the intemal network.
C. Authenticate users using OAuth for more resiliency.
D. Use a new and updated RADIUS server to mamntain the best solution
E. Use the existing network and allow communscation to the internal network and servers
F. Create a new network for the mobile devices and block the commurycaton to the intemal network and servers
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 151
Which of the following describes where an attacker can purchase DDoS or ransomware services?
A. Threat intelligence
B. Open-source intelligence
C. Vulnerability database
D. Dark web
Answer: (SHOW ANSWER)
The best option to describe where an attacker can purchase DDoS or ransomware services is the dark web. The dark web is an anonymous, untraceable part of the internet where a variety of illicit activities take place, including the purchase of DDoS and ransomware services. According to the CompTIA Security+ SY0-601 Official Text Book, attackers can purchase these services anonymously and without the risk of detection or attribution. Additionally, the text book recommends that organizations monitor the dark web to detect any possible threats or malicious activity.

NEW QUESTION: 152
A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?
A. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
B. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
C. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.
D. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 153
To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain Which of the following is being used?
A. DMARC
B. PFS
C. DNSSEC
D. SPF
Answer: (SHOW ANSWER)

NEW QUESTION: 154
An administrator needs to protect user passwords and has been advised to hash the passwords. Which of the following BEST describes what the administrator is being advised to do?
A. Add extra data to the passwords so their length is increased, making them harder to brute force
B. Perform a mathematical operation on the passwords that will convert them into umgue stnngs
C. Store all passwords in the system in a rainbow table that has a centralized location
D. Enforce the use of one-time passwords that are changed for every login session.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 155
A company has limited storage available and online presence that cannot for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time In the event of a failure, which being maindful of the limited available storage space?
A. Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
B. Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00
C. Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
D. Implement nightly full backups every Sunday at 8:00 p.m
Answer: (SHOW ANSWER)

NEW QUESTION: 156
Which of the following would BEST provide a systems administrator with the ability to more efficiently identify systems and manage permissions and policies based on location, role, and service level?
A. Domain services
B. Standard naming conventions
C. Diagrams
D. Baseline configurations
Answer: D (LEAVE A REPLY)

NEW QUESTION: 157
A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)
A. Antivirus software
B. Full disk encryption
A VPN
C. A host-based firewall
D. A DLP solution
E. Trusted Platform Module
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 158
A security analyst needs to be able to search and correlate logs from multiple sources in a single tool Which of the following would BEST allow a security analyst to have this ability?
A. SOAR
B. SIEM
C. Log collectors
D. Network-attached storage

Answer: (SHOW ANSWER)
SIEM event correlation is an essential part of any SIEM solution. It aggregates and analyzes log data from across your network applications, systems, and devices, making it possible to discover security threats and malicious patterns of behaviors that otherwise go unnoticed and can lead to compromise or data loss.

NEW QUESTION: 159
Which of the following provides a calculated value for known vulnerabilities so organizations can prioritize mitigation steps?
A. CVSS
B. SIEM
C. SOAR
D. CVE
Answer: (SHOW ANSWER)
CVSS is maintained by the Forum of Incident Response and Security Teams (first.org/cvss). CVSS metrics generate a score from 0 to 10 based on characteristics of the vulnerability, such as whether it can be triggered remotely or needs local access, whether user intervention is required, and so on

NEW QUESTION: 160
Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?
A. The document is a backup file if the system needs to be recovered.
B. The document is a keylogger that stores all keystrokes should the account be compromised.
C. The document is a standard file that the OS needs to verify the login credentials.
D. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
Answer: (SHOW ANSWER)

NEW QUESTION: 161
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?
A. An incident response plan
B. A disaster recovery plan
C. A communications plan
D. A business continuity plan
Answer: (SHOW ANSWER)

NEW QUESTION: 162
An organization wants to participate in threat intelligence information sharing with peer groups. Which of the following would MOST likely meet the organizations requirement?
A. Implement a TAXII server

B. Subscribe to threat intelligence feeds
C. Submit RFCs
D. Perform OSINT investigations
Answer: (SHOW ANSWER)

NEW QUESTION: 163
During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?
A. The chain of custody form did not note time zone offsets between transportation regions
B. The forensic investigator forgot to run a checksum on the disk image after creation
C. The hard drive was not properly kept in an antistatic bag when rt was moved
D. The computer was turned off. and a RAM image could not be taken at the same time
Answer: B (LEAVE A REPLY)

NEW QUESTION: 164
Which of the following should a data owner require all personnel to sign to legally protect intellectual property?
A. An MOU
B. An ISA
C. An NDA
D. An AUP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 165
A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following
* The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.
* One of the websites the manager used recently experienced a data breach
* The manager's corporate email account was successfully accessed in the last fve days by an IP address located in a foreign country Which of the following attacks has MOST hkely been used to compromise the manager's corporate account?
A. Remote access Trojan
B. Password spraying
C. Oicbonary
D. Credential stuffing
E. Brute-force
Answer: D (LEAVE A REPLY)

NEW QUESTION: 166

A security engineer is concerned about using an agent on devices that relies completely on defined known-bad signatures. The security engineer wants to implement a tool with multiple components including the ability to track, analyze, and monitor devices without reliance on definitions alone. Which of the following solutions BEST fits this use case?

A. EDR

B. DLP

C. NGFW

D. HIPS

Answer: A (LEAVE A REPLY)

The acronym EDR stands for Endpoint Detection and Response and is also known as EDTR. It is an endpoint security solution that is responsible for continuous monitoring of endpoints. This permanent monitoring enables the technology to detect and respond to cyber threats such as malware or ransomware at an early stage. The basis for this is always the analysis of context-related information, which can be used to make corrective proposals for recovery.

NEW QUESTION: 167

An organization has hired a ted team to simulate attacks on its security posture Which of the following will the blue team do after detecting an IoC?

A. Conduct passive reconnaissance to gather information

B. Conduct forensics on the compromised system

C. Activate runbooks for incident response

D. Reimage the impacted workstations

Answer: (SHOW ANSWER)

NEW QUESTION: 168

A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboars are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

A. Credential exposure

B. Social engineering

C. Loss of proprietary information

D. Damage to the company's reputation
Answer: (SHOW ANSWER)

NEW QUESTION: 169
During a Chiet Information Securty Officer (CISO) comvenbon to discuss security awareness, the affendees are provided with a network connection to use as a resource. As the Convention progresses. ane of the attendees starts to notice delays in the connection. and the HTTPS ste requests are reverting to HTTP. Which of the folowing BEST describes what is happening?
A. A SSL/TLS downgrade
B. Birtuday colfisices on the cartificate key
C. DNS hijackeng to reroute tratic
D. Brute force 1 tho access point
Answer: (SHOW ANSWER)

NEW QUESTION: 170
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?
A. HSM
B. SED
C. DLP
D. TPM
Answer: (SHOW ANSWER)

NEW QUESTION: 171
A company discovered that terabytes of data have been exfiltrated over the past year after an employee clicked on an email link. The threat continued to evolve and remain undetected until a security analyst noticed an abnormal amount of external connections when the employee was not working. Which of the following is the MOST likely threat actor?
A. Shadow IT
B. Script kiddies
C. APT
D. Insider threat
Answer: C (LEAVE A REPLY)
An APT attack is characterized by using toolkits to achieve a presence on a target network and then, instead of just moving to steal information, focusing on the long game by maintaining a persistent presence on the target network. The tactics, tools, and procedures of APTs are focused on maintaining administrative access to the target network and avoiding detection. Then, over the long haul, the attacker can remove intellectual property and more from the organization, typically undetected.

NEW QUESTION: 172

A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business Which of the following constraints BEST describes the reason the findings cannot be remediated?

A. Implied trust

B. Lack of computing power

C. inability to authenticate

D. Unavailable patch

Answer: D (LEAVE A REPLY)

NEW QUESTION: 173

An attacked is attempting to exploit users by creating a fake website with the URL www.validwebsite.com.

The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

A. Impersonation

B. Watering-hole attack

C. Type squatting

D. Information elicitation

Answer: (SHOW ANSWER)

NEW QUESTION: 174

The Chief information Securtty Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside cornpany. Additionally, the CISO would Ske this solution to provide the same protections even when a company laptop or mobile device ts away from # home office. Which of the following should the CISO choose?

A. CASB

B. Web-application firewall

C. NGFW

D. Next-generation SWG

Answer: A (LEAVE A REPLY)

NEW QUESTION: 175

A cybersecunty administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO)

A. WAF

B. NIPS

C. NIDS

D. HSM

E. HIDS
F. HIPS
G. Stateless firewall
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 176
A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage. Which of the following is MOST likely the cause?
A. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
B. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.
C. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.
D. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
Answer: (SHOW ANSWER)

NEW QUESTION: 177
Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations. Which of the following documents did Ann receive?
A. A non-disclosure agreement
B. A memorandum of understanding
C. A privileged-user agreement
D. An annual privacy notice
Answer: D (LEAVE A REPLY)

NEW QUESTION: 178
Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).
A. Video surveillance
B. Bollards
C. Mantraps
D. Security guards
E. Fences
F. Antivirus
Answer: (SHOW ANSWER)

NEW QUESTION: 179

A secunity engineer needs to create a network segment that can be used for servers thal require connections from untrusted networks. Which of the following should the engineer implement?
A. A hot site
B. An air gap
C. A VUAN
D. A screened subnet
Answer: D (LEAVE A REPLY)

NEW QUESTION: 180
A business operations manager is concerned that a PC that is critical to business operations will have a costly hardware failure soon. The manager is looking for options to continue business operations without incurring large costs. Which of the following would mitigate the manager's concerns?
A. Implement a full system upgrade
B. Install uninterruptible power supplies
C. Purchase cybersecurity insurance
D. Perform a physical-to-virtual migration
Answer: (SHOW ANSWER)

NEW QUESTION: 181
A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?
A. PCI DSS
B. ISO 22301
C. ISO 27001
D. NIST CSF
Answer: A (LEAVE A REPLY)
Additionally, many organizations should abide by certain standards. For example, organizations handling credit card information need to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS includes six control objectives and 12 specific requirementsthat help prevent fraud

NEW QUESTION: 182
A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of (he following should the manager request to complete the assessment?
A. A service-level agreement
B. A memorandum of understanding
C. A business partnership agreement
D. A SOC 2 Type 2 report
Answer: A (LEAVE A REPLY)

NEW QUESTION: 183
it a current private key is compromised, which of the following would ensure it cannot be used to decrypt ail historical data?
A. Homomorphic encryption
B. Key stretching
C. Pertect forward secrecy
D. Eiliptic-curve cryptography
Answer: D (LEAVE A REPLY)

NEW QUESTION: 184
Which of the following BEST describes a security exploit for which a vendor patch is not readily available?
A. Integer overflow
B. Race condition
C. Zero-day
D. End of life
Answer: C (LEAVE A REPLY)

NEW QUESTION: 185
An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?
A. Application management
B. Screen locks
C. Geofencing
D. Containerization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 186
Against the recommendation of the IT security analyst, a company set all user passwords on a server as "P@)55wOrD". Upon review of the /etc/pesswa file, an attacker found the following: hich of the following BEST explains why the encrypted passwords do not match?
A. Salting
B. Perfect forward secrecy
C. Hashing
D. Key stretching
Answer: A (LEAVE A REPLY)

NEW QUESTION: 187
A recent security assessment revealed that an actor explolied a vuinerable workstation willvin an organization and has persisted on the network for several months. The organization realizes the need to reassess Its seourlty strategy for mitigating risks within the perimeter Which of the following solutions woukl BEST support the organization's strategy?
A. FIM
B. OOP
C. EOR
D. DUT
Answer: A (LEAVE A REPLY)
The best solution to support the organization's security strategy in this situation is File Integrity Monitoring (FIM). FIM is a technique used to detect and monitor unauthorized changes to critical files and system configurations on a computer or network. It is used to detect malicious activity such as malware, unauthorized modifications, and malicious user activity. FIM can also be used to detect and monitor compliance with security policies and procedures.

NEW QUESTION: 188
A security analyst has been reading about a newly discovered cyberattack from a known threat actor. Which of the following would BEST support the analyst's review of the tactics, techniques, and protocols the threat actor was observed using in previous campaigns?
A. Security research publications
B. The Diamond Model of Intrusion Analysis
C. The MITRE ATT&CK framework
D. The Cyber Kill Chain
Answer: C (LEAVE A REPLY)

NEW QUESTION: 189
A security analyst Is hardening a Linux workstation and must ensure It has public keys forwarded to remote systems for secure login Which of the following steps should the analyst perform to meet these requirements?
(Select TWO).

A. Forward the keys using ssh-keyger.
B. Forward the keys using ssh-copy-id.
C. Forward the keys using ash -i.
D. Forward the keys using scp.
E. Forward the keys using openssl -s.
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 190
During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:
Which of the following attacks occurred?
A. Buffer overflow
B. SQL injection
C. Pass the hash
D. Replay attack
Answer: (SHOW ANSWER)

NEW QUESTION: 191
A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:
Which of the following attacks does the analyst MOST likely see in this packet capture?
A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning
Answer: B (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack
One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an evil twin access point which then can be used to capture network packets transferred between the client and the access point.

NEW QUESTION: 192
A company is considering transitioning to the cloud. The company employs individuals from various locations around the world The company does not want to increase its on-premises infrastructure blueprint and only wants to pay for additional compute power required. Which of the following solutions would BEST meet the needs of the company?
A. Private cloud
B. Hybrid environment
C. Hot backup site
D. Managed security service provider

Answer: B (LEAVE A REPLY)

NEW QUESTION: 193
A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted Which of the following resiliency techniques was applied to the network to prevent this attack?
A. High availability
B. Port mirroring
C. Geographic dispersal
D. NIC Teaming
E. Defense in depth
Answer: E (LEAVE A REPLY)

NEW QUESTION: 194
Which of the following describes a social engineering technique that seeks to exploit a person's sense of urgency?
A. A phishing email stating a cash settlement has been awarded but will expire soon
B. A smishing message stating a package is scheduled for pickup
C. A vishing call that requests a donation be made to a local charity
D. A SPIM notification claiming to be undercover law enforcement investigating a cybercrime
Answer: A (LEAVE A REPLY)
Phishing
As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.
https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Phishing,curiosity%20or%20fear%20in%20victims.

NEW QUESTION: 195
A software company adopted the following processes before releasing software to production;
* Peer review
* Static code scanning
* Signing
A considerable number of vulnerabilities are still being detected when code is executed on production Which of the following security tools can improve vulnerability detection on this environment?
A. Endpoint detection and response solution
B. Encrypted code repository
C. File integrity monitonng for the source code
D. Dynamic code analysis tool

Answer: (SHOW ANSWER)

NEW QUESTION: 196
Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution. The security team has received the following requirements:
* There must be visibility into how teams are using cloud-based services.
* The company must be able to identify when data related to payment cards is being sent to the cloud.
* Data must be available regardless of the end user's geographic location
* Administrators need a single pane-of-glass view into traffic and trends.
Which of the following should the security analyst recommend?
A. Implement a CASB solution.
B. Create firewall rules to restrict traffic to other cloud service providers.
C. Configure a web-based content filter.
D. Install a DLP solution to monitor data in transit.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 197
Field workers in an organization are issued mobile phones on a daily basis All the work is performed within one city and the mobile phones are not used for any purpose other than work The organization does not want these pnones used for personal purposes. The organization would like to issue the phones to workers as permanent devices so the pnones do not need to be reissued every day Qven the conditions described, which of the following technologies would BEST meet these requirements'
A. Mobile device management
B. Remote wiping
C. Geofencing
D. Containenzation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 198

Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?

A. SLA

B. MOU

C. EOL

D. EOSL

Answer: A (LEAVE A REPLY)

NEW QUESTION: 199

Which of the following typically uses a combination of human and artificial intelligence to analyze event data and take action without intervention?

A. SOAR

B. SIEM

C. OSINT

D. TTP

Answer: A (LEAVE A REPLY)

NEW QUESTION: 200

An organization is planning lo open other data centers to sustain operations in the event of a natural disaster. Which of the following considerations would BEST support the organization's resiliency?

A. Generator power

B. Fire suppression

C. Geographic dispersal

D. Facility automation

Answer: C (LEAVE A REPLY)

NEW QUESTION: 201

Which of Ihe following control types is patch management classified under?

A. Deterrent

B. Physical

C. Corrective

D. Detective

Answer: (SHOW ANSWER)

Patch management is classified as a corrective control because it is used to correct vulnerabilities or weaknesses in systems and applications after they have been identified. It is a reactive approach that aims to fix problems that have already occurred rather than prevent them from happening in the first place.

NEW QUESTION: 202

A company recently experienced an inside attack using a corporate machine that resulted in data compromise. Analysis indicated an unauthorized change to the software circumvented technological protection measures, The analyst was tasked with determining the best method to ensure the integrity of the systems remains intact and local and remote boot attestation can take place. Which of the following would provide the BEST solution?

A. HIPS

B. Flm

C. TPM

D. DLP

Answer: (SHOW ANSWER)

https://docs.microsoft.com/en-us/azure/security/fundamentals/measured-boot-host-attestation

NEW QUESTION: 203

An organization is outlining data stewardship roles and responsibilities. Which of the following employee roles would determine the purpose of data and how to process it?

A. Data custodian

B. Data proton officer

C. Data processor

D. Data controller

Answer: B (LEAVE A REPLY)

NEW QUESTION: 204

A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Revoke the client's network access certificates

B. Quarantine the host from other parts of the network

C. Add a deny-all rule to that host in the network ACL

D. Implement a network-wide scan for other instances of the malware.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 205

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS

Click on each firewall to do the following:

Deny cleartext web traffic.

Ensure secure management protocols are used. Please Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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

Answer:
Firewall 1:
DNS Rule - ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound - 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT
Management - ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound - ANY --> ANY --> HTTPS --> PERMIT
HTTP Inbound - ANY --> ANY --> HTTP --> DENY
Firewall 2: No changes should be made to this firewall
Firewall 3:
DNS Rule - ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound - 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT
Management - ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound - ANY --> ANY --> HTTPS --> PERMIT
HTTP Inbound - ANY --> ANY --> HTTP --> DENY

NEW QUESTION: 206
During a recent security incident at a multinational corporation a security analyst found the following logs for an account called user:
Which Of the following account policies would BEST prevent attackers from logging in as user?
A. Impossible travel time
B. Geofencing
C. Time-based logins
D. Geolocation
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Which of the following BEST reduces the security risks introduced when running systems that have expired vendor support and lack an immediate replacement?
A. Classify the system as shadow IT.
B. Increase the frequency of vulnerability scans
C. Implement proper network access restrictions B. Initiate a bug bounty program
Answer: C (LEAVE A REPLY)

NEW QUESTION: 208
Which of the following are the BEST ways to implement remote home access to a company's intranet systems if establishing an always-on VPN is not an option? (Select Two)
A. Enable MFA for intranet systems
B. Establish SSH access to a jump server
C. Configure SNMPv3 server and clients.
D. Install VPN concentrations at home offices
E. Implement a SSO solution

F. Create NAT on the firewall for intranet systems
Answer: (SHOW ANSWER)

NEW QUESTION: 209
An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would BEST support the new office?
A. Full tunnel
B. Always On
C. Site-to-site
D. Remote access
Answer: C (LEAVE A REPLY)

NEW QUESTION: 210
Which of the following employee roles is responsible for protecting an organization's collected personal information?
A. CTO
B. DPO
C. CEO
D. DBA
Answer: (SHOW ANSWER)
Many companies also have a data protection officer or DPO. This is a higher-level manager who is responsible for the organization's overall data privacy policies.
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/#:~:text=Many%20companies%20also%20have%20a,organization's%20overall%20data%20privacy%20policies.

NEW QUESTION: 211
During an incident response, a security analyst observes the following log entry on the web server.
Which of the following BEST describes the type of attack the analyst is experience?
A. SQL injection
B. Directory traversal
C. Pass-the-hash
D. Cross-site scripting
Answer: B (LEAVE A REPLY)

NEW QUESTION: 212
A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?
A. View the document's metadata for origin clues
B. Detonate the document in an analysis sandbox
C. Open the document on an air-gapped network
D. Search for matching file hashes on malware websites
Answer: (SHOW ANSWER)

NEW QUESTION: 213
A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site Upon investigation, a security analyst the identifies the following:
* The legitimate websites IP address is 10.1.1.20 and eRecruit local resolves to the IP
* The forged website's IP address appears to be 10.2.12.99. based on NetFtow records
* AH three at the organization's DNS servers show the website correctly resolves to the legitimate IP
* DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.
Which of the following MOST likely occurred?
A. An attacker temporarily pawned a name server
B. A reverse proxy was used to redirect network traffic
C. An SSL strip MITM attack was performed
D. An ARP poisoning attack was successfully executed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 214
A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST descnbes this technique?
A. Smishing
B. Phishing
C. Whaling
D. Vishing

Answer: A (LEAVE A REPLY)

NEW QUESTION: 215
The management team has requested that the security team implement 802.1X into the existing wireless network setup. The following requirements must be met:
* Minimal interruption to the end user
* Mutual certificate validation
Which of the following authentication protocols would meet these requirements?
A. EAP-FAST
B. PSK
C. EAP-TTLS
D. EAP-TLS
Answer: D (LEAVE A REPLY)
EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses certificates to provide mutual authentication between the client and the authentication server. It also allows for the encryption of user credentials, making EAP-TLS a secure and reliable authentication protocol. According to the CompTIA Security+ SY0-601 Official Text Book, EAP-TLS is well-suited for wireless networks due to its mutual authentication capabilities and its ability to securely store credentials. It is also the preferred authentication protocol for 802.1X wireless networks.

NEW QUESTION: 216
A security analyst is reviewing the following attack log output:
Which of the following types of attacks does this MOST likely represent?
A. Rainbow table
B. Brute-force
C. Password-spraying
D. Dictionary
Answer: C (LEAVE A REPLY)
Password spraying is a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts. https://us-cert.cisa.gov/ncas/current-activity/2019/08/08/acsc-releases-advisory-password-spraying-attacks#:~:text=Password%20spraying%20is%20a%20type,rapid%20or%20frequent%20account%20lockouts.

NEW QUESTION: 217
A security proposal was set up to track requests for remote access by creating a baseline of the users' common sign-in properties. When a baseline deviation is detected, an Iv1FA challenge will be triggered. Which of the following should be configured in order to deploy the proposal?
A. Context-aware authentication

B. Simultaneous authentication of equals
C. Extensive authentication protocol
D. Agentless network access control
Answer: A (LEAVE A REPLY)
An access control scheme that verifies an object's identity based on various environmental factors, like time, location, and behavior.

NEW QUESTION: 218
Which of the following prevents an employee from seeing a colleague who is visting an inappropriate website?
A. Job roration policy
B. Separation of duties policy
C. NDA
D. AUP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 219
A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)
A. Scan for rogue access points
B. Perform a site survey
C. Deploy an FTK Imager
D. Create a heat map
E. Upgrade the security protocols
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 220
A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?
A. Credential stuffing
B. Bluejacking
C. SQL injection
D. Man in the browser
E. Shadow IT
Answer: (SHOW ANSWER)

NEW QUESTION: 221

An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?
A. The IPS signatures
B. The endpoint configurations
C. The adversary behavior profiles
D. The baseline
Answer: C (LEAVE A REPLY)

NEW QUESTION: 222
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?
A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. SSO would reduce the resilience and availability of system if the provider goes offline.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 223
Accompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?
A. AES
B. WPS
C. WPA3
D. RADIUS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 224
A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?
A. BYOD
B. CYOD
C. VDI

D. COPE
Answer: A (LEAVE A REPLY)

NEW QUESTION: 225
A database administrator wants to grant access to an application that will be reading and writing data to a database. The database is shared by other applications also used by the finance department Which of the following account types Is MOST appropriate for this purpose?
A. eneric
B. Admin
C. Shared
D. Service
Answer: D (LEAVE A REPLY)

NEW QUESTION: 226
Which of the following in the incident response process is the BEST approach to improve the speed of the identification phase?
A. Increase the number of sensors present on the environment.
B. Redirect all events to multiple syslog servers.
C. Tune monitoring in order to reduce false positive rates.
D. Activate verbose logging in all critical assets.
Answer: (SHOW ANSWER)

NEW QUESTION: 227
A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?
A. Checksums
B. Watermarks
C. Oder of volatility
D. A log analysis
E. A right-to-audit clause
Answer: D (LEAVE A REPLY)

https://www.sumologic.com/glossary/log-analysis/
"While companies can operate private clouds, forensics in a public cloud are complicated by the right to audit permitted to you by your service level agreement (SLA) with the cloud provider."

NEW QUESTION: 228
A network engineer created two subnets that will be used for production and development servers. Per security policy, production and development servers must each have a dedicated network that cannot communicate with one another directly. Which of the following should be deployed so that server administrators can access these devices?
A. NIDS
B. VLANS
C. Jump servers
D. Internet proxy servers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 229
A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?
A. Normalization
B. Staging
C. Validation
D. Verification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 230
Which of the following secure coding techniques makes compromised code more difficult for hackers to use?
A. Obfuscation
B. Normalization
C. Execution
D. Reuse
Answer: (SHOW ANSWER)
https://en.wikipedia.org/wiki/Obfuscation_(software)

NEW QUESTION: 231
The Spread of misinformation sorrounding the outbreak of a novel on election day led to eligible voters choosing not take risk of going to the polls.
This is an example of:
A. An inflence campaign
B. Prepending

C. Information elicition
D. A watering-hole attack
E. Itimidation
Answer: E (LEAVE A REPLY)

NEW QUESTION: 232
Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically. Which of the following concepts does this BEST represent?
A. Functional testing
B. Continuous integration
C. Stored procedures
D. Elasticity
Answer: (SHOW ANSWER)

NEW QUESTION: 233
A user attempts to load a web-based application, but the expected login screen does not appear
A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user's PC
The help desk analyst then runs the same command on the local PC
Which of the following BEST describes the attack that is being detected?
A. Evil twin
B. DNS poisoning
C. Domain hijacking
D. MAC flooding
Answer: B (LEAVE A REPLY)

NEW QUESTION: 234
A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?
A. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
B. Configuring signature-based antivirus io update every 30 minutes
C. Implementing application execution in a sandbox for unknown software.
D. Fuzzing new files for vulnerabilities if they are not digitally signed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 235
A manufacturer creates designs for very high security products that are required to be protected and controlled
A. ARP poisoning

B. Bluejacking
C. Evil twin
D. Session replay
Answer: C (LEAVE A REPLY)

NEW QUESTION: 236
A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?
A. Enforcing encryption
B. Deploying GPOs
C. Removing administrative permissions
D. Applying MDM software
Answer: D (LEAVE A REPLY)
MDM stands for Mobile Device Management, is software that assists in the implementation of the process of managing, monitoring, and securing several mobile devices such as tablets, smartphones, and laptops used in the organization to access the corporate information.

NEW QUESTION: 237
Which of the following documents provides guidance regarding the recommended deployment of network security systems from the manufacturer?
A. CIS Top 20
B. Reference architecture
C. NIST RMF
D. Cloud control matrix
Answer: C (LEAVE A REPLY)

NEW QUESTION: 238
While investigating a recent security incident, a security analyst decides to view all network connections on a particular server, Which of the following would provide the desired information?
A. netstat
B. nmap
C. nslookup
D. arp
Answer: A (LEAVE A REPLY)

NEW QUESTION: 239
The SIEM at an organization has detected suspicious traffic coming a workstation in its internal network. An analyst in the SOC the workstation and discovers malware that is associated with a botnet is installed on the device A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The CIRT
B. The NOC team
C. The read team
D. The vulnerability management team
Answer: A (LEAVE A REPLY)

NEW QUESTION: 240
A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal dat a. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?
A. Configure MDM for FDE without enabling the lock screen.
B. Configure the MDM software to enforce the use of PINs to access the phone.
C. Enable the remote-wiping option in the MDM software in case the phone is stolen.
D. Perform a factory reset on the phone before installing the company's applications.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 241
An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?
A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
B. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
C. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.
D. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 242

A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST these requirement?

A. CRL

B. RA

C. OCSP

D. CSR

Answer: A (LEAVE A REPLY)

NEW QUESTION: 243

Asecurity engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses Which of the following will the engineer MOST likely recommend?

A. Anext-generation firewall

B. AWAF

C. An IDS

D. Acontent filter

Answer: (SHOW ANSWER)

NEW QUESTION: 244

A security Daalyst is taking part in an evaluation process that analyzes and categorizes threat actors of real-world events in order to improve the incident response team's process.
Which of the following is the analyst MOST likely participating in?

A. Red team

B. TAXII

C. Purple team

D. MITRE ATT&CK

B Walk-through

Answer: A (LEAVE A REPLY)

NEW QUESTION: 245

Which of the following BEST describes when an organization utilizes a ready-to-use application from a cloud provider?

A. laaS

B. SaaS

C. Paas

D. XaaS

Answer: B (LEAVE A REPLY)

SaaS, or software as a service, is on-demand access to ready-to-use, cloud-hosted application software.
https://www.ibm.com/cloud/learn/iaas-paas-saas

NEW QUESTION: 246
An engineer is setting up a VDI environment for a factory tocation, and the business wants to deploy a low-cost solution to enadle users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?
A. Workstations
B. Laptops
C. Thin clients
D. Containers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 247
An attacker replaces a digitally signed document with another version that goes unnoticed Upon reviewing the document's contents the author notices some additional verbiage that was not originally in the document but cannot validate an integrity issue. Which of the following attacks was used?
A. Cryptomalware
B. Hash substitution
C. Collision
D. Phishing
Answer: B (LEAVE A REPLY)
This type of attack occurs when an attacker replaces a digitally signed document with another version that has a different hash value. The author would be able to notice the additional verbiage, however, since the hash value would have changed, they would not be able to validate an integrity issue.

NEW QUESTION: 248
Which of the following is a risk that is specifically associated with hosting applications in the public cloud?
A. Zero-day
B. Unsecured root accounts
C. Insider threat
D. Shared tenancy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 249
The website http://companywebsite.com requires users to provide personal information including security responses, for registration. which of the following would MOST likely cause a date breach?
A. UNSCECURE PROTOCOL
B. OPEN PERMISSIONS

C. LACK OF INPUT VALIDATION
D. MISSING PATCHES
Answer: (SHOW ANSWER)

NEW QUESTION: 250
A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned tf servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).
A. 139
B. 143
C. 161
D. 443
E. 445
F. 135
Answer: D,F (LEAVE A REPLY)

NEW QUESTION: 251
Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)
A. Private key
B. Hashing
C. Salting
D. Perfect forward secrecy
E. Block cipher
F. Symmetric keys
Answer: (SHOW ANSWER)

NEW QUESTION: 252
Which of the following is a reason why an organization would define an AUP?
A. To define the set of rules and behaviors for users of the organization's IT systems
B. To define the intended partnership between two organizations
C. To define the availability and reliability characteristics between an IT provider and consumer
D. To define the lowest level of privileges needed for access and use of the organization's resources
Answer: D (LEAVE A REPLY)

NEW QUESTION: 253
Given the following logs:

Which of the following BEST describes the type of attack that is occurring?
A. Rainbow table
B. Dictionary
C. Password spraying
D. Pass-the-hash
Answer: C (LEAVE A REPLY)

NEW QUESTION: 254
After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices. Which of the following will achieve the administrator's goal? (Select TWO).
A. Disabling service accounts
B. Storing LAN manager hash values
C. Enabling NTLM
D. Enabling network sharing
E. Disabling NetBIOS over TCP/IP
F. Disabling guest accounts
Answer: E,F (LEAVE A REPLY)

NEW QUESTION: 255
An organization has implemented a two-step verification process to protect user access to data that s stored in the coud Ic scssnncsitcibin a vdiemiietanebins code to access the dat a. Which of the following authentication methods did the organization implement?
A. Token key
B. B Static code
C. Push notification
Answer: A (LEAVE A REPLY)
'D. HOTP

NEW QUESTION: 256
A Chief Executive Officer (CEO) is dissatisfied with the level of service from the company's new service provider. The service provider is preventing the CEO from sending email from a work account to a personal account. Which of the following types of service providers is being used?
A. Master managed service provider
B. Cloud service provider
C. Telecommunications service provider
D. Managed security service provider
Answer: B (LEAVE A REPLY)

NEW QUESTION: 257
Whiich of the following Gieuster recovery tests ie the LEAST time coneuntng for tie easier recovery tearm?
A. Tabletop
B. Parallel
C. Simulation
D. Full interruption
Answer: (SHOW ANSWER)

NEW QUESTION: 258
Atocompany wants to modify its current backup strategy to modity its current backup strategy to minenize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy
A. Full backup followed by different backups
B. Full backups followed by incremental backups
C. Incremental backups followed by delta backups
D. Incremental backups followed by differential backups
E. Delta backups followed by differental backups
Answer: D (LEAVE A REPLY)

NEW QUESTION: 259
Which of the following control Types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?
A. Recovery
B. Deterrent
C. Corrective
D. Detective
Answer: C (LEAVE A REPLY)
Corrective controls are implemented after detective controls to rectify the problem and (ideally) prevent it from happening again.

NEW QUESTION: 260
A symmetric encryption algorithm Is BEST suited for:

A. implementing non-repudiation.
B. providing hashing capabilities,
C. protecting large amounts of data.
D. key-exchange scalability.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 261
To mitigate the impact of a single VM being compromised by another VM on the same hypervisor, an administrator would like to utilize a technical control to further segregate the traffic. Which of the following solutions would BEST accomplish this objective?
A. Install a hypervisor firewall to filter east-west traffic.
B. Implement a zero-trust policy and physically segregate the hypervisor servers.
C. Move exposed or vulnerable VMs to the DMZ.
D. Add more VLANs to the hypervisor network switches.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 262
A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?
A. Compensating
B. Detective
C. Physical
D. Preventive
Answer: (SHOW ANSWER)

NEW QUESTION: 263
An information security policy states that separation of duties is required for all highly sensitive database changes that involve customers' financial dat a. Which of the following will this be BEST to prevent?
A. An insider threat
B. Least privilege
C. Adata breach
D. A change control violation
Answer: (SHOW ANSWER)

NEW QUESTION: 264
The human resources department of a large online retailer has received multiple customer complaints about the rudeness of the automated chatbots it uses to interface and assist online shoppers. The system, which continuously learns and adapts, was working fine when it was

installed a few months ago. Which of the following BEST describes the method being used to exploit the system?
A. Cryptographic manipulation
B. Baseline modification
C. A fileless virus
D. Tainted training data
Answer: D (LEAVE A REPLY)

NEW QUESTION: 265
A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?
A. Security
B. Application
C. Dump
D. Syslog
Answer: C (LEAVE A REPLY)
Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated by Windows or by the apps that crash, but you can also manually generate them https://www.digitalcitizen.life/view-contents-dump-file/

NEW QUESTION: 266
An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the incident could have been prevented?
A. The correlation of events
B. The baseline report
C. The security logs
D. The vulnerability scan output
Answer: D (LEAVE A REPLY)

NEW QUESTION: 267
A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab. The researchers collaborate with other machines using port 445 and on the Internet using port 443. The unauthorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMB. The security team has been instructed to resolve the problem as quickly as possible causing minimal disruption to the researchers. Which of the following contains the BEST course of action in this scenario?
A. Update the host firewalls to block outbound SMB.

B. Implement a content filter to block the unauthorized software communication.
C. Place the unauthorized application in a blocklist.
D. Place the machines with the unapproved software in containment.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 268
A security analyst is hardening a network infrastructure. The analyst is given the following requirements:
* Preserve the use of public IP addresses assigned to equipment on the core router.
* Enable "in transport" encryption protection to the web server with the strongest ciphers.
Which of the following should the analyst implement to meet these requirements? (Select TWO).
A. Configure NAT on the core router.
B. Enable 3DES encryption on the web server.
C. Enable TLSv2 encryption on the web server.
D. Configure VLANs on the core router.
E. Enable AES encryption on the web server.
F. Configure BGP on the core router.
Answer: (SHOW ANSWER)

NEW QUESTION: 269
Business partners are working on a secunty mechanism lo validate transactions securely. The requirement is for one company to be responsible for deploying a trusted solution that will register and issue artifacts used to sign encrypt, and decrypt transaction files. Which of the following is the BEST solution to adopt?
A. SAML
B. OAuth
C. PKI
D. Blockchain
Answer: C (LEAVE A REPLY)

NEW QUESTION: 270
Which of the following is a reason to publish files' hashes?
A. To use the hash as a software activation key
B. To verify if the software was digitally signed
C. To validate the integrity of the files
D. To use the hash as a decryption passphrase
Answer: (SHOW ANSWER)

NEW QUESTION: 271
A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an Item, the password for the wireless network is printed on the recent so the

customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?
A. WEP-TKIP
B. WPA-EAP
C. WPA-PSK
D. WPS-PIN
Answer: (SHOW ANSWER)

NEW QUESTION: 272
After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?
A. An error in the correlation rules triggered multiple alerts.
B. Multiple alerts were generated due to an attack occurring at the same time.
C. The unexpected traffic correlated against multiple rules, generating multiple alerts.
D. The SIEM was unable to correlate the rules, triggering the alerts.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 273
hich of the following is the BEST method for ensuring non-repudiation?
A. SSO
B. Token
C. SSH key
D. Digital certificate
Answer: D (LEAVE A REPLY)

NEW QUESTION: 274
A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?
A. Security patches were uninstalled due to user impact.

B. An adversary altered the vulnerability scan reports
C. A zero-day vulnerability was used to exploit the web server
D. The scan reported a false negative for the vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 275
An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device. Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?
A. Jamming
B. Evil twin
C. Rogue access point
D. Bluesnarfing
Answer: (SHOW ANSWER)

NEW QUESTION: 276
An IT security manager requests a report on company information that is publicly available. The manager's concern is that malicious actors will be able to access the data without engaging in active reconnaissance. Which of the following is the MOST efficient approach to perform the analysis?
A. Check public DNS entries using dnsenum.
B. Provide a domain parameter to tool.
C. Perform a vulnerability scan targeting a public company's IR
D. Execute nmap using the options: scan all ports and sneaky mode.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 277
A company is auditing the manner in which its European customers' personal information is handled Which of the following should the company consult?
A. GDPR
B. ISO
C. PCI DSS
D. NIST
Answer: A (LEAVE A REPLY)

NEW QUESTION: 278
To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials.
Which of the following will BEST ensure the site's users are not compromised after the reset?
A. A geofencing policy based on login history
B. A password reuse policy

C. Encrypted credentials in transit
D. Account lockout after three failed attempts
Answer: C (LEAVE A REPLY)

NEW QUESTION: 279
During a recent incident an external attacker was able to exploit an SMB vulnerability over the internet. Which of the following action items should a security analyst perform FIRST to prevent this from occurring again?
A. Check for any recent SMB CVEs
B. Deploy a NIDS in the affected subnet
C. Install AV on the affected server
D. Block unneeded TCP 445 connections
Answer: D (LEAVE A REPLY)

NEW QUESTION: 280
You received the output of a recent vulnerability assessment.
Review the assessment and scan output and determine the appropriate remedialion(s} 'or ach dewce.
Remediation options may be selected multiple times, and some devices may require more than one remediation.
If at any time you would like to biing bade the initial state ot the simulation, please dick me Reset All button.
Answer:

NEW QUESTION: 281
wo organizations are discussing a possible merger, Both organizations' Chief Financial Officers would like to safely share payroll data with each other to determine if the pay scales for different roles are similar at both organizations. Which of the following techniques would be BEST to protect employee data while allowing the companies to successfully share this information?
A. Tokenization
B. Encryption
C. Data masking
D. Pseudo-anonymization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 282
A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has 100 databases that are on premises. Which of the following solutions will require the LEAST management and support from the company?
A. SaaS
B. IaaS

C. PaaS
D. SDN
Answer: A (LEAVE A REPLY)
In order from the least amount of management, to the most amount of management for the company:
SaaS > PaaS > IaaS > On-site
SaaS - Basically everything is managed by the provider
PaaS - The provider manages everything other than applications and data IaaS - The middle-ground of services. The provider takes on half, while you take on the other half. Provider is responsible for virtualization, networking, servers, and storage. The company is responsible for applications, data, runtime, OS, and middleware.
On-site - There is no service provider. The company is responsible for the whole pie.
https://www.pcmag.com/picks/the-best-database-as-a-service-solutions

NEW QUESTION: 283
A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?
A. Physical security training
B. Baste awareness training
C. A capture-the-flag competition
D. A phishing simulation
Answer: (SHOW ANSWER)

NEW QUESTION: 284
An organization implemented a process that compares the settings currently configured on systems against secure configuration guidelines in order to identify any gaps Which of the following control types has the organization implemented?
A. Compensating
B. Corrective
C. Preventive
D. Detective
Answer: (SHOW ANSWER)
the control acts to eliminate or reduce the likelihood that an attack can succeed. A preventative control operates before an attack can take place. Compensating means to substitute one control with another (not happened here), Corrective means the attack has already happened (no mentioning), and detective is incorrect because the detective control detects ATTACKS, not vulnerabilities.

NEW QUESTION: 285

A scurity analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:
* Ensure mobile devices can be tracked and wiped.
* Confirm mobile devices are encrypted.
Which of the following should the analyst enable on all the devices to meet these requirements?
A. Geotagging
B. Biometric authentication
C. A Geofencing
D. Geolocation
Answer: (SHOW ANSWER)

NEW QUESTION: 286
A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?
A. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
B. It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
C. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach
D. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
Answer: D (LEAVE A REPLY)

NEW QUESTION: 287
A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)
A. Reverse proxy
B. Active Directory
C. DNSSEC
D. VPN concentrator
E. RADIUS

F. PKI
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 288
Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)
A. Alarms
B. Signage
C. Lighting
D. Access control vestibules
E. Fencing
F. Sensors
Answer: D,E (LEAVE A REPLY)
Alarms=deterrent, Signage=deterrent, Lighting=deterrent, Mantraps=physical countermeasure, Fencing=physical countermeasure and Sensors are either reactive or technical.
https://www.professormesser.com/security-plus/sy0-501/physical-security-controls-2/

NEW QUESTION: 289
A user's account is constantly being locked out. Upon further review, @ security analyst found the following in the SIEM:
Which of the following describes what is occurring?
A. An attacker is utilizing a dictionary attack against the account
B. An attacker is utilizing a rainbow table attack against the account
C. An attacker is utilizing a brute-force attack against the account
D. An attacker is utilizing a password-spraying attack against the account
Answer: (SHOW ANSWER)

NEW QUESTION: 290
An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained Which of the following roles would MOST likely include these responsibilities?
A. Data protection officer
B. Data owner
C. Backup administrator
D. Data custodian
E. Internal auditor
Answer: (SHOW ANSWER)
The role that would most likely include the responsibilities of implementing technical controls to protect data and ensuring backups are properly maintained would be a Backup Administrator. A Backup Administrator is responsible for maintaining and managing an organization's backup systems and procedures, which includes ensuring that backups are properly configured, tested

and securely stored. They are also responsible for the recovery of data in case of a disaster or data loss.

NEW QUESTION: 291
A Chief Security Officer (CSO) is concerned about the volume and integrity of sensitive information that is exchanged between the organization and a third party through email. The CSO is particularly concerned about an unauthorized party who is intercepting information that is in transit between the two organizations. Which of the following would address the CSO's concerns?
A. SPF
B. TLS
C. DMARC
D. DKIM
E. SSL
Answer: B (LEAVE A REPLY)

NEW QUESTION: 292
A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?
A. Discretionary
B. Rule-based
C. Mandatory
D. Role-based
Answer: C (LEAVE A REPLY)

NEW QUESTION: 293
In which of the following common use cases would steganography be employed?
A. Obfuscation
B. Blockchain
C. Non-repudiation
D. Integrity
Answer: A (LEAVE A REPLY)

NEW QUESTION: 294
A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?
A. The ICS firmware was outdated
B. A local machine has a RAT installed.
C. The HVAC was connected to the maintenance vendor.
D. A malicious USB was introduced by an unsuspecting employee.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 295
A security auditor is reviewing vulnerability scan data provided by an internal security team.
Which of the following BEST indicates that valid credentials were used?
A. The scan identified expired SSL certificates
B. The scan enumerated software versions of installed programs
C. The scan results show open ports, protocols, and services exposed on the target host
D. The scan produced a list of vulnerabilities on the target host
Answer: (SHOW ANSWER)

NEW QUESTION: 296
A security analyst is reviewing web-application logs and finds the following log:
Which of the following attacks is being observed?
A. XSS
B. On-path attack
C. Directory traversal
D. CSRF
Answer: C (LEAVE A REPLY)

NEW QUESTION: 297
A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?
A. An incident response plan
B. A communications plan
C. A disaster recovery plan
D. A business continuity plan
Answer: D (LEAVE A REPLY)
Business continuity may be defined as "the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident",[1] and business continuity planning [2][3] (or business continuity and resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to a company.[4] In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery.[5] Business continuity is the intended outcome of proper execution of both business continuity planning and disaster recovery.

NEW QUESTION: 298
A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfilltrated. The report also indicates that users tend to choose the same

credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfilltrated credentials?

A. Lockout

B. MFA

C. Password history

D. Time-based logins

Answer: A (LEAVE A REPLY)

NEW QUESTION: 299

A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

A. Plug the storage device in to the UPS

B. Change the default settings on the PC.

C. Encrypt the disk on the storage device.

D. Define the PC firewall rules to limit access.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 300

A company recently expenenced an attack dunng which #5 main website was directed to the atacker's web server, allowing the attacker to harvest credentials from unsuspecting customers. Vhich of the following snould the company Implement to prevent this type of attack from accurting in the future?

A. DNSSEC

B. IPSec

C. S/MIME

D. SSL/TLS

Answer: (SHOW ANSWER)

NEW QUESTION: 301

Which of the following describes the continuous delivery software development methodology?

A. V-shaped

B. Agile

C. Spiral

D. Waterfall

Answer: B (LEAVE A REPLY)

NEW QUESTION: 302
Multiple business accounts were compromised a few days after a public website had its credentials database leaked on the internet No business emails were Identified in the breach, but the security team thinks that the list of passwords exposed was later used to compromise business accounls Which of Ihe following would mitigate the issue?
A. Password history
B. Shared accounts
C. Acceptable use policy
D. Complexity requirements
Answer: C (LEAVE A REPLY)

NEW QUESTION: 303
The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schem a. The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs Which of the following is the BEST solution to meet the requirement?
A. Tokenization
B. Mirroring
C. Full disk encryption
D. Masking
Answer: D (LEAVE A REPLY)

NEW QUESTION: 304
A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet, While reviewing logs and tool output, the analyst sees the following:
Which of the following attacks has occurred?
A. IP conflict
B. Pass-the-hash
C. MAC flooding
D. Directory traversal
E. ARP poisoning
Answer: E (LEAVE A REPLY)
https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning

NEW QUESTION: 305
Which of the fofowing should an organization conskier implementing in the event executives need to speak to the media after a publicized data breach?
A. Business continuity plan
B. Disaster recovery plan
C. incident response pian
D. Communication pian
Answer: D (LEAVE A REPLY)

NEW QUESTION: 306
A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan Types would produce the BEST vulnerability scan report?
A. Credentialed
B. Port
C. Host discovery
D. Intrusive
Answer: A (LEAVE A REPLY)

NEW QUESTION: 307
Developers are writing code and merging it into shared repositones several times a day, where it is tested automabecally. Which of the following concepts does this BEST represent?
A. Functional testing
B. Stored procedures
C. Continuous integration
D. Elasticity
Answer: (SHOW ANSWER)

NEW QUESTION: 308
An organization's finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).
A. Preventive
B. Deterrent
C. Separation of duties
D. Mandatory vacations
E. Corrective
F. Job rotation
Answer: D,F (LEAVE A REPLY)

NEW QUESTION: 309

An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan, the analyst identifies that a server has sont insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE).

A. POP, IMAP
B. TEIP, FIP
C. SNMPv1, SNMPv2
D. SNMPv2, SNMPv3
E. HTTP, HTTPS
F. SFTP, FTPS
G. Telnet, SSH
H. TLS, SSL
I. Login, rlogin
Answer: C,F,H (LEAVE A REPLY)

NEW QUESTION: 310
Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report
B. Arisk register
C. A business impact analysis
D. An asset value register
Answer: B (LEAVE A REPLY)
E: A disaster recovery plan

NEW QUESTION: 311
Which of the following is the correct order of volatility from MOST to LEAST volatile? >

A. Memory, disk, temporary filesystems, cache, archival media
B. Cache, memory, temporary filesystems, disk, archival media
C. Cache, disk, temporary filesystems, network storage, archival media
D. Memory, temporary filesystems, routing tables, disk, network storage
Answer: B (LEAVE A REPLY)

NEW QUESTION: 312
After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:

A. privilege escalation
B. footprinting

C. pivoting.
D. persistence
Answer: A (LEAVE A REPLY)

NEW QUESTION: 313
Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?
A. Blue team
B. Green team
C. Red team
D. Purple team
E. White team
Answer: A (LEAVE A REPLY)

NEW QUESTION: 314
While preparing a software Inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. Which of the following mitigations would BEST secure the server environment?
A. Revoke the code signing certificate used by both programs.
B. Block all unapproved file hashes from installation.
C. Update the code signing certificate for the approved application.
D. Add the accounting application file hash to the allowed list.
Answer: (SHOW ANSWER)

NEW QUESTION: 315
A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?
A. Implementing a group policy to block user access to system files
B. Blocking removable-media devices and write capabilities using a host-based security tool
C. Developing mandatory training to educate employees about the removable media policy
D. Monitoring large data transfer transactions in the firewall logs
Answer: (SHOW ANSWER)

NEW QUESTION: 316
A company ts required to continue using legacy softveare to support a critical serwce. Whech of the folowing BEST explans a reek of this prachce?
A. Weak encryption
B. Unsecure protocols
C. Default system configuraton

D. Lack of vendor support
Answer: B (LEAVE A REPLY)

NEW QUESTION: 317
An application developer accidentally uploaded a company's code-signing certificate private key to a public web server. The company is concerned about malicious use of its certificate. Which of the following should the company do FIRST?
A. Delete the private key from the repository.
B. Verify the public key is not exposed as well.
C. Update the DLP solution to check for private keys.
D. Revoke the code-signing certificate.
Answer: A (LEAVE A REPLY)
We need to revoke the code-signing certificate as this is the most secure way to ensure that the comprised key wont be used by attackers. Usually there are bots crawking all over repos searching this kind of human errors.

NEW QUESTION: 318
A security analyst reviews a company's authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?
A. Rainbow table
B. Spraying
C. Brute-force
D. Dictionary
Answer: C (LEAVE A REPLY)

NEW QUESTION: 319
A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?
A. Log aggregation
B. Log enrichment

C. Log parser
D. Log collector
Answer: D (LEAVE A REPLY)

NEW QUESTION: 320
Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?
A. Footprinting
B. A drone/UAV
C. Pivoting
D. White-box testing
Answer: (SHOW ANSWER)

NEW QUESTION: 321
An information security manager for an organization is completing a PCI DSS self-assessment for the first time. which of the is following MOST likely reason for this type of assessment?
A. The organization is expecting to process credit card information.
B. Outside consultants utilize this tool to measure security maturity.
C. An international expansion project is currently underway.
D. A government regulator has requested this audit to be completed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 322
A securily analysl has receved several reporls of an issue on an inlemal web application. Users state they are having to provide their credentials brice to log in. The analyst checks with he application team and noles Unis is not an expected bohavier. After looking at several lags, the analysi deciies to in some commands on the gateway and obtains the following output:
Which of the following BEST describes the attack the company is experiencing?
A. ARP paisoning
B. MAC fleoding
C. URL redirection
D. DNS hijacking
Answer: A (LEAVE A REPLY)

NEW QUESTION: 323
The help desk has received calls from users in multiple locations who are unable to access core network services The network team has identified and turned off the network switches using remote commands. Which of the following actions should the network team take NEXT?
A. Turn on all the network switches by using the centralized management software
B. Send response teams to the network switch locations to perform updates
C. Disconnect all external network connections from the firewall

D. Initiate the organization's incident response plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 324
A security administrator is trying to determine whether a server is vulnerable to a range of attacks. After using a tool, the administrator obtains the following output:
Which of the following attacks was successfully implemented based on the output?
A. SQL injection
B. Race conditions
C. Memory leak
D. Directory traversal
Answer: (SHOW ANSWER)

NEW QUESTION: 325
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?
A. Firewall whitelisting
B. isolation
C. Segmentation
D. Containment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 326
Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).
A. Acceptable use
B. Job rotation
C. Background checks
D. Offboarding
E. Separation of duties
F. Mandatory vacation
Answer: B,F (LEAVE A REPLY)

NEW QUESTION: 327
Which of the following tools is effective in preventing a user from accessing unauthorized removable media?
A. Cable lock
B. USB data blocker

C. Faraday cage
D. Proximity reader
Answer: C (LEAVE A REPLY)

NEW QUESTION: 328
A systems administrator is looking for a solution that will help prevent OAuth applications from being leveraged by hackers to tick users into authonzing the use of their corporate credentials. Which of the following BEST describes this solution?
A. WAF
B. VPC
C. UEM
D. CASB
Answer: C (LEAVE A REPLY)

NEW QUESTION: 329
A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this talk?
A. Nessus
B. Netcat
C. Nmap
D. Netstat
Answer: (SHOW ANSWER)

NEW QUESTION: 330
A compart jut heplmanieg 6 new tlewor ploy thet owe eriptoyens f wee personel doce or ocala and fe aherag wo wong tow howe. Some of ie
* Employees must provide an alternate work location (i.e., a home address)
* Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.
Which of the following BEST describes the MDM options the company is using?
A. Geofencing, content management, remote wipe, containerization, and storage segmentation
B. Application management, remote wipe, geofencing, context-aware authentication, and containerization
C. Content management, remote wipe, geolocation, context-aware authentication, and containerization
D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption
Answer: D (LEAVE A REPLY)

NEW QUESTION: 331

A workwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

A. Impossible travel time

B. Network location

C. Geolocation

D. Geofencing

Answer: (SHOW ANSWER)

NEW QUESTION: 332

An engineer wants to inspect traffic to a cluster of web servers in a cloud environment. Which of the following solutions should the engineer implement?

A. VPN

B. Load balancer

C. Proxy server

D. WAF

Answer: (SHOW ANSWER)

NEW QUESTION: 333

An amusement park is implementing a btomelnc system that validates customers' fingerpnnts to ensure they are not sharing tickets The park's owner values customers above all and would prefer customers' convenience over security For this reason which of the following features should the security team prioritize FIRST?

A. Low FAR

B. Low efficacy

C. Low FRR

D. Low CER

Answer: C (LEAVE A REPLY)

FAR (False Acceptance Rate)

FRR (False Rejection Rate)

CER (Crossover Error Rate) AKA ERR (Equal Error Rate)

since he is willing to sacrifice Security for Customer Service, Best way to understand this is.
FAR has to go up in order for FRR to go down.
typical business practice is in the middle of both which would be near the CER.

NEW QUESTION: 334
An organization is repairing the damage after an incident, Which of the following controls es being implemented?
A. Preventive
B. Detective
C. Corrective
D. Compensating
Answer: (SHOW ANSWER)

NEW QUESTION: 335
An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?
A. SLA
B. BPA
C. MOU
D. NDA
Answer: (SHOW ANSWER)

NEW QUESTION: 336
A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement Which of the following tools if available on the server, will provide the MOST useful information for the next assessment step?
A. Autopsy
B. Cuckoo
C. Memdump
D. Nmap
Answer: D (LEAVE A REPLY)
Nmap is basically mapping a network. The purpose of lateral pivoting is to gain a new perspective, or new information that will allow you to either privilege escalate, or to achieve the goal of the attack. If the compromised server the pen tester is exploiting has nmap enabled, the pen tester will be able to get an in-depth inside view of the internal network structure.

NEW QUESTION: 337
A large bank with two geographically dispersed data centers is concerned about major power disruptions at both locations Every day each location expenences very bnef outages that last for a few seconds However dunng the summer a high risk of intentional brownouts that last up to an

hour exists particularly at one of the locations near an jndustnal smelter. Which of the following is the BEST solution to reduce the risk of data loss?

A. Generator

B. Dual supply

C. Daily backups

D. PDU

Answer: A (LEAVE A REPLY)

NEW QUESTION: 338

Which of the following is the purpose of a risk register?

A. To formally log the type of risk mitigation strategy the organization is using

B. To define the level or risk using probability and likelihood

C. To identify the risk, the risk owner, and the risk measures

D. To register the risk with the required regulatory agencies

Answer: C (LEAVE A REPLY)

NEW QUESTION: 339

Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

A. The data owner

B. The data processor

C. The data steward

D. The data privacy officer.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 340

The SOC for a large MSSP is meeting to discuss the lessons learned from a recent incident that took much too long to resolve This type of incident has become more common in recent weeks and is consuming large amounts of the analysts' time due to manual tasks being performed Which of the following solutions should the SOC consider to BEST improve its response time?

A. Configure a NIDS appliance using a Switched Port Analyzer

B. Collect OSINT and catalog the artifacts in a central repository

C. Implement a SOAR with customizable playbooks

D. Install a SIEM with community-driven threat intelligence

Answer: C (LEAVE A REPLY)

SOAR (Security Orchestration, Automation, and Response) Can use either playbook or runbook. It assists in collecting threat related data from a range of sources and automate responses to low level threats. (frees up some of the CSIRT time)

NEW QUESTION: 341

A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?
A. Phishing
B. Vishing
C. Spear phishing
D. Whaling
Answer: B (LEAVE A REPLY)

NEW QUESTION: 342
An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:
* Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
* Internal users in question were changing their passwords frequently during that time period.
* A jump box that several domain administrator users use to connect to remote devices was recently compromised.
* The authentication method used in the environment is NTLM.
Which of the following types of attacks is MOST likely being used to gain unauthorized access?
A. Pass-the-hash
B. Directory traversal
C. Replay
D. Brute-force
Answer: A (LEAVE A REPLY)

NEW QUESTION: 343
A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?
A. PCI DSS
B. GDPR
C. NIST
D. ISO 31000
Answer: B (LEAVE A REPLY)

NEW QUESTION: 344
The concept of connecting a user account across the systems of multiple enterprises is BEST known as:
A. a remote access policy.
B. single sign-on.
C. multifactor authentication.
D. federation.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 345
Users are presented with a banner upon each login to a workstation. The banner mentions that users are not entitled to any reasonable expectation of privacy and access is for authorized personnel only.
In order to proceed past that banner. users must click the OK button. Which of the following is this an example of?
A. MOU
B. NDA
C. AUP
D. SLA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 346
Which of the following authentication methods is considered to be the LEAST secure?
A. TOTP
B. Token key
C. HOTP
D. SMS
Answer: (SHOW ANSWER)

NEW QUESTION: 347
A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?
A. Implement open PSK on the APs
B. Configure WIPS on the APs
C. Deploy a WAF
D. Install a captive portal
Answer: D (LEAVE A REPLY)

NEW QUESTION: 348
Whictpof the following will MOST likely cause machine-learning and AI-enabled systems to operate with unintended consequences?
A. Buffer overflows
B. Code reuse
C. Stored procedures
D. Data bias
Answer: (SHOW ANSWER)

NEW QUESTION: 349
A technician was dispatched to complete repairs on a server in a data center. While locating the server, the technician entered a restricted area without authorization. Which of the following security controls would BEST prevent this in the future?
A. Enforce escorts to monitor all visitors.
B. Use appropriate signage to mark all areas.
C. Utilize cameras monitored by guards.
D. Implement access control vestibules.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 350
A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:
http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us
The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:
http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us
Which of the following application attacks is being tested?
A. Pass-the-hash
B. Session replay
C. Cross-site request forgery
D. Object deference
Answer: B (LEAVE A REPLY)

NEW QUESTION: 351
Which of the following refers to applications and systems that are used within an organization without consent or approval?
A. Dark web
B. Shadow IT
C. Insider threats
D. OSINT

Answer: B (LEAVE A REPLY)

NEW QUESTION: 352
A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?
A. Implementation of deterrent controls
B. Implementation of preventive controls
C. Implementation of detective controls
D. Implementation of corrective controls
Answer: C (LEAVE A REPLY)

NEW QUESTION: 353
Which of the following will increase cryptographic security?
A. Algorithms that require less computing power
B. Hashing
C. Longer key longevity
D. High data entropy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 354
Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics?
A. Production
B. Staging
C. Development
D. Test
Answer: D (LEAVE A REPLY)

NEW QUESTION: 355
A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:
Which ol the following types of attacks is being attempted and how can it be mitigated?
A. CSRF. implement an IPS
B. Directory traversal implement a WAF
C. SQL infection, mplement an IDS
D. XSS. mplement a SIEM
Answer: B (LEAVE A REPLY)

NEW QUESTION: 356

Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

A. SIEM

B. CASB

C. UTM

D. DLP

Answer: B (LEAVE A REPLY)

Microsoft has a straightforward definition and it includes DLP. "is a security policy enforcement point positioned between enterprise users and cloud service providers" https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb A cloud access security broker (CASB) works by securing data flowing to and from in-house IT architectures and cloud vendor environments using an organization's security policies. CASBs protect enterprise systems against cyberattacks through malware prevention and provide data security through encryption, making data streams unreadable to outside parties. CASBs were created with one thing in mind: protecting proprietary data stored in external, third-party media. CASBs deliver capabilities not generally available in traditional controls such as secure web gateways (SWGs) and enterprise firewalls. CASBs provide policy and governance concurrently across multiple cloud services and provide granular visibility into and control over user activities. https://www.forcepoint.com/cyber-edu/casb-cloud-access-security-broker

NEW QUESTION: 357

Which of the following environments minimizes end-user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?

A. Production

B. Test

C. Development

D. Staging

Answer: B (LEAVE A REPLY)

NEW QUESTION: 358

A Chief Information Security Officer wants to ensure the organization is validating and checking the Integrity of zone transfers. Which of the following solutions should be implemented?

A. NGFW

B. LOAPS

C. DLP

D. DNSSEC

Answer: C (LEAVE A REPLY)

NEW QUESTION: 359

The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?
A. Shadow IT
B. Hacktivism
C. White-hat
D. A script kiddie
Answer: A (LEAVE A REPLY)

NEW QUESTION: 360
A security analyst has identified malv/are spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT? A
A. Update all endpomt antivirus solutions with the latest updates
B. Create help desk tickets to get infected systems reimaged
C. Attempt to quarantine all infected hosts to limit further spread
D. Review how the malware was introduced to the network
Answer: (SHOW ANSWER)

NEW QUESTION: 361
Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?
A. Watering-hole attack
B. Credential harvesting
C. Pharming
D. Hybrid warfare
Answer: (SHOW ANSWER)

NEW QUESTION: 362
Accompany has a flat network that is deployed in the cloud. Security policy states that all production and development servers must be segmented. Which of the following should be used to design the network to meet the security requirements?

A. VPC
B. WAF
C. Perimeter network
D. CASB
Answer: (SHOW ANSWER)

NEW QUESTION: 363
A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?
A. Autopsy
B. Memdump
C. FTK imager
D. Wireshark
Answer: (SHOW ANSWER)
Some common applications that can open .pcap files are Wireshark, WinDump, tcpdump, Packet Square - Capedit and Ethereal.

NEW QUESTION: 364
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)
A. Unsecure protocols
B. Weak passwords
C. Outdated anti-malware software
D. Use of penetration-testing utilities
E. Included third-party libraries
F. Vendors/supply chain
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 365
Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities After further investigation, a security analyst notices the following
* All users share workstations throughout the day
* Endpoint protection was disabled on several workstations throughout the network.
* Travel times on logins from the affected users are impossible
* Sensitive data is being uploaded to external sites
* All usee account passwords were forced lo be reset and the issue continued Which of the following attacks is being used to compromise the user accounts?
A. Rainbow
B. Brute-force
C. Keylogger

D. Dictionary
Answer: (SHOW ANSWER)

NEW QUESTION: 366
A security administrator checks the table of a network switch, which shows the following output:
Which of the following is happening to this switch?
A. DNS poisoning
B. ARP poisoning
C. MAC cloning
D. MAC Flooding
Answer: D (LEAVE A REPLY)

NEW QUESTION: 367
A security team will be outsourcing several key functions to a third party and will require that:
* Several of the functions will carry an audit burden.
* Attestations will be performed several times a year.
* Reports will be generated on a monthly basis.
Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?
A. MOU
B. AUP
C. SLA
D. MSA
Answer: C (LEAVE A REPLY)
A service level agreement (SLA) is a contract between a service provider and a customer that outlines the services that are to be provided and the expected levels of performance. It is used to define the requirements for the service, including any attestations and reports that must be generated, and the timescales in which these must be completed. It also outlines any penalties for failing to meet these requirements. SLAs are essential for ensuring that third-party services are meeting the agreed upon performance levels.
Reference:
CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide by Darril Gibson
https://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-601/dp/1260117558 Note: SLA is the best document that is used to define these requirements and stipulate how and when they are performed by the third party.

NEW QUESTION: 368
A news article states that a popular web browser deployed on all corporate PCs is vulnerable to a zero-day attack. Which of the following MOST concerns the Chief Information Security Officer about the information in the news article?
A. No patches are available for the web browser.

B. Antivirus signatures are required to be updated immediately.
C. Web browsing is not functional for the entire network.
D. Insider threats have compromised this network.
Answer: (SHOW ANSWER)

NEW QUESTION: 369
In a phishing attack, the perpetrator is pretending to be someone in a position of power in an effort to influence the target to click or follow the desired response. Which of the following principles is being used?
A. Intimidation
B. Authority
C. Consensus
D. Scarcity
Answer: A (LEAVE A REPLY)

NEW QUESTION: 370
An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise. Which of the following will accomplish this goal?
A. IPS.
B. Antivirus
C. FIM
D. FTP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 371
A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?
A. Implement an MDM.
B. Implement a URL filter.
C. Implement an SWG.
D. Implement NAC.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 372
A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investiga-tion, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized

downloads are occurring. The analyst also discov-ers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

A. Evil twin

B. Jamming

C. DNS poisoning

D. DDoS

E. Bluesnarfing

Answer: (SHOW ANSWER)

NEW QUESTION: 373

A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?

A. POP3S is not supported

B. Secure IMAP was not implemented

C. The S/MME plug-in is not enabled.

D. The SLL certificate has expired.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 374

An attacker is exploiting a vulnerability that does not have a patch available. Which of the following is the attacker exploiting?

A. Unsecure root accounts

B. Default permissions

C. Zero-day

D. Weak encryption

Answer: C (LEAVE A REPLY)

NEW QUESTION: 375

During an incident a company CIRT determine it is necessary to observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Emulate the malware in a heavily monitored DM Z segment.

B. Physical move the PC to a separate internet pint of presence

C. Apply network blacklisting rules for the adversary domain

D. Create and apply microsegmantion rules.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 376

A secullly operations analyst is using the company's SIEM solufon to correlate alens. Which of the following stages of the Inciden reapanse process is this an example af?

A. Recowery

B. Eradication

C. identiticalion

D. Preparation

Answer: C (LEAVE A REPLY)

NEW QUESTION: 377

A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

A. A RAT

B. A worm

C. Ransomware

D. Polymophic

Answer: D (LEAVE A REPLY)

NEW QUESTION: 378

A Chief Security Officer (CSO) was notified that a customer was able to access confidential internal company files on a commonly used file-sharing service. The file-sharing service is the same one used by company staff as one of its approved third-party applications. After further investigation, the security team determines the sharing of confidential files was accidental and not malicious. However, the CSO wants to implement changes to minimize this type of incident from reoccurring but does not want to impact existing business processes. Which of the following would BEST meet the CSO's objectives?

A. DLP

B. SWG

C. CASB

D. Virtual network segmentation

Answer: A (LEAVE A REPLY)

E; Container security

NEW QUESTION: 379
A securtly analyst wants to reference a standard to develop a risk management program. Which af the following ts the BEST source for the analyst to use?
A. GDPR
B. SSAE SOC 2
C. SO 31000
D. NIST CSF
Answer: C (LEAVE A REPLY)

NEW QUESTION: 380
An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?
A. VDI
B. MDM
C. MAM
D. DLP
Answer: (SHOW ANSWER)

NEW QUESTION: 381
A security administrator Is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).
A. IPSec
B. SFTP
C. SRTP
D. LDAPS
E. S/MIME
F. SSL VPN
Answer: A,F (LEAVE A REPLY)
IPSec (Internet Protocol Security) is a technology that provides secure communication over the internet by encrypting traffic and authenticating it at both the sender and receiver. It can be used to create secure tunnels between two or more devices, allowing users to access resources securely and privately.
SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses an SSL/TLS connection to encrypt traffic between two or more devices. It is a secure and reliable solution for providing remote access, as all traffic is encrypted and authenticated. Additionally, SSL VPNs can also be used to restrict access to certain websites and services, making them a secure and robust solution for remote access.

NEW QUESTION: 382
A company wants to build a new website to sell products online. The website will host a storefront application that will allow visitors to add products to a shopping cart and pay for the products using a credit card. Which of the following protocols would be the MOST secure to implement?
A. SNMP
B. FTP
C. TLS
D. SSL
Answer: C (LEAVE A REPLY)

NEW QUESTION: 383
A user enters a password to log in to a workstation and is then prompted to enter an authentication code.
Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).
A. Somewhere you are
B. Something you are
C. Something you can do
D. Something you know
E. Someone you are
F. Something you have
Answer: B,F (LEAVE A REPLY)

NEW QUESTION: 384
A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?
A. Credential harvesting
B. Dumpster diving
C. Shoulder surfing
D. Information elicitation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 385
A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?
A. Unsecure protocols
B. Weak encryption
C. Lack of vendor support
D. Default system configuration
Answer: (SHOW ANSWER)

NEW QUESTION: 386
Local guidelines require that all information systems meet a minimum-security baseline to be compliant.
Which of the following can security administrators use to assess their system configurations against the baseline?
A. Risk management framework
B. Benchmarks
C. SOAR playbook
D. Security control matrix
Answer: B (LEAVE A REPLY)

NEW QUESTION: 387
Which of the following would a European company interested in implementing a technical, hands-on set of security standards MOST likely choose?
A. Is0 37000
B. CIS controls
C. . ISO 27001
D. GOPR
Answer: D (LEAVE A REPLY)

NEW QUESTION: 388
A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation, Which of the following would dispute the analyst's claim of innocence?
A. Order of volatility
B. Legal hold
C. Non-repudiation
D. Chain of custody
Answer: (SHOW ANSWER)

NEW QUESTION: 389
A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:
Which of the following is the router experiencing?
A. DDoS attack
B. Memory leak
C. Resource exhaustion
D. Buffer overflow
Answer: C (LEAVE A REPLY)

NEW QUESTION: 390
A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?
A. Full-disk encryption
B. Geofencing
C. Remote wipe
D. Containerization
Answer: A (LEAVE A REPLY)

NEW QUESTION: 391
A nationwide company is experiencing unauthorized logins at all hours of the day. The logins appear to originate from countries in which the company has no employees. Which of the following controls.
should the company consider using as part of its IAM strategy? (Select TWO).
A. A complex password policy
B. Geolocation
C. An impossible travel policy
D. Self-service password reset
E. Geofencing
Answer: (SHOW ANSWER)
F Time-based logins

NEW QUESTION: 392
A security analyst is evaluating solutions to deploy an additional layer of protection for a web application The goal is to allow only encrypted communications without relying on network devices Which of the following can be implemented?
A. DNSSEC implementation
B. SRTP
C. S/MIME
D. HTTP security header

Answer: B (LEAVE A REPLY)

NEW QUESTION: 393
A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?
A. False rejection
B. Cross-over error rate
C. Efficacy rale
D. Attestation
Answer: (SHOW ANSWER)
where a legitimate user is not recognized. This is also referred to as a Type I error or false non-match rate (FNMR). FRR is measured as a percentage.

NEW QUESTION: 394
After a recent external audit, the compliance team provided a list of several non-compliant, in-scope hosts that were not encrypting cardholder data at rest, Which of the following compliance frameworks would address the compliance team's GREATEST concern?
A. GDPR
B. NIST CSF
C. ISO 27001
D. PCI DSS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 395
A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:
Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?
A. ARP poisoning
B. Denial of service
C. Command injection
D. MAC flooding
Answer: D (LEAVE A REPLY)

NEW QUESTION: 396
A security architect is working on an email solution that will send sensitive dat a. However, funds are not currently available in the budget for building additional infrastructure. Which of the following should the architect choose?
A. POP

B. IPSec
C. IMAP
D. PGP
Answer: D (LEAVE A REPLY)
PGP (Pretty Good Privacy) is a commonly used encryption method for email communications to secure the sensitive data being sent. It allows for the encryption of the entire message or just the sensitive parts. It would be an appropriate solution in this case as it doesn't require additional infrastructure to implement.

NEW QUESTION: 397
Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?
A. GDPR
B. PCI DSS
C. NIST 800-53
D. ISO 27000
Answer: (SHOW ANSWER)

NEW QUESTION: 398
A company is moving its retail website to a public cloud provider. The company wants to tokenize credit card data but not allow the cloud provider to see the stored credit card information. Which of the following would BEST meet these objectives?
A. CASB
B. TLS
C. WAF
D. VPN
Answer: A (LEAVE A REPLY)

NEW QUESTION: 399
Which of the following holds staff accountable while escorting unathorized personal?
A. Badges
B. Visitor logs
C. Locks
D. Cameras
Answer: B (LEAVE A REPLY)

NEW QUESTION: 400
Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?
A. Data masking

B. Tokenization
C. Data encryption
D. Anonymization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 401
Which of the following involves the inclusion of code in the main codebase as soon as it is written?
A. Continuous deployment
B. Continuous Validation
C. Continuous integration
D. Continuous monitoring
Answer: C (LEAVE A REPLY)

NEW QUESTION: 402
An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:
A. MTBF
B. RPO
C. MTTR
D. RTO
Answer: (SHOW ANSWER)
https://www.enterprisestorageforum.com/management/rpo-and-rto-understanding-the-differences/

NEW QUESTION: 403
A new security engineer has started hardening systems. One o(the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability lo use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Which of the following is the MOST likely cause of this issue?
A. TFTP was disabled on the local hosts.
B. SSH was turned off instead of modifying the configuration file.
C. Remote login was disabled in the networkd.conf instead of using the sshd. conf.
D. Network services are no longer running on the NAS
Answer: (SHOW ANSWER)
SSH is used to securely transfer files to the remote server and is required for SCP to work. Disabling SSH will prevent users from being able to use SCP to transfer files to the server. To enable SSH, the security engineer should modify the SSH configuration file (sshd.conf) and make sure that SSH is enabled. For more information on hardening systems and the security

techniques that can be used, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION: 404
An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be BEST to use to update and reconfigure the OS-level security configurations?
A. CIS benchmarks
B. GDPR guidance
C. Regional regulations
D. ISO 27001 standards
Answer: A (LEAVE A REPLY)
https://www.beyondtrust.com/resources/glossary/systems-hardening

NEW QUESTION: 405
A company suspects that some corporate accounts were compromised. The number of suspicious logins from locations not recognized by the users is increasing Employees who travel need their accounts protected without the nsk of blocking legitimate login requests that may be made over new sign-in properties. Which of the following security controls can be implemented?
A. Shift the access control scheme to a discretionary access control
B. Enforce MFA when an account request reaches a nsk threshold
C. Enforce time-based login requests that align with business hours
D. Implement geofencing to only allow access from headquarters
Answer: (SHOW ANSWER)

NEW QUESTION: 406
A global pandemic is forcing a private organization to close some business units and reduce staffing at others.
Which of the following would be BEST to help the organization's executives determine the next course of action?
A. A disaster recovery plan
B. A business continuity plan
C. An incident response plan
D. A communications plan
Answer: (SHOW ANSWER)

NEW QUESTION: 407
An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?
A. Spear phishing
B. Whaling
C. Phishing
D. Vishing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 408
A cyber-security administrator is using an enterprise firewall. The administrator created some rules, but now Seems to be unresponsive. All connections being dropped by the firewall. Which of the following would be the BEST option to remove the rules?
A. # iptables -f
B. # iptables -z
C. # iptables -t mangle -x
D. # iptables -p input -j drop
Answer: C (LEAVE A REPLY)

NEW QUESTION: 409
A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two- drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?
A. 0
B. 6
C. 1
D. 5
Answer: C (LEAVE A REPLY)

NEW QUESTION: 410
A security architect is required to deploy to conference rooms some workstations that will allow sensitive data to be displayed on large screens. Due to the nature of the data, it cannot be stored in the conference rooms. The fiieshare is located in a local data center. Which of the following should the security architect recommend to BEST meet the requirement?
A. Private cloud and DLP
B. VDI and thin clients

C. Full drive encryption and thick clients
D. Fog computing and KVMs
Answer: (SHOW ANSWER)

NEW QUESTION: 411
A security manager runs Nessus scans of the network after every maintenance vandow Which of the following ts the securty manager MOST likely trying to accomplish?
A. identifying assets on the network that may not exist on the network asset inventory
B. Validating the hosts do not have vulnerable ports exposed to the Intemet
C. Checking the status of the automated malware analyses that is beang performed
D. A Verifying that system patching has effectively removed known vulnerabilities
Answer: D (LEAVE A REPLY)

NEW QUESTION: 412
A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?
A. MTTR
B. RPO
C. RTO
D. MTBF
Answer: C (LEAVE A REPLY)

NEW QUESTION: 413
A company needs to validate its updated incident response plan using a real-world scenario that will test decision points and relevant incident response actions without interrupting daily operations. Which of the following would BEST meet the company's requirements?
A. Red-team exercise
B. Phishing exercise
C. Tabletop exercise
D. Capture-the-flag exercise
Answer: (SHOW ANSWER)

NEW QUESTION: 414
An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?
A. HSM
B. TPM
C. DLP
D. CASB
Answer: A (LEAVE A REPLY)

NEW QUESTION: 415
An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of the following would be BEST to minimize this risk?
A. Log and alert on unusual scanner account logon times.
B. Use non-credentialed scans against high-risk servers.
C. Require a complex, eight-character password that is updated every 90 days.
D. Perform only non-intrusive scans of workstations.
Answer: (SHOW ANSWER)

NEW QUESTION: 416
A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?
A)
B)
C)
D)
A. Option A
B. Option C
C. Option B
D. Option D
Answer: (SHOW ANSWER)

NEW QUESTION: 417
A company is implementing MFA for all applications that store sensitive dat a. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?
A. Push notifications
B. One-time passwords
C. Hardware authentication
D. Email tokens
Answer: A (LEAVE A REPLY)

NEW QUESTION: 418
An ofgantzation has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk is greater than the five-year cost of the insurance policy. The organization is enabling risk
A. mitigation
B. transference

C. avoidance
D. acceptance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 419
The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?
A. Type squatting
B. Pharming
C. Phishing
D. Whaling
Answer: D (LEAVE A REPLY)

NEW QUESTION: 420
A RAT that was used to compromise an organization's banking credentials was found on a user's computer.
The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?
A. Enforce application whitelisting.
B. Implement DLP at the network boundary
C. Segment the network into trusted and untrusted zones.
D. Create a new acceptable use policy.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 421
A security researcher is using an adversary's infrastructure and TTPs and creating a named group to track those targeted Which of the following is the researcher MOST likely using?
A. The Cyber Kill Chain
B. The Diamond Model of Intrusion Analysis
C. The incident response process
D. MITRE ATT&CK
Answer: B (LEAVE A REPLY)

NEW QUESTION: 422
A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?
A. Retina scan
B. Hard token
C. Keypad PIN
D. SMS text
Answer: A (LEAVE A REPLY)

NEW QUESTION: 423
A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).
A. Use a captive portal for user authentication.
B. Implement SSO and allow communication to the internal network
C. Create a new network for the mobile devices and block the communication to the internal network and servers
D. Use the existing network and allow communication to the internal network and servers.
E. Authenticate users using OAuth for more resiliency
F. Use a new and updated RADIUS server to maintain the best solution
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 424
A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?
A. RA1D 0
B. RAID1
C. RAID 5
D. RAID 10
Answer: A (LEAVE A REPLY)
https://techgenix.com/raid-10-vs-raid-5/

NEW QUESTION: 425
An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email

regarding the credit card statement with unusual purchases. Which of the following attacks took place?

A. Protocol poisoning

B. Domain hijacking

C. Bluejacking

D. On-path attack

Answer: (SHOW ANSWER)

NEW QUESTION: 426

An organization is moving away from the use of client-side and server-side certificates for EAR The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

A. EAP-TLS

B. EAP-FAST

C. EAP-TTLS

D. PEAP

Answer: (SHOW ANSWER)

NEW QUESTION: 427

After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

A. The IDS logs

B. The SIEM alerts

C. The full packet capture data

D. The vulnerability scan output

Answer: D (LEAVE A REPLY)

NEW QUESTION: 428

A company labeled some documents with the public sensitivity classification This means the documents can be accessed by:

A. only the individuate listed in the documents

B. employees of other companies and the press

C. all members of the department that created the documents

D. only the company's employees and those listed in the document

Answer: B (LEAVE A REPLY)

NEW QUESTION: 429

After multiple on premises security solutions were migrated to the cloud, the incident response time increased. The analyst are spending a long time to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

A. CASB

B. SWG

C. VPC

D. CMS

Answer: A (LEAVE A REPLY)

NEW QUESTION: 430

A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

A. validate the vulnerability exists in the organization's network through penetration testing

B. research the appropriate mitigation techniques in a vulnerability database

C. find the software patches that are required to mitigate a vulnerability

D. prioritize remediation of vulnerabilities based on the possible impact.

Answer: D (LEAVE A REPLY)

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

NEW QUESTION: 431

A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies will the coffee shop MOST likely use in place of PSK?

A. WEP

B. MSCHAP

C. SAE

D. wes

Answer: C (LEAVE A REPLY)

NEW QUESTION: 432

An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

A. Option C

B. Option A

C. Option D

D. Option B
Answer: (SHOW ANSWER)

NEW QUESTION: 433
A systoms administrator needs to instal the seme X.509 certificate on multiple servers. Which of the following should the administrator use?
A. Key escrow
B. Cerificate chaining
C. Asself-signed certificate
D. An extended validation certificate
Answer: (SHOW ANSWER)

NEW QUESTION: 434
A SOC is currently being outsourced. Which of the following is being used?
A. MSSP
B. PaaS
C. SaaS
D. Microservice
Answer: A (LEAVE A REPLY)

NEW QUESTION: 435
A user downloaded an extension for a browser, and the user's device later became infected. The analyst who is investigating the incident saw various logs where the attacker was hiding activity by deleting dat a. The following was observed running:
Which of the following is the malware using to execute the attack?
A. PowerShell
B. Macros
C. Python
D. Bash
Answer: A (LEAVE A REPLY)

NEW QUESTION: 436
A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?
A. Change the default password for the switch.
B. Install a cable lock on the switch
C. Set up an air gap for the switch.
D. Place the switch In a Faraday cage.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 437
A security engineer needs to Implement the following requirements:
* All Layer 2 switches should leverage Active Directory tor authentication.
* All Layer 2 switches should use local fallback authentication If Active Directory Is offline.
* All Layer 2 switches are not the same and are manufactured by several vendors.
Which of the following actions should the engineer take to meet these requirements? (Select TWO).
Implement RADIUS.
A. Implement a DHCP server
B. Configure port security on the switch with the secondary login method.
C. Implement TACACS+
D. Configure AAA on the switch with local login as secondary
E. Enable the local firewall on the Active Directory server.
Answer: (SHOW ANSWER)

NEW QUESTION: 438
A DBA reports that several production server hard drives were wiped over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data toss?
A. Ransomware
B. Fileless virus
C. Logic bomb
D. Remote access Trojans
E. Rootkit
Answer: C (LEAVE A REPLY)

Valid SY0-601 Dumps shared by Actual4test.com for Helping Passing SY0-601 Exam! Actual4test.com now offer the **newest SY0-601 exam dumps**, the Actual4test.com SY0-601 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-601 dumps with Test Engine here: https://www.actual4test.com/SY0-601_examcollection.html (**1061** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)