ISC2

Exam Questions CC

Certified in Cybersecurity (CC)

NEW QUESTION 1
Structured way to align IT with business goals while managing risks and meeting all industry and government regulations

A. GRC
B. Policies
C. Law
D. Stanfard

Answer: A

NEW QUESTION 2
What federal law requires the use of vulnerability scanning on information systems operated by federal government agencies?

A. FISMA
B. HIPAA
C. GLBA
D. FERPA

Answer: A

NEW QUESTION 3
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 4
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 5
What are registered port used for

A. Common protocols at the core of TCP/IP model
B. Used for web servers
C. Used for in housed or opensource applications
D. Proprietary applications from vendors and develope

Answer: D

NEW QUESTION 6
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 7
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 8

Common network device used to connect networks?

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

Answer: C

NEW QUESTION 9
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 10
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 10
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 12
255.255.255.0 Address represents

A. Broadcast
B. Unicast
C. Subnet mask
D. Global Address

Answer: C

NEW QUESTION 14
Requires that all instances of the data be identical in form,

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

Answer: C

NEW QUESTION 17
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 20
Example of Token based Authentication

A. Kerberos
B. Basic
C. OAuth

D. NTLN

Answer: C

NEW QUESTION 24
TCP and UDP reside at which layer of the osi model?

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

Answer: D

NEW QUESTION 27
Mark has purchased a MAC LAPTOP. He is scared of losing his screen and planning to buy an insurance policy. So, which risk management strategy is?

A. Risk acceptance
B. Risk deterrence
C. Risk transference
D. Risk mitigation

Answer: C

NEW QUESTION 31
Which OSI layer VPN works

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

Answer: D

NEW QUESTION 36
A popular way of implementing "least privilege"

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

Answer: C

NEW QUESTION 37
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 type of attack does the attacker store and reuse login information. Select the BEST answer?

A. Man-in-the-middle attack
B. Smurf attack
C. DDoS attack
D. Replay attack

Answer: D

NEW QUESTION 40
What is meant by non-repudiation?

A. If a user does something, they can't later claim that they didn't do it.
B. Controls to protect the organization's reputation from harm due to inappropriate social media postings by employees, even if on their private accounts and personal time.
C. It is part of the rules set by administrative controls.
D. It is a security feature that prevents session replay attacks.

Answer: A

NEW QUESTION 43
Which is the Not the component of a Business Continuity (BC) plan

A. Immediate response procedures and checklists
B. Notification systems and call trees for alerting personnel
C. Guidance for management, including designation of authority for specific managers
D. Manacomont

Answer: D

NEW QUESTION 45
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 49
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 52
DNS works in which OSI layer

A. Physical Layer
B. Network Layer
C. Application layer
D. DataLink Layer

Answer: C

NEW QUESTION 57
A company wants to ensure that its employees can evacuate the building in case of an emergency which physical control is best suited for this scenario

A. Fire Alarms
B. Exit signs
C. Emergency lighting
D. Emergency exit doors

Answer: D

NEW QUESTION 59
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 62
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 66
Which one of the following controls is not particularly effective against the insider threat?

A. Least privilege
B. Background checks

C. Firewalls
D. Separation of duties

Answer: C

NEW QUESTION 68
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 73
Which type of attack takes advantage of vulnerabilities in validation?

A. ARP spoofing
B. Pharming attacks
C. Cross-site scripting (XSS)
D. DNS poisoning

Answer: C

NEW QUESTION 78
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 82
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 85
Scans networks to determine everything that is connected as well as other information.

A. Burbsuite
B. Wireshark
C. Fiddler
D. Zen Mao

Answer: D

NEW QUESTION 86
What is a type of system architecture where a single instance can serve multiple distinct user groups.

A. Mutli-threading
B. Multi-processing
C. Multitenancy
D. Multi-cloud

Answer: C

NEW QUESTION 88
Are a measure of an organization's baseline of security performance

A. Security Assessment
B. Secuirty Audit
C. Security Benchmark
D. Security Management

Answer: C

NEW QUESTION 91
What is the range of well known ports

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

Answer: A

NEW QUESTION 94
After an Earthquake disrupting business operations, which documents contains the reactive procedures required to return business to normal operations

A. The Business Impact Analysis
B. The Business Continuity Plan
C. The Disaster Recovery plan
D. The Business Impact Plan

Answer: C

NEW QUESTION 98
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 103
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 107
Faking the sending address of a transmission to gain illegal entry into a secure system.

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

Answer: C

NEW QUESTION 109
Port forwarding is also known as

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

Answer: D

NEW QUESTION 112
Which TLS extension is used to optimize the TLS handshake process by reducing the number of round trips between the client and server?

A. TLS Renegotiation
B. TLS Heartbeat
C. TLS Session Resumption
D. TLS FastTrack

Answer: C

NEW QUESTION 117
Which of the following is a subject?

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

Answer: D

NEW QUESTION 120
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 125
What is the difference between business continuity planning and disaster recovery planning?

A. Business continuity planning is abount restoring IT and communincations back to full operations after a dustruption, while disaster recovery planning is about maintaining criticla business functions
B. Disaster recovery planning is about restoring IT and communications back to full operations after a disruption, while business continuity planning is about maintaining critical business functions
C. Business continuity planning and disaster recovery planning are the same thisg
D. Business continuity planning is about maintainig criticla business funtions before disasteroccurs

Answer: B

NEW QUESTION 128
The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

A. DDOS
B. Authetication
C. Authentication
D. Availablity

Answer: A

NEW QUESTION 131
Which version of TLS is considered to be the most secure and recommended for use?

A. TLS 1.0
B. TLS 1.1
C. TLS 1.2
D. TLS 1.3

Answer: D

NEW QUESTION 132
What does Personally Identifiable Information (Pll) pertain to?

A. Information about an individual's health status
B. Data about an individual that could be used to identify them (Correct)
C. Trade secrets, research, business plans and intellectual property
D. The importance assigned to information by its owner

Answer: B

NEW QUESTION 135
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 140
What security feature used in HTTPS

A. IPSec
B. SSH

C. ICMP
D. SSL/TLS

Answer: D

NEW QUESTION 141
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 145
Difference between Sniffing and Snooping

A. Sniffing is the process of intercepting and collecting network traffic as it passes over a digital networ
B. Spoofing is the act of disguising a communication from an unknown source as being trustworthy.
C. Snooping is the process of intercepting and collecting network traffic as it passes over a digital networ
D. Sniffing is the act of disguising a communication from an unknown source as being trustworthy.
E. Both are same
F. Sniffing is not thread and snoofing is a thread

Answer: A

NEW QUESTION 147
What does Criticality represents?

A. The need for consultation with the involved business ensure critical systems are identified and available
B. The importance an organization gives to data or an information system in performing its operations or achieving its mission
C. The need for security professional to ensure the appropriate levels of availavility are provided
D. All of the above

Answer: B

NEW QUESTION 150
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 151
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 154
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 158
A company needs to protect its confidential data from unauthorized access which logical control is best suited for this scenario

A. Encryption
B. Firewall
C. Antivirus
D. Hashing

Answer: A

NEW QUESTION 162
6 Which access control method uses attributes and rules to define access policies that are evaluate by a central Policy Decision Point (PDP)

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

Answer: D

NEW QUESTION 165
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 168
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 171
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 172
Which is the component of a Business Continuity (BC) plan

A. Immediate response procedures and checklists
B. Notification systems and call trees for alerting personnel
C. Guidance for management, including designation of authority for specific managers
D. ALL

Answer: D

NEW QUESTION 175
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 179
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 180
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 182
Which of the following uses registered port

A. HTTP
B. SMB
C. TCP
D. MS Sql server

Answer: D

NEW QUESTION 186
Which of the following is a characteristic of cloud

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

Answer: B

NEW QUESTION 189
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 193
Which of the following is not a source of redundant power

A. Generator
B. Utility
C. UPS
D. HVAC

Answer: D

NEW QUESTION 197
Which of these tool is commonly used to crack passwords

A. Bup Suite
B. Nslookup
C. Wireshark
D. John the ripper

Answer: D

NEW QUESTION 198
Which of the following security controls is designed to prevent unauthorized access to sensitive information by ensuring that it is only accessible to authorized users?

A. Encryption
B. Firewall
C. Antivirus
D. Access control

Answer: D

NEW QUESTION 202
The requirement of both the manager and the accountant to approve the transaction fund exceeding $ 50000. Which security concept best suits this

A. MAC
B. Defence in Depth
C. Two Person integrity
D. Principle of least privilege

Answer: C

NEW QUESTION 207
Created by switches to logically segment a network without altering its physical topology.

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

Answer: C

NEW QUESTION 209
What does a breach refer to in the context of cybersecurity

A. An unauthorized access to a system or system recours
B. Any observable occurance in a network or system
C. A deiberate security incident
D. A previously know system vulnerablity

Answer: A

NEW QUESTION 210
Removing the design belief that the network has any trusted space. Security is managed at eachpossible level, representing the most granular asset. Micro segmentation of workloads is a tool of the model.

A. Zero Trust
B. DMZ
C. VLAN
D. Micro Segmentation

Answer: A

NEW QUESTION 213
Who should participate in creating a BCP

A. Only members from the IT department
B. Only members from the management team
C. Members from across the organization
D. Only members from the finanace department

Answer: C

NEW QUESTION 218
Which type of encryption uses only one shared key to encrypt and decrypt?

A. Public key
B. Asymmetric
C. Symmetric
D. TCB key

Answer: C

NEW QUESTION 219
Type of cyber attack carried out over a LAN that involves sending malicious packets to a default gateway on a LAN

A. ARP Poisoning
B. Syn Flood
C. Ping of death
D. Trojan

Answer: A

NEW QUESTION 224
Hashing used to safe guard which CIA triad

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

Answer: C

NEW QUESTION 228

Which maintains that a user or entity should only have access to the spec data, resources and applications needed to complete a required task.

A. Zero Trust
B. Defence in Depth
C. Least Privileges
D. AII

Answer: C

NEW QUESTION 231
Which phase of the access control process(AAA) does a user prove his/her identity?

A. Authentication
B. Authorization
C. Identification
D. Accounting

Answer: A

NEW QUESTION 233
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 236
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. Administrative Access control

Answer: A

NEW QUESTION 237
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 238
Security control used to protect against environmental threats such as fire, flood and earth quakes

A. Physical control
B. Logical Control
C. Adminstrative Control
D. Thechnical control

Answer: A

NEW QUESTION 242
How does IPSec protect against reply attacks

A. By using sequence numbers
B. By limiting access to the network
C. By using digital signatures
D. By encryption all network traffic

Answer: A

NEW QUESTION 246
Which is the SSH port

A. 21
B. 23
C. 24

D. 22

Answer: D

NEW QUESTION 250
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 252
How often should an organization test its business continuity plan

A. Continually
B. Annually
C. Routinely
D. Daily

Answer: C

NEW QUESTION 255
What is the range of private ports

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

Answer: C

NEW QUESTION 259
Selvaa presents a userid and a password to a system in order to log on. Which of the following characteristics must the userid have?

A. Autherization
B. Authentication
C. Availability
D. Identification

Answer: D

NEW QUESTION 264
Which access control model grants permission based on the sensitivity of the data and the user job functions

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

Answer: B

NEW QUESTION 269
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 272
Which of the following cloud service models provides the most suitable environment for customers to build and operate their own software?

A. SaaS
B. laaS
C. PaaS

Answer: A

NEW QUESTION 276

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 279
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 282
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 286
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 291
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 293
The mitigation of violations of security policies and recommended practices

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

Answer: D

NEW QUESTION 297
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 300
Which of the following documents contains elements that are NOT mandatory

A. Procedures

B. Policies
C. Regulations
D. Guidelines

Answer: D

NEW QUESTION 303
What is the benefit of subnet

A. By increasing network bandwidth
B. By improving network security
C. By reducing network congestion
D. By simplifying network management

Answer: C

NEW QUESTION 306
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 308
are events that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed

A. Exploit
B. Security Incident
C. Threat
D. Rreach

Answer: B

NEW QUESTION 311
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 314
Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.

A. BC
B. DR
C. IR
D. AII

Answer: A

NEW QUESTION 318
Which of the following is often associated with DR planning?

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

Answer: D

NEW QUESTION 323
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 327
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 330
Which layer of the OSI layer model is responsible for associate MAC addresses to network devices

A. Physical layer
B. Network layer C Data link layer
C. Transport layer

Answer: C

NEW QUESTION 333
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 336
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 341
Which of the following best describes the type of technology the team should implement to increase the work effort of buffer overflow attacks?

A. Address space layout randomization
B. Memory induction application
C. Input memory isolation
D. Read-only memory integrity checks

Answer: A

NEW QUESTION 346
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 347
Which of the following types of vulnerabilities cannot be discovered in the course of a routine vulnerability assessment?

A. Zero-day vulnerability
B. Kernel flaw
C. Buffer overflow
D. File and directory permissions

Answer: A

NEW QUESTION 350
Which type of authentication is something which you

A. Type1
B. Type 2

C. Type 3
D. Type 4

Answer: C

NEW QUESTION 355
Why is the recovery of IT often crucial to the recovery and sustainment of business operations

A. IT is not important to business operation
B. IT often the cause for the disaster
C. IT can be easily recovers without any impact of business operations
D. Many business rely heavily on IT for their operations

Answer: D

NEW QUESTION 359
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 363
Exhibit.

Symmetric Encryption	Asymmetric Encryption
• Symmetric encryption consists of one key for encryption and decryption.	• Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**.
• Symmetric Encryption is a lot quicker compared to the Asymmetric method.	• As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably.
• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

How many keys would be required to support 50 users in an asymmetric cryptography system?

A. 100
B. 200
C. 50
D. 1225

Answer: A

NEW QUESTION 366
An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available.

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

Answer: B

NEW QUESTION 370
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 374
Which is strongly used for Securing Wi-Fi

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

Answer: A

NEW QUESTION 378
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 380
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 384
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 388
The purpose of risk identification:

A. Employees at all levels of the organization are responsible for identifying risk.
B. Identify risk to communicate it clearly.
C. Identify risk to protect against it.
D. ALL

Answer: D

NEW QUESTION 390
True or False? The IT department is responsible for creating the organization's business continuity plan

A. True
B. False

Answer: B

NEW QUESTION 393
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 396
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 397
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 401
What is the purpose of multi-factor authentication (MFA) in 1AM?

A. To simplify user access
B. To eliminate the need for authentication
C. To add an additional layer of security by requiring multiple forms of verification
D. To grant unrestricted access to all users

Answer: C

NEW QUESTION 403
What kind of control is, when we add a backup firewall that takes over if the main one stops working?

A. Clustering
B. High availability(HA)
C. Load balancing
D. Component redundancy

Answer: B

NEW QUESTION 404
John joined the ISC2 Organizations, his manager asked to check the authentications in security module. What would John use to ensure a certain control is working as he want and expect it to?

A. Security Testing
B. Security assessment
C. Security audit
D. Security walkthrough

Answer: A

NEW QUESTION 405
What cybersecurity principle focuses on granting users only the privileges necessary to perform their job functions?

A. Least privilege (Correct)
B. defense in depth
C. separation of duties
D. need-to-know basis

Answer: A

NEW QUESTION 407
Permitting authorized access to information while protecting it from improper disclosure

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

Answer: B

NEW QUESTION 411
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 414
Ignoring the risk and proceeding the business operations

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

Answer: A

NEW QUESTION 418
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 419
What should been done to limit the damage caused by the ransomware attack

A. Use a different email client to prevent malicious attachments
B. Add more Administrative users to the Domain Admins group
C. Delete all emails with attachments
D. Limit the use of administrative privileges to only when required

Answer: D

NEW QUESTION 420
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 425
A security event, or combination of security events, that constitutes a secu incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization

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

Answer: A

NEW QUESTION 430
Which access control model can grant access to a given object based on complex rules

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

Answer: A

NEW QUESTION 431
An attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant

A. Eavesdropping Attack

B. CSRF
C. XSS
D. ARP Spoofing

Answer: A

NEW QUESTION 432
Which type of control is used to restore systems or processes to their normal state after an attack has occurred

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

Answer: D

NEW QUESTION 436
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 439
Who should participate in creation a business continuity plan

A. Onlymembersfrom the management team
B. only members from the IT department
C. Onlymembersfrom thefinancedepartment
D. Members from across the organization

Answer: D

NEW QUESTION 442
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 443
What are the primary responsibilities of a computer incident response team (CIRT) during an incident?

A. To determine the difference between minor and major incident
B. To troubleshoot network and system issues
C. To provide medical assistance at accident scenes
D. To asses the amount and scope of damage caused by the incident

Answer: D

NEW QUESTION 444
The process of applying secure configurations (to reduce the attack surface)

A. Security Assessment
B. Security Evaluation
C. Security Benchmark
D. Security Hardening

Answer: D

NEW QUESTION 445
What is the primary goal of implementing input validation in application security?

A. To ensure all inputs are stored in a secure database
B. To prevent unauthorized access to the application
C. To validate and sanitize user inputs to prevent code injection attacks (Correct)
D. To encrypt sensitive data transmitted between the client and server

Answer: C

NEW QUESTION 450
Which is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target

A. MITRE ATT&CK
B. CVE
C. Risk Management framework
D. Security Management

Answer: A

NEW QUESTION 454
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 457
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 459
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 461
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 464
Walmart has large ecommerce presence in world. Which of these solutions would ensure the LOWEST possible latency for their customers using their services?

A. CDN
B. SaaS
C. Load Balancing
D. Decentralized Data Centers

Answer: A

NEW QUESTION 466
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 471
Set of rules that everyone must comply with and usually carry monetary penalties for noncompliance

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

Answer: A

NEW QUESTION 472
Provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient.

A. Hashing
B. Encoding
C. Cryptography
D. AII

Answer: C

NEW QUESTION 473
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 475
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 479
Which of the following properties is not guaranteed by Digital signatures

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

Answer: B

NEW QUESTION 480
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 485
A company's governing board may agree that legal services will examine any third-party contracts, so they create a _____ stating that aside from legal services, no other department in the companvhahppn pivpn nprmkcinn to review third-party contracts

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

Answer: B

NEW QUESTION 488
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 489
Load balancing safe guard which CIA triad

A. Confidentiality
B. Availablity
C. Integrity
D. All

Answer: B

NEW QUESTION 490
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 communication system back to full operations after the disruptions.
D. Guiding the actions of emergency response personnel during the disruption

Answer: C

NEW QUESTION 494
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

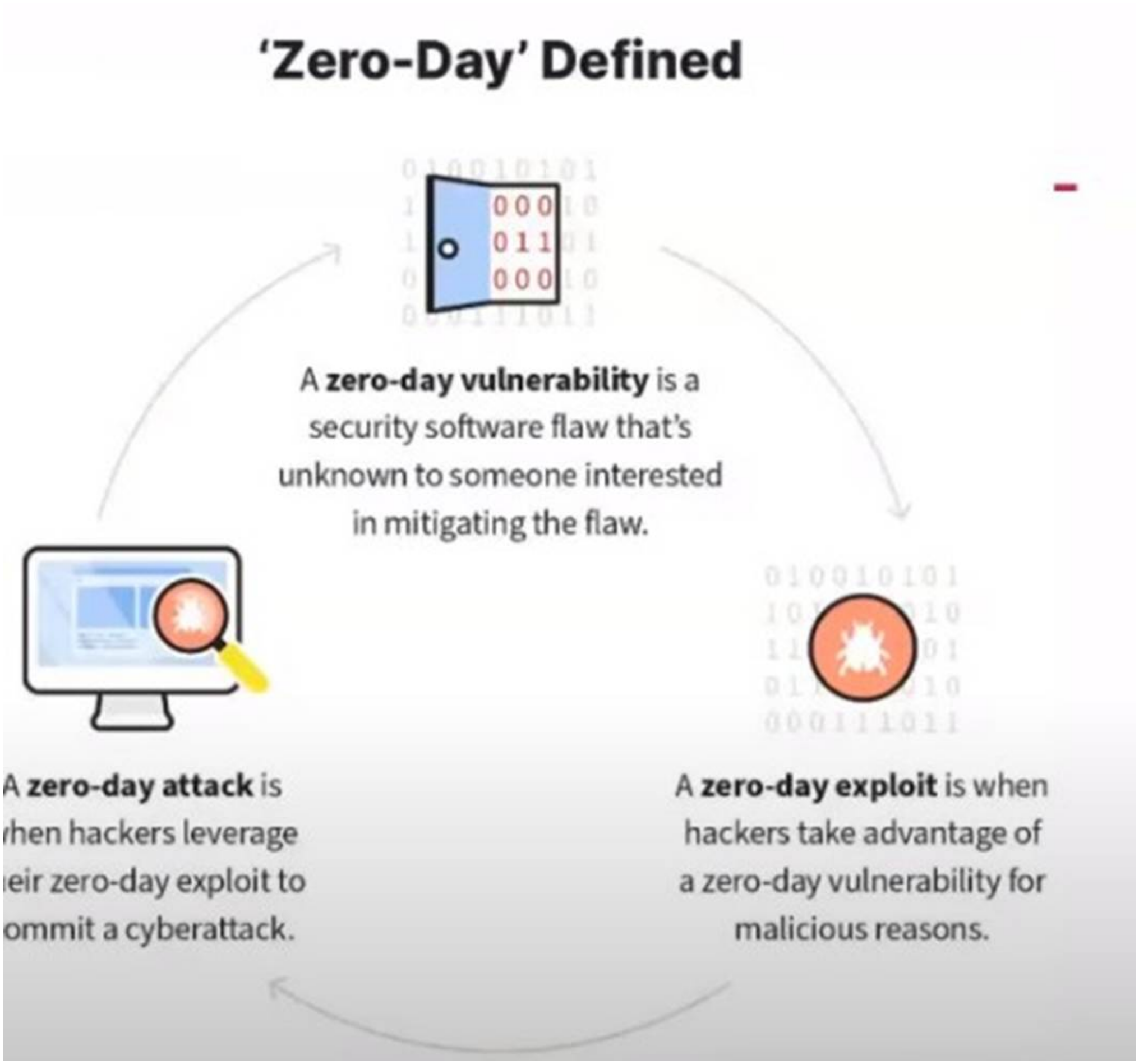
Answer: A

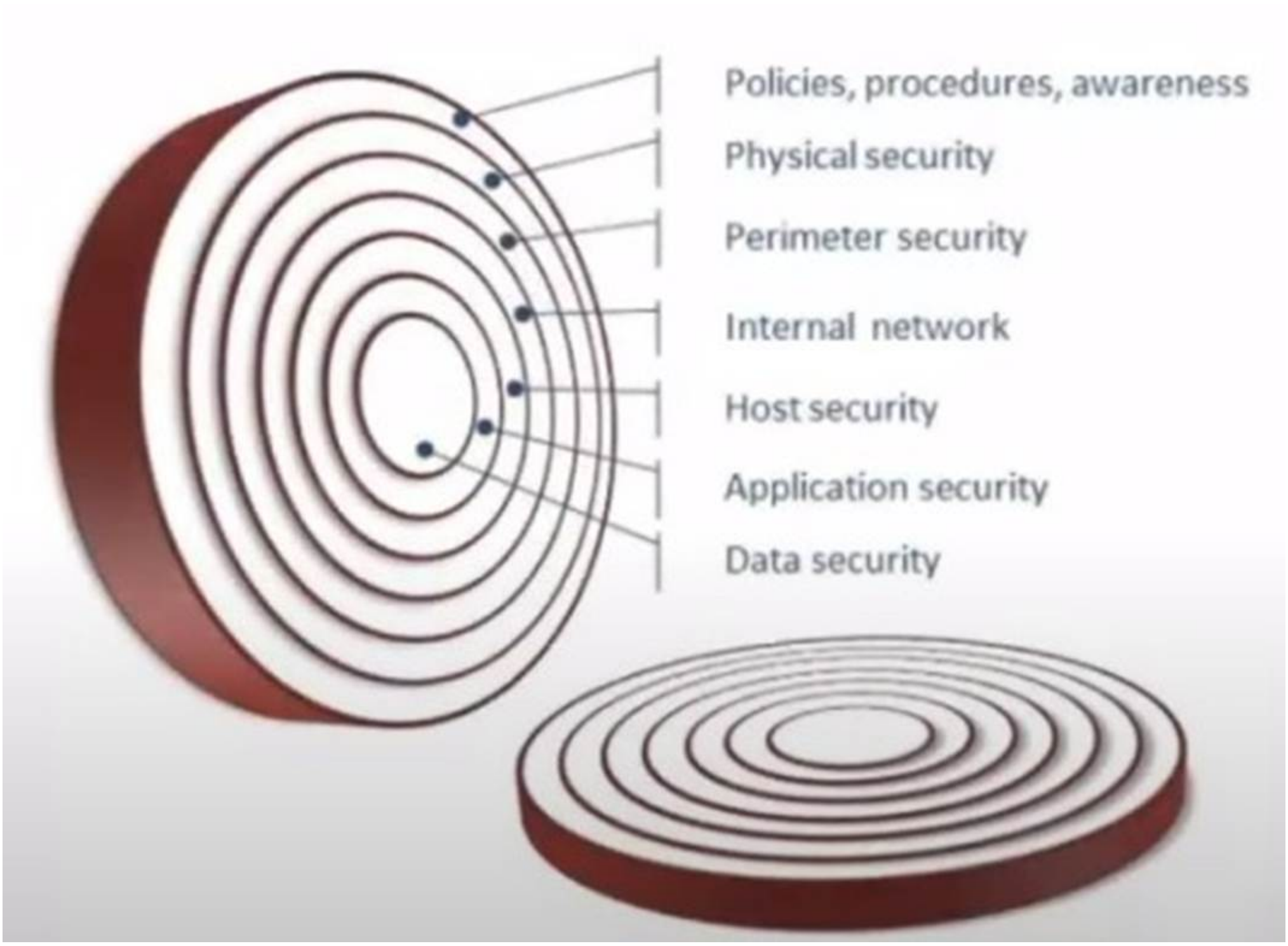
NEW QUESTION 498
What does the concept of integrity applied to

A. Organization
B. Information system and processes for business operations
C. People
D. ALL

Answer: D

NEW QUESTION 500
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 503
Risk tolerance also known as

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

Answer: D

NEW QUESTION 505
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 509
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 511
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 516
Which of these is the most efficient and effective way to test a business continuity plan

A. Simulations
B. Discussions
C. Walkthroughs
D. Reviews

Answer: A

NEW QUESTION 520
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 521
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 522
Port scanning attack target which OSI layer

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

Answer: A

NEW QUESTION 524
Which is not possible models for an Incident Response Team (IRT):

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

Answer: D

NEW QUESTION 526
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 531
What is the purpose of the post incident phase of incident response?

A. To detect and analyze incidents
B. To prepare for future incidents
C. To document lessons learned and improve future incident response effectiveness
D. To containment and eradicate incidents

Answer: C

NEW QUESTION 534
A hacker is trying to gain access to a company network which of the following scenarios would be an example of defense in depth

A. The company relies solely on a firewall to block unauthorized access
B. The company stores all sensitive data on a single server
C. The hacker is required to enter a username and password
D. None

Answer: C

NEW QUESTION 538
Four main components of Incident Response are

A. Preparation, Detection and Analysis, Containment, Eradication a
B. Preparation, Detection, Analysis and Containment
C. Detection, Analysis, Containment, Eradication and Recovery
D. AII

Answer: A

NEW QUESTION 541
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 544
A standard that defines wired communications of network devices

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

Answer: D

NEW QUESTION 549
Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data.

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

Answer: C

NEW QUESTION 553
Which of the following is unlikely to be a member of the disaster recovery team

A. Executive Management
B. Public Relations
C. Billing Clerk
D. IT personnel

Answer: C

NEW QUESTION 555
EKristal is the security administrator for a large online service provider. Kristal learns that the company is harvesting personal data of its customers and sharing the

data with local governments where the company operates, without the knowledge of the users, to allow the governments to persecute users on the basis of their political and philosophical beliefs. The published user agreement states that the company will not share personal user data with any entities without the users' explicit permission. According to the ISC2 Code of Ethics, to whom does Kristal ultimately report in this situation?

A. The company Kristal works for
B. The governments of the countries where the company operates
C. ISC2
D. The users

Answer: D

NEW QUESTION 559
A backup is which type for security control

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

Answer: C

NEW QUESTION 560
Token Ring used in which OSI Layer

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

Answer: D

NEW QUESTION 564
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 567
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CC Practice Exam Features:

* CC Questions and Answers Updated Frequently

* CC Practice Questions Verified by Expert Senior Certified Staff

* CC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year