ISC2

Exam Questions CC

Certified in Cybersecurity (CC)

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
In the context of cybersecurity, typical threat actors include the following:

A. Insiders (either deliberately, by simple human error, or by gross incompetence).
B. Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability).
C. Technology (such as free-running bots and artificial intelligence
D. All

Answer: D

NEW QUESTION 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
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 6
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 7
Ping flood attack target which OSI layer

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

Answer: B

NEW QUESTION 8
Which is related to Standard

A. NIST

B. GDPR
C. HIPAA
D. ALL

Answer: A

NEW QUESTION 9
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 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 15
A organization's security system which involves in preventing, detecting, analyzing, and responding to cybersecurity incidents.

A. Business continuity team
B. Disaster recovery team
C. Incident response team
D. Security operations center

Answer: D

NEW QUESTION 20
TCP and UDP reside at which layer of the osi model?

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

Answer: D

NEW QUESTION 25
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 30
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 34
Which OSI layer VPN works

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

Answer: D

NEW QUESTION 39
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 40
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 42
A popular way of implementing "least privilege"

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

Answer: C

NEW QUESTION 47
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 50
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 51
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 55
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 59
IDS can be described in terms of what fundamental functional components?

A. Response
B. Information Sources
C. Analysis
D. All of the choices.

Answer: D

NEW QUESTION 60
Timiting access to resources based on the sensitivity of the information that the resource contains and the authorization of the user to access information with that level of sensitivity.

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

Answer: B

NEW QUESTION 64
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 66
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 71
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 72
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 75
Which of the following is endpint

A. Router
B. Firewall
C. Laptop

D. Switch

Answer: C

NEW QUESTION 78
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 81
Which layer does VLAN hopping belong to?

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

Answer: D

NEW QUESTION 82
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 85
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 87
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 91
In information systems terms, the activities necessary to restore IT and communications services of an organization during and after an outage

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

Answer: D

NEW QUESTION 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 96
What security feature used in HTTPS

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

Answer: D

NEW QUESTION 99
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 104
What is the difference between hub and switch

A. A hub is less likely to be used in home network
B. A hub can create separate broad cast domains when used to create Vlan
C. A hub retransmits traffic to all devices, while a switch route traffic to a specific devices
D. A switch retransmits traffic to all devices, while a hub route traffic to a specific devices

Answer: C

NEW QUESTION 109
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 113
A company needs to protect its confidential data from unauthorized access which logical control is best suited for this scenario

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

Answer: A

NEW QUESTION 118
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 119
Is an integrated platform and graphical tool for performing security testing of web applications.

A. Burb suite
B. Wireshark C Fiddler
C. ZenMap

Answer: A

NEW QUESTION 123
A security practitioner who needs step-by-step instructions to complete a provisioning task

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

Answer: C

NEW QUESTION 124
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 131
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 133
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 136
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 138
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 141
Which of the following is a characteristic of cloud

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

Answer: B

NEW QUESTION 146
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 151
Which of these tool is commonly used to crack passwords

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

Answer: D

NEW QUESTION 152
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 157
Exhibit.

information security is not built on which of the following?

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

Answer: C

NEW QUESTION 158
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 161
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 163
provide integrity services that allow a recipient to verify that a message has not been altered.

A. Hashing
B. encryption
C. decryption
D. encoding

Answer: A

NEW QUESTION 165
Modern solutions try to provide a more holistic approach detecting rootkits, ransomware and spyware.

A. Antivirus
B. IDS
C. IPS
D. Anti Malware

Answer: D

NEW QUESTION 167
What is the primary factor in the reliability of information and system

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

Answer: C

NEW QUESTION 171
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 173
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 178
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 183
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 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 191
Security control used to protect against environmental threats such as fire, flood and earth quakes

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

Answer: A

NEW QUESTION 196
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 199
What is the range of private ports

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

Answer: C

NEW QUESTION 204
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 205
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 210
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 212
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 215
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 216
A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high.

A. Quantitative Risk Analysis
B. Risk Assessment
C. Risk Mitigation
D. Qualitative Risk Analys

Answer: D

NEW QUESTION 218
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 220
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 221
Which of the following is NOT one of the three main components of a sql database?

A. Views
B. Schemas
C. Tables
D. Object-oriented interfaces

Answer: D

NEW QUESTION 224
The mitigation of violations of security policies and recommended practices

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

Answer: D

NEW QUESTION 228
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 232
Which of the following documents contains elements that are NOT mandatory

A. Procedures

B. Policies
C. Regulations
D. Guidelines

Answer: D

NEW QUESTION 237
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 238
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 240
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 242
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 243
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 246
_____ 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 247
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 252
A company wants to ensure that its employees cannot bring unauthorized electronic devices into the workspace which physical control is best suited for this

A. Metal Detectors
B. Security gaurds
C. RFID scanners
D. Baggage X-ray machinces

Answer: A

NEW QUESTION 257
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 259
Example of Deterrent controls

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

Answer: A

NEW QUESTION 262
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 265
Which type of authentication is something which you

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

Answer: C

NEW QUESTION 266
Which is related to Privacy

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

Answer: D

NEW QUESTION 267
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 269
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 274
Restoring IT and communications back to full operation after a disruption.

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

Answer: C

NEW QUESTION 278
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 279
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 280
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 283
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 288
Granting a user access to services or the system

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

Answer: C

NEW QUESTION 289
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 290
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 291
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 293
Which of the following protocols is a secure alternative to using telnet?

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

Answer: B

NEW QUESTION 294
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 297
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 301
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 304
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 307

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 308
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 309
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
Permitting authorized access to information while protecting it from improper disclosure

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

Answer: B

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 322
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 325
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 330
The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats.

A. Segregation of Duties
B. Principle of Least Privilege
C. Privileged Account
D. Rule-based access control

Answer: A

NEW QUESTION 331
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 333
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 337
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 342
An attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant

A. Eavesdropping Attack
B. CSRF
C. XSS
D. ARP Spoofing

Answer: A

NEW QUESTION 343
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 345
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 348
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 350
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 353
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 358
Which uses encrypted, machine-generated codes to verify a user's identity.

A. Basic Authentication
B. Form Based Authentication
C. Token Based Authentication
D. AII

Answer: C

NEW QUESTION 362
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 366
A new BYOD policy has been enforced in NEW Corp which type of control is used to enforce thissecurity policies

A. Physical control
B. Logical Control
C. Administrative Control
D. Technical Control

Answer: C

NEW QUESTION 368
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 371
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 372
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 375
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 377
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 380
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 385
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 388
Often offered by third-party organizations and cover specific
advisory or compliance objectives.

A. Standard
B. PolicyC Procedure
C. Laws or Regulations

Answer: A

NEW QUESTION 390
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 393
The primary goal of a risk assessment

A. Avoid Risk
B. Estimate and Prioritize Risk
C. Ignore risk
D. Evaluate the Impact

Answer: B

NEW QUESTION 395
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 397
Natalia is concerned about the security of his organization's domain name records and would like to adopt a technology that ensures their authenticity by adding digital signatures. Select the MOST appropriate technology to use?

A. DNSSIGN
B. DNSSEC
C. CERTDNS
D. DNS2

Answer: B

NEW QUESTION 402
A device that routes traffic to the port of a known device

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

Answer: A

NEW QUESTION 407
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 409
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 413
Exhibit.

What is the purpose of a Security Information and Event Management (SIEM) system?

A. Encrypting files
B. Monitoring and analyzing security events -
C. Blocking malicious websites
D. Managing user passwords

Answer: B

NEW QUESTION 418
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 423
Incident management is also known as

A. Risk Management
B. Business Continuity management
C. Incident management
D. Crisis management

Answer: D

NEW QUESTION 425
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 429
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 431
A company primary data center goes down due to a hardware failure causing a major disruption to the IT and communications systems. What is the focus of disaster recovery planning in this scenario

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

Answer: C

NEW QUESTION 432
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 437
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 438
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 442
Risk tolerance also known as

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

Answer: D

NEW QUESTION 445
Devid is worried about distributed denial of service attacks against his company's primary web application, which of the following options will provide the MOST resilience against large-scale ddos attacks?

A. Implement a CDN
B. Increase the number of servers in the web application server cluster
C. Contract for DDoS mitigation services via the company's IPS

D. Increase the amount of bandwidth available from one or more ISPs

Answer: A

NEW QUESTION 449
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 452
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 455
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 459
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 462
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 467
Port scanning attack target which OSI layer

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

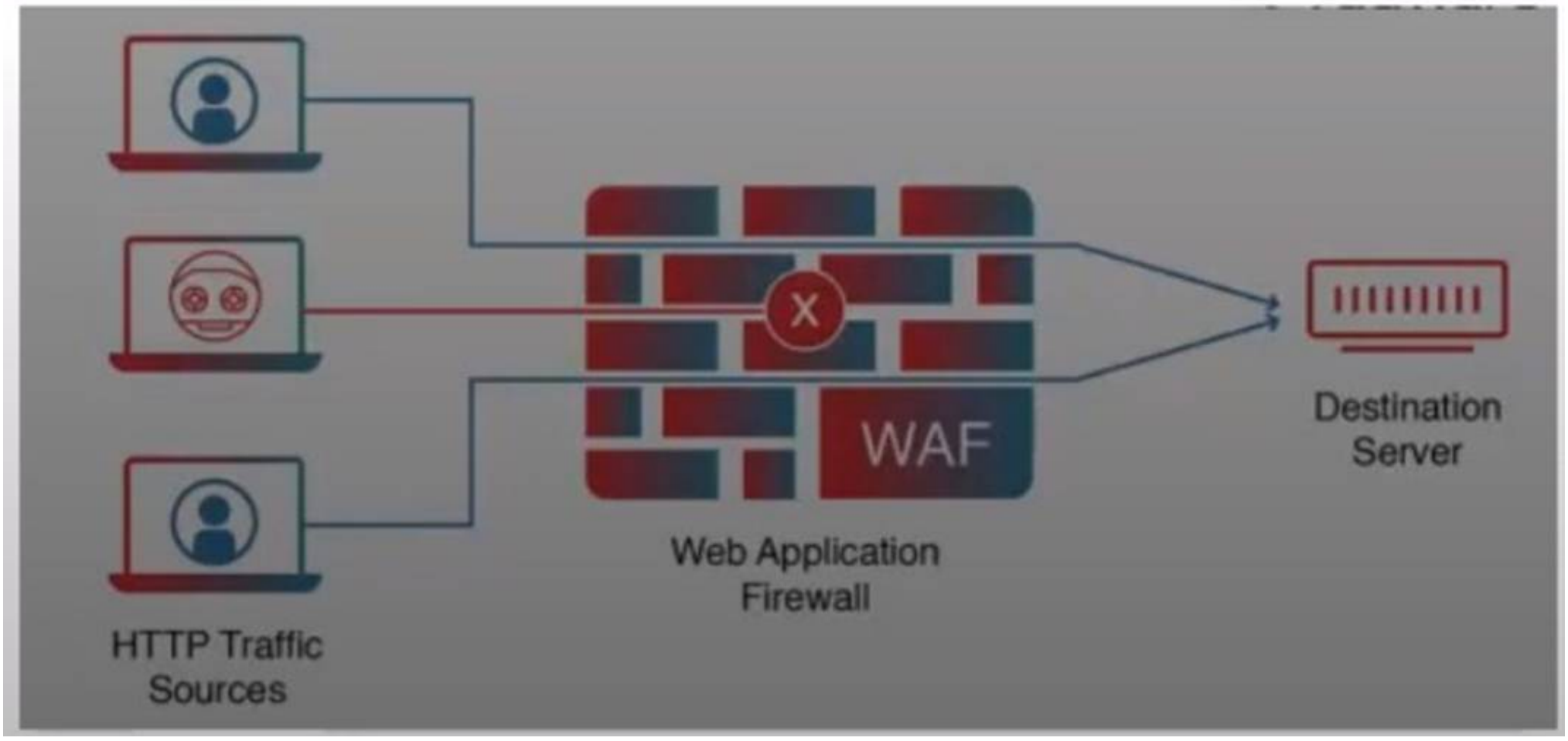
Answer: A

NEW QUESTION 471
Which is not possible models for an Incident Response Team (IRT):

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

Answer: D

NEW QUESTION 473
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 475
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 476
A hacker is trying to gain access to a company network which of the following scenarios would be an example of defense in depth

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

Answer: C

NEW QUESTION 479
A standard that defines wired communications of network devices

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

Answer: D

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 487
Which device is used to control traffic flow in network

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

Answer: D

NEW QUESTION 488
.....

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