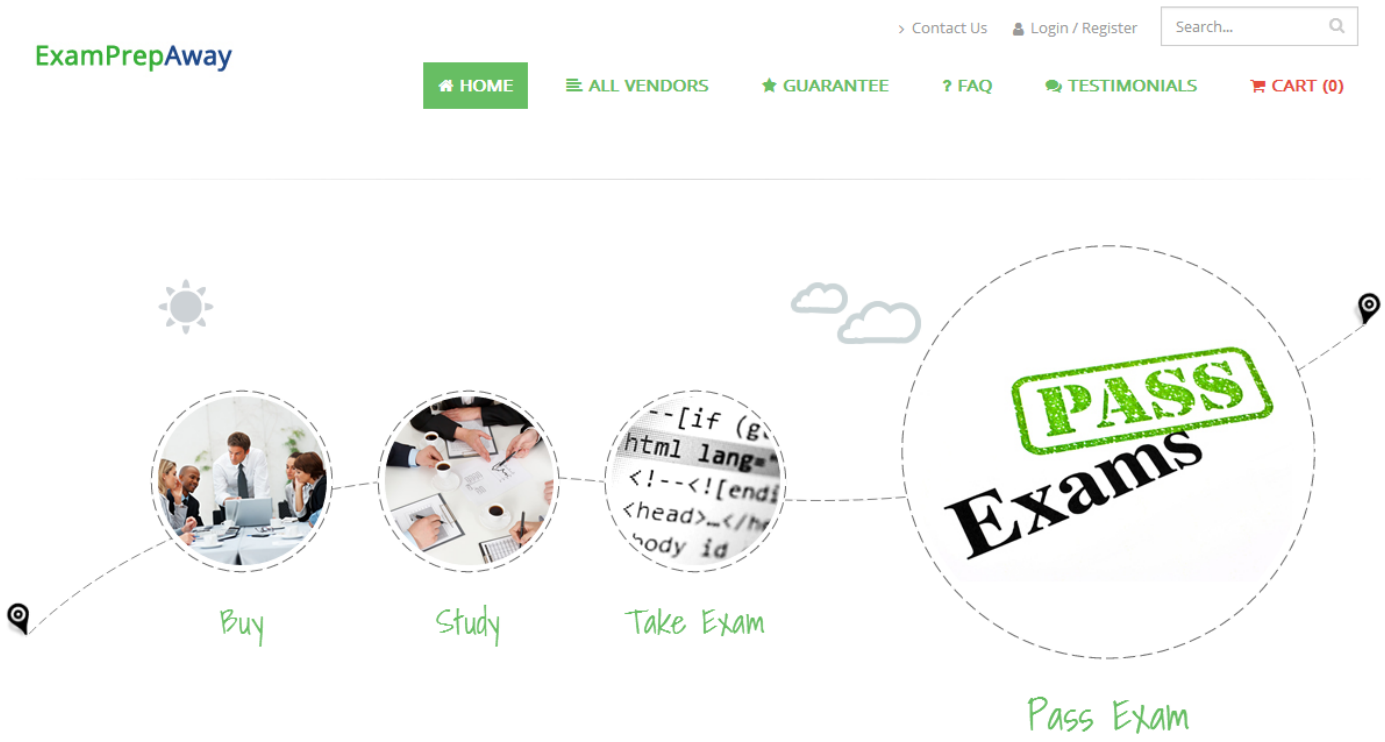
ExamPrepAway



Try **Online Engine** before you buy

We're not the only ones **happy** about ExamPrepAway Practice Material ...

56295+ customers in 100+ countries use ExamPrepAway Test Engine. Meet our customers.

GetCustom JET ORANGE iCompany Paradoxx iMessenger VOREED

http://www.examprepaway.com/

Latest Exam Guide & Learning Materials

Exam : **CAS-004-JPN**

Title : CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004日本語版)

Vendor : CompTIA

Version : DEMO

QUESTION NO: 1
ユーザーが不審な電子メールをレビューのためにセキュリティ
アナリストに転送しました。アナリストが電子メールを検査したところ、URL
にも添付ファイルにも悪意のあるアクティビティの兆候は見られませんでした。アナリストは電子メールの正当性を確認するために、次の情報収集方法のうちどれを使用する必要がありますか?
A. ヒューミント
B. ウエバ
C. OSINT
D. レース
Answer: C
Explanation:
Open-source intelligence (OSINT) refers to the collection and analysis of information that is gathered from public, or open, sources. In the context of confirming the legitimacy of an email, OSINT couldinvolve checking online databases, public records, or using search engines to find information related to the email's domain, the sender, links included in the email, or file hashes of attachments. This method can help determine if the email is part of a known phishing campaign or if it has been flagged by others as suspicious.

QUESTION NO: 2
米国に拠点を置く顧客のみを持つ企業が、他国の開発者に自社の Web
サイトでの作業を許可したいと考えています。ただし、企業は他国からの通常のインターネット
トラフィックをブロックする予定です。この目的を達成するために、企業はどの戦略を採用すべきですか (2 つ選択してください)。
A. 外部IPアドレスからのウェブサイトへのアクセスをブロックする
B. 開発者に会社のVPNを使用してもらう
C. ウェブサイトにWAPを実装する
D. 開発者にネットワーク上のジャンプボックスへのアクセス権を与える
E. 開発者向けにリバースプロキシを採用する
F. NATを使用して開発者のアクセスを有効にする
Answer: B D
Explanation:
Having developers use the company's VPN can provide them with secure access to the network while still allowing the company to block normal internet traffic from the other country. A jump box serves as a secure entry point for administrators or in this case, developers, to connect before launching any administrative tasks or accessing further areas of the network. This setup maintains security while still providing necessary access.

QUESTION NO: 3
セキュリティ エンジニアは、会社の Web
サイトでユーザーに次の例を許可していることに気付きました。
hitps://mycompany.com/main.php?Country=US
次の脆弱性のうち、このサイトに最も影響を与える可能性のあるものはどれですか?

A. SQLインジェクション
B. リモートファイルのインクルード
C. ディレクトリトラバーサル -
D. 安全でない参照
Answer: B
Explanation:
Remote file inclusion (RFI) is a web vulnerability that allows an attacker to include malicious external files that are later run by the website or web application12. This can lead to code execution, data theft, defacement, or other malicious actions. RFI typically occurs when a web application dynamically references external scripts using user-supplied input without proper validation or sanitization23.
In this case, the website allows users to specify a country parameter in the URL that is used to include a file from another domain. For example, an attacker could craft a URL like this:
https://mycompany.com/main.php?Country=https://malicious.com/evil.php
This would cause the website to include and execute the evil.php file from the malicious domain, which could contain any arbitrary code3.

QUESTION NO: 4
企業は、コードを本番環境にプロモートする際の変更管理アクティビティをレビューするための監査を受けています。監査により、次のことが明らかになりました。
* 一部の開発者は、コードを本番環境に直接公開できます。
* 静的コード レビューが適切に行われている。
* 脆弱性スキャンは、ポリシーごとに定期的にスケジュールされて実行されます。
次のうち、監査報告書に推奨事項として記載する必要があるのはどれですか?
A. 短いメンテナンス ウィンドウを実装します。
B. 定期的なアカウント レビューを実行します。
C. ジョブローテーションを実施する。
D. 職務の分離を改善します。
Answer: D

QUESTION NO: 5
エンジニアリングチームは、特殊な在庫管理用途に使用するモバイルデバイス群を開発・導入しています。これらのデバイスには、以下の要件を満たす必要があります。
* ユーザーの親しみやすさと使いやすさを考慮して、オープンソースの Android をベースにしています。
* 物理資産の在庫管理のための単一のアプリケーションを提供します。
* スキャン目的の在庫管理アプリケーションのみにカメラの使用を許可する
* あらゆる構成ベースラインの変更を禁止します。
* 要件以外のデバイス リソースへのすべてのアクセスを制限しますか?
A. アプリケーション ラッピング ポリシーを設定し、アプリケーションをラップし、MAM ツールを使用してインベントリ APK を配布し、アプリケーションの制限をテストします。
B. ルールを使用してドメインを定義する MAC sepolicy を記述し、インベントリ アプリケーションにラベルを付け、ポリシーを構築して、強制モードに設定します。
C. Android

Linuxカーネルバージョンを2,4,0以上にスワップアウトしますが、インターネットでAndroidをビルドし、MDLを介して不要な機能を削除し、ネットワークアクセスをブロックするように構成し、統合テストを実行します。
D. 要件が追加された Android ミドルウェア
ポリシーをビルドしてインストールし、ファイルを /user/init にコピーして、インベントリアプリケーションをビルドします。
Answer: A

QUESTION NO: 6
セキュリティ
コンサルタントは、製造施設で使用される工ネルギーの監視と制御に使用される電気リレーのネットワークを保護する必要があります。
コンサルタントが推奨を行う前に確認する必要があるシステムは、次のうちどれですか?
A. できます
B.ASIC
C. FPGA
D. SCADA
Answer: D
Reference: https://www.sciencedirect.com/topics/computer-science/protective-relay

QUESTION NO: 7
世界的な拠点を持つ地元の大学は、Web
サイトと関連システムの全面的な見直しに取り組んでいます。要件の一部は次のとおりです。
- 顧客のリソース需要の増加に対応する
- 情報への迅速かつ簡単なアクセスを提供します
- 高品質のストリーミングメディアを提供します
- ユーザーフレンドリーなインターフェースを作成する
次のどのアクションを最初に実行する必要がありますか?
A. 高可用性 Web サーバーを展開します。
B. ネットワークアクセス制御を強化します。
C. コンテンツ配信ネットワークを実装します。
D. 仮想化環境に移行します。
Answer: C
Explanation:
A content delivery network (CDN) is a geographically distributed network of servers that can cache content close to end users, allowing for faster and more efficient delivery of web content, such as images, videos, and streaming media. A CDN can also handle an increase in customer demand of resources, provide high-quality streaming media, and create a user-friendly interface by reducing latency and bandwidth consumption. A CDN can also improve the security and availability of the website by mitigating DDoS attacks and providing redundancy. Verified References:
https://www.cloudflare.com/learning/cdn/what-is-a-cdn/
https://learn.microsoft.com/en-us/azure/cdn/cdn-overview

https://en.wikipedia.org/wiki/Content_delivery_network

QUESTION NO: 8
SaaSソリューションを提供する組織が、最近、顧客データの損失を伴うインシデントを経験しました。このシステムには、パフォーマンスと利用可能なリソースの監視を含む自己修復機能が備わっています。システムが問題を検出すると、自己修復プロセスによってソフトウェアの一部が再起動されます。
インシデント発生時、自己修復システムがサービスの再起動を試みましたが、データドライブの空きディスク容量が不足していたため、すべてのサービスを再起動することができませんでした。自己修復システムは、一部のサービスが完全に再起動していないことを検出できず、システムが完全に稼働していると判断されました。サイレント障害が発生した理由として最も適切なものは次のうちどれですか？
A. システム ログが早期にローテーションされました。
B. ディスク使用率アラームは、サービスの再起動に必要な値よりも高くなっています。
C. 自己修復クラスタ内のノードの数は正常でした。
D. サービスの再起動前の条件チェックが成功しました。
Answer: D

QUESTION NO: 9
最高情報セキュリティ責任者 (CISO)
は新しい会社と協力しており、評価中にすべての関係者が自分たちの役割を確実に理解できるようにするための法的文書が必要です。CISO
は次のうちどれに各関係者に署名させる必要がありますか?
A. SLA
B. ISA
C. 権限とアクセス
D. 関与規則
Answer: D
Explanation:
Rules of engagement are legal documents that should be signed by all parties involved in an assessment to ensure they understand their roles and responsibilities. Rules of engagement define the scope, objectives, methods, deliverables, limitations, and expectations of an assessment project. They also specify the legal and ethical boundaries, communication channels, escalation procedures, and reporting formats for the assessment.
Rules of engagement help to avoid misunderstandings, conflicts, or liabilities during or after an assessment.
References: [CompTIA CASP+ Study Guide, Second Edition, page 34]

QUESTION NO: 10
セキュリティ
アナリストは、一般向けの銀行アプリケーションをサポートする脆弱で非推奨のランタイムエンジンを特定しました。開発者は、最新の開発環境への移行には少なくとも 1
か月かかると予想しています。移行中にサービスを中断することなくリスクを軽減するには、次のどのコントロールが最適ですか。
A. コードが準備できるまでシステムをシャットダウンする

B. 影響を受けるランタイムエンジンをアンインストールする
C. 影響を受けるポート上のトラフィックを選択的にブロックする
D. シグネチャを使用した IPS と WAF の設定
Answer: D
Explanation:
Given the vulnerability in the deprecated runtime engine, configuring an IPS (Intrusion Prevention System) and WAF (Web Application Firewall) with appropriate signatures is the best temporary control. This allows the organization to monitor and block potential attacks targeting known vulnerabilities in the runtime engine while the developers work on the transition. Shutting down the systems or uninstalling the runtime engine would cause service interruptions, and blocking traffic might disrupt legitimate users. IPS and WAF provide an active layer of defense without interrupting service. CASP+ emphasizes the use of layered security, including IPS and WAF, to mitigate risks in public-facing applications.
References:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Web Application Firewalls, Intrusion Prevention Systems) CompTIA CASP+ Study Guide: Mitigating Application Vulnerabilities with WAFs and IPS

QUESTION NO: 11
サイバーセキュリティアナリストは、潜在的なインシデントが発生していることを示すチケットを受け取りました。「お問い合わせ」フォームを含むウェブサイトで大量のログファイルが生成されています。アナリストは、ウェブサイトのトラフィック増加が最近のマーケティングキャンペーンによるものなのか、それとも潜在的なインシデントなのかを判断する必要があります。アナリストにとって最も役立つ情報は次のどれでしょうか？
A. 「お問い合わせ」フォームで適切な入力検証が構成されていることを確認する
B. 公開ウェブサイトの前に WAF を展開する
C. 受信ネットワークIPSベンダーからの新しいルールをチェックしています
D. ログ削減および分析ツールでウェブサイトのログファイルを実行する
Answer: D

QUESTION NO: 12
SOC アナリストは侵害の可能性に関するアラートを受け取り、次の SIEM ログを確認しています。

```
1:15:02PM JDoe successful login on laptop314
1:15:45PM JDoe launched outlook.exe on laptop314
1:17:03PM Process outlook.exe launched cmd.exe on laptop314
1:17:04PM Process cmd.exe launched rdp.exe on laptop314
1:17:04PM Process cmd.exe launched rdp.exe on laptop314
1:17:05PM JDoe successful login on server112
1:17:05PM JDoe successful login on server113
1:17:07PM JDoe launched cmd.exe on server112
```

SOC アナリストが推奨する最も適切なアクションは次のうちどれですか?
A. さらなる横方向の移動を防ぐためにアカウント JDoe を無効にします
B. ネットワークからラップトップ 314 を隔離しています

C. アカウント侵害の可能性について JDoe に警告します
D. ログインを防止するための HIPS ルールと NIPS ルールの作成
Answer: B
Explanation:
The SIEM logs indicate suspicious behavior that could be a sign of a compromise, such as the launching of cmd.exe after Outlook.exe, which is atypical user behavior and could indicate that a machine has been compromised to perform lateral movement within the network. Isolating laptop314 from the network would contain the threat and prevent any potential spread to other systems while further investigation takes place.

QUESTION NO: 13
組織がデジタル署名されたコードの利用を好む理由を最もよく説明しているのは次のどれですか? (2 つ選択してください)。
A. 原産地保証を提供します。
B. 整合性を検証します。
C. 機密性が向上します。
D. DRM と統合します。
E. 受信者の身元を確認します。
F. コードにマルウェアが含まれていないことを確認します。
Answer: A B
Explanation:
Option A (Origin assurance):Digital signatures ensure that the code originates from a trusted source.
Option B (Integrity verification):Digital signatures verify that the code has not been tampered with since it was signed.
Option C (Confidentiality):Digital signatures do not provide encryption or confidentiality.
Option D (DRMs):Digital signatures are not specifically related to Digital Rights Management.
Option E (Recipient verification):Digital signatures validate the sender, not the recipient.
Option F (Free of malware):While digital signatures verify integrity, they cannot guarantee that the code is free of malware.
References:
CompTIA CASP+ Exam Objective 2.1: Implement cryptographic solutions to protect application integrity.
CASP+ Study Guide, 5th Edition, Chapter 9, Digital Signatures and Code Signing.

QUESTION NO: 14
組織の既存のインフラストラクチャには、データセンター間のサイト間 VPN が含まれています。昨年、巧妙な攻撃者が VPN コンセントレータのゼロデイ脆弱性を悪用しました。したがって、最高情報セキュリティ責任者 (CISO) は、VPN ソリューションに対して別のゼロデイ エクスプロイトが使用された場合にサービスが失われるリスクを軽減するために、インフラストラクチャの変更を行っています。
次の設計のうち、CISO が使用するのに最適なものはどれですか?
A. 代替ベンダーの VPN コンセントレータの 2 番目の冗長層を追加する

B. 既存のサイト間 VPN 接続内で Base64 エンコーディングを使用する
C. VPN サイト間でのセキュリティ リソースの分散
D. 各 VPN コンセントレータで IDS サービスを実装する
E. サイトベース サービスのコンテナ ベース アーキテクチャへの移行
Answer: A
Explanation:
If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

QUESTION NO: 15
組織は、会社所有の資産がネットワーク外にある場合、または VPN
経由で接続されていない場合を把握できません。可視性が欠如していると、組織はセキュリティと運用の目標を達成できなくなります。リスクを軽減するために、組織は次のクラウドホスト型ソリューションのうちどれを実装する必要がありますか?
A. ウイルス対策
B. ウエバ
C. EDR
D. HIDS
Answer: C
Explanation:
Endpoint Detection and Response (EDR) solutions provide continuous monitoring and response to advanced threats. They can help mitigate the risk of not having visibility into off-network activities by detecting, investigating, and responding to suspicious activities on endpoints, regardless of their location.

QUESTION NO: 16
コンサルタントは顧客のクラウド環境にアクセスする必要があります。顧客は次のエンゲージメント要件を強制したいと考えています。
* すべての顧客データは常に顧客の管理下に置かれなければなりません。
* お客様の環境へのサードパーティのアクセスは、お客様が制御する必要があります。
* 認証資格情報とアクセス制御は顧客の管理下にある必要があります。
クラウド環境にアクセスするときに顧客の要件をすべて満たすためにコンサルタントが行うべきことは次のうちどれですか?
A. 読み取り専用認証情報で顧客の SSO
を使用し、顧客がプロビジョニングした安全なネットワーク
ストレージを使用してデータを共有します。
B. お客様が提供する VDI ソリューションを使用して、お客様の環境で作業を実行します。
C. コード
スニペットを顧客に提供し、顧客にコードを実行してその出力を安全に提供してもらいます。
D. 顧客に API 認証情報を要求し、顧客の環境へのアクセスには API
呼び出しのみを使用します。
Answer: B
Explanation:

The consultant should use the customer-provided VDI solution to perform work on the customer's environment. VDI stands for virtual desktop infrastructure, which is a technology that allows users to access a virtual desktop hosted on a remote server. VDI can help meet the customer's requirements by ensuring that all customer data remains under the customer's control at all times, that third-party access to the customer environment is controlled by the customer, and that authentication credentials and access control are under the customer's control. Verified References:
https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks
https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social- engineering-attacks/
https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

QUESTION NO: 17
最高情報セキュリティ責任者 (CISO) は、モバイル デバイスが会社のデータセンターの機密エリアに侵入するたびに警告を送信するシステムを設定するようセキュリティ管理者に依頼しました。CISO はまた、エリアに入ろうとしている個人に、アクセスが記録され監視されていることを警告できるようにしたいと考えています。これらの要件を満たすものは次のうちどれですか?
A. 近距離無線通信
B.ショートメッセージサービス
C. ジオフェンシング
D. Bluetooth
Answer: C
Explanation:
Geofencing is a location-based service that allows an organization to define and enforce a virtual boundary around a sensitive area, such as a data center. Geofencing can use various technologies, such as GPS, Wi-Fi, cellular data, or RFID, to detect when a mobile device enters or exits the geofence. Geofencing can also trigger certain actions or notifications based on the device's location. For example, the organization can set up a geofencing policy that sends an alert to the CISO and the device user when a mobile device enters the data center area. Geofencing can also be used to restrict access to certain apps or features based on the device's location. Verified References:
https://developer.android.com/training/location/geofencing
https://www.manageengine.com/mobile-device-management/mdm-geofencing.html
https://www.koombea.com/blog/mobile-geofencing/

QUESTION NO: 18
サードパーティベンダーからの特定の受信トラフィックが高リスク国からのものではないことを保証するのは次のどれですか?
A. マイクロセグメンテーション
B. サプライチェーンの可視性
C. ジオコードされたファイアウォールルール
D. ソースコードレビュー
Answer: C
Explanation:

Comprehensive and Detailed in-Depth Explanation:
Why the Correct Answer is C (Geocoded firewall rules):
Geocoded firewall rulesare security configurations thatfilter traffic based on geographic location(commonly by IP address).
These rules can be configured to:
Allow or denyinbound and outbound trafficbased on the country of origin.
Restrictthird-party vendor connectionsfromhigh-risk or banned countries.
For example:
Blocking allincoming connections from countries with high cyber threat levels.
Allowing only vendors frompre-approved regions.
Geocoded rules are especially useful inregulatory compliance scenarioswheredata sovereigntyis a concern.
Why the Other Options Are Incorrect:
A). Microsegmentation:
Microsegmentation involvesisolating network segmentsto enhance internal security.
Itdoes not addressthe geographic origin of traffic.
Primarily used forreducing lateral movementwithin a network rather than filtering external sources.
B). Supply chain visibility:
This involvesmonitoring and understandingthe components and processes involved in thesupply chain.
It does notactively block or restrict trafficfrom specific geographic locations.
D). Source code reviews:
These are conducted toidentify vulnerabilities in application code.
They do notrestrict inbound trafficbased on geographic criteria.
Real-World Scenario:
A financial services company needs toblock access from countries under sanctionsor known forcybercrime activities.
Thefirewall is configuredto drop all inbound traffic from IP ranges associated withhigh-risk countries, maintaining compliance with regulations likeOFAC.
Example of Geocoded Firewall Configuration:
Example Rule in an IPTables Configuration:
bash
CopyEdit
iptables -A INPUT -m geoip --src-cc CN,RU,IR -j DROP
This ruleblocks trafficfromChina (CN),Russia (RU), andIran (IR).
Benefits of Geocoded Firewall Rules:
Risk Reduction:Minimizes exposure tothreat actors from known high-risk regions.
Compliance:Helps organizations comply withregulatory requirementsthat restrict data from certain countries.
Operational Efficiency:Automatically blocks traffic without requiring manual intervention.
Extract from CompTIA SecurityX CAS-005 Study Guide:
TheCompTIA SecurityX CAS-005 Official Study Guideemphasizes the importance ofgeolocation-based access controlin environments wherethird-party access is common.
Geocoded firewall rules enable organizations toeffectively control and reduce the attack

surfaceby blocking traffic fromhigh-risk regions.

QUESTION NO: 19
最高情報セキュリティ責任者は、Web アプリケーションに使用されているコード
セキュリティの状態を懸念しています。最初のレビューを正しく行うことが重要であり、会社は開発者が記述されたコードを検証できるツールを使用するつもりです。会社が使用すべき方法は次のどれですか。
A. 標準
B. ダスト
C. ファズテスト
D. プロキシを傍受する
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.
References:
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 NO: 20
ある企業がオンプレミス サービスをクラウドに移行しました。最近の監査で、クラウドサービス全体のデータが適切に分類され、文書化されていることが確認されましたが、他のシステムはこの情報に基づいて動作したりフィルタリングしたりすることができません。他のクラウドベースのシステムがこの情報を利用できるようにするには、次のどれを導入する必要がありますか。
A. データマッピング
B. データのラベル付け
C. ログスクレイピング
D. リソースのタグ付け
Answer: B
Explanation:
Step by Step Explanation:
Data labeling enables metadata tagging for data classification, which allows systems to filter, act, and enforce policies based on the labels.
Data mapping is used for understanding data flows but does not support automation.
Log scraping and resource tagging are unrelated to enabling system actions based on data classification.
Reference: CASP+ Exam Objectives 5.1 - Implement controls based on data classifications.

QUESTION NO: 21
ある企業は、新しい決済システム オファリングのフロント エンドを提供するために CSP を使用しています。新しいオファリングは現在、PCI
準拠として認定されています。統合ソリューションが準拠するために、顧客は次のことを行う必要があります。
A. リスクがプロバイダーに移管されるため、PCI 準拠も必要です。
B. プロバイダーの管理対象サーバーレス サービスに対して独自の PCI
評価を実行する必要があります。
C. クラウド プロバイダーの環境の侵入テストを実行する必要があります。
D. 新しいオファリングの対象範囲内のシステムも PCI
に準拠していることを確認する必要があります。
Answer: D
Explanation:
Even though the company uses a cloud service provider (CSP) that is PCI compliant, the customer must still ensure that in-scope systems related to their new payment system offering are also PCI compliant. PCI DSS (Payment Card Industry Data Security Standard) applies to any system that processes, stores, or transmits credit card data, and this includes customer-owned systems, services, or applications integrated into the solution. The responsibility is shared between the CSP and the customer, and compliance is not automatically inherited just because the CSP is compliant. CASP+ emphasizes that organizations must ensure all components within their control are also PCI compliant.
References:
CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (Compliance and PCI DSS) CompTIA CASP+ Study Guide: Cloud Services and PCI Compliance

QUESTION NO: 22
最高情報責任者は、高価な SAN
ストレージの費用を節約するために、すべての会社データをクラウドに移行することを検討しています。
移行中に対処する必要がある可能性が最も高いセキュリティ上の懸念は次のうちどれですか？
A. レイテンシー
B. データ漏洩
C. データ損失
D. データ分散
Answer: B
Explanation:
Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but a

availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or control of data.
VerifiedReferences: https://www.comptia.org/blog
/what-is-data-exposure https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION NO: 23
リスク担当者がリスク評価を行う前にセキュリティ境界を決定する主な理由は次のうちどれですか?
A. リスク評価の範囲を決定するため
B. システムのビジネス所有者を決定するため
C. 定量的分析を実行するか定性的分析を実行するかを決定します。
D. どの法律や規制が適用されるかを決定するため
Answer: A
Explanation:
Identifying the security boundary is an essential first step in a risk assessment process as it defines the scope of the assessment. It delineates the environment where the risk assessment will take place and sets the limits for what assets, systems, and processes will be included in the assessment.

QUESTION NO: 24
クラウド セキュリティ エンジニアは、クラウドでホストされる WAF
をセットアップしています。エンジニアは、組織がホストする複数の Web
サイトを保護するソリューションを実装する必要があります。組織の Web
サイトは次のとおりです。
* www.mycompany.org
* www.mycompany.com
*campus.mycompany.com
*ウィキ。mycompany.org
ソリューションはコストを節約し、すべての Web
サイトを保護できる必要があります。ユーザーは、パス上の攻撃をクラウド セキュリティ
エンジニアに通知できる必要があります。最良の解決策は次のうちどれですか?
A. SAN 証明書を 1 つ購入します。
B. 自己署名証明書を実装します。
C. Web サイトごとに 1 つの証明書を購入します。
D. ワイルドカード証明書を 1 つ購入します。
Answer: D
Explanation:
Purchasing one wildcard certificate is the best solution to protect multiple websites hosted by an organization in a cloud-hosted WAF. A wildcard certificate is a type of SSL/TLS certificate thatcan secure a domain name and any number of its subdomains with a single certificate. For example, a wildcard certificate for *.
mycompany.com can secure www.mycompany.com, campus.mycompany.com, and any other subdomain under mycompany.com. A wildcard certificate can save costs and simplify management compared to purchasing individual certificates for each website.

References: [CompTIA CASP+ Study Guide, Second Edition, page 301]

QUESTION NO: 25
セキュリティ アナリストは、次の出力を確認しています。

```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

このタイプの攻撃を最も緩和するのは、次のうちどれですか?
A. ネットワーク ファイアウォールのインストール
B. WAF をインラインに配置する
C. IDS の実装
D. ハニーポットのデプロイ
Answer: B
Explanation:
The output shows a SQL injection attack that is trying to exploit a web application. A WAF (Web Application Firewall) is a security solution that can detect and block malicious web requests, such as SQL injection, XSS, CSRF, etc. Placing a WAF inline would prevent the attack from reaching the web server and database.
References: https://owasp.org/www-community/attacks/SQL_Injection
https://www.cloudflare.com/learning
/ddos/glossary/web-application-firewall-waf/

QUESTION NO: 26
押収されたラップトップからファイル ハッシュを取得する最も適切な理由はどれですか。
A. 各ファイルのメタデータの改ざんを防ぐため
B. 各ファイルの整合性を後で検証するため
C. 各ファイルに一意の識別子を生成する
D. ファイルの保管チェーンを維持するため
Answer: B
Explanation:
File hashing is used to create a digital fingerprint of files to detect unauthorized changes. By comparing the hash values before and after analysis, the integrity of the files can be validated. This aligns with CASP+ objective 5.2, which includes forensic evidence integrity and validation methods.

QUESTION NO: 27
ある SaaS スタートアップは、DevSecOps プログラムを成熟させつつあり、サーバーレス アプリケーションの脆弱性を特定する平均時間と修復に関連するコストを削減するために、開発プロセスの早い段階で弱点を特定したいと考えています。このスタートアップは、公開

されているセキュリティを力バーするために、DAST を使用して初期のセキュリティ
テストの取り組みを開始しました。アプリケーション
コンポーネントに直面しており、最近バグ報奨金プログラムを導入しました。
次のうち、会社の目的を最もよく達成できるのはどれですか?

A. RASP

B.SAST

C.WAF

D. CMS

Answer: B

Explanation:

Static application security testing (SAST) is a method of analyzing the source code of an application for vulnerabilities and weaknesses before it is deployed. SAST can help identify security issues earlier in the development process, reducing the time and cost of remediation. Dynamic application security testing (DAST) is a method of testing the functionality and behavior of an application at runtime for vulnerabilities and weaknesses. DAST can cover public-facing application components, but it cannot detect issues in the source code or in serverless applications. Runtime application self-protection (RASP) is a technology that monitors and protects an application from attacks in real time by embedding security features into the application code or runtime environment. RASP can help prevent exploitation of vulnerabilities, but it cannot identify or fix them. A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can help protect an application from common attacks, but it cannot detect or fix vulnerabilities in the application code or in serverless applications. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 3: Enterprise Security Operations, Objective 3.4: Conduct security assessments using appropriate tools

QUESTION NO: 28

大規模な組織は、オンプレミスからクラウドへの移行を計画しています。最高情報セキュリティ責任者 (CISO)
は、セキュリティの責任について懸念しています。企業がクラウドへの移行を決定した場合、新しい物理データセンターのセキュリティの責任者は次のどれですか?

A. 第三者評価機関

B. CSP

C. 組織

D. 共有責任

Answer: B

Explanation:

In cloud computing models, the security of the physical data center is the responsibility of the Cloud Service Provider (CSP). The CSP is responsible for protecting the infrastructure that runs all of the services offered in the cloud, which includes the physical security of the data center.

QUESTION NO: 29

次の用語のうち、CASB またはサードパーティ
エンティティへの暗号化キーの配信を指すものはどれですか?

A. 鍵共有
B. キー配布
C. キーリカバリ
D. キーエスクロー
Answer: D
Explanation:
Key escrow is a process that involves storing encryption keys with a trusted third party, such as a CASB (Cloud Access Security Broker) or a government agency. Key escrow can enable authorized access to encrypted data in case of emergencies, legal issues, or data recovery. However, key escrow also introduces some risks and challenges, such as trust, security, and privacy.References: https://www.techopedia.com /definition/1772/key-escrow https://searchsecurity.techtarget.com/definition/key-escrow

QUESTION NO: 30
顧客は、サブスクライブした Web
サービスの安全な通信を常に要求していますが、会社は現在、内部 CA
への独自の証明書要求に署名しています。
次のアプローチのうち、顧客の要件を最もよく満たすのはどれでしょうか?
A. 電子メールの暗号化のためにローカル CA への CSR を生成します。
B. ワイルドカード証明書の CSR をパブリック CA に送信します。
C. パブリック CA からソフトウェア署名証明書を要求します。
D. サーバー認証証明書の CSR を処理します。
Answer: D
Explanation:
Step by Step Explanation:
Server authentication certificates are used to secure web communication (e.g., HTTPS). Submitting a CSR (Certificate Signing Request) for a server authentication certificate ensures the web services can securely establish encrypted communication.
Other options, such as email encryption or software signing, do not apply in this scenario.
Reference: CASP+ Exam Objectives 2.3 - Apply cryptographic techniques to secure communications.

QUESTION NO: 31
お客様から、www.test.com の Web
サイトに接続してサービスを利用できないという報告がありました。顧客は、Web
アプリケーションに次の公開された暗号スイートがあることに気付きました。

```
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>
```

お客様が接続できない原因として最も可能性が高いのは次のうちどれですか?

A. 弱い暗号が使用されています。

B. 公開鍵は ECDSA を使用する必要があります。

C. デフォルトはポート 80 です。

D. サーバー名は test.com にする必要があります。

Answer: A

Reference: https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy- answers-for-which-to-choose-when

QUESTION NO: 32

企業は SSL インスペクションを実装しています。今後 6
か月の間に、サブドメインで分離される複数の Web アプリケーションが展開されます。
複数の証明書をデプロイしなくてもデータを検査できるのは、次のうちどれですか?

A. 利用可能なすべての暗号スイートを含めます。

B. ワイルドカード証明書を作成します。

C. サードパーティ CA を使用します。

D. 証明書のピン留めを実装します。

Answer: B

Explanation:

A wildcard certificate is a certificate that can be used for multiple subdomains of a domain, such as *.example.
com. This would allow the inspection of the data without multiple certificate deployments, as one wildcard certificate can cover all the subdomains that will be separated out with subdomains. Including all available cipher suites may not help with inspecting the data without multiple certificate deployments, as cipher suites are used for negotiating encryption and authentication algorithms, not for verifying certificates. Using a third- party CA (certificate authority) may not help with inspecting the data without multiple certificate deployments, as a third-party CA is an entity that issues and validates certificates, not a type of certificate. Implementing certificate pinning may not help with inspecting the data without multiple certificate deployments, as certificate pinning is a technique that hardcodes the expected

certificate or public key in the application code, not a type of certificate. Verified References:https://www.comptia.org/blog/what-is-a- wildcard-certificate https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION NO: 33
災害復旧の目標をサポートするために、サードパーティは 99.999%
の稼働率を提供することに同意しました。最近、ハードウェア障害がファイアウォールに影響を与えましたが、サービスの低下はありませんでした。次のどの回復力コンセプトが最も可能性が高いでしょうか?
A. クラスタリング
B. 高可用性
C. 冗長性
D. レプリケーション
Answer: B
Explanation:
High availability ensures continuous operation despite hardware failures by leveraging redundant components like clustered firewalls or failover systems. This aligns with CASP+ objective 3.1, which focuses on implementing availability and redundancy mechanisms in disaster recovery planning.

QUESTION NO: 34
一般的な産業用プロトコルには、次の特性があります。
* 認証/セキュリティは提供されません
* クライアント/サーバー関係で実装されることが多い
* RTUまたはTCP/IPのいずれかとして実装されます
次のどれが説明されていますか?
A. プロフィネット
B. モドバス
C. ジグビー
D. Z-Wave
Answer: B
Explanation:
The protocol described is Modbus, which is a commonly used industrial protocol that lacks built-in authentication and security features. Modbus operates in a client/server model and can be implemented over RTU (Remote Terminal Unit) or TCP/IP for communication between devices. The other protocols mentioned either have different characteristics or are used in different contexts (such as Profinet for industrial automation, Zigbee for wireless IoT devices, and Z-Wave for home automation). CASP+ identifies Modbus as a critical protocol in industrial environments that lacks security and requires additional protective measures.
References:
CASP+ CAS-004 Exam Objectives: Domain 4.0 - Industrial Control Systems (ICS) and Modbus Protocol CompTIA CASP+ Study Guide: Industrial Protocols and Modbus Security

QUESTION NO: 35

大規模な多国籍メーカーのセキュリティ
アーキテクトは、トラフィックを監視するセキュリティ
ソリューションを設計および実装する必要があります。
ソリューションを設計する際、セキュリティ アーキテクトは、##
ネットワークに対する攻撃を防ぐために、次のどの脅威に重点を置く必要がありますか?
A. サイズまたは長さが間違っているパケット
B. DNP3ポートでの非DNP3通信の使用
C. 時間の経過に伴う複数の要請応答
D. サポートされていない暗号化アルゴリズムの適用
Answer: C