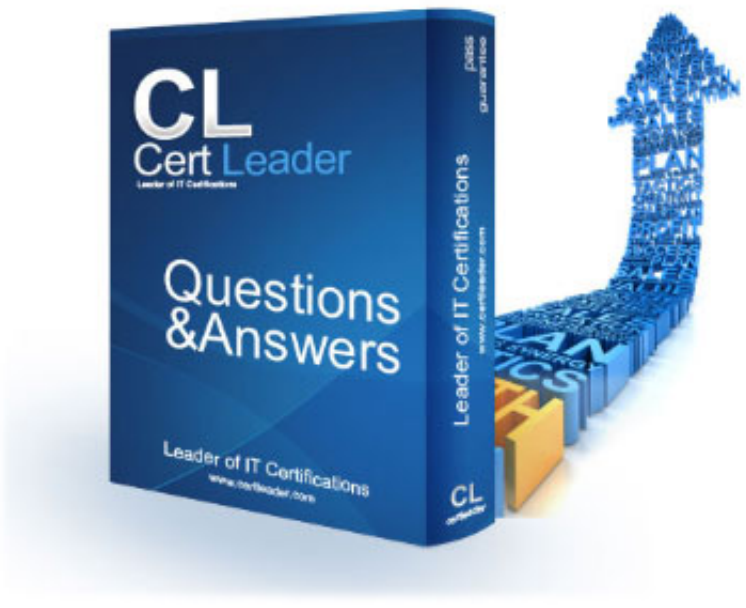
SY0-601 Dumps

CompTIA Security+ Exam

https://www.certleader.com/SY0-601-dumps.html



NEW QUESTION 1
An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

A. Quarantining the compromised accounts and computers, only providing them with network access
B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
C. Isolating the compromised accounts and computers, cutting off all network and internet access.
D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

Answer: B

NEW QUESTION 2
An organization has decided to host its web application and database in the cloud Which of the following BEST describes the security concerns for this decision?

A. Access to the organization's servers could be exposed to other cloud-provider clients
B. The cloud vendor is a new attack vector within the supply chain
C. Outsourcing the code development adds risk to the cloud provider
D. Vendor support will cease when the hosting platforms reach EOL.

Answer: B

NEW QUESTION 3
Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continues to evade detection. Which of the following should administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus.
B. Implement an IDS/IPS
C. Implement a heuristic behavior-detection solution.
D. Implement CASB to protect the network shares.

Answer: C

NEW QUESTION 4
A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization’s vulnerabilities. Which of the following would BEST meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

Answer: D

NEW QUESTION 5
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. Object deference
D. Cross-site request forgery

Answer: B

NEW QUESTION 6
In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Answer: A

NEW QUESTION 7
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. Telecommunications service provider
B. Cloud service provider

C. Master managed service provider
D. Managed security service provider

Answer: B

NEW QUESTION 8
Which of the following relets to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

Answer: A

NEW QUESTION 9
Which of the following would MOST likely support the integrity of a voting machine?

A. Asymmetric encryption
B. Blockchain
C. Transport Layer Security
D. Perfect forward secrecy

Answer: D

NEW QUESTION 10
A desktop support technician recently installed a new document-scanning software program on a computer However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application.
B. The system was quarantined for missing software updates
C. The software was not added to the application whitelist.
D. The system was isolated from the network due to infected software.

Answer: C

NEW QUESTION 10
A large enterprise has moved all Hs data to the cloud behind strong authentication and encryption A sales director recently had a laptop stolen and later, enterprise data was round to have been compromised database. Which of the following was the MOST likely cause?

A. Shadow IT
B. Credential stuffing
C. SQL injection
D. Man-in-the-browser
E. Bluejacking

Answer: A

NEW QUESTION 13
A security analyst is reviewing the following command-line output:
Which of the following Is the analyst observing?

A. IGMP spoofing
B. URL redirection
C. MAC address cloning
D. DNS poisoning

Answer: C

NEW QUESTION 18
A security analyst has been reading about a newly discovered cyber attack 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 MITRE ATT&CK framework
C. The Diamond Model of Intrusion Analysis
D. The Cyber Kill Chain

Answer: B

NEW QUESTION 20
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. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

Answer: C

NEW QUESTION 23
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 ARO
B. An MOU
C. An SLA
D. A BPA

Answer: B

NEW QUESTION 26
A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?
• The solution must be inline in the network
• The solution must be able to block known malicious traffic
• The solution must be able to stop network-based attacks
Which of the following should the network administrator implement to BEST meet these requirements?

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

Answer: D

NEW QUESTION 29
A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

Which of the following network attacks is the researcher MOST likely experiencing?

A. MAC cloning
B. Evil twin
C. Man-in-the-middle
D. ARP poisoning

Answer: C

NEW QUESTION 33
A security an alyst 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

NEW QUESTION 35
A security operations analyst is using the company's SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

A. Eradication
B. Recovery
C. Identification
D. Preparation

Answer: C

NEW QUESTION 36
A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:
* Protection from power outages
* Always-available connectivity In case of an outage
The owner has decided to implement battery backups for the computer equipment Which of the following would BEST fulfill the owner's second need?

A. Lease a point-to-point circuit to provide dedicated access.
B. Connect the business router to its own dedicated UPS.
C. Purchase services from a cloud provider for high availabilityD Replace the business's wired network with a wireless network.

Answer: C

NEW QUESTION 40
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 syslog server
C. The application logs
D. The log retention policy

Answer: B

NEW QUESTION 42
Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

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

Answer: C

NEW QUESTION 43
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. Open the document on an air-gapped network
B. View the document's metadata for origin clues
C. Search for matching file hashes on malware websites
D. Detonate the document in an analysis sandbox

Answer: D

NEW QUESTION 48
Which of the following often operates in a client-server architecture to act as a service repository. providing enterprise consumers access to structured threat intelligence data?

A. STIX
B. CIRT
C. OSINT
D. TAXII

Answer: B

NEW QUESTION 53
While reviewing the wireless router, the 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 rogue system without impacting availability?

A. Conduct a ping sweep.
B. Physically check each system,
C. Deny Internet access to the "UNKNOWN" hostname.
D. Apply MAC filtering,

Answer: D

NEW QUESTION 57
A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

A. Security information and event management
B. A web application firewall
C. A vulnerability scanner

D. A next-generation firewall

Answer: A

NEW QUESTION 62
A company Is concerned about is security after a red-team exercise. The report shows the team was able to reach the critical servers due to the SMB being exposed to the Internet and running NTLMV1, Which of the following BEST explains the findings?

A. Default settings on the servers
B. Unsecured administrator accounts
C. Open ports and services
D. Weak Data encryption

Answer: C

NEW QUESTION 67
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. SOAR playbook
B. Security control matrix
C. Risk management framework
D. Benchmarks

Answer: D

NEW QUESTION 70
An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

Answer: BD

NEW QUESTION 71
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. The order of volatility
B. A checksum
C. The location of the artifacts
D. The vendor's name
E. The date and time
F. A warning banner

Answer: AE

NEW QUESTION 75
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. 135
B. 139
C. 143
D. 161
E. 443
F. 445

Answer: BF

NEW QUESTION 80
A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

A. logger
B. Metasploit
C. tcpdump
D. netstat

Answer: D

NEW QUESTION 81
A hospital's administration is concerned about a potential loss of patient data that is stored on tablets. A security administrator needs to implement controls to alert the SOC any time the devices are near exits. Which of the following would BEST achieve this objective?

A. Geotargeting
B. Geolocation
C. Geotagging
D. Geofencing

Answer: D

NEW QUESTION 85
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

NEW QUESTION 86
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. RA
B. OCSP
C. CRL
D. CSR

Answer: C

NEW QUESTION 89
A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

A. FDE
B. NIDS
C. EDR
D. DLP

Answer: C

NEW QUESTION 93
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: D

NEW QUESTION 95
A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

A. Semi-authorized hackers
B. State actors
C. Script kiddies
D. Advanced persistent threats

Answer: B

NEW QUESTION 99
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 replay attack is being conducted against the application.
B. An injection attack is being conducted against a user authentication system.
C. A service account password may have been changed, resulting in continuous failed logins within the application.

D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Answer: C

NEW QUESTION 104
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. Set up an air gap for the switch.
B. Change the default password for the switch.
C. Place the switch In a Faraday cage.
D. Install a cable lock on the switch

Answer: B

NEW QUESTION 106
A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

A. A packet capture
B. A user behavior analysis
C. Threat hunting
D. Credentialed vulnerability scanning

Answer: C

NEW QUESTION 107
A small business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the business network. Which of the following would BEST support the office's business needs? (Select TWO)

A. Installing WAPs with strategic placement
B. Configuring access using WPA3
C. Installing a WIDS
D. Enabling MAC filtering
E. Changing the WiFi password every 30 days
F. Reducing WiFi transmit power throughout the office

Answer: BD

NEW QUESTION 112
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. Unsecme protocols
B. Default settings
C. Open permissions
D. Weak encryption

Answer: D

NEW QUESTION 115
A retail company that is launching a new website to showcase the company's product line and other information for online shoppers registered the following URLs:

Which of the following should the company use to secure its website rf the company is concerned with convenience and cost?

A. A self-signed certificate
B. A root certificate
C. A code-signing certificate
D. A wildcard certificate
E. An extended validation certificate

Answer: B

NEW QUESTION 117
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

Answer: B

NEW QUESTION 119
Ann, a forensic analyst, needs to prove that the data she originally acquired has remained unchanged while in her custody. Which of the following should Ann use?

A. Chain of custody
B. Checksums
C. Non-repudiation
D. Legal hold

Answer: A

NEW QUESTION 122
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. dd
B. chmod
C. dnsenum
D. logger

Answer: A

NEW QUESTION 127
A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
B. Restrict administrative privileges and patch ail systems and applications.
C. Rebuild all workstations and install new antivirus software
D. Implement application whitelisting and perform user application hardening

Answer: A

NEW QUESTION 129
A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

A. An air gap
B. A Faraday cage
C. A shielded cable
D. A demilitarized zone

Answer: A

NEW QUESTION 131
A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

A. VPN
B. Drive encryption
C. Network firewall
D. File level encryption
E. USB blocker
F. MFA

Answer: BE

NEW QUESTION 133
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 worm that has propagated itself across the intranet, which was initiated by presentation media
B. A fileless virus that is contained on a vCard that is attempting to execute an attack
C. A Trojan that has passed through and executed malicious code on the hosts
D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

Answer: A

NEW QUESTION 137
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. A malicious USB was introduced by an unsuspecting employee.
B. The ICS firmware was outdated
C. A local machine has a RAT installed.
D. The HVAC was connected to the maintenance vendor.

Answer: A

NEW QUESTION 139
A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

A. Preventive
B. Compensating
C. Corrective
D. Detective

Answer: D

NEW QUESTION 141
A financial institution would like to stare is customer data a could but still allow the data ta he accessed and manipulated while encrypted. Doing se would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concern about computational overheads and slow speeds, Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmatric
B. Symmetric
C. Homeomorphic
D. Ephemeral

Answer: B

NEW QUESTION 144
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. Document the collection and require a sign-off when possession changes.
B. Lock the device in a safe or other secure location to prevent theft or alteration.
C. Place the device in a Faraday cage to prevent corruption of the data.
D. Record the collection in a blockchain-protected public ledger.

Answer: A

NEW QUESTION 145
A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted
web-browsing protocols. A security engineer runs a port scan against the server from the Internet and sees the following output:
Which of the following steps would be best for the security engineer to take NEXT?

A. Allow DNS access from the internet.
B. Block SMTP access from the Internet
C. Block HTTPS access from the Internet
D. Block SSH access from the Internet.

Answer: D

NEW QUESTION 146
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 that 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. 135
B. 139
C. 143
D. 161
E. 443
F. 445

Answer: AE

NEW QUESTION 150
An.. that has a large number of mobile devices is exploring enhanced security controls to manage unauthorized access if a device is lost or stolen. Specifically, if mobile devices are more
than 3mi (4 8km) from the building, the management team would like to have the security team alerted and server resources restricted on those devices. Which of the following controls should the
organization implement?

A. Geofencing
B. Lockout
C. Near-field communication
D. GPS tagging

Answer: A

NEW QUESTION 151
Which of the following will MOST likely cause machine learning and AI-enabled systems to operate with unintended consequences?

A. Stored procedures
B. Buffer overflows
C. Data bias
D. Code reuse

Answer: A

Explanation:
https://lionbridge.ai/articles/7-types-of-data-bias-in-machine-learning/

NEW QUESTION 155
An information security incident recently occurred at an organization, and the organization was required to report the incident to authorities and notify the affected parties. When the organization's customers became of aware of the incident, some reduced their orders or stopped placing orders entirely. Which of the following is the organization experiencing?

A. Reputation damage
B. Identity theft
C. Anonymlzation
D. Interrupted supply chain

Answer: A

NEW QUESTION 157
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 communications plan
C. A business continuity plan
D. A disaster recovery plan

Answer: A

NEW QUESTION 162
Which of the following algorithms has the SMALLEST key size?

A. DES
B. Twofish
C. RSA
D. AES

Answer: B

NEW QUESTION 163
A security analyst is reviewing a penetration-testing report from a third-party contractor. The penetration testers used the organization's new API to bypass a driver to perform privilege escalation on the
organization's web servers. Upon looking at the API, the security analyst realizes the particular API call was to a legacy system running an outdated OS. Which of the following is the MOST likely attack
type?

A. Request forgery
B. Session replay
C. DLL injection
D. Shimming

Answer: A

NEW QUESTION 165
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. Information elicitation
B. Typo squatting
C. Impersonation
D. Watering-hole attack

Answer: D

NEW QUESTION 170
An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:

Which of the following BEST describes the type of password attack the attacker is performing?

A. Dictionary
B. Pass-the-hash
C. Brute-force
D. Password spraying

Answer: A

NEW QUESTION 174
A security analyst sees the following log output while reviewing web logs:
Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

A. Secure cookies
B. Input validation
C. Code signing
D. Stored procedures

Answer: B

NEW QUESTION 179
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. The end user purchased and installed a PUP from a web browser
B. A bot on the computer is brute forcing passwords against a website
C. A hacker is attempting to exfiltrate sensitive data
D. Ransomware is communicating with a command-and-control server.

Answer: A

NEW QUESTION 180
Which of the following would cause a Chief Information Security Officer (CISO) the MOST concern regarding newly installed Internet-accessible 4K surveillance cameras?

A. An inability to monitor 100%, of every facility could expose the company to unnecessary risk.
B. The cameras could be compromised if not patched in a timely manner.
C. Physical security at the facility may not protect the cameras from theft.
D. Exported videos may take up excessive space on the file servers.

Answer: A

NEW QUESTION 181
In which of the following common use cases would steganography be employed?

A. Obfuscation
B. Integrity
C. Non-repudiation
D. Blockchain

Answer: A

NEW QUESTION 183

Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

A. Unsecured root accounts
B. Zero day
C. Shared tenancy
D. Insider threat

Answer: C

NEW QUESTION 184
A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

A. Code signing
B. Fuzzing
C. Manual code review
D. Dynamic code analysis

Answer: D

NEW QUESTION 187
A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:
Which of the following types of attack is MOST likely being conducted?

A. SQLi
B. CSRF
C. Session replay
D. API

Answer: C

NEW QUESTION 191
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?

A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

Answer: B

NEW QUESTION 196
A major clothing company recently lost a large amount of proprietary information The security officer must find a solution to ensure this never happens again Which of the following is the BEST technical implementation to prevent this from happening again?

A. Configure DLP solutions
B. Disable peer-to-peer sharing.
C. Enable role-based access controls
D. Mandate job rotation.
E. Implement content filters

Answer: A

NEW QUESTION 200
A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

A. Mobile device management
B. Full-device encryption
C. Remote wipe
D. Biometrics

Answer: A

NEW QUESTION 205
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. NDA
D. MOU

Answer: A

NEW QUESTION 209

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. Buffer overflow
D. Resource exhaustion

Answer: D

NEW QUESTION 213
An attacker is attempting, to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password. the logon screen displays the following message:
Which of the following should the analyst recommend be enabled?

A. Input validation
B. Obfuscation
C. Error handling
D. Username lockout

Answer: B

NEW QUESTION 216
A company wants to modify its current backup strategy to minimize 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 to implement?

A. Incremental backups followed by differential backups
B. Full backups followed by incremental backups
C. Delta backups followed by differential backups
D. Incremental backups followed by delta backups
E. Full backups followed by differential backups

Answer: B

NEW QUESTION 218
A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO).

A. Full-device encryption
B. Network usage rules
C. Geofencing
D. Containerization
E. Application whitelisting
F. Remote control

Answer: AB

NEW QUESTION 219
A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

A. Dual power supply
B. Off-site backups
C. Automatic OS upgrades
D. NIC teaming
E. Scheduled penetration testing
F. Network-attached storage

Answer: AB

NEW QUESTION 220
Which of the following represents a biometric FRR?

A. Authorized users being denied access
B. Users failing to enter the correct PIN
C. The denied and authorized numbers being equal
D. The number of unauthorized users being granted access

Answer: A

NEW QUESTION 223
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-copy-id.
B. Forward the keys using scp.
C. Forward the keys using ash -i.
D. Forward the keys using openssl -s.
E. Forward the keys using ssh-keyger.

Answer: AD

NEW QUESTION 227
An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

A. Nmap
B. cURL
C. Netcat
D. Wireshark

Answer: D

NEW QUESTION 230
The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

A. install a smart meter on the staff WiFi.
B. Place the environmental systems in the same DHCP scope as the staff WiFi.
C. Implement Zigbee on the staff WiFi access points.
D. Segment the staff WiFi network from the environmental systems network.

Answer: D

NEW QUESTION 233
A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.

B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

NEW QUESTION 235
A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

A. SDP
B. AAA
C. IaaS
D. MSSP
E. Microservices

Answer: D

NEW QUESTION 236
A cybersecurity department purchased o new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

A. Randomize the shared credentials
B. Use only guest accounts to connect.
C. Use SSH keys and remove generic passwords
D. Remove all user accounts.

Answer: C

NEW QUESTION 239
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. A reverse proxy was used to redirect network traffic
B. An SSL strip MITM attack was performed
C. An attacker temporarily pawned a name server
D. An ARP poisoning attack was successfully executed

Answer: B

NEW QUESTION 243
A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

A. Create consultant accounts for each region, each configured with push MFA notifications.
B. Create one global administrator account and enforce Kerberos authentication
C. Create different accounts for each regio
D. limit their logon times, and alert on risky logins
E. Create a guest account for each regio
F. remember the last ten passwords, and block password reuse

Answer: C

NEW QUESTION 245
Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

A. Offboarding
B. Mandatory vacation
C. Job rotation
D. Background checks
E. Separation of duties
F. Acceptable use

Answer: BC

NEW QUESTION 249
A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent data? (Select TWO)

A. VPN

B. Drive encryption
C. Network firewall
D. File-level encryption
E. USB blocker
F. MFA

Answer: BE

NEW QUESTION 251
A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to Implement a high availability pair to:

A. decrease the mean ne between failures
B. remove the single point of failure
C. cut down the mean tine to repair
D. reduce the recovery time objective

Answer: B

NEW QUESTION 256
A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

A. Automated information sharing
B. Open-source intelligence
C. The dark web
D. Vulnerability databases

Answer: C

NEW QUESTION 258
A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

A. Salting the magnetic strip information
B. Encrypting the credit card information in transit.
C. Hashing the credit card numbers upon entry.
D. Tokenizing the credit cards in the database

Answer: C

NEW QUESTION 263
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. LACK OF INPUT VALIDATION
B. OPEN PERMISSIONS
C. UNSCECURE PROTOCOL
D. MISSING PATCHES

Answer: A

NEW QUESTION 266
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

NEW QUESTION 267
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

NEW QUESTION 270

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

NEW QUESTION 271
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
E. Container security

Answer: A

NEW QUESTION 274
Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2
B. PCI DSS
C. GDPR
D. ISO 31000

Answer: C

NEW QUESTION 279
In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

A. Identification
B. Preparation
C. Eradiction
D. Recovery
E. Containment

Answer: E

NEW QUESTION 283
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:
Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection
B. CSRF
C. XSS
D. XSRF

Answer: B

NEW QUESTION 284
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. Corrective
B. Deterrent
C. Preventive
D. Mandatory vacations
E. Job rotation
F. Separation of duties

Answer: DE

NEW QUESTION 285
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX using the most secure encryption and protocol available.

Perform the following slops:
* 1. Configure the RADIUS server.
* 2. Configure the WiFi controller.
* 3. Preconfigure the client for an incoming guest.
The guest AD credentials are: User: guest01
Password: guestpass

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Use the same settings as describe in below images.
Graphical user interface, application Description automatically generated

Graphical user interface, text, application, chat or text message Description automatically generated

NEW QUESTION 287
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. OAuth
B. SSO
C. SAML
D. PAP

Answer: C

NEW QUESTION 291
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. Trusted Platform Module
B. A host-based firewall
C. A DLP solution
D. Full disk encryption
E. A VPN
F. Antivirus software

Answer: AB

NEW QUESTION 296
Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

A. Risk matrix
B. Risk tolerance
C. Risk register
D. Risk appetite

Answer: B

NEW QUESTION 301
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. Ransomware
C. Polymophic
D. A worm

Answer: C

NEW QUESTION 306
Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function property. Which of the following should the security administrator consider implementing to address this issue?

A. Application code signing
B. Application whitellsting
C. Data loss prevention
D. Web application firewalls

Answer: B

NEW QUESTION 309
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 GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.
B. 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.
C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

Answer: D

NEW QUESTION 311
Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

A. Least privilege
B. Awareness training

C. Separation of duties
D. Mandatory vacation

Answer: C

NEW QUESTION 314
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 is colluding with human resources
C. The employee's biometrics were harvested
D. A criminal used lock picking tools to open the door.

Answer: A

NEW QUESTION 318
When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization
B. Data masking
C. Normalization
D. Obfuscation

Answer: C

NEW QUESTION 322
An end user reports a computer has been acting slower than normal for a few weeks, During an investigation, an analyst determines the system 3 sending the users email address and a ten-digit number ta an IP address once a day. The only resent log entry regarding the user's computer is the following:

Which of the following is the MOST likely cause of the issue?

A. The end user purchased and installed 2 PUP from a web browser.
B. 4 bot on the computer is rule forcing passwords against a website.
C. A hacker Is attempting to exfilltrated sensitive data.
D. Ransomwere is communicating with a command-and-control server.

Answer: A

NEW QUESTION 326
Joe, an employee, is transferring departments and is providing copies of his files to a network share folder for his previous team to access. Joe is granting read-write-execute permissions to his manager but giving read-only access to the rest of the team. Which of the following access controls is Joe using?

A. FACL
B. DAC
C. ABAC
D. MAC

Answer: D

NEW QUESTION 330
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. Hard token
B. Retina scan
C. SMS text
D. Keypad PIN

Answer: B

NEW QUESTION 333
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. MTBF
B. RPO
C. RTO
D. MTTR

Answer: C

NEW QUESTION 336
The cost of '©movable media and the security risks of transporting data have become too great for a laboratory. The laboratory has decided to interconnect with partner laboratones 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 lo prevent unwanted data exposure to users in partner laboratories?

A. VLAN zoning with a file-transfer server in an external-facing zone
B. DLP running on hosts to prevent file transfers between networks
C. NAC that permits only data-transfer agents to move data between networks
D. VPN with full tunneling and NAS authenticating through the Active Directory

Answer: B

NEW QUESTION 338
Which of the following refers to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

Answer: A

NEW QUESTION 343
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

NEW QUESTION 346
A SOC is implementing an in sider-threat-detection program. The primary concern is that users may be accessing confidential data without authorization. Which of the following should be deployed to detect a potential insider threat?

A. A honeyfile
B. ADMZ
C. DLP
D. File integrity monitoring

Answer: A

NEW QUESTION 348
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. Phishing
B. Whaling
C. Typo squatting
D. Pharming

Answer: B

NEW QUESTION 353
A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:
• Mobile device OSs must be patched up to the latest release
• A screen lock must be enabled (passcode or biometric)
• Corporate data must be removed if the device is reported lost or stolen
Which of the following controls should the security engineer configure? (Select TWO)

A. Containerization

B. Storage segmentation
C. Posturing
D. Remote wipe
E. Full-device encryption
F. Geofencing

Answer: DE

NEW QUESTION 355
A company is designing the layout of a new datacenter so it will have an optimal environmental temperature Which of the following must be included? (Select TWO)

A. An air gap
B. A cold aisle
C. Removable doors
D. A hot aisle
E. An loT thermostat
F. A humidity monitor

Answer: EF

NEW QUESTION 358
A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN? (Select TWO).

A. Due to foreign travel, the user's laptop was isolated from the network.
B. The user's laptop was quarantined because it missed the latest patch update.
C. The VPN client was blacklisted.
D. The user's account was put on a legal hold.
E. The laptop is still configured to connect to an international mobile network operator.
F. The user in unable to authenticate because they are outside of the organization's mobile geofencingconfiguration.

Answer: AB

NEW QUESTION 359
A security administrator is analyzing the corporate wireless network The network only has two access points running on channels 1 and 11. While using airodump-ng. the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access ports Which erf the following attacks in happening on the corporate network?

A. Man in the middle
B. Evil twin
C. Jamming
D. Rogue access point
E. Disassociation

Answer: B

NEW QUESTION 362
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).

A. Implement RADIUS.
B. Configure AAA on the switch with local login as secondary.
C. Configure port security on the switch with the secondary login method.
D. Implement TACACS+
E. Enable the local firewall on the Active Directory server.
F. Implement a DHCP server.

Answer: AB

NEW QUESTION 364
A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

Which of the following attacks MOST likely occurred?

A. Dictionary
B. Credential-stuffing
C. Password-spraying
D. Brute-force

Answer: D

NEW QUESTION 365

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. PFS
B. SPF
C. DMARC
D. DNSSEC

Answer: D

NEW QUESTION 367
A security administrator needs to inspect in-transit files on the enterprise network to search for Pll, credit card data, and classification words. Which of the following would be the BEST to use?

A. IDS solution
B. EDR solution
C. HIPS software solution
D. Network DLP solution

Answer: D

NEW QUESTION 370
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. SED
B. HSM
C. DLP
D. TPM

Answer: A

NEW QUESTION 373
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. Install a NIDS device at the boundary.
B. Segment the network with firewalls.
C. Update all antivirus signatures daily.
D. Implement application blacklisting.

Answer: B

NEW QUESTION 375
Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

A. Alarms
B. Signage
C. Lighting
D. Mantraps
E. Fencing
F. Sensors

Answer: DE

NEW QUESTION 376
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. PFS
C. ESP
D. AH

Answer: A

NEW QUESTION 380
A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM
B. Vishing
C. Spear phishing
D. Smishing

Answer: D

NEW QUESTION 381
A user contacts the help desk to report the following:
Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
The user was able to access the Internet but had trouble accessing the department share until the next day.
The user is now getting notifications from the bank about unauthorized transactions. Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point
B. Evil twin
C. DNS poisoning
D. ARP poisoning

Answer: A

NEW QUESTION 384
A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

A. Repository transaction logs
B. Common Vulnerabilities and Exposures
C. Static code analysis
D. Non-credentialed scans

Answer: C

NEW QUESTION 388
An attacker was easily able to log in to a company's security camera by performing a basic online search for a setup guide for that particular camera brand and model Which of the following BEST describes the configurations the attacker exploited?

A. Weak encryption
B. Unsecure protocols
C. Default settings
D. Open permissions

Answer: C

NEW QUESTION 390
A company uses specially configured workstations tor any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

A. Fileless malware
B. A downgrade attack
C. A supply-chain attack
D. A logic bomb
E. Misconfigured BIOS

Answer: C

NEW QUESTION 392
A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirements?

A. RAID 0+1
B. RAID 2
C. RAID 5
D. RAID 6

Answer: C

NEW QUESTION 395
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. isolation

Answer: A

NEW QUESTION 397
Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.

B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
C. A security control objective cannot be met through a technical change, so the company changes as method of operation
D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

Answer: B

NEW QUESTION 402
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. Hybrid warfare
D. Pharming

Answer: A

NEW QUESTION 407
A forensics examiner is attempting to dump password cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

A. The examiner does not have administrative privileges to the system
B. The system must be taken offline before a snapshot can be created
C. Checksum mismatches are invalidating the disk image
D. The swap file needs to be unlocked before it can be accessed

Answer: D

NEW QUESTION 409
A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

A. AH
B. ESP
C. SRTP
D. LDAP

Answer: B

NEW QUESTION 414
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load Which of the following are the BEST options to accomplish this objective'? (Select TWO)

A. Load balancing
B. Incremental backups
C. UPS
D. RAID
E. Dual power supply
F. NIC teaming

Answer: AD

NEW QUESTION 417
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SY0-601 Exam with Our Prep Materials Via below:

https://www.certleader.com/SY0-601-dumps.html