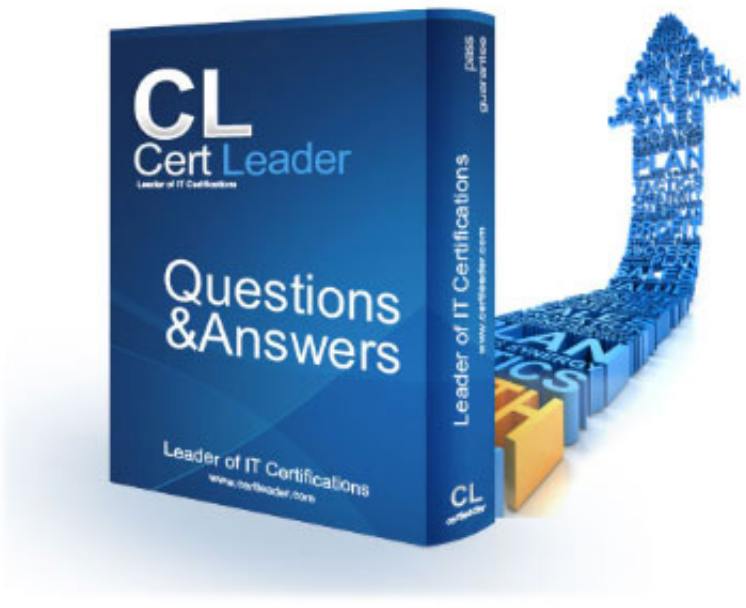
CC Dumps

Certified in Cybersecurity (CC)

https://www.certleader.com/CC-dumps.html



NEW QUESTION 1
In the context of cybersecurity, typical threat actors include the following:

A. Insiders (either deliberately, by simple human error, or by gross incompetence).
B. Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability).
C. Technology (such as free-running bots and artificial intelligence
D. All

Answer: D

NEW QUESTION 2
What is multi-factor authentication (MFA)?

A. A type of authentication that uses only one method
B. A type of authentication that uses only two methods
C. A type of authentication that uses more than two methods (Correct)
D. A type of authentication that uses only one factor

Answer: C

NEW QUESTION 3
What is the recommended fire suppression system for server rooms

A. Foam based
B. Water based
C. Powder based
D. ftac hacorl

Answer: D

NEW QUESTION 4
What is the importance of non-repudiation in todays world of ecommerce

A. It ensures that people are not held responsible for transaction that did not conduct
B. It ensures that people are held responsible for transactions they conducted
C. It ensures that transactions are not conducted online
D. It ensures that transactions are conducted online

Answer: B

NEW QUESTION 5
A set of security controls or system settings used to ensure uniformity of configuration through the IT environment?

A. Patches
B. Inventory
C. Baseline
D. Policy

Answer: C

NEW QUESTION 6
Which is related to Standard

A. NIST
B. GDPR
C. HIPAA
D. ALL

Answer: A

NEW QUESTION 7
What is the first phase in System Development Life Cycle

A. Requirements Analysis Phase
B. Feasibilty Study
C. Design Phase
D. Development Phase

Answer: B

NEW QUESTION 8
Which of the following is not a Social engineering technique

A. Pretexting
B. Baiting
C. Quid pro quo
D. Double Dealing

Answer: D

NEW QUESTION 9
In which of the following phases of an incident recovery plan the incident responses prioritized

A. Post incident activity
B. Containment eradication and recovery
C. Detection and analysis
D. Preparation

Answer: C

NEW QUESTION 10
Type 1 authentication posses

A. Users may share their credential with others
B. User may forgot their passwords
C. Passwords may be intercepted and stolen
D. ALL

Answer: D

NEW QUESTION 10
Which drives for the IPv6 introduction

A. IPv4 was not secured
B. IPv4 not combatible with new devices
C. Because IPv4 was projected to be exhausted
D. IPV6 support WiFi

Answer: C

NEW QUESTION 14
Embedded systems and network-enabled devices that communicate with the internet are considered as

A. Endpoint
B. Node
C. IOT
D. Router

Answer: C

NEW QUESTION 17
IDS can be described in terms of what fundamental functional components?

A. Response
B. Information Sources
C. Analysis
D. All of the choices.

Answer: D

NEW QUESTION 19
The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization

A. Standard
B. Policy
C. Procedure
D. Governance

Answer: D

NEW QUESTION 21
Centralized organizational function fulfilled by an information security team that monitors, detects and analyzes events on the network or system to prevent and resolve issues before they result in business disruptions.

A. IRP
B. BCP
C. SOC
D. DRP

Answer: C

NEW QUESTION 22
Which of the following is endpint

A. Router
B. Firewall
C. Laptop
D. Switch

Answer: C

NEW QUESTION 27
Which of the following is a subject?

A. file
B. fence
C. filename
D. user

Answer: D

NEW QUESTION 28
COVID-19 is one of the perfect example of a situation, where a _____ plan is enacted to sustain the business

A. IRP
B. DRP
C. BCP
D. ALL

Answer: C

NEW QUESTION 31
A scammer will attempt to make a malicious website look exactly like a legitimate one that the victim knows and trusts

A. DOS
B. Virus
C. Spoofing
D. Phishing

Answer: C

NEW QUESTION 32
Which Regulation addresses personal privacy

A. HIPAA
B. GDPR
C. NIST
D. ISO

Answer: B

NEW QUESTION 36
Which component of the incident response plan involves identifying critical data and systems?

A. Detection and Analysis
B. Preparation
C. Cantainment
D. Eradication

Answer: B

NEW QUESTION 37
Which of the following principles aims primarily at fraud detection

A. Defense in depth
B. Least privilege
C. Separation of duties
D. Privileged account

Answer: C

NEW QUESTION 42
Is an integrated platform and graphical tool for performing security testing of web applications.

A. Burb suite
B. Wireshark C Fiddler
C. ZenMap

Answer: A

NEW QUESTION 46
What is the purpose of non-repudiation in information security?

A. To ensure data is always accessible when needed
B. To protect data from unauthorized access
C. To prevent the sender or recipient of a message from denying having sent or received the message
D. To ensure data is accurate and unchanged

Answer: C

NEW QUESTION 51
What is the primary goal of network segmentation in cybersecurity?

A. To increase network speed
B. To isolate and protect critical assets
C. To centralize data storage
D. To expand the network's coverage

Answer: B

NEW QUESTION 53
In DAC, the policy specifies that a subject who has been granted access to information can do the following:

A. Change security attributes on subjects, objects, information systems or system components
B. Choose the security attributes to be associated with newly created or revised objects
C. Change the rules governing access control
D. ALL

Answer: D

NEW QUESTION 55
Which is an authorized simulated attack performed on a computer system to evaluate its security.

A. Penetration test
B. Security Testing
C. Automated Testing
D. Regression Testing

Answer: A

NEW QUESTION 59
What is the primary purpose of a firewall in network security?

A. Encrypt data transmissions
B. Prevent unauthorized access
C. Monitor network traffic
D. Backup critical data

Answer: B

NEW QUESTION 63
Which of the following is a characteristic of cloud

A. Broad Network Access
B. Rapid Elasticity
C. Measured Service
D. AII

Answer: B

NEW QUESTION 64
Exhibit.

information security is not built on which of the following?

A. Confidentiality
B. Availability
C. Accessibility
D. Integrity

Answer: C

NEW QUESTION 68
A company primary data center goes down due to a hardware failure causing a major disruption to the IT and communications systems. What is the focus of disaster recovery planning in this scenario

A. Maintaining critical business functions during the disruption
B. Fixing the hardware failure
C. Restoring IT and communications back to full operations after the disruptions
D. Guiding the actions of emergency response personnel during the disruption

Answer: C

NEW QUESTION 71
A company network has been infected with malware and all its servers are down. What is the first step that the Disaster Recovery team should take to restore the systems?

A. Disconnect the affected systems from the network
B. Conduct a risk assessment of determine the extent of the damage
C. Restore data from backup systems
D. Contact the enforcement to investigate the cyberattack

Answer: A

NEW QUESTION 72
What is IPSEC reply attack

A. An attack where an attacker modifies packets in transit
B. An attack where an attacker eavesdrops on network traffic
C. An attack where an attacker overloads a network with traffic
D. An attack where an attacker attempts to inject packets in an existing sessio

Answer: D

NEW QUESTION 74
A company network experience a sudden flood of network packets that causes major slowdown in internet traffic. What type of event it this?

A. Security incident
B. Natural disaster
C. Exploit
D. Adverse event

Answer: D

NEW QUESTION 79
Which is the SSH port

A. 21
B. 23
C. 24
D. 22

Answer: D

NEW QUESTION 83
What is the main purpose of creating baseline in ensuring system integrity

A. To compare the baseline with the current state of the systems
B. To protect the information
C. To understand the current state of the system
D. AII

Answer: A

NEW QUESTION 88
A logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution.

A. LAN
B. VPN
C. WLAN
D. VLAN

Answer: D

NEW QUESTION 92
Which of these components is very likely to be instrumental to any disaster recovery (DR) effort?

A. Routers
B. Laptops
C. Firewalls
D. Backups

Answer: D

NEW QUESTION 93
What is the priority of incident response in the context of incident management

A. Protect the organization mission and objectives
B. Reduce the impact of the incident
C. Protect life health and safety
D. Resume interrupted operations as soon as possible

Answer: C

NEW QUESTION 98
Which penetration testing technique requires the team to do the MOST work and effort?

A. White box
B. Blue box

C. Gray box
D. Black box

Answer: D

NEW QUESTION 103
Juli is listening to network traffic and capturing passwords as they are sent to the authentication server. She plans to use the passwords as part of a future attack. What type of attack is this?

A. Brute-force attack
B. Dictionary attack
C. Social engineering attack
D. Replay attack

Answer: D

NEW QUESTION 106
Which access control model is best suited for a large organization with many departments that have different data access needs

A. DAC
B. RBAC
C. MAC
D. RUBAC

Answer: B

NEW QUESTION 109
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

A. Security Assessment
B. Risk Assessment
C. DRP
D. IRP

Answer: A

NEW QUESTION 113
Which type of malware encrypts a users file system and demands payment in exchange of decrypting key

A. Worm
B. Trojan
C. virus
D. Ransomware

Answer: D

NEW QUESTION 116
The Bell and LaPadula access control model is a form of

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

Answer: B

NEW QUESTION 119
Which of the following is often associated with DR planning?

A. Checklists
B. Antivirus
C. firewall
D. AII

Answer: D

NEW QUESTION 122
Who must follow HIPAA Compliance

A. Energy Sector
B. Health Care
C. Finance Sector
D. ALL

Answer: B

NEW QUESTION 127
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information

A. Risk Management
B. Risk Assessment
C. Risk Mitigation
D. Adequate Security

Answer: D

NEW QUESTION 128
Devid's team recently implemented a new system that gathers information from a variety of different log sources, analyses that information, and then triggers automated playbooks in response to security events, what term BEST describes this technology?

A. SIEM
B. Log Repository
C. IPS
D. SOAR

Answer: D

NEW QUESTION 132
_____ are virtual separations within a switch and are used mainly to limit broadcast traffic

A. LAN
B. WAN
C. VLAN
D. MAN

Answer: C

NEW QUESTION 135
Which type of application can intercept sensitive information such as passwords on a network segment?

A. Log server
B. Network Scanner
C. Firewall
D. Protocol Analyzer

Answer: D

NEW QUESTION 139
A company wants to ensure that its employees cannot bring unauthorized electronic devices into the workspace which physical control is best suited for this

A. Metal Detectors
B. Security gaurds
C. RFID scanners
D. Baggage X-ray machinces

Answer: A

NEW QUESTION 141
Which type of authentication is something which you

A. Type1
B. Type 2
C. Type 3
D. Type 4

Answer: C

NEW QUESTION 144
What is the process of verifying a users identity called?

A. Confidentiality
B. Autentication
C. Authorization
D. Identification

Answer: B

NEW QUESTION 147

Networks are often micro segmented networks, with firewalls at nearly every connecting point

A. DMZ
B. VPN
C. VLAN
D. Zero Trust

Answer: A

NEW QUESTION 151
Which document serve as specifications for the implementation of policy and dictates mandatory requirements

A. Policy
B. Guideline
C. Standard
D. Procedures

Answer: C

NEW QUESTION 152
Access control used in in high-security situations such as military and government organizations.

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

Answer: B

NEW QUESTION 155
Restoring IT and communications back to full operation after a disruption.

A. BCP
B. IRP
C. DRP
D. None

Answer: C

NEW QUESTION 160
A Company IT system experienced a system crash that result in a loss of data. What term best describes this event?

A. Breach
B. Incident
C. Event
D. Adverse Event

Answer: A

NEW QUESTION 162
An organization develops a set of procedures to restore critical business processes after a significant disruption. What type of plan is this?

A. bcp
B. IRP
C. DRP
D. None

Answer: A

NEW QUESTION 165
Which is strongly used for Securing Wi-Fi

A. WPA2
B. WEP
C. WPA
D. SSL

Answer: A

NEW QUESTION 169
Measure of the extent to which an entity is threatened by a potential circumstance or event and likelihood of occurrence

A. Impact
B. Risk
C. Threat

D. Threat Vector

Answer: B

NEW QUESTION 174
What is the first component the new security engineer should learn about in the incident response plan?

A. Detection and analysis
B. Preparation
C. Containment
D. Eradication

Answer: B

NEW QUESTION 175
An employee unintentionally shares confidential information with an unauthorized party. What term best describes this situation?

A. Event
B. Exploit
C. Intrusion
D. Breach

Answer: D

NEW QUESTION 176
Which of the following best describes a zero-day vulnerability?

A. A vulnerability that has been identified and patched by software vendors
B. A vulnerability that has not yet been discovered or publicly disclosed.
C. A vulnerability that can only be exploited by experienced hackers.
D. A vulnerability that affects only legacy systems.

Answer: B

NEW QUESTION 181
WF attack in which a subscriber currently authenticated to an Server and connected through a secure session browses to an attacker's website, causing the subscriber to unknowingly invoke unwanted actions at the Server

A. XSS
B. CSRF
C. Spoofing
D. ALL

Answer: B

NEW QUESTION 186
A/hich layer of the OSI Layer model is the target of a buffer overflow attack

A. Layer 7
B. Layer 3
C. Layer 5
D. Layer 4

Answer: A

NEW QUESTION 189
A company experiences a major IT outage and cannot perform its critical business functions. What type of plan will hep the company recover from this event?

A. BCP
B. IRP C DRP
C. BIA

Answer: C

NEW QUESTION 192
A set of instructions to help IT staff detect, respond to, and recover from network security incidents?

A. BCP
B. IRP
C. DRP
D. None

Answer: B

NEW QUESTION 197
Duke would like to restrict users from accessing a list of prohibited websites while connected to his network. Which one of the following controls would BEST achieve his objective?

A. URL Filter
B. IP Address Block
C. DLP Solution
D. IPS Solution

Answer: A

NEW QUESTION 198
organization experiences a security event that potentially jeopardizes the confidentiality, integrity or availability of its information system. What term best describes this situation?

A. Breach
B. Event
C. Incident
D. Exploit

Answer: C

NEW QUESTION 199
Ignoring the risk and proceeding the business operations

A. Risk Acceptance
B. Risk Mitigation
C. Risk Avoidance
D. Risk Transfer

Answer: A

NEW QUESTION 201
The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats.

A. Segregation of Duties
B. Principle of Least Privilege
C. Privileged Account
D. Rule-based access control

Answer: A

NEW QUESTION 205
Which of the following physical controls is used to protect against eavesdropping and data theft through electromagnetic radiation

A. EMI Shielding
B. Screening rooms
C. White noise generators
D. ALL

Answer: A

NEW QUESTION 209
What is the main challenge in achieving non repudiation in electronic transactions

A. Ensuring the identity of the sender and recipient is verified
B. Ensuring the authenticity and integrity of the message
C. Making sure the message is not tampered with during transmission
D. All of the above

Answer: D

NEW QUESTION 210
Which of the following documents identifies the principles and rules governing an organization's protection of information systems and data

A. Procudure
B. Guideline
C. Policy
D. Standard

Answer: C

NEW QUESTION 211
Which type of network is set up similar to the internet but is private to an organization. Select the MOST appropriate?

A. Extranet
B. VLAN
C. Intranet
D. VPN

Answer: B

NEW QUESTION 216
A new BYOD policy has been enforced in NEW Corp which type of control is used to enforce thissecurity policies

A. Physical control
B. Logical Control
C. Administrative Control
D. Technical Control

Answer: C

NEW QUESTION 219
An outward-facing IP address used to access the Internet.

A. Global Address
B. Private Address
C. Public Address
D. DNS

Answer: C

NEW QUESTION 221
Port used in DNS

A. 53
B. 80
C. 45
D. 54

Answer: A

NEW QUESTION 225
A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

A. Turnstile
B. ManTrap
C. Bollard
D. Gate

Answer: A

NEW QUESTION 226
An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

A. BIA
B. DR
C. BCP
D. IRP

Answer: A

NEW QUESTION 229
Can be considered to be a fingerprint of the file or message

A. Hashing .
B. encryption
C. decryption
D. encoding

Answer: A

NEW QUESTION 230
Natalia is concerned about the security of his organization's domain name records and would like to adopt a technology that ensures their authenticity by adding digital signatures. Select the MOST appropriate technology to use?

A. DNSSIGN
B. DNSSEC
C. CERTDNS

D. DNS2

Answer: B

NEW QUESTION 233
A device that routes traffic to the port of a known device

A. Switch
B. Hub
C. Router
D. Ethernet

Answer: A

NEW QUESTION 235
An external entity has tried to gain access to your organization's IT environment without proper authorization. This is an example of a(n)

A. Exploit
B. Intrusion
C. Event
D. Malware

Answer: B

NEW QUESTION 236
Which of the following is not a feature of a cryptographic hash function

A. Deterministic
B. Unique
C. Useful
D. Reversible

Answer: D

NEW QUESTION 238
The practice of sending fraudulent communications that appear to come from a reputable source

A. DOS
B. Virus
C. Spoofing
D. Phishing

Answer: D

NEW QUESTION 241
What is the most important aspect of security awareness/training?

A. Maximizing business capabilities
B. Protecting assets
C. Protecting health and human safety
D. Ensuring the confidentiality of data

Answer: C

NEW QUESTION 243
Duke would like to restrict users from accessing a list of prohibited websites while connected to his network. Which one of the following controls would BEST achieve his objective?

A. URL Filter
B. IP Address Block
C. DLP Solution
D. IPS Solution

Answer: A

NEW QUESTION 245
What is the BEST defense against dumpster diving attacks?

A. Anti-malware software
B. Clean desk policy
C. Data loss prevention tools
D. Shredding

Answer: D

NEW QUESTION 248
Which authentication helps build relationships between different technology providers, enabling automatic identification and user access. Employees no longer need to enter separate usernames and passwords when visiting a new service provider

A. Basic
B. Kerberos
C. Token Based
D. Federated

Answer: D

NEW QUESTION 251
Risk tolerance also known as

A. Risk threshold
B. Risk appetite
C. Acceptable risk
D. AII

Answer: D

NEW QUESTION 256
Devid is worried about distributed denial of service attacks against his company's primary web application, which of the following options will provide the MOST resilience against large-scale ddos attacks?

A. Implement a CDN
B. Increase the number of servers in the web application server cluster
C. Contract for DDoS mitigation services via the company's IPS
D. Increase the amount of bandwidth available from one or more ISPs

Answer: A

NEW QUESTION 258
An attackers place themselves between two devices (often a web browser and a web server)

A. Phishing
B. Spoofing
C. On Path
D. All

Answer: C

NEW QUESTION 263
DDOS attack affect which OSI layer

A. Network layer
B. Transport layer
C. Physical Layer
D. Both A and B

Answer: D

NEW QUESTION 268
Port scanning attack target which OSI layer

A. Layer 4
B. Layer 3
C. Layer 5
D. Layer 6

Answer: A

NEW QUESTION 269
Why is an asset inventory much important?

A. It tells you what to encrypt
B. The law requires it
C. It contains a price list
D. You can't protect what you don't know you have

Answer: D

NEW QUESTION 272
What is the potential impact of an IPSec reply attack

A. Modification of network traffic
B. Disruption of network communication
C. Unauthorized access to network resources
D. ALL

Answer: A

NEW QUESTION 275
Mark works in the security office. During research, Mark learns that a configuration change could better protect the organization's IT environment. Mark makes a proposal for this change, but the change cannot be implemented until it is approved, tested, and then cleared for deployment by the Change Control Board. This is an example of _____

A. Holistic security
B. Defense in depth
C. Threat intelligence
D. Segregation of duties

Answer: D

NEW QUESTION 276
A standard that defines wired communications of network devices

A. Switch
B. Hub
C. router
D. Ethernet

Answer: D

NEW QUESTION 280
Methods or mechanisms cybercriminals use to gain illegal, unauthorized access to computer systems and networks.

A. Attacker
B. Threat Vector
C. Threat
D. Threat actor

Answer: B

NEW QUESTION 281
.....

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 CC Exam with Our Prep Materials Via below:

https://www.certleader.com/CC-dumps.html