Comptia Advanced Security Practitioner (CAS+) Exam (Japanese version)

1. セキュリティ技術者が、新しいSIEMのRFPに次の要件を組み入れています。

A. ビッグデータ分析

B. マルチセンサー展開

C. 機械学習

D. オートスケール検索機能

E. 集中ログ集計

F. クラウドベースの管理

Answer(s): A,C

---

2. Kaliのセキュリティツールからの次の出力があるとします。

A. ネットワーク列挙子

B. ファザー

C. ログ削減

D. SCAPスキャナー

Answer(s): D

---

3. 組織はクラウドコンピューティングの実装を望んでいますが、どのサービスを選択するかがわかりません。組織は、プライベートネットワーク上で完全に管理されているアプリケーションを共有し、共同作業し、使用できるようにしたいと考えています。組織がニーズに基づいて実装する必要があるクラウドコンピューティングサービスのタイプは次のうちどれですか？

A. CaaS

B. laaS

C. PaaS

D. SaaS

Answer(s): B

---

4. ある企業が、組み込み環境で使用されるカスタマイズされたOSビルドの要件を開発しています。実行可能ファイルの処理中にバッファオーバーランが成功する可能性を減らすことができるハードウェアを同社は調達しました。この重要なハードウェアベースの対策を利用するには、OSに次の機能のうちどれを含める必要がありますか？

A. TrustZone

B. NX / XNビット

C. アプリケーションホワイトリスト登録

D. ASLR

E. SCP

Answer(s): B

---

5. セキュリティアナリストは、地域の医療施設での脆弱性評価を完了する責任があります。アナリストは、次のNmap出力を確認します。

A. Nmapスクリプト10はSMBサーバーを実行します

B. SMBサーバーを停止するためのNmapスクリプト

C. 脆弱なSMBサーバーをスキャンするためのNmapスクリプト

D. スキャンするNmapスクリプト（またはUOP445の安全でないサーバー）

Answer(s): D

---

6. セキュリティ管理者は、会社所有のモバイルデバイスを強化するためのコントロールを実装したいと考えています。 会社のポリシーでは、次の要件を指定しています。

A. Disable 802.11

B. Enable remote wipe

C. Enable secure boot

D. Enable DLP

E. Enable EDR

F. Disable Bluetooth

G. Enable SEAndroid

H. Disable geotagging

Answer(s): A,F,G

---

7. セキュリティアナリストは、適切な技術管理設定とパラメータを選択する前に、次の企業要件を検討しています。

A. 地域ごとに分散したクラウド環境

B. 毎日のスナップショットを実装するバックアップソリューション

C. 5ナインのアップタイムを実現するロードバランサの背後にあるサーバーファーム

D. リアルタイムSyslog機能を収集するSyslog機能

Answer(s): B

---

8. 次のうち、利害関係者の関与の主な目標はどれですか？

A. ユーザー権限昇格を制限するための最良の方法を理解する

B. どのセキュリティ要件を安全性を延期できるかを判断する

C. リスクコンプライアンスのアウトリーチと理解を完了する

D. セキュリティ要件がビジネス目標をサポートすることを保証する

Answer(s): D

---

9. システムモダナイゼーションプログラムの一部として、弱い暗号化アルゴリズムの使用が特定されています。ウェットサービスAPI APIを使用しているクライアントは、システムをアップグレードできず、一時的なものとして安全なアルゴリズムセットの使用をサポートします。回避策クライアントはそのIPスペースを提供し、ネットワーク管理者はACLを介したAPIへのアクセスをクライアントが保持するIPスペースのみに制限します。この状況でのACLの使用例は次のうちどれですか？

A. 回避

B. 緩和策

C. 転移

D. 受け入れ

E. 評価

Answer(s): B

---

10. いくつかの業界の競合他社がサイバー攻撃の結果としてデータ損失を被った後、会社の最高執行責任者（COO）は情報セキュリティ管理者に連絡して組織のセキュリティスタンスをレビューしました。議論の結果、COOは組織が次の基準を満たすことを望んでいます。

A. EDRプラットフォームを実装する

B. 既存のIPSリソースを再構成します

C. WAFを実装する

D. UTMソリューションをデプロイする

E. SIEMソリューションをデプロイする

Answer(s): D

---

11. セキュリティエンジニアは、既知のインシデントに続いてDNSサーバーを調べています。エンジニアは、次のコマンドをサーバーのシェル履歴の最新のエントリと見なします。

A. ドライブはフォレンジック分析のために複製されました。

B. ハードドライブはインシデント後にフォーマットされました。

C. サーバーのテープバックアップが実行されました。

D. DNSログファイルは期待どおりに毎日ロールされました

Answer(s): A

---

12. 何千人ものユーザーがいる大企業では、インサイダーの脅威による悪意のある活動が比較的頻繁に発生しています。活動の多くは、特権ユーザーやネットワークファイル共有に対する標的型攻撃を引き起こす内部偵察を伴うように思われます。このシナリオで、次のうちどれがこれらの攻撃を防止または阻止する可能性がありますか。（2つ選んでください。）

A. ホストオペレーティングシステムが脆弱性をスキャンされる頻度を高め、脆弱性の特定と対応するパッチの適用との間の許容時間を短縮する

B. 既存の動作規則を修正して、利用可能なツールを使用してユーザーやファイルディレクトリを列挙したり、自分の職務に直接関係しない目に見えるリソースにアクセスしたりすることを禁止する明示的ステートメントを含める

C. すべてのワークステーションで、フルディスク暗号化を実装し、認証に複雑なパスワードを要求するようにUEFIインスタンスを構成します。

D. 企業内のすべてのマシンのオペレーティングシステムによって強制されるアプリケーションブラックリストを実装する

E. 特権ユーザー向けのロールベースのトレーニングを実施し、彼らに対する一般的な脅威を明らかにし、攻撃を阻止するためのベストプラクティスをカバーする

F. デフォルトですべてのワークステーションにグループポリシーを介してコマンドシェル制限を適用し、どのネイティブオペレーティングシステムツールが使用可能かを制限します。

Answer(s): B,F

---

13. 外部の赤いチームメンバーが侵入テストを実施し、ブランチオフィスにある大規模な組織のサーバールームへの物理的なアクセスを試みます。偵察中、赤いチームメンバーは、タンブラーロックのある、ロビーの隣にあるサーバールームへの明確にマークされたドアを見ます。

A. Bump key

B. RFID duplicator

C. Screwdriver set

D. Rake picking

Answer(s): A

---

14. サイバーセキュリティアナリストは、セキュリティを企業の姿勢で確認するために雇われています。サイバーセキュリティアナリストは、少数のIPアドレスからのSYNフラッドが原因で、非常に高いネットワーク帯域幅の消費に気付いています。次のうちどれがインシデント対応をサポートするために取るべき最良の行動でしょうか？

A. すべてのSYNパケットをブロックします。

B. ルーターに入力フィルタを適用します。

C. パケットキャプチャツールをインストールします。

D. 会社の帯域幅を広げます。

Answer(s): B

---

15. 大規模な組織では、1人のスタッフが、企業が承認したファイル共有のクラウドコラボレーションサービスに関するドキュメントを誤って共有した後、データ侵害に見舞われています。セキュリティ管理者は、別のチャネルを介して同様のイベントが再発する可能性を減らすための制御を実装する必要があります。コントロールは、イベントが再発した場合の早期検出と修復を支援する必要もあります。

A. VPNソフトウェアを展開し、すべてのリモートスタッフが企業プロキシを介してインターネットに接続するようにします。

B. すべての外部コラボレーションサイトへのアクセスを警告するようにSIEMを構成します。

C. CASBソリューションを展開して、ファイル共有クラウドサービスを監視および制限します。

D. アウトバウンドHTTPS接続専用のSSL復号化機能を実装します。

E. プロキシのウェブメールとファイル共有のカテゴリをブロックします。

F. 。企業ネットワーク上にある場合にのみアクセスできるオンプレミスのファイル共有サービスをインストールします。

G. すべてのスタッフをクラウドベースのプロキシサービスに移行します。

H. sfelTPおよびHTTPS / HTTPコンテンツをスキャンするDLPソリューションを展開します。

Answer(s): D,E,H

---

16. 資産管理ライフサイクルの一環として、企業は、認定された機器廃棄ベンダーと連携して、使用されなくなった企業資産を適切にリサイクルおよび破壊します。ベンダーのデューデリジェ

ンスの一環として、ベンダーから入手するのに最も重要なものは次のうちどれですか？

A. 認証要件への準拠を示すために使用される手順のコピー。

B. ベンダーが保持している現在の監査レポートと認証のコピー。

C. ベンダーの情報セキュリティポリシーのコピー。

D. 企業システムに含まれるすべてのデータをカバーする署名付きNDA。

Answer(s): D

---

17. セキュリティ管理者が、特権アクセスアカウントを持つ雇用者に定期的な検査と特定の職務遂行データの見直しを求めるようにするという新しい方針の執行を主張しています。 次のポリシーのどれにセキュリティ管理者が最も言及している可能性がありますか？

A. Mandatory vacation

B. Separation of duties

C. Background investigation

D. Least privilege

Answer(s): A

---

18. 企業は、多要素認証の使用を強制することにより、特定のWebベースのアプリケーションを保護しようとしています。 現在、企業はアプリケーションのサインインページを変更して余分なフィールドを含めることはできません。

A. 企業内のすべてのWebベースのアプリケーションにShibbolethを展開する

B. より複雑なパスワードと頻繁な変更を強制する

C. マルチファクター認証をサポートするSSOアプリケーションを使用する

D. WebアプリケーションがLDAP統合をサポートできるようにする

Answer(s): A

---

19. 頻繁なリリースサイクル中にセキュリティ慣行が維持されるように、セキュリティエンジニアがアジャイル開発チームに組み込まれたばかりです。新しいWebアプリケーションには、入力フォームが含まれています。セキュリティエンジニアがアプリケーションがエラー状態をどのように処理するかをテストできるようにするために、次のうちどれが最も効果的ですか？

A. コードの実行時分析を実行します

B. 静的コード分析の実行

C. フォームのファジング可能な入力

D. フォーム送信時に動的分析を実行する

Answer(s): D

---

20. コーポレートエグゼクティブのアンは、先進的で十分な資金を調達した手段を通じて競合他社が企業秘密を取得しようとする試みを増やす最近のターゲットになっています。 アンは、旅行中にホテルの部屋で頻繁にラップトップを無人で物理的に安全な状態のままにします。 セキュリティエンジニアは、ユーザートレーニングの必要性を最小限に抑えるAnnの実用的なソリューションを見つける必要があります。 このシナリオのベストソリューションは次のうちどれですか？

A. Two-factor authentication

B. An eFuse-based solution

C. Full disk encryption

D. Biometric authentication

Answer(s): C
