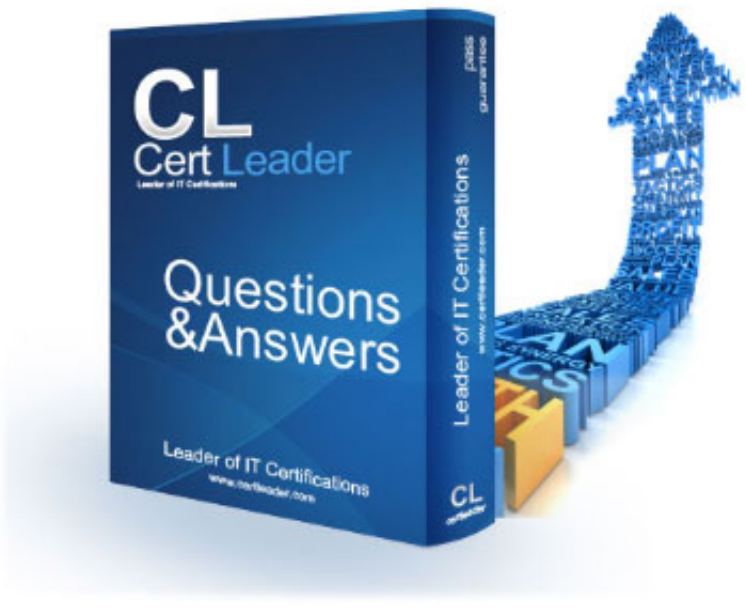
CC Dumps

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
How do you distinguish Authentication and Identification

A. Both Same
B. Authentication is the process of verifying user identity and a user of a system or an application
C. Authentication is the process of verifying user identity and Identification is the ability to identify uniquely quely Identification is the process to allow resource access
D. Identification is the process of verifying user identity and Authentication is the process to allow resource access

Answer: B

NEW QUESTION 4
Faking the sender address in a transmission to gain illegal entry into a secure system

A. Phishing
B. ARP
C. Spoofing
D. ALL

Answer: C

NEW QUESTION 5
A chief information security officer (CISO) at a large organization documented a policy that establishes the acceptable use of cloud environments for all staff. This is an example of

A. Technical control
B. Physical control
C. Cloud control
D. Management/Administrative control

Answer: D

NEW QUESTION 6
Common network device used to connect networks?

A. Server
B. Endpoint
C. Router
D. Switch

Answer: C

NEW QUESTION 7
Configuration settings or parameters stored as data, managed through a software graphical user interface (GUI) is

A. Logical access control
B. Physical access control
C. Administratirve Access control

Answer: A

NEW QUESTION 8
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 9
Which is related to Standard

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

Answer: A

NEW QUESTION 10
Requires that all instances of the data be identical in form,

A. Confidentiality
B. Availability
C. Consistency
D. ALL

Answer: C

NEW QUESTION 10
Which is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

A. VLAN
B. SDN
C. VPN
D. SAN

Answer: B

NEW QUESTION 13
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 18
TCP and UDP reside at which layer of the osi model?

A. Session
B. Transport
C. Data link
D. Presentation

Answer: D

NEW QUESTION 21
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 25
Which OSI layer VPN works

A. Layer 5
B. Layer 6
C. Layer 1
D. Layer 3

Answer: D

NEW QUESTION 27
System capabilities designed to detect and prevent the unauthorized use and transmission of information.

A. SOC
B. SIEM solutions
C. Data Loss Prevention
D. Crytography

Answer: C

NEW QUESTION 32
Which of the following is not a protocol of the OSI layer 3

A. IGMP
B. IP
C. ICMP
D. SSH

Answer: D

NEW QUESTION 34
A popular way of implementing "least privilege"

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

Answer: C

NEW QUESTION 35
Which type of control is used to minimize the impact of an attack and to restore normal operations as quick as possible

A. Compensatory Control
B. Corrective Control
C. Recovery control
D. Detective Control

Answer: C

NEW QUESTION 39
What is the primary goal of incident management

A. To potect life health and safety
B. To reduce the impacrt of an incident
C. To prepare for any incident
D. To resume interrupted operations as soon as possible

Answer: C

NEW QUESTION 40
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 43
What is the importance of identifying roles and responsibilities in incident response planning?

A. To prevent incidents from happening
B. To ensure that everyone knows their job in the incident response process
C. To reduce the impact of the incident
D. To choose an appropriate containment strategy

Answer: B

NEW QUESTION 47
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 48
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 51
Timiting access to resources based on the sensitivity of the information that the resource contains and the authorization of the user to access information with that level of sensitivity.

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

Answer: B

NEW QUESTION 55
What is an incident in the context of cybersecurity

A. Any observable occurrence in a network or system
B. A deliberate security incident in which an intruder gains access to a system or system resource without authorization
C. A particular attack that exploits system vulnerabilities
D. An event that actually or potentially jeopardizes the confidentiality integrity or availability of an information system.

Answer: D

NEW QUESTION 59
Which element of the security policy framework includes recommendation that are NOT bindings?

A. Procedures
B. Guidelines
C. Standards
D. Policies

Answer: C

NEW QUESTION 64
A _____ creates an encrypted tunnel to protect your personal data and communications

A. HTTPS
B. VPN
C. Anti-virus
D. IDS

Answer: B

NEW QUESTION 67
The common term used to describe the mechanisms that control the temperature and humidity in a data center

A. VLAN (virtual local area network)
B. STAT (system temperature and timing)
C. TAWC (temperature and water control)
D. HVAC (heating, ventilation and air conditioning)

Answer: D

NEW QUESTION 71
Finance Server and Transactions Server has restored its original facility after a disaster, what should be moved in FIRST?

A. Management
B. Most critical systems
C. Most critical functions
D. Least critical functions

Answer: D

NEW QUESTION 73
What is the range of well known ports

A. 0 - 1023
B. 1023-49151
C. 49152 - 65535
D. None

Answer: A

NEW QUESTION 74
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 78
The documentation of a predetermined set of instructions or procedures to detect, respond to andlimit consequences of a malicious cyberattack against an organization's information systems(s).

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

Answer: B

NEW QUESTION 81
Port forwarding is also known as

A. Port mapping
B. Tunneling
C. Punch through
D. ALL

Answer: D

NEW QUESTION 82
Which of the following is endpint

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

Answer: C

NEW QUESTION 86
Which of the following is a subject?

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

Answer: D

NEW QUESTION 91
What is the best practise to clear SSD storage after usage in term of cyber security

A. Zero fill
B. Degaussing
C. Clearing
D. Disintegration

Answer: D

NEW QUESTION 94
In information systems terms, the activities necessary to restore IT and communications services of an organization during and after an outage

A. IR
B. BC
C. Risk Management
D. DR

Answer: D

NEW QUESTION 96
What security feature used in HTTPS

A. IPSec
B. SSH
C. ICMP
D. SSL/TLS

Answer: D

NEW QUESTION 101
which is the short form of IPv6 address 2001:0db8:0000:0000:0000:ffff:0000:0001

A. 2001:db8::ffff:0:1
B. 2001:db8:0000:ffff:0:1
C. 2001:db80::ffff:0000:1
D. 2001:db8::ffff:0000:0001

Answer: A

NEW QUESTION 102
The primary functionality of PAM is?

A. Validate the level of access a user have to a file
B. Prevent unauthorized access to organizational assets
C. Provide just-in-time access to critical resources
D. Manage centralized access control

Answer: C

NEW QUESTION 105
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 108
Which Prevents Threat

A. Antivirus
B. IDS
C. SIEM
D. HIDS

Answer: A

NEW QUESTION 113
Which of the following attacks can TLS help mitigate?

A. Cross-site Scripting (XSS) Attacks
B. Social Engineering Attacks
C. Man-in-the-middle (MiTm) Attacks (Correct)
D. SQL Injection Attacks

Answer: C

NEW QUESTION 117
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 121
In what way do a victim's files get affected by ransomware?

A. By destroying them
B. By encrypting them
C. By stealing them
D. By selling them

Answer: B

NEW QUESTION 124
Which of the following is a type of risk that involves the unauthorized use or disclosure of confidential information such as passwords, financial data or personal information?

A. Compliance risk
B. Reputatuinal risk
C. Operational risk
D. Information risk

Answer: D

NEW QUESTION 128
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 130
A structured approach used to oversee and manage risk for an enterprise

A. Risk Assessment
B. Risk threshold
C. Risk Management Framework
D. Risk appetite

Answer: C

NEW QUESTION 135
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 140
The magnitude of the harm expected as a result of the consequences of an unauthorized disclosure, modification, destruction or loss of information is known as

A. Threat
B. Vulnerability
C. Impact
D. Likelihood

Answer: C

NEW QUESTION 145
Which type of software testing focuses on examining the source code for vulnerabilities and security issues?

A. Black-box testing
B. White-box testing
C. Functional testing
D. User acceptance testing

Answer: B

NEW QUESTION 146
The means by which a threat actor carries out their objectives

A. Threat
B. Threat Vector
C. Exploit
D. Intrusion

Answer: B

NEW QUESTION 151
What is a threat in the context of cybersecurity

A. An inherent weakness or flaw in a system
B. Something in need of protection
C. The means by which a threat actor carries out their objectives
D. A person or thing that takes action to exploit a target organizations system vulnerabilities

Answer: D

NEW QUESTION 154
What is knowledge based authentication

A. Authentication based on a passphrase or secret code
B. Autheication based on a token or memory card
C. Authentication based on biometrics or measurble charestrisirtcs
D. Authencication based on something you do

Answer: A

NEW QUESTION 158
If a device is found that is not compliant with the security baseline, what will be the security team action

A. Report
B. Evaluate
C. Ignore
D. Disabled or isolated into a quarantine area until it can be checked and updated.

Answer: D

NEW QUESTION 159
What goal of security is enhanced by a strong business continuity program?

A. non-repudiation
B. Availability
C. Confidentiality
D. Integrity

Answer: B

NEW QUESTION 163
What is the primary factor in the reliability of information and system

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

Answer: C

NEW QUESTION 167
When responding to a security incident, your team determines that the vulnerability that was exploited was not widely known to the security community, and that there are no currently known definitions/listings in common vulnerability databases or collections. This vulnerability and exploit might be called _____

A. Malware
B. Zero-day
C. Event
D. Attack

Answer: B

NEW QUESTION 170
Which plan provides the team with immediate response procedures and check lists and guidance for management?

A. BCP

B. IRP
C. DRP
D. ALL

Answer: A

NEW QUESTION 172
The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards

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

Answer: C

NEW QUESTION 177
Organization experiences a security event that does not affect the confidentiality integrity and availability of its information system. What term BEST describes this situation?

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

Answer: D

NEW QUESTION 182
A portion of the organization's network that interfaces directly with the outside world; typically, this exposed area has more security controls and restrictions than the rest of the internal IT environment.

A. Virtual private network (VPN)
B. Virtual local area network (VLAN)
C. Zero Trust
D. Demilitarized zone (DMZ)

Answer: D

NEW QUESTION 185
What is the range of private ports

A. 0 - 1023
B. 1023-49151
C. 49152 - 65535
D. None

Answer: C

NEW QUESTION 187
A type of malware that is capable of self propagation and can infect multiple systems on network without the need for human intervention

A. Worm
B. Spy ware
C. Adwre
D. Virus

Answer: A

NEW QUESTION 188
What is the recommended range of temperature for optimized maximum uptime and hardware life in a data center?

A. 62 F to 69 F
B. 64 F to 81 F
C. 82 F to 90 F
D. 91 F to 100 F

Answer: B

NEW QUESTION 191
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 192
Which of the following best describes the puposes of a business impact analysis?

A. To document a predetermined set of instructions or procedures for restoring IT and communications services after a disruption
B. To mitigate security violation and ensure that business operation can continue during a contigency
C. To provide a high level overview of the disaster recovery plan
D. To analyze an information systems requirements and functions in order to determine system contingency priorities

Answer: D

NEW QUESTION 195
A company has implemented Mandatory access control for its confidential data which of the following statement is true

A. The data can be accessed by users who possess a need to know
B. Access controls cannot be changed by anyone except the system administrato
C. The owner of the data can modify the access control
D. The system adminstrator can change the access contrls

Answer: B

NEW QUESTION 196
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 198
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 201
An agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing- specific terms

A. Memorandum of Understanding
B. Memorandam on Agreement
C. SLA
D. AII

Answer: C

NEW QUESTION 202
A type of malware that downloads onto a computer disguised as a legitimate program

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

Answer: B

NEW QUESTION 204
The mitigation of violations of security policies and recommended practices

A. DR
B. IR
C. Threat hunting
D. Incident response

Answer: D

NEW QUESTION 207

What is a security token used to authenticate a user to a web application, typically after they log in?

A. Captcha
B. API key
C. CSRF token
D. Session token

Answer: D

NEW QUESTION 210
John was recently offered a consulting opportunity as a side job. He is concerned that this might constitute a conflict of interest. Which one of the following sources that he needs to refer to take an appropriate decision?

A. ISC2 Code of ethics
B. Organizational code of ethics
C. Country code of ethics
D. Organizational security policy

Answer: B

NEW QUESTION 212
Which of the following documents contains elements that are NOT mandatory

A. Procedures
B. Policies
C. Regulations
D. Guidelines

Answer: D

NEW QUESTION 215
DevOps team has updated the application source code, Tom has discovered that many unauthorized changes have been made. What is the BEST control Tom can implement to prevent a recurrence of this problem?

A. Backup
B. File labels
C. Security audit
D. Hashing

Answer: D

NEW QUESTION 219
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 221
Which type of attack will most effectively maintain remote access and control over the victims computer

A. Phising
B. Trojans
C. XSS
D. RootKits

Answer: D

NEW QUESTION 226
The Bell and LaPadula access control model is a form of

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

Answer: B

NEW QUESTION 231
A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

A. Availability
B. Criticality
C. Authorization
D. Confidentiality

Answer: B

NEW QUESTION 234
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 236
_____ 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 237
What does internal consistency of information refer to

A. Data being accurate, usefull and complete
B. Data being protected from errors or loss of information
C. All instances of data being identical in form content and meaning
D. Data being displayed and stored the same way on all system

Answer: C

NEW QUESTION 239
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 242
What is the main purpose of using digital signatures in communication security?

A. To encrypt sensitive data during transmission
B. To verify the identity of the sender and ensure the integrity of the message (Correct)
C. To prevent unauthorized access to a network
D. To compress data to reduce bandwidth usage

Answer: B

NEW QUESTION 244
What is the primary goal of Identity and Access Management (1AM) in cybersecurity?

A. To ensure 100% security against all threats
B. To provide secure and controlled access to resources
C. To eliminate the need for user authentication
D. To monitor network traffic for performance optimization

Answer: A

NEW QUESTION 247
What is the term used to denote the inherent set of privileges assigned to a user upon the creation of a new account?

A. Aggregation
B. Transitivity
C. Baseline
D. Entitlement

Answer: C

NEW QUESTION 252
Which type of authentication is something which you

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

Answer: C

NEW QUESTION 257
Which is related to Privacy

A. GDPR
B. FIPS
C. MOU
D. AII

Answer: D

NEW QUESTION 261
What is the process of verifying a users identity called?

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

Answer: B

NEW QUESTION 263
What is privacy in the context of Information Security?

A. Protecting data from unauthorized access
B. Ensuring data is accurate and unchanged
C. Making sure data is always accessible when needed.
D. Disclosed without their consent

Answer: A

NEW QUESTION 267
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 269
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 273
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 276

What is sensitivity in the context of confidentiality

A. The harm caused to externl stakeholders if information is disclosed or modified
B. The ability of information to be accessed only by authorized individuals
C. The need for protection assigned to information by its owner
D. The Health status of the individuals

Answer: C

NEW QUESTION 280
Which is the first step in the risk management process

A. Risk response
B. Risk mitigation
C. Risk identification
D. Risk assessment

Answer: C

NEW QUESTION 283
Which type of fire suppression system is more friendly to electronics

A. Carbon di Oxide based
B. Chemical based
C. Water based
D. Foam based

Answer: A

NEW QUESTION 285
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 287
The highest-level governance documents in an organization, usually approved and issued by management, usually to support a compliance initiative

A. Standard
B. Policy
C. Procedure
D. Laws or Regulations

Answer: B

NEW QUESTION 290
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 291
Permitting authorized access to information while protecting it from improper disclosure

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

Answer: B

NEW QUESTION 294
Malicious code that acts like a remotely controlled "robot" for an attacker, with other Trojan and worm capabilities.

A. Rootkit
B. Ma I ware
C. Bot

D. Virus

Answer: C

NEW QUESTION 298
Ignoring the risk and proceeding the business operations

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

Answer: A

NEW QUESTION 300
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 303
Which plan is activated when both the Incident response and BCP fails

A. Risk Management
B. BIA
C. DRP
D. None

Answer: C

NEW QUESTION 305
What is Remanence

A. The ability of retaining magnetization in storage disk after deletion
B. Files or pieces of files get scattered throughout your disks.
C. Data corruption due to disk failure
D. AII

Answer: A

NEW QUESTION 310
Which one of the following cryptographic algorithms does not depend upon the prime factorization problem?

A. RSA - Rivest-Shamir-Adleman
B. GPG - GNU Privacy Guard
C. ECC - Elliptic curve cryptosystem
D. PGP - Pretty Good Privacy

Answer: C

NEW QUESTION 315
A company data center has been breached by hackers and all its systems have been taken down what is the main objective of the DRP in such a scenario?

A. To relocate the data center to another location
B. To ensure the physical safety of employees in the data center
C. To investigate and prosecute the hackers responsible of the attack
D. To restore the IT systems to their last known state

Answer: D

NEW QUESTION 318
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 321
In incident terminology the Zero day is

A. Days with a cybersecurity incident
B. A previously unknown system vulnerability
C. Days without a cybersecurity incident
D. Days to solve a previously unknown system vulnerability

Answer: B

NEW QUESTION 323
A Hacker launched a specific attack to exploit a known system vulnerability. What term best describes this situation?

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

Answer: C

NEW QUESTION 325
Which protocol is used for secure email

A. POP3S
B. IMAPS
C. SMTPS
D. AII

Answer: D

NEW QUESTION 329
What does the term "Two-factor authentication" refer to in Cybersecurity?

A. Using two different antivirus programs
B. Verifying identity with two independent factors
C. Accessing two different networks simultaneously
D. Changing passwords every two weeks

Answer: B

NEW QUESTION 333
Which of the following does not normally influence an organization's retention policy for logs?

A. Laws
B. Corporate governance
C. Regulations
D. Audits

Answer: D

NEW QUESTION 338
The amount of risk, at a broad level, that an organization is willing to accept in pursuit of its strategic objectives.

A. Risk Assessment
B. Risk Transfer
C. Risk Appetite
D. Risk Management

Answer: C

NEW QUESTION 343
What is the primary purpose of a honeytoken in cybersecurity?

A. To lure and detect attackers
B. To encrypt sensitive data
C. To enhance network performance
D. To manage user access

Answer: A

NEW QUESTION 347
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 351
In which cloud model does the cloud customer have less responsibility over the infrastructure

A. FaaS
B. SaaS
C. laaS
D. PaaS

Answer: B

NEW QUESTION 356
Which of the following properties is not guaranteed by Digital signatures

A. Authentication
B. Confidentiality
C. Non-Repudiation
D. Integrity

Answer: B

NEW QUESTION 358
A collection of actions that must be followed in order to complete a task or process in accordance with a set of rules

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

Answer: B

NEW QUESTION 362
Why Red book is important in BCP

A. To have hard copy for easy access
B. Easy to carry and transfer
C. A hurricane hits, the power is out and all the facilities are compromised and there is no access to electronic backups
D. AII

Answer: C

NEW QUESTION 364
Which of the following is very likely to be used in a disaster recovery (DR) effort?

A. Guard dogs
B. Contract personnel
C. Data backups
D. Anti-malware solutions

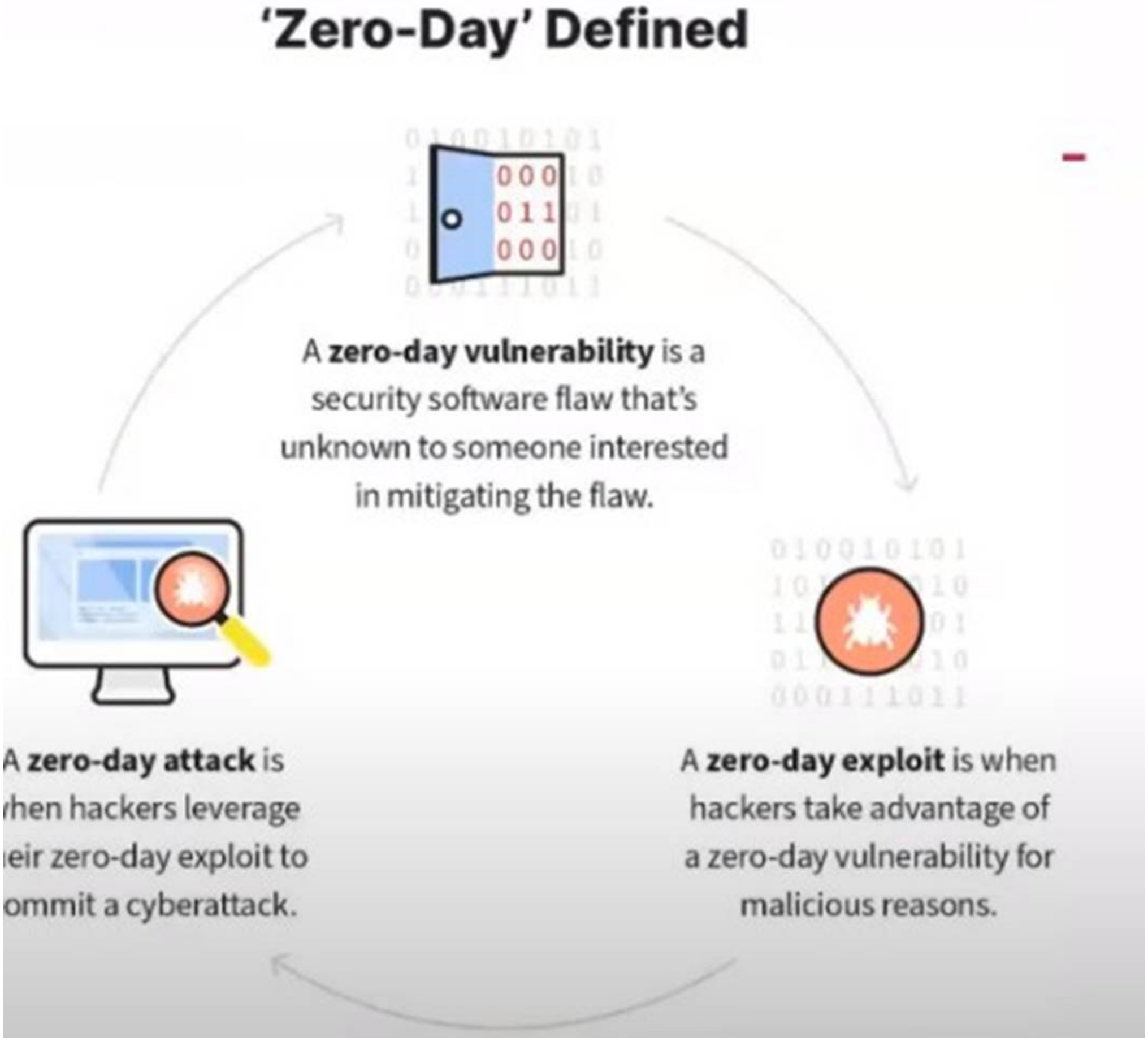
Answer: C

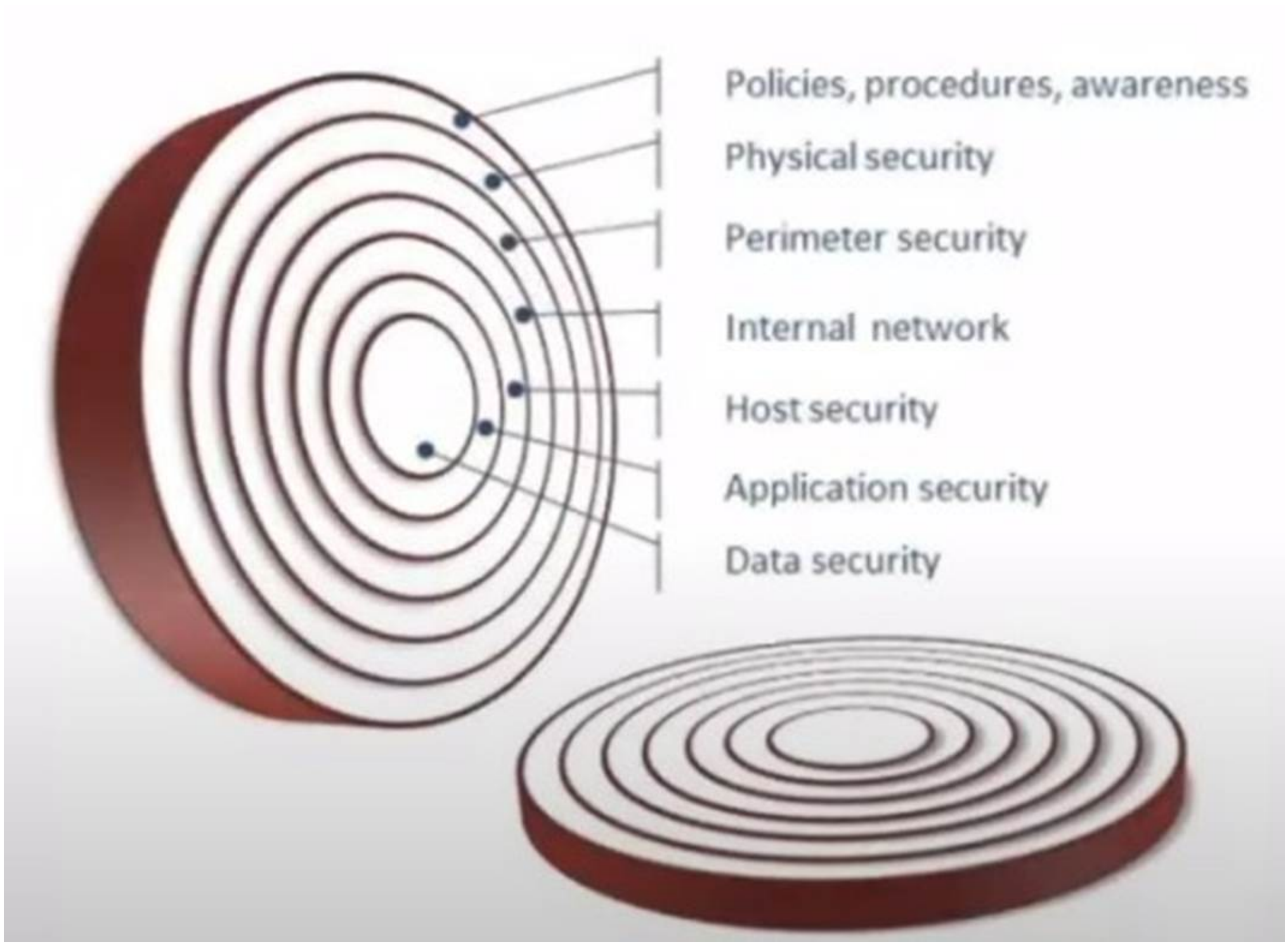
NEW QUESTION 369
What is the primary goal of a risk management process in cybersecurity?

A. to eliminate all cybersecurity risks
B. to transfer all cybersecurity risks to a third party
C. to identify, assess, and mitigate cybersecurity risks to an acceptable level (Correct)
D. to ignore cybersecurity risks and focus on incident response

Answer: C

NEW QUESTION 371
Exhibit.


'Zero-Day' Defined
000
011
000
A zero-day vulnerability is a security software flaw that's unknown to someone interested in mitigating the flaw.
A zero-day attack is when hackers leverage their zero-day exploit to commit a cyberattack.
A zero-day exploit is when hackers take advantage of a zero-day vulnerability for malicious reasons.



What kind of vulnerability is typically not identifiable through a standard vulnerability assessment?

A. File permissions
B. Buffer overflow
C. Zero-day vulnerability
D. Cross-site scripting

Answer: C

NEW QUESTION 376
Raj is considering a physical deterrent control to dissuade unauthorized people from entering the organization's property. Which of the following would serve this purpose?

A. A wall
B. Razor tape
C. A sign
D. A hidden camera

Answer: A

NEW QUESTION 381
Is the right of an individual to control the distribution of information about themselves

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

Answer: C

NEW QUESTION 382
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 387
What does the term business in business continuity planning refer to?

A. The financial performance of the organization
B. The technical systems of the organization
C. The operation aspects of the organization
D. The physical infrastructure of the organization

Answer: C

NEW QUESTION 388
The prevention of authorized access to resources or the delaying of time critical operations.

A. ARP Poisoning
B. Syn Flood
C. Denial-of-Service (DoS)
D. AII

Answer: C

NEW QUESTION 389
How do IT professionals differentiate between typical IT problems and security incidents?

A. By providing medical assistance at accident scenes
B. By collection evidence and reposting the incident
C. By receiving specific training on incident response
D. By participating in remediation and lessons learns stages

Answer: C

NEW QUESTION 392
Which is not possible models for an Incident Response Team (IRT):

A. Leveraged
B. Dedicated
C. Hybrid
D. Outsourced

Answer: D

NEW QUESTION 395
Uses multiple types of access controls in literal or theoretical layers to help an organization avoid a monolithic security

A. DMZ
B. VLAN
C. Defence in Depth
D. VPN

Answer: C

NEW QUESTION 399
A Company critical functions were disrupted due to a system outage. What plan should theorganization have in place to sustain these operations during and after a significant disruptions?

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

Answer: B

NEW QUESTION 400
A backup is which type for security control

A. Preventive
B. Deterrent
C. Recovery
D. Corrective

Answer: C

NEW QUESTION 402

Token Ring used in which OSI Layer

A. Application
B. Network
C. Transport
D. Physical

Answer: D

NEW QUESTION 404
Which device is used to control traffic flow in network

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

Answer: D

NEW QUESTION 409
.....

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