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
What is multi-factor authentication (MFA)?

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

Answer: C

NEW QUESTION 4
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 5
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 6
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 7
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 8
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 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
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 14
Which is related to Standard

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

Answer: A

NEW QUESTION 18
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 19
Requires that all instances of the data be identical in form,

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

Answer: C

NEW QUESTION 21
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 23
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 26
Example of Token based Authentication

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

Answer: C

NEW QUESTION 31
Which term describes a communication tunnel that provides point-to-point transmission of both authentication and data traffic over an untrusted network?

A. Zero Trust
B. DMZ
C. VPN
D. None of the Above

Answer: C

NEW QUESTION 32
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 35
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 38
A popular way of implementing "least privilege"

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

Answer: C

NEW QUESTION 40
Also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs)

A. Hypervisor
B. Simulation
C. Emulation
D. Cloud Controller

Answer: A

NEW QUESTION 41
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 42
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 46
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 49
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
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 52
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 53
The last phase in the data security cycle is

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

Answer: B

NEW QUESTION 55
Finance Server and Transactions Server has restored its original facility after a disaster, what should be moved in FIRST?

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

Answer: D

NEW QUESTION 56
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 59
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 60
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 65
What is the difference between BCP and DRP

A. BCP is about restoring IT and communications back to full operations after a disruption, while DRP is about maintaining critical business functions
B. DRP is about restoring IT and communications back to full operations after a disruption, while BCP i about maintaining critical business functions
C. DRP and BCP are the same
D. BCP is about maintaining critical business functions before a disaster occurs

Answer: B

NEW QUESTION 69
Which layer does VLAN hopping belong to?

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

Answer: D

NEW QUESTION 72
Is a way to prevent unwanted devices from connecting to a network.

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

Answer: D

NEW QUESTION 73
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 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 75
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 77
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 79
Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Micro segmentation of workloads is a tool of the model

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

Answer: A

NEW QUESTION 82
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 86
Which Prevents Threat

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

Answer: A

NEW QUESTION 88
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 91

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 94
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 96
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 98
Which of the following uses registered port

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

Answer: D

NEW QUESTION 102
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 106
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 108
The means by which a threat actor carries out their objectives

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

Answer: B

NEW QUESTION 112
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 113
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 114
Exhibit.

information security is not built on which of the following?

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

Answer: C

NEW QUESTION 117
A company primary data center goes down due to a hardware failure causing a major disruption to the IT and communications systems. What is the focus of disaster recovery planning in this scenario

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

Answer: C

NEW QUESTION 120
Which layer of OSI the Firewall works

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

Answer: D

NEW QUESTION 123
Which addresses reserved for internal network use and are not routable on the internet.

A. acOO:: to adff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
B. fcOO:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
C. bcOO:: to bdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
D. ccOO:: to cdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Answer: B

NEW QUESTION 127
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 132
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 133
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 136
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 137
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 138
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 142
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 147
Which of the following is not an element of system security configuration management

A. Baselines
B. Updates
C. Inventory
D. Audit logs

Answer: D

NEW QUESTION 150
XenServer, LVM, Hyper-V, ESXi are

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

Answer: B

NEW QUESTION 154
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 157
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 158
Organization experiences a security event that does not affect the confidentiality integrity and availability of its information system. What term BEST describes this situation?

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

Answer: D

NEW QUESTION 163
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 167
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 169
How often should an organization test its business continuity plan

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

Answer: C

NEW QUESTION 170
A _____ is a distributed denial-of-service (DDoS) attack in which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets.

A. DOS
B. Syn flood
C. Smurf attack
D. Phishing attack

Answer: C

NEW QUESTION 175
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 179
What is the recommended range of temperature for optimized maximum uptime and hardware life in a data center?

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

Answer: B

NEW QUESTION 180
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 183
Which of these components is very likely to be instrumental to any disaster recovery (DR) effort?

A. Routers

B. Laptops
C. Firewalls
D. Backups

Answer: D

NEW QUESTION 187
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 191
An agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing- specific terms

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

Answer: C

NEW QUESTION 194
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 198
The mitigation of violations of security policies and recommended practices

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

Answer: D

NEW QUESTION 201
Derrick logs on to a system in order to read a file. In this example. Derrick is the _____?

A. Subject
B. Object
C. Process
D. Predicate

Answer: A

NEW QUESTION 204
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 205
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

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

Answer: A

NEW QUESTION 207
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 210
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 212
Which of the following is often associated with DR planning?

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

Answer: D

NEW QUESTION 217
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 220
_____ 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 221
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 224
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 228
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 230
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 232
Example of Deterrent controls

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

Answer: A

NEW QUESTION 235
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 237
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 241
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 246
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 250
Which is related to Privacy

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

Answer: D

NEW QUESTION 251
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 253
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 255
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 260
Which of these is an example of deterrent control

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

Answer: B

NEW QUESTION 261
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 262
A Company IT system experienced a system crash that result in a loss of data. What term best describes this event?

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

Answer: A

NEW QUESTION 264
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 268

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 271
Which of the following best describes a zero-day vulnerability?

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

Answer: B

NEW QUESTION 274
What is sensitivity in the context of confidentiality

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

Answer: C

NEW QUESTION 279
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 281
True or False? The IT department is responsible for creating the organization's business continuity plan

A. True
B. False

Answer: B

NEW QUESTION 283
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 288
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 292
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 297
Which of the following protocols is a secure alternative to using telnet?

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

Answer: B

NEW QUESTION 300
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 301
Which of the following is the least secure communications protocol?

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

Answer: C

NEW QUESTION 306
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 311
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 312
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 314
Example of Type 1 Authentication

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

Answer: A

NEW QUESTION 318

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 319
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 320
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 325
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 328
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 331
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 336
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 337
Who is responsible for publishing and signing the organization s policies?

A. The security office
B. Human resources
C. Senior management
D. The legal department

Answer: C

NEW QUESTION 338
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 339
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 340
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 345
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 347
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 351
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 356
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 361
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 366
Which protocol is used for secure email

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

Answer: D

NEW QUESTION 368
Port used in DNS

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

Answer: A

NEW QUESTION 369
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 372
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 375
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 378
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 380
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 385
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 389
Government can imposes financial penalties as a consequence of breaking a

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

Answer: B

NEW QUESTION 390
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 391
A hacker gains access to an organization system without authorization and steal confidential data. What term best describes this ?

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

Answer: C

NEW QUESTION 396
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 397
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 399
The practice of sending fraudulent communications that appear to come from a reputable source

A. DOS
B. Virus

C. Spoofing
D. Phishing

Answer: D

NEW QUESTION 400
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 402
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 403
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 407
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 408
Load balancing safe guard which CIA triad

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

Answer: B

NEW QUESTION 411
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 414
What is the BEST defense against dumpster diving attacks?

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

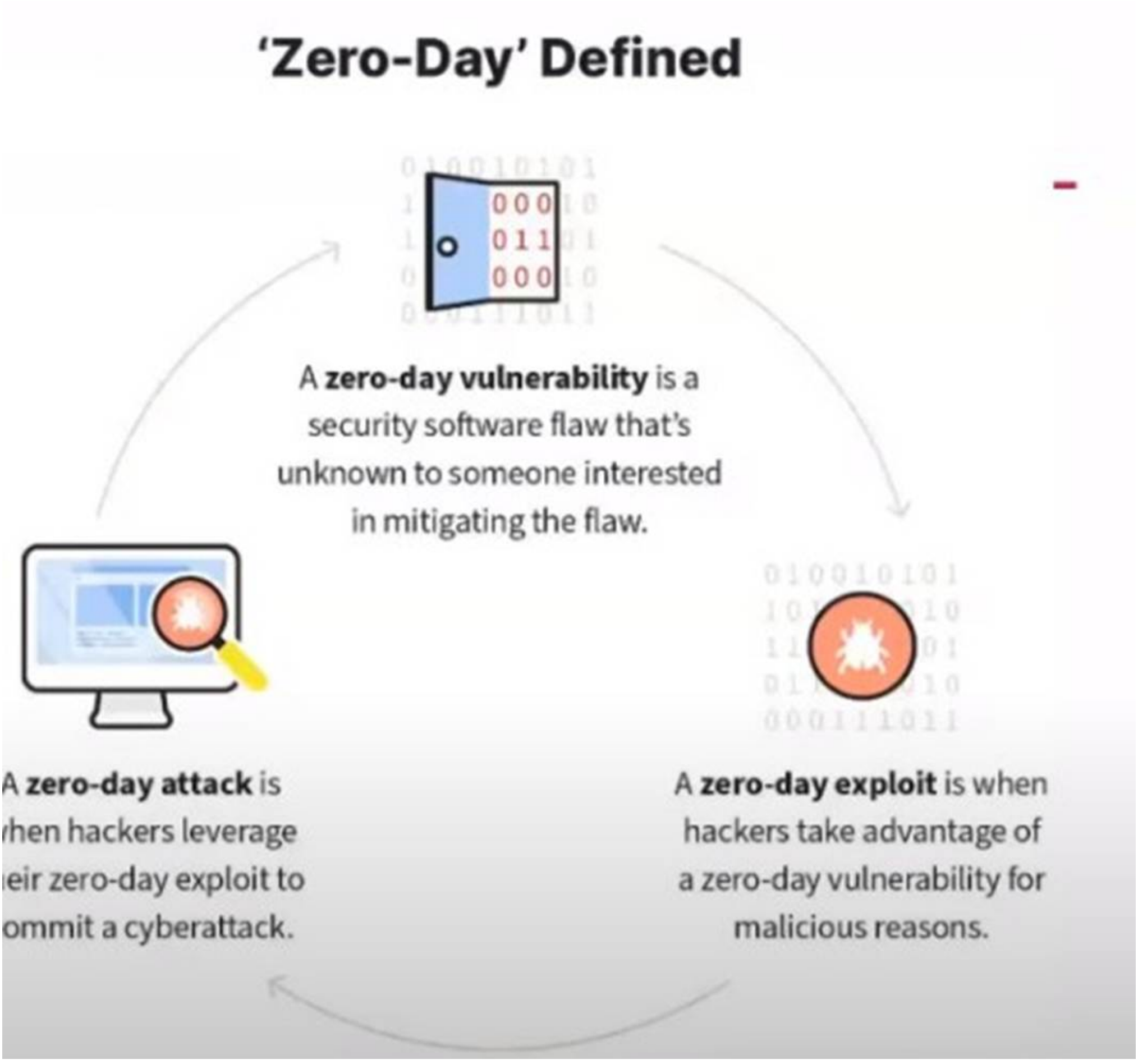
Answer: D

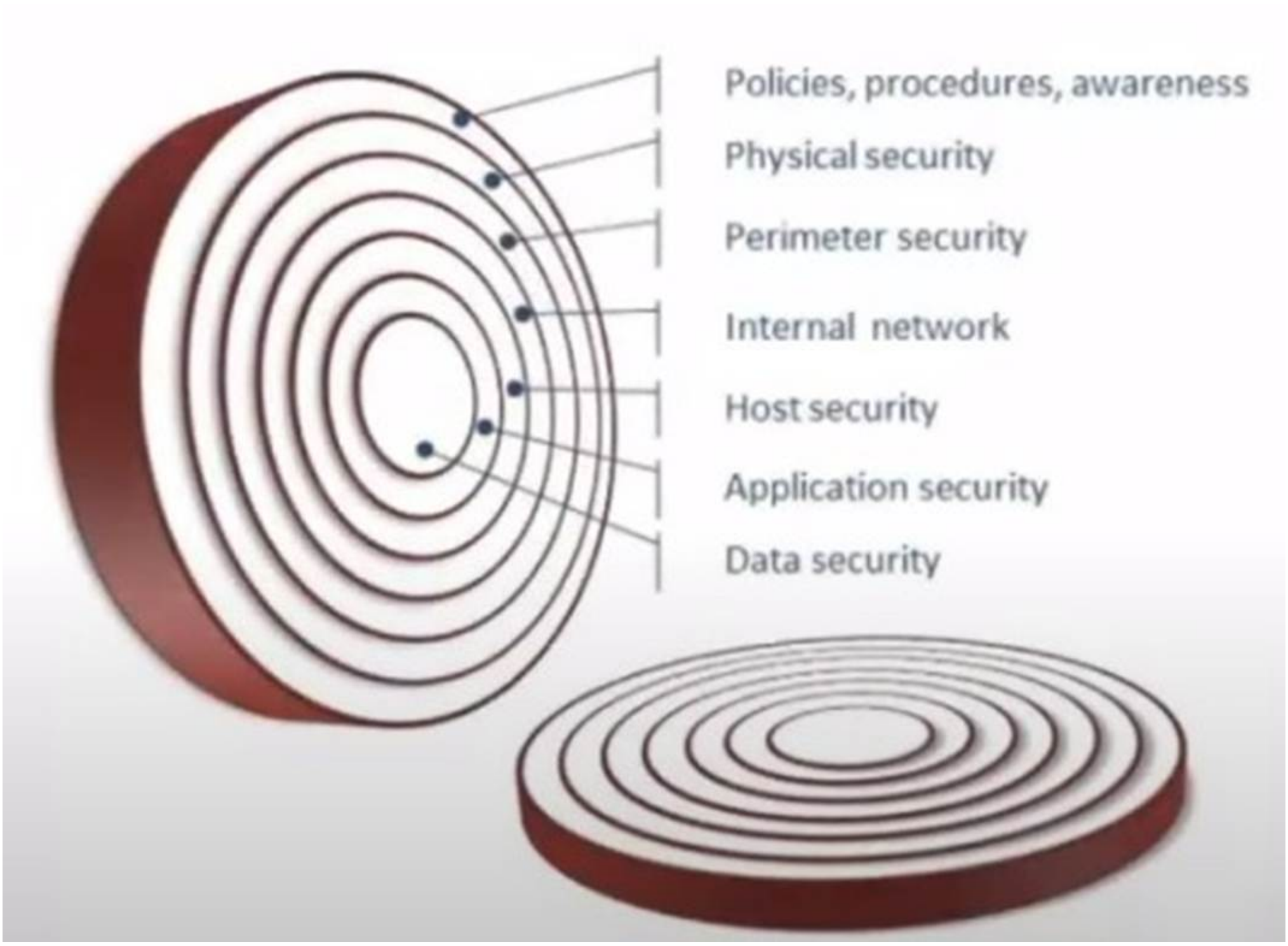
NEW QUESTION 418
Which authentication helps build relationships between different technology providers, enabling automatic identification and user access. Employees no longer need to enter separate usernames and passwords when visiting a new service provider

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

Answer: D

NEW QUESTION 423
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 427
Which one of the following groups is NOT normally part of an organization's cybersecurity incident response team?

A. Technical Subject Matter Experts
B. Cybersecurity Experts
C. Management
D. Law Enforcement

Answer: D

NEW QUESTION 429
Risk tolerance also known as

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

Answer: D

NEW QUESTION 432
DDOS attack affect which OSI layer

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

Answer: D

NEW QUESTION 433
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 435
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 439
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 441
Port scanning attack target which OSI layer

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

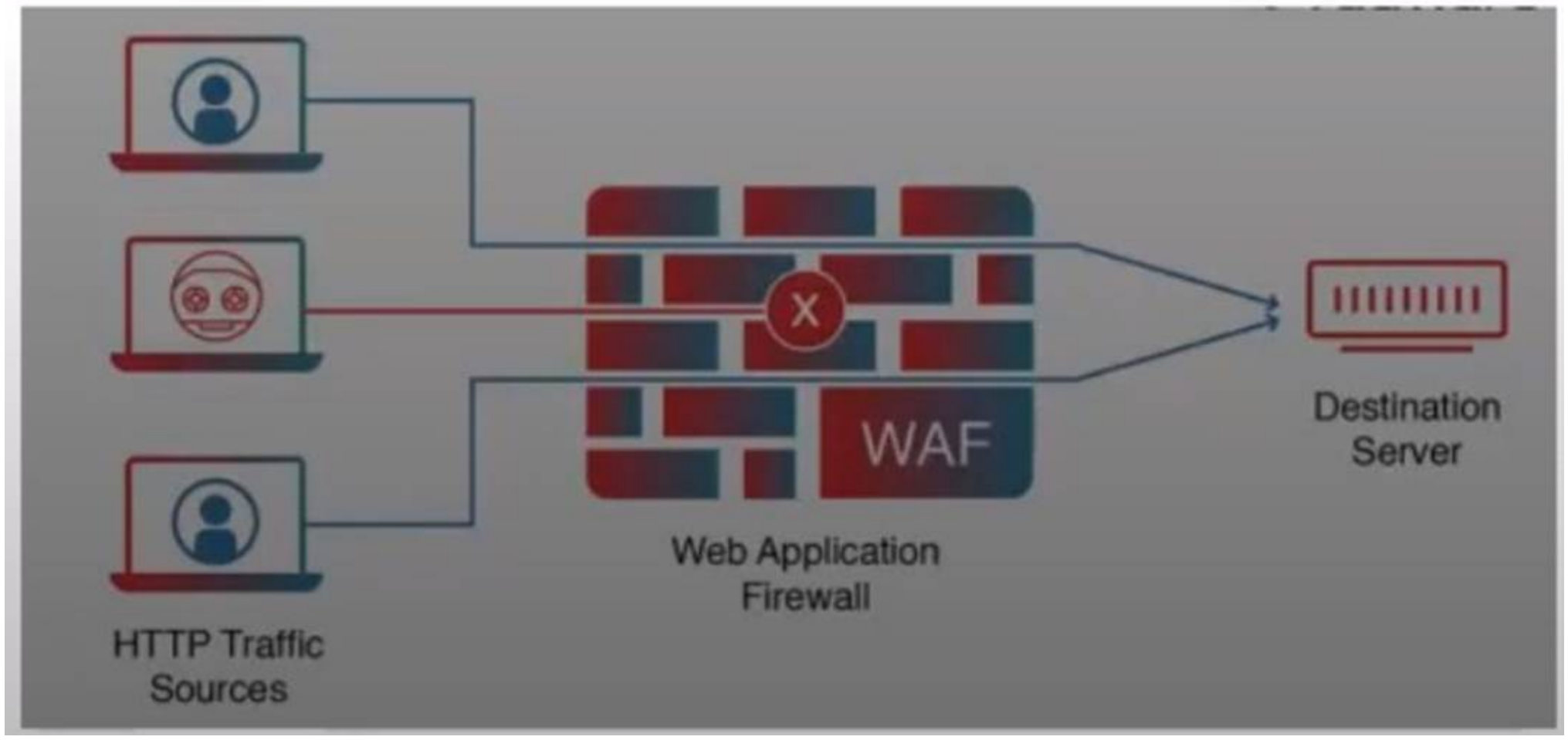
Answer: A

NEW QUESTION 446
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 451
Exhibit.



What is the PRIMARY purpose of a web application firewall (WAF)?

A. To protect the web server from DDoS attacks
B. To monitor network traffic for intrusions
C. To filter and block malicious web traffic and requests
D. To manage SSL certificates

Answer: C

NEW QUESTION 454
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 455
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 459
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 462
A standard that defines wired communications of network devices

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

Answer: D

NEW QUESTION 465
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 466
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 467
A backup is which type for security control

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

Answer: C

NEW QUESTION 469
Token Ring used in which OSI Layer

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

Answer: D

NEW QUESTION 473
Which device is used to control traffic flow in network

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

Answer: D

NEW QUESTION 474
.....

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