ISC2

Exam Questions CC

Certified in Cybersecurity (CC)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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 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
4 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 4
Faking the sender address in a transmission to gain illegal entry into a secure system

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

Answer: C

NEW QUESTION 5
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
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 7
Common network device used to connect networks?

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

Answer: C

NEW QUESTION 8

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 9
Part of a zero-trust strategy that breaks LANs into very small and highly localized zones using firewalls.

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

Answer: D

NEW QUESTION 10
An entity that acts to exploit a target organizations system vulnerabilities is a

A. Attacker
B. Threat vector
C. Threat
D. Threat Actor

Answer: D

NEW QUESTION 10
255.255.255.0 Address represents

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

Answer: C

NEW QUESTION 13
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 16
Requires that all instances of the data be identical in form,

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

Answer: C

NEW QUESTION 20
Example of Token based Authentication

A. Kerberos
B. Basic
C. OAuth
D. NTLN

Answer: C

NEW QUESTION 23
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
A hacker gains access to a compony network and begins to intercept network traffic in order to steal login credentials which OSI layer is being attacked

A. Data Link layer
B. Physical layer
C. Network Layer
D. Application laver

Answer: D

NEW QUESTION 29
Which of the following is not a protocol of the OSI layer 3

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

Answer: D

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

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

Answer: C

NEW QUESTION 38
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 42
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 45
Which drives for the IPv6 introduction

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

Answer: C

NEW QUESTION 47
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 51
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 55
DNS works in which OSI layer

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

Answer: C

NEW QUESTION 56
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 57
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 60
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 61
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 64
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 66
What is the main purpose of using multi-factor authentication (MFA) in a security system?

A. To prevent data breaches

B. To protect against malware
C. To ensure data integrity
D. To add an extra layer of security to user authentication

Answer: D

NEW QUESTION 67
The last phase in the data security cycle is

A. Encryption
B. Destruction
C. Archival
D. Backup

Answer: B

NEW QUESTION 70
What is the range of well known ports

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

Answer: A

NEW QUESTION 71
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 76
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 81
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 82
Which of the following is a subject?

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

Answer: D

NEW QUESTION 85
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 89
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 94
A tool used to inspect outbound traffic to reduce threats

A. Anti-ma I ware
B. NIDC
C. DLP
D. Firewall

Answer: C

NEW QUESTION 98
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 99
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 101
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 105
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 110
Information should be consistently and readily accessible for authorized parties ?

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

Answer: C

NEW QUESTION 113
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 114
Which of the following attacks can TLS help mitigate?

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

Answer: C

NEW QUESTION 117
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 122
What is the primary goal of network segmentation in cybersecurity?

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

Answer: B

NEW QUESTION 126
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 130
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 134
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 137
Which type of database combines related records and fields into a logical tree structure?

A. Relational
B. Hierarchical

C. Object-oriented
D. Network

Answer: B

NEW QUESTION 141
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 145
What is an IP address

A. A physical address used to connect multiple devices in a network
B. An address that denotes the vendor or manufacturer of the physical network interface
C. A Logical address associated with a unique network interface within the network
D. An Address that represents the network interface within the network

Answer: C

NEW QUESTION 148
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 149
Which of the following uses registered port

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

Answer: D

NEW QUESTION 151
Which is the loopback address

A. ::1
B. 127.0.0.1
C. 255.255.255.0
D. Both A and B

Answer: D

NEW QUESTION 156
The magnitude of the harm expected as a result of the consequences of an unauthorized disclosure, modification, destruction or loss of information is known as

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

Answer: C

NEW QUESTION 158
Which aspect of cybersecurity is MOST impacted by Distributed Denial of Service (DDoS) attacks?

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

Answer: C

NEW QUESTION 163
Which of the following is not a source of redundant power

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

Answer: D

NEW QUESTION 164
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 167
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 168
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 171
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 176
Which layer of OSI the Firewall works

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

Answer: D

NEW QUESTION 181
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 183
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 185
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 189
What goal of security is enhanced by a strong business continuity program?

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

Answer: B

NEW QUESTION 190
A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time.

A. Spoofing
B. Phishing
C. DOS
D. Advanced Persistent Threat

Answer: D

NEW QUESTION 195
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 197
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 199
Which is the SSH port

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

Answer: D

NEW QUESTION 203
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 207
A portion of the organization's network that interfaces directly with the outside world; typically, this exposed area has more security controls and restrictions than the rest of the internal IT environment.

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

Answer: D

NEW QUESTION 212
What is the range of private ports

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

Answer: C

NEW QUESTION 214
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 216
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 221
Exhibit.

OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

IPSec works in which layer of OSI Model

A. Layer 2
B. Layer 5
C. Layer 3
D. Layer 7

Answer: C

NEW QUESTION 223
A company performs an analysis of its information systems requirements functions and interdependences in order to prioritize contingency requirement. What is this process called?

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

Answer: D

NEW QUESTION 227
Which type of control is used to identify that an attack has occurred or is currently occurring

A. Preventive control
B. Detective control
C. Corrective control
D. Recovery control

Answer: B

NEW QUESTION 232
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 236
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 240
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 243
Which of the following documents contains elements that are NOT mandatory

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

Answer: D

NEW QUESTION 245
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 250
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 254
The Bell and LaPadula access control model is a form of

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

Answer: B

NEW QUESTION 259
Who must follow HIPAA Compliance

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

Answer: B

NEW QUESTION 262
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 267
_____ are virtual separations within a switch and are used mainly to limit broadcast traffic

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

Answer: C

NEW QUESTION 269
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 271
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 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 278
Works via encapsulation and wrapping a packet inside another packet.

A. Network segmentation
B. Load balancing
C. Tunnelling
D. Data encryption

Answer: C

NEW QUESTION 280
Example of Deterrent controls

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

Answer: A

NEW QUESTION 284
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 285
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
A Company wants to ensure that its employees can access the network resources from anywhere in the world which access control model is best suited for this scenario

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

Answer: D

NEW QUESTION 293
Which is related to Privacy

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

Answer: D

NEW QUESTION 296
What is the process of verifying a users identity called?

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

Answer: B

NEW QUESTION 299
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 301
Which document serve as specifications for the implementation of policy and dictates mandatory requirements

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

Answer: C

NEW QUESTION 304
Which security control mostly used to prevent data breach

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

Answer: B

NEW QUESTION 306
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 309
Restoring IT and communications back to full operation after a disruption.

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

Answer: C

NEW QUESTION 314
Measure of the extent to which an entity is threatened by a potential circumstance or event and likelihood of occurrence

A. Impact
B. Risk
C. Threat
D. Threat Vector

Answer: B

NEW QUESTION 319
An employee unintentionally shares confidential information with an unauthorized party. What term best describes this situation?

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

Answer: D

NEW QUESTION 323
Granting a user access to services or the system

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

Answer: C

NEW QUESTION 325
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 329
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 330
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 331
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 332
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 337
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 342
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
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 352
Example of Type 1 Authentication

A. Password
B. Smart Card
C. Finger Print
D. RSA Token

Answer: A

NEW QUESTION 355
Ignoring the risk and proceeding the business operations

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

Answer: A

NEW QUESTION 356
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 357
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 360
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 361
What is Remanence

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

Answer: A

NEW QUESTION 366
Which one of the following cryptographic algorithms does not depend upon the prime factorization problem?

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

Answer: C

NEW QUESTION 370
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 372
Which layer provides the services to user?

A. Application layers
B. Session Layers
C. Presentation Layer
D. Physical Layer

Answer: A

NEW QUESTION 377
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 378
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 381
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 383
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 386
Which type of network is set up similar to the internet but is private to an organization. Select the MOST appropriate?

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

Answer: B

NEW QUESTION 391
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 393
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 395
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 399
Which protocol is used for secure email

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

Answer: D

NEW QUESTION 402
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 405
Which of the following does not normally influence an organization's retention policy for logs?

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

Answer: D

NEW QUESTION 407
A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

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

Answer: A

NEW QUESTION 410
allows for extremely granular restrictions within the IT environment, to the point where rules can be applied to individual machines and/or users,

A. DMZ
B. Microsegmentation
C. VLAN
D. NAC

Answer: B

NEW QUESTION 413
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 416
A common network device used to filter traffic?

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

Answer: D

NEW QUESTION 420
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 422

Government can imposes financial penalties as a consequence of breaking a

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

Answer: B

NEW QUESTION 424
Which of the following properties is not guaranteed by Digital signatures

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

Answer: B

NEW QUESTION 426
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 429
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 431
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 435
What is the purpose of the CIA triad terms

A. To make security more understable to management and users
B. To describe security using relevant and meaningful words
C. To define the purpose of security
D. AII

Answer: D

NEW QUESTION 438
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 440
Load balancing safe guard which CIA triad

A. Confidentiality
B. Availablity
C. Integrity

D. All

Answer: B

NEW QUESTION 443
What is the BEST defense against dumpster diving attacks?

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

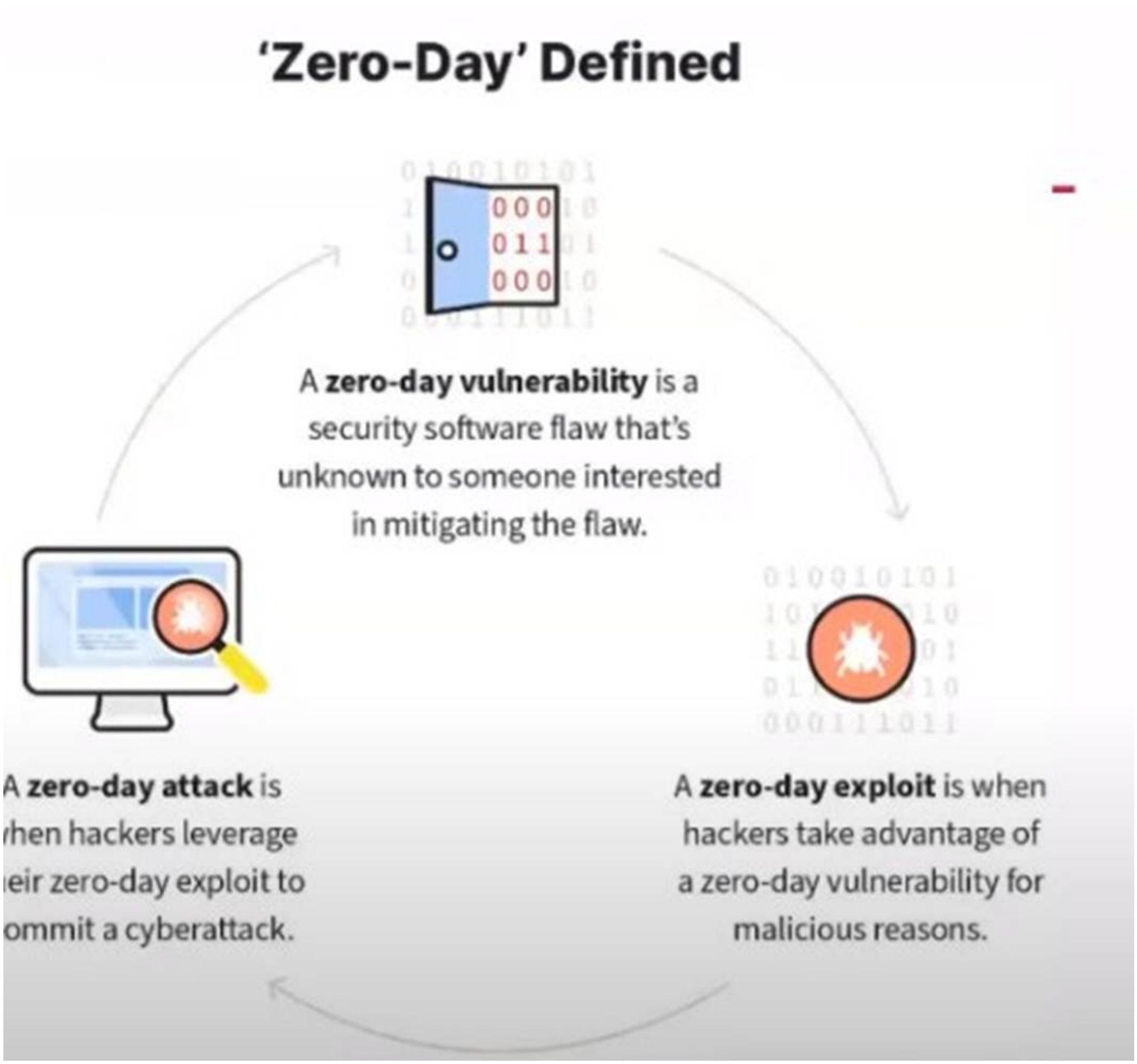
Answer: D

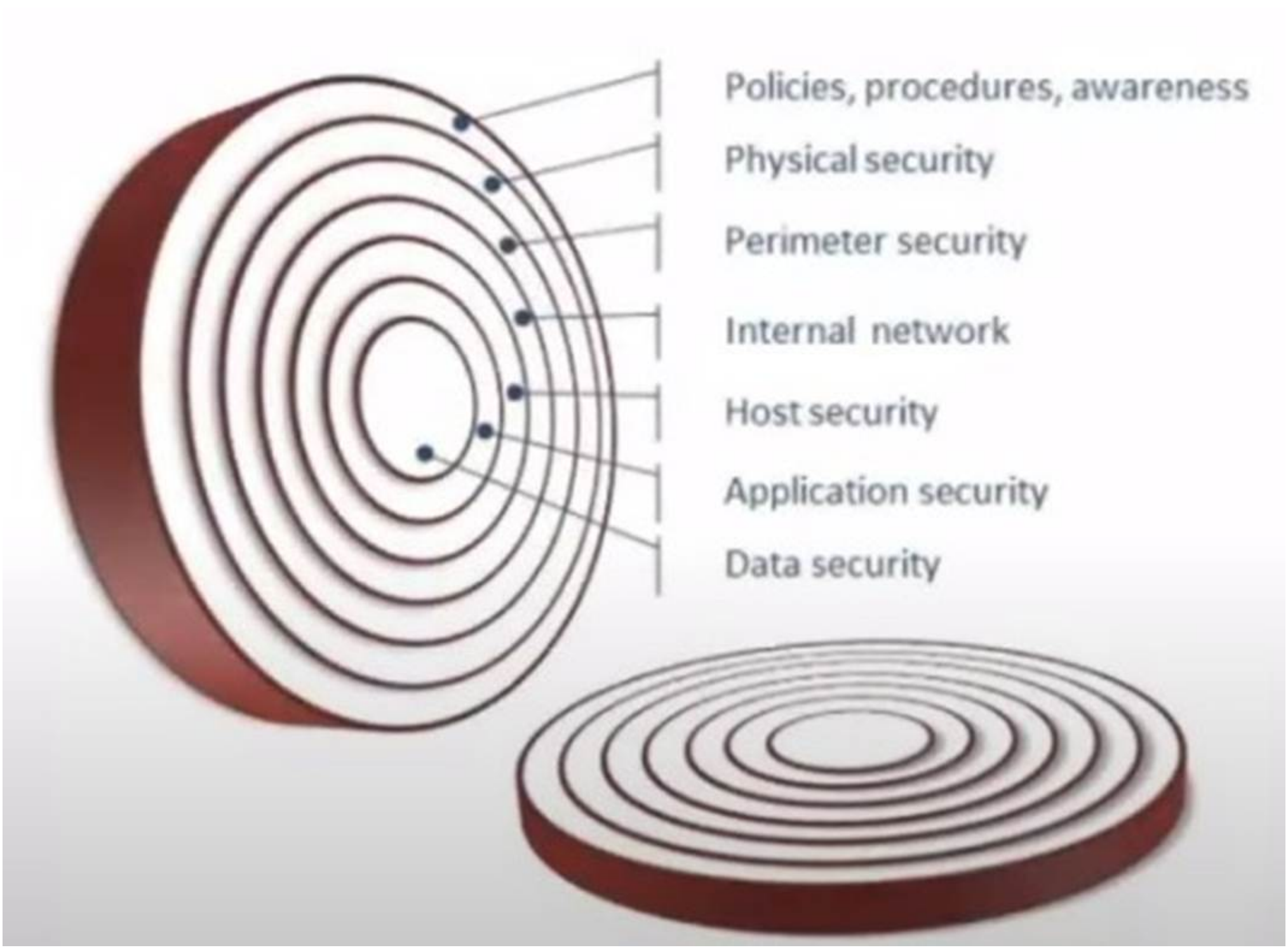
NEW QUESTION 448
Which authentication helps build relationships between different technology providers, enabling automatic identification and user access. Employees no longer need to enter separate usernames and passwords when visiting a new service provider

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

Answer: D

NEW QUESTION 451
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 452
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 457
Risk tolerance also known as

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

Answer: D

NEW QUESTION 459
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 460
DDOS attack affect which OSI layer

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

Answer: D

NEW QUESTION 463
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 466
Port scanning attack target which OSI layer

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

Answer: A

NEW QUESTION 469
You experienced a power outage that disrupted access to your data center. What type of security concern occurred?

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

Answer: A

NEW QUESTION 471
Why is an asset inventory much important?

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

Answer: D

NEW QUESTION 474
A standard that defines wired communications of network devices

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

Answer: D

NEW QUESTION 475
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 478
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 482
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 484
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 489
Which device is used to control traffic flow in network

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

Answer: D

NEW QUESTION 494
.....

Relate Links

100% Pass Your CC Exam with Exambible Prep Materials

https://www.exambible.com/CC-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/