Free Questions for CAS-004

Shared by Austin on 04-10-2024

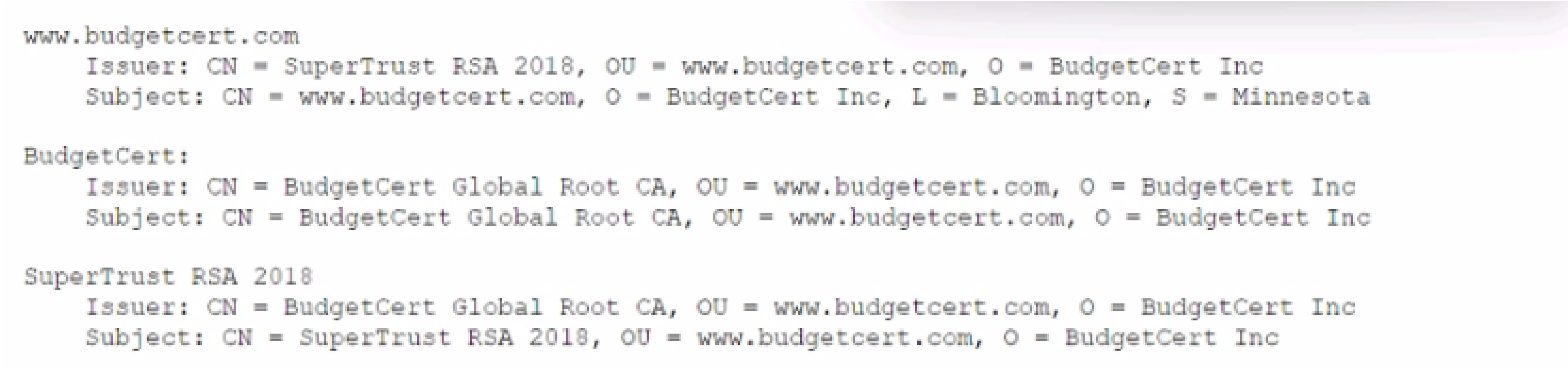
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A security administrator has been provided with three separate certificates and is trying to organize them into a single chain of trust to deploy on a website. Given the following certificate properties:



```
www.budgetcert.com
    Issuer: CN = SuperTrust RSA 2018, OU = www.budgetcert.com, O = BudgetCert Inc
    Subject: CN = www.budgetcert.com, O = BudgetCert Inc, L = Bloomington, S = Minnesota

BudgetCert:
    Issuer: CN = BudgetCert Global Root CA, OU = www.budgetcert.com, O = BudgetCert Inc
    Subject: CN = BudgetCert Global Root CA, OU = www.budgetcert.com, O = BudgetCert Inc

SuperTrust RSA 2018
    Issuer: CN = BudgetCert Global Root CA, OU = www.budgetcert.com, O = BudgetCert Inc
    Subject: CN = SuperTrust RSA 2018, OU = www.budgetcert.com, O = BudgetCert Inc
```

Which of the following are true about the PKI hierarchy? (Select two).

Options:

A- www.budgetcert.com.is the top-level CA.

B- www.budgetcert.com. is an intermediate CA.

C- SuperTrust RSA 2018 is the top-level CA.

D- SuperTrust RSA 2018 is an intermediate CA.

E- BudgetCert is the top-level CA

F- BudgetCert is an intermediate CA.

Answer:

C, E

Explanation:

Based on the given certificate properties:

SuperTrust RSA 2018 is an intermediate certificate authority (CA) because it is issued by BudgetCert Global Root CA, which is the top-level certificate authority.

BudgetCert is the top-level CA (root CA) in this public key infrastructure (PKI) hierarchy, as it issues certificates to SuperTrust RSA 2018 and has no issuer of its own.

Therefore, SuperTrust RSA 2018 is the intermediate CA, and BudgetCert is the top-level (root) CA in this PKI chain of trust. The www.budgetcert.com certificate is the leaf or end-entity certificate, which is used for the website itself.

CASP+ CAS-004 Exam Objectives: Domain 3.0 -- Enterprise Security Architecture (PKI and Certificate Chains of Trust)

CompTIA CASP+ Study Guide: PKI Hierarchy and Certificate Trust Models

Question 2

Question Type: **MultipleChoice**

A software developer has been tasked with creating a unique threat detection mechanism that is based on machine learning. The information system for which the tool is being developed is on a rapid CI/CD pipeline, and the tool developer is considered a supplier to the process. Which of the following presents the most risk to the development life cycle and lo the ability to deliver the security tool on time?

Options:

A- Deep learning language barriers

B- Big Data processing required for maturity

C- Secure, multiparty computation requirements

D- Computing capabilities available to the developer

Answer:

B

Explanation:

The most significant risk to the development of a machine-learning-based threat detection tool is the Big Data processing required for maturity. Machine learning models often require large datasets to train effectively, and processing and analyzing this data can be time-consuming and resource-intensive. This can delay the development timeline, especially in a rapid CI/CD pipeline environment where timely delivery is crucial. CASP+ highlights the challenges associated with machine learning and Big Data in security tool development, particularly the resource demands and the need for extensive data to ensure accuracy and maturity.

CASP+ CAS-004 Exam Objectives: Domain 2.0 -- Enterprise Security Operations (Big Data and Machine Learning Challenges)

CompTIA CASP+ Study Guide: Implementing and Managing Machine Learning in Security Environments

Question 3

Question Type: MultipleChoice

The primary advantage of an organization creating and maintaining a vendor risk registry is to:

Options:

A- define the risk assessment methodology.

B- study a variety of risks and review the threat landscape.

C- ensure that inventory of potential risk is maintained.

D- ensure that all assets have low residual risk.

Answer:

C

Explanation:

The primary advantage of creating and maintaining a vendor risk registry is to ensure that an inventory of potential risks is maintained. A vendor risk registry helps organizations keep track of the risks associated with third-party vendors, especially as they may introduce vulnerabilities or non-compliance issues. By maintaining this registry, the organization can continuously monitor and manage vendor-related risks in a structured way, improving its overall security posture. CASP+ emphasizes the importance of vendor risk management in an organization's broader risk management strategy.

CASP+ CAS-004 Exam Objectives: Domain 1.0 -- Risk Management (Vendor Risk Management)

CompTIA CASP+ Study Guide: Third-Party Risk Management and Risk Registries

Question 4

Question Type: **MultipleChoice**

A mobile device hardware manufacturer receives the following requirements from a company that wants to produce and sell a new mobile platform:

*The platform should store biometric data.

*The platform should prevent unapproved firmware from being loaded.

* A tamper-resistant, hardware-based counter should track if unapproved firmware was loaded.

Which of the following should the hardware manufacturer implement? (Select three).

Options:

A- ASLR

B- NX

C- eFuse

D- SED

E- SELinux

F- Secure boot

G- Shell restriction

H- Secure enclave

Answer:

C, F, H

Explanation:

To meet the mobile platform security requirements, the manufacturer should implement the following technologies:

eFuse: This hardware feature helps track and prevent unauthorized firmware by physically 'blowing' fuses to record events, such as firmware tampering, making it impossible to revert to older, unapproved firmware.

Secure boot: This ensures that only trusted and authorized firmware can be loaded during the boot process, preventing malicious or unauthorized software from running.

Secure enclave: A secure enclave is used to store sensitive information like biometric data in a hardware-isolated environment, protecting it from tampering or unauthorized access.

These three solutions provide the tamper resistance, secure firmware validation, and protection of sensitive data required for the platform. CASP+ emphasizes the use of hardware-based security features for protecting sensitive information and enforcing secure boot processes in embedded and mobile systems.

CASP+ CAS-004 Exam Objectives: Domain 3.0 -- Enterprise Security Architecture (Secure Hardware and Firmware Protection)

CompTIA CASP+ Study Guide: Hardware Security Features (eFuse, Secure Boot, Secure Enclave)

Question 5

Question Type: MultipleChoice

A Chief Information Security Officer is concerned about the condition of the code security being used for web applications. It is important to get the review right the first time, and the company is willing to use a tool that will allow developers to validate code as it is written. Which of the following methods should the company use?

Options:

A- SAST

B- DAST

C- Fuzz testing

D- Intercepting proxy

Answer:

A

Explanation:

Static Application Security Testing (SAST) is the best method for validating code as it is written. SAST analyzes the source code or binaries of an application for vulnerabilities before the code is executed, allowing developers to identify and fix security flaws early in the development process. This method integrates into the development environment and provides real-time feedback, which is critical for ensuring secure coding practices from the start. CASP+ highlights the importance of SAST in secure software development lifecycles (SDLCs) as a proactive measure to prevent security issues before the code is deployed.

CASP+ CAS-004 Exam Objectives: Domain 2.0 -- Enterprise Security Operations (SAST for Secure Code Validation)

CompTIA CASP+ Study Guide: Secure Software Development and Static Code Analysis

Question 6

Question Type: MultipleChoice

Two companies that recently merged would like to unify application access between the companies, without initially merging internal authentication stores. Which of the following technical strategies would best meet this objective?

Options:

A- Federation

B- RADIUS

C- TACACS+

D- MFA

E- ABAC

Answer:

A

Explanation:

Federation is the best strategy for unifying application access between two companies without merging their internal authentication stores. Federation allows users from different organizations to authenticate and access resources using their existing credentials through trusted third-party identity providers. This enables seamless access without the need to merge or consolidate internal authentication systems. CASP+ emphasizes federation as a key technology for enabling cross-organizational authentication while maintaining the integrity of separate identity stores.

CASP+ CAS-004 Exam Objectives: Domain 2.0 -- Enterprise Security Operations (Federated Identity and Authentication)

CompTIA CASP+ Study Guide: Federated Identity Management for Mergers and Cross-Company Access

Question 7

Question Type: **MultipleChoice**

A security analyst is participating in a risk assessment and is helping to calculate the exposure factor associated with various systems and processes within the organization. Which of the following resources would be most useful to calculate the exposure factor in this scenario?

Options:

A- Gap analysis

B- Business impact analysis

C- Risk register

D- Information security policy

E- Lessons learned

Answer:

B

Explanation:

A business impact analysis (BIA) is the most useful resource for calculating the exposure factor in a risk assessment. The BIA helps identify the criticality of systems and processes and quantifies the potential financial and operational impact of vulnerabilities being exploited. By understanding the business impact, the security team can more accurately determine the exposure factor, which is the proportion of an asset's value that is at risk in the event of a security incident. CASP+ highlights the role of BIAs in understanding risk exposure and supporting effective risk management decisions.

CASP+ CAS-004 Exam Objectives: Domain 1.0 -- Risk Management (Business Impact Analysis and Risk Exposure)

CompTIA CASP+ Study Guide: Business Impact Analysis for Risk Assessment

Question 8

Question Type: MultipleChoice

A company is migrating its data center to the cloud. Some hosts had been previously isolated, but a risk assessment convinced the engineering team to reintegrate the systems. Because the systems were isolated, the risk associated with vulnerabilities was low. Which of the following should the security team recommend be performed before migrating these servers to the cloud?

Options:

A- Performing patching and hardening

B- Deploying host and network IDS

C- Implementing least functionality and time-based access

D- Creating a honeypot and adding decoy files

Answer:

A

Explanation:

Before migrating previously isolated systems to the cloud, it is essential to perform patching and hardening. These systems may have been neglected while isolated, so updating them with the latest security patches and applying hardening measures (such as disabling unnecessary services and implementing strict access controls) is crucial to reduce vulnerabilities. This ensures that the systems are secure before they are exposed to the wider cloud environment. CASP+ emphasizes the importance of securing systems through patch management and hardening before integrating them into more exposed environments like the cloud.

CASP+ CAS-004 Exam Objectives: Domain 2.0 -- Enterprise Security Operations (Patching, Hardening, and Cloud Migration Security)

CompTIA CASP+ Study Guide: Securing and Hardening Systems Before Cloud Migration

Question 9

Question Type: **MultipleChoice**

A Chief Information Security Officer (CISO) received a call from the Chief Executive Officer (CEO) about a data breach from the SOC lead around 9:00 a.m. At 10:00 a.m. The CEO informs the CISO that a breach of the firm is being reported on national news. Upon investigation, it is determined that a network administrator has reached out to a vendor prior to the breach for information on a security patch that failed to be installed. Which of the following should the CISO do to prevent this from happening again?

Options:

A- Properly triage events based on brand imaging and ensure the CEO is on the call roster.

B- Create an effective communication plan and socialize it with all employees.

C- Send out a press release denying the breach until more information can be obtained.

D- Implement a more robust vulnerability identification process.

Answer:

B

Explanation:

To prevent similar issues from occurring again, the CISO should create an effective communication plan and ensure all employees are aware of it. A clear communication plan ensures that critical security information, such as breaches or vulnerabilities, is promptly communicated to the right stakeholders (e.g., the CEO) in a timely manner, preventing situations where the media reports on breaches before internal teams are fully informed. CASP+ emphasizes the importance of having structured communication protocols during security incidents to ensure accurate and timely responses.

CASP+ CAS-004 Exam Objectives: Domain 2.0 -- Enterprise Security Operations (Incident Communication Plans)

CompTIA CASP+ Study Guide: Developing and Implementing Effective Incident Communication Plans