Actual exam question from ISC's CISSP

Question #: 1

Topic #: 1

[All CISSP Questions]

Physical assets defined in an organization's business impact analysis (BIA) could include which of the following?

A. Personal belongings of organizational staff members

B. Disaster recovery (DR) line-item revenues

C. Cloud-based applications

D. Supplies kept off-site a remote facility

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 2

Topic #: 1

[All CISSP Questions]

When assessing the audit capability of an application, which of the following activities is MOST important?

A. Identify procedures to investigate suspicious activity.

B. Determine if audit records contain sufficient information.

C. Verify if sufficient storage is allocated for audit records.

D. Review security plan for actions to be taken in the event of audit failure.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 3

Topic #: 1

[All CISSP Questions]

An organization would like to implement an authorization mechanism that would simplify the assignment of various system access permissions for many users with similar job responsibilities. Which type of authorization mechanism would be the BEST choice for the organization to implement?

A. Role-based access control (RBAC)

B. Discretionary access control (DAC)

C. Content-dependent Access Control

D. Rule-based Access Control

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 4

Topic #: 1

[All CISSP Questions]

What is the PRIMARY reason for criminal law being difficult to enforce when dealing with cybercrime?

A. Jurisdiction is hard to define.

B. Law enforcement agencies are understaffed.

C. Extradition treaties are rarely enforced.

D. Numerous language barriers exist.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 5

Topic #: 1

[All CISSP Questions]

Wi-Fi Protected Access 2 (WPA2) provides users with a higher level of assurance that their data will remain protected by using which protocol?

A. Extensible Authentication Protocol (EAP)

B. Internet Protocol Security (IPsec)

C. Secure Sockets Layer (SSL)

D. Secure Shell (SSH)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 6

Topic #: 1

[All CISSP Questions]

Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

A. Reference monitor

B. Trusted Computing Base (TCB)

C. Time separation

D. Security kernel

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 7

Topic #: 1

[All CISSP Questions]

What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

A. Performance testing

B. Risk assessment

C. Security audit

D. Risk management

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 8

Topic #: 1

[All CISSP Questions]

Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this IAM action?

A. Clothing retailer acts as User Self Service, confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.

B. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.

C. Clothing retailer acts as Service Provider, confirms identity of user using industry standards, then sends credentials to partner businesses that act as an identity provider (IdP) and allows access to resources.

D. Clothing retailer acts as Access Control Provider, confirms access of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to resources.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 9

Topic #: 1

[All CISSP Questions]

Which of the following statements BEST describes least privilege principle in a cloud environment?

A. A single cloud administrator is configured to access core functions.

B. Internet traffic is inspected for all incoming and outgoing packets.

C. Routing configurations are regularly updated with the latest routes.

D. Network segments remain private if unneeded to access the internet.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 10

Topic #: 1

[All CISSP Questions]

An organization has been collecting a large amount of redundant and unusable data and filling up the storage area network (SAN). Management has requested the identification of a solution that will address ongoing storage problems. Which is the BEST technical solution?

A. Compression

B. Caching

C. Replication

D. Deduplication

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 11

Topic #: 1

[All CISSP Questions]

Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other routers in the path to make independent determinations?

A. Synchronous Optical Networking (SONET)

B. Multiprotocol Label Switching (MPLS)

C. Fiber Channel Over Ethernet (FCoE)

D. Session Initiation Protocol (SIP)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 12

Topic #: 1

[All CISSP Questions]

Which of the following would an information security professional use to recognize changes to content, particularly unauthorized changes?

A. File Integrity Checker

B. Security information and event management (SIEM) system

C. Audit Logs

D. Intrusion detection system (IDS)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 13

Topic #: 1

[All CISSP Questions]

Which of the following is included in change management?

A. Technical review by business owner

B. User Acceptance Testing (UAT) before implementation

C. Cost-benefit analysis (CBA) after implementation

D. Business continuity testing

Show Suggested Answer

Actual exam question from ISC's CISSP
Question #: 14
Topic #: 1
[All CISSP Questions]

A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

A. Pinning
B. Single-pass wipe
C. Multi-pass wipes
D. Degaussing

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 15

Topic #: 1

[All CISSP Questions]

When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

A. SOC 1 Type 1

B. SOC 2 Type 1

C. SOC 2 Type 2

D. SOC 3

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 16

Topic #: 1

[All CISSP Questions]

Which application type is considered high risk and provides a common way for malware and viruses to enter a network?

A. Instant messaging or chat applications

B. Peer-to-Peer (P2P) file sharing applications

C. E-mail applications

D. End-to-end applications

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 17

Topic #: 1

[All CISSP Questions]

An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

A. 0

B. 1

C. 2

D. 3

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 18

Topic #: 1

[All CISSP Questions]

Which of the following is the BEST way to protect an organization's data assets?

A. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.

B. Monitor and enforce adherence to security policies.

C. Require Multi-Factor Authentication (MFA) and Separation of Duties (SoD).

D. Create the Demilitarized Zone (DMZ) with proxies, firewalls and hardened bastion hosts.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 19

Topic #: 1

[All CISSP Questions]

Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

A. Training department

B. Internal audit

C. Human resources

D. Information technology (IT)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 20

Topic #: 1

[All CISSP Questions]

Which of the following is the PRIMARY purpose of installing a mantrap within a facility?

A. Control traffic

B. Control air flow

C. Prevent piggybacking

D. Prevent rapid movement

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 21

Topic #: 1

[All CISSP Questions]

In the "Do" phase of the Plan-Do-Check-Act model, which of the following is performed?

A. Maintain and improve the Business Continuity Management (BCM) system by taking corrective action, based on the results of management review.

B. Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.

C. Ensure the business continuity policy, controls, processes, and procedures have been implemented.

D. Ensure that business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity have been established.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 22

Topic #: 1

[All CISSP Questions]

What industry-recognized document could be used as a baseline reference that is related to data security and business operations or conducting a security assessment?

A. Service Organization Control (SOC) 1 Type 2

B. Service Organization Control (SOC) 1 Type 1

C. Service Organization Control (SOC) 2 Type 2

D. Service Organization Control (SOC) 2 Type 1

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 23

Topic #: 1

[All CISSP Questions]

A criminal organization is planning an attack on a government network. Which of the following scenarios presents the HIGHEST risk to the organization?

A. Organization loses control of their network devices.

B. Network is flooded with communication traffic by the attacker.

C. Network management communications is disrupted.

D. Attacker accesses sensitive information regarding the network topology.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 24

Topic #: 1

[All CISSP Questions]

Which reporting type requires a service organization to describe its system and define its control objectives and controls that are relevant to users' internal control over financial reporting?

A. Statement on Auditing Standards (SAS) 70

B. Service Organization Control 1 (SOC1)

C. Service Organization Control 2 (SOC2)

D. Service Organization Control 3 (SOC3)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 25

Topic #: 1

[All CISSP Questions]

Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

A. Scheduled team review of coding style and techniques for vulnerability patterns

B. The regular use of production code routines from similar applications already in use

C. Using automated programs to test for the latest known vulnerability patterns

D. Ensure code editing tools are updated against known vulnerability patterns

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 26

Topic #: 1

[All CISSP Questions]

When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should the considerations be prioritized?

A. Public safety, duties to individuals, duties to the profession, and duties to principals

B. Public safety, duties to principals, duties to the profession, and duties to individuals

C. Public safety, duties to principals, duties to individuals, and duties to the profession

D. Public safety, duties to the profession, duties to principals, and duties to individuals

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 27

Topic #: 1

[All CISSP Questions]

Which service management process BEST helps information technology (IT) organizations with reducing cost, mitigating risk, and improving customer service?

A. Kanban

B. Lean Six Sigma

C. Information Technology Service Management (ITSM)

D. Information Technology Infrastructure Library (ITIL)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 28

Topic #: 1

[All CISSP Questions]

A company is attempting to enhance the security of its user authentication processes. After evaluating several options, the company has decided to utilize Identity as a Service (IDaaS). Which of the following factors leads the company to choose an IDaaS as their solution?

A. In-house team lacks resources to support an on-premise solution.

B. Third-party solutions are inherently more secure.

C. Third-party solutions are known for transferring the risk to the vendor.

D. In-house development provides more control.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 29

Topic #: 1

[All CISSP Questions]

An organization recently suffered from a web-application attack that resulted in stolen user session cookie information. The attacker was able to obtain the information when a user's browser executed a script upon visiting a compromised website. What type of attack MOST likely occurred?

A. SQL injection (SQLi)

B. Extensible Markup Language (XML) external entities

C. Cross-Site Scripting (XSS)

D. Cross-Site Request Forgery (CSRF)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 30

Topic #: 1

[All CISSP Questions]

An attack utilizing social engineering and a malicious Uniform Resource Locator (URL) link to take advantage of a victim's existing browser session with a web application is an example of which of the following types of attack?

A. Clickjacking

B. Cross-site request forgery (CSRF)

C. Cross-Site Scripting (XSS)

D. Injection

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 31

Topic #: 1

[All CISSP Questions]

Which of the following encryption technologies has the ability to function as a stream cipher?

A. Cipher Block Chaining (CBC) with error propagation

B. Electronic Code Book (ECB)

C. Cipher Feedback (CFB)

D. Feistel cipher

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 32

Topic #: 1

[All CISSP Questions]

In a disaster recovery (DR) test, which of the following would be a trait of crisis management?

A. Process

B. Anticipate

C. Strategic

D. Wide focus

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 33

Topic #: 1

[All CISSP Questions]

Which of the following BEST describes the purpose of the reference monitor when defining access control to enforce the security model?

A. Strong operational security to keep unit members safe

B. Policies to validate organization rules

C. Cyber hygiene to ensure organizations can keep systems healthy

D. Quality design principles to ensure quality by design

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 34

Topic #: 1

[All CISSP Questions]

Which of the following is security control volatility?

A. A reference to the impact of the security control.

B. A reference to the likelihood of change in the security control.

C. A reference to how unpredictable the security control is.

D. A reference to the stability of the security control.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 35

Topic #: 1

[All CISSP Questions]

When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

A. Planning

B. Risk assessment

C. Due diligence

D. Requirements

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 36

Topic #: 1

[All CISSP Questions]

What is the term used to define where data is geographically stored in the cloud?

A. Data privacy rights

B. Data sovereignty

C. Data warehouse

D. Data subject rights

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 37

Topic #: 1

[All CISSP Questions]

Which of the following does the security design process ensure within the System Development Life Cycle (SDLC)?

A. Proper security controls, security objectives, and security goals are properly initiated.

B. Security objectives, security goals, and system test are properly conducted.

C. Proper security controls, security goals, and fault mitigation are properly conducted.

D. Security goals, proper security controls, and validation are properly initiated.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 38

Topic #: 1

[All CISSP Questions]

Which of the following is MOST important to follow when developing information security controls for an organization?

A. Use industry standard best practices for security controls in the organization.

B. Exercise due diligence with regard to all risk management information to tailor appropriate controls.

C. Review all local and international standards and choose the most stringent based on location.

D. Perform a risk assessment and choose a standard that addresses existing gaps.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 39

Topic #: 1

[All CISSP Questions]

When recovering from an outage, what is the Recovery Point Objective (RPO), in terms of data recovery?

A. The RPO is the minimum amount of data that needs to be recovered.

B. The RPO is the amount of time it takes to recover an acceptable percentage of data lost.

C. The RPO is a goal to recover a targeted percentage of data lost.

D. The RPO is the maximum amount of time for which loss of data is acceptable.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 40

Topic #: 1

[All CISSP Questions]

Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

A. A brute force password attack on the Secure Shell (SSH) port of the controller

B. Sending control messages to open a flow that does not pass a firewall from a compromised host within the network

C. Remote Authentication Dial-In User Service (RADIUS) token replay attack

D. Sniffing the traffic of a compromised host inside the network

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 41

Topic #: 1

[All CISSP Questions]

Which of the following is the BEST option to reduce the network attack surface of a system?

A. Disabling unnecessary ports and services

B. Ensuring that there are no group accounts on the system

C. Uninstalling default software on the system

D. Removing unnecessary system user accounts

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 42

Topic #: 1

[All CISSP Questions]

The security architect is designing and implementing an internal certification authority to generate digital certificates for all employees. Which of the following is the BEST solution to securely store the private keys?

A. Physically secured storage device

B. Trusted Platform Module (TPM)

C. Encrypted flash drive

D. Public key infrastructure (PKI)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 43

Topic #: 1

[All CISSP Questions]

The existence of physical barriers, card and personal identification number (PIN) access systems, cameras, alarms, and security guards BEST describes this security approach?

A. Access control

B. Security information and event management (SIEM)

C. Defense-in-depth

D. Security perimeter

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 44

Topic #: 1

[All CISSP Questions]

A hospital enforces the Code of Fair Information Practices. What practice applies to a patient requesting their medical records from a web portal?

A. Purpose specification

B. Collection limitation

C. Use limitation

D. Individual participation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 45

Topic #: 1

[All CISSP Questions]

A colleague who recently left the organization asked a security professional for a copy of the organization's confidential incident management policy. Which of the following is the BEST response to this request?

A. Access the policy on a company-issued device and let the former colleague view the screen.

B. E-mail the policy to the colleague as they were already part of the organization and familiar with it.

C. Do not acknowledge receiving the request from the former colleague and ignore them.

D. Submit the request using company official channels to ensure the policy is okay to distribute.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 46

Topic #: 1

[All CISSP Questions]

Which of the following BEST describes when an organization should conduct a black box security audit on a new software protect?

A. When the organization wishes to check for non-functional compliance

B. When the organization wants to enumerate known security vulnerabilities across their infrastructure

C. When the organization is confident the final source code is complete

D. When the organization has experienced a security incident

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 47

Topic #: 1

[All CISSP Questions]

In software development, which of the following entities normally signs the code to protect the code integrity?

A. The organization developing the code

B. The quality control group

C. The developer

D. The data owner

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 48

Topic #: 1

[All CISSP Questions]

Which of the following technologies can be used to monitor and dynamically respond to potential threats on web applications?

A. Field-level tokenization

B. Web application vulnerability scanners

C. Runtime application self-protection (RASP)

D. Security Assertion Markup Language (SAML)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 49

Topic #: 1

[All CISSP Questions]

A security architect is developing an information system for a client. One of the requirements is to deliver a platform that mitigates against common vulnerabilities and attacks. What is the MOST efficient option used to prevent buffer overflow attacks?

A. Access control mechanisms

B. Process isolation

C. Address Space Layout Randomization (ASLR)

D. Processor states

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 50

Topic #: 1

[All CISSP Questions]

In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews?

A. Implement bi-annual reviews.

B. Create policies for system access.

C. Implement and review risk-based alerts.

D. Increase logging levels.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 51

Topic #: 1

[All CISSP Questions]

A corporation does not have a formal data destruction policy. During which phase of a criminal legal proceeding will this have the MOST impact?

A. Sentencing

B. Trial

C. Discovery

D. Arraignment

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 52

Topic #: 1

[All CISSP Questions]

What is considered the BEST explanation when determining whether to provide remote network access to a third-party security service?

A. Contract negotiation

B. Supplier request

C. Business need

D. Vendor demonstration

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 53

Topic #: 1

[All CISSP Questions]

The acquisition of personal data being obtained by a lawful and fair means is an example of what principle?

A. Collection Limitation Principle

B. Openness Principle

C. Purpose Specification Principle

D. Data Quality Principle

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 54

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST appropriate control for asset data labeling procedures?

A. Categorizing the types of media being used

B. Logging data media to provide a physical inventory control

C. Reviewing off-site storage access controls

D. Reviewing audit trails of logging records

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 55

Topic #: 1

[All CISSP Questions]

What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

A. Swapping data

B. Randomizing data

C. Encoding data

D. Encrypting data

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 56

Topic #: 1

[All CISSP Questions]

Which of the following departments initiates the request, approval, and provisioning business process?

A. Operations

B. Security

C. Human resources (HR)

D. Information technology (IT)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 57

Topic #: 1

[All CISSP Questions]

An organization is setting a security assessment scope with the goal of developing a Security Management Program (SMP). The next step is to select an approach for conducting the risk assessment. Which of the following approaches is MOST effective for the SMP?

A. Security controls driven assessment that focuses on controls management

B. Business processes based risk assessment with a focus on business goals

C. Asset driven risk assessment with a focus on the assets

D. Data driven risk assessment with a focus on data

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 58

Topic #: 1

[All CISSP Questions]

Which technique helps system designers consider potential security concerns of their systems and applications?

A. Threat modeling

B. Manual inspections and reviews

C. Source code review

D. Penetration testing

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 59

Topic #: 1

[All CISSP Questions]

A security professional can BEST mitigate the risk of using a Commercial Off-The-Shelf (COTS) solution by deploying the application with which of the following controls in place?

A. Network segmentation

B. Blacklisting application

C. Whitelisting application

D. Hardened configuration

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 60

Topic #: 1

[All CISSP Questions]

Which of the following BEST describes centralized identity management?

A. Service providers perform as both the credential and identity provider (IdP).

B. Service providers identify an entity by behavior analysis versus an identification factor.

C. Service providers agree to integrate identity system recognition across organizational boundaries.

D. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 61

Topic #: 1

[All CISSP Questions]

What is the MOST significant benefit of role-based access control (RBAC)?

A. Reduces inappropriate access

B. Management of least privilege

C. Most granular form of access control

D. Reduction in authorization administration overhead

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 62

Topic #: 1

[All CISSP Questions]

What is the MOST common security risk of a mobile device?

A. Data spoofing

B. Malware infection

C. Insecure communications link

D. Data leakage

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 63

Topic #: 1

[All CISSP Questions]

What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

A. RAID-0

B. RAID-1

C. RAID-5

D. RAID-6

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 64

Topic #: 1

[All CISSP Questions]

What type of risk is related to the sequences of value-adding and managerial activities undertaken in an organization?

A. Control risk

B. Demand risk

C. Supply risk

D. Process risk

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 65

Topic #: 1

[All CISSP Questions]

International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

A. International Traffic in Arms Regulations (ITAR)

B. Palermo convention

C. Wassenaar arrangement

D. General Data Protection Regulation (GDPR)

Show Suggested Answer

Actual exam question from ISC's CISSP
Question #: 66
Topic #: 1
[All CISSP Questions]

An organization has implemented a protection strategy to secure the network from unauthorized external access. The new Chief Information Security Officer (CISO) wants to increase security by better protecting the network from unauthorized internal access. Which Network Access Control (NAC) capability BEST meets this objective?

A. Port security
B. Two-factor authentication (2FA)
C. Strong passwords
D. Application firewall

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 67

Topic #: 1

[All CISSP Questions]

Which section of the assessment report addresses separate vulnerabilities, weaknesses, and gaps?

A. Findings definition section

B. Risk review section

C. Executive summary with full details

D. Key findings section

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 68

Topic #: 1

[All CISSP Questions]

Why is data classification control important to an organization?

A. To enable data discovery

B. To ensure security controls align with organizational risk appetite

C. To ensure its integrity, confidentiality and availability

D. To control data retention in alignment with organizational policies and regulation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 69

Topic #: 1

[All CISSP Questions]

To monitor the security of buried data lines inside the perimeter of a facility, which of the following is the MOST effective control?

A. Fencing around the facility with closed-circuit television (CCTV) cameras at all entry points

B. Ground sensors installed and reporting to a security event management (SEM) system

C. Regular sweeps of the perimeter, including manual inspection of the cable ingress points

D. Steel casing around the facility ingress points

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 70

Topic #: 1

[All CISSP Questions]

An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

A. It should be expressed as general requirements.

B. It should be expressed as technical requirements.

C. It should be expressed in business terminology.

D. It should be expressed in legal terminology.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 71

Topic #: 1

[All CISSP Questions]

Which access control method is based on users issuing access requests on system resources, features assigned to those resources, the operational or situational context, and a set of policies specified in terms of those features and context?

A. Mandatory Access Control (MAC)

B. Attribute Based Access Control (ABAC)

C. Role Based Access Control (RBAC)

D. Discretionary Access Control (DAC)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 72

Topic #: 1

[All CISSP Questions]

What is a security concern when considering implementing software-defined networking (SDN)?

A. It has a decentralized architecture.

B. It increases the attack footprint.

C. It uses open source protocols.

D. It is cloud based.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 73

Topic #: 1

[All CISSP Questions]

What is the BEST way to restrict access to a file system on computing systems?

A. Use least privilege at each level to restrict access.

B. Restrict access to all users.

C. Allow a user group to restrict access.

D. Use a third-party tool to restrict access.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 74

Topic #: 1

[All CISSP Questions]

Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

A. Avoid lengthy audit reports

B. Enable generation of corrective action reports

C. Facilitate a root cause analysis (RCA)

D. Lower costs throughout the System Development Life Cycle (SDLC)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 75

Topic #: 1

[All CISSP Questions]

What is the correct order of execution for security architecture?

A. Governance, strategy and program management, operations, project delivery

B. Governance, strategy and program management, project delivery, operations

C. Strategy and program management, project delivery, governance, operations

D. Strategy and program management, governance, project delivery, operations

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 76

Topic #: 1

[All CISSP Questions]

An international organization has decided to use a Software as a Service (SaaS) solution to support its business operations. Which of the following compliance standards should the organization use to assess the international code security and data privacy of the solution?

A. Service Organization Control (SOC) 2

B. Information Assurance Technical Framework (IATF)

C. Health Insurance Portability and Accountability Act (HIPAA)

D. Payment Card Industry (PCI)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 77

Topic #: 1

[All CISSP Questions]

An authentication system that uses challenge and response was recently implemented on an organization's network, because the organization conducted an annual penetration test showing that testers were able to move laterally using authenticated credentials. Which attack method was MOST likely used to achieve this?

A. Hash collision

B. Pass the ticket

C. Brute force

D. Cross-Site Scripting (XSS)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 78

Topic #: 1

[All CISSP Questions]

Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation (GDPR)?

A. For the establishment, exercise, or defense of legal claims

B. The personal data has been lawfully processed and collected

C. For the reasons of private interest

D. The personal data remains necessary to the purpose for which it was collected

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 79

Topic #: 1

[All CISSP Questions]

Dumpster diving is a technique used in which stage of penetration testing methodology?

A. Attack

B. Reporting

C. Planning

D. Discovery

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 80

Topic #: 1

[All CISSP Questions]

Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

A. Employee evaluation of the training program

B. Internal assessment of the training program's effectiveness

C. Multiple choice tests to participants

D. Management control of reviews

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 81

Topic #: 1

[All CISSP Questions]

The security team is notified that a device on the network is infected with malware. Which of the following is MOST effective in enabling the device to be quickly located and remediated?

A. Data loss protection (DLP)

B. Intrusion detection

C. Vulnerability scanner

D. Information Technology Asset Management (ITAM)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 82

Topic #: 1

[All CISSP Questions]

Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

A. Distributed denial-of-service (DDoS) attack

B. Advanced persistent threat (APT) attempt

C. Zero-day attack

D. Phishing attempt

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 83

Topic #: 1

[All CISSP Questions]

As a design principle, which one of the following actors is responsible for identifying and approving data security requirement in a cloud ecosystem?

A. Cloud auditor

B. Cloud broker

C. Cloud provider

D. Cloud consumer

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 84

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network?

A. Network Access Control (NAC)

B. Privileged Access Management (PAM)

C. Group Policy Object (GPO)

D. Mobile Device Management (MDM)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 85

Topic #: 1

[All CISSP Questions]

Which one of the following BEST protects vendor accounts that are used for emergency maintenance?

A. Vendor access should be disabled until needed

B. Frequent monitoring of vendor access

C. Role-based access control (RBAC)

D. Encryption of routing tables

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 86

Topic #: 1

[All CISSP Questions]

Which event magnitude is defined as deadly, destructive, and disruptive when a hazard interacts with human vulnerability?

A. Crisis

B. Catastrophe

C. Accident

D. Disaster

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 87

Topic #: 1

[All CISSP Questions]

Which of the following BEST describes the purpose of software forensics?

A. To analyze possible malicious intent of malware

B. To perform cyclic redundancy check (CRC) verification and detect changed applications

C. To determine the author and behavior of the code

D. To review program code to determine the existence of backdoors

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 88

Topic #: 1

[All CISSP Questions]

A web developer is completing a new web application security checklist before releasing the application to production. The task of disabling unnecessary services is on the checklist. Which web application threat is being mitigated by this action?

A. Session hijacking

B. Security misconfiguration

C. Broken access control

D. Sensitive data exposure

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 89

Topic #: 1

[All CISSP Questions]

What is the BEST method to use for assessing the security impact of acquired software?

A. Threat modeling

B. Common vulnerability review

C. Software security compliance validation

D. Vendor assessment

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 90

Topic #: 1

[All CISSP Questions]

Which of the following ensures old log data is not overwritten?

A. Log retention

B. Implement Syslog

C. Increase log file size

D. Log preservation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 91

Topic #: 1

[All CISSP Questions]

Under the General Data Protection Regulation (GDPR), what is the maximum amount of time allowed for reporting a personal data breach?

A. 24 hours

B. 48 hours

C. 72 hours

D. 96 hours

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 92

Topic #: 1

[All CISSP Questions]

A financial organization that works according to agile principles has developed a new application for their external customer base to request a line of credit. A security analyst has been asked to assess the security risk of the minimum viable product (MVP). Which is the MOST important activity the analyst should assess?

A. The software has been signed off for release by the product owner.

B. The software had been branded according to corporate standards.

C. The software has the correct functionality.

D. The software has been code reviewed.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 93

Topic #: 1

[All CISSP Questions]

An application developer receives a report back from the security team showing their automated tools were able to successfully enter unexpected data into the organization's customer service portal, causing the site to crash. This is an example of which type of testing?

A. Performance

B. Positive

C. Non-functional

D. Negative

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 94

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST effective strategy to prevent an attacker from disabling a network?

A. Design networks with the ability to adapt, reconfigure, and fail over.

B. Test business continuity and disaster recovery (DR) plans.

C. Follow security guidelines to prevent unauthorized network access.

D. Implement network segmentation to achieve robustness.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 95

Topic #: 1

[All CISSP Questions]

What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

A. Policy creation

B. Information Rights Management (IRM)

C. Data classification

D. Configuration management (CM)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 96

Topic #: 1

[All CISSP Questions]

Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

A. Change driver

B. Project manager

C. Program sponsor

D. Change implementer

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 97

Topic #: 1

[All CISSP Questions]

A company needs to provide shared access of sensitive data on a cloud storage to external business partners. Which of the following identity models is the BEST to blind identity providers (IdP) and relying parties (RP) so that subscriber lists of other parties are not disclosed?

A. Proxied federation

B. Dynamic registration

C. Federation authorities

D. Static registration

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 98

Topic #: 1

[All CISSP Questions]

A security professional needs to find a secure and efficient method of encrypting data on an endpoint. Which solution includes a root key?

A. Bitlocker

B. Trusted Platform Module (TPM)

C. Virtual storage array network (VSAN)

D. Hardware security module (HSM)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 99

Topic #: 1

[All CISSP Questions]

Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

A. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) > 128 bits Digital Signature: Digital Signature Algorithm (DSA) (>=2048 bits)

B. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) > 128 bits Digital Signature: Rivest-Shamir-Adleman (RSA) (1024 bits)

C. Diffie-hellman (DH) key exchange: DH (<=1024 bits) Symmetric Key: Blowfish Digital Signature: Rivest-Shamir-Adleman (RSA) (>=2048 bits)

D. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) < 128 bits Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) (>=256 bits)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 100

Topic #: 1

[All CISSP Questions]

What is the PRIMARY purpose of creating and reporting metrics for a security awareness, training, and education program?

A. Measure the effect of the program on the organization's workforce.

B. Make all stakeholders aware of the program's progress.

C. Facilitate supervision of periodic training events.

D. Comply with legal regulations and document due diligence in security practices.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 101

Topic #: 1

[All CISSP Questions]

In a DevOps environment, which of the following actions is MOST necessary to have confidence in the quality of the changes being made?

A. Prepare to take corrective actions quickly.

B. Automate functionality testing.

C. Review logs for any anomalies.

D. Receive approval from the change review board.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 102

Topic #: 1

[All CISSP Questions]

What is the MAIN purpose of a security assessment plan?

A. Provide education to employees on security and privacy, to ensure their awareness on policies and procedures.

B. Provide the objectives for the security and privacy control assessments and a detailed roadmap of how to conduct such assessments.

C. Provide guidance on security requirements, to ensure the identified security risks are properly addressed based on the recommendation.

D. Provide technical information to executives to help them understand information security postures and secure funding.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 103

Topic #: 1

[All CISSP Questions]

What documentation is produced FIRST when performing an effective physical loss control process?

A. Deterrent controls list

B. Security standards list

C. Asset valuation list

D. Inventory list

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 104

Topic #: 1

[All CISSP Questions]

Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

A. Legal

B. Audit

C. Compliance

D. Security

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 105

Topic #: 1

[All CISSP Questions]

A cloud service provider requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of three months. The audit logging gene has extremely high amount of logs. What is the MOST appropriate strategy for the log retention?

A. Keep all logs in an online storage.

B. Keep last week's logs in an online storage and the rest in an offline storage.

C. Keep last week's logs in an online storage and the rest in a near-line storage.

D. Keep all logs in an offline storage.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 106

Topic #: 1

[All CISSP Questions]

In Federated Identity Management (FIM), which of the following represents the concept of federation?

A. Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories or applications

B. Collection of information logically grouped into a single entity

C. Collection of information for common identities in a system

D. Collection of domains that have established trust among themselves

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 107

Topic #: 1

[All CISSP Questions]

Which of the following is an indicator that a company's new user security awareness training module has been effective?

A. There are more secure connections to internal e-mail servers.

B. More incidents of phishing attempts are being reported.

C. Fewer incidents of phishing attempts are being reported.

D. There are more secure connections to the internal database servers.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 108

Topic #: 1

[All CISSP Questions]

An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

A. IM clients can interoperate between multiple vendors.

B. IM clients can run as executables that do not require installation.

C. IM clients can utilize random port numbers.

D. IM clients can run without administrator privileges.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 109

Topic #: 1

[All CISSP Questions]

Using the cipher text and resultant cleartext message to derive the monoalphabetic cipher key is an example of which method of cryptanalytic attack?

A. Known-plaintext attack

B. Ciphertext-only attack

C. Frequency analysis

D. Probable-plaintext attack

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 110

Topic #: 1

[All CISSP Questions]

When developing an organization's information security budget, it is important that the:

A. requested funds are at an equal amount to the expected cost of breaches.

B. expected risk can be managed appropriately with the funds allocated.

C. requested funds are part of a shared funding pool with other areas.

D. expected risk to the organization does not exceed the funds allocated.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 111

Topic #: 1

[All CISSP Questions]

A subscription service which provides power, climate control, raised flooring, and telephone wiring but NOT the computer and peripheral equipment is BEST described as a:

A. cold site.

B. warm site.

C. hot site.

D. reciprocal site.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 112

Topic #: 1

[All CISSP Questions]

An international trading organization that holds an International Organization for Standardization (ISO) 27001 certification is seeking to outsource their security monitoring to a managed security service provider (MSSP). The trading organization's security officer is tasked with drafting the requirements that need to be included in the outsourcing contract. Which of the following MUST be included in the contract?

A. A detailed overview of all equipment involved in the outsourcing contract

B. The right to perform security compliance tests on the MSSP's equipment

C. The MSSP having an executive manager responsible for information security

D. The right to audit the MSSP's security process

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 113

Topic #: 1

[All CISSP Questions]

Which of the following is the PRIMARY type of cryptography required to support non-repudiation of a digitally signed document?

A. Hashing

B. Message digest (MD)

C. Symmetric

D. Asymmetric

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 114

Topic #: 1

[All CISSP Questions]

What is the MOST effective method to enhance security of a single sign-on (SSO) solution that interfaces with critical systems?

A. Two-factor authentication

B. Reusable tokens for application level authentication

C. High performance encryption algorithms

D. Secure Sockets Layer (SSL) for all communications

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 115

Topic #: 1

[All CISSP Questions]

Which of the following is MOST appropriate to collect evidence of a zero-day attack?

A. Honeypot

B. Antispam

C. Antivirus

D. Firewall

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 116

Topic #: 1

[All CISSP Questions]

When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test?

A. Information may be found on hidden vendor patches.

B. The actual origin and tools used for the test can be hidden.

C. Information may be found on related breaches and hacking.

D. Vulnerabilities can be tested without impact on the tested environment.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 117

Topic #: 1

[All CISSP Questions]

The quality assurance (QA) department is short-staffed and is unable to test all modules before the anticipated release date of an application. What security control is MOST likely to be violated?

A. Change management

B. Separation of environments

C. Program management

D. Mobile code controls

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 118

Topic #: 1

[All CISSP Questions]

Which of the following criteria ensures information is protected relative to its importance to the organization?

A. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification

B. The value of the data to the organization's senior management

C. Organizational stakeholders, with classification approved by the management board

D. Legal requirements determined by the organization headquarters' location

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 119

Topic #: 1

[All CISSP Questions]

What is the FIRST step when developing an Information Security Continuous Monitoring (ISCM) program?

A. Collect the security-related information required for metrics, assessments, and reporting.

B. Establish an ISCM program determining metrics, status monitoring frequencies, and control assessment frequencies.

C. Define an ISCM strategy based on risk tolerance.

D. Establish an ISCM technical architecture.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 120

Topic #: 1

[All CISSP Questions]

An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

A. RAID level 1

B. RAID level 3

C. RAID level 4

D. RAID level 5

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 121

Topic #: 1

[All CISSP Questions]

Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

A. Centralized network provisioning

B. Reduced network latency when scaled

C. Centralized network administrative control

D. Reduced hardware footprint and cost

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 122

Topic #: 1

[All CISSP Questions]

What is the MOST effective response to a hacker who has already gained access to a network and will attempt to pivot to other resources?

A. Warn users of a breach.

B. Reset all passwords.

C. Segment the network.

D. Shut down the network.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 123

Topic #: 1

[All CISSP Questions]

Which of the following is a common term for log reviews, synthetic transactions, and code reviews?

A. Application development

B. Spiral development functional testing

C. Security control testing

D. DevOps Integrated Product Team (IPT) development

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 124

Topic #: 1

[All CISSP Questions]

A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

A. Data sanitization

B. Data validation

C. Service accounts removal

D. Logging and monitoring

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 125

Topic #: 1

[All CISSP Questions]

The Industrial Control System (ICS) Computer Emergency Response Team (CERT) has released an alert regarding ICS-focused malware specifically propagating through Windows-based business networks. Technicians at a local water utility note that their dams, canals, and locks controlled by an internal Supervisory Control and Data Acquisition (SCADA) system have been malfunctioning. A digital forensics professional is consulted in the Incident Response (IR) and recovery. Which of the following is the MOST challenging aspect of this investigation?

A. Group policy implementation

B. SCADA network latency

C. Physical access to the system

D. Volatility of data

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 126

Topic #: 1

[All CISSP Questions]

What term is commonly used to describe hardware and software assets that are stored in a configuration management database (CMDB)?

A. Configuration item

B. Configuration element

C. Ledger item

D. Asset register

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 127

Topic #: 1

[All CISSP Questions]

A company is planning to implement a private cloud infrastructure. Which of the following recommendations will support the move to a cloud infrastructure?

A. Implement software-defined networking (SDN) to provide the ability to apply high-level policies to shape and reorder network traffic based on users, devices and applications.

B. Implement a virtual local area network (VLAN) for each department and create a separate subnet for each VLAN.

C. Implement software-defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes.

D. Implement a virtual local area network (VLAN) to logically separate the local area network (LAN) from the physical switches.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 128

Topic #: 1

[All CISSP Questions]

Which is MOST important when negotiating an Internet service provider (ISP) service-level agreement (SLA) by an organization that solely provides Voice over Internet Protocol (VoIP) services?

A. Mean time to repair (MTTR)

B. Quality of Service (QoS) between applications

C. Financial penalties in case of disruption

D. Availability of network services

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 129

Topic #: 1

[All CISSP Questions]

A company hired an external vendor to perform a penetration test of a new payroll system. The company's internal test team had already performed an in-depth application and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive personal data was being sent unencrypted to the tax processing systems. What is the MOST likely cause of the security issues?

A. Inadequate performance testing

B. Inadequate application level testing

C. Failure to perform negative testing

D. Failure to perform interface testing

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 130

Topic #: 1

[All CISSP Questions]

An organization wants to define as physical perimeter. What primary device should be used to accomplish this objective if the organization's perimeter MUST cost-efficiently deter casual trespassers?

A. Fences three to four feet high with a turnstile

B. Fences six to seven feet high with a painted gate

C. Fences accompanied by patrolling security guards

D. Fences eight or more feet high with three strands of barbed wire

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 131

Topic #: 1

[All CISSP Questions]

Which of the following vulnerabilities can be BEST detected using automated analysis?

A. Multi-step process attack vulnerabilities

B. Business logic flaw vulnerabilities

C. Valid cross-site request forgery (CSRF) vulnerabilities

D. Typical source code vulnerabilities

Show Suggested Answer

Actual exam question from ISC's CISSP
Question #: 132
Topic #: 1
[All CISSP Questions]

A project manager for a large software firm has acquired a government contract that generates large amounts of Controlled Unclassified Information (CUI). The organization's information security manager had received a request to transfer project-related CUI between systems of differing security classifications. What role provides the authoritative guidance for this transfer?

A. PM

B. Information owner

C. Data Custodian

D. Mission/Business Owner

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 133

Topic #: 1

[All CISSP Questions]

Which of the following determines how traffic should flow based on the status of the infrastructure layer?

A. Control plane

B. Application plane

C. Traffic plane

D. Data plane

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 134

Topic #: 1

[All CISSP Questions]

When testing password strength, which of the following is the BEST method for brute forcing passwords?

A. Conduct an offline attack on the hashed password information.

B. Use a comprehensive list of words to attempt to guess the password.

C. Use social engineering methods to attempt to obtain the password.

D. Conduct an online password attack until the account being used is locked.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 135

Topic #: 1

[All CISSP Questions]

Which of the following is the name of an individual or group that is impacted by a change?

A. Change agent

B. End User

C. Stakeholder

D. Sponsor

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 136

Topic #: 1

[All CISSP Questions]

The European Union (EU) General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The Data Owner should therefore consider which of the following requirements?

A. Never to store personal data of EU citizens outside the EU

B. Data masking and encryption of personal data

C. Only to use encryption protocols approved by EU

D. Anonymization of personal data when transmitted to sources outside the EU

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 137

Topic #: 1

[All CISSP Questions]

What is the PRIMARY benefit of incident reporting and computer crime investigations?

A. Complying with security policy

B. Repairing the damage and preventing future occurrences

C. Providing evidence to law enforcement

D. Appointing a computer emergency response team

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 138

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST common method of memory protection?

A. Error correction

B. Virtual local area network (VLAN) tagging

C. Segmentation

D. Compartmentalization

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 139

Topic #: 1

[All CISSP Questions]

What testing technique enables the designer to develop mitigation strategies for potential vulnerabilities?

A. Source code review

B. Threat modeling

C. Penetration testing

D. Manual inspections and reviews

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 140

Topic #: 1

[All CISSP Questions]

Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

A. Store information about browsing activities on the personal device.

B. Prevent information about browsing activities from being stored on the personal device.

C. Prevent information about browsing activities from being stored in the cloud.

D. Store browsing activities in the cloud.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 141

Topic #: 1

[All CISSP Questions]

A software engineer uses automated tools to review application code and search for application flaws, back doors, or other malicious code. Which of the following is the FIRST Software Development Life Cycle (SDLC) phase where this takes place?

A. Deployment

B. Development

C. Test

D. Design

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 142

Topic #: 1

[All CISSP Questions]

A company developed a web application which is sold as a Software as a Service (SaaS) solution to the customer. The application is hosted by a web server running on a specific operating system (OS) on a virtual machine (VM). During the transition phase of the service, it is determined that the support team will need access to the application logs. Which of the following privileges would be the MOST suitable?

A. Administrative privileges on the hypervisor

B. Administrative privileges on the application folders

C. Administrative privileges on the web server

D. Administrative privileges on the OS

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 143

Topic #: 1

[All CISSP Questions]

A security practitioner detects an Endpoint attack on the organization's network. What is the MOST reasonable approach to mitigate future Endpoint attacks?

A. Remove all non-essential client-side web services from the network.

B. Harden the client image before deployment.

C. Screen for harmful exploits of client-side services before implementation.

D. Block all client-side web exploits at the perimeter.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 144

Topic #: 1

[All CISSP Questions]

What are the essential elements of a Risk Assessment Report (RAR)?

A. Executive summary, body of the report, and appendices

B. Executive summary, graph of risks, and process

C. Table of contents, testing criteria, and index

D. Table of contents, chapters, and executive summary

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 145

Topic #: 1

[All CISSP Questions]

The security operations center (SOC) has received credible intelligence that a threat actor is planning to attack with multiple variants of a destructive virus. After obtaining a sample set of this virus' variants and reverse engineering them to understand how they work, a commonality was found. All variants are coded to write to a specific memory location. It is determined this virus is of no threat to the organization because they had the foresight to enable what feature on all endpoints?

A. Address Space Layout Randomization (ASLR)

B. Trusted Platform Module (TPM)

C. Virtualization

D. Process isolation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 146

Topic #: 1

[All CISSP Questions]

The Chief Information Security Officer (CISO) is to establish a single, centralized, and relational repository to hold all information regarding the software and hardware assets. Which of the following s ions would be the BEST option?

A. Information Security Management System (ISMS)

B. Configuration Management Database (CMDB)

C. Security Information and Event Management (SIEM)

D. Information Technology Asset Management (ITAM)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 147

Topic #: 1

[All CISSP Questions]

What type of investigation applies when malicious behavior is suspected between two organizations?

A. Regulatory

B. Operational

C. Civil

D. Criminal

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 148

Topic #: 1

[All CISSP Questions]

Which of the following techniques evaluates the secure design principles of network or software architectures?

A. Risk modeling

B. Waterfall method

C. Threat modeling

D. Fuzzing

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 149

Topic #: 1

[All CISSP Questions]

Which element of software supply chain management has the GREATEST security risk to organizations?

A. Unsupported libraries are often used.

B. Applications with multiple contributors are difficult to evaluate.

C. Vulnerabilities are difficult to detect.

D. New software development skills are hard to acquire.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 150

Topic #: 1

[All CISSP Questions]

Which of the following should be done at a disaster site before any item is removed, repaired, or replaced?

A. Communicate with the press following the communications plan

B. Dispatch personnel to the disaster recovery (DR) site

C. Take photos of the damage

D. Notify all of the Board of Directors

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 151

Topic #: 1

[All CISSP Questions]

When designing a new Voice over Internet Protocol (VoIP) network, an organization's top concern is preventing unauthorized users accessing the VoIP network. Which of the following will BEST help secure the VoIP network?

A. 802.11g

B. Web application firewall (WAF)

C. Transport Layer Security (TLS)

D. 802.1x

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 152

Topic #: 1

[All CISSP Questions]

A user's credential for an application is stored in a relational database. Which control protects the confidentiality of the credential while it is stored?

A. Use a salted cryptographic hash of the password.

B. Validate passwords using a stored procedure.

C. Allow only the application to have access to the password field in order to verify user authentication.

D. Encrypt the entire database and embed an encryption key in the application.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 153

Topic #: 1

[All CISSP Questions]

Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

A. Common Vulnerabilities and Exposures (CVE)

B. Center for Internet Security (CIS)

C. Common Vulnerability Scoring System (CVSS)

D. Open Web Application Security Project (OWASP)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 154

Topic #: 1

[All CISSP Questions]

A security architect is reviewing plans for an application with a Recovery Point Objective (RPO) of 15 minutes. The current design has all of the application infrastructure located within one co-location data center. Which security principle is the architect currently assessing?

A. Disaster recovery (DR)

B. Availability

C. Redundancy

D. Business continuity (BC)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 155

Topic #: 1

[All CISSP Questions]

Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

A. System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements

B. Compliance office roles and responsibilities, classified material handling standards, storage system lifecycle requirements

C. Data stewardship roles, data handling and storage standards, data lifecycle requirements

D. System authorization roles and responsibilities, cloud computing standards, lifecycle requirements

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 156

Topic #: 1

[All CISSP Questions]

The Chief Information Security Officer (CISO) of a small organization is making a case for building a security operations center (SOC). While debating between an in-house, fully outsourced, or a hybrid capability, which of the following would be the MAIN consideration, regardless of the model?

A. Headcount and capacity

B. Scope and service catalog

C. Skill set and training

D. Tools and technologies

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 157

Topic #: 1

[All CISSP Questions]

An organization would like to ensure that all new users have a predefined departmental access template applied upon creation. The organization would also like additional access for users to be granted on a per-project basis. What type of user access administration is BEST suited to meet the organization's needs?

A. Decentralized

B. Hybrid

C. Centralized

D. Federated

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 158

Topic #: 1

[All CISSP Questions]

Which of the following is a secure design principle for a new product?

A. Restrict the use of modularization.

B. Do not rely on previously used code.

C. Build in appropriate levels of fault tolerance.

D. Utilize obfuscation whenever possible.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 159

Topic #: 1

[All CISSP Questions]

What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

A. Standardize specifications between software security products.

B. Achieve organizational compliance with international standards.

C. Improve vulnerability assessment capabilities.

D. Save security costs for the organization.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 160

Topic #: 1

[All CISSP Questions]

What are the three key benefits that application developers should derive from the northbound application programming interface (API) of software defined networking (SDN)?

A. Network syntax, abstraction of network flow, and abstraction of network protocols

B. Network syntax, abstraction of network commands, and abstraction of network protocols

C. Familiar syntax, abstraction of network topology, and definition of network protocols

D. Familiar syntax, abstraction of network topology, and abstraction of network protocols

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 161

Topic #: 1

[All CISSP Questions]

Which of the following is a unique feature of attribute-based access control (ABAC)?

A. A user is granted access to a system at a particular time of day.

B. A user is granted access to a system based on username and password.

C. A user is granted access to a system based on group affinity.

D. A user is granted access to a system with biometric authentication.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 162

Topic #: 1

[All CISSP Questions]

Which of the following is the BEST approach to implement multiple servers on a virtual system?

A. Implement one primary function per virtual server and apply individual security configuration for each virtual server.

B. Implement multiple functions within the same virtual server and apply individual security configurations to each function.

C. Implement one primary function per virtual server and apply high security configuration on the host operating system.

D. Implement multiple functions per virtual server and apply the same security configuration for each virtual server.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 163

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST common cause of system or security failures?

A. Lack of physical security controls

B. Lack of change control

C. Lack of logging and monitoring

D. Lack of system documentation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 164

Topic #: 1

[All CISSP Questions]

The Chief Information Officer (CIO) has decided that as part of business modernization efforts the organization will move towards a cloud architecture. All business-critical data will be migrated to either internal or external cloud services within the next two years. The CIO has a PRIMARY obligation to work with personnel in which role in order to ensure proper protection of data during and after the cloud migration?

A. Chief Security Officer (CSO)

B. Information owner

C. Chief Information Security Officer (CISO)

D. General Counsel

Show Suggested Answer

Actual exam question from ISC's CISSP
Question #: 165
Topic #: 1
[All CISSP Questions]

A developer is creating an application that requires secure logging of all user activity. What is the BEST permission the developer should assign to the log file to ensure requirements are met?

A. Execute

B. Read

C. Write

D. Append

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 166

Topic #: 1

[All CISSP Questions]

When performing an investigation with the potential for legal action, what should be the analyst's FIRST consideration?

A. Data decryption

B. Chain-of-custody

C. Authorization to collect

D. Court admissibility

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 167

Topic #: 1

[All CISSP Questions]

Building blocks for software-defined networks (SDN) require which of the following?

A. The SDN is composed entirely of client-server pairs.

B. Random-access memory (RAM) is used in preference to virtual memory.

C. The SDN is mostly composed of virtual machines (VM).

D. Virtual memory is used in preference to random-access memory (RAM).

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 168

Topic #: 1

[All CISSP Questions]

What is the MINIMUM standard for testing a disaster recovery plan (DRP)?

A. Quarterly or more frequently depending upon the advice of the information security manager

B. As often as necessary depending upon the stability of the environment and business requirements

C. Annually or less frequently depending upon audit department requirements

D. Semi-annually and in alignment with a fiscal half-year business cycle

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 169

Topic #: 1

[All CISSP Questions]

Which security audit standard provides the BEST way for an organization to understand a vendor's Information Systems (IS) in relation to confidentiality, integrity, and availability?

A. Service Organization Control (SOC) 2

B. Statement on Standards for Attestation Engagements (SSAE) 18

C. Statement on Auditing Standards (SAS) 70

D. Service Organization Control (SOC) 1

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 170

Topic #: 1

[All CISSP Questions]

An application team is running tests to ensure that user entry fields will not accept invalid input of any length. What type of negative testing is this an example of?

A. Allowed number of characters

B. Population of required fields

C. Reasonable data

D. Session testing

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 171

Topic #: 1

[All CISSP Questions]

An organization is considering partnering with a third-party supplier of cloud services. The organization will only be providing the data and the third-party supplier will be providing the security controls. Which of the following BEST describes this service offering?

A. Platform as a Service (PaaS)

B. Anything as a Service (XaaS)

C. Infrastructure as a Service (IaaS)

D. Software as a Service (SaaS)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 172

Topic #: 1

[All CISSP Questions]

Which of the following factors should be considered characteristics of Attribute Based Access Control (ABAC) in terms of the attributes used?

A. Mandatory Access Control (MAC) and Discretionary Access Control (DAC)

B. Discretionary Access Control (DAC) and Access Control List (ACL)

C. Role Based Access Control (RBAC) and Mandatory Access Control (MAC)

D. Role Based Access Control (RBAC) and Access Control List (ACL)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 173

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST significant key management problem due to the number of keys created?

A. Exponential growth when using symmetric keys

B. Exponential growth when using asymmetric keys

C. Storage of the keys require increased security

D. Keys are more difficult to provision and revoke

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 174

Topic #: 1

[All CISSP Questions]

Systems Security Professional (CISSP) with identity and access management (IAM) responsibilities is asked by the Chief Information Security Officer (CISO) to perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit. The CISSP has never performed this before. According to the (ISC)

Code of Professional Ethics, which of the following should the CISSP do?

A. Inform the CISO that they are unable to perform the task because they should render only those services for which they are fully competent and qualified

B. Since they are CISSP certified, they have enough knowledge to assist with the request, but will need assistance in order to complete it in a timely manner

C. Review the CISSP guidelines for performing a vulnerability assessment before proceeding to complete it

D. Review the PCI requirements before performing the vulnerability assessment

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 175

Topic #: 1

[All CISSP Questions]

While performing a security review for a new product, an information security professional discovers that the organization's product development team is proposing to collect government-issued identification (ID) numbers from customers to use as unique customer identifiers. Which of the following recommendations should be made to the product development team?

A. Customer identifiers should be a variant of the user's government-issued ID number.

B. Customer identifiers should be a cryptographic hash of the user's government-issued ID number.

C. Customer identifiers that do not resemble the user's government-issued ID number should be used.

D. Customer identifiers should be a variant of the user's name, for example, "jdoe" or "john.doe."

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 176

Topic #: 1

[All CISSP Questions]

The development team has been tasked with collecting data from biometric devices. The application will support a variety of collection data streams. During the testing phase, the team utilizes data from an old production database in a secure testing environment. What principle has the team taken into consideration?

A. Biometric data cannot be changed.

B. The biometric devices are unknown.

C. Biometric data must be protected from disclosure.

D. Separate biometric data streams require increased security.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 177

Topic #: 1

[All CISSP Questions]

Information security practitioners are in the midst of implementing a new firewall. Which of the following failure methods would BEST prioritize security in the event of failure?

A. Failover

B. Fail-Closed

C. Fail-Safe

D. Fail-Open

Show Suggested Answer

Actual exam question from ISC's CISSP
Question #: 178
Topic #: 1
[All CISSP Questions]

Which of the following services can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities?

A. Multi-factor authentication (MFA)

B. Directory

C. User database

D. Single sign-on (SSO)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 179

Topic #: 1

[All CISSP Questions]

Which of the following statements is TRUE about Secure Shell (SSH)?

A. SSH supports port forwarding, which can be used to protect less secured protocols.

B. SSH does not protect against man-in-the-middle (MITM) attacks.

C. SSH is easy to deploy because it requires a Web browser only.

D. SSH can be used with almost any application because it is concerned with maintaining a circuit.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 180

Topic #: 1

[All CISSP Questions]

What is considered a compensating control for not having electrical surge protectors installed?

A. Having dual lines to network service providers built to the site

B. Having a hot disaster recovery (DR) environment for the site

C. Having network equipment in active-active clusters at the site

D. Having backup diesel generators installed to the site

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 181

Topic #: 1

[All CISSP Questions]

What is the FIRST step in risk management?

A. Identify the factors that have potential to impact business.

B. Establish the scope and actions required.

C. Identify existing controls in the environment.

D. Establish the expectations of stakeholder involvement.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 182

Topic #: 1

[All CISSP Questions]

Which of the following is the PRIMARY goal of logical access controls?

A. Restrict access to an information asset.

B. Ensure availability of an information asset.

C. Restrict physical access to an information asset.

D. Ensure integrity of an information asset.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 183

Topic #: 1

[All CISSP Questions]

Which of the following is a covert channel type?

A. Pipe

B. Memory

C. Storage

D. Monitoring

Show Suggested Answer

Actual exam question from ISC's CISSP
Question #: 184
Topic #: 1
[All CISSP Questions]

A software developer wishes to write code that will execute safely and only as intended. Which of the following programming language types is MOST likely to achieve this goal?

A. Weakly typed

B. Dynamically typed

C. Strongly typed

D. Statically typed

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 185

Topic #: 1

[All CISSP Questions]

Which of the following roles is responsible for ensuring that important datasets are developed, maintained, and are accessible within their defined specifications?

A. Data Custodian

B. Data Reviewer

C. Data User

D. Data Owner

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 186

Topic #: 1

[All CISSP Questions]

What is static analysis intended to do when analyzing an executable file?

A. Search the documents and files associated with the executable file.

B. Analyze the position of the file in the file system and the executable file's libraries.

C. Collect evidence of the executable file's usage, including dates of creation and last use.

D. Disassemble the file to gather information about the executable file's function.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 187

Topic #: 1

[All CISSP Questions]

A network security engineer needs to ensure that a security solution analyzes traffic for protocol manipulation and various sorts of common attacks. In addition, all Uniform Resource Locator (URL) traffic must be inspected and users prevented from browsing inappropriate websites. Which of the following solutions should be implemented to enable administrators the capability to analyze traffic, blacklist external sites, and log user traffic for later analysis?

A. Application-Level Proxy

B. Intrusion detection system (IDS)

C. Host-based Firewall

D. Circuit-Level Proxy

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 188

Topic #: 1

[All CISSP Questions]

What is the PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses?

A. ICS often run on UNIX operating systems.

B. ICS often do not have availability requirements.

C. ICS are often sensitive to unexpected traffic.

D. ICS are often isolated and difficult to access.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 189

Topic #: 1

[All CISSP Questions]

The security team plans on using automated account reconciliation in the corporate user access review process. Which of the following must be implemented for the BEST results with fewest errors when running the audit?

A. Frequent audits

B. Segregation of Duties (SoD)

C. Removal of service accounts from review

D. Clear provisioning policies

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 190

Topic #: 1

[All CISSP Questions]

In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

A. Organizational Security Policy

B. Security Target (ST)

C. Protection Profile (PP)

D. Target of Evaluation (TOE)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 191

Topic #: 1

[All CISSP Questions]

Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

A. Data on the device cannot be restored from backup.

B. Data on the device cannot be backed up.

C. Data in transit has been compromised when the user has authenticated to the device.

D. Data at rest has been compromised when the user has authenticated to the device.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 192

Topic #: 1

[All CISSP Questions]

What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

A. Implement network access control lists (ACL).

B. Implement an intrusion prevention system (IPS).

C. Implement a web application firewall (WAF).

D. Implement egress filtering at the organization's network boundary.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 193

Topic #: 1

[All CISSP Questions]

A large organization's human resources and security teams are planning on implementing technology to eliminate manual user access reviews and improve compliance. Which of the following options is MOST likely to resolve the issues associated with user access?

A. Implement a Privileged Access Management (PAM) system.

B. Implement a role-based access control (RBAC) system.

C. Implement identity and access management (IAM) platform.

D. Implement a single sign-on (SSO) platform.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 194

Topic #: 1

[All CISSP Questions]

A cloud service accepts Security Assertion Markup Language (SAML) assertions from users to exchange authentication and authorization data between security domains. However, an attacker was able to spoof a registered account on the network and query the SAML provider. What is the MOST common attack leveraged against this flaw?

A. Attacker leverages SAML assertion to register an account on the security domain.

B. Attacker forges requests to authenticate as a different user.

C. Attacker exchanges authentication and authorization data between security domains.

D. Attacker conducts denial-of-service (DoS) against the security domain by authenticating as the same user repeatedly.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 195

Topic #: 1

[All CISSP Questions]

An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

A. Perform incremental assessments.

B. Engage a third-party auditing firm.

C. Review security architecture.

D. Conduct penetration testing.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 196

Topic #: 1

[All CISSP Questions]

What Hypertext Transfer Protocol (HTTP) response header can be used to disable the execution of inline JavaScript and the execution of eval()-type functions?

A. X-XSS-Protection

B. Content-Security-Policy

C. X-Frame-Options

D. Strict-Transport-Security

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 197

Topic #: 1

[All CISSP Questions]

A security professional was tasked with rebuilding a company's wireless infrastructure. Which of the following are the MOST important factors to consider while making a decision on which wireless spectrum to deploy?

A. Facility size, intermodulation, and direct satellite service

B. Performance, geographic location, and radio signal interference

C. Existing client devices, manufacturer reputation, and electrical interference

D. Hybrid frequency band, service set identifier (SSID), and interpolation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 198

Topic #: 1

[All CISSP Questions]

A software development company has a short timeline in which to deliver a software product. The software development team decides to use open-source software libraries to reduce the development time. What concept should software developers consider when using open-source software libraries?

A. Open source libraries contain known vulnerabilities, and adversaries regularly exploit those vulnerabilities in the wild.

B. Open source libraries can be used by everyone, and there is a common understanding that the vulnerabilities in these libraries will not be exploited.

C. Open source libraries contain unknown vulnerabilities, so they should not be used.

D. Open source libraries are constantly updated, making it unlikely that a vulnerability exists for an adversary to exploit.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 199

Topic #: 1

[All CISSP Questions]

A security engineer is assigned to work with the patch and vulnerability management group. The deployment of a new patch has been approved and needs to be applied. The research is complete, and the security engineer has provided recommendations. Where should the patch be applied FIRST?

A. Lower environment

B. Desktop environment

C. Server environment

D. Production environment

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 200

Topic #: 1

[All CISSP Questions]

What BEST describes the confidentiality, integrity, availability triad?

A. A vulnerability assessment to see how well the organization's data is protected

B. The three-step approach to determine the risk level of an organization

C. The implementation of security systems to protect the organization's data

D. A tool used to assist in understanding how to protect the organization's data

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 201

Topic #: 1

[All CISSP Questions]

Why is it important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision?

A. To provide each manager with precise direction on selecting an appropriate recovery alternative

B. To demonstrate to the board of directors that senior management is committed to continuity recovery efforts

C. To provide a formal declaration from senior management as required by internal audit to demonstrate sound business practices

D. To demonstrate to the regulatory bodies that the company takes business continuity seriously

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 202

Topic #: 1

[All CISSP Questions]

A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

A. Magnetism

B. Generation

C. Consumption

D. Static discharge

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 203

Topic #: 1

[All CISSP Questions]

Which of the following MUST the administrator of a security information and event management (SIEM) system ensure?

A. All sources are synchronized with a common time reference.

B. All sources are reporting in the exact same Extensible Markup Language (XML) format.

C. Data sources do not contain information infringing upon privacy regulations.

D. Each source uses the same Internet Protocol (IP) address for reporting.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 204

Topic #: 1

[All CISSP Questions]

An organization wants to share data securely with their partners via the Internet. Which standard port is typically used to meet this requirement?

A. Setup a server on User Datagram Protocol (UDP) port 69

B. Setup a server on Transmission Control Protocol (TCP) port 21

C. Setup a server on Transmission Control Protocol (TCP) port 22

D. Setup a server on Transmission Control Protocol (TCP) port 80

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 205

Topic #: 1

[All CISSP Questions]

When designing a business continuity plan (BCP), what is the formula to determine the Maximum Tolerable Downtime (MTD)?

A. Estimated Maximum Loss (EML) + Recovery Time Objective (RTO)

B. Business impact analysis (BIA) + Recovery Point Objective (RPO)

C. Annual Loss Expectancy (ALE) + Work Recovery Time (WRT)

D. Recovery Time Objective (RTO) + Work Recovery Time (WRT)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 206

Topic #: 1

[All CISSP Questions]

In systems security engineering, what does the security principle of modularity provide?

A. Minimal access to perform a function

B. Documentation of functions

C. Isolated functions and data

D. Secure distribution of programs and data

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 207

Topic #: 1

[All CISSP Questions]

Which of the following is the strongest physical access control?

A. Biometrics, a password, and personal identification number (PIN)

B. Individual password for each user

C. Biometrics and badge reader

D. Biometrics, a password, and badge reader

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 208

Topic #: 1

[All CISSP Questions]

An access control list (ACL) on a router is a feature MOST similar to which type of firewall?

A. Stateful firewall

B. Packet filtering firewall

C. Application gateway firewall

D. Heuristic firewall

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 209

Topic #: 1

[All CISSP Questions]

While dealing with the consequences of a security incident, which of the following security controls are MOST appropriate?

A. Detective and recovery controls

B. Corrective and recovery controls

C. Preventative and corrective controls

D. Recovery and proactive controls

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 210

Topic #: 1

[All CISSP Questions]

A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

A. SOC 1

B. SOC 2 Type 1

C. SOC 2 Type 2

D. SOC 3

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 211

Topic #: 1

[All CISSP Questions]

Which of the following is TRUE for an organization that is using a third-party federated identity service?

A. The organization specifies alone how to authenticate other organization's users

B. The organization defines internal standard for overall user identification

C. The organization establishes a trust relationship with the other organizations

D. The organization enforces the rules to other organization's user provisioning

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 212

Topic #: 1

[All CISSP Questions]

Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

A. Maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools

B. Maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools

C. Maintaining the inventory through a combination of on premise storage configuration, cloud management, and partner management tools

D. Maintaining the inventory through a combination of system configuration, network management, and license management tools

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 213

Topic #: 1

[All CISSP Questions]

Which of the following outsourcing agreement provisions has the HIGHEST priority from a security operations perspective?

A. Conditions to prevent the use of subcontractors

B. Terms for contract renegotiation in case of disaster

C. Root cause analysis for application performance issue

D. Escalation process for problem resolution during incidents

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 214

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST comprehensive Business Continuity (BC) test?

A. Full interruption

B. Full simulation

C. Full table top

D. Full functional drill

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 215

Topic #: 1

[All CISSP Questions]

A security practitioner needs to implement a solution to verify endpoint security protections and operating system (OS) versions. Which of the following is the BEST solution to implement?

A. An intrusion prevention system (IPS)

B. Network Access Control (NAC)

C. Active Directory (AD) authentication

D. A firewall

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 216

Topic #: 1

[All CISSP Questions]

During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are identified. In which of the following management stages are nonconformities reviewed, assessed and/or corrected by the organization?

A. Assessment

B. Planning

C. Improvement

D. Operation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 217

Topic #: 1

[All CISSP Questions]

When developing an external facing web-based system, which of the following would be the MAIN focus of the security assessment prior to implementation and production?

A. Ensuring Secure Sockets Layer (SSL) certificates are signed by a certificate authority

B. Ensuring Secure Sockets Layer (SSL) certificates are internally signed

C. Assessing the Uniform Resource Locator (URL)

D. Ensuring that input validation is enforced

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 218

Topic #: 1

[All CISSP Questions]

A financial services organization has employed a security consultant to review processes used by employees across various teams. The consultant interviewed a member of the application development practice and found gaps in their threat model. Which of the following correctly represents a trigger for when a threat model should be revised?

A. After operating system (OS) patches are applied

B. A new developer is hired into the team.

C. After a modification to the firewall rule policy

D. A new data repository is added.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 219

Topic #: 1

[All CISSP Questions]

The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a particular system over a 12-month period. Which type of SOC report should be utilized?

A. SOC 1 Type 1

B. SOC 1 Type 2

C. SOC 2 Type 2

D. SOC 3 Type 1

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 220

Topic #: 1

[All CISSP Questions]

An organization recently upgraded to a Voice over Internet Protocol (VoIP) phone system. Management is concerned with unauthorized phone usage. The security consultant is responsible for putting together a plan to secure these phones. Administrators have assigned unique personal identification number (PIN) codes for each person in the organization. What is the BEST solution?

A. Have the administrator enforce a policy to change the PIN regularly. Implement call detail records (CDR) reports to track usage.

B. Have the administrator change the PIN regularly. Implement call detail records (CDR) reports to track usage.

C. Use phone locking software to enforce usage and PIN policies. Inform the user to change the PIN regularly.

D. Implement call detail records (CDR) reports to track usage.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 221

Topic #: 1

[All CISSP Questions]

Which of the following protection is provided when using a Virtual Private Network (VPN) with Authentication Header (AH)?

A. Sender non-repudiation

B. Multi-factor authentication (MFA)

C. Payload encryption

D. Sender confidentiality

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 222

Topic #: 1

[All CISSP Questions]

An organization contracts with a consultant to perform a System Organization Control (SOC) 2 audit on their internal security controls. An auditor documents a finding a related to an Application Programming Interface (API) performing an action that is not aligned with the scope or objective of the system. Which trust service principle would be MOST applicable in th is situation?

A. Confidentiality

B. Processing Integrity

C. Security

D. Availability

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 223

Topic #: 1

[All CISSP Questions]

In which process MUST security be considered during the acquisition of new software?

A. Request for proposal (RFP)

B. Implementation

C. Vendor selection

D. Contract negotiation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 224

Topic #: 1

[All CISSP Questions]

Which of the following is the MAIN difference between a network-based firewall and a host-based firewall?

A. A network-based firewall is stateful, while a host-based firewall is stateless.

B. A network-based firewall blocks network intrusions, while a host-based firewall blocks malware.

C. A network-based firewall controls traffic passing through the device, while a host-based firewall controls traffic destined for the device.

D. A network-based firewall verifies network traffic, while a host-based firewall verifies processes and applications.

Show Suggested Answer

Actual exam question from ISC's CISSP
Question #: 225
Topic #: 1
[All CISSP Questions]

Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high- risk countries?

A. Review applicable destination country laws, forensically clean devices prior to travel, and only download sensitive data over a virtual private network (VPN) upon arriving at the destination.

B. Leverage a Secure Socket Layer (SSL) connection over a virtual private network (VPN) to download sensitive data upon arriving at the destination.

C. Keep laptops, external storage devices, and smartphones in the hotel room when not in use.

D. Use multi-factor authentication (MFA) to gain access to data stored on laptops or external storage devices and biometric fingerprint access control mechanisms to unlock smartphones.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 226

Topic #: 1

[All CISSP Questions]

When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

A. Confirm that confidentiality agreements are signed

B. Employ strong access controls

C. Log all activities associated with sensitive systems

D. Provide links to security policies

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 227

Topic #: 1

[All CISSP Questions]

Which of the following regulations dictates how data breaches are handled?

A. Payment Card Industry Data Security Standard (PCI-DSS)

B. National Institute of Standards and Technology (NIST)

C. Sarbanes-Oxley (SOX)

D. General Data Protection Regulation (GDPR)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 228

Topic #: 1

[All CISSP Questions]

In software development, developers should use which type of queries to prevent a Structured Query Language (SQL) injection?

A. Parameterised

B. Controlled

C. Dynamic

D. Static

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 229

Topic #: 1

[All CISSP Questions]

Which type of access control includes a system that allows only users that are type=managers and department=sales to access employee records?

A. Role-based access control (RBAC)

B. Attribute-based access control (ABAC)

C. Discretionary access control (DAC)

D. Mandatory access control (MAC)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 230

Topic #: 1

[All CISSP Questions]

Which of the following examples is BEST to minimize the attack surface for a customer's private information?

A. Data masking

B. Authentication

C. Obfuscation

D. Collection limitation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 231

Topic #: 1

[All CISSP Questions]

Which evidence collecting technique would be utilized when it is believed an attacker is employing a rootkit and a quick analysis is needed?

A. Forensic disk imaging

B. Live response

C. Memory collection

D. Malware analysis

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 232

Topic #: 1

[All CISSP Questions]

An application is used for funds transfers between an organization and a third-party. During a security audit, an auditor has found an issue with the business continuity disaster recovery policy and procedures for this application. Which of the following reports should the auditor file with the organization?

A. Statement on Auditing Standards (SAS) 70-1

B. Statement on Auditing Standards (SAS) 70

C. Service Organization Control (SOC) 1

D. Service Organization Control (SOC) 2

Show Suggested Answer

Actual exam question from ISC's CISSP
Question #: 233
Topic #: 1
[All CISSP Questions]

When determining data and information asset handling, regardless of the specific toolset being used, which of the following is one of the common components of big data?

A. Distributed storage locations

B. Centralized processing location

C. Distributed data collection

D. Consolidated data collection

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 234

Topic #: 1

[All CISSP Questions]

A Chief Information Security Officer (CISO) of a firm which decided to migrate to cloud has been tasked with ensuring an optimal level of security. Which of the following would be the FIRST consideration?

A. Analyze the firm's applications and data repositories to determine the relevant control requirements.

B. Request a security risk assessment of the cloud vendor be completed by an independent third-party.

C. Define the cloud migration roadmap and set out which applications and data repositories should be moved into the cloud.

D. Ensure that the contract between the cloud vendor and the firm clearly defines responsibilities for operating security controls.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 235

Topic #: 1

[All CISSP Questions]

Which of the following BEST describes the purpose of Border Gateway Protocol (BGP)?

A. Provide Routing Information Protocol (RIP) version 2 advertisements to neighboring layer 3 devices.

B. Maintain a list of network paths between internet routers.

C. Provide firewall services to cloud-enabled applications.

D. Maintain a list of efficient network paths between autonomous systems.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 236

Topic #: 1

[All CISSP Questions]

What is the BEST design for securing physical perimeter protection?

A. Closed-circuit television (CCTV)

B. Business continuity planning (BCP)

C. Barriers, fences, gates, and walls

D. Crime Prevention through Environmental Design (CPTED)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 237

Topic #: 1

[All CISSP Questions]

The security organization is looking for a solution that could help them determine with a strong level of confidence that attackers have breached their network.

Which solution is MOST effective at discovering a successful network breach?

A. Developing a sandbox

B. Installing an intrusion detection system (IDS)

C. Deploying a honeypot

D. Installing an intrusion prevention system (IPS)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 238

Topic #: 1

[All CISSP Questions]

Which of the following is a benefit of implementing data-in-use controls?

A. If the data is lost, it must be decrypted to be opened.

B. When the data is being viewed, it can only be printed by authorized users.

C. When the data is being viewed, it can be accessed using secure protocols.

D. If the data is lost, it may not be accessible to unauthorized users.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 239

Topic #: 1

[All CISSP Questions]

When configuring Extensible Authentication Protocol (EAP) in a Voice over Internet Protocol (VoIP) network, which of the following authentication types is the MOST secure?

A. EAP-Protected Extensible Authentication Protocol (PEAP)

B. EAP-Transport Layer Security (TLS)

C. EAP-Tunneled Transport Layer Security (TLS)

D. EAP-Flexible Authentication via Secure Tunneling

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 240

Topic #: 1

[All CISSP Questions]

Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

A. Monitor mail servers for sensitive data being exfiltrated.

B. Educate end-users on methods of attacks on sensitive data.

C. Establish report parameters for sensitive data.

D. Store sensitive data only when necessary.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 241

Topic #: 1

[All CISSP Questions]

An organization with divisions in the United States (US) and the United Kingdom (UK) processes data comprised of personal information belonging to subjects living in the European Union (EU) and in the US. Which data MUST be handled according to the privacy protections of General Data Protection Regulation (GDPR)?

A. Only the UK citizens' data

B. Only the EU residents' data

C. Only data processed in the UK

D. Only the EU citizens' data

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 242

Topic #: 1

[All CISSP Questions]

What are the first two components of logical access control?

A. Authentication and availability

B. Authentication and identification

C. Identification and confidentiality

D. Confidentiality and authentication

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 243

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST effective measure for dealing with rootkit attacks?

A. Restoring the system from the last backup

B. Finding and replacing the altered binaries with legitimate ones

C. Turning off unauthorized services and rebooting the system

D. Reinstalling the system from trusted sources

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 244

Topic #: 1

[All CISSP Questions]

Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

A. Storage

B. Training

C. Legal

D. Business

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 245

Topic #: 1

[All CISSP Questions]

A new employee formally reported suspicious behavior to the organization security team. The report claims that someone not affiliated with the organization was inquiring about the member's work location, length of employment, and building access controls. The employee's reporting is MOST likely the result of which of the following?

A. Security engineering

B. Security awareness

C. Phishing

D. Risk avoidance

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 246

Topic #: 1

[All CISSP Questions]

The disaster recovery (DR) process should always include:

A. periodic inventory review

B. financial data analysis

C. plan maintenance

D. periodic vendor review

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 247

Topic #: 1

[All CISSP Questions]

An organization has determined that its previous waterfall approach to software development is not keeping pace with business demands. To adapt to the rapid changes required for product delivery, the organization has decided to move towards an Agile software development and release cycle. In order to ensure the success of the Agile methodology, who is the MOST critical in creating acceptance criteria for each release?

A. Business customers

B. Software developers

C. Independent testers

D. Project managers

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 248

Topic #: 1

[All CISSP Questions]

What is the FIRST step for an organization to take before allowing personnel to access social media from a corporate device or user account?

A. Publish an acceptable usage policy.

B. Publish a social media guidelines document.

C. Deliver security awareness training.

D. Document a procedure for accessing social media sites.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 249

Topic #: 1

[All CISSP Questions]

A hospital has allowed virtual private networking (VPN) access to remote database developers. Upon auditing the internal configuration, the network administrator discovered that split-tunneling was enabled. What is the concern with this configuration?

A. The network intrusion detection system (NIDS) will fail to inspect Secure Sockets Layer (SSL) traffic.

B. Remote sessions will not require multi-layer authentication.

C. Remote clients are permitted to exchange traffic with the public and private network.

D. Multiple Internet Protocol Security (IPSec) tunnels may be exploitable in specific circumstances.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 250

Topic #: 1

[All CISSP Questions]

In an IDEAL encryption system, who has sole access to the decryption key?

A. Data custodian

B. System owner

C. System administrator

D. Data owner

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 251

Topic #: 1

[All CISSP Questions]

Which type of disaster recovery plan (DRP) testing carries the MOST operational risk?

A. Cutover

B. Parallel

C. Walkthrough

D. Tabletop

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 252

Topic #: 1

[All CISSP Questions]

Which of the following methods provides the MOST protection for user credentials?

A. Forms-based authentication

B. Self-registration

C. Basic authentication

D. Digest authentication

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 253

Topic #: 1

[All CISSP Questions]

An organization is planning a penetration test that simulates the malicious actions of a former network administrator. What kind of penetration test is needed?

A. Functional test

B. Unit test

C. Grey box

D. White box

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 254

Topic #: 1

[All CISSP Questions]

How does Radio-Frequency Identification (RFID) assist with asset management?

A. It uses biometric information for system identification.

B. It uses two-factor authentication (2FA) for system identification.

C. It transmits unique serial numbers wirelessly.

D. It transmits unique Media Access Control (MAC) addresses wirelessly.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 255

Topic #: 1

[All CISSP Questions]

Which of the following is the FIRST step an organization's professional performs when defining a cyber-security program based upon industry standards?

A. Review the past security assessments

B. Define the organization's objectives regarding security and risk mitigation

C. Map the organization's current security practices to industry standards and frameworks

D. Select from a choice of security best practices

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 256

Topic #: 1

[All CISSP Questions]

What is the MOST important criterion that needs to be adhered to during the data collection process of an active investigation?

A. Maintaining the chain of custody

B. Capturing an image of the system

C. Outlining all actions taken during the investigation

D. Complying with the organization's security policy

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 257

Topic #: 1

[All CISSP Questions]

Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

A. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network bridge in order to communicate

B. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network router in order to communicate

C. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network bridge in order to communicate

D. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network router in order to communicate

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 258

Topic #: 1

[All CISSP Questions]

Security Software Development Life Cycle (SDLC) expects application code to be written in a consistent manner to allow ease of auditing and which of the following?

A. Protecting

B. Copying

C. Enhancing

D. Executing

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 259

Topic #: 1

[All CISSP Questions]

Which of the following is a risk matrix?

A. A tool for determining risk management decisions for an activity or system.

B. A database of risks associated with a specific information system.

C. A two-dimensional picture of risk for organizations, products, projects, or other items of interest.

D. A table of risk management factors for management to consider.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 260

Topic #: 1

[All CISSP Questions]

What part of an organization's strategic risk assessment MOST likely includes information on items affecting the success of the organization?

A. Threat analysis

B. Vulnerability analysis

C. Key Performance Indicator (KPI)

D. Key Risk Indiaitor (KRI)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 261

Topic #: 1

[All CISSP Questions]

A company needs to provide employee access to travel services, which are hosted by a third-party service provider. Employee experience is important, and when users are already authenticated, access to the travel portal is seamless. Which of the following methods is used to share information and grant user access to the travel portal?

A. Single sign-on (SSO) access

B. Security Assertion Markup Language (SAML) access

C. Open Authorization (OAuth) access

D. Federated access

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 262

Topic #: 1

[All CISSP Questions]

The Chief Executive Officer (CEO) wants to implement an internal audit of the company's information security posture. The CEO wants to avoid any bias in the audit process; therefore, has assigned the Sales Director to conduct the audit. After significant interaction over a period of weeks the audit concludes that the company's policies and procedures are sufficient, robust and well established. The CEO then moves on to engage an external penetration testing company in order to showcase the organization's robust information security stance. This exercise reveals significant failings in several critical security controls and shows that the incident response processes remain undocumented. What is the MOST likely reason for this disparity in the results of the audit and the external penetration test?

A. The audit team lacked the technical experience and training to make insightful and objective assessments of the data provided to them.

B. The scope of the penetration test exercise and the internal audit were significantly different.

C. The external penetration testing company used custom zero-day attacks that could not have been predicted.

D. The information technology (IT) and governance teams have failed to disclose relevant information to the internal audit team leading to an incomplete assessment being formulated.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 263

Topic #: 1

[All CISSP Questions]

An information security administrator wishes to block peer-to-peer (P2P) traffic over Hypertext Transfer Protocol (HTTP) tunnels. Which of the following layers of the Open Systems Interconnection (OSI) model requires inspection?

A. Application

B. Transport

C. Session

D. Presentation

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 264

Topic #: 1

[All CISSP Questions]

A Chief Information Officer (CIO) has delegated responsibility of their system security to the head of the information technology (IT) department. While corporate policy dictates that only the CIO can make decisions on the level of data protection required, technical implementation decisions are done by the head of the IT department. Which of the following BEST describes the security role filled by the head of the IT department?

A. System security officer

B. System processor

C. System custodian

D. System analyst

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 265

Topic #: 1

[All CISSP Questions]

Which of the following actions should be undertaken prior to deciding on a physical baseline Protection Profile (PP)?

A. Conduct a site survey.

B. Choose a suitable location.

C. Check the technical design.

D. Categorize assets.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 266

Topic #: 1

[All CISSP Questions]

Management has decided that a core application will be used on personal cellular phones. As an implementation requirement, regularly scheduled analysis of the security posture needs to be conducted. Management has also directed that continuous monitoring be implemented. Which of the following is required to accomplish management's directive?

A. Routine reports generated by the user's cellular phone provider that detail security events

B. Strict integration of application management, configuration management (CM), and phone management

C. Management application installed on user phones that tracks all application events and cellular traffic

D. Enterprise-level security information and event management (SIEM) dashboard that provides full visibility of cellular phone activity

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 267

Topic #: 1

[All CISSP Questions]

A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the BEST design approach to securing this environment?

A. Use reverse proxies to create a secondary "shadow" environment for critical systems.

B. Place firewalls around critical devices, isolating them from the rest of the environment.

C. Layer multiple detective and preventative technologies at the environment perimeter.

D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 268

Topic #: 1

[All CISSP Questions]

Which of the following techniques is MOST useful when dealing with advanced persistent threat (APT) intrusions on live virtualized environments?

A. Memory forensics

B. Logfile analysis

C. Reverse engineering

D. Antivirus operations

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 269

Topic #: 1

[All CISSP Questions]

Which of the following types of web-based attack is happening when an attacker is able to send a well-crafted, malicious request to an authenticated user realizing it?

A. Process injection

B. Cross-Site request forgery (CSRF)

C. Cross-Site Scripting (XSS)

D. Broken Authentication And Session Management

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 270

Topic #: 1

[All CISSP Questions]

A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?

A. Mitigate the risks with compensating controls.

B. Upgrade the software affected by the vulnerability.

C. Remove the affected software from the servers.

D. Inform management of possible risks.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 271

Topic #: 1

[All CISSP Questions]

A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light fi lters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

A. Remove the ultraviolet light filters on the HVAC intake and replace the fire suppression system on the upper floors with a dry system

B. Elevate the HVAC intake by constructing a plenum or external shaft over it and convert the server room fire suppression to a pre-action system

C. Add additional ultraviolet light fi lters to the HVAC intake supply and return ducts and change server room fire suppression to FM-200

D. Apply additional physical security around the HVAC intakes and update upper floor fire suppression to FM-200

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 272

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST common use of the Online Certificate Status Protocol (OCSP)?

A. To verify the validity of an X.509 digital certificate

B. To obtain the expiration date of an X.509 digital certificate

C. To obtain the revocation status of an X.509 digital certificate

D. To obtain the author name of an X.509 digital certificate

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 273

Topic #: 1

[All CISSP Questions]

A security professional has been assigned to assess a web application. The assessment report recommends switching to Security Assertion Markup Language (SAML). What is the PRIMARY security benefit in switching to SAML?

A. It enables single sign-on (SSO) for web applications.

B. It uses Transport Layer Security (TLS) to address confidentiality.

C. It limits unnecessary data entry on web forms.

D. The users' password is not passed during authentication.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 274

Topic #: 1

[All CISSP Questions]

An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization's dedicated environment with a cloud service provider. What is the BEST way to prevent and correct the software's security weaknesses?

A. Follow the software end-of-life schedule

B. Implement a dedicated COTS sandbox environment

C. Transfer the risk to the cloud service provider

D. Examine the software updating and patching process

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 275

Topic #: 1

[All CISSP Questions]

What type of database attack would allow a customer service employee to determine quarterly sales results before they are publicly announced?

A. Inference

B. Aggregation

C. Polyinstantiation

D. Data mining

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 276

Topic #: 1

[All CISSP Questions]

In a multi-tenant cloud environment, what approach will secure logical access to assets?

A. Controlled configuration management (CM)

B. Transparency/Auditability of administrative access

C. Virtual private cloud (VPC)

D. Hybrid cloud

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 277

Topic #: 1

[All CISSP Questions]

An information technology (IT) employee who travels frequently to various countries remotely connects to an organization's resources to troubleshoot problems. Which of the following solutions BEST serves as a secure control mechanism to meet the organization's requirements?

A. Install a third-party screen sharing solution that provides remote connection from a public website.

B. Install a bastion host in the demilitarized zone (DMZ) and allow multi-factor authentication (MFA) access.

C. Implement a Dynamic Domain Name Services (DONS) account to initiate a virtual private network (VPN) using the DONS record.

D. Update the firewall rules to include the static Internet Protocol (IP) addresses of the locations where the employee connects from.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 278

Topic #: 1

[All CISSP Questions]

Which of the following is the BEST way to determine the success of a patch management process?

A. Change management

B. Configuration management (CM)

C. Analysis and impact assessment

D. Auditing and assessment

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 279

Topic #: 1

[All CISSP Questions]

An organization has discovered that organizational data is posted by employees to data storage accessible to the general public. What is the PRIMARY step an organization must take to ensure data is properly protected from public release?

A. Implement a user reporting policy.

B. Implement a data encryption policy.

C. Implement a user training policy.

D. Implement a data classification policy.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 280

Topic #: 1

[All CISSP Questions]

A security engineer is required to integrate security into a software project that is implemented by small groups that quickly, continuously, and independently develop, test, and deploy code to the cloud. The engineer will MOST likely integrate with which software development process?

A. Devops Integrated Product Team (IPT)

B. Structured Waterfall Programming Development

C. Service-oriented architecture (SOA)

D. Spiral Methodology

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 281

Topic #: 1

[All CISSP Questions]

Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

A. Agile software development

B. Secure software development

C. Application threat modeling

D. Penetration testing

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 282

Topic #: 1

[All CISSP Questions]

Which Open Systems Interconnection (OSI) layer(s) BEST corresponds to the network access layer in the Transmission Control Protocol/Internet Protocol (TCP/IP) model?

A. Data Link and Physical Layers

B. Session and Network Layers

C. Transport Layer

D. Application, Presentation, and Session Layers

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 283

Topic #: 1

[All CISSP Questions]

An organization's retail website provides its only source of revenue, so the disaster recovery plan (DRP) must document an estimated time for each step in the plan. Which of the following steps in the DRP will list the GREATEST duration of time for the service to be fully operational?

A. Update the Network Address Translation (NAT) table.

B. Update Domain Name System (DNS) server addresses with domain registrar.

C. Update the Border Gateway Protocol (BGP) autonomous system number.

D. Update the web server network adapter configuration.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 284

Topic #: 1

[All CISSP Questions]

In supervisory control and data acquisition (SCADA) systems, which of the following controls can be used to reduce device exposure to malware?

A. Disallow untested code in the execution space of the SCADA device.

B. Disable all command line interfaces.

C. Disable Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port 138 and 139 on the SCADA device.

D. Prohibit the use of unsecure scripting languages.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 285

Topic #: 1

[All CISSP Questions]

Which of the following secure transport protocols is often used to secure Voice over Internet Protocol (VoIP) communications on a network from end to end?

A. Secure File Transfer Protocol (SFTP)

B. Secure Real-time Transport Protocol (SRTP)

C. Generic Routing Encapsulation (GRE)

D. Internet Protocol Security (IPSec)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 286

Topic #: 1

[All CISSP Questions]

A healthcare insurance organization chose a vendor to develop a software application. Upon review of the draft contract, the information security professional notices that software security is not addressed. What is the BEST approach to address the issue?

A. Update the contract to require the vendor to perform security code reviews.

B. Update the service level agreement (SLA) to provide the organization the right to audit the vendor.

C. Update the contract so that the vendor is obligated to provide security capabilities.

D. Update the service level agreement (SLA) to require the vendor to provide security capabilities.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 287

Topic #: 1

[All CISSP Questions]

Which of the following security tools will ensure authorized data is sent to the application when implementing a cloud-based application?

A. Host-based intrusion prevention system (HIPS)

B. Access control list (ACL)

C. Data loss prevention (DLP)

D. File integrity monitoring (FIM)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 288

Topic #: 1

[All CISSP Questions]

A client server infrastructure that provides user-to-server authentication describes which one of the following?

A. Secure Sockets Layer (SSL)

B. User-based authorization

C. Kerberos

D. X.509

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 289

Topic #: 1

[All CISSP Questions]

A system developer has a requirement for an application to check for a secure digital signature before the application is accessed on a user's laptop. Which security mechanism addresses this requirement?

A. Trusted Platform Module (TPM)

B. Certificate revocation list (CRL) policy

C. Key exchange

D. Hardware encryption

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 290

Topic #: 1

[All CISSP Questions]

Which of the following is a term used to describe maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions?

A. Information Security Continuous Monitoring (ISCM)

B. Risk Management Framework (RMF)

C. Information Sharing & Analysis Centers (ISAC)

D. Information Security Management System (ISMS)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 291

Topic #: 1

[All CISSP Questions]

Which of the following types of firewall only examines the "handshaking" between packets before forwarding traffic?

A. Proxy firewalls

B. Circuit-level firewalls

C. Network Address Translation (NAT) firewalls

D. Host-based firewalls

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 292

Topic #: 1

[All CISSP Questions]

What is a use for mandatory access control (MAC)?

A. Allows for mandatory user identity and passwords based on sensitivity

B. Allows for mandatory system administrator access control over objects

C. Allows for labeling of sensitive user accounts for access control

D. Allows for object security based on sensitivity represented by a label

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 293

Topic #: 1

[All CISSP Questions]

An organization has developed a way for customers to share information from their wearable devices with each other. Unfortunately, the users were not informed as to what information collected would be shared. What technical controls should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals?

A. Share only what the organization decides is best.

B. Stop sharing data with the other users.

C. Default the user to not share any information.

D. Inform the user of the sharing feature changes after implemented.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 294

Topic #: 1

[All CISSP Questions]

Which of the following system components enforces access controls on an object?

A. Security perimeter

B. Access control matrix

C. Trusted domain

D. Reference monitor

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 295

Topic #: 1

[All CISSP Questions]

In setting expectations when reviewing the results of a security test, which of the following statements is MOST important to convey to reviewers?

A. The accuracy of testing results can be greatly improved if the target(s) are properly hardened.

B. The results of the tests represent a point-in-time assessment of the target(s).

C. The deficiencies identified can be corrected immediately.

D. The target's security posture cannot be further compromised.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 296

Topic #: 1

[All CISSP Questions]

What is the benefit of an operating system (OS) feature that is designed to prevent an application from executing code from a non-executable memory region?

A. Identifies which security patches still need to be installed on the system

B. Reduces the risk of polymorphic viruses from encrypting their payload

C. Stops memory resident viruses from propagating their payload

D. Helps prevent certain exploits that store code in buffers

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 297

Topic #: 1

[All CISSP Questions]

What is the overall goal of software security testing?

A. Identifying the key security features of the software

B. Ensuring all software functions perform as specified

C. Reducing vulnerabilities within a software system

D. Making software development more agile

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 298

Topic #: 1

[All CISSP Questions]

Which of the following implementations will achieve high availability in a website?

A. Disk mirroring of the web server with redundant disk drives in a hardened data center

B. Disk striping of the web server hard drives and large amounts of bandwidth

C. Multiple geographically dispersed web servers that are configured for failover

D. Multiple Domain Name System (DNS) entries resolving to the same web server and large amounts of bandwidth

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 299

Topic #: 1

[All CISSP Questions]

Which of the following is an important design feature for the outer door of a mantrap?

A. Allow it to be opened by an alarmed emergency button.

B. Do not allow anyone to enter it alone.

C. Do not allow it to be observed by closed-circuit television (CCTV) cameras.

D. Allow it be opened when the inner door of the mantrap is also open.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 300

Topic #: 1

[All CISSP Questions]

Which of the following is the MOST important rule for digital investigations?

A. Ensure original data is never modified.

B. Ensure systems are powered on.

C. Ensure event logs are rotated.

D. Ensure individual privacy is protected.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 301

Topic #: 1

[All CISSP Questions]

An information security professional is reviewing user access controls on a customer-facing application. The application must have multi-factor authentication (MFA) in place. The application currently requires a username and password to login. Which of the following options would BEST implement MFA?

A. Geolocate the user and compare to previous logins

B. Require a pre-selected number as part of the login

C. Have the user answer a secret question that is known to them

D. Enter an automatically generated number from a hardware token

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 302

Topic #: 1

[All CISSP Questions]

Which of the following is a MAJOR consideration in implementing a Voice over Internet Protocol (VoIP) network?

A. Use of Request for Comments (RFC) 1918 addressing.

B. Use of Network Access Control (NAC) on switches.

C. Use of separation for the voice network.

D. Use of a unified messaging.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 303

Topic #: 1

[All CISSP Questions]

During testing, where are the requirements to inform parent organizations, law enforcement, and a computer incident response team documented?

A. Security Assessment Report (SAR)

B. Security assessment plan

C. Unit test results

D. System integration plan

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 304

Topic #: 1

[All CISSP Questions]

The security architect has been mandated to assess the security of various brands of mobile devices. At what phase of the product lifecycle would this be MOST likely to occur?

A. Implementation

B. Operations and maintenance

C. Disposal

D. Development

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 305

Topic #: 1

[All CISSP Questions]

Which of the following statements is MOST accurate regarding information assets?

A. International Organization for Standardization (ISO) 27001 compliance specifies which information assets must be included in asset inventory.

B. Information assets include any information that is valuable to the organization.

C. Building an information assets register is a resource-intensive job.

D. Information assets inventory is not required for risk assessment.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 306

Topic #: 1

[All CISSP Questions]

Which of the following attack types can be used to compromise the integrity of data during transmission?

A. Synchronization flooding

B. Session hijacking

C. Keylogging

D. Packet sniffing

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 307

Topic #: 1

[All CISSP Questions]

A malicious user gains access to unprotected directories on a web server. Which of the following is MOST likely the cause for this information disclosure?

A. Broken authentication management

B. Security misconfiguration

C. Cross-site request forgery (CSRF)

D. Structured Query Language injection (SQLi)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 308

Topic #: 1

[All CISSP Questions]

When reviewing the security logs, the password shown for an administrative login event was ' OR ' '1'='1' --. This is an example of which of the following kinds of attack?

A. Structured Query Language (SQL) Injection

B. Brute Force Attack

C. Rainbow Table Attack

D. Cross-Site Scripting (XSS)

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 309

Topic #: 1

[All CISSP Questions]

Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

A. File hashing

B. Storage encryption

C. Data retention policy

D. Data processing

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 310

Topic #: 1

[All CISSP Questions]

Which of the following BEST describes why software assurance is critical in helping prevent an increase in business and mission risk for an organization?

A. Request for proposals (RFP) avoid purchasing software that does not meet business needs.

B. Contracting processes eliminate liability for security vulnerabilities for the purchaser.

C. Decommissioning of old software reduces long-term costs related to technical debt.

D. Software that does not perform as intended may be exploitable which makes it vulnerable to attack.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 311

Topic #: 1

[All CISSP Questions]

An employee's home address should be categorized according to which of the following references?

A. The consent form terms and conditions signed by employees

B. An organization security plan for human resources

C. Existing employee data classifications

D. The organization's data classification model

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 312

Topic #: 1

[All CISSP Questions]

Which of the following activities should a forensic examiner perform FIRST when determining the priority of digital evidence collection at a crime scene?

A. Gather physical evidence.

B. Assign responsibilities to personnel on the scene.

C. Establish a list of files to examine.

D. Establish order of volatility.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 313

Topic #: 1

[All CISSP Questions]

Which software defined networking (SDN) architectural component is responsible for translating network requirements?

A. SDN Controller

B. SDN Datapath

C. SDN Northbound Interfaces

D. SDN Application

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 314

Topic #: 1

[All CISSP Questions]

An internal audit for an organization recently identified malicious actions by a user account. Upon further investigation, it was determined the offending user account was used by multiple people at multiple locations simultaneously for various services and applications. What is the BEST method to prevent this problem in the future?

A. Ensure each user has their own unique account.

B. Allow several users to share a generic account.

C. Ensure the security information and event management (SIEM) is set to alert.

D. Inform users only one user should be using the account at a time.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 315

Topic #: 1

[All CISSP Questions]

Who should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC)?

A. A security subject matter expert (SME)

B. A developer subject matter expert (SME)

C. The business owner

D. The application owner

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 316

Topic #: 1

[All CISSP Questions]

The initial security categorization should be done early in the system life cycle and should be reviewed periodically. Why is it important for this to be done correctly?

A. It determines the functional and operational requirements.

B. It determines the security requirements.

C. It affects other steps in the certification and accreditation process.

D. The system engineering process works with selected security controls.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 317

Topic #: 1

[All CISSP Questions]

When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

A. Detection of sophisticated attackers

B. Topology of the network used for the system

C. Risk assessment of the system

D. Resiliency of the system

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 318

Topic #: 1

[All CISSP Questions]

Which of the following events prompts a review of the disaster recovery plan (DRP)?

A. Change in senior management

B. Completion of the security policy review

C. Organizational merger

D. New members added to the steering committee

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 319

Topic #: 1

[All CISSP Questions]

A user is allowed to access the file labeled "Financial Forecast," but only between 9:00 a.m. and 5:00 p.m., Monday through Friday. Which type of access mechanism should be used to accomplish this?

A. Minimum access control

B. Limited role-based access control (RBAC)

C. Access control list (ACL)

D. Rule-based access control

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 320

Topic #: 1

[All CISSP Questions]

What is the benefit of using Network Admission Control (NAC)?

A. NAC only supports Windows operating systems (OS).

B. NAC supports validation of the endpoint's security posture prior to allowing the session to go into an authorized state.

C. NAC can require the use of certificates, passwords, or a combination of both before allowing network admission.

D. Operating system (OS) versions can be validated prior to allowing network access.

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 321

Topic #: 1

[All CISSP Questions]

When MUST an organization's information security strategic plan be reviewed?

A. Whenever there are major changes to the business

B. Quarterly, when the organization's strategic plan is updated

C. Every three years, when the organization's strategic plan is updated

D. Whenever there are significant changes to a major application

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 322

Topic #: 1

[All CISSP Questions]

An established information technology (IT) consulting firm is considering acquiring a successful local startup. To gain a comprehensive understanding of the startup's security posture, which type of assessment provides the BEST information?

A. A security audit

B. A tabletop exercise

C. A penetration test

D. A security threat model

Show Suggested Answer