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

1. ある企業は、データベースに保存されているデータを隠すソリューションを探しています。ソリューションは次の要件を満たす必要があります。

A. マスキング

B. ランダム置換

C. アルゴリズム

D. トークン化

Answer(s): A

---

2. 会社 A が会社 B を買収しました。初期評価中に、両社は同じ SSO システムを使用していることがわかりました。ユーザーの移行を支援するために、会社 A は次のことを要求しています。

A. 新しいグループ ポリシー オブジェクト ポリシーをインストールしています

B. 会社Bから会社Aへの一方向の信頼を確立する

C. 多要素認証を有効にする

D. 属性ベースのアクセス制御の実装

E. 会社 A の Kerberos システムを会社 B のネットワークにインストールする

F. ログインスクリプトの更新

Answer(s): B,D

3. フォレンジック対応でステガナリシス技術を使用する利点は次のうちどれですか?

A. 安全な音声通信で使用される対称暗号の解読

B. DRM 保護されたメディアに対する固有の攻撃の頻度の決定

C. 取得した証拠の保管の連鎖の維持

D. .wav ファイル内のデータの最下位ビット エンコーディングの識別

Answer(s): D

---

4. 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(s): D

---

5. 開発者は次のコード スニペットを実装します。

A. SQL インジェクション

B. バッファオーバーフロー

C. セッション制限がありません

D. 情報漏洩

Answer(s): A

6. ある企業は、識別属性を追加せずに、独自の文書内に秘密裏に所有権のサインを埋め込むプロセスを使用したいと考えています。ドキュメントの著作権保護をサポートするプロセスの一部として使用するのに最適なものは次のうちどれですか?

A. ステガノグラフィー

B. 電子署名

C. 透かし

D. 暗号化

Answer(s): A

---

7. LOT デバイスは、SoC 内に組み込まれた暗号化モジュールを実装しており、非対称秘密キーは SoC ハードウェアのライトワンスリードメニー部分で定義されています。 秘密キーが侵害された場合、LOT 製造業者は次のうちどれを行うべきですか?

A. 無線アップデートを使用して秘密キーを置き換えます

B. 再設計された SoC を備えた新しい LoT デバイスを製造します。

C. サーバー上の IoT キーの公開部分を置き換えます

D. SoC ソフトウェアのパッチをリリースします。

Answer(s): B

---

8. 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。

A. 偽陰性。

B. 偽陽性。

C. 真陽性。

D. 真陰性。

Answer(s): B

---

9. ある企業が新製品に関連する規制要件を検討した結果、経営陣が生産中止を決定しました。このシナリオで企業が採用しているリスク戦略は次のどれですか。

A. 回避

B. 軽減

C. 拒否

D. 承認

Answer(s): A

---

10. 企業のネットワーク上のホストが、SMB 経由で拡散していると思われるワームに感染しました。セキュリティ アナリストは、インシデントを封じ込めると同時に、その後の調査とマルウェア分析のための証拠を維持する任務を負っています。

A. すべてのネットワーク接続を削除して、感染したホストをネットワークから隔離します。

B. 感染したホストをすぐにオフにします。

C. ホストの smb.conf ファイルを変更して、発信 SMB 接続を防止します。

D. 感染したホストで完全なマルウェア対策スキャンを実行します。

Answer(s): A

---

11. モバイル管理者は、次のモバイル デバイスの DHCP ログを確認して、適切なモバイル設定が管理対象デバイスに適用されていることを確認しています。

A. サービスセット識別子認証

B. ワイヤレスネットワーク自動参加

C. 802.1X 相互認証あり

D. アソシエーション MAC アドレスのランダム化

Answer(s): B

---

12. CIRT メンバーの Ann は、数百の仮想サーバーと数千のエンドポイントとユーザーで構成されるネットワーク上でインシデント対応活動を行っています。ネットワークは、1 秒あたり 10,000 を超えるログ メッセージを生成します。企業は大規模な Web ベースの暗号通貨スタートアップに属しており、Ann は関連情報を要約して、経営陣向けの簡単に消化できるレポートを作成しました。ただし、事件の原因となった侵入の証拠を収集する必要があります。アンが必要な情報を収集するために使用する必要があるのは、次のうちどれですか?

A. トラフィック インターセプターのログ分析

B. プルーフ・オブ・ワーク分析

C. 台帳分析ソフト

D. ログの削減と可視化ツール

Answer(s): D

---

13. システム管理者は、組織内の一連の情報システムに対して脆弱性スキャンを実行する準備をしています。システム管理者は、対象となるシステムが、特に構成設定に関して正確な情報を生成することを確認したいと考えています。

A. 資格情報を持たない受動的なスキャン

B. アクティブな認証済みスキャン

C. パッシブな認証済みスキャン

D. アクティブな認証されていないスキャン

Answer(s): B

---

14. 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(s): C

---

15. 会社の財務部門は、システム上の暗号化されていないファイルにデータをエクスポートする新しい支払いシステムを取得しました。同社は、適切な担当者のみがアクセスできるように、ファイルに制御を実装しました。この状況で部門が使用したリスク手法は次のうちどれですか?

A. 軽減

B. 避ける

C. 転送

D. 受け入れる

Answer(s): A

---

16. 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. 事業継続計画

B. 事後報告

C. 教訓

D. 根本原因分析

Answer(s): D

---

17. 保管過程が壊れた場合に何が起こるかを最もよく説明しているものは次のうちどれですか?

A. 追跡レコードの詳細が適切にラベル付けされていません。

B. 重要な証拠は認められないとみなされる可能性があります。

C. 証拠は法廷に提出されません。

D. 証拠を再収集する必要があります。

Answer(s): B

---

18. 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(s): A

---

19. セキュリティ アナリストは、悪意のあるコードが Linux システムにダウンロードされたことを懸念しています。いくつかの調査の後、アナリストは、疑わしいコード部分がディスク ドラ

イブ上で大量の入出力 (I/O) を実行していることを突き止めました。

A. 65

B. 77

C. 83

D. 87

Answer(s): D

---

20. 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(s): B
