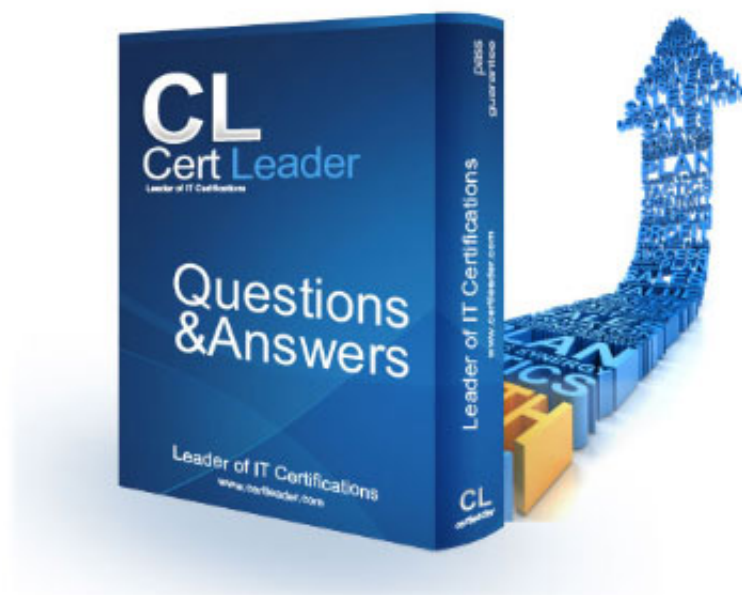


SY0-601 Dumps

CompTIA Security+ Exam

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



NEW QUESTION 1

Which of the following ISO standards is certified for privacy?

- A. ISO 9001
- B. ISO 27002
- C. ISO 27701
- D. ISO 31000

Answer: C

NEW QUESTION 2

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 3

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 China. Payments for services are managed by a 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. Payment Card Industry Data Security Standard
- B. Cloud Security Alliance Best Practices
- C. ISO/IEC 27032 Cybersecurity Guidelines
- D. General Data Protection Regulation

Answer: A

NEW QUESTION 4

An attacker was easily able to log in to a company's security camera by performing a baste 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 5

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

NEW QUESTION 6

A security administrator currently spends a large amount of time on common security tasks, such aa report generation, phishing investigations, and user provisioning and deprovisioning This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

- A. DAC
- B. ABAC
- C. SCAP
- D. SOAR

Answer: D

NEW QUESTION 7

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 8

A security analyst is investigating a vulnerability in which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management.

Which of the following tools can the analyst use to verify the permissions?

- A. ssh
- B. chmod
- C. 1s
- D. setuid
- E. nessus
- F. nc

Answer: B

NEW QUESTION 9

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 availability
- D Replace the business's wired network with a wireless network.

Answer: C

NEW QUESTION 10

A web server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the following should the administrator implement to avoid disruption?

- A. NIC teaming
- B. High availability
- C. Dual power supply
- D. IaaS

Answer: B

NEW QUESTION 10

Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

- A. DLP
- B. HIDS
- C. EDR
- D. NIPS

Answer: C

NEW QUESTION 14

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:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

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 18

An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the

evidence, which of the following forensic techniques should be used?

- A. Order of volatility
- B. Data recovery
- C. Chain of custody
- D. Non-repudiation

Answer: C

NEW QUESTION 19

An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions. Which of the following sources of information would BEST support this solution?

- A. Web log files
- B. Browser cache
- C. DNS query logs
- D. Antivirus

Answer: C

NEW QUESTION 20

A startup company is using multiple SaaS and IaaS platform to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

- A. SIEM
- B. DLP
- C. CASB
- D. SWG

Answer: C

NEW QUESTION 23

A cloud administrator is configuring five compute instances under the same subnet in a VPC. Three instances are required to communicate with one another, and the other two must be logically isolated from all other instances in the VPC. Which of the following must the administrator configure to meet this requirement?

- A. One security group
- B. Two security groups
- C. Three security groups
- D. Five security groups

Answer: B

NEW QUESTION 28

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 experiencing?

- A. SQL injection
- B. Cross-site scripting
- C. Pass-the-hash
- D. Directory traversal

Answer: B

NEW QUESTION 29

An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

- A. An external security assessment
- B. A bug bounty program
- C. A tabletop exercise
- D. A red-team engagement

Answer: C

NEW QUESTION 30

Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

- A. SaaS
- B. PaaS
- C. IaaS
- D. DaaS

Answer: C

NEW QUESTION 35

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 39

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 40

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

NEW QUESTION 41

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 45

A company is launching a new internet platform for its clients. The company does not want to implement its own authorization solution but instead wants to rely on the authorization provided by another platform. Which of the following is the BEST approach to implement the desired solution?

- A. OAuth
- B. TACACS+
- C. SAML
- D. RADIUS

Answer: D

NEW QUESTION 46

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 50

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:

- www.companysite.com
- shop.companysite.com
- about-us.companysite.com
- contact-us.companysite.com
- secure-logon.companysite.com

Which of the following should the company use to secure its website if 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 55

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

NEW QUESTION 60

Which of the following would be the BEST resource lor a software developer who is looking to improve secure coding practices for web applications?

- A. OWASP
- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

Answer: A

NEW QUESTION 63

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. Role-based
- D. Mandatory

Answer: D

NEW QUESTION 66

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force
- D. Spraying

Answer: D

NEW QUESTION 68

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. Dual power supplies
- B. A UPS
- C. A generator
- D. APDU

Answer: B

NEW QUESTION 69

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 74

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 76

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 80

Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
- B. DNS query logging
- C. Exact mail exchanger records in the DNS
- D. The addition of DNS conditional forwarders

Answer: C

NEW QUESTION 85

A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multicloud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location. Which of the following would BEST meet the architect's objectives?

- A. Trusted Platform Module
- B. IaaS
- C. HSMaaS
- D. PaaS
- E. Key Management Service

Answer: A

NEW QUESTION 87

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

- A. Bug bounty
- B. Black-box
- C. Gray-box
- D. White-box

Answer: A

NEW QUESTION 90

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: D

NEW QUESTION 92

A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

- A. Create an OSCP
- B. Generate a CSR
- C. Create a CRL
- D. Generate a .pfx file

Answer: B

NEW QUESTION 93

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 97

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:

```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdftodocx.msi
Connection Details: 35.242.219.204:80
```

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 101

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 104

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 108

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 110

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII
- E. Configure the application to encrypt the PII

Answer: D

NEW QUESTION 115

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 120

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 some 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. SFTP FTPS
- B. SNMPv2 SNMPv3
- C. HTTP, HTTPS
- D. TFTP FTP
- E. SNMPv1, SNMPv2
- F. Telnet SSH
- G. TLS, SSL
- H. POP, IMAP
- I. Login, rlogin

Answer: BCF

NEW QUESTION 124

A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization's network. Which of the following will the analyst MOST likely use to accomplish the objective?

- A. A table exercise
- B. NST CSF
- C. MTRE ATT\$CK
- D. OWASP

Answer: C

NEW QUESTION 127

Which of the following types of controls is a turnstile?

- A. Physical
- B. Detective
- C. Corrective
- D. Technical

Answer: A

NEW QUESTION 129

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 130

Which of the following BEST explains the difference between a data owner and a data custodian?

- A. 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
- 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 grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer: B

NEW QUESTION 133

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

- A. To define the level of risk using probability and likelihood
- B. To register the risk with the required regulatory agencies
- C. To identify the risk, the risk owner, and the risk measures
- D. To formally log the type of risk mitigation strategy the organization is using

Answer: C

NEW QUESTION 134

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. Least privilege
- C. An acceptable use policy
- D. Ofboarding

Answer: D

NEW QUESTION 137

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 138

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 141

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 data breach?

- A. LACK OF INPUT VALIDATION
- B. OPEN PERMISSIONS
- C. UNSECURE PROTOCOL
- D. MISSING PATCHES

Answer: A

NEW QUESTION 146

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 149

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. Something you know
- B. Something you have
- C. Somewhere you are
- D. Someone you are
- E. Something you are
- F. Something you can do

Answer: BE

NEW QUESTION 152

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 153

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 157

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 vulnerability scan output
- B. The security logs
- C. The baseline report
- D. The correlation of events

Answer: A

NEW QUESTION 160

A company recently experienced an attack in which a malicious actor was able to exfiltrate data by cracking stolen passwords, using a rainbow table the sensitive data. Which of the following should a security engineer do to prevent such an attack in the future?

- A. Use password hashing.
- B. Enforce password complexity.
- C. Implement password salting.
- D. Disable password reuse.

Answer: D

NEW QUESTION 162

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 167

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. Polymorphic
- D. A worm

Answer: C

NEW QUESTION 169

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. MDM
- B. MAM
- C. VDI
- D. DLP

Answer: A

NEW QUESTION 171

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

Answer: A

NEW QUESTION 176

A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:

- * 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. Content management, remote wipe, geolocation, context-aware authentication, and containerization
- C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
- D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

Answer: D

NEW QUESTION 177

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 178

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:

```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: (movical-arddisk)volume00\users\jordan\appdata\local\microsoft\windows\NetCache\81p4fho3aw.mai
Connection Details: 19.242.213.274:80
```

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. 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 179

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. A capture-the-flag competition
- B. A phishing simulation
- C. Physical security training
- D. Baste awareness training

Answer: B

NEW QUESTION 183

After consulting with the Chief Risk Officer (CRO), a manager decides to acquire cybersecurity insurance for the company. Which of the following risk management strategies is the manager adopting?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transference
- D. Risk mitigation

Answer: C

NEW QUESTION 187

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors'?

- A. IP restrictions
- B. Multifactor authentication
- C. A banned password list
- D. A complex password policy

Answer: B

NEW QUESTION 188

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. WPS
- D. SAE

Answer: D

NEW QUESTION 191

A university is opening a facility in a location where there is an elevated risk of theft. The university wants to protect the desktops in its classrooms and labs. Which of the following should the university use to BEST protect these assets deployed in the facility?

- A. Visitor logs
- B. Cable locks
- C. Guards
- D. Disk encryption
- E. Motion detection

Answer: B

NEW QUESTION 194

Entering a secure area requires passing through two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?

- A. Cameras
- B. Faraday cage
- C. Access control vestibule
- D. Sensors
- E. Guards

Answer: C

NEW QUESTION 195

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 200

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?

- 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 path update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.

Answer: A

NEW QUESTION 202

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 205

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. Baseline modification
- B. A fileless virus
- C. Tainted training data
- D. Cryptographic manipulation

Answer: C

NEW QUESTION 208

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 211

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 216

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 encryption
- B. Data masking
- C. Anonymization
- D. Tokenization

Answer: A

NEW QUESTION 218

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. Limit the use of third-party libraries.
- B. Prevent data exposure queries.
- C. Obfuscate the source code.
- D. Submit the application to QA before releasing it.

Answer: D

NEW QUESTION 223

A security analyst is running a vulnerability scan to check for missing patches during a suspected security incident. During which of the following phases of the response process is this activity MOST likely occurring?

- A. Containment
- B. Identification
- C. Recovery
- D. Preparation

Answer: D

NEW QUESTION 228

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 230

.....

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>