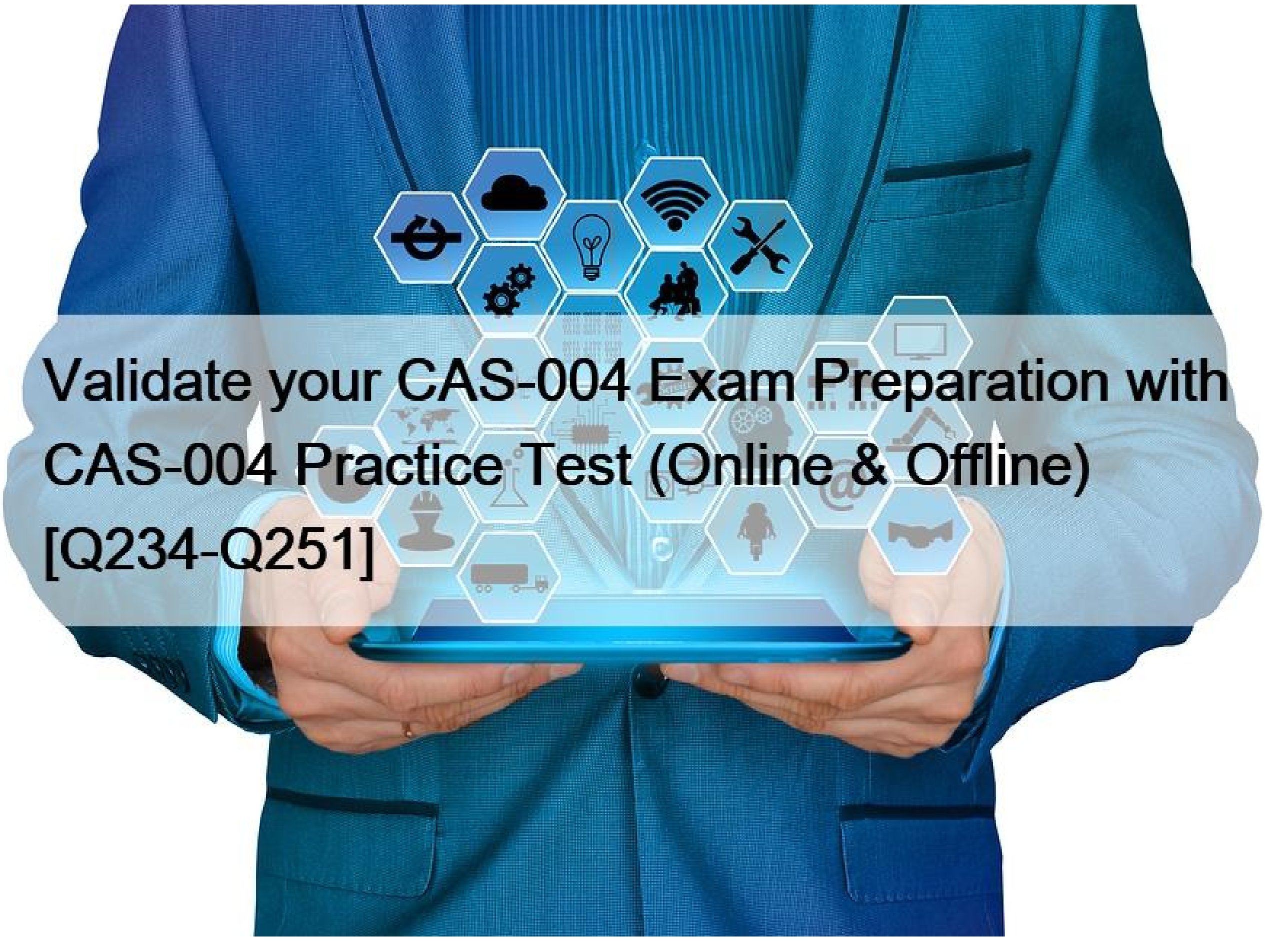
Validate your CAS-004 Exam Preparation with CAS-004 Practice Test (Online & Offline) [Q234-Q251


Validate your CAS-004 Exam Preparation with
CAS-004 Practice Test (Online & Offline)
[Q234-Q251]

Validate your CAS-004 Exam Preparation with CAS-004 Practice Test (Online & Offline) Get all the Information About CompTIA CAS-004 Exam 2024 Practice Test Questions NEW QUESTION 234

An organization is facing budget constraints The Chief Technology Officer (CTO) wants to add a new marketing platform but the organization does not have the resources to obtain separate servers to run the new platform.

The CTO recommends running the new marketing platform on a virtualized video-conferencing server because video conferencing is rarely used.

The Chief Information Security Officer (CISO) denies this request.

Which of the following BEST explains the reason why the CISO has not approved the request?
* Privilege escalation attacks
* Performance and availability
* Weak DAR encryption
* Disparate security requirements

NEW QUESTION 235

To save time, a company that is developing a new VPN solution has decided to use the OpenSSL library within Its proprietary software. Which of the following should the company consider to maximize risk reduction from vulnerabilities introduced by OpenSSL?
* Include stable, long-term releases of third-party libraries instead of using newer versions.
* Ensure the third-party library implements the TLS and disable weak ciphers.
* Compile third-party libraries into the main code statically instead of using dynamic loading.
* Implement an ongoing, third-party software and library review and regression testing.
Implementing an ongoing, third-party software and library review and regression testing is the best way to maximize risk reduction from vulnerabilities introduced by OpenSSL. Third-party software and libraries are often used by developers to save time and resources, but they may also introduce security risks if they are not properly maintained and updated. By reviewing and testing the third-party software and library regularly, the company can ensure that they are using the latest and most secure version of OpenSSL, and that their proprietary software is compatible and functional with it.

NEW QUESTION 236

A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack.

Which of the following is t he NEXT step of the incident response plan?
* Remediation
* Containment
* Response
* Recovery
Reference: https://www.sciencedirect.com/topics/computer-science/containment-strategy

NEW QUESTION 237

A company based in the United States holds insurance details of EU citizens.

Which of the following must be adhered to when processing EU citizens&#8217; personal, private, and confidential data?
* The principle of lawful, fair, and transparent processing
* The right to be forgotten principle of personal data erasure requests
* The non-repudiation and deniability principle
* The principle of encryption, obfuscation, and data masking
https://gdpr-info.eu/recitals/no-39/

NEW QUESTION 238

A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

Unauthorized insertions into application development environments

Authorized insiders making unauthorized changes to environment configurations Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)
* Perform static code analysis of committed code and generate summary reports.
* Implement an XML gateway and monitor for policy violations.
* Monitor dependency management tools and report on susceptible third-party libraries.

* Install an IDS on the development subnet and passively monitor for vulnerable services.
* Model user behavior and monitor for deviations from normal.
* Continuously monitor code commits to repositories and generate summary logs.

Explanation

Modeling user behavior and monitoring for deviations from normal and continuously monitoring code commits to repositories and generating summary logs are actions that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations. Modeling user behavior and monitoring for deviations from normal is a technique that uses baselines, analytics, machine learning, or other methods to establish normal patterns of user activity and identify anomalies or outliers that could indicate malicious or suspicious behavior. Modeling user behavior and monitoring for deviations from normal can help detect unauthorized insertions into application development environments, as it can alert on unusual or unauthorized access attempts, commands, actions, or transactions by users. Continuously monitoring code commits to repositories and generating summary logs is a technique that uses tools, scripts, automation, or other methods to track and record changes made to code repositories by developers, testers, reviewers, or other parties involved in the software development process. Continuously monitoring code commits to repositories and generating summary logs can help detect authorized insiders making unauthorized changes to environment configurations, as it can audit and verify the source, time, reason, and impact of code changes made by authorized users. Performing static code analysis of committed code and generate summary reports is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to detect vulnerabilities, errors, bugs, or quality issues in committed code. Implementing an XML gateway and monitor for policy violations is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to protect XML-based web services from threats or attacks by validating XML messages against predefined policies. Monitoring dependency management tools and report on susceptible third-party libraries is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to identify outdated or vulnerable third-party libraries used in software development projects. Installing an IDS (intrusion detection system) on the development subnet and passively monitor for vulnerable services is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes

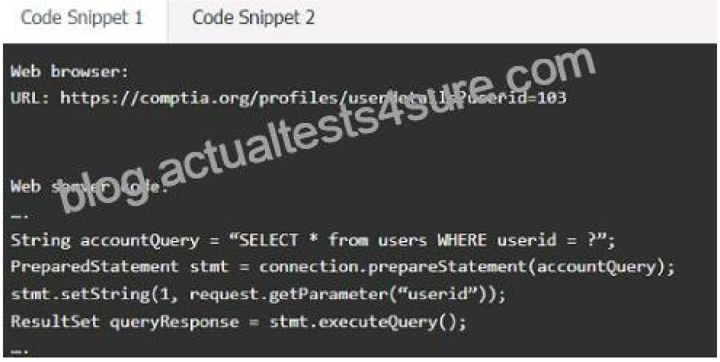
NEW QUESTION 239

A product development team has submitted code snippets for review prior to release.

INSTRUCTIONS

Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

Code Snippet 1

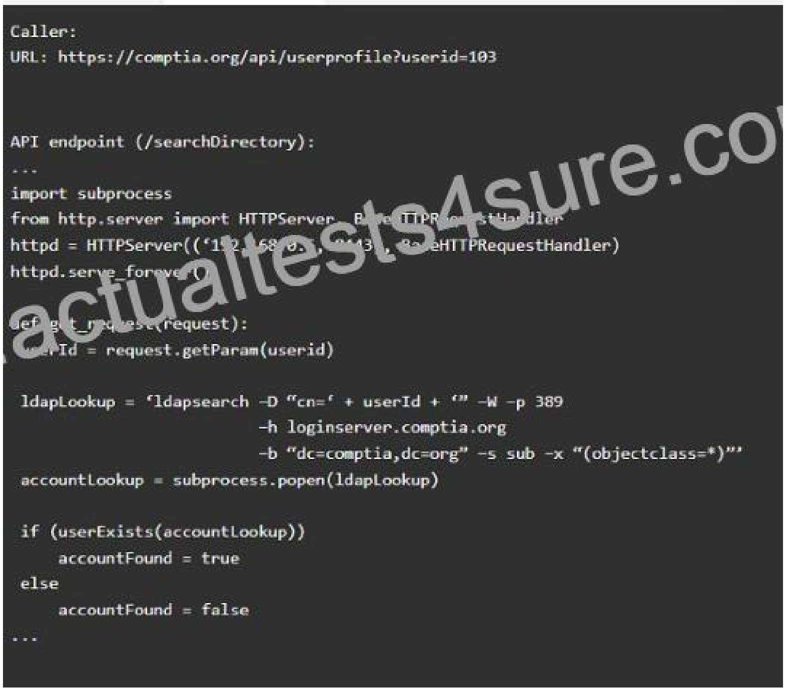


```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103



Web server code:
...
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
...
```

Code Snippet 2



```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.[illegible]', 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                        -h loginserver.comptia.org
                        -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

Vulnerability 1:

SQL injection

Cross-site request forgery

Server-side request forgery

Indirect object reference

Cross-site scripting

Fix 1:

Perform input sanitization of the userid field.

Perform output encoding of queryResponse,

Ensure usex:ia belongs to logged-in user.

Inspect URLS and disallow arbitrary requests.

Implement anti-forgery tokens.

Vulnerability 2

1) Denial of service

2) Command injection

3) SQL injection

4) Authorization bypass

5) Credentials passed via GET

Fix 2

A) Implement prepared statements and bind

variables.

B) Remove the serve_forever instruction.

C) Prevent the &#8220;authenticated&#8221; value from being overridden by a GET parameter.

D) HTTP POST should be used for sensitive parameters.

E) Perform input sanitization of the userid field.
See the solution belowin explanation

Explanation:

Code Snippet 1

Vulnerability 1: SQL injection

SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.

Fix 1: Perform input sanitization of the userid field.

Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2

Vulnerability 2: Cross-site request forgery

Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting dat a. This can result in unauthorized actions, data loss, or account compromise.

Fix 2: Implement anti-forgery tokens.

Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user&#8217;s browser can be accepted by the server.

NEW QUESTION 240

Which of the following BEST sets expectation between the security team and business units within an organization?
* Risk assessment
* Memorandum of understanding
* Business impact analysis
* Business partnership agreement
* Services level agreement
A service level agreement (SLA) is the best option to set expectations between the security team and business units within an organization. An SLA is a document that defines the scope, quality, roles, responsibilities, and metrics of a service provided by one party to another. An SLA can help align the security team&#8217;s objectives and activities with the business units&#8217; needs and expectations, as well as establish accountability and communication channels. Verified Reference:
https://www.comptia.org/training/books/casp-cas-004-study-guide ,
https://searchitchannel.techtarget.com/definition/service-level-agreement

NEW QUESTION 241

A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee&#8217; PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?
* The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.
* The DHCP server has a reservation for the PC&#8217;s MAC address for the wired interface.
* The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
* The DHCP server is unavailable, so no IP address is being sent back to the PC.

NEW QUESTION 242

Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage. Which of the following should be created to prevent this type of issue in the future?
* SLA
* BIA
* BCM
* BCP
* RTO
Explanation

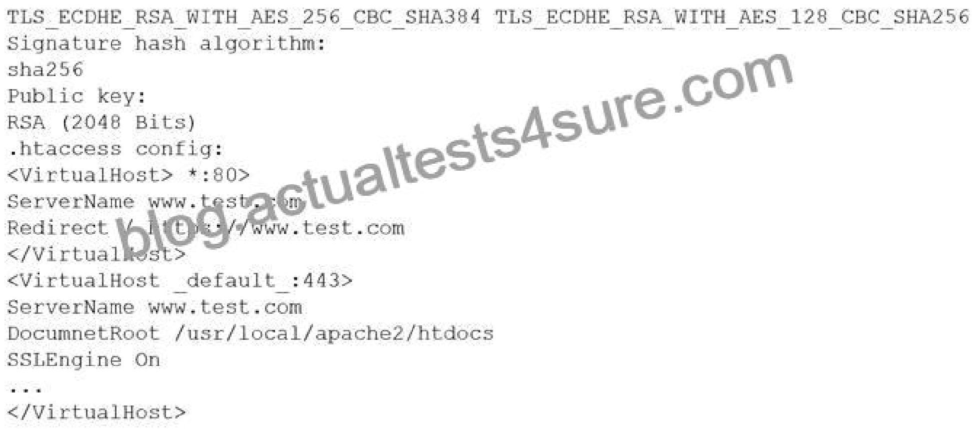
A Business Continuity Plan (BCP) is a set of policies and procedures that outline how an organization should respond to and recover from disruptions [1]. It is designed to ensure that critical operations and services can be quickly restored and maintained, and should include steps to identify risks, develop plans to mitigate those risks, and detail the procedures to be followed in the event of a disruption. Resources:

CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 4: &#8220;Business Continuity Planning,&#8221; Wiley,

2018. https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C

NEW QUESTION 243

A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:



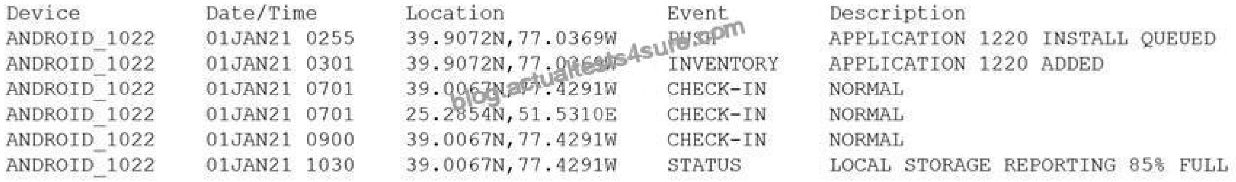
```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Signature hash algorithm:
sha256
Public key:
RSA (2048 Bits)
.htaccess config:
<VirtualHost> *:80>
ServerName www.test.com
Redirect / https://www.test.com
</VirtualHost>
<VirtualHost _default_:443>
ServerName www.test.com
DocumnetRoot /usr/local/apache2/htdocs
SSLEngine On
...
</VirtualHost>
```

Which of the following is the MOST likely cause of the customer&#8217;s inability to connect?
* Weak ciphers are being used.
* The public key should be using ECDSA.
* The default should be on port 80.
* The server name should be test.com.
Reference:

https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy-answers-for-whic

NEW QUESTION 244

Device event logs sources from MDM software as follows:



```
Device          Date/Time       Location            Event       Description
ANDROID_1022    01JAN21 0255    39.9072N,77.0369W   PUSH        APPLICATION 1220 INSTALL QUEUED
ANDROID_1022    01JAN21 0301    39.9072N,77.0369W   INVENTORY   APPLICATION 1220 ADDED
ANDROID_1022    01JAN21 0701    39.0067N,77.4291W   CHECK-IN    NORMAL
ANDROID_1022    01JAN21 0701    25.2854N,51.5310E   CHECK-IN    NORMAL
ANDROID_1022    01JAN21 0900    39.0067N,77.4291W   CHECK-IN    NORMAL
ANDROID_1022    01JAN21 1030    39.0067N,77.4291W   STATUS      LOCAL STORAGE REPORTING 85% FULL
```

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?
* Malicious installation of an application; change the MDM configuration to remove application ID 1220.

* Resource leak; recover the device for analysis and clean up the local storage.
* Impossible travel; disable the device&#8217;s account and access while investigating.
* Falsified status reporting; remotely wipe the device.

The device event logs show that the device was in two different locations (New York and London) within a short time span (one hour), which indicates impossible travel. This could be a sign of a compromised device or account. The best response action is to disable the device&#8217;s account and access while investigating the incident. Malicious installation of an application is not evident from the logs, nor is resource leak or falsified status reporting. Verified Reference:
https://www.comptia.org/blog/what-is-impossible-travel
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 245

An organization&#8217;s senior security architect would like to develop cyberdefensive strategies based on standardized adversary techniques, tactics, and procedures commonly observed. Which of the following would BEST support this objective?

* OSINT analysis
* The Diamond Model of Intrusion Analysis
* MITRE ATT&CK
* Deepfake generation
* Closed-source intelligence reporting

MITRE ATT&CK is a knowledge base that provides information on different types of adversary tactics, techniques, and procedures (TTPs) that are commonly observed in cyberattacks.

NEW QUESTION 246

A security engineer needs to select the architecture for a cloud database that will protect an organization&#8217;s sensitive dat a. The engineer has a choice between a single-tenant or a multitenant database architecture offered by a cloud vendor. Which of the following best describes the security benefits of the single-tenant option? (Select two).

* Most cost-effective
* Ease of backup and restoration
* High degree of privacy
* Low resilience to side-channel attacks
* Full control and ability to customize
* Increased geographic diversity

Single-tenant architectures provide a dedicated environment for each client, which enhances data privacy since the resources are not shared with other tenants. This isolation minimizes the risk of data leakage or interference from other tenants, offering a high degree of privacy. Additionally, single-tenancy allows for full control over the database environment, including customization options tailored to specific security requirements or compliance needs, which is not always possible in a multi-tenant architecture.

NEW QUESTION 247

A city government&#8217;s IT director was notified by the city council that the following cybersecurity requirements must be met to be awarded a large federal grant:

&#8211; Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting.

&#8211; All privileged user access must be tightly controlled and tracked to

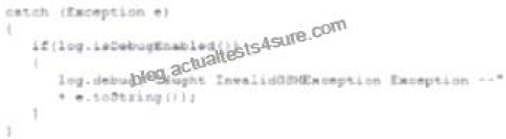
mitigate compromised accounts.

&#8211; Ransomware threats and zero-day vulnerabilities must be quickly identified.

Which of the following technologies would BEST satisfy these requirements? (Choose three.)
* Endpoint protection
* Log aggregator
* Zero trust network access
* PAM
* Cloud sandbox
* SIEM
* NGFW

NEW QUESTION 248

A developer implement the following code snippet.



```
catch (Exception e)
{
    if(log.isDebugEnabled())
    {
        log.debug("Caught InvalidGSMException Exception --"
        + e.toString());
    }
}
```

Which of the following vulnerabilities does the code snippet resolve?
* SQL inject
* Buffer overflow
* Missing session limit
* Information leakage
Explanation

SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL commands on a database by inserting them into an input field. The code snippet resolves this vulnerability by using parameterized queries, which prevent the input from being interpreted as part of the SQL command. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide ,

https://owasp.org/www-community/attacks/SQL_Injection

NEW QUESTION 249

A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens&#8217; personal, private, and confidential data?
* The principle of lawful, fair, and transparent processing
* The right to be forgotten principle of personal data erasure requests
* The non-repudiation and deniability principle
* The principle of encryption, obfuscation, and data masking

NEW QUESTION 250

A threat hunting team receives a report about possible APT activity in the network.

Which of the following threat management frameworks should the team implement?

* NIST SP 800-53
* MITRE ATT&CK
* The Cyber Kill Chain
* The Diamond Model of Intrusion Analysis

Explanation

MITRE ATT&CK is a threat management framework that provides a comprehensive and detailed knowledge base of adversary tactics and techniques based on real-world observations. It can help threat hunting teams to identify, understand, and prioritize potential threats, as well as to develop effective detection and response strategies. MITRE ATT&CK covers the entire lifecycle of a cyberattack, from initial access to impact, and provides information on how to mitigate, detect, and hunt for each technique. It also includes threat actor profiles, software descriptions, and data sources that can be used for threat intelligence and analysis. Verified References:

https://attack.mitre.org/

https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-att

https://www.ibm.com/topics/threat-management

NEW QUESTION 251

A recent data breach revealed that a company has a number of files containing customer data across its storage environment. These files are individualized for each employee and are used in tracking various customer orders, inquiries, and issues. The files are not encrypted and can be accessed by anyone. The senior management team would like to address these issues without interrupting existing processes.

Which of the following should a security architect recommend?

* A DLP program to identify which files have customer data and delete them
* An ERP program to identify which processes need to be tracked
* A CMDB to report on systems that are not configured to security baselines
* A CRM application to consolidate the data and provision access based on the process and need

CompTIA CAS-004 (CompTIA Advanced Security Practitioner (CASP+)) exam is an advanced-level certification designed for experienced IT professionals who want to enhance their skills and knowledge in the field of cybersecurity. CompTIA Advanced Security Practitioner (CASP+) Exam certification validates the skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments.

Check Real CompTIA CAS-004 Exam Question for Free (2024): https://www.actualtests4sure.com/CAS-004-test-questions.html]