Comptia Security+ Certification Exam (SY0-601 - Japanese Version)

1. 企業は、Web アクセスを制限し、従業員がアクセスする Web サイトを監視する機能を必要としています。これらの要件を最もよく満たすものは次のうちどれですか?

A. インターネットプロキシ

B. VPN

C. WAF

D. ファイアウォール

Answer(s): A

---

2. 次のセキュリティ設計機能のうち、開発チームがデータ セットのコピーの削除を分析できるのはどれですか?

A. コンティニュアス

B. バージョン管理

C. ストアド プロシージャ

D. コードの再利用

Answer(s): B

---

3. 従業員は、会社の最高経営責任者を名乗る未知の番号からテキスト メッセージを受信し、数枚のギフト カードを購入するよう求められます。これは次のタイプの攻撃のうちどれを表しますか?

A. プリテキスティング

B. スミッシング

C. ビッシング

D. フィッシング

Answer(s): B

---

4. 次のうち、インターネットボットによって常にスキャンされ、デフォルト構成の場合に攻撃のリスクが最も高いのはどれですか?

A. ウェアラブルセンサー

B. ラズベリーパイ

C. 監視システム

D. リアルタイム オペレーティング システム

Answer(s): C

---

5. RADIUS サーバーのインストールによって達成されるセキュリティ概念は次のうちどれですか?

A. PEM

B. ACL

C. AAA

D. CIA

Answer(s): C

---

6. 攻撃者は企業を標的にしています。攻撃者は、会社の従業員が特定の Web サイトに頻繁にアクセスしていることに気付きました。攻撃者は Web サイトをマルウェアに感染させることを決定し、従業員のデバイスも感染することを望んでいます。攻撃者が使用している手法は次のうちどれですか?

A. 水飲み場攻撃

B. 口実

C. タイポスクワッティング

D. なりすまし

Answer(s): A

---

7. セキュリティ チームは、最近の電力消費の過負荷の原因は、ネットワーク ラック内の空の電源コンセントの不正使用であると疑っています。利用可能なコンセントの数を損なうことなく、この問題を軽減する次のオプションはどれですか?

A. ラック専用 UPS の新規追加

B. 管理対象 PDU の取り付け

C. 二電源ユニットのみ使用

D. 発電機容量の増加

Answer(s): B

---

8. 次の認証方法のうち、安全性が最も低いと見なされるのはどれですか?

A. TOTP

B. SMS

C. HOTP

D. トークンキー

Answer(s): B

---

9. 次のうち、潜在的な脆弱性に対処するために定期的に更新する必要があるネットワーク ハードウェア上のソフトウェアを説明しているものはどれですか?

A. ベンダー管理

B. アプリケーション プログラミング インターフェイス

C. 消失

D. 暗号強度

E. ファームウェア

Answer(s): E

---

10. セキュリティ アナリストが次のログを調査しています。

A. アカウントの偽造

B. ハッシュを渡す

C. ブルートフォース

D. パスワードのスプレー

Answer(s): D

---

11. LOT デバイスを使用して自動化を実装する場合、ネットワークの安全性を保つために最初に考慮すべきものは次のうちどれですか?

A. Z-Wave 互換性

B. ネットワーク範囲

C. Zigbee 構成

D. 通信プロトコル

Answer(s): D

---

12. 管理者は、展開前にサーバーの強化を実行する必要があります。管理者は次のどの手順を実行する必要がありますか? (2 つ選択してください)。

A. サーバーを企業ドメインに参加させます。

B. 不要なサービスを削除します。

C. デフォルトのパスワードを文書化します。

D. デフォルトのアカウントを無効にします。

E. サーバーを資産インベントリに追加します。

F. サーバー ログを SIEM に送信します。

Answer(s): B,D

---

13. セキュリティ アナリストは、企業インフラストラクチャに対する大規模な攻撃で最近利用されたコンピュータ上の次のシステム コマンド履歴を調査しています。

A. ユーザーがどのレベルの権限を持っているかを決定するユーザー

B. 地上に存在しないバイナリを利用する試み

C. 定期的なメンテナンスを実行するシステム管理者

D. ローカル ユーザーによる権限昇格攻撃の成功

Answer(s): D

14. ネットワーク チームは、サポートが終了した重要なサーバーを、特定のデバイスのみがアクセスでき、境界ネットワークからはアクセスできない VLAN にセグメント化しました。次のテストのうち、チームが実装したコントロールを説明しているものはどれですか? (2 つ選択してください)。

A. 物理的

B. 技術的

C. 管理職

D. 補償中

E. 刑事

F. 修正

G. 抑止力

Answer(s): B,D

---

15. 組織のクラウド導入戦略を検討する際、最高情報セキュリティ責任者は、ファームウェア、オペレーティング システム、およびアプリケーションのパッチ適用を、選択したクラウド ベンダーにアウトソースするという目標を設定します。

A. プライベート クラウド

B. コミュニティ クラウド

C. IaaS

D. PaaS

E. コンテナ化

F. SaaS

Answer(s): F

---

16. インシデント対応の一環として根本原因分析を実施する必要がある理由を説明しているものは次のうちどれですか?

A. どのシステムが影響を受けているかを検出するため

B. 調査のために場所を収集するため

C. ネットワーク上のマルウェアの痕跡を消去するため

D. 今後の同じ性質のインシデントを防ぐため

Answer(s): D

---

17. 動的アプリケーション脆弱性スキャンにより、Web フォームを使用してコード インジェクションが実行される可能性があることが特定されました。この脆弱性を防ぐための最善の修復方法は次のうちどれですか?

A. 入力検証を実装する

B. MFA をデプロイする

C. WAFを活用する

D. HIPS の構成

Answer(s): A

---

18. ネットワーク セキュリティ マネージャーは、制御されたスクリプト化された方法でインシデントに対するセキュリティ チームの準備状況をテストする定期的なイベントを実装したいと考えています。次の概念のうち、このシナリオを説明しているものはどれですか?

A. 赤組演習

B. 事業継続計画のテスト

C. 卓上運動

D. ファンクショナルエクササイズ

Answer(s): C

---

19. セキュリティ管理者は、敵の行動に関する現実世界のナレッジ ベースを参照することで、企業システムを強化し、適切な緩和策を適用しています。管理者が参照するのに最適なのは次のうちどれですか?

A. CVSS

B. 急上昇

C. マイター攻撃&CK

D. CSIRT

Answer(s): C

---

20. 企業は、重要なサービスをサポートするためにレガシー ソフトウェアを引き続き使用する必要があります。次のうち、この行為のリスクを最もよく説明しているのはどれですか?

A. デフォルトのシステム構成

B. 安全でないプロトコル

C. ベンダー サポートの欠如

D. 弱い暗号化

Answer(s): C
