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
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 3
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 4
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 5
Common network device used to connect networks?

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

Answer: C

NEW QUESTION 6
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 7
In Which of the following access control models can the creator of an object delegate permission

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

Answer: C

NEW QUESTION 8
Ping flood attack target which OSI layer

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

Answer: B

NEW QUESTION 9
255.255.255.0 Address represents

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

Answer: C

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

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

Answer: C

NEW QUESTION 13
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 14
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 17
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 19
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 20
Which OSI layer VPN works

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

Answer: D

NEW QUESTION 21
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 25
A popular way of implementing "least privilege"

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

Answer: C

NEW QUESTION 28
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 29
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 33
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 37
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 40

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 41
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 45
DNS works in which OSI layer

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

Answer: C

NEW QUESTION 49
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 50
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 51
Which of the following is a systematic approach to protecting against cyber threats that involves a continuous cycle of identifying, assessing and prioritizing risks and implementing measures to reduce or eliminate those risks?

A. Security Assessment
B. Incident response
C. Peneteration testing
D. Risk Management

Answer: D

NEW QUESTION 52
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 54
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 57
What is the range of well known ports

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

Answer: A

NEW QUESTION 58
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 62
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 63
Which layer does VLAN hopping belong to?

A. Layer 3
B. Layer 4
C. Layer 7
D. Layer 2

Answer: D

NEW QUESTION 66
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 67
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 69
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 74
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 78
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 80
What security feature used in HTTPS

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

Answer: D

NEW QUESTION 85
A cyber security professional observes an unusual occurrence in the network or system. What term best describes this situations

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

Answer: C

NEW QUESTION 90
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 93
Which Regulation addresses personal privacy

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

Answer: B

NEW QUESTION 96
While taking the certification exam for ISC2 CC, You notice another candidate for the certification cheating. What should you do?

A. Yell at the other candidate for violating test security.
B. Nothing—each person is responsible for their own actions.
C. Report the candidate to ISC2.
D. Call local law enforcement.

Answer: C

NEW QUESTION 97
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 98
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 103
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
Information should be consistently and readily accessible for authorized parties ?

A. Confidentiality
B. Authentication
C. Availability
D. Non-repudiation

Answer: C

NEW QUESTION 109
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 113
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 115
Dylan is creating a cloud architecture that requires connections between systems in two different private VPCs. What would be the best way for Dylan to enable this access?

A. VPN Connection
B. Internet Gateway
C. Public IP Address
D. VPC Endpoint

Answer: D

NEW QUESTION 117
Is defined as the process of identifying, estimating and prioritizing risks

A. Risk Assessment

B. Risk Treatment
C. Risk mitigation
D. Risk Management

Answer: A

NEW QUESTION 118
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 121
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 124
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 125
Which of the following is NOT one of the four typical ways of managing risk?

A. Accept
B. Avoid
C. Mitigate
D. Monitor

Answer: D

NEW QUESTION 127
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 129
Which of these is WEAKEST form of authentication we can implement?

A. Something you know
B. Something you are
C. Something you have
D. Biometric authentications

Answer: A

NEW QUESTION 132
When is the Business Continuity Plan Enacted?

A. When there is a event
B. When there is a incident
C. When there is a loss of business operations
D. When there is a natural disaster

Answer: C

NEW QUESTION 133
Which of the following is not a source of redundant power

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

Answer: D

NEW QUESTION 134
The means by which a threat actor carries out their objectives

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

Answer: B

NEW QUESTION 138
The method of distributing network traffic equally across a pool of resources that support an application

A. Vlan
B. DNS
C. VPN
D. Load Balancing

Answer: D

NEW QUESTION 143
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 145
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 148
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 149
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 153

How many bits represent the organization unique identifier (oui) in mac addresses?

A. 16 Bits
B. 48 Bits
C. 24 Bits
D. 32 Bits

Answer: C

NEW QUESTION 157
Which layer of OSI the Firewall works

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

Answer: D

NEW QUESTION 162
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 165
Communication between end systems is encrypted using a key, often known as _____?

A. Temporary Key
B. Section Key
C. Public Key
D. Session Key

Answer: D

NEW QUESTION 169
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 172
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 174
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 178
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 179
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 184
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 188
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 193
XenServer, LVM, Hyper-V, ESXi are

A. Type 2 Hypervisor
B. Type 1 Hypervisor
C. Both
D. None

Answer: B

NEW QUESTION 196
Which is the SSH port

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

Answer: D

NEW QUESTION 197
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 199
The process of running a simulated instances of a computer system in a layer abstracted from the underlying hardware server or workstation

A. Containerization
B. Simulation
C. Emulation
D. Virtualization

Answer: D

NEW QUESTION 201
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 205
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 207
Which Prevent crime by designing a physical environment that positively influences human behavior.

A. DMZ
B. Security Alarm
C. CPTED
D. CCTV

Answer: C

NEW QUESTION 209
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 211
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 212
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 217
Mark is configuring an automated data transfer between two hosts and is choosing an authentication technique for one host to connect to the other host. What approach would be best-suited for this scenario?

A. Biometric
B. Smart Card
C. SSH Key
D. Hard Coded Password

Answer: C

NEW QUESTION 218
Sending employees to work at a customer's home can open your business to more risk of bodily injury or property damage claims. So, to reduce risk and avoid potential losses, you decide not to offer those kinds of services

A. Risk Acceptance
B. Risk Assessment
C. Risk Avoidance
D. Risk Control

Answer: C

NEW QUESTION 222
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 227
The mitigation of violations of security policies and recommended practices

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

Answer: D

NEW QUESTION 231
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 235
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 239
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 241
Which of the following documents contains elements that are NOT mandatory

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

Answer: D

NEW QUESTION 244
Which encryption type used in HTTPS communication

A. Symentric
B. Assymentric
C. None

D. Both A and B

Answer: D

NEW QUESTION 248
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 249
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 252
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 254
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 257
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 260
The Bell and LaPadula access control model is a form of

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

Answer: B

NEW QUESTION 261
Which of the following is often associated with DR planning?

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

Answer: D

NEW QUESTION 262
Shaun is planning to protect their data in all states(Rest, Motion, use), defending against data leakage. What would be the BEST solution to implement?

A. End to end encryption.
B. Hashing
C. DLP
D. Threat Modeling

Answer: C

NEW QUESTION 263
Who must follow HIPAA Compliance

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

Answer: B

NEW QUESTION 266
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 268
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 269
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 272
A company security team detected a cyber attack against it information systems and activates a set of procedures to mitigate the attack., What type of plan is this?

A. Business continuty plan
B. Incident response plan
C. Disaster recvoery plan
D. Security operation plan

Answer: B

NEW QUESTION 273
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 274
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 278
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 280
Which of these is WEAKEST form of authentication we can implement?

A. Something you know
B. Something you are
C. Something you have
D. Biometric authentications

Answer: A

NEW QUESTION 284
Natalia is concerned that users on her network may be storing sensitive information, such as social security numbers, on their hard drives without proper authorization or security controls. What 3rd -party security service can she implement to best detect this activity?

A. IDS - Intrusion Detection System
B. IPS - Intrusion Prevention System
C. DLP - Data Loss Protection
D. TLS - Transport Layer Security

Answer: C

NEW QUESTION 289
Which is related to Privacy

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

Answer: D

NEW QUESTION 291
What is the process of verifying a users identity called?

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

Answer: B

NEW QUESTION 292
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 296
Which security control mostly used to prevent data breach

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

Answer: B

NEW QUESTION 299
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 303
Why is security training important?

A. Because it fulfills regulatory requirements.
B. Because it helps people to perform their job duties more efficiently.
C. Because it reduces the risk of certain types of attacks, like social engineering.
D. AII

Answer: C

NEW QUESTION 305
Restoring IT and communications back to full operation after a disruption.

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

Answer: C

NEW QUESTION 308
Which of these is an example of deterrent control

A. Biometric
B. Guard Dog
C. Encryption
D. Trunstile

Answer: B

NEW QUESTION 310
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 312
Granting a user access to services or the system

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

Answer: C

NEW QUESTION 313
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 314
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 316
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 319
Which protocol would be most suitable to fulfill the secure communication requirements between clients and the server for a company deploying a new application?

A. FTP
B. HTTP
C. HTTPS
D. SMTP

Answer: C

NEW QUESTION 321
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 322
When the ISC2 Mail server sends mail to other mail servers it becomes —?

A. SMTP Server
B. SMTP Peer
C. SMTP Master
D. SMTP Client

Answer: D

NEW QUESTION 324
Which type of attack attempts to gain information by observing the devices power consumption

A. DOS
B. Side Channles
C. XSS
D. XSRF

Answer: B

NEW QUESTION 329
Which of the following protocols is a secure alternative to using telnet?

A. SSH
B. HTTPS
C. SFTP
D. LDAPS

Answer: B

NEW QUESTION 334
Which of these activities is often associated with DR efforts?

A. Running anti-malware solutions
B. Scanning the IT environment for vulnerabilities
C. Zero-day exploits
D. Employees returning to the primary production location

Answer: D

NEW QUESTION 338
What is the purpose of immediate response procedures and checklists in a BCP

A. To notify personnel that the BCP is being enacted
B. To provide guidance for management
C. To safeguard the confidentiality, integrity and availability of information
D. To ensure business operations are accounted for in the plan

Answer: A

NEW QUESTION 342
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 344
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 347
Which of the following is the least secure communications protocol?

A. CHAP
B. Ipsec
C. PAP
D. EAP

Answer: C

NEW QUESTION 352
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 354
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 355
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 358
Permitting authorized access to information while protecting it from improper disclosure

A. Integrity

B. Confidentiality
C. Availability
D. ALL

Answer: B

NEW QUESTION 359
1 _____ is a weighted factor based on a subjective analysis of the probability that a given threat or set of threats is capable of exploiting a given vulnerability or set of vulnerabilities.

A. Likelihood of occurrence
B. Threat Vector
C. Risk
D. Impact

Answer: A

NEW QUESTION 360
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 362
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 365
A company experiences a power outage that causes a major disruption in its operations. What type of plan will help the company sustain operations?

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

Answer: C

NEW QUESTION 366
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 369
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 373
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 374
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 379
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 384
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 387
What is the primary goal of the incident management team in the organization

A. Reduce the impact and resore services
B. Gathering and analyzing information
C. Conducting Leason learn meeting
D. RCA of the impact

Answer: A

NEW QUESTION 390
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 393
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 396
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 398
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 402
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 407
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 408
Port used in DNS

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

Answer: A

NEW QUESTION 412
Dani is an ISC2 member and an employee of New Corporation. One of Dani's colleagues offers to share a file that contains an illicit copy of a newly released movie. What should Dani do

A. Inform ISC2
B. Inform law enforcement
C. Accept the movie
D. Refuse to accept

Answer: D

NEW QUESTION 416
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 417
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 419
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 423
A common network device used to filter traffic?

A. Server
B. Endpoint
C. Ethernet
D. Firewa

Answer: D

NEW QUESTION 424
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 426
Government can imposes financial penalties as a consequence of breaking a

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

Answer: B

NEW QUESTION 430
Which is not the function of IPS

A. To encrypt network traffic
B. To monitor network traffic
C. To filter network traffic
D. To detect and prevent attacks

Answer: A

NEW QUESTION 434
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 439
Which of the following is a common security measure to prevent Cross Site Scripting (XSS) attacks in web applications?

A. implementing strong password policies
B. using a firewall to block incoming traffic
C. validating and sanitizing user input (Correct)
D. encrypting data during transmission

Answer: C

NEW QUESTION 441
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 443
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 447
The DLP solution should be deployed so that it can inspect all forms of data leaving the organization, including:

A. Posting to web pages/websites
B. Applications/application programming interfaces (APIs)
C. Copy to portable media
D. AII

Answer: D

NEW QUESTION 448
Which ensure maintaining business operations during or after an incident

A. Incident Response
B. Business Continuity
C. Disaster Recovery
D. AII

Answer: C

NEW QUESTION 450
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 453
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 454
Load balancing safe guard which CIA triad

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

Answer: B

NEW QUESTION 459
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

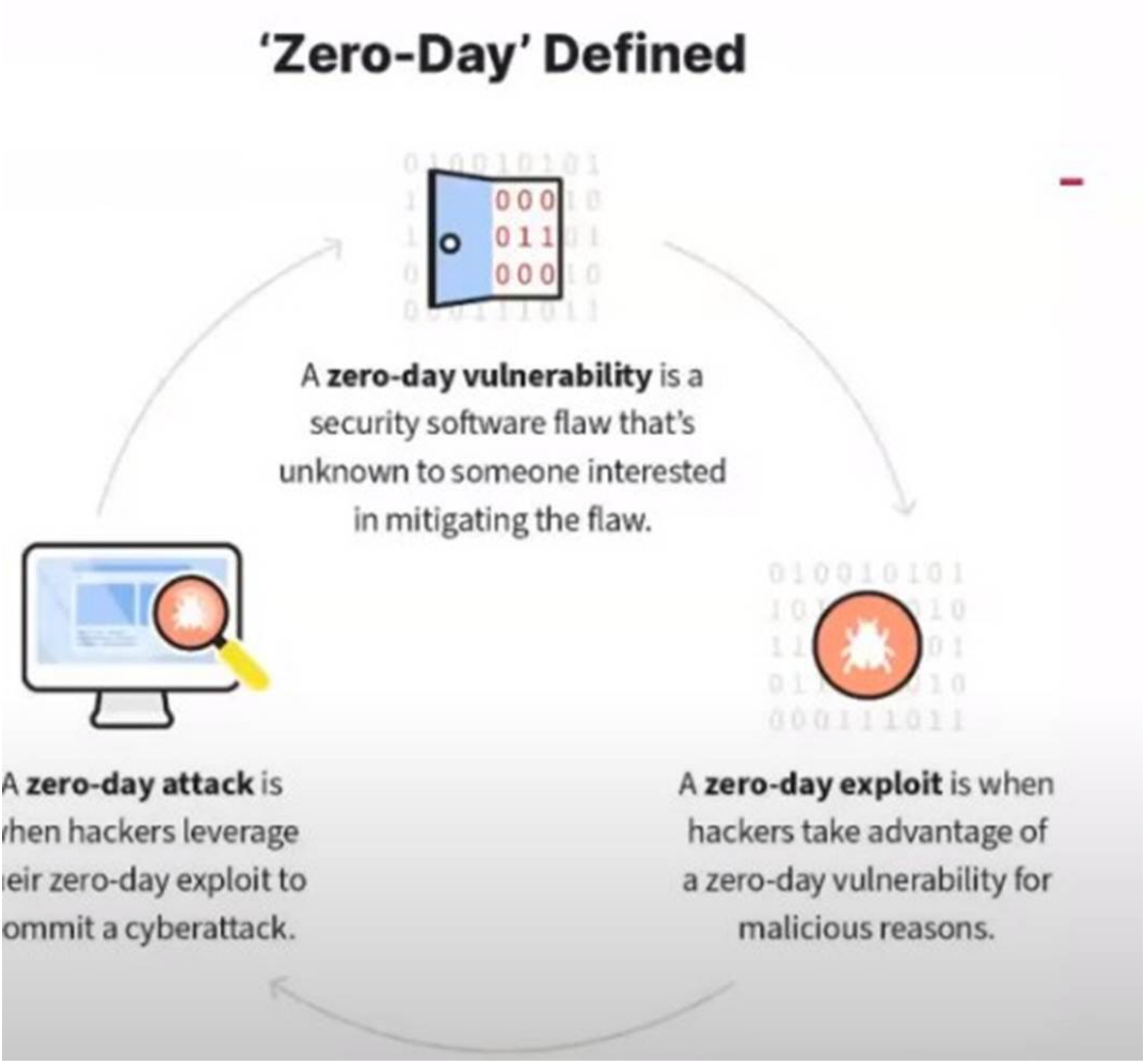
NEW QUESTION 463
Which authentication helps build relationships between different technology providers, enabling automatic identification and user access. Employees no longer

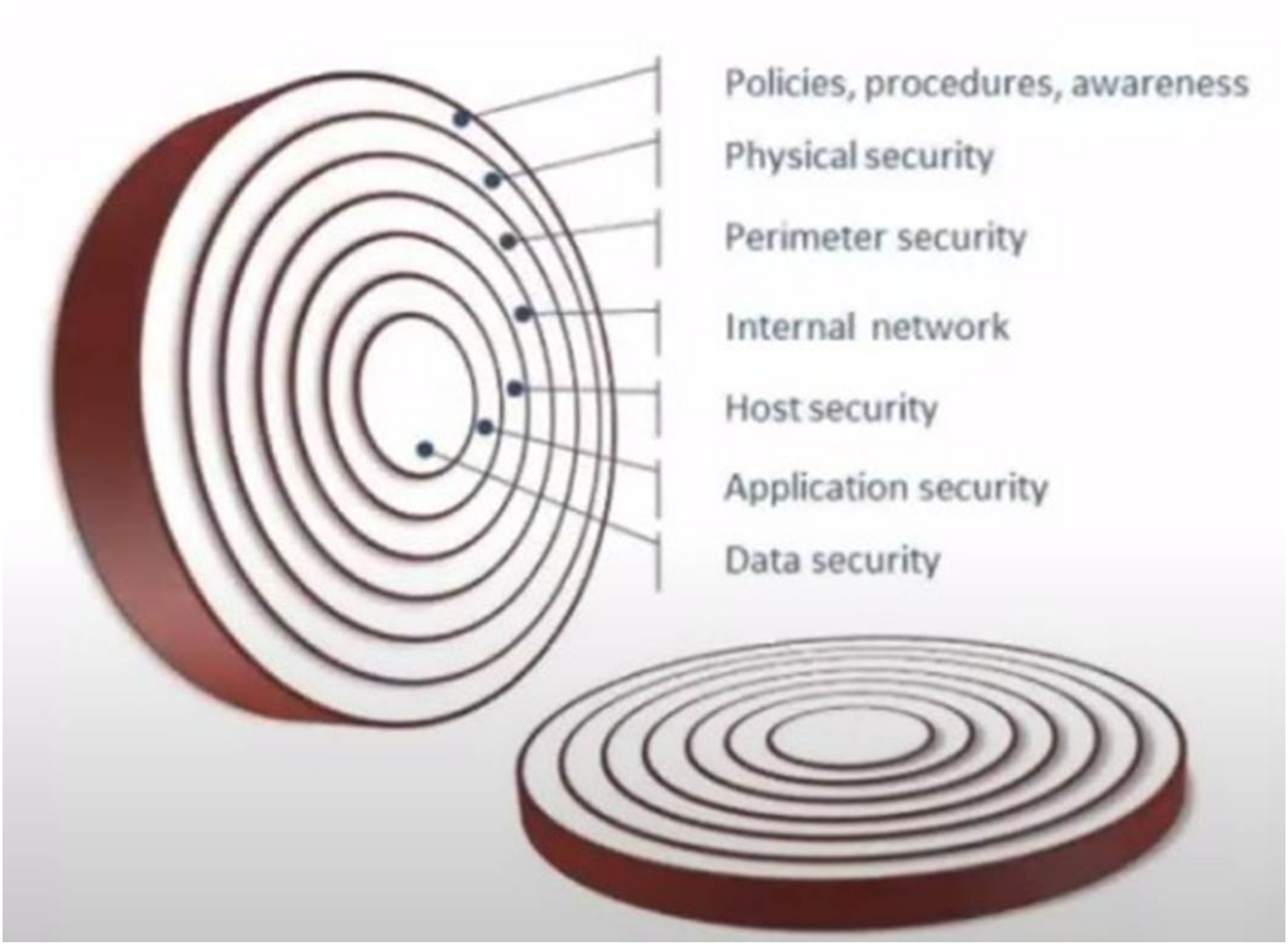
need to enter separate usernames and passwords when visiting a new service provider

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

Answer: D

NEW QUESTION 466
Exhibit.





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 470
The Order of controls used in Defence in Depth

A. Assests, Physical control
B. Administrative Controls, Logical/Techincal Controls
C. Assests, Administrative Controls, Physical controls, Logical/Techincal Controls
D. Physical control
E. Administrative Controls, Logical/Techincal Controls, Assests
F. Assests, Administrative Controls, Logical/Techincal Controls, Physical controls

Answer: D

NEW QUESTION 475
Risk tolerance also known as

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

Answer: D

NEW QUESTION 477
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 481
DDOS attack affect which OSI layer

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

Answer: D

NEW QUESTION 485
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 490
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 491
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 493
Port scanning attack target which OSI layer

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

Answer: A

NEW QUESTION 498
Which is not possible models for an Incident Response Team (IRT):

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

Answer: D

NEW QUESTION 503
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 507
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 508
A standard that defines wired communications of network devices

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

Answer: D

NEW QUESTION 511
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 512
The harmonization of automated computing tasks, providing a consolidated and reusable workflow

A. Cloud Orchestration
B. Cloud Manager
C. Cloud broker
D. Cloud Controller

Answer: A

NEW QUESTION 514
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 516
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 520
.....

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