CompTIA.CS0-002.v2024-06-27.q394

試験コード:	CS0-002
試験名称:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
認定資格:	CompTIA
無料問題数:	394
バージョン:	v2024-06-27
アクセス数:	1149
ページビュー数:	3940
https://www.jpnpdf.com/CompTIA.CS0-002.v2024-06-27.q394-mondaishu.html	

最新問題: **1**
脆弱性スキャナーにより、サーバー上で実行されているサポート対象外のデータベース ソフトウェア バージョンが特定されました。ソフトウェアのアップデートが完了するまでに 6 ～ 9 か月かかります。経営陣はソフトウェアベンダーと1年間の延長サポート契約を結ぶことに同意した。このシナリオにおけるリスクへの対応を最も適切に説明しているのは次のうちどれですか?
A. 延長サポートにより、ソフトウェアに関連するリスクが軽減されます。
B. 延長サポート契約により、この脆弱性の発見は誤検知に変更されます。
C. 会社は脆弱性のリスクをソフトウェア ベンダーに移転しています。
D. 会社は脆弱性の固有のリスクを受け入れています。
Answer: D (メーッセージを残す)
リスクの受け入れ
o リスクが組織のリスク内にあると判断することを伴うリスク対応
食欲はあり、継続的なモニタリング以外の対策は必要ありません。
* 緩和
* コントロール
*回避
* 計画の変更
* 転移
* 保険
※受付
* リスクが低い

最新問題: **2**
ある組織が環境内で、製造プロセス中に物理的に変更されたと思われるマザーボードを発見しました。この再発のリスクを軽減するための最善の行動は次のうちどれですか?
A. ファームウェアの評価を実行して、悪意のある変更がないか確認します。
B. IT 部門と協力して、デバイスを既知の改変されたマザーボードと交換します。

C. サプライ チェーンの評価を調整して、ハードウェアの信頼性を確認します。
D. 取引調査を実施して、追加のリスクがさらなる行動を構成するかどうかを判断します。
Answer: (解答を表示する**)**

最新問題**: 3**
ある企業は最近、複数の地理的地域にわたる顧客に影響を与える機密情報の侵害を経験しました。侵害通知の要件を決定するのに最も適しているのは次の役割のうちどれですか?
A. 法執行機関
B. 最高セキュリティ責任者
C. 人事
D. 法律顧問
Answer: (解答を表示する**)**

最新問題**: 4**
セキュリティ アナリストは、生データを関連付け、ランク付けし、強化して、人間または機械が解釈して結論を引き出し、実用的な推奨事項を作成するレポートを作成しています。セキュリティ アナリストは、インテリジェンス サイクルの次のどのステップを実行していますか?
A. データ収集
B. 分析と生成
C. 計画と方向性
D. 普及と評価
E. 処理と悪用
Answer: (解答を表示する**)**

最新問題**: 5**
セキュリティ アナリストは、脅威、脆弱性、および修復策を明確に特定しました。アナリストは是正管理を導入する準備ができています。修正の適用を最も阻害するものは次のうちどれですか?
A. ファイアウォールの再起動が必要です。
B. すべての管理者パスワードをリセットします。
C. ビジネス プロセスの中断。
D. デスクトップの完全バックアップ。
Answer: D (メーッセージを残す**)**

最新問題**: 6**
ある組織は、その独自データがインターネット上で販売されているのが発見された後、侵害の可能性について警告を受けました。アナリストは、この侵害の証拠を見つけるために、次世代 UTM からのログを調査しています。次の出力があるとします。
調査の焦点は次のうちどれですか?
A. webserver.org-dmz.org
B. sftp.org-dmz.org
C. 83hht23.org-int.org
D. ftps.bluemed.net

Answer: A (メーッセージを残す)

最新問題: **7**
ある最高経営責任者 (CEO) は、このリスクを軽減するための新しいプライバシー規制の結果、同社がデータ主権の問題にさらされるのではないかと懸念している。最高情報セキュリティ責任者 (CISO) は、適切な技術的管理を実装したいと考えています。要件を満たすのは次のうちどれですか?
A. データマスキング手順
B. 強化された暗号化機能
C. 通常のビジネス影響分析機能
D. 地理的アクセス要件
Answer: D (メーッセージを残す)
説明
データ主権とは、データが収集および処理される地理的場所の法律および規制にデータが従うことを意味します。データ主権は、データがその発信元の管轄区域内に留まらなければならないという国固有の要件です。データ主権の核心は、機密の個人データを保護し、データが所有者の管理下にあることを保証することです。それを心配するのは、複数の場所にいる場合だけです。。https://www.virtru.com/blog/gdpr-data-sovereignty-matters-globally

最新問題: **8**
ユーザーが Web ページにアクセスしようとすると、ユーザーのコンピュータの動作が遅くなります。セキュリティ アナリストはコマンド ラインから netstat -aon コマンドを実行し、次の出力を受け取ります。
次の行のうち、コンピュータが侵害されている可能性があることを示しているのはどれですか?
A. 5 行目
B. 1 行目
C. 6 行目
D. 3 行目
E. 2 行目
F. 4 行目
Answer: F (メーッセージを残す)

最新問題: **9**
セキュリティ アナリストは、従業員のアカウントが侵害されたことを示す情報をサードパーティのインテリジェンス共有リソースから受け取りました。
問題に対処するために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. すべての従業員のアクセス許可を監査して、最小限の権限を確保します。
B. 影響を受ける従業員のパスワードを強制的にリセットし、トークンをすべて取り消します。
C. パスワードがローカル ネットワークの外に流出しないように SSO を構成します。
D. 監査が確実に有効になるように特権アクセス管理を設定します。
Answer: (解答を表示する)
説明/参照:

最新問題: **10**
企業の最高情報セキュリティ責任者 (CISO) は、従業員が無許可の Web サイトにアクセスすることを禁止するインターネット使用ポリシーを公開しました。IT 部門は、ビジネス ニーズに使用される Web サイトをホワイトリストに登録しました。CISO は、セキュリティを向上させ、従業員の士気をサポートするソリューションをセキュ

リティ アナリストに推奨してもらいたいと考えています。次のセキュリティ推奨事項のうち、従業員がビジネスに関係のない Web サイトを閲覧できるものはどれですか?
A. 新しい安全なブラウザを開発します。
B. 個人ビジネス VLAN を構成します。
C. 仮想マシンの代替を実装します。
D. 建物全体にキオスクを設置します。
Answer: B (メーッセージを残す**)**

最新問題**: 11**
ある企業の IDP/DLP ソリューションが次のアラートをトリガーしました。
セキュリティ アナリストが最初に調査すべきアラートは次のうちどれですか?
A. D
B. A
C. B
D. E
E. C
Answer: A (メーッセージを残す**)**

最新問題**: 12**
セキュリティ アナリストは、次のログに基づいてセキュリティ チームがアクションを実行する必要があると判断しました。
システムのセキュリティ体制を改善するには、次のうちどれを使用する必要がありますか?
A. パスワードの複雑さの要件を増やします。
B. ファイアウォールをアップグレードします。
C. ログイン試行の失敗回数を制限します。
D. ログイン アカウントの監査を有効にします。
Answer: C (メーッセージを残す**)**

最新問題**: 13**
Windows を仮想マシンのホスト OS として使用する場合の脆弱性は次のうちどれですか?
A. Windows では頻繁にパッチを適用する必要があります。
B. Windows 仮想化環境は通常、不安定です。
C. Windows は 「ping of death」に対して脆弱です。
D. Windows が動作するには、何百もの開いたファイアウォール ポートが必要です。
Answer: C (メーッセージを残す**)**

最新問題**: 14**
ホットスポットの質問
環境内のサーバーにマルウェアが存在する可能性があります。アナリストには、環境内のサーバーからコマンドの出力が提供され、サーバーの 1 つで実行されているどのプロセスがマルウェアである可能性があるかを判断するために、すべての出力ファイルを確認する必要があります。サーバー 1、2、4 はクリック可能です。マルウェアをホストするサーバーを選択し、このマルウェアをホストするプロセスを選択します。

説明書：
シミュレーションの初期状態に戻したい場合は、[リセット] ボタンを選択してください。シミュレーションが完了したら、[完了] ボタンを選択して送信してください。シミュレーションが送信されたら、 次へ」ボタンを選択して続行してください。

Answer:

最新問題: **15**
サイバーセキュリティ アナリストが Web サーバー上の Apache ログを確認しているところ、一部のログが欠落していることに気づきました。アナリストは、システム管理者が誤っていくつかのログ ファイルを削除したことを特定しました。このインシデントの再発を防ぐために、次のアクションまたはルールを実装する必要があるのはどれですか?
A. 職務の分離
B. 人材トレーニング
C. バックアップサーバー
D. 強制休暇
Answer: C (メーッセージを残す**)**

最新問題: **16**
セキュリティ アナリストは、従業員が組織を退職するときに機密性の高い SaaS ベースのシステムのアカウントが適時に削除されていないことを発見しました。問題を最善に解決するには、組織は次の実装を行う必要があります。
A. ロールベースのアクセス制御。
B. アカウントの手動レビュー
C. 多要素認証。
D. フェデレーション認証
Answer: D (メーッセージを残す**)**

最新問題: **17**
アナリストは、脆弱性スキャンの次のコード出力をレビューしています。
これは次のタイプの脆弱性のうちどれを表す可能性が最も高いですか?
A. 安全でない直接オブジェクト参照の脆弱性
B. HTTP 応答分割の脆弱性
C. XSS の脆弱性
D. 資格情報バイパスの脆弱性
Answer: D (メーッセージを残す**)**

最新問題: **18**

ある企業が複数の大量 DoS 攻撃の被害を受けています。問題のあるトラフィックのパケット分析により、次のことがわかります。
上記の攻撃に対して最も効果的な緩和手法は次のうちどれですか?
A. 企業は、ゲートウェイ NIPS の DoS リソース枯渇保護機能を有効にする必要があります。
B. 企業は、ネットワークベースのシンクホールを実装して、次からのすべてのトラフィックをドロップする必要があります。
ゲートウェイ ルーターでは 192.168.1.1。
C. 企業は、ゲートウェイ ファイアウォールに次の ACL を実装する必要があります:DENY IP HOST
192.168.1.1 170.43.30.0/24。
D. 企業は上流の ISP に連絡し、RFC1918 トラフィックをドロップするように依頼する必要があります。
Answer: (解答を表示する**)**

最新問題**: 19**
セキュリティ アナリストは、侵害されたマシンのフォレンジック分析中に、異常な動作を示しているいくつかのバイナリを発見しました。文字列を抽出した後、アナリストは予期しないコンテンツを発見します。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. 承認リストにあるバイナリのみの実行を許可します。
B. バイナリに対してウイルス対策プログラムを実行して、マルウェアをチェックします。
C. ファイル整合性モニタリングを使用してデジタル署名を検証します
D. 信頼できるソースからのバイナリのハッシュを検証します。
Answer: D (メーッセージを残す**)**
異常な動作を示しているバイナリを発見し、その文字列内に予期しないコンテンツが見つかった後に、アナリストが行うべき次のステップは、信頼できるソースからのバイナリのハッシュを検証することです。ハッシュは、ファイルまたはメッセージの内容を一意に表す固定長の値です。侵害されたマシン上のバイナリのハッシュと、ソフトウェア ベンダーやリポジトリなどの信頼できるソースからの元のバイナリまたは正規のバイナリのハッシュを比較することで、分析者は、バイナリが変更されているか、悪意のあるコードによって置き換えられているかどうかを判断できます。ハッシュが一致しない場合は、バイナリが改ざんされており、マルウェアが含まれている可能性があることを示します。

最新問題**: 20**
小規模な組織には、社内で使用される独自のソフトウェアがあります。システムはメンテナンスされていないため、残りの部分や環境を更新できません。最良の解決策は次のうちどれですか?
A. ID アクセスのための特権アクセス管理を実装します。
B. システムを仮想化し、物理マシンを廃止します。
C. 特定のシステムに MFA を実装します。
D. ネットワークから削除し、エアギャップが必要です。
Answer: (解答を表示する**)**

最新問題**: 21**
サービス プロバイダーとパブリック クラウドの関係を結ぶ際のロギングと監視の仕組みを最もよく説明しているものは次のうちどれですか?
A. パブリック クラウド環境ではロギングとモニタリングは必要ありません
B. ロギングとモニタリングはデータ所有者によって行われます。
C. ロギングとモニタリングの義務は SLA と契約で指定されています
D. ロギングとモニタリングはサービス プロバイダーによって行われます。
Answer: D (メーッセージを残す**)**

クラウド ソリューションに移行すると、組織は、特に PaaS または SaaS ソリューションを利用している場合、テクノロジー スタック上の特定のポイントが見えなくなる可能性があります。スタックの一部を保護する責任はサービスプロバイダーにあるため、良くも悪くも組織が監視機能を失うことを意味する場合があります。チャップマン、ブレント。マイミ、フェルナンド。CompTIA CySA+ サイバーセキュリティ アナリスト認定資格オールインワン試験ガイド、第 2 版 (試験 CS0-002) (p. 158)。マグロウヒルLLC. キンドル版。

最新問題: **22**
ある組織は、その独自データがインターネット上で販売されているのが発見された後、侵害の可能性について警告を受けました。アナリストは、この侵害の証拠を見つけるために、次世代 UTM からのログを調査しています。次の出力があるとします。
調査の焦点は次のうちどれですか?
A. ftps.bluemed.net
B. sftp.org-dmz.org
C. 83hht23.org-int.org
D. webserver.org-dmz.org
Answer: D (メーッセージを残す**)**

最新問題: **23**
組織には次のポリシーがあります。
*サービスは標準ポートで実行する必要があります。
※不要なサービスは無効化する必要があります。
組織には次のサーバーがあります。
*192.168.10.1 - ウェブサーバー
*192.168.10.2 - データベースサーバー
セキュリティ アナリストはサーバー上でスキャンを実行し、次の出力を確認します。
アナリストは次のどのアクションをとるべきですか?
A. 192.168.10.1 で HTTPS を無効にします。
B. 192.168.10.1 で IIS を無効にします。
C. 192.168.10.2 で DNS を無効にします。
D. 192.168.10.2 で MSSQL を無効にします。
E. 両方のサーバーで SSH を無効にします。
Answer: (解答を表示する**)**
SSH は Secure Shell の略で、サーバーのリモート アクセスと管理を可能にするプロトコルです。組織にサービスを標準ポートで実行し、不要なサービスを無効にする必要があるというポリシーがある場合、SSH は Web サーバーやデータベース サーバーの標準ポートではないポート 22 で実行されるため、両方のサーバーで無効にする必要があります。これらのサーバーが適切に機能するためには必要ありません。192.168.10.1 で HTTPS を無効にする、192.168.10.1 で IIS を無効にする、192.168.10.1 で DNS を無効にする、または 192.168.10.2 で MSSQL を無効にすることは、Web サーバーまたはデータベース サーバーの機能に影響を及ぼし、次の規則に違反するため、適切なアクションではありません。標準ポートでサービスを実行するという組織のポリシー。参考 :https://www.ssh.com/ssh/port

最新問題: **24**
Fagan コード検査中に、どのプロセスが計画段階にリダイレクトできますか?
A. やり直し
B. 概要

C. 会議
D. 準備
Answer: A (メーッセージを残す**)**

最新問題**: 25**
システムの操作権限 (ATO) は 4 日後に期限切れになるように設定されています。他の活動と限られた人員のため、この組織はこれまで再認証活動の開始を怠ってきました。サイバーセキュリティ グループは脆弱性スキャンを実行し、以下に示す結果の一部を取得しました。
シナリオと脆弱性スキャンの出力に基づいて、セキュリティ チームはこの発見に対して次のどれを行う必要がありますか?
A. これは重大度が 高」であるため、現時点ではこのリスクを受け入れてください。ただし、テストには利用可能な 4 日以上の時間が必要であり、システム ATO と競合する必要があります。
B. サーバーを再起動して、HTTP 検証が有効になっていることを確認します。
C. 無視します。これは誤検知であり、組織は他の発見に注力する必要があります。
D. Web 構成ファイルに移動し、HTTP 検証を強制する設定を検索し、正しい設定に手動で更新することで修復します。
Answer: D (メーッセージを残す**)**

最新問題**: 26**
ヘルプ デスクの技術者が、会社の CRM n の認証情報を平文で従業員の個人電子メール アカウントに誤って送信してしまいました。その後、技術者は適切なプロセスと従業員の会社メールを使用して従業員のアカウントをリセットし、セキュリティ チームにインシデントを通知しました。インシデント対応手順に従って、セキュリティ チームが次に行うべきことは次のうちどれですか?
A. CRM ベンダーに問い合わせてください。
B. インシデント概要レポートを作成します。
C. 事後データの相関関係を実行します。
D. インシデント対応計画を更新します。
Answer: (解答を表示する**)**
セキュリティ チームは、ヘルプ デスク技術者からインシデントの通知を受け取った後、次に事後データの関連付けを実行する必要があります。事後データ相関関係は、さまざまなソース (ログ、アラート、レポートなど) からのデータを分析して、根本原因、影響、侵害の兆候 (IoC)、学んだ教訓、インシデント後の改善の推奨事項を特定するアクティビティです3。事後データの関連付けは、セキュリティ チームが次のことを行うのに役立ちます。
インシデントがどのように発生し、どのように検出および解決されたかを特定する インシデントの範囲と重大度、および機密性、整合性、可用性への影響を評価する インシデントの一因となったセキュリティ制御またはプロセスのギャップや弱点を特定する アクションプランまたは修復を作成する再発防止または将来のインシデントを軽減するための戦略

最新問題**: 27**
新しいベンダーのオンボーディング プロセス中に、セキュリティ アナリストはベンダーの最新の侵入テストの概要のコピーを入手します。
実行者: Vendor Red Team 最終実行日: 14 日前
アナリストは次のどれを最初に行うべきですか?
A. より最近の侵入テストを実行します。
B. ベンダーのオンボーディングを続行します。
C. 調査結果に関する詳細を開示します。
D. 中立的な第三者に侵入テストを実行してもらいます。

Answer: C (メーッセージを残す)
アナリストは、ベンダーの最新の侵入テストの概要の結果に関する詳細を最初の推奨事項として開示する必要があります。これは、ベンダーのセキュリティ体制を評価し、組織に影響を与える可能性のある潜在的なリスクや問題を特定するのに役立ちます。アナリストは調査結果を確認し、侵入テストの範囲、方法論、修復アクション、さらに調査結果を裏付ける証拠やアーティファクトに関する詳細情報を求める必要があります。

最新問題: **28**
会社のソフトウェアの脆弱性を除去するソフトウェア パッチがリリースされました。
セキュリティ アナリストは、ソフトウェアをテストして、脆弱性が修正され、アプリケーションが引き続き適切に機能していることを確認する任務を負っています。
次に実行すべきテストは次のうちどれですか?
A. 侵入テスト
B. ユーザー受け入れテスト
C. 回帰テスト
D. ファジング
Answer: C (メーッセージを残す)

最新問題: **29**
セキュリティ アナリストは、ユーザーがクリックした後にマルウェアをダウンロードしたことによってマルウェア感染が引き起こされたのではないかと疑っています。
エラー！ハイパーリンク参照が無効です。フィッシングメールで。
他のコンピュータが同じマルウェアのバリエーションに感染するのを防ぐために、アナリストは にルールを作成する必要があります。
A. <malwaresource> へのすべての接続をブロックするプロキシ。
B. 添付された実行可能ファイルを自動的に削除する電子メール サーバー。
C. ダイナミック DNS ホストへの接続試行をブロックするファイアウォール。
D. マルウェア サンプルと一致する IDS。
Answer: A (メーッセージを残す)

最新問題: **30**
ある組織は、その独自データがインターネット上で販売されているのが発見された後、侵害の可能性について警告を受けました。アナリストは、この侵害の証拠を見つけるために、次世代 UTM からのログを調査しています。次の出力があるとします。
調査の焦点は次のうちどれですか?
A. webserver.org-dmz.org
B. 83hht23.org-int.org
C. sftp.org-dmz.org
D. ftps.bluemed.net
Answer: (解答を表示する)

最新問題: **31**
セキュリティ アナリストは、次のインターネット使用傾向レポートを検討しています。
セキュリティ アナリストがさらに調査する必要があるユーザー名は次のうちどれですか?
A. ユーザー 2
B. ユーザー 1

C. ユーザー 4
D. ユーザー 3
Answer: (解答を表示する**)**

最新問題: **32**
サービス プロバイダーとパブリック クラウドの関係を結ぶ際のロギングと監視の仕組みを最もよく説明しているものは次のうちどれですか?
A. パブリック クラウド環境ではロギングとモニタリングは必要ありません
B. ロギングとモニタリングはデータ所有者によって行われます。
C. ロギングとモニタリングの義務は SLA と契約で指定されています
D. ロギングとモニタリングはサービス プロバイダーによって行われます。
Answer: D (メーッセージを残す**)**
説明
クラウド ソリューションに移行すると、組織は、特に PaaS または SaaS ソリューションを利用している場合、テクノロジー スタック上の特定のポイントが見えなくなる可能性があります。スタックの一部を保護する責任はサービスプロバイダーにあるため、良くも悪くも組織が監視機能を失うことを意味する場合があります。チャップマン、ブレント。マイミ、フェルナンド。CompTIA CySA+ サイバーセキュリティ アナリスト認定資格オールインワン試験ガイド、第 2 版 (試験 CS0-002) (p. 158)。マグロウヒルLLC. キンドル版。

最新問題: **33**
サイバーセキュリティ アナリストは複数の脅威フィードにアクセスでき、それらを整理しながら、同時にネットワーク トラフィックに対するインテリジェンスを比較したいと考えています。
この目標を最もよく達成できるのは次のうちどれですか?
A. 情報の共有と分析
B. 自動化とオーケストレーション
C. 継続的な統合と展開
D. 静的および動的分析
Answer: D (メーッセージを残す**)**

最新問題: **34**
次の一連の属性のうち、セキュリティの観点から内部関係者の脅威の特徴を最もよく表しているものはどれですか?
A. 無許可、意図的、悪意のある
B. 承認済み、意図的ではない、無害
C. 無許可、意図的ではない、害のないもの
D. 認可済み、意図的、悪意のある
Answer: D (メーッセージを残す**)**

最新問題: **35**
従業員がインターネットで調査を行っていたとき、サイバー犯罪者からのメッセージが画面に表示され、ハードドライブがランサムウェアの亜種によって暗号化されたばかりであると述べられました。アナリストは次のことを観察しています。
ウイルス対策シグネチャが最近更新されました
デスクトップの背景が変更されました
Web プロキシ ログには、さまざまな情報セキュリティ サイトの閲覧と広告ネットワーク トラフィックが記録されます。
ファイルサーバー上で大量のハードディスクアクティビティが発生しています
SMTP サーバーは、従業員がブロックされた送信者から最近いくつかの電子メールを受信したことを示しました
同社は最近ウェブホスティングプロバイダーを切り替えました
外部ポート スキャンに関する IPS アラートがいくつかあります
従業員がこのタイプのランサムウェアを入手した経緯を説明しているものは次のうちどれですか?
A. 従業員がウイルス対策シグネチャを更新しました
B. 従業員は別のユーザーの資格情報を使用していました
C. 従業員が電子メールの添付ファイルを開いた
D. 従業員が CSRF 攻撃の被害に遭いました
Answer: (解答を表示する**)**

最新問題: **36**
あるセキュリティ アナリストは、会社の電子メール システムのセキュリティを向上させて、企業幹部になりすました電子メールを軽減する方法を研究しています。この目的を達成するためにアナリストが構成するのに最適なのは次のうちどれですか?
A. SPF のネームサーバー上の TXT レコード
B. レプリケーションを保護するための DNSSEC キー
C. ドメイン キーが識別されました Man
D. 受信した Mad をチェックするためのサンドボックス
Answer: C (メッセージを残す**)**
Domain Keys Identified Mail (DKIM) は、デジタル署名を使用して、メッセージがドメインの所有者によって送信され承認されたことを電子メールの受信者に知らせる電子メール認証方法です1。DKIM は、他のドメインになりすましたり、なりすましたりするフィッシング電子メールを防ぐのに役立ちます。送信者の身元と完全性を検証します。DKIM は、各送信電子メール メッセージに DKIM 署名ヘッダーを追加することで機能します。このヘッダーには、メッセージの選択された部分のハッシュ値と送信者のドメイン名が含まれます。送信者のドメインは、DNS レコード内の公開キーも公開します。受信者はこの公開キーを使用して、DKIM 署名を復号し、メッセージの独自のハッシュ値と比較できます。それらが一致する場合、メッセージが転送中に変更されておらず、要求されたドメインから送信されたことを意味します。

最新問題: **37**
セキュリティのすべての領域に適切な制御が行われていることを確認することが、組織が以下を使用する主な理由です。
A. フレームワーク。
B. 取締役および役員。
C. インシデント対応計画。
D. エンジニアリングの厳密さ。
Answer: A (メッセージを残す**)**

セキュリティのすべての領域に適切な制御が行われていることを確認することが、組織がフレームワークを使用する主な理由です。フレームワークは、組織がセキュリティ体制を評価し、運用に必要なセキュリティ対策を実装するための組織的な構造を提供します。NIST、COBIT、ISO 27001 などのフレームワークは、組織のセキュリティ ポリシー、管理、手順を開発、実装、監視する方法に関するガイダンスを提供します。さらに、フレームワークは、組織がセキュリティ体制を測定し、継続的な改善に向けたロードマップを作成するためのベンチマークを提供します。

最新問題: **38**
組織は多数のリモート ユーザーをサポートしています。リモート ユーザーのラップトップ上のデータを保護するための最良のオプションは次のうちどれですか?
A. VPN の使用が必要です。
B. 従業員に NDA への署名を要求します。
C. DLP ソリューションを実装します。
D. ディスク全体の暗号化を使用します。
Answer: D (メーッセージを残す**)**
ディスク全体の暗号化を使用することは、リモート ユーザーのラップトップ上のデータを保護するための最良のオプションです。ディスク全体の暗号化は、オペレーティング システム、アプリケーション、ファイルなど、ハードディスク ドライブ上のすべてのデータを暗号化する技術です。ディスク全体の暗号化により、ラップトップの紛失、盗難、または侵害があった場合でも、データへの不正アクセスを防ぐことができます。ディスク全体の暗号化により、ハードディスクを取り外して別のデバイスに接続するなどの物理的な攻撃からデータを保護することもできます。

最新問題: **39**
出力エンコードを使用することで防止できる攻撃は次のうちどれですか?
A. クロスサイト スクリプティング
B. SQL インジェクション
C. ディレクトリ トラバーサル
D. コマンドインジェクション
E. サーバー側のリクエストフォージェリ
F. クロスサイト リクエスト フォージェリ
Answer: A (メーッセージを残す**)**

最新問題: **40**
悪意のある外部スキャンの可能性を検出した後、内部脆弱性スキャンが実行され、古いバージョンの JBoss を使用する重要なサーバーが見つかりました。実行中のレガシー アプリケーションは、そのバージョンの JBoss に依存します。サーバーの侵害とビジネスの中断を同時に防ぐために、最初に実行すべきアクションは次のうちどれですか?
A. サーバーのバックアップを作成し、そのサーバー上で実行されている JBoss サーバーを更新します。
B. レガシー アプリケーションのベンダーに連絡し、更新バージョンをリクエストします。
C. 古いコンポーネント用に適切な DMZ を作成し、JBoss サーバーを分離します。
D. 新しいプラットフォームを使用してサーバー上に視覚化を適用し、レガシー アプリケーションの JBoss サービスを外部サービスとして提供します。
Answer: C (メーッセージを残す**)**
説明
その申請は何のためにあるのでしょうか？ DMZ は、Web サーバーや電子メール サーバーなど、外部からの接続を受信するシステムを収容するために設計された特別なネットワーク ゾーンです。健全なファイアウォール設計により、これらのシステムは隔離されたネットワーク上に配置され、侵害された場合でも、システムに対する

脅威はほとんどありません。」内部ネットワークは、DMZ と内部ネットワーク間の接続は引き続きファイアウォールを通過する必要があり、そのセキュリティ ポリシーの影響を受けるためです。」

最新問題: **41**
攻撃ベクトルを理解し、インテリジェンス ソースを統合することは、以下の重要な要素です。
A. インシデント対応計画。
B. 脆弱性管理計画。
C. リスク管理コンプライアンス。
D. プロアクティブな脅威ハンティング
Answer: C (メーッセージを残す**)**

最新問題: **42**
組織の最高情報セキュリティ責任者 (CISO) は、部門リーダーに、さまざまなサイバーセキュリティ インシデントのトリガーに対応して実行できるコミュニケーション プランについて調整するよう依頼しました。これらのコミュニケーション プランを作成する利点は次のうちどれですか?
A. 有害な情報が組織外に不用意に漏洩することを防ぐのに役立ちます。
B. 回復フェーズの早い段階でヘルプ デスク担当者と連携することで、ワームの蔓延を制限できます。
C. 復旧フェーズ中に組織の上級幹部にパッチ適用のステータスを常に知らせるのに役立ちます。
D. 侵害が検出され次第、広報チームにすぐにメディアとの調整を開始するよう通知できます。
Answer: (解答を表示する**)**

最新問題: **43**
プロアクティブな脅威ハンティング手法として、ハンターは、入手可能な脅威インテリジェンス情報から得られる可能性のある攻撃シナリオに基づいて状況ケースを作成する必要があります。シナリオの基礎を形成した後、脅威ハンターは脅威評価のフレームワークを確立するために次のどれを構築できますか?
A. 攻撃プロファイル
B. 仮説
C. 脅威ベクトル
D. 重要な資産リスト
Answer: D (メーッセージを残す**)**

最新問題: **44**
エンタープライズ ヘルプ デスク システムへようこそ。エスカレーションされたチケットをデスクのチケットキューで処理してください。
説明書
 チケット」をクリックしてチケットの詳細を表示します 追加コンテンツはチケット内のタブで利用できます
まず、ドロップダウン メニューから適切な問題を選択します。次に、2 番目のドロップダウン メニューから最も可能性の高い根本原因を選択します。
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: **45**

アナリストは、SOC によって報告された異常なイベントを調査しています。システム ログを確認した後、アナリストは、エンドポイント上で root レベルの権限を持つユーザーが予期せず追加されていることを特定します。次のデータ ソースのうち、アナリストがこのイベントがインシデントに該当するかどうかを判断するのに最も役立つものはどれですか?

A. 変更リクエスト
B. パッチ適用ログ
C. バックアップログ
D. 脅威フィード
E. データ分類行列
Answer: A (メーッセージを残す**)**

最新問題**: 46**
一部の顧客がアカウントでの不正なアクティビティを報告しているため、セキュリティ アナリストは会社の API サーバーからのネットワーク パケット キャプチャを調査しています。キャプチャ ファイルの一部を以下に示します。

POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.s/soap/envelope/"><s:Body><GetIPLoc ation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.o rg/2001/XMLSchema-instance"></s:Body></ s:Envelope> 192.168.1.22 - - api.somesite.com 200 0 1006 1001 0 192.168.1.22 POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"
/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com</a:Username></request></Login></s:Body></s:E
nvelope> 192.168.5.66 - - api.somesite.com 200 0 11558 1712 2024
192.168.4.89
POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body
><GetIPLocation+xmlns="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></requ est></GetIPLocation></s:Body></s:Envelope> 192.168 .1.22 - - api.somesite.com 200 0 1003 1011 307 192.168.1.22 POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body
><IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+ xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><a:認証>
<a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:Imp ersonateUserId>0</a:ImpersonateUserId><a:LocationId>161222</a:LocationId>
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId
>13026046</a:UserId></a:Authentication></request></IsLoggedIn></s:Body>
</s:Envelope> 192.168.5.66 - - api.somesite.com 200 0 1378 1209 48
192.168.4.89

クライアントのアカウントがどのように侵害されたかを説明する可能性が最も高いのは次のうちどれですか?

A. SQL インジェクション攻撃がサーバー上で実行されました。
B. クライアントのユーザー名とパスワードはクリアテキストで送信されました。
C. クライアントの認証トークンが偽装されて再生されました。

D. XSS スクリプト攻撃がサーバー上で実行されました。
Answer: C (メーッセージを残す**)**

最新問題: **47**
SIEM アナリストは、次の URL を含むアラートを受け取ります。
この攻撃を最もよく説明しているのは次のうちどれですか?
A. パスワードのスプレー
B. バッファオーバーフロー
C. ディレクトリ トラバーサル
D. 安全でないオブジェクト アクセス
Answer: C (メーッセージを残す**)**

最新問題: **48**
セキュリティ アナリストは不審なトラフィックを発見し、ホストが既知の悪意のある Web サイトに接続していると判断しました。アナリストがとるべき最も適切なアクションは、次の変更リクエストを実装することです。
A. ドメインの IPS 署名を作成します
B. ドメインをブラックリストに追加します
C. ウイルス対策ソフトウェアを更新します
D. ドメインへのトラフィックをブロックするようにファイアウォールを構成します
Answer: D (メーッセージを残す**)**

最新問題: **49**
ある大企業のコンプライアンス責任者が、同社のベンダー管理プログラムをレビューしましたが、サードパーティのリスクやハードウェア ソースの信頼性を評価するための管理が定義されていないことがわかりました。コンプライアンス担当者は、サードパーティによる管理の実施に関して、定期的にある程度の保証を獲得したいと考えています。
コンプライアンス担当者が定義した目標を最もよく満たすものは次のうちどれですか?
(2つお選びください。)
A. 重要なデータを第三者と共有する前に NDA を締結する
B. 組織のリスク評価を四半期ごとに維持およびレビューする
C. サードパーティの監査レポートを年次ベースで要求する
D. 組織のセキュリティ管理に対するベンダー コンプライアンス評価の実行
E. エンドポイント レベルと境界レベルの両方で DLP 機能を利用する
F. すべての重要なサービス プロバイダーのビジネス影響評価を完了する
Answer: D,F (メーッセージを残す**)**

最新問題: **50**
データ流出は、従業員が機密ファイルを誤って外部の受信者に電子メールで送信したときに発生しました。
次の制御のうち、このインシデントを防ぐ可能性が最も高いのはどれですか?
A. SSO
B. DLP
C. WAF
D. VDI
Answer: B (メーッセージを残す**)**
説明/参照: https://greenlightcorp.com/blog/cyber-security-solutions-data-spillage-and-how-to-create-an-after- Incident-to-do-list/

最新問題: **51**
データ流出は、従業員が機密ファイルを誤って外部の受信者に電子メールで送信したときに発生しました。
次の制御のうち、このインシデントを防ぐ可能性が最も高いのはどれですか?
A. VDI
B. DLP
C. SSO
D. WAF
Answer: B (メーッセージを残す**)**

最新問題: **52**
セキュリティ アナリストは、ホストがネットワーク上でアクティブかどうかを判断しようとしています。アナリストはまず次のことを試みます。
次にアナリストは次のコマンドを実行します。
結果の違いを説明できるのは次のうちどれですか?
A. ICMP はファイアウォールによってブロックされています。
B. hping3 が誤検知を返しています。
C. 元の ping コマンドを実行するには root 権限が必要でした。
D. ping と hping3 のルーティング テーブルが異なりました。
Answer: (解答を表示する**)**

最新問題: **53**
アナリストは、プロセッサとメモリの消費量が多い PC のトラブルシューティングを行っています。
調査の結果、システム上で次のプロセスが実行されていることが判明しました。
lsass.exe
csrss.exe
ワードパッド.exe
メモ帳.exe
不正なプロセスを特定するためにアナリストが利用すべきツールは次のうちどれですか?
A. Nessus を使用します。
B. grep を使用して検索します。

C. ping 127.0.0.1。
D. Netstat を使用します。
Answer: D (メーッセージを残す)

最新問題: **54**
セキュリティ アナリストは、ネットワークが侵害された場合に潜在的な攻撃者が最初に悪用する可能性のある脆弱性を特定したいと考えています。最良の結果が得られるのは次のうちどれですか?
A. 外部侵入テスト
B. ネットワーク ping スイープ
C. ベースライン構成の評価
D. 認証されていないスキャン
Answer: D (メーッセージを残す)

最新問題: **55**
アジャイル スプリント プロセスを使用すると、前の図のステップ 2 でどのステップが発生しますか?
A. デザイン
B. テスト中
C. 開発
D. ユーザー ストーリーの収集
Answer: C (メーッセージを残す)

最新問題: **56**
データ主権法に基づいてデータに課される規制を決定する要因は次のどれですか?
A. 会社が所在する国のデータ法
B. 会社が保存するデータの種類
C. 会社のデータ セキュリティ ポリシー
D. 企業が所有するデータをどのように扱うつもりか
Answer: A (メーッセージを残す)

最新問題: **57**
セキュリティ アナリストは、240 台のデバイスがあるネットワーク上で毎週脆弱性スキャンを実行し、2,450 ページのレポートを受け取ります。誤検知の数を減らす可能性が最も高いのは次のうちどれですか?
A. 手動検証
B. 侵入テスト
C. 既知の環境評価
D. 資格情報付きスキャン
Answer: D (メーッセージを残す)
資格情報スキャンは、有効なユーザー資格情報を使用してターゲット システムにアクセスし、セキュリティ体制のより徹底的かつ正確な評価を実行する脆弱性スキャンの方法です。資格情報付きスキャンは、スキャナーが構成ファイル、レジストリ キー、インストールされているソフトウェア、パッチ、アクセス許可など、システム上のより多くの情報とリソースにアクセスできるようにすることで、誤検知の数を減らすのに役立ちます。

最新問題: **58**
セキュリティ アナリストがマルウェア分析ラボを構築しています。アナリストは、悪意のあるアプリケーションが仮想マシンを脱出して他のネットワークに移行できないようにしたいと考えています。
このリスクを最大限に軽減するには、アナリストは _____ を使用する必要があります。
A. ラボ ネットワークを他のすべてのネットワークから分離するファイアウォール。
B. エアギャップを作成するための 802.11ac ワイヤレス ブリッジ。
C. 環境を相互にセグメント化するためのアンマネージド スイッチ。
D. ラボを別の VLAN にセグメント化するためのマネージド スイッチ。
Answer: D (メーッセージを残す**)**

最新問題: **59**
アナリストは、会社の Web サーバーからの次のログを確認しています。
これは次のどれに該当しますか?
A. オンラインハイブリッド攻撃
B. オフライン辞書攻撃
C. オフライン総当たり攻撃
D. オンライン レインボー テーブル攻撃
Answer: C (メーッセージを残す**)**

最新問題: **60**
企業は、業界の規制に準拠するために、すべての資産のベースラインに対する不正な変更を監視する必要があります。リモート ユニットのうち 2 つは、資産に対してスキャンを実行した後も回復しませんでした。アナリストは再発を防ぐための解決策を推奨する必要があります。同様の資産の可用性に影響を与えず、持続不可能なプロセスを生み出すことなく、規制要件を満たす最善の方法は次のうちどれですか?
A. 毎日ベースラインを手動で確認し、結果を変更履歴ログに文書化します。
B. リスク軽減の取り組みを実証するために、補償コントロールを備えた例外を文書化します。
C. 監視要件を満たし、チームをトレーニングするために新しいスキャン テクノロジを実装します。
D. スキャン要件をサポートする能力が実証されている他のベンダーから新しいリモート ユニットを購入します。
Answer: (解答を表示する**)**
A) 毎日ベースラインを手動で確認し、結果が正しくないことを変更履歴ログに記録します。このオプションは、スキャンの実行後にリモート ユニットが回復しなかった根本原因に対処するものではないため、問題の再発を防ぐことはできません。さらに、このオプションでは、すべての資産のベースラインを毎日手動で確認して文書化するには多大な時間とリソースが必要になるため、持続不可能なプロセスが作成されます。
C) 監視要件を満たし、チームをトレーニングするために新しいスキャン技術を実装するのは正しくありません。新しいスキャン技術によってリモート ユニットやその他の資産にも問題が発生する可能性があるため、このオプションは問題が再発しないことを保証するものではありません。さらに、このオプションでは、新しいスキャン テクノロジの取得、導入、保守、およびその使用方法に関するチームのトレーニングに追加のコストと労力が発生します。
D) スキャン要件をサポートする能力が実証されている他のベンダーから新しいリモート ユニットを購入することは正しくありません。このオプションは、すべてのリモート ユニットを異なるベンダーの新しいものと交換する必要があるため、実現可能ではなく、費用対効果も高くありません。このオプションでは、互換性、相互運用性、ベンダー ロックインなどの新たなリスクや課題も生じる可能性があります。
Explanation:

正解は B です。リスク軽減の取り組みを実証するために、補償コントロールを備えた例外を文書化します。補償制御は、主要な制御または必須の制御が実行不可能または効果的でない場合に実装される代替または追加の制御です。補償制御は、文書化され正当化されている限り、リスクを許容レベルまで低減し、規制要件を満たすのに役立ちます1。

最新問題: **61**
API の不正使用を防ぐための最良の方法は次のどれですか?
A. ジオフェンシング
B. HTTPS
C. 認証
D. レート制限
Answer: C (メーッセージを残す**)**

最新問題: **62**
セキュリティ アナリストがシステム侵害を調査しています。アナリストは、侵害時にシステムの OS パッチが最新のものであったことを確認します。悪用された可能性が最も高い脆弱性の種類は次のうちどれですか?
A. 高度な持続的脅威
B. 内部関係者の脅威
C. ゼロデイ
D. バッファオーバーフロー
Answer: C (メーッセージを残す**)**

最新問題: **63**
ホストが意図せずネットワークにスパム送信を行っています。この状況に対処するには、次の制御タイプのうちどれを使用する必要がありますか?
A. 動作中
B. 修正
C. 技術的
D. 管理職
Answer: (解答を表示する**)**

最新問題: **64**
重要なサーバーがマルウェアによって侵害され、すべての機能が失われました。このサーバーのバックアップが作成されました。しかし、管理者はルートキットによって論理爆弾が注入された可能性があると考えています。機能を迅速に復元するには、セキュリティ アナリストが実行する必要があるのは次のうちどれですか?
A. 以前のバックアップを復元し、ライブ ブートマルウェア対策スキャナーでスキャンします。
B. 逆方向に作業し、サーバーがクリーンになるまで各バックアップを復元します

C. 重要なデータを新しいサーバーにオフロードし、運用を継続します。
D. 新しいサーバーを立ち上げ、重要なデータをバックアップから復元します
Answer: (解答を表示する**)**

最新問題: **65**
広範囲に分散した店舗と IP スペースを持つ小売企業は、脆弱性スキャンに関する PCI 要件を満たす必要があります。同組織はコスト削減のため、この機能を第三者に委託する予定だ。
スキャンの実行に関連する期待を伝えるために使用すべきものは次のうちどれですか?
A. 脆弱性評価レポート
B. 教訓ドキュメント
C. SLA
D. 覚書
Answer: (解答を表示する**)**

最新問題: **66**
最高情報セキュリティ責任者 (CISO) は、請負業者で構成される開発チームに関心を持っています。
顧客データへのアクセスが多すぎる A. 開発者は個人用ワークステーションを使用しているため、会社は開発活動をほとんど、またはまったく把握できません。
CISO の懸念を軽減するには、次のうちどれを実装するのが最善でしょうか?
A. NDA
B. DLP
C. 暗号化
D. テストデータ
Answer: A (メーッセージを残す**)**

最新問題: **67**
インシデント対応者は、後のフォレンジック分析のためにモバイル デバイスからアプリケーション バイナリを取得することに成功しました。
アナリストが次に行うべきことは次のうちどれですか?
A. 各バイナリを逆コンパイルしてソース コードを取得します。
B. 各バイナリの SHA-256 ハッシュを計算します。
C. 各アプリケーション内の権限マニフェストを検査します。
D. 認証された AES-256 動作モードを使用してバイナリを暗号化します。
E. 影響を受けるモバイル デバイスを出荷時設定にリセットします。
Answer: B (メーッセージを残す**)**

最新問題: **68**
ある企業が脅威ハンティング チームを設立したいと考えています。インテリジェンスを狩猟作戦に統合する理論的根拠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. チームが会社の環境内で重点分野と戦術に優先順位を付けることができます。
B. 主要なエンタープライズ サーバーおよびサービスの重要性分析を提供します。
C. インシデント中およびインシデント後の迅速な対応と回復をサポートします。

D. アナリストは、新たに発見されたソフトウェアの脆弱性に関する定期的な更新を受け取ることができます。
Answer: (解答を表示する**)**

最新問題: **69**
ある大手ソフトウェア会社は、ソース管理および展開パイプラインをクラウド コンピューティング環境に移行したいと考えています。ビジネスの性質上、管理者は復旧時間の目標を 1 時間以内にする必要があると判断します。次の戦略のうち、企業が望ましい回復時間を達成するために最も有利な立場に立つのはどれですか?
A. 災害時のフェイルオーバーに使用できる複製コピーをオンプレミスで作成します。
B. 同じリージョンに重複環境を構成し、両方のインスタンス間の負荷分散を行います。
C. 複製されたコピーと自動スケーリングをオンにして、すべてのクラウド コンポーネントをセットアップします。
D. 他のリージョンへのアクティブなレプリケーションを備えた代替サイトを確立します。
Answer: (解答を表示する**)**

最新問題: **70**
もともと同じように構成されていた 3 台の運用サーバーのスイートは、同じ脆弱性スキャンを受けました。しかし、最近の結果では、3 つのサーバーにそれぞれ異なる重大な脆弱性があることが明らかになりました。サーバーにはインターネットからアクセスできず、AV プログラムはマルウェアを検出していません。サーバーの syslog ファイルは、オフサイトのデータセンターに設置され物理的に隔離されているため、異常なトラフィックを示していません。ランダムな実行可能ファイルのチェックサム テストでは改ざんは検出されません。次のシナリオのうち、最も可能性が高いのはどれですか?
A. サーバーは最新の脆弱性シグネチャでスキャンされていません
B. 以前のパッチ管理イベント中にサーバーはさまざまなレベルの注目を受けました
C. サーバーがゼロデイ脆弱性を使用して部外者によって攻撃されました
D. サーバーは異なるメーカーによって製造されています
Answer: (解答を表示する**)**

最新問題: **71**
あなたは、A 社のサーバーからのスキャン データを解釈する任務を負ったサイバーセキュリティ アナリストです。すべてのサーバーの要件が満たされていることを確認し、満たされていないことが判明した場合は変更を推奨する必要があります。
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。
* TLS 1.2 は、実行されている TLS の唯一のバージョンです。
※Apache 2.4.18以降を使用してください。
* デフォルトのポートのみを使用する必要があります。
説明書
提供されたデータを使用して、サーバーごとに企業のガイドラインの遵守状況を記録します。
質問には 2 つの部分が含まれています。パート 1 とパート 2 を必ず完了してください。提供された強化ガイドラインのみに基づいて問題に対する推奨事項を作成してください。
Answer:
以下の説明を参照してください。
説明
パート 1 答え:
次の点を確認してください。

AppServ1 は TLS.1.2 のみを使用しています
AppServ4 は TLS.1.2 のみを使用しています
AppServ1 は Apache 2.4.18 以降を使用しています
AppServ3 は Apache 2.4.18 以降を使用しています
AppServ4 は Apache 2.4.18 以降を使用しています
パート 2 の答え:
おすすめ：
AppServ2 および AppServ3 で TLS v1.1 を無効にすることをお勧めします。また、AppServ2 Apache を現在のバージョン 2.3.48 からバージョン 2.4.48 にアップグレードします。

最新問題: **72**
ある企業は、社内データセンターでホストされている Web サーバーの使用から、コンテナ化されたクラウド プラットフォームへの移行を進めています。アナリストは、コンテナ化された環境における侵害の兆候を特定するように依頼されました。実行中のコンテナが侵害されたことを最も適切に示すものは次のうちどれですか?
A. 承認されたソフトウェア イメージのコンテナが応答を停止しました
B. 承認されたソフトウェア イメージのコンテナがドリフトしました
C. 承認されたソフトウェア イメージのコンテナが起動に失敗します
D. 承認されたソフトウェア オーケストレーション コンテナが root 権限で実行されています
Answer: B (メーッセージを残す**)**

最新問題: **73**
セキュリティ アナリストは、以下にリストされているネットワーク セキュリティ監視ログを確認しています。
アナリストが最も注目している可能性が高いのは次のうちどれですか? (2 つ選択してください)。
A. 10.1.1.129 は悪意のないリクエストを送信しましたが、アラートは誤検知です。
B. 10.1.1.128 が悪意のあるリクエストを送信しました。アラートは誤検知です。
C. 10.1.1.128 は、潜在的な悪意のあるトラフィックを Web サーバーに送信しました。
D. 10.1.1 .129 は Web サーバーの脆弱性を悪用することに成功しました。
E. 10.1.1.129 は、潜在的な悪意のあるリクエストを Web サーバーに送信しました。
Answer: A,B (メーッセージを残す**)**

最新問題: **74**
開発チームは新しいアプリケーションのリリースをテストしています。チームは、精度と機能をテストするために、既存のクライアント PHI データ レコードを運用環境からテスト環境にインポートする必要があります。
チームがテストを実行できるようにしながら、このデータの機密性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. 暗号化
B. 匿名化
C. エンコーディング
D. 透かし
Answer: B (メーッセージを残す**)**

最新問題: **75**

脅威を与えるチームは、脅威アクターのプロフィールと活動を追跡する新しい LoC を ISAC から受け取りました。次に更新する必要があるのは次のうちどれですか?
A. ホワイトリスト
B. DNS
C. ブロックリスト
D. IDS 署名
Answer: D (メーッセージを残す**)**
IDS シグネチャは、脅威アクターのプロファイルとアクティビティを追跡する新しい IoC (侵害の痕跡) を ISAC (情報共有および分析センター) から受け取った後に更新する必要があります。IoC は、システムまたはネットワークが脅威アクターによって侵害または攻撃されたことを示唆する証拠または成果物です4。IoC は、IP アドレス、ドメイン名、URL、ファイル ハッシュ、電子メール アドレス、レジストリ キーなどです。ISAC は、脅威インテリジェンスを収集、分析し、特定の分野のメンバー間でベスト プラクティスを共有する非営利組織です。産業5. ISAC は、新たな脅威やインシデントに関するタイムリーな関連情報を提供することで、メンバーのセキュリティ意識と備えを向上させるのに役立ちます。

最新問題**: 76**
次の一連の属性のうち、セキュリティの観点から内部関係者の脅威の特徴を最もよく表しているものはどれですか?
A. 無許可、意図的ではない、良性
B. 無許可、意図的、悪意のある
C. 認可済み、意図的、悪意のある
D. 承認済み、意図的ではない、無害
Answer: C (メーッセージを残す**)**
解説 参考 : https://www.sciencedirect.com/topics/computer-science/insider-attach

最新問題**: 77**
組織では、外部受信者に送信される電子メールで問題が発生しています。組織への受信電子メールは正常に動作しています。セキュリティ アナリストは、ヘルプ デスクから次のスクリーンショットまたは電子メール エラーを受け取りました。
アナリストは電子メール サーバーをチェックし、ログに次のメッセージの多くを確認します。
エラー 550 - メッセージが拒否されました
問題の可能性が最も高いのは次のうちどれですか?
A. DKIM 秘密キーの有効期限が切れています
B. SPF が失敗しています。
C. DMARC キューがいっぱいです
D. ポート 25 が開いていません。
Answer: C (メーッセージを残す**)**

最新問題**: 78**

別の組織との合併の一環として、最高情報セキュリティ責任者 (CISO) は評価者と協力して、データ プライバシー コンプライアンスに焦点を当てたリスク評価を実行しています。CISO は主に、データ プライバシーに関連する潜在的な法的責任と罰金を懸念しています。CISO の懸念に基づいて、評価者はおそらく次の点に焦点を当てるでしょう。
A. 量的な大きさ。
B. 定性的な確率。
C. 定性的な大きさ。
D. 定量的な確率。
Answer: A (メーッセージを残す**)**

最新問題: **79**
セキュリティ アナリストは、ネットワーク上の特定のハードウェアに影響を与える組織内でのいくつかのインシデントを観察しました。さらに調査を進めると、機器ベンダーが以前にパッチをリリースしていたことが判明しました。
これらのインシデントに対する最も適切な脅威分類は次のうちどれですか?
A. 既知の脅威
B. 高度な持続的脅威
C. ゼロデイ
D. 未知の脅威
Answer: (解答を表示する**)**

最新問題: **80**
サイバー セキュリティ アナリストは、物理的な攻撃の可能性を防ぐために、既存のネットワーク アクセス層に新しいネットワーク構成を実装しています。適用され、展開段階で発生する問題が少ないソリューションを最もよく説明しているものは次のうちどれですか?
A. DHCP と動的 VLAN を使用してネットワーク アドレス保護を展開します。
B. スイッチのネットワーク ポートごとに 1 つの MAC アドレスを使用してポート セキュリティを実装します。
C. ネットワーク全体で 802.1X と EAPOL を構成します。
D. 分離のためにソフトウェア定義ネットワーキングとセキュリティ グループを実装します。
Answer: C (メーッセージを残す**)**

最新問題: **81**
脅威を与えるチームは、脅威アクターのプロフィールと活動を追跡する新しい LoC を ISAC から受け取りました。次に更新する必要があるのは次のうちどれですか?
A. DNS
B. ブロックリスト
C. ホワイトリスト
D. IDS 署名
Answer: (解答を表示する**)**

最新問題: **82**
ホットスポットの質問
セキュリティ アナリストは、さまざまな種類の脆弱性スキャンを実行します。脆弱性スキャンの結果を確認して、実行されたスキャンの種類を特定し、各デバイスで誤検知が発生したかどうかを判断する必要があります。

説明書：
結果が認証情報付きスキャン、認証情報なしスキャン、またはコンプライアンス スキャンのいずれから生成されたのかについて、ドロップ オプションを選択します。
認証情報付きスキャンと認証情報なしのスキャンのみについて、誤検知の結果を評価し、誤検知を示す結果を確認します。
注: 現在選択されているオプションのチェックを外したい場合は、そのオプションをもう一度クリックします。最後に、脆弱性スキャンの結果に基づいて、サーバーを結果にドラッグしてサーバーの種類を特定します。
Linux Web サーバー、ファイル プリント サーバー、およびディレクトリ サーバーはドラッグ可能です。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 [リセット] ボタンを選択してください。シミュレーションが完了したら、[完了] ボタンを選択して送信してください。シミュレーションが送信されたら、 次へ]ボタンを選択して続行してください。
Answer:

最新問題: **83**
認可された侵入テストのタイムラインと時間帯の境界を慎重に選択する背後にある理由を表すものは次のうちどれですか? (2 つ選択してください)。
A. テスト活動に必要な人員リソースをスケジュールするため
B. テストが運用に測定可能な影響を与えることを確認するため
C. チームのコミュニケーションと報告の頻度を決定するため
D. 発生する可能性のある実際の侵入との競合を回避するため
E. 運用への予期せぬ影響を軽減するため
Answer: A,E (メーッセージを残す)

最新問題: **84**
ある企業は、内部ネットワークに接続している未知のデバイスに気づき、企業が管理していないすべてのマシンをブロックするソリューションを実装したいと考えています。この目標を達成するには、次のソリューションのうちどれが最適ですか?
A. W1F1 ネットワークの WPA2
B. 802.1X 実装による NAC
C. 拡張可能な認証プロトコル
D. チャレンジ/レスポンスのある RADIUS
Answer: B (メーッセージを残す)
このソリューションは、企業管理以外のすべてのマシンが内部ネットワークに接続するのをブロックするという目標を達成するのに最適です。NAC はネットワーク アクセス コントロールの略で、ネットワーク デバイスの ID、役割、場所、その他の属性に基づいてポリシーとルールを強制する方法です。802.1X はポートベースのネットワーク アクセス制御の標準であり、ネットワーク ポートまたはワイヤレス アクセス ポイントへのアクセスを許可する前にデバイスを認証します。

最新問題: **85**
ある組織は、包括的なインシデント対応ポリシーを策定しました。経営陣は方針とそれに関連する手順を承認しました。インシデント対応手順に対する担当者の習熟度を評価するのに最も有益な活動は次のうちどれですか?
A. 全従業員による年次情報セキュリティ意識向上トレーニングの完了
B. サードパーティによる外部および内部の侵入テスト
C. コンピュータ セキュリティ インシデント対応チームによる教訓から得た文書の完成
D. インシデント対応チームが関与するシミュレートされた侵害シナリオ
E. 事業継続チームのメンバーが参加する机上活動
Answer: (解答を表示する)

最新問題: **86**
サイバーインシデント対応チームは、病院ネットワーク上のネットワーク侵入インシデントに対応しています。データを法廷で証拠として使用できるようにするためにチームが準備しなければならないものは次のうちどれですか?
A. コンピューターフォレンジックフォーム
B. インシデントフォーム
C. 加工管理フォーム
D. HIPAA 応答フォーム
Answer: D (メーッセージを残す**)**

最新問題: **87**
組織のポリシーでは、重大度 7 以上の脆弱性を 1 週間以内に修復することが求められています。
重大度が 7 未満のものは 30 日以内に修復する必要があります。また、組織はセキュリティ チームに対して、修復を実行する前に脆弱性の詳細を調査することも求めています。調査の結果、検出結果が誤検知であると判断された場合、修復は実行されず、今後のスキャンから誤検知を除外するように脆弱性スキャナー構成が更新されます。
組織には 3 つの Apache Web サーバーがあります。
最近の脆弱性スキャンの結果を以下に示します。
チームはいくつかの調査を実行し、Apache からの次の声明を発見しました。
セキュリティ チームが実行すべきアクションは次のうちどれですか?
A. 30 日以内に 192.168.1.22 を修復します
B. 192.168.1.22 での誤検知を無視します。
C. 30 日以内に 192.168.1.20 を修復します
D. 192.168.1.20 の偽陰性を調査します。
Answer: A (メーッセージを残す**)**

最新問題: **88**
secutily アナリストが WAF アラートを確認していると、次のリクエストが表示されます。
この攻撃を最もよく説明しているのは次のうちどれですか?
A. コマンドの実行
B. SQL インジェクション
C. サービス拒否
D. LDAP インジェクション
Answer: B (メーッセージを残す**)**

最新問題: **89**
サイバーセキュリティ アナリストは、成長を続ける組織に脅威ハンティングおよびインテリジェンス グループを設立しています。この目的で使用される可能性が最も高い共同リソースは次のうちどれですか?
A. ISAC
B. IoC フィード
C. スクラム

D. VSS スコア
Answer: B (メーッセージを残す**)**

最新問題**: 90**
セキュリティ アナリストは、電子メール セキュリティ サービスからの次のログを確認しています。
電子メールがブロックされた理由を最もよく説明しているものは次のうちどれですか?
A. IP アドレスとリモート サーバー名が同じです。
B. IP アドレスはブラックリストに登録されました。
C. 電子メールは www.spamfilter.org URL から送信されました。
D. To アドレスが無効です。
E. From アドレスが無効です。
Answer: A (メーッセージを残す**)**

最新問題**: 91**
ある組織は、Web サーバーを強化し、潜在的な攻撃者によって公開される可能性のある情報を削減しようとしています。セキュリティ アナリストは、最近の Web サーバー スキャンの脆弱性スキャン結果を検討しています。
スキャン結果の一部を以下に示します。
次の行のうち、修復する必要があるホストに関する情報の開示を示しているものはどれですか?
A. 応答: :\Documents\MarySmith\mailingList.pdf
B. 初めて検出 2015 年 11 月 10 日 09:00 GMT-0600
C. リクエスト: GET http://myOrg.com/mailingList.aspx?content=volunteer
D. アクセス パス: http://myOrg.com/mailingList.htm
E. 調査結果#5144322
Answer: A (メーッセージを残す**)**

最新問題**: 92**
機械学習をセキュリティ分析の自動化に効果的に適用するには、_____ が必要です。
A. 関連するトレーニング データ。
B. 異常なトラフィック シグネチャ。
C. 脅威フィード API。
D. マルチコア、マルチプロセッサ システム。
Answer: B (メーッセージを残す**)**

最新問題**: 93**

最近、ブートローダー マルウェアがいくつかの会社のワークステーションで発見されました。すべてのワークステーションは Windows を実行し、UEFI 機能を備えた最新モデルです。
次の UEFI 設定のうち、感染の原因として最も考えられるものはどれですか?
A. ネイティブ モード
B. 高速ブート モード
C. 互換モード
D. セキュア ブート モード
Answer: (解答を表示する**)**

最新問題: **94**
API の不正使用を防ぐための最良の方法は次のどれですか?
A. HTTPS
B. ジオフェンシング
C. レート制限
D. 認証
Answer: D (メーッセージを残す**)**
認証は、ユーザーが知っているもの (パスワードなど)、ユーザーが持っているもの (トークンなど)、またはユーザーであるもの (指紋など) など、何らかの証拠を要求することによってユーザーの身元を確認する方法です。認証は、正当なユーザーのみが API 関数またはデータにアクセスまたは使用できるようにするため、API の不正使用を防止するための最良の方法です。HTTPS、ジオフェンシング、レート制限なども API のセキュリティやパフォーマンスを強化できる方法ですが、API の不正使用を防ぐことはできません。参考: https://www.redhat.com/en/topics/api/what-is-api-security

最新問題: **95**
アナリストは Nmap を使用してホストの定期的なスキャンを実行し、次の出力を受け取ります。
アナリストが最初に調査すべきなのは次のうちどれですか?
A. ポート 22
B. ポート 23
C. ポート 21
D. ポート 80
Answer: (解答を表示する**)**

最新問題: **96**
ある企業は、脆弱性管理手順の導入を計画していると警告しました。ただし、セキュリティの成熟度は低いため、リスクの計算と優先順位付けの前に完了する必要がある前提条件がいくつかあります。
次のうちどれを最初に完了する必要がありますか?
A. システム評価
B. リスク特定プロセス
C. 危険因子の伝達
D. ビジネスへの影響分析
Answer: B (メーッセージを残す**)**

最新問題: **97**
Windows サーバー上で Massivelog ログが 40GB に増加しました このサイズでは、ローカル ツールはファイルを読み取ることができず、ファイルが配置されている仮想サーバーからファイルを移動することもできません。PowerShell スクリプトの次の行のうち、ユーザーがレビューのために loq の最後の 10,000 行を抽出できるようにするものはどれですか?
A. 末尾 -10000 Massivelog.log > extract.txt
B. 情報末尾 n -10000 Massivelog.log | 抽出.txt;
C. コンテンツ 「/Massivelog.log」を取得 -Last 10000 | 抽出.txt
D. get-content './Massivelog.log' -Last 10000 > extract.txt;
Answer: D (メーッセージを残す**)**
https://social.technet.microsoft.com/Forums/en-US/d7a84189-fa3f-4431-8b03-30a7d57d076a/getcontent-read-last-line-and-action?forum=winserverpowershell

最新問題: **98**
Linux サーバーを利用する会社に勤めているセキュリティ アナリストは、脆弱性スキャンから次の結果を受け取りました。
誤検知の可能性が最も高いのは次のうちどれですか?
A. サポートされていない Web サーバーの検出
B. \srvsvc による Windows SMB サービスの列挙
C. ICMP タイムスタンプ要求のリモート日付開示
D. 匿名 FTP が有効になっています
Answer: B (メーッセージを残す**)**

最新問題: **99**
ある企業のセキュリティ チームは最近、寿命を迎えた多数のワークステーションを発見しました。ワークステーションのベンダーは、製品がサポートされなくなり、パッチも入手できなくなったことをチームに通知しました。会社は、これらのワークステーションの使用を中止する準備ができていません。これらのワークステーションを脅威から保護するための最良の方法は次のうちどれですか?
A. 特定されたワークステーションにホワイトリストを展開して攻撃対象領域を制限します
B. システム プロセスの中心性を決定し、それを文書化します。
C. ワークステーションを分離し、可能な場合はエアギャップを設けます。
D. ワークステーションのセキュリティ監視を強化します。
Answer: A (メーッセージを残す**)**
特定されたワークステーションにホワイトリストを導入することは、これらのワークステーションを脅威から保護する最良の方法です。ホワイトリスト登録は、承認されたアプリケーション、プロセス、またはユーザーのみにシステムまたはリソースの実行またはアクセスを許可する手法です。ホワイトリストは、攻撃対象領域を制限し、マルウェアや不正なソフトウェアがシステム上で実行されるのを防ぐのに役立ちます3。サポートが終了したワークステーションにホワイトリストを導入すると、ベンダーからのパッチやサポートの欠如による悪用のリスクを軽減できます。

最新問題: **100**
セキュリティ アナリストは、ホストのリストで Web サーバーのバージョンを評価して、脆弱なバージョンのソフトウェアを実行しているホストを特定し、そのリストを Webserverlist という名前の XML ファイルに出力する必要があります。XML。ホスト リストは、werbserverlist,text という名前のファイルで提供されます。次の Nmap コマンドのうち、この目的を最もよく達成できるのはどれですか?
A)
B)

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

最新問題**: 101**
あなたは、会社のシステム強化ガイドラインをレビューしているペネトレーション テスターです。硬化ガイドラインは次のことを示しています。
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。
企業のインターネット プレゼンスは、保護されたサブネットに配置する必要があります
説明書 ：
利用可能なツールを使用して、企業ネットワーク上のデバイスと、それらのデバイス上で実行されているサービスを検出します。
決定する必要があります
各デバイスのIPアドレス
プライマリサーバーまたは各デバイスのサービス
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
Answer:
答えは画像の下にあります

最新問題**: 102**
一部の顧客がアカウントでの不正なアクティビティを報告しているため、セキュリティ アナリストは会社の API サーバーからのネットワーク パケット キャプチャを調査しています。キャプチャ ファイルの一部を以下に示します。
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/
"><s:Body><GetIPLocation+xmlns
<request+xmlns:a="http://schemas.somesite.org http://www.w3.org/2001/XMLSchema-instance
"></s:Body></s:Envelope> 192.168.1.22 - - api.somesite.com 200 0 1006 1001 0 192.168.1.22 POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com
192.168.5.66 - - api.somesite.com 200 0 11558 1712 2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body><
192.168.1.22 - - api.somesite.com 200 0 1003 1011 307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="

http://www.w3.org/2001/XMLSchema-instance"><a:Authentication>
<a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:ImpersonateUserId>0<
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authe
192.168.5.66 - - api.somesite.com 200 0 1378 1209 48 192.168.4.89
クライアントのアカウントがどのように侵害されたかを説明する可能性が最も高いのは次のうちどれですか?
A. SQL インジェクション攻撃がサーバー上で実行されました。
B. XSS スクリプト攻撃がサーバー上で実行されました。
C. クライアントの認証トークンが偽装されて再生されました。
D. クライアントのユーザー名とパスワードはクリアテキストで送信されました。
Answer: C (メーッセージを残す**)**

最新問題**: 103**
ヘルプ デスクは、新しい電子メール サーバーからの電子メールが送信されていないことにセキュリティ アナリストに気づきました。最近、新しい電子メール サーバーが既存の電子メール サーバーに追加されました。アナリストは、新しいサーバー上で次のコマンドを実行します。
出力を考慮して、セキュリティ アナリストは次のどれをチェックする必要がありますか?
A. DMARC ポリシー
B. 新しい電子メール サーバーの DNS 名
C. 新しい電子メール サーバーの IP アドレス
D. 使用されている SPF のバージョン
Answer: (解答を表示する**)**

最新問題**: 104**
SIEM に対する SOAR の利点は次のうちどれですか?
A. SOAR ははるかに安価です。
B. SOAR は、必要な人間の介入の量を減らします。
C. SOAR は多くのソースからデータを集約できます。
D. SOAR は、より堅牢な暗号化プロトコルを使用します。
Answer: (解答を表示する**)**
説明
SOAR システムとサービスは、ワークフロー管理のレイヤーを追加する傾向があります。つまり、SOAR デプロイメントは実際に SIEM アラートやその他のデータを取り込み、それらにワークフローや自動化を適用する可能性があります。SIEM ツールと SOAR ツールは相互に区別するのが難しい場合がありますが、現時点での違いの 1 つは、SOAR サービスが統合するツールの範囲が広いことです。SIEM 機能を提供する同じベンダーが、多くの場合、Splunk、Rapid7、IBM (QRadar) をすべて含む SOAR システムも提供しています。
ただし、ServiceNow のような ITSM ツールもこの分野で機能するため、違いがあります。アナリストは、SOAR のサービスとツールが存在し、これらを活用して従来の SIEM システムがこれまで処理してきたものを超える追加要素をカバーできることを知っておく必要があります。

最新問題**: 105**
セキュリティ管理者は、次の要件を満たす組織内の隔離されたラボ ネットワークへのパートナーからのアクセスを提供する必要があります。
※パートナーのPCは研究室のネットワークに直接接続しないでください。
* ラボネットワーク上でパートナーがアクセスする必要があるツールは、すべてのパートナーが利用できる必要があります

* パートナーは、ラボのネットワーク上で分析を実行できる必要があります。完了までに数時間かかる場合があります。次の機能のうち、リクエストのセキュリティ目標を最も満たす可能性が高いのはどれですか?
A. 分析に必要なツールを提供するために、研究室ネットワークへのアクセスと永続モードでの VDI の使用を可能にするジャンプ ボックスの展開
B. 研究室ネットワークへのアクセスを許可するファイアウォールの導入と、分析に必要なツールを提供するための非永続モードでの VDI の使用を許可します。
C. 研究室ネットワークへのアクセスと分析に必要なツールを提供する永続モードでの VDI の使用を許可するファイアウォールの導入
D. 分析に必要なツールを提供するために、ラボのネットワークへのアクセスと非永続モードでの VDI の使用を可能にするジャンプ ボックスの展開
Answer: D (メーッセージを残す)
ジャンプ ボックスは、2 つのネットワークに接続され、ネットワーク間のゲートウェイまたは仲介として機能するシステムです1。ジャンプ ボックスは、他のネットワークからのネットワークへの直接アクセスを制限することで、ネットワークを分離し、セキュリティを確保するのに役立ちます。ジャンプ ボックスは、ネットワーク上のトラフィックとアクティビティの監視と監査にも役立ちます。VDI (仮想デスクトップ インフラストラクチャ) は、サーバー上でホストされている仮想デスクトップにユーザーがアクセスできるようにするテクノロジです2。VDI は、ユーザーが自分の PC にインストールすることなく、分析に必要なツールやアプリケーションを提供するのに役立ちます。VDI は、デスクトップのメンテナンスと管理のコストを削減するのにも役立ちます。VDI は、永続モードと非永続モードの 2 つのモードで動作できます。永続モードでは、各ユーザーはセッション間で設定とデータを保持する専用の仮想デスクトップを持ちます。非永続モードでは、各ユーザーは一時的な仮想デスクトップを持ち、セッションごとに削除またはリセットされます3。このシナリオでは、ジャンプ ボックスを展開して研究室ネットワークへのアクセスを許可し、VDI を非永続モードで使用することで、要求のセキュリティ目標を満たすことができます。ジャンプ ボックスを使用すると、パートナーの PC が研究室のネットワークに直接接続するのを防ぎ、不正アクセスや侵害のリスクを軽減できます。非永続モードの VDI は、パートナーの PC や仮想デスクトップにデータを保存せずに、分析に必要なツールを提供できます。非永続モードの VDI を使用すると、パートナーは進行状況や結果を失うことなく長時間の分析を実行することもできます。ファイアウォール (B) の導入は、ルールに基づいてトラフィックをフィルタリングまたはブロックするだけであり、分析のためのアクセスやツールを提供しないため、十分または効果的ではない可能性があります。永続モードでは機密性の高いデータが仮想デスクトップに保存されるため、VDI を永続モード (A) で使用することは安全または効率的ではない可能性があります。

最新問題: **106**
コードをデプロイする前に脆弱なサードパーティ ライブラリを検出できるのは次のうちどれですか?
A. 静的解析
B. プロトコル分析
C. 影響分析
D. 動的分析
Answer: A (メーッセージを残す)

最新問題: **107**
企業のマーケティング電子メールがスパム フォルダーに見つかるか、まったく配信されません。セキュリティ アナリストは問題を調査し、問題の電子メールが会社に代わってサードパーティ in1marketingpartners.com によって送信されていることを発見しました。以下は既存の SPP ワードです。
電子メールがスパムとしてマークされたりブロックされたりするのを防ぐために、SPF レコードに対する次の更新のうち、最も効果的なのはどれですか?
A)

B)
C)
D)
A. オプション D
B. オプション C
C. オプション B
D. オプション A
Answer: (解答を表示する**)**

最新問題**: 108**
インシデント対応チームは、PII と PHI を含む複数のシステムの侵害に対応しています。外部団体へのインシデントの開示は、以下に基づく必要があります。
A. 応答者の裁量。
B. 広報ポリシー。
C. 通信計画。
D. 上級管理チームのガイダンス。
Answer: C (メーッセージを残す**)**
コミュニケーション計画は、インシデントに関する情報をいつ、どのように外部組織と共有するかを概説するため、インシデント対応の重要な部分です。
コミュニケーション計画は、緊急時またはセキュリティインシデント時に組織が外部エンティティとどのように通信するかを定義する一連の手順とプロトコルです。この計画では通常、インシデントに関する情報をいつどのように共有するかについて概要を示し、関連する利害関係者にインシデントがタイムリーに通知されるようにします。また、どのような情報を外部の関係者と共有するかを決定するためのガイドとしても機能します。参考までに、インシデント対応におけるコミュニケーション計画の重要性に関する CompTIA の Web サイトの記事へのリンクを示します: https://www.comptia.org/content/incident-response-communication-plan

最新問題**: 109**
インシデント中に、サイバーセキュリティ アナリストは、評判の悪い IP に関連するいくつかのエントリを Web サーバー ログで発見しました。アナリストがインシデントをさらに検討する原因となるのは次のうちどれですか?
A. BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=../../.ssh/id_rsa" 200 15036
B. BadReputationIp - - [2019-04-12 10:43Z] "GET /etc/passwd" 403 1023
C. BadReputationIp - - [2019-04-12 10:43Z] "GET /favicon.ico?src=../usr/share/ アイコン" 200 19064
D. BadReputationIp - - [2019-04-12 10:43Z] "GET /index.html?src=../.ssh/id_rsa" 401 17044
E. BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=/etc/passwd" 403 11056
Answer: C (メーッセージを残す**)**

最新問題**: 110**
アナリストは電子メールのヘッダーを調べて、電子メールが正当な送信者から送信されたかどうかを判断しています。組織は SPF を使用して電子メールの発信元を検証します。次のうち、無効な発信者を示す可能性が最も高いのはどれですか?
A. 受信 SPF: ニュートラル
B. 受信した SPF: なし
C. 受信した SPF ソフトフェイル
D. 受信した SPF: エラー
Answer: C (メーッセージを残す**)**

受信した SPF: ソフトフェイル。SPF は Sender Policy Framework の略で、送信者の IP アドレスを、DNS レコード内のドメイン所有者によって公開された承認された IP アドレスのリストと照合することにより、電子メールの送信元を検証する方法です。SPF は、送信者の信頼性を検証することにより、電子メールのなりすましやフィッシングを防ぐのに役立ちます1。
Received-SPF は、受信者のメール サーバーによって実行された SPF チェックの結果を示すヘッダー フィールドです。このフィールドにはいくつかの値が考えられますが、最も一般的な値は次のとおりです。
pass: 送信者の IP アドレスは、ドメインの承認された IP アドレスの 1 つと一致します。これは有効な発信者を示します。
失敗: 送信者の IP アドレスがドメインの承認された IP アドレスのいずれにも一致せず、ドメイン所有者はそのような電子メールを拒否する必要があると明示的に述べています。これは発信者が無効であることを示します。
中立: 送信者の IP アドレスはドメインの承認された IP アドレスのいずれにも一致しませんが、ドメイン所有者はそのような電子メールの処理方法を示していません。これは発信者が不明であることを示します。
none: ドメインに SPF レコードがないか、SPF レコードが無効か不正な形式です。これは、SPF ポリシーが欠落しているか無効であることを示しています。
Softfail: 送信者の IP アドレスは、ドメインの承認された IP アドレスのいずれにも一致しませんが、ドメイン所有者は、そのような電子メールは慎重に受け入れる必要があると述べています。これは、疑わしい発信者を示しています2。
したがって、4 つのオプションのうち、Received-SPF:softfail は、送信者がドメイン所有者によって承認されておらず、ドメインのなりすましまたはスプーフィングを試みている可能性があることを示唆しているため、無効な発信者を示している可能性が最も高くなります。
1: SPFとは何ですか? 2: SPF記録チェック

最新問題**: 111**
ある組織は、予算を満たし、人員要件を削減するために、インフラストラクチャをクラウドに移行しています。組織には、開発、テスト、運用という 3 つの環境があります。これらの環境には相互依存関係がありますが、相対的にセグメント化されたままにする必要があります。
次の方法のうち、会社のインフラストラクチャを保護するのに最適で、管理と保守が最も簡単なのはどれですか?
A. 環境ごとに 3 つの個別のクラウド アカウントを作成します。
アカウント ピアリングとセキュリティ ルールを構成して、各環境へのアクセスと各環境からのアクセスを許可します。
B. すべての環境に対して 1 つの VPC を持つ 1 つのクラウド アカウントを作成します。
仮想ファイアウォールを購入し、きめ細かいセキュリティ ルールを作成します。
C. 環境ごとに 1 つのクラウド アカウントと 3 つの個別の VPC を作成します。
各環境へのアクセスおよび各環境からのアクセスを許可するセキュリティ ルールを作成します。
D. 環境ごとに 3 つの個別のクラウド アカウントを作成し、ネットワーク サービス用に 1 つのコア アカウントを作成します。
すべてのトラフィックをコア アカウント経由でルーティングします。
Answer: (解答を表示する**)**

最新問題**: 112**
リスク評価中に、上級マネージャーは、特殊な出来事が重要なサービスの可用性に影響を与える場合のコストがいくらになるかを尋ねます。このサービスは組織に 1,000 ドルの収益をもたらします。攻撃の影響により、サーバーのジョブ実行能力の 20% が影響を受ける可能性があります。同組織は、年内に 20 件中 5 件の攻撃が成功すると予想しています。計算された単一損失の期待値は次のうちどれですか?
A. $200
B. $800
C. $5,000
D. 20,000 ドル

Answer: A (メーッセージを残す)
単一損失期待 (SLE) は、リスクの 1 回の発生に関連する金銭的損失の尺度です。SLE は、資産価値 (AV) に、リスクが発生した場合に資産が被る損失の割合であるエクスポージャー係数 (EF) を乗じることによって計算できます。この場合、資産価値はサービスによって生成された収益、つまり 1,000 ドルです。エクスポージャーファクターは、サーバーの容量に対する攻撃の影響であり、20% です。したがって、SLE は 1,000 ドル x 0.2 = 2001 ドルとなります。

最新問題: **113**
ゼロデイ暗号ワームは内部ネットワークのポート 25 を介して急速に拡散し、電子メール サーバー内で見つかったソフトウェアの脆弱性を悪用しています。ワームの蔓延を防ぐために、できるだけ早く実装する必要がある対策は次のうちどれですか?
A. 影響を受けるシステムにパッチを適用します。
B. 影響を受けるサーバーを隔離します。
C. トラフィック シンクホールを実装します。
D. すべての既知のポート/サービスをブロックします。
Answer: B (メーッセージを残す)

最新問題: **114**
サイバーセキュリティ アナリストがインシデントに対応しています。同社の経営陣は、このインシデントは攻撃グループによるものだと考えている。この状況に最もよく当てはまるのは次のモデルのうちどれですか?
A. 侵入分析のダイヤモンド モデル
B. キルチェーン
C. マイター攻撃&CK
D. インテリジェンス サイクル
Answer: A (メーッセージを残す)

最新問題: **115**
最高情報セキュリティ責任者 (CISO) は、請負業者で構成される開発チームが顧客データに過度にアクセスできることを懸念している。
開発者は個人用ワークステーションを使用しているため、会社は開発活動をほとんど、またはまったく把握できません。
CISO の懸念を軽減するには、次のうちどれを実装するのが最善でしょうか?
A. DLP
B. テストデータ
C. 暗号化
D. NDA
Answer: D (メーッセージを残す)

最新問題: **116**
開発者は最近、新しいコードを 3 つの Web サーバーにデプロイしました。daffy の自動外部デバイス スキャン レポートには、PCI DSS に基づく障害項目であるサーバーの脆弱性が表示されます。
由緒が有効でない場合、分析者はスキャンをクリーンにするために適切な手順を実行する必要があります。
由緒が有効な場合、分析者はその結果を修正する必要があります。
ネットワーク図で提供される情報を確認した後、ステップ 2 タブを選択し、ドロップダウン オプションを使用してリストされた各サーバーの正しい検証結果と修復アクションを選択してシミュレーションを完了します。

注意事項:
シミュレーションには 2 つのステップが含まれます。
ステップ 1:ネットワーク図に表示されている情報を確認し、[ステップ 2] タブに移動します。
ステップ 2: 与えられたシナリオに基づいて、脆弱性に対処するためにどの修復アクションが必要かを判断します。
Answer:

最新問題**: 117**
最高経営責任者 (CEO) は、新しい最高情報セキュリティ責任者 (CISO) に対し、会社のサイバーセキュリティ運用の強化リストを提供するよう指示しました。その結果、CISO はセキュリティ運用を業界のベスト プラクティスに合わせる必要性を認識しました。これを達成するために適切な業界の参考文献は次のうちどれですか?
A. OSSIM
B. NIST
C. PCI
D. OWASP
Answer: B (メーッセージを残す**)**
https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf

最新問題**: 118**
セキュリティ アナリストは、フォレンジック分析のためにハード ドライブのコピーを提供する必要があります。アナリストがタスクを実行できるのは次のうちどれですか?
A)
B)
C)
D)
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: D (メーッセージを残す**)**

最新問題**: 119**
アプリケーションが次のゲートに進むには、脆弱性評価に合格する必要があります。したがって、セキュリティ上の問題が見つかった場合は、次のゲートに進む前に修正する必要があります。エンドツーエンドの脆弱性評価の方法を最もよく表しているのは次のうちどれですか?
A. セキュリティ回帰テスト
B. 静的解析
C. 動的分析
D. ストレステスト
Answer: C (メーッセージを残す**)**
動的分析は、エンドツーエンドの脆弱性評価の方法であり、ユーザー入力、ネットワーク トラフィック、または環境条件をシミュレートすることにより、実行中のアプリケーションをテストすることが含まれます。動的分析は、ロジックの欠陥、入力検証エラー、セッション管理の弱点など、アプリケーションのさまざまなコンポーネント間の相互作用から発生する可能性のあるセキュリティ問題を特定するのに役立ちます。

最新問題: **120**
セキュリティ アナリストは、通常の地理的ゾーン外のユーザーからの多数のログイン試行が、すべて Web ベースのメール サーバー経由で開始されたことを示すアラートを SIEM から受け取りました。ログには、すべてのドメイン アカウントで同じ時間枠内に 2 回のログイン試行があったことが示されています。
この問題の原因として最も考えられるのは次のうちどれですか?
A. 組織に対してパスワード スプレー攻撃が実行されました。
B. 組織に対して DDoS 攻撃が実行されました。
C. これは通常のシフト勤務活動でした。SIEM の AI は学習しています。
D. 認証済みの外部脆弱性スキャンが実行されました。
Answer: A (メーッセージを残す**)**
説明/参照: https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

最新問題: **121**
アナリストが組織のセキュリティ体制の評価を開始しました。
このレビューの一環として、アナリストは組織に関する情報がどの程度外部に公開されているかを判断したいと考えています。
アナリストがこの目標を達成するのに最も役立つのは次のテクニックのうちどれですか? (2つ選択してください。)
A. インターネット検索
B. バナーの取得
C. フィンガープリンティング
D. DNS クエリ ログのレビュー
E. 技術的管理監査
F. ソーシャル ネットワーク サイトの調達
G. イントラネット ポータルのレビュー
Answer: C,F (メーッセージを残す**)**

最新問題: **122**
アナリストは、10.200.2.0/24 ネットワーク内のいくつかのエンドポイントと IP アドレス 10.200.2.5 のユーザー マシン間のノード間通信の複数のインスタンスを特定しました。
IP アドレス 10.200.2.5 のこのユーザー マシンは、最近脅威フィードに登場したいくつかの IP アドレスとの異常な営業時間中にアウトバウンド通信を開始していることも特定されています。
このアクティビティから推測できるのは次のうちどれですか?
A. 10.200.2.0/24 はルーティング可能なアドレス空間ではありません。
B. 10.200.2.0/24 はランサムウェアに感染しています。
C. 10.200.2.5 はデータを漏洩しています。

D. 10.200.2.5 は不正なエンドポイントです。
Answer: C (メッセージを残す**)**

最新問題**: 123**
ある組織は侵害の疑いがあり、潜在的な影響を特定しようとしています。
組織は次のことを認識しています。
- 侵害の原因は、外国にある IP にリンクされています。
国。
- 侵害は研究開発サーバーに限定されます。
- 侵害前後のデータのハッシュ値は次のとおりです。
変更なし。
- 影響を受けるサーバーには定期的にパッチが適用されており、最近のスキャンでは脆弱性は検出されませんでした。
脅威と影響に関して導き出せる結論は次のうちどれですか? (2つお選びください。)
A. データの整合性は影響を受けません。
B. 脅威は内部関係者です。
C. 脅威は APT です。
D. データの機密性は影響を受けません。
E. 脅威の送信元 IP がスプーフィングされています。
Answer: A,C (メッセージを残す**)**

最新問題**: 124**
アナリストは、脆弱性スキャンの次のコード出力をレビューしています。
これは次のタイプの脆弱性のうちどれを表す可能性が最も高いですか?
A. XSS の脆弱性
B. HTTP 応答分割の脆弱性
C. 安全でない直接オブジェクト参照の脆弱性
D. 資格情報バイパスの脆弱性
Answer: (解答を表示する**)**

最新問題**: 125**
最近の脆弱性スキャンにより、組織のインターネットに接続されているパブリック IP アドレスに 4 つの脆弱性が見つかりました。
組織への侵害のリスクを軽減するために優先順位を付けるには、次のうちどれを最初に修正する必要がありますか?
A. リモート コードの実行を可能にするバッファ オーバーフロー。
B. 自己署名 SSL 証明書を使用する Web サイト。
C. 内部 IP アドレスを明らかにする HTTP 応答。
D. 暗号的に弱いことが知られている暗号。
Answer: (解答を表示する**)**

最新問題**: 126**

サイバーセキュリティ アナリストは、よく知られている ロール ホーム」メッセージがネットワーク境界にあるネットワーク センサーによって継続的に監視されているという警告を受け取りました。
プロキシ ファイアウォールはメッセージを正常にドロップします。アラートが真陽性であると判断した後、最も考えられる原因は次のうちどれですか?
A. マルウェアが会社のシステムで実行されています。
B. 攻撃者は会社のリソースに対して偵察を行っています。
C. 内部関係者が情報をリモート ネットワークに流出させようとしています。
D. コマンドは、ボットネット トロイの木馬に感染したシステムに到達しようとしています。
Answer: (解答を表示する**)**

最新問題: **127**
アナリストはネットワーク上で発生した攻撃を調査していました。ユーザーは適切な認証なしでシステムにアクセスできました。アクセスを制御するために、管理アプローチに関連してアナリストは次のどれを推奨しますか? 3つお選びください。)
A. MAC
B. BCP
C. PEAP
D. DAC
E. RBAC
F. リープ
G. SCAP
Answer: A,D,E (メーッセージを残す**)**

最新問題: **128**
大規模な組織は、より高速な処理と弾力性のメリットを得るために、アカウント登録サービスをクラウドに移行したいと考えています。組織に対する潜在的なリスクを判断するには、次のどれを最初に行う必要がありますか?
A. 移動するサーバーのインベントリを実行し、それぞれに優先順位を割り当てます。
B. 移動されるシステムの目標復旧時間と目標復旧時点を確立します。
C. 移行されるビジネス プロセスとそれぞれの重要度を特定します。
D. システムをクラウドに移行するためのリソース要件を計算します。
E. クラウドベースのシステムに移動する資産のリカバリ優先順位を決定します。
Answer: (解答を表示する**)**

最新問題: **129**
大企業のセキュリティ チームは、支払い処理チームが法規制遵守監査の準備を整え、次の目標を達成できるよう支援しています。
* 監査人による潜在的な指摘事項の数を減らします。
* 監査の範囲を、規制の直接影響を受ける活動のために支払い処理チームが使用するデバイスのみに限定します。
* 他のチームが使用する外部向け Web インフラストラクチャが範囲に入らないようにします。
* 支払い処理チームが使用するシステムが侵害された場合に会社が直面する危険の量を制限します。
セキュリティ チームがこれらの目的を達成するための最も効果的な方法は次のうちどれですか?
A. 支払処理チームの従業員が使用するラップトップにフルディスク暗号化を実装します。
B. 権限を制限して、他の従業員が事業部門が所有するデータにアクセスできないようにします。

C. 組織全体のすべてのサーバーとワークステーションにパッチを展開します。
D. ビジネス ユニットが使用するサーバーとシステムをネットワークの残りの部分からセグメント化します。
Answer: D (メーッセージを残す**)**

最新問題**: 130**
組織は、ネットワークの潜在的な脆弱性を特定するために侵入テストを実施しています。ペネトレーション テスターは、最新のスキャンから次の出力を受け取りました。
ペネトレーション テスターは、組織が Timbuktu サーバーを使用していないことを知っており、Nmap にターゲット上のポートをより詳細に調査させたいと考えています。ペネトレーションテスターは次のコマンドのうちどれを使用する必要がありますか?
A. nmap 192.168.1.13 -v
B. nmap -sS 192.168.1.13 -p1417
C. nmap -sV 192.168.1.13 -p1417
D. sudo nmap -sS 192.168.1.13
Answer: C (メーッセージを残す**)**

最新問題**: 131**
情報セキュリティ管理の運営委員会は、組織のセキュリティインシデント登録を毎年レビューして、傾向や体系的な問題を探します。運営委員会は、来年のセキュリティプログラムを改善するために、過去のインシデントに基づいてリスクをランク付けしたいと考えています。以下は組織の事件記録です。
可用性の潜在的な影響を考慮して、組織は次のどれへの投資を最初に検討すべきですか?
A. 脆弱性管理を支援するマネージド サービス プロバイダーを雇います。
B. システム停止に備えてウォーム サイトを構築します。
C. 必要に応じて、フェイルオーバーおよび冗長システムに投資します。
D. 脆弱性管理とログ レビューを支援する IT 部門のスタッフを追加雇用します。
Answer: C (メーッセージを残す**)**
過去のインシデントに基づいて、組織のシステムの可用性を向上させるには、必要に応じてフェイルオーバーおよび冗長システムに投資することが最善の解決策です。フェイルオーバー システムは、障害や停止が発生した場合にプライマリ システムの動作を自動的に引き継ぐバックアップ システムです。冗長システムは、プライマリ システムと同時に実行され、必要に応じてバックアップ機能を提供する二重システムです。フェイルオーバーおよび冗長システムへの投資は、組織のシステムが常に利用可能であり、中断や機能低下なしにワークロードを処理できるようにするのに役立ちます。

最新問題**: 132**
クライアントは企業の API にアクセスして価格データを取得できません。アナリストは、クライアント以外のソースがデータの API をスクレイピングしており、それが原因でサーバーが利用可能なリソースを超過していることを発見しました。API の可用性を保護するには、次のうちどれが最適ですか?
A. 仮想プライベート ネットワーク
B. Web アプリケーション ファイアウォール
C. 証明書ベースの認証
D. IP ホワイトリスト
Answer: (解答を表示する**)**

最新問題**: 133**
セキュリティ アナリストは、侵害された Linux サーバーを調査しています。アナリストは ps コマンドを発行し、次の出力を受け取ります。

侵害されたシステムをさらに分析するには、管理者が NEXT を実行する必要があるコマンドは次のうちどれですか?
A. キル -9 1301
B. rpm -V openash-server
C. /bin/la -1 /proc/1301/exe
D. strace /proc/1301
Answer: D (メーッセージを残す**)**

最新問題**: 134**
これを防ぐには、クエリをパラメータ化することが重要です。
A. データベースに対する不正なアクションの実行。
B. 昇格した特権でコードを実行するメモリ オーバーフロー。
C. 不正アクセスを許可する Web シェルの確立。
D. セキュリティの脆弱性のある古いライブラリを使用したクエリ。
Answer: A (メーッセージを残す**)**
参照：
https://stackoverflow.com/質問番号:s/4712037/what-is-parameterized-query

最新問題**: 135**
カスタムスクリプトによるリアルタイム監視
A. ログ データは他の顧客に表示される可能性があります。
B. ログへのアクセスはしばらく遅れる可能性があります。
C. ログには誤った情報が含まれている可能性があります
D. SAML ログはクラウドベースの認証ではサポートされていません。
Answer: (解答を表示する**)**

最新問題**: 136**
セキュリティ アナリストは、経理部門が公共文書サービスで売掛金フォームをホストしていることを発見しました。リンクを知っている人は誰でもアクセスできます。この状況に当てはまる脅威は次のうちどれですか?
A. 外部ユーザーへのデータ損失の可能性
B. 公開鍵/秘密鍵管理の喪失
C. クラウドベースの認証攻撃
D. 識別と認証の失敗
Answer: A (メーッセージを残す**)**
外部ユーザーへのデータ損失の可能性は、経理部門が公共文書サービスで売掛金フォームをホストしているこの状況に当てはまる脅威です。リンクを知っている人は誰でもアクセスできます。データ損失とは、機密データの破壊、破損、または不正な開示を引き起こすイベントです。データ損失は、人的エラー、ハードウェア障害、マルウェア感染、サイバー攻撃など、さまざまな理由で発生する可能性があります。この場合、売掛金フォームをパブリック ドキュメント サービスでホストすると、外部ユーザーがそのデータに不正にアクセスしたり、悪意を持って変更または削除したりする可能性があるため、データが損失する可能性があります。

最新問題: **137**
アナリストは次の出力をレビューしています。
これを発見するために使用された可能性が最も高いのは次のうちどれですか?
A. デバッガを使用したリバース エンジニアリング
B. Web アプリケーションの脆弱性スキャン
C. 静的分析の脆弱性スキャン
D. パッシブな脆弱性スキャン
Answer: D (メーッセージを残す**)**

最新問題: **138**
大手金融機関のセキュリティ アナリストは、組織の金融資産を標的とする可能性が高い特定の攻撃者に対する脅威モデルを作成しています。
この攻撃者が使用している高度な技術のレベルを示す最良の例は次のうちどれですか?
A. 脅威アクターによる以前の攻撃で使用されたネットワーク資産
B. 攻撃者がコマンド アンド コントロールに使用する IP アドレス
C. 脅威アクターに起因するソーシャル メディア アカウント
D. 以前の攻撃で脅威アクターに起因すると考えられたカスタム マルウェア
E. 脅威アクターに関連付けられた電子メール アドレスと電話番号
Answer: (解答を表示する**)**

最新問題: **139**
セキュリティ アナリストは、Web ファームに対して定期的な脆弱性スキャンを実行しています。ファームは、負荷分散リバース プロキシとして機能する単一のサーバーで構成され、暗号化プロセスをバックエンド サーバーにオフロードします。バックエンド サーバーは、フロントエンドへの問い合わせを処理する 4 つのサーバーで構成されます。
各サーバーの Web サービス SSL クエリは、同じ出力で応答します。
接続済み (0x000003)
Depth=0 /0=farm.company.com/CN=farm.company.com/OU=Domain Control Validated これらの調査結果に最もよく対処する結果は次のうちどれですか?
A. バックエンド サーバー上の SSL 証明書を取り消し、ホスト名と一致するように再発行する必要があることをアプリケーション開発チームにアドバイスします。
B. アプリケーション開発チームがファーム証明書を更新し、証明書の SAN フィールドに 『ローカル』ドメインのワイルドカードを含めることを要求します。
C. アプリケーション開発チームに結果を通知し、結果の管理にアドバイスします。
D. 脆弱性スキャナーで結果と誤検知として例外を作成し、無視しても安全です
Answer: D (メーッセージを残す**)**

最新問題: **140**
セキュリティ アナリストは、フォレンジック分析のためにハード ドライブのコピーを提供する必要があります。アナリストがタスクを実行できるのは次のうちどれですか?

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

最新問題**: 141**
エンタープライズ ヘルプ デスク システムへようこそ。エスカレーションされたチケットをデスクのチケットキューで処理してください。
説明書
「チケット」をクリックすると、チケットの詳細が表示されます。追加のコンテンツは、チケット内のタブで利用できます。まず、ドロップダウン メニューから適切な問題を選択します。次に、2 番目のドロップダウン メニューから最も考えられる根本原因を選択します。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:

最新問題**: 142**
サイバーセキュリティ アプリケーションで使用される教師あり機械学習アルゴリズムと教師なし機械学習アルゴリズムの主な違いを説明しているものは次のうちどれですか?
A. 教師ありアルゴリズムは攻撃をブロックするために使用できますが、教師なしアルゴリズムは攻撃をブロックできません。
B. 教師なしアルゴリズムでは、より多くの誤検知が発生します。教師ありアルゴリズムよりも。
C. 教師ありアルゴリズムにはセキュリティ アナリストのフィードバックが必要ですが、教師なしアルゴリズムには必要ありません。
D. 教師なしアルゴリズムは IDS システムには適していません。ホワイト教師ありアルゴリズムは IDS システムに適しています。
Answer: C (メーッセージを残す**)**

最新問題**: 143**
サービス デスクのリクエストを検討する際、経営陣はセキュリティ アナリストに対し、新しい人事マネージャーが提出したリクエストを調査するよう要求しました。リクエストは、以前の人間のマネージャーに属していたファイルの「ロック解除」で構成されます。セキュリティ アナリストは、5 段階のパスワードを表示するために使用されるツールを発見しました。このツールは、サービス デスクの数人のメンバーがファイルのロックを解除するために使用しています。これらの特定のファイルの内容は、個人に関する非常に機密性の高い情報です。
このシナリオを最も適切に説明しているのは次のうちどれですか? (2つお選びください。)
A. 不正なデータマスキング
B. 不正なコントロール
C. 不正アクセス
D. 不正なデータの引き出し
E. 不正なソフトウェア
Answer: B,C (メーッセージを残す**)**

最新問題: **144**
あなたは、A 社のサーバーからのスキャン データを解釈する任務を負ったサイバーセキュリティ アナリストです。すべてのサーバーの要件が満たされていることを確認し、満たされていないことが判明した場合は変更を推奨する必要があります。
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。
* TLS 1.2 は、実行されている TLS の唯一のバージョンです。
※Apache 2.4.18以降を使用してください。
* デフォルトのポートのみを使用する必要があります。
説明書
提供されたデータを使用して、サーバーごとに企業のガイドラインの遵守状況を記録します。
質問には 2 つの部分が含まれています。パート 1 とパート 2 を必ず完了してください。提供された強化ガイドラインのみに基づいて問題に対する推奨事項を作成してください。
A. パート 1 の答え:
次の点を確認してください。
AppServ1 は TLS.1.2 のみを使用しています
AppServ4 は TLS.1.2 のみを使用しています
AppServ1 は Apache 2.4.18 以降を使用しています
AppServ4 は Apache 2.4.18 以降を使用しています
パート 2 の答え:
おすすめ :
AppServ2 および AppServ3 で TLS v1.1 を無効にすることをお勧めします。また、AppServ2 Apache を現在のバージョン 2.3.48 からバージョン 2.4.48 にアップグレードします。
B. パート 1 の答え:
次の点を確認してください。
AppServ1 は TLS.1.2 のみを使用しています
AppServ4 は TLS.1.2 のみを使用しています
AppServ1 は Apache 2.4.18 以降を使用しています
AppServ3 は Apache 2.4.18 以降を使用しています
AppServ4 は Apache 2.4.18 以降を使用しています
パート 2 の答え:
おすすめ :
AppServ2 および AppServ3 で TLS v1.1 を無効にすることをお勧めします。また、AppServ2 Apache を現在のバージョン 2.3.48 からバージョン 2.4.48 にアップグレードします。
Answer: (解答を表示する**)**

最新問題: **145**
組織は、ネットワーク偵察に関連するリスクを軽減したいと考えています。ICMP はすでにファイアウォールでブロックされています。ただし、侵入テスト チームは組織のネットワークに対する偵察を実行し、アクティブなホストを特定することができました。アナリストは、パケット キャプチャから次の出力を確認します。
テスト チームがどのようにして ICMP ファイアウォール ルールを回避しているかに関する情報を提供する出力の次のフレーズはどれですか?
A. ttl=64 は、テスト チームが生存時間をファイアウォールのしきい値未満に設定していることを示します
B. フラグが設定されていない場合は、テスト チームが hping を使用していることを示します

C. flags=RA は、テスト チームがクリスマス ツリー攻撃を使用していることを示します
D. 0 データ バイトは、テスト チームが空の ICMP パケットを作成していることを示します
Answer: B (メーッセージを残す**)**

最新問題: **146**
セキュリティ管理者は、root による FTP ログイン試行を警告する IDS ルールを作成する必要があります。次のルールのうち、最良の解決策はどれですか?
A. オプション C
B. オプション B
C. オプション D
D. オプション A
Answer: B (メーッセージを残す**)**

最新問題: **147**
脅威インテリジェンス部門は最近、システム ルーターを悪用する新種のマルウェアを悪用する高度な永続的脅威を知りました。会社は現在同じデバイスを使用しています
脅威レポートに記載されています。次の構成変更のうち、組織のセキュリティ体制を最も改善するのはどれですか?
A. マルウェア亜種のコンテンツを含む IPS ルールを実装し、脆弱性から保護するためにルーターにパッチを適用します。
B. 高度な持続的脅威からの IP アドレスを含む IDS ルールを実装し、脆弱性から保護するためにルーターにパッチを適用します。
C. 高度な持続的脅威からの IP アドレスを含む IPS ルールを実装し、脆弱性から保護するためにルーターにパッチを適用します。
D. マルウェア亜種のコンテンツを含む IDS ルールを実装し、脆弱性から保護するためにルーターにパッチを適用します。
Answer: A (メーッセージを残す**)**

最新問題: **148**
企業の従業員の大多数が、ワークステーションが古いために職務を遂行できないと述べているため、同社は BYOD を導入することを決定しました。提案されたソリューションを保護するためにセキュリティ アナリストが推奨する可能性が最も高いのは次のうちどれですか?
A. Linux ベースのシステムと、すべての BYOD ユーザーに対する Linux に関する必須トレーニング
B. クライアント デバイス用のファイアウォール環境と BYOO ユーザー用の安全な VDI
C. 標準化されたマルウェア対策プラットフォームと統合オペレーティング システム ベンダー
D. 802.1X は BYOD ユーザー ハードウェアに企業ポリシーを適用します
Answer: B (メーッセージを残す**)**
VDIとは仮想デスクトップインターフェースのことです。VDI を使用すると、標準イメージを維持し、感染したマシンがネットワークに接続する脅威を排除できます。

最新問題: **149**
システム侵害のレポートを調査する場合、セキュリティ アナリストは次の /var/log/secure ログ ファイルを確認します。
アナリストがログ ファイルを確認して結論付けることができるのは次のうちどれですか?
A. comptia ユーザーは sudo パスワードを知っています。
B. comptia ユーザーが sudo su コマンドを実行しました。
C. comptia ユーザーは root パスワードを知っています。
D. comptia ユーザーが自分自身を /etc/sudoers ファイルに追加しました。
Answer: C (メーッセージを残す**)**

説明
ユーザーは sudoers ファイルに存在しません。そのためには独自のパスワードを使用します。ユーザーは su コマンドを使用してユーザー アカウントを切り替えました。ユーザーが指定されていない場合、su コマンドはデフォルトで root アカウントになります。これで、ユーザーは root アカウントにログインしました。root アカウントにログインするには、root パスワードを知っている必要があります。

最新問題: **150**
サイバーセキュリティ アナリストは現在、Nessus を使用して複数の FTP サーバーをスキャンしています。スキャンの結果を受け取ったら、アナリストはさらにテストを行って、見つかった脆弱性が存在するかどうかを確認する必要があります。
アナリストは次のコード スニペットを使用します。
アナリストがチェックしている脆弱性は次のうちどれですか?
A. SQL インジェクション
B. フォーマット文字列攻撃
C. デフォルトのパスワード
D. バッファオーバーフロー
Answer: A (メーッセージを残す**)**

最新問題: **151**
中小企業では、経理部門に職務を分離するのに十分な人員がいません。管理者はビジネスのために小切手を書き、元帳と照合します。不正行為が発生していないことを確認するために、企業は四半期ごとにレビューを実施し、社内の別の役員がすべての清算された小切手を台帳と比較します。このタイプのコントロールを最もよく説明しているものは次のうちどれですか?
A. 抑止力
B. 予防的
C. 補償中
D. 刑事
Answer: C (メーッセージを残す**)**
説明
代替制御とも呼ばれる補償制御は、現時点では実装が困難または非現実的であると考えられるセキュリティ対策の要件を満たすために導入されるメカニズムです。
補償制御は、根本的な問題を解決せずに脆弱性に対処するために講じる追加のセキュリティ対策です。」

最新問題: **152**
セキュリティ アナリストがネットワーク トラフィックを調査すると、不審なアクティビティが検出されます。
上記のログに基づいて、次のどの脆弱性攻撃が発生していますか?
A. シェルショック
B. 溺死

C. ゼウス
D. ハートブリード
E. プードル
Answer: E (メーッセージを残す**)**
DROWN (Obsolete and Weakened eNcryption による RSA の復号化) 攻撃は、最新の TLS プロトコル スイートをサポートするサーバーを、時代遅れで安全でない SSL v2 プロトコルのサポートを利用して攻撃し、最大DROWN は、2 つのプロトコル間で同じ公開キー資格情報を共有している限り、TLS で暗号化されたサービスを提供しながら SSLv2 をサポートするすべてのタイプのサーバーに影響を与える可能性があります。さらに、SSLv2 をサポートする別のサーバーで同じ公開キー証明書が使用されている場合、SSLv2 サーバーが TLS サーバーに対して使用できるキー情報を漏洩するため、TLS サーバーも脆弱になります。

最新問題**: 153**
次のログ スニペットがあるとします。
起こった出来事を説明しているのは次のうちどれですか?
A. ネットワーク外部から SSH 接続を確立しようとしましたが、PKI を使用して行われました。
B. §uperman」からの SSH 接続の試行がパスワードを使用して行われました。
C. 192.168.1.166 からの SSH 接続の試行が、PKI を使用して行われました。
D. パスワードを使用して、不明な IP アドレスから SSH 接続を確立しようとしました。
Answer: (解答を表示する**)**

最新問題**: 154**
セキュリティ アナリストは、マルウェアが複数の重要なシステムに拡散しており、正当な管理者の資格情報を持つサイバー インフラストラクチャ チームのメンバーに属する単一のワークステーションから発生していることを発見しました。トラフィックを分析すると、ワークステーションがネットワーク上を一掃して感染対象の脆弱なホストを探していたことがわかります。この感染症の拡大を防ぐために最も効果的だったのは次のうちどれですか?
A. 異常な動作をカタログ化し、IPS を更新するために使用されるハニーポット。
B. 論理ネットワークのセグメンテーションとジャンプ ボックスの使用
C. 適切に構成され、更新された EDR ソリューション。
D. ネットワークの脆弱性スキャンと適切なパッチ適用。
Answer: (解答を表示する**)**

最新問題**: 155**
組織では、偵察の試みを阻止する方法として、非標準のポートで一部の管理サービスを実行する慣例があります。ホスト上の最新のスキャンの出力 192.168.1.13 を以下に示します。
次の記述のうち、正しいものはどれですか?
A. デフォルトのセキュア ポートでの OpenSSH の使用は、他のリモート接続の試行よりも優先されます。
B. リモート SSH 接続は、デフォルトで標準の SSH ポートに自動的に設定されます。
C. スキャンの結果にもかかわらず、ポート 23 で実行されているサービスは実際には SSH ではなく Telnet であり、追加の脆弱性が生じます。
D. Telnet ポートで実行中の SSH は、暗号化されていないポート経由で送信されるようになります。
E. ポート 23 で SSH を実行すると、標準ポートで実行する場合に比べてセキュリティがほとんど強化されません。
Answer: (解答を表示する**)**

最新問題: **156**
A 社は、従業員が USB メモリを介して PII を流出させた疑いがあります。アナリストは、ドライブ上の情報を見つけようとする任務を負っています。問題の PII には次のものが含まれます。
アナリストに割り当てられたタスクを最もよく達成できるのは次のうちどれですか?
A. \d[9] `XXX-XX-XX'
B. \d(3)-d(2)-\d(4)
C. 3 [0-9]\d-2[0-9]\d-4[0-9]\d
D. ?[3]-?[2]-?[3]
Answer: (解答を表示する**)**

最新問題: **157**
クラウド評価の実施中に、セキュリティ アナリストは Prowler スキャンを実行し、レポート内に次の情報が生成されます。
Prowler レポートに基づくと、最も良い推奨事項は次のうちどれですか?
A. アクセスキー 1 を削除します。
B. アクセスキー 2 を削除します。
C. CloudDev アクセス キー 1 を削除します。
D. BusinessUsr アクセス キー 1 を削除します。
Answer: B (メーッセージを残す**)**

最新問題: **158**
開発者は最近、新しいコードを 3 つの Web サーバーにデプロイしました。daffy の自動外部デバイス スキャン レポートには、PCI DSS に基づく障害項目であるサーバーの脆弱性が表示されます。
由緒が有効でない場合、分析者はスキャンをクリーンにするために適切な手順を実行する必要があります。
由緒が有効な場合、分析者はその結果を修正する必要があります。
ネットワーク図で提供される情報を確認した後、ステップ 2 タブを選択し、ドロップダウン オプションを使用してリストされた各サーバーの正しい検証結果と修復アクションを選択してシミュレーションを完了します。
注意事項:
シミュレーションには 2 つのステップが含まれます。
ステップ 1:ネットワーク図に表示されている情報を確認し、[ステップ 2] タブに移動します。
ステップ 2: 与えられたシナリオに基づいて、脆弱性に対処するためにどの修復アクションが必要かを判断します。
Answer:

最新問題: **159**
管理チームは、最初のリスク評価中に、プライバシー規制の不注意違反に次の値を割り当てました。
確率 = 25%
規模 = レコードあたり 1,015 ドル
合計レコード = 10,000
当会計年度中に2件の侵害が発生しました。1 つ目は 35 レコードを侵害し、2 つ目は 65 レコードを侵害しました。侵害された記録の価値は次のうちどれですか?
A. 2,537,500 ドル
B. $10,150

C. 101,500 ドル
D. $25,375
Answer: B (メーッセージを残す**)**

最新問題**: 160**
ある企業がネットワーク内でマルウェア攻撃を受けています。セキュリティ エンジニアは、影響を受ける資産の多くが多数のリモート接続先に送信接続し、データを漏洩していることに気付きました。
ａ.セキュリティ エンジニアは、導入された最新のウイルス対策シグネチャが効果がないことも認識しています。将来同様の攻撃による会社への影響を防ぐための最善のアプローチは次のうちどれですか?
A. IDS 署名
B. データ損失防止
C. シンクホール
D. ポートセキュリティ
Answer: (解答を表示する**)**

最新問題**: 161**
フォレンジック アナリストが、インシデントに関係したワークステーションの画像を撮影しました。画像が改ざんされていないことを最も確実に確認するには、アナリストは以下を使用する必要があります。
A. バックアップテープ
B. 訴訟ホールド
C. 保管過程。
D. ハッシュ化
Answer: (解答を表示する**)**

最新問題**: 162**
ある企業は、ストレージ メディア ファイルの機密データを確実にサニタイズして、ドライブが再利用できないようにしたいと考えています。最良のアプローチは次のうちどれですか?
A. 消磁
B. シュレッディング
C. 書式設定
D. 暗号化中
Answer: (解答を表示する**)**
https://legalshred.com/degaussing-vs-hard-drive-shredding/
ハードドライブの情報を完全に使用できなくする最善かつ最も安全な方法は、ハードドライブのシュレッディングによって完全に破壊することです。シュレッダーとは、シュレッダーと呼ばれる機械を使用してストレージ メディア ファイルを細かく切断し、物理的に破壊する方法です。シュレッディングを行うと、ストレージ メディア ファイルの機密データが確実にサニタイズされ、シュレッディングされた断片からデータを回復することが不可能になるため、ドライブを再利用できなくなります。

最新問題**: 163**
セキュリティ アナリストは、悪意があると思われる電子メールのヘッダーを検査し、次のことを確認します。
ヘッダーの残りの部分と矛盾しており、疑わしいものとして扱う必要があるものは次のうちどれですか?

A. 宛先メールサーバー
B. 件名
C. 送信者の電子メール アドレス
D. TLS 暗号の使用
Answer: C (メーッセージを残す)

最新問題: **164**
組織の情報セキュリティ ガバナンス プロセスの一環として、最高情報セキュリティ責任者 (CISO) はコンプライアンス責任者と協力して、新しい規制および法的要件に関連する記述を含むポリシーを更新しています。すべての従業員がポリシーの変更を適切に認識できるようにするには、次のどれを行うべきですか?
A. ポリシーの改訂版を従業員に配布し、従業員から署名入りの確認書を取得します。
B. ポリシーを組織のイントラネットに投稿し、改訂されたポリシーのコピーをすべての有効なベンダーに提供します。
C. すべての従業員に最新のセキュリティ意識向上トレーニングに参加し、承認書に署名することを要求します。
D. 新しく改訂されたポリシーで定義された管理に基づいてリスク評価を実施します。
Answer: C (メーッセージを残す)

最新問題: **165**
セキュリティ アナリストは、ヘッダー ファイルとフッター ファイルを検査した後、ハードディスクの生データ バイトをスキャンして再構築することにより、ファイルの再構築を開始します。アナリストは次のどの手法を使用していますか?
A. ファイル彫刻
B. データ回復
C. ヘッダー分析
D. メタデータ分析
Answer: A (メーッセージを残す)

最新問題: **166**
Modbus プロトコルに関連する脆弱性は次のうちどれですか?
A. 弱い暗号化
B. サービス拒否
C. 未チェックのユーザー入力
D. 認証がありません
Answer: D (メーッセージを残す)
Modbus は、産業用制御システム (ICS) および監視制御およびデータ収集 (SCADA) システムで広く使用されている通信プロトコルです。ただし、Modbus はセキュリティを提供するように設計されていないため、さまざまなサイバー攻撃に対して脆弱です。Modbus の主な脆弱性の 1 つは認証の欠如です。これは、ネットワーク上のすべてのデバイスがその ID や権限を検証することなくコマンドを送受信できることを意味します。これにより、ICS または SCADA システムに対する不正アクセス、データ操作、またはサービス拒否攻撃が発生する可能性があります。
Modbus での認証の欠如を悪用した攻撃の例は次のとおりです。
検出攻撃: 攻撃者は、Modbus リクエストを送信し、その応答を観察することで、ネットワークをスキャンし、デバイスとそのアドレス、機能、レジスタを検出できます。これにより、システム構成と操作に関する機密情報が漏洩する可能性があります1。
コマンド インジェクション攻撃: 攻撃者は悪意のあるコマンドをデバイスに送信し、その設定、値、または出力を変更する可能性があります。たとえば、攻撃者はモーターの速度を変更したり、バルブを開閉したり、スイッチをオフにしたりすることができます23。

レスポンス インジェクション攻撃: 攻撃者は、デバイスからのレスポンスを傍受して変更し、システムの実際の状態についてマスターまたは他のデバイスを欺くことができます。たとえば、攻撃者はエラーやアラームが発生したときに通常の応答を装うことができます23。
サービス拒否攻撃: 攻撃者はネットワークに Modbus リクエストやコマンドを大量に送り込み、デバイスや通信チャネルに過負荷をかける可能性があります。これにより、正当なリクエストやコマンドの処理が妨げられ、システムの通常の動作が中断される可能性があります14。
これらの攻撃を軽減するために、Modbus に適用できるいくつかのセキュリティ対策は次のとおりです。
暗号化: Modbus メッセージを暗号化すると、権限のない者による盗聴や改ざんを防ぐことができます。ただし、暗号化によって通信に追加のオーバーヘッドと遅延が発生する可能性もあります56。
認証: Modbus に認証メカニズムを追加すると、許可されたデバイスのみがコマンドを送受信できるようになります。認証は、パスワード、証明書、トークン、またはその他の方法に基づいて行うことができます56。
ファイアウォール: Modbus ネットワークと他のネットワークの間にファイアウォールを設置すると、不要なトラフィックをフィルタリングして、不正なアクセスをブロックできます。ファイアウォールは、Modbus 通信のルールとポリシーを強制することもできます24。
侵入検知システム: Modbus ネットワークに侵入検知システム (IDS) を導入すると、トラフィックを監視し、異常または悪意のあるアクティビティを検出できます。IDS は、攻撃が検出されたときにオペレーターに警告したり、対策を発動したりすることもできます24。

最新問題: **167**
SNMP の脆弱性を悪用したネットワーク攻撃が検出されました。
サイバーセキュリティアナリストが最初にすべきことは次のうちどれですか?
A. 脆弱性を修正するために必要なパッチを適用します。
B. インシデントを上級管理者にエスカレーションして指導を求めます。
C. ネットワーク上のすべての特権ユーザー アカウントを無効にします。
D. 攻撃している IP アドレスを一時的にブロックします。
Answer: D (メーッセージを残す)
参照: https://beyondsecurity.com/scan-pentest-network-vulnerabilities-snmp-protocol-version-detection.html

最新問題: **168**
セキュリティ アナリストは、脆弱性スキャンの完了後、OWASP ZAP の [スパイダー] タブからの次の出力を分析しています。
アナリストは、提供された出力に基づいて結論付けることができるオプションは次のうちどれですか?
A. スキャン ベンダーはロボットを使用してスキャン ジョブを高速化しました
B. スキャン ジョブは正常に完了し、脆弱性は検出されませんでした
C. 範囲外のエラーのため、スキャン ジョブは正常に完了しませんでした。
D. スキャナーは、評価対象のページを検出するためにクロール プロセスを実行しました。
Answer: D (メーッセージを残す)

出力には、脆弱性スキャンが完了した後に OWASP ZAP のスパイダー タブを使用した結果が示されています。[スパイダー] タブを使用すると、ユーザーは Web アプリケーションをクロールし、脆弱性を評価できるページやリソースを検出できます。出力には、スキャナーが /admin/、/blog/、/contact/ などのさまざまなディレクトリの下にあるさまざまなページと、入力と出力のテストに使用できるいくつかのパラメーターとフォームを検出したことが示されています。参考資料: CompTIA サイバーセキュリティ アナリスト (CySA+) 認定試験の目的 (CS0-002)、9 ページ。https://www.zaproxy.org/docs/desktop/start/features/spider/

最新問題: **169**
特定のデータセットに割り当てられる分類レベルを決定する最終的な責任を負うのは、次の役割のうちどれですか?
A. データ管理者
B. データ所有者
C. データプロセッサ
D. 上級管理職
Answer: B (メーッセージを残す**)**
参考: https://www.pearsonitcertification.com/articles/article.aspx?p=2731933&seqNum=3

最新問題: **170**
ドラッグ アンド ドロップの質問
企業ネットワーク上の複数のノードで、無関係なセキュリティ イベントが複数発生したのではないかと考えられます。各ノードをクリックして各セキュリティ イベントを検出するには、すべてのログを確認し、必要に応じてイベントを関連付ける必要があります。修正が必要なセキュリティ イベントがログに示されている場合にのみ、修正アクションを選択します。適切な修正措置をドラッグ アンド ドロップして、影響を受ける各デバイスで発生する特定のセキュリティ イベントを軽減します。
説明書：
Webサーバー、データベースサーバー、IDS、開発用PC、経理用PC、マーケティング用PCをクリック可能です。一部のアクションは必須ではない場合があり、各アクションはノードごとに 1 回のみ使用できます。
是正措置の順序は重要ではありません。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 [リセット] ボタンを選択してください。シミュレーションが完了したら、[完了] ボタンを選択して送信してください。シミュレーションが送信されたら、 次へ]ボタンを選択して続行してください。

Answer:

最新問題: **171**
システム管理者は、実行中のさまざまなサービスの脆弱性を判断するために、企業の外部ネットワークのネットワーク偵察を行っています。いくつかのサンプル トラフィックを外部ホストに送信すると、管理者は次のパケット キャプチャを取得します。
出力に基づいて、次のどのサービスの脆弱性をさらにテストする必要がありますか?
A. HTTP
B. SMB
C. HTTPS
D. SSH
Answer: (解答を表示する**)**

最新問題: **172**
組織には、昇格されたアクセス許可が必要な場合、ユーザーは常に自分のアカウントでコマンドを実行し、必要に応じて一時的な管理者権限を付与する必要があるという厳格なポリシーがあります。セキュリティ アナリストが syslog エントリを確認しているところ、次のことがわかりました。

次のエントリのうち、アナリストにとって最も懸念されるのはどれですか?
A. <100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM ' su vi httpd.conf' がジョーに対して失敗しました
B. <100>2 2020-01-10T20:36:36.0010z Financeserver su 201 32001 = BOM ' sudo vi users.txt 成功
C. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi syslog.conf が jos で失敗しました
D. <100> 2020-01-10T19:34..002z Financeserver su 201 32001 = BOM ' su vi 成功
E. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi httpd.conf' 成功
Answer: (解答を表示する**)**
syslog エントリには、ユーザーが 2 つのサーバー (webserver と Financeserver) 上で昇格されたアクセス許可を使用してコマンドを実行しようとしたことが示されています。エントリには、日付と時刻、サーバー名、使用されたコマンド (su または sudo)、ユーザー名、および結果 (成功または失敗) が含まれます。組織のポリシーでは、ユーザーは常に自分のアカウントでコマンドを実行し、必要に応じて一時的な管理者権限を付与する必要があると規定されています。これは、ユーザーが別のユーザー (通常は root) としてコマンドを実行するには、su を使用して別のユーザーのアカウントに切り替えるのではなく、sudo を使用する必要があることを意味します。したがって、アナリストが最も懸念するエントリは D です。<100> 2020-01-10T19:34...002z Financeserver su 201 32001 = BOM ' su vi success。このエントリは、誰かが su を使用して Financeserver 上の別のユーザーのアカウントに切り替え、vi でファイルを正常に編集したことを示しています。これは、不正アクセスまたはアカウントの侵害を示している可能性があります。

最新問題**: 173**
Windows サーバー上で Massivelog ログが 40GB に増加しました このサイズでは、ローカル ツールはファイルを読み取ることができず、ファイルが配置されている仮想サーバーからファイルを移動することもできません。PowerShell スクリプトの次の行のうち、ユーザーがレビューのために loq の最後の 10,000 行を抽出できるようにするものはどれですか?
A. 末尾 -10000 Massivelog.log > 抽出、テキスト
B. info tail n -10000 Massrvelog.log txt を抽出します:
C. get-content * ./Massivelog. log' -最後の 10000 > extract.txt;
D. コンテンツ 「Massivelog.log」を取得 -Last 10000 | 抽出.txt
Answer: C (メーッセージを残す**)**

最新問題**: 174**
セキュリティ アナリストは、侵害されてデータ作成マシンとして使用されていたサーバー 1 台と、作成されたハード ドライブの一部を特定しました。マシンがいつ、どのように侵害されたか、またマルウェアがどこにあるかについての情報を提供する可能性が最も高いのは次のうちどれですか?
A. システム タイムラインの再構築
B. システム レジストリの抽出
C. データカービング
D. 揮発性メモリ アナリスト
Answer: (解答を表示する**)**
説明
情報セキュリティの専門家は、メモリ フォレンジックを実施して、ハード ドライブ データに簡単に検出できない痕跡を残さない攻撃や悪意のある動作を調査および特定します。

最新問題**: 175**

セキュリティ アナリストは、Web ファームに対して定期的な脆弱性スキャンを実行しています。ファームは、負荷分散リバース プロキシとして機能する単一のサーバーで構成され、暗号化プロセスをバックエンド サーバーにオフロードします。バックエンド サーバーは、フロントエンドへの問い合わせを処理する 4 つのサーバーで構成されます。
各サーバーの Web サービス SSL クエリは、同じ出力で応答します。
接続済み (0x000003)
Depth=0 /0=farm.company.com/CN=farm.company.com/OU=Domain Control Validated これらの調査結果に最もよく対処する結果は次のうちどれですか?
A. 脆弱性スキャナーで結果と誤検知として例外を作成し、安全に無視できます。
B. アプリケーション開発チームに結果を通知し、結果の管理者にアドバイスします。
C. アプリケーション開発チームがファーム証明書を更新し、証明書の SAN フィールドに ローカル」ドメインのワイルドカードを含めることを要求します。
D. バックエンド サーバー上の SSL 証明書を取り消し、ホスト名と一致するように再発行する必要があることをアプリケーション開発チームにアドバイスします。
Answer: A (メーッセージを残す**)**

最新問題**: 176**
組織のネットワーク管理者は、スイッチの特性をエミュレートしている不正なデバイスをネットワーク上で発見しました。デバイスはプロトコルをトランキングし、タグ付け VA を挿入しています。
データリンク層のトラフィックの流れ
この攻撃を最もよく説明しているのは次のうちどれですか?
A. インジェクション攻撃
B. VLAN ホッピング
C. スプーフィング
D. DNS ファーミング
Answer: (解答を表示する**)**

最新問題**: 177**
セキュリティ アナリストは、マルウェアが含まれている疑いのある特定のサーバーのパケット キャプチャを調査し、次のパケットを発見しました。
セキュリティ アナリストにとって最も懸念されるトラフィック パターンまたはデータは次のうちどれですか?
A. 103.34.243.12 によって許可された匿名アクセス
B. 202.53.245.78 からの HTTP トラフィックに使用されるポート
C. 73.252.34.101 からの SMTP トラフィックに使用されるポート
D. 103.34.243.12 から送信された暗号化されていないパスワード
Answer: (解答を表示する**)**

最新問題**: 178**
ヘルプ デスクは、複数のユーザーから報告された不審な電子メールに関して発生し始めている傾向をセキュリティ アナリストに通知しました。アナリストは、電子メールに次のファイルを含む invoice.zip という名前の添付ファイルが含まれていると判断しました。
Locky.js
xerty.ini
xerty.lib
さらに分析したところ、.zip ファイルを開くと、新しいバージョンのランサムウェアがデバイスにインストールされることがわかりました。会社の NAS 上のデータが感染したデバイスによって暗号化されるのを防ぐために、最初に行うべきことは次のうちどれですか?

A. ファイル共有のアクセス許可を読み取り専用に設定します。
B. 請求書の添付ファイルを開かないように従業員に電子メールで指示します。
C. .js ファイルに含まれる URL を会社の Web プロキシ フィルターに追加します。
D. 会社の VPN へのアクセスを無効にします。
Answer: B (メーッセージを残す)

最新問題: **179**
ソフトウェア開発チームは、会計部門向けに新しい Web アプリケーションを実稼働環境にプッシュしました。アプリケーションが公開された直後、会計部門の責任者は、アプリケーションが意図したとおりに動作していないことを IT 運用部門に通知しました。次の SDLC のベスト プラクティスのうち、欠けているものはどれですか?
A. ファジング
B. 静的コード分析
C. ユーザー受け入れテスト
D. 回帰テスト
E. ピアコードのレビュー
Answer: (解答を表示する)

最新問題: **180**
セキュリティ アナリストが SIEM ログを確認し、次のエラー イベントを発見しました。
アナリストがイベントのトラブルシューティングを続行するには、次の環境のうちどれを調べる必要がありますか?
A. プロキシサーバー
B. DNS サーバー
C. SQL サーバー
D. Windows ドメイン コントローラー
E. WAF アプライアンス
Answer: B (メーッセージを残す)

最新問題: **181**
システム管理者は、実行中のさまざまなサービスの脆弱性を判断するために、企業の外部ネットワークのネットワーク偵察を行っています。いくつかのサンプル トラフィックを外部ホストに送信すると、管理者は次のパケット キャプチャを取得します。
出力に基づいて、次のどのサービスの脆弱性をさらにテストする必要がありますか?
A. SMB
B. SSH
C. HTTP
D. HTTPS
Answer: A (メーッセージを残す)

最新問題: **182**
セキュリティ アナリストは、通常の地理的ゾーン外のユーザーからの多数のログイン試行が、すべて Web ベースのメール サーバー経由で開始されたことを示すアラートを SIEM から受け取りました。ログには、すべてのドメイン アカウントで同じ時間枠内に 2 回のログイン試行があったことが示されています。
この問題の原因として最も考えられるのは次のうちどれですか?
A. 組織に対してパスワード スプレー攻撃が実行されました。
B. 組織に対して DDoS 攻撃が実行されました。
C. これは通常のシフト勤務活動でした。SIEM の AI は学習しています。
D. 認証済みの外部脆弱性スキャンが実行されました。
Answer: A (メーッセージを残す**)**
説明
説明/参照: https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

最新問題: **183**
SIEM アナリストは、ゲスト ワイヤレス ネットワークからいくつかの電子医療記録 (EHR) システムへのアクティビティが急増していることに気付きました。さらに分析した結果、アナリストは過去 6 か月間に大量のデータがクラウド プロバイダーにアップロードされたことを発見しました。アナリストが最初に行うべきアクションは次のうちどれですか?
A. 公民権局 (OCR) に連絡して違反を報告してください
B. ゲートウェイ ルーターに ACL を設定します。
C. 最高プライバシー責任者 (CPO) に通知します。
D. インシデント対応計画をアクティブ化します
Answer: B (メーッセージを残す**)**

最新問題: **184**
脅威ハンティング チームのセキュリティ アナリストは、ワークステーションの標準 OS 導入の一部として現在実行されている不要な無害なサービスのリストを作成しました。アナリストはこのリストを運用チームに提供し、組織内のすべてのワークステーションのサービスを自動的に無効にするポリシーを作成します。
セキュリティ アナリストの目標を最もよく表しているものは次のうちどれですか?
A. システム ベースラインを作成するには
B. 攻撃対象領域を減らすため
C. システムのパフォーマンスを最適化するため
D. マルウェアの検出を向上させるため
Answer: B (メーッセージを残す**)**
攻撃対象領域を縮小するということは、攻撃者が利用できる機能を制限することを意味します。たとえば、1 つを除いて施設へのすべてのドアをロックすると、攻撃対象領域が減少します。攻撃対象領域を減らすことを表す別の用語は、システムの強化です。システムの強化には、すべてのシステムが可能な範囲で強化され、機能を提供できるようにすることが含まれます。

最新問題: **185**
セキュリティ アナリストは、複数のセンサーからのアクティビティを分析して関連付けた結果、高リスク国のグループが企業ネットワークへの高度な侵害と、過去 3 か月にわたる標的型攻撃の継続的な管理に関与していると判断しました。これまで、攻撃は気づかれませんでした。これは次の例です。
A. スピア フィッシング。
B. 悪意のある内部関係者の脅威。
C. 高度で持続的な脅威。
D. 権限昇格。
Answer: C (メーッセージを残す**)**

最新問題: **186**
セキュリティ アナリストは、侵害された Linux サーバーを調査しています。アナリストは ps コマンドを発行し、次の出力を受け取ります。
侵害されたシステムをさらに分析するには、管理者が次に実行する必要があるコマンドは次のうちどれですか?
A. gbd /proc/1301
B. rpm -V openssh-server
C. /bin/ls -1 /proc/1301/exe
D. キル -9 1301
Answer: C (メーッセージを残す**)**
/bin/ls -1 /proc/1301/exe は、プロセス ID 1301 に関連付けられた実行バイナリ ファイルへの絶対パス (./usr/sbin/sshd) を表示するコマンドです。この情報は、セキュリティ アナリストがバイナリが正式バージョンで変更されていないことを判断するのに役立ちます。これは侵害の兆候である可能性があります。/proc/1301/exe は、プロセス 1301 を開始するために使用された実行可能ファイルを指す特別なシンボリック リンクです。

最新問題: **187**
会社員がインターネットからアプリケーションをダウンロードします。インストール後、従業員は顕著なパフォーマンスの問題を経験し始め、デスクトップにファイルが表示されるようになります。
タスク マネージャーで実行されているプロセスを考慮すると、セキュリティ アナリストは次のプロセスのうち、システム侵害の可能性が最も高い兆候として特定するのはどれですか?
A. taskmgr.exe
B. mstsc.exe
C. Chrome.exe
D. Explorer.exe
E. Word.exe
Answer: (解答を表示する**)**

最新問題: **188**
クラウド評価の実施中に、セキュリティ アナリストは Prowler スキャンを実行し、レポート内に次の情報が生成されます。
Prowler レポートに基づくと、最も良い推奨事項は次のうちどれですか?
A. BusinessUsr アクセス キー 1 を削除します。
B. アクセスキー 1 を削除します。
C. アクセスキー 2 を削除します。
D. CloudDev アクセス キー 1 を削除します。

Answer: C (メーッセージを残す)

最新問題: **189**
管理は、ネットワーク外部から社内のキー サーバーへの管理者アクセスに関係します。具体的には、ファイアウォール ルールにより、社内のどこからでもサーバーへのアクセスが許可されます。効果的な解決策は次のうちどれですか?
A. 跳び箱
B. マルウェア対策
C. ハニーポット
D. サーバーの強化
Answer: A (メーッセージを残す)

最新問題: **190**
サイバーセキュリティ アナリストは、組織の脆弱性を管理するために使用される企業プロセスに従うように求められました。アナリストは、ポリシーが 3 年間更新されていないことに気づきました。ポリシーが依然として正確であることを確認するために、アナリストは次のどれをチェックする必要がありますか?
A. 準拠規則
B. 技術的な制約
C. 脅威インテリジェンス レポート
D. 企業議事録
Answer: (解答を表示する)

最新問題: **191**
セキュリティ アナリストは、社内ドメイン ユーザーが企業ストアフロント Web サイトにアクセスできないと報告するサービス チケットをいくつか受け取りました。ただし、外部ユーザーは問題なく Web サイトにアクセスしています。この動作の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. 時刻同期サーバーが破損しています。
B. 証明書の有効期限が切れています。
C. DNS サーバーが破損しています。
D. FQDN が正しくありません。
Answer: C (メーッセージを残す)

最新問題: **192**
次の組織のうち、組み込みコントローラーの脆弱性を修正する必要があるのはどれですか?
A. 規制当局
B. 銀行機関
C. 水力発電施設
D. 公立大学
Answer: C (メーッセージを残す)

最新問題: **193**
セキュリティ アナリストは、侵害された認証サーバーを調査しているときに、次の隠しファイルを発見しました。

さらに分析すると、これらのユーザーはサーバーにログインしたことがないことがわかります。ファイルを取得するために使用された攻撃の種類は次のうちどれですか?また、この種類の攻撃の再発を防ぐためにアナリストは何を推奨する必要がありますか?
A. フィッシング攻撃がアカウントを侵害するために使用されました。アナリストは、フィッシング リンクを無効にするためにエンドポイント保護をインストールすることをユーザーに推奨する必要があります。
B. パスワード スプレー攻撃がパスワードを侵害するために使用されました。アナリストは、すべてのユーザーに固有のパスワードを受け取ることを推奨する必要があります。
C. アカウントを侵害するためにレインボー テーブル攻撃が使用されました。アナリストは、将来のパスワード ハッシュにソルトを含めることを推奨する必要があります。
D. 不正な LDAP サーバーがシステムにインストールされており、パスワードを接続しています。アナリストは、サーバーを消去して再インストールすることを推奨する必要があります。
Answer: B (メーッセージを残す**)**

最新問題**: 194**
脅威を与えるチームは、脅威アクターのプロフィールと活動を追跡する新しい LoC を ISAC から受け取りました。
次に更新する必要があるのは次のうちどれですか?
A. DNS
B. ブロックリスト
C. IDS 署名
D. ホワイトリスト
Answer: (解答を表示する**)**

最新問題**: 195**
最高情報セキュリティ責任者は、ネットワーク上の特定のトラフィックをリダイレクトするためのセキュリティ対策を講じるよう要求しました。この問題を最もよく解決するのは次のうちどれですか?
A. シンクホール
B. ブロックリストに登録
C. ジオブロッキング
D. サンドボックス化
Answer: A (メーッセージを残す**)**
シンクホールは、ネットワーク内のデータ フローを操作する手法です。トラフィックを目的の宛先から選択したサーバーにリダイレクトします。これは、正当なトラフィックを意図した受信者から遠ざけるために悪意を持って使用される可能性がありますが、セキュリティ専門家はシンクホールを研究や攻撃への対応のためのツールとして使用することが一般的です1。
たとえば、シンクホールを使用すると、ボットネットまたはマルウェアに感染したホストからのトラフィックを、防御者の制御下にあるサーバーにリダイレクトでき、そこでトラフィックを分析、ブロック、または無力化できます。これは、侵害されたデバイスを特定して隔離し、コマンドアンドコントロール通信を防止し、悪意のある活動を妨害するのに役立ちます2。
他のオプションは、次の理由から最適なソリューションではありません。
ブロックリストは、悪意があることがわかっている、または疑わしい特定の IP アドレス、ドメイン、またはアプリケーションへのアクセスまたは通信を防止するための技術です。ブロックリストは、ファイアウォール、ルーター、プロキシ、またはソフトウェア ツールを使用して実装できます。ブロックリストは、不要なトラフィックまたは有害なトラフィックからネットワークを保護できますが、トラフィックを別の宛先にリダイレクトしません。

ジオブロッキングは、地理的位置に基づいて、特定の IP アドレス、ドメイン、またはアプリケーションへのアクセスまたは通信を制限する技術です。ジオブロッキングは、ファイアウォール、ルーター、プロキシ、またはソフトウェア ツールを使用して実装できます。ジオブロッキングは、特定の地域や国からの不正なトラフィックや望ましくないトラフィックからネットワークを保護できますが、トラフィックを別の宛先にリダイレクトするわけではありません。
サンドボックス化は、悪意のある可能性のあるコードやアプリケーションを分離した安全な環境で隔離して実行するための技術です。サンドボックスは、仮想マシン、コンテナ、またはソフトウェア ツールを使用して実装できます。サンドボックスは、マルウェアの感染や損傷からネットワークを保護できますが、ネットワーク トラフィックを別の宛先にリダイレクトしません。

最新問題: **196**
セキュリティ アナリストは、ビットコインに関連する IP アドレスにトラフィックを送信しているため、クリプトマイニング ツールを実行している可能性があるステージング環境のホスト (10.0 1.25) 上の脅威検出プラットフォームからのアラートに関連するクライアントが存在しないことを調査しています。
インスタンスのネットワーク ルールは次のとおりです。
ホストを隔離してトリアージするための最良の方法は次のうちどれですか?
A. ルール 1.2 を削除します。3.4. そして5.
B. ルール 1.2 を削除します。4.と5.
C. ルール 1.2 を削除します。そして5.
D. ルール 1.2 を削除します。そして3.
E. ルール 4 と 5 を削除します。
F. ルール 1.4 を削除します。そして5.
Answer: (解答を表示する**)**

最新問題: **197**
セキュリティ アナリストは、侵害されてデータ作成マシンとして使用されていたサーバー 1 台と、作成されたハード ドライブの一部を特定しました。マシンがいつ、どのように侵害されたか、またマルウェアがどこにあるかについての情報を提供する可能性が最も高いのは次のうちどれですか?
A. システム タイムラインの再構築
B. システム レジストリの抽出
C. データカービング
D. 揮発性メモリ アナリスト
Answer: D (メーッセージを残す**)**
情報セキュリティの専門家は、メモリ フォレンジックを実施して、ハード ドライブ データに簡単に検出できない痕跡を残さない攻撃や悪意のある動作を調査および特定します。

最新問題: **198**

Windows サーバー上で Massivelog ログが 40GB に増加しました このサイズでは、ローカル ツールはファイルを読み取ることができず、ファイルが配置されている仮想サーバーからファイルを移動することもできません。PowerShell スクリプトの次の行のうち、ユーザーがレビューのために loq の最後の 10,000 行を抽出できるようにするものはどれですか?
A. コンテンツ 「/Massivelog.log」を取得 -Last 10000 | 抽出.txt
B. get-content './Massivelog.log' -Last 10000 > extract.txt;
C. 情報末尾 n -10000 Massivelog.log | 抽出.txt;
D. 末尾 -10000 Massivelog.log > extract.txt
Answer: B (メーッセージを残す**)**

最新問題**: 199**
セキュリティ アナリストは、公開されている企業サーバーへのアクセスが非常に遅く、断続的に発生するという報告を受けました。
システムが侵害されている可能性があると考え、アナリストは次のコマンドを実行します。
上記のコマンドの出力に基づいて、アナリストが調査を進めるために次に実行すべきことは次のうちどれですか?
A. サーバー ログを調べて、Web アプリケーションの侵害を示すさらなる兆候を確認します。
B. /tmp/.t/t ファイルは不正な SSHD サーバーである可能性があるため、バイナリ分析を実行します。
C. kill -9 1325 を実行して負荷平均を下げ、サーバーを再び使用できるようにします。
D. crontab -r を実行します。rm -rf /tmp/.t を実行して、システム上のマルウェアを削除して無効にします。
Answer: (解答を表示する**)**

最新問題**: 200**
サイバーセキュリティ アナリストは、最高レベルのセキュリティを実現するために、ファイアウォールと VPN サーバーを使用してネットワークを再設計する必要があります。このタスクを最適に完了するには、アナリストは次のものを配置する必要があります。
A. VPN サーバーの背後にあるファイアウォール
B. ファイアウォールの背後にある VPN サーバー
C. ファイアウォール上の VPN
D. ファイアウォールと並列の VPN サーバー
Answer: B (メーッセージを残す**)**

最新問題**: 201**
エンタープライズ ヘルプ デスク システムへようこそ。エスカレーションされたチケットをデスクのチケットキューで処理してください。
説明書
「チケット」をクリックすると、チケットの詳細が表示されます。追加のコンテンツは、チケット内のタブで利用できます。まず、ドロップダウン メニューから適切な問題を選択します。次に、2 番目のドロップダウン メニューから最も考えられる根本原因を選択します。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:

最新問題**: 202**
コードをデプロイする前に脆弱なサードパーティ ライブラリを検出できるのは次のうちどれですか?
A. 影響分析
B. 動的分析

C. 静的解析
D. プロトコル分析
Answer: C (メーッセージを残す)
静的解析とは、アプリケーションを実行せずにソースコードやバイナリコードを解析する手法です。静的分析では、コードをスキャンして既知の脆弱なライブラリまたはバージョンへの参照を確認し、問題やリスクを報告することで、コードを展開する前に脆弱なサードパーティ ライブラリを検出できます12。
影響分析は、パフォーマンス、可用性、セキュリティ、互換性など、システムまたはサービスに対する変更の潜在的な影響を評価するプロセスです。影響分析は、コードをデプロイする前に脆弱なサードパーティ ライブラリを検出するのではなく、変更の結果を評価して伝達するのに役立ちます。
動的分析は、さまざまな条件または入力の下でアプリケーションを実行することにより、アプリケーションの動作またはパフォーマンスを分析する方法です。動的分析は、コードをデプロイする前に脆弱なサードパーティ ライブラリを検出するのではなく、実行時に発生するエラーや欠陥を特定するのに役立ちます。
プロトコル分析は、パケットまたはメッセージをキャプチャして解釈することにより、ネットワーク上のデバイスまたはアプリケーション間で交換されるデータを検査する方法です。プロトコル分析は、コードを展開する前に脆弱なサードパーティ ライブラリを検出しませんが、ネットワーク通信の監視とトラブルシューティングに役立ちます。

最新問題: **203**
エンタープライズ ヘルプ デスク システムへようこそ。エスカレーションされたチケットをデスクのチケットキューで処理してください。
説明書
 チケット」をクリックすると、チケットの詳細が表示されます。追加のコンテンツは、チケット内のタブで利用できます。まず、ドロップダウン メニューから適切な問題を選択します。次に、2 番目のドロップダウン メニューから最も考えられる根本原因を選択します。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:

最新問題: **204**
組織には次のリスク軽減ポリシーがあります。
95% 以上の確率のリスクは、その影響に関係なく、他のリスクよりも先に対処されます。
他のすべての優先順位はリスク値に基づいて決定されます。
組織は次のリスクを特定しました。
リスク軽減の優先順位は、高いものから低いものまで次のうちどれですか?
A. D、A、B、C
B. A、B、D、C
C. D、A、C、B
D. A、B、C、D
Answer: C (メーッセージを残す)

最新問題: **205**
サイバーセキュリティ アナリストは、特定のユーザー ワークステーションに関するインシデント レポートを調査しています。
ワークステーションは、最初の起動時であっても CPU とメモリの使用率が高く、ネットワーク帯域幅の使用率が非常に高くなっています。ユーザーは、仕事の習慣に大きな変化が生じていないにもかかわらず、アプリケーションが頻繁にクラッシュすると報告しています。ウイルス対策スキャンでは既知の脅威は報告されません。この理由として最も可能性が高いのは次のうちどれですか?
A. 高度な持続的脅威

B. トロイの木馬
C. ゼロデイ
D. ロジックボム
Answer: (解答を表示する**)**

最新問題**: 206**
次の出力は、企業ネットワークのエッジにある tcpdump からのものです。
潜在的なセキュリティ上の懸念を最もよく説明しているものは次のうちどれですか?
A. ペイロード長は、コードの実行を可能にするバッファのオーバーフローに使用される可能性があります。
B. カプセル化されたトラフィックはセキュリティの監視と防御を回避する可能性があります
C. このトラフィックは、ネットワーク フットプリントを作成するための偵察技術を示します。
D. トラフィック ペイロードの内容により、VLAN ホッピングが許可される場合があります。
Answer: B (メーッセージを残す**)**
カプセル化されたトラフィックは、トラフィックの実際のコンテンツやソースを隠したり難読化したりすることで、セキュリティの監視や防御を回避する可能性があります。カプセル化は、追加のヘッダーまたはプロトコルでデータ パケットをラップし、さまざまなネットワーク タイプまたはレイヤー間での通信を可能にする技術です。カプセル化は、トンネリング、VPN、NAT などの正当な目的に使用できますが、攻撃者がカプセル化されたトラフィックを検査または分析できないセキュリティ制御や検出メカニズムをバイパスするために使用することもできます。

最新問題**: 207**
ある組織は、必須ではないサービスをクラウド コンピューティング環境に移行したいと考えています。経営陣はコストを重視しており、12 時間という復旧時間の目標を達成したいと考えています。望ましい結果を達成するには、次のクラウド回復戦略のうちどれが最も効果的ですか?
A. フェールオーバーに使用できる別のクラウド プロバイダーのコールド サイトを使用してシステムを構成します。
B. 同じクラウド プロバイダー内の別のリージョンへのアクティブなレプリケーションを備えたホット サイトを確立します。
C. すべてのサービスを別のインスタンスに複製し、インスタンス間の負荷分散を行います。
D. 別のリージョンにある同じクラウド プロバイダーを使用してウォーム ディザスタ リカバリ サイトをセットアップします。
Answer: D (メーッセージを残す**)**

最新問題**: 208**
セキュリティ アナリストは悪意のあるソフトウェアのサンプルを持っていますが、そのサンプルが何を行うかを知る必要がありますか? アナリストは、慎重に制御および監視された仮想マシンでサンプルを実行し、ソフトウェアの動作を観察します。
これは次のマルウェア分析アプローチのうちどれですか?
A. サンドボックス化
B. ホワイトボックステスト
C. ファジング
D. 静的コード分析
Answer: (解答を表示する**)**

最新問題**: 209**
セキュリティ アナリストは、Web サーバーのログを確認しているときに、次のコードに気づきました。
このコードによる悪意のあるアクションの実行を防ぐのは次のうちどれですか?

A. アプリケーションの前にネットワーク ファイアウォールをインストールします
B. Web アプリケーション侵入テストの実行
C. HTTP の使用を無効にし、HTTPS の使用を要求する
D. アプリケーションに入力検証の使用を要求します。
Answer: C (メーッセージを残す)

最新問題: **210**
人事担当者は、人事記録を含む電子メールを全従業員に一斉送信します。今後このようなことが起こらないようにする方法についての人事部長の懸念に対処するために、セキュリティ アナリストが呼ばれました。
ディレクターに推奨する最善の解決策は次のうちどれですか?
A. データ損失防止システムをインストールし、人事担当者にその使用法をトレーニングします。社内の全従業員に PII トレーニングを提供します。PII 情報を暗号化します。
B. PII データを保護する人事ポリシーを作成するための特定の機器を設置します。会社の従業員に PII データの取り扱い方法を研修します。すべての PII を別の会社に委託します。人事部長を PII の取り扱いに関するトレーニングに派遣します。
C. すべての従業員をトレーニングします。社内ネットワーク上で送信されるデータを暗号化します。プライバシー担当者を招いて、PII をどのように扱うべきかについての計画を提示します。
D. 社内で送信されるすべての電子メールに暗号化を適用します。データの処理方法に関する PII プログラムとポリシーを作成します。すべての人事担当者をトレーニングします。
Answer: (解答を表示する)

最新問題: **211**
IT セキュリティ アナリストは、同社が最近購入した新しい車両の脆弱性に関する電子メール アラートを受け取りました。次の攻撃ベクトルのうち、最も可能性が高い脆弱性はどれですか?
A. SCADA
B. CAN バス
C. Modbus
D. IoT
Answer: (解答を表示する)
コントローラー エリア ネットワーク - CAN バスは、今日の自動車やその他のデバイスに搭載されている電子制御ユニット (ECU) が、信頼性の高い優先順位主導の方法で相互に通信できるように設計されたメッセージ ベースのプロトコルです。メッセージまたは 「フレーム」はネットワーク内のすべてのデバイスによって受信され、ホスト コンピューターは必要ありません。
CAN バスは、Controller Area Network Bus の略で、車両内のさまざまなデバイスやコンポーネントが通信してデータを交換できるようにする通信プロトコルです。新しい車両群の脆弱性は、攻撃者が車両の操作や操作を妨害できる可能性があるため、CAN バスをターゲットにしている可能性が最も高くなります。SCADA、Modbus、IoT なども通信プロトコルやシステムに関連する用語ですが、車両に固有のものではありません。参考: https://www.csoonline.com/article/3218104/what-is-a-can-bus-and-how-can-it-be-hacked.html

最新問題: **212**
情報セキュリティ アナリストは、アーカイブ データ セットの排除に重点を置いたプロジェクトの一環として、バックアップ データ セットをレビューしています。電子データを廃棄する前に、最初に考慮すべきことは次のうちどれですか?
A. サニタイズポリシー
B. 暗号化ポリシー
C. 保存基準
D. データ主権
Answer: C (メーッセージを残す**)**

最新問題: **213**
セキュリティ エンジニアは、企業の内部脅威プログラムの一環としてユーザーによる悪意のある行為を識別するセキュリティ製品をレビューしています。この目的に最も適切な製品カテゴリは次のうちどれですか?
A. ウエバ
B. SCAP
C. WAF
D. ソアリング
Answer: (解答を表示する)

最新問題: **214**
RDP にリモートでコードが実行される脆弱性が発見されました。組織は現在、VDI 環境の一部へのリモート アクセスに RDP を使用しています。アナリストはネットワークレベルを検証しました
認証が有効になっています
この脆弱性に対する最善の修復策は次のうちどれですか?
A. 脆弱性に対応するパッチがインストールされていることを確認します^
B. 脅威インテリジェンス フィードが最新のソリューションで更新されていることを確認します。
C. システム ログに侵害の痕跡が含まれていないことを確認します。
D. 最新のエンドポイント保護署名が配置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: **215**
セキュリティ アナリストが最近のネットワーク キャプチャを確認し、TCP ポート 465 上の暗号化された受信トラフィックがデータベース サーバーから会社のネットワークに入っていることに気付きました。セキュリティ アナリストがこのポートのトラフィックの原因として最も多く特定する可能性が高いのは次のうちどれですか?
A. サーバーは新しい TLS 1.3 標準を使用して安全な接続を受信しています
B. トラフィックは、Windows サーバーが Microsoft に送信する一般的な静的データです。
C. 誰かが SSL 経由で未承認の SMTP アプリケーションを構成しました

D. データベースから Web フロントエンドへの接続がポート上で通信しています。
Answer: C (メーッセージを残す)

最新問題: **216**
情報セキュリティ アナリストは、仮想マシン サーバーが攻撃者によって侵害されたことを発見しました。インシデントを確認して対応するための最初のステップは次のうちどれですか? (2 つ選択してください)。
A. 仮想マシンを一時停止します。
B. 仮想マシンをシャットダウンします。
C. 仮想マシンのスナップショットを取得します。
D. 仮想マシンから NIC を削除します。
E. 仮想マシンのホスト ハイパーバイザー ログを確認します。
F. 仮想マシンの移行を実行します。
Answer: A,C (メーッセージを残す)
これらの手順は、さらなる分析と証拠収集のために侵害されたサーバーの状態を保存するため、インシデントを確認して対応するのに最適です。仮想マシンを一時停止すると、攻撃者によるさらなる変更や損害が防止され、スナップショットを作成すると、仮想マシンのメモリとディスクの内容のコピーが作成されます。

最新問題: **217**
セキュリティ アナリストがマルウェア分析ラボを構築しています。アナリストは、悪意のあるアプリケーションが仮想マシンを脱出して他のネットワークに移行できないようにしたいと考えています。
このリスクを最大限に軽減するには、アナリストは を使用する必要があります。
A. ラボ ネットワークを他のすべてのネットワークから分離するファイアウォール。
B. エア ギャップを作成する 802.11ac ワイヤレス ブリッジ。
C. ラボを別の VLAN にセグメント化するためのマネージド スイッチ。
D. 環境を相互にセグメント化するためのアンマネージド スイッチ。
Answer: (解答を表示する)

最新問題: **218**
セキュリティ アナリストは脆弱性スキャンの結果を確認しており、新しいワークステーションに古いウイルス対策シグネチャがあるとしてフラグが立てられていることに気付きました。アナリストは次のプラグイン出力を観察します。
アナリストはベンダーの Web サイトを使用して、サポートされている最も古いバージョンが正しいことを確認します。状況を最もよく説明しているものは次のうちどれですか?
A. これは真の陰性であり、新しいコンピュータには正しいバージョンのソフトウェアがインストールされています。
B. これは真陽性であり、新しいコンピューターは古いバージョンのソフトウェアでイメージ化されました。
C. これは誤検知であり、スキャン プラグインはベンダーによって更新される必要があります。
D. これは偽陰性であり、新しいコンピュータはデスクトップ チームによって更新される必要があります。
Answer: B (メーッセージを残す)

最新問題: **219**

企業のマーケティング電子メールがスパム フォルダーに見つかるか、まったく配信されません。セキュリティ アナリストは問題を調査し、問題の電子メールが会社に代わってサードパーティ in1marketingpartners.com によって送信されていることを発見しました。以下は既存の SPP ワードです。
電子メールがスパムとしてマークされたりブロックされたりするのを防ぐために、SPF レコードに対する次の更新のうち、最も効果的なのはどれですか?
A)
B)
C)
D)
A. オプション C
B. オプション D
C. オプション A
D. オプション B
Answer: D (メーッセージを残す**)**

最新問題**: 220**
セキュリティ アナリストは、組織内で使用できる 2 つの脆弱性管理ツールを評価しています。アナリストは、各ベンダーの指示に従って各ツールをセットアップし、同じターゲット サーバーに対して実行される脆弱性のレポートを作成しました。
ツール A は次のことを報告しました。
ツール B は次のことを報告しました。
各ツールで使用される方法を最もよく説明しているものは次のうちどれですか? (2つお選びください。)
A. ツール B は認証されていません。
B. ツール A は認証されていません。
C. ツール B はエージェントベースです。
D. ツール A はファジング ロジックを使用して脆弱性をテストしました。
E. ツール B は機械学習テクノロジーを利用しました。
F. ツール A はエージェントベースです。
Answer: (解答を表示する**)**

最新問題**: 221**
セキュリティ アナリストは、過去の SIEM アラートの対象となったマシンに対してフォレンジック分析を実行しています。
アナリストは、非共通ポートで SSL を利用した一部のネットワーク接続、%TEMP% フォルダ内の svchost.exe と cmd.exe のコピー、および外部 IP に接続されていた RDP ファイルに気づきました。
セキュリティ アナリストが発見した脅威は次のうちどれですか?
A. APT
B. DDoS
C. ランサムウェア
D. ソフトウェアの脆弱性
Answer: A (メーッセージを残す**)**

最新問題**: 222**

サイバーセキュリティ アナリストは、企業の内部ネットワーク上の複数のシステムに影響を与える潜在的なインシデントを調査しています。パフォーマンスへの影響はごくわずかですが、影響を受ける各システムに次の症状が発生します。
* 新しい予期しない svchost exe プロセスの存在
* ルーチンのキープアライブ転送による未知の外部ホストへの永続的なアウトバウンド TCP/IP 接続
* インターネットに常駐するダイナミック DNS ドメインの名前解決が成功したことを示す DNS クエリ ログ この状況が未解決のままである場合、最も可能性が高いのは次のうちどれですか?
A. 影響を受けるホスト上のキー ファイルが暗号化され、ロックを解除するには身代金の支払いが必要になる可能性があります。
B. 敵対者は中間者攻撃を実行しようとする可能性があります。
C. 攻撃者は、影響を受けるホストを利用して、会社のルーター ACL を再構成する可能性があります。
D. 影響を受けるホストは、コマンドによる協調的な DDoS 攻撃に参加する可能性があります。
Answer: D (メーッセージを残す**)**

最新問題: **223**
セキュリティ アナリストは、エンドポイント デバイスからの散発的な帯域幅消費に関する一連のイベントに対応しています。次に、セキュリティ アナリストは次の追加の詳細を特定します。
* ネットワーク使用率のバーストは、約 7 日ごとに発生します。
* 転送されるコンテンツは暗号化または難読化されているようです。
* ホストからサードパーティ クラウド内のインフラストラクチャへの別個の永続的なアウトバウンド TCP 接続が確立されています。
* デバイス上の HDD 使用率は、7 日ごとに 10 GB から 12 GB ずつ増加します。
※1ファイルサイズは10GBとなります。
問題の原因として最も考えられるものは次のうちどれですか?
A. メモリ消費量
B. 非標準ポートの使用
C. データの引き出し
D. システムアップデート
E. ボットネット参加者
Answer: C (メーッセージを残す**)**
データの引き出しとは、通常はスパイ活動、妨害行為、盗難などの悪意のある目的で、組織のネットワークから外部の宛先にデータを不正に転送することです。質問に記載されている詳細は、データの漏洩がエンドポイント デバイスから発生していることを示唆しています。7 日ごとのネットワーク使用率のバーストは、定期的なデータ転送を示しています。転送されるコンテンツは、検出や分析を避けるために暗号化または難読化されているようです。ホストからサードパーティ クラウド内のインフラストラクチャへの永続的なアウトバウンド TCP 接続は、攻撃者にとってコマンド アンド コントロール チャネルの可能性があることを示しています。デバイス上の HDD 使用率は 7 日ごとに 10 GB から 12 GB 増加し、単一ファイルのサイズは 10 GB です。これは、大量のデータが収集され、抽出される前に圧縮されていることを示しています。

最新問題: **224**
セキュリティ アナリストは、企業環境全体で特定のアクティビティを追跡するために、組織の脅威ハンティング チームに異動されました。アナリストは、このアクティビティが発生する回数を観察および評価し、結果を集計する必要があります。アナリストが使用するのに最適な脅威ハンティング方法は次のうちどれですか?
A. 検索中
B. クラスタリング
C. グループ化

D. スタックカウント
Answer: (解答を表示する**)**

最新問題**: 225**
セキュリティ アナリストは、侵害された認証サーバーを調査しているときに、次の隠しファイルを発見しました。
さらに分析すると、これらのユーザーはサーバーにログインしたことがないことがわかります。ファイルを取得するために使用された攻撃の種類は次のうちどれですか?また、この種類の攻撃の再発を防ぐためにアナリストは何を推奨する必要がありますか?
A. 不正な LDAP サーバーがシステムにインストールされており、パスワードを接続しています。アナリストは、サーバーを消去して再インストールすることを推奨する必要があります。
B. アカウントを侵害するためにレインボー テーブル攻撃が使用されました。アナリストは、将来のパスワード ハッシュにソルトを含めることを推奨する必要があります。
C. パスワード スプレー攻撃がパスワードを侵害するために使用されました。アナリストは、すべてのユーザーに固有のパスワードを受け取ることを推奨する必要があります。
D. フィッシング攻撃がアカウントを侵害するために使用されました。アナリストは、フィッシング リンクを無効にするためにエンドポイント保護をインストールすることをユーザーに推奨する必要があります。
Answer: (解答を表示する**)**

最新問題**: 226**
セキュリティ アナリストは、ホストがネットワーク上でアクティブかどうかを判断しようとしています。アナリストはまず次のことを試みます。
次にアナリストは次のコマンドを実行します。
結果の違いを説明できるのは次のうちどれですか?
A. ICMP はファイアウォールによってブロックされています。
B. ping と hping3 のルーティング テーブルが異なりました。
C. 元の ping コマンドを実行するには root 権限が必要でした。
D. hping3 は誤検知を返します。
Answer: A (メーッセージを残す**)**
説明

最新問題**: 227**
セキュリティ アナリストは、企業の SIEM コンソールでのインシデントを調査しているときに、SSH ログイン試行が数百回失敗し、すべて立て続けに発生していることを発見しました。失敗した試行の後に、root ユーザーでのログインが成功しました。会社のポリシーにより、システム管理者は、割り当てられた企業ログインを使用して会社の内部ネットワークからのみシステムを管理できます。さらなる侵害を阻止するためにアナリストが実行できる最善の行動は次のうちどれですか? (2 つ選択してください)。
A. 影響を受けるシステム上のすべてのアカウントのパスワードをリセットします。

B. SSH ユーザー セッションをブロックするルールをネットワーク IPS に追加します。
C. 送信元 IP アドレスをブロックするルールを境界ファイアウォールに追加します。
D. root ログインを拒否し、SSHD サービスを再起動するように /etc/passwd を構成します。
E. ポート TCP/22 へのアクセスをブロックするルールを影響を受けるシステムに追加します。
F. root ログインを拒否し、SSHD サービスを再起動するように /etc/sshd_config を構成します。
Answer: (解答を表示する**)**

最新問題**: 228**
ある企業は 1 年以上前にワイヤレス ネットワークを設置し、単一のサブネット内の同じモデルの AP を標準化しました。最近、インターネット閲覧のタイムアウトや接続の問題が複数のユーザーから報告されています。セキュリティ管理者は、ユーザーの協力を得て問題の再現を試みるため、ネットワークに関する情報を収集しました。
管理者はネットワーク上のすべてのデバイスに ping を実行し、ネットワークが非常に遅いことを確認できます。
出力：
上記の結果を考慮すると、管理者は次のどれを最初に調査する必要がありますか?
A. AP-IT デバイス
B. ユーザーの PC
C. AP-Workshop デバイス
D. 192.168.1.4 のデバイス
E. AP 受信デバイス
Answer: C (メーッセージを残す**)**

最新問題**: 229**
ある企業が複数の大量 DoS 攻撃の被害を受けています。問題のあるトラフィックのパケット分析により、次のことがわかります。
上記の攻撃に対して最も効果的な緩和手法は次のうちどれですか?
A. 企業は、ゲートウェイ NIPS の DoS リソース枯渇保護機能を有効にする必要があります。
B. 企業は、ゲートウェイ ファイアウォールに次の ACL を実装する必要があります:DENY IP HOST 192.168.1.1 170.43.30.0/24。
C. 企業は、ネットワークベースのシンクホールを実装して、次からのすべてのトラフィックをドロップする必要があります。
ゲートウェイ ルーターでは 192.168.1.1。
D. 企業は上流の ISP に連絡し、RFC1918 トラフィックをドロップするように依頼する必要があります。
Answer: (解答を表示する**)**

最新問題**: 230**
セキュリティ チームは、歴史的にセキュリティ体制が不十分な環境に新しい脆弱性管理プログラムを実装しています。チームは環境内のパッチ管理の問題を認識しており、多数の発見が得られることを期待しています。組織のセキュリティ体制を最短時間で強化する最も効率的な方法は次のうちどれですか?
A. さまざまなサーバーに存在するデータの分類基準を作成し、機密データを格納しているサーバーにのみ修復を提供します。
B. セキュリティ チームが運用環境にパッチを迅速に展開して、見つかった脆弱性のリスクを軽減できるようにする変更管理ポリシーを実装します。
C. 修復プロセスに優先順位レベルを組み込み、重要な発見事項に最初に対処します。
D. すべてのレベルの脆弱性について、発見から 30 日以内に修復アクションを実行する必要があることを示す SLA を作成します。
Answer: C (メーッセージを残す**)**

最新問題: **231**
セキュリティ アナリストは、組織内で使用できる 2 つの脆弱性管理ツールを評価しています。アナリストは、各ベンダーの指示に従って各ツールをセットアップし、同じターゲット サーバーに対して実行される脆弱性のレポートを作成しました。
ツール A は次のことを報告しました。
ツール B は次のことを報告しました。
各ツールで使用される方法を最もよく説明しているものは次のうちどれですか? (2つお選びください。)
A. ツール A はファジング ロジックを使用して脆弱性をテストしました。
B. ツール A は認証されていません。
C. ツール B は認証されていません。
D. ツール B は機械学習テクノロジーを利用しました。
E. ツール A はエージェントベースです。
F. ツール B はエージェントベースです。
Answer: (解答を表示する**)**

最新問題: **232**
フォレンジック アナリストが、インシデントに関係したワークステーションの画像を撮影しました。画像が改ざんされていないことを最も確実に確認するには、アナリストは以下を使用する必要があります。
A. バックアップ テープ
B. 保管過程。
C. 訴訟ホールド
D. ハッシュ
Answer: (解答を表示する**)**

最新問題: **233**
プロダクト マネージャーはアナリストと協力して、データ分析プラットフォームとして機能し、Web ブラウザーからアクセスできる新しいアプリケーションを設計しています。製品マネージャーは、PaaS プロバイダーを使用してアプリケーションをホストすることを提案します。PaaS ソリューションを使用する際にセキュリティ上の懸念があるのは次のうちどれですか?
A. コードとしてのインフラストラクチャ機能を使用すると、攻撃対象領域が増加します。
B. 基礎となるアプリケーション サーバーへのパッチ適用はクライアントの責任となります。
C. アプリケーションはデータベース レベルで暗号化を使用できません。
D. 安全でないアプリケーション プログラミング インターフェイスは、データの侵害につながる可能性があります。
Answer: (解答を表示する**)**
PaaS ソリューションを使用する場合、安全でないアプリケーション プログラミング インターフェイス (API) はデータの侵害につながる可能性があります。API は、アプリケーションが相互に通信したり、基礎となるプラットフォームと通信したりできるようにするインターフェイスです。API は、適切に設計、実装、または保護されていない場合、機密データや機能を未承認のユーザーや悪意のあるユーザーに公開する可能性があります。安全でない API は、データ侵害、サービス拒否、不正アクセス、コード インジェクションを引き起こす可能性があります。

最新問題: **234**
アナリストは、最近の脆弱性スキャンに基づいて推奨事項を提供する必要があります。

潜在的な脆弱性を確実に特定するために、アナリストは次のどれに対処することを推奨する必要がありますか?
A. SMB はドメイン SID を使用してユーザーを列挙します
B. SYN スキャナー
C. SSL 証明書は信頼できません
D. スキャンは管理者権限では実行されませんでした
Answer: (解答を表示する**)**
これは、脆弱性スキャンが一部のリソースにアクセスできなかったり、ターゲット システム上でより高い権限を必要とするアクションを実行できなかったことを示すため、潜在的な脆弱性を確実に特定するために対処する必要があります。これにより、一部の脆弱性が検出または検証されない可能性があるため、検出結果が欠落または不正確になる可能性があります。

最新問題**: 235**
アナリストは、侵入に関与している疑いのあるシステムを調査しています。
アナリストはコマンド `cat/etc/passwd' を使用し、次の部分的な出力を受け取ります。
上記の出力に基づいて、アナリストは次のどれをさらに調査する必要がありますか?
A. ユーザー `daemon' には /usr/sbin のホーム ディレクトリがあってはなりません
B. ユーザー `news' はデフォルトのシェル /bin/bash を持つべきではありません
C. ユーザー `mail' には /usr/sbin/nologin のデフォルト シェルがあってはなりません
D. ユーザー `root' には /root のホーム ディレクトリがあってはなりません
Answer: B (メーッセージを残す**)**

最新問題**: 236**
非産業用 IT ベンダーと比較して、ICS 機器ベンダーは一般的に次のような特徴を持っています。
A. ハードウェア製品の独自コードへの依存度が低くなります。
B. より成熟したソフトウェア開発モデルを持っています。
C. より高価な脆弱性レポートを提供します。
D. ソフトウェア アップデートのリリース頻度を下げます。
Answer: A (メーッセージを残す**)**

最新問題**: 237**
脆弱性スキャンにより、複数の Wiki サイトをホストする Web サーバーに対して次の結果が返されました。
Apache-HTTPD-cve-2014-023: Apache HTTPD: mod_cgid のサービス拒否 CVE-2014- mog_cgid で見つかった欠陥により、CGI スクリプトをホストするために mod_cgid を使用しているサーバーは、リモート攻撃者によって引き起こされる DoS 攻撃に対して脆弱になる可能性があります。非標準入力の弱点が悪用され、プロセスが無期限にハングアップします。
セキュリティ アナリストは、サーバーが Wiki サイトの標準 CGI スクリプトをホストしており、mod_cgid がインストールされておらず、Apache 2.2.22 を実行しており、WAF の背後にないことを確認しました。サーバーは DMZ 内に配置されており、サーバーの目的は、顧客が公的にアクセス可能なデータベースにエントリを追加できるようにすることです。
この発見に対処する最も効率的な方法は次のうちどれですか?
A. 検出結果を誤検知として文書化します。
B. HTTP サービスを無効にし、HTTPS のみを使用してサーバーにアクセスします。
C. Apache の最新バージョンにアップグレードします。

D. DoS 攻撃の発生を防ぐために、サーバーを WAF の背後に配置します。
Answer: (解答を表示する**)**

最新問題**: 238**
セキュリティ アナリストは次のサーバー統計を調査しています。
最も可能性が高いのは次のうちどれですか?
A. 競合状態
B. VM エスケープ
C. リソース枯渇
D. 権限昇格
Answer: C (メーッセージを残す**)**

最新問題**: 239**
セキュリティ アナリストは、情報セキュリティ通知メールボックスを監視しているときに、いくつかの電子メールがスパムとして再ポットされていることに気付きました。アナリストが最初に行うべきことは次のうちどれですか?
A. 電子メール ゲートウェイで送信者をブロックします。
B. 会社の電子メール サーバーから電子メールを削除します。
C. 送信者にメッセージの送信を停止するように依頼します。
D. 安全な環境でメッセージを確認します。
Answer: D (メーッセージを残す**)**
セキュリティ アナリストは、まず安全な環境でメッセージを確認する必要があります。これは、メッセージが実際にスパムであるかどうか、またはマルウェアの添付ファイルやフィッシング リンクなどの悪意のあるコンテンツが含まれているかどうかを判断するのに役立ちます。安全な環境でメッセージを確認するということは、アナリストのシステムやネットワークに対する潜在的な損害を防ぐことができるサンドボックスまたは分離されたシステムを使用することを意味します。メッセージがスパムまたは悪意のあるものであると確認された場合、アナリストは送信者のブロック、電子メールの削除、ユーザーへの通知などのさらなる措置を講じることができます3。

最新問題**: 240**
攻撃ベクトルを理解し、インテリジェンス ソースを統合することは、以下の重要な要素です。
A. インシデント対応計画。
B. リスク管理コンプライアンス。
C. 脆弱性管理計画。
D. プロアクティブな脅威ハンティング
Answer: C (メーッセージを残す**)**

最新問題**: 241**
フォレンジック アナリストが侵害されたサーバーで調査を行っています。証拠を保存するためにアナリストは次のどれを最初に行うべきですか。」
A. 破損したデータをバックアップ メディアから復元します
B. システム タイムラインを作成する
C. 侵害されたシステムへのユーザー アクセスを監視します
D. すべてのログ ファイルと監査証跡をバックアップします。

Answer: D (メーッセージを残す)
フォレンジックアナリストが侵害されたサーバーの調査を行っています。証拠を保存するためにアナリストが行うべき最初のステップは、すべてのログ ファイルと監査証跡をバックアップすることです。これにより、分析者は分析と検証に使用できる元のデータのコピーを確実に保持できるようになります。ログ ファイルと監査証跡をバックアップすると、攻撃者やその他の当事者による証拠の改ざんや変更も防ぐことができます。他のオプションは最初のステップではないか、証拠を変更または破壊する可能性があります。参考資料: CompTIA サイバーセキュリティ アナリスト (CySA+) 認定試験の目的 (CS0-002)、16 ページ。https://www.nist.gov/publications/guide-collection-and-preservation-digital-evidence

最新問題: **242**
レガシー アプリケーションの一部は、動的 SQL の使用を中止するためにリファクタリングされています。レガシー アプリケーションに実装するのに最適なものは次のうちどれですか?
A. 入力の検証
B. SQL インジェクション
C. Web アプリケーション ファイアウォール
D. パラメータ化されたクエリ
E. 多要素認証
Answer: E (メーッセージを残す)

最新問題: **243**
ソフトウェア開発チームはセキュリティ アナリストに、いくつかのコードにセキュリティの脆弱性がないかレビューするよう依頼しました。セキュリティ アナリストがこのタスクを実行する際に最も役立つのは次のうちどれですか?
A. 静的解析
B. 回帰テスト
C. ユーザー受け入れテスト
D. 動的分析
Answer: B (メーッセージを残す)

最新問題: **244**
XSS 攻撃によるセッション ID の盗難を防ぐのに役立つセッション管理手法は次のうちどれですか?
A. セッション識別子の長さが十分であることを確認する
B. 適切なセッション識別子エントロピーの作成
C. すべてのリクエストでトランスポート層暗号化を使用します。
D. HttpOnly フラグを使用したセッション Cookie の実装
E. セッション Cookie にセキュア属性を適用する
Answer: (解答を表示する)

最新問題: **245**
システム管理者は、実行中のさまざまなサービスの脆弱性を判断するために、企業の外部ネットワークのネットワーク偵察を行っています。いくつかのサンプル トラフィックを外部ホストに送信すると、管理者は次のパケット キャプチャを取得します。
出力に基づいて、次のどのサービスの脆弱性をさらにテストする必要がありますか?
A. HTTP
B. SSH
C. HTTPS
D. SMB
Answer: (解答を表示する**)**

最新問題: **246**
マネージャーはセキュリティ アナリストに、従業員の Web 閲覧履歴を提供するよう依頼しました。アナリストは次のうちどれを最初に行うべきですか?
A. 検索を実行する権限を取得します。
B. プロキシから Web 閲覧履歴を取得します。
C. 従業員のネットワーク ID を取得してクエリを作成します。
D. 閲覧履歴をダウンロードし、暗号化します。そしてそれをハッシュする
Answer: (解答を表示する**)**
これにはプライバシーや法的問題が含まれる可能性があるため、アナリストは従業員の Web 閲覧履歴にアクセスする前に、検索を実行する許可を取得する必要があります。アナリストは組織のポリシーと手順に従い、マネージャー、人事部、法務部などの適切な権限を得る必要があります。

最新問題: **247**
企業に PKI を実装する際、セキュリティ アナリストは、中間証明書の署名にのみ使用される certAcate 機関として専用サーバーを利用することを計画しています。認証局サーバーが使用されていないとき、最も安全な状態は次のうちどれですか? (2つ選択してください)
A. プライベート VLAN 上
B. フルディスク暗号化
C. 電源がオフになっています
D. 1 時間ごとにバックアップされます
E. VPN のみアクセス可能
F. エアギャップあり
Answer: (解答を表示する**)**
認証局サーバーが使用されていないときの最も安全な状態は、電源がオフでエアギャップが設定されている状態です。サーバーの電源をオフにすると、アイドル状態のサーバーへの不正アクセスや改ざんが防止されます。サーバーをエアギャップすると、サーバーがネットワーク接続から隔離され、リモートの攻撃者やマルウェアがアクセスできなくなります。これらの対策は、認証局サーバーとそのキーの整合性と機密性を保護するのに役立ちます。

最新問題: **248**
セキュリティ アナリストは、いくつかの既知のポートをスキャンしてファイアウォールの動作と応答をチェックすることを目的として、ファイアウォール ルールを監査しています。アナリストは次のコマンドを実行します。
ファイアウォール ルールを最もよく説明しているものは次のうちどれですか?
A. DNAt から宛先 1.1.1.1:3000

B. ドロップ
C. LOG -log-tcp-sequence
D. --tcp-reset で拒否
Answer: (解答を表示する**)**

最新問題**: 249**
一部の顧客がアカウントでの不正なアクティビティを報告しているため、セキュリティ アナリストは会社の API サーバーからのネットワーク パケット キャプチャを調査しています。キャプチャ ファイルの一部を以下に示します。
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/"><s:Body><GetIPLocation+xmlns="http: //tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance"></s:Body></s :エンベロープ> 192.168.1.22 - -
api.somesite.com 200 0 1006 1001 0 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="
true"/><a:Username>somebody@companyname.com</a:Username></request></Login></s:Body></s:Envelope> 192.168.5.66 - - api.somesite.com 200 0 11558 1712
2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation+xmlns="
http://tempuri.org/"> <a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:本文></s:エンベロープ> 192.168.1.22 - -
api.somesite.com 200 0 1003 1011 307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><IsLoggedIn+xmlns="
http://tempuri.org/"> <request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="http://www.w3.org /2001/XMLSchema-
instance"><a:Authentication>
<a:ApiToken>kmL4krg2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken><a:ImpersonateUserId>0</a:ImpersonateUserId><a:LocationId>161222</a:LocationId>
<
a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authentication></request>< /IsLoggedIn></s:Body></s:Envelope>
192.168.5.66 - - api.somesite.com 200 0 1378 1209 48 192.168.4.89
クライアントのアカウントがどのように侵害されたかを説明する可能性が最も高いのは次のうちどれですか?
A. SQL インジェクション攻撃がサーバー上で実行されました。
B. クライアントの認証トークンが偽装されて再生されました。
C. クライアントのユーザー名とパスワードはクリアテキストで送信されました。
D. XSS スクリプト攻撃がサーバー上で実行されました。
Answer: C (メーッセージを残す**)**

最新問題**: 250**
IT セキュリティ アナリストは、同社が最近購入した新しい車両の脆弱性に関する電子メール アラートを受け取りました。次の攻撃ベクトルのうち、最も可能性が高い脆弱性はどれですか?
A. SCADA
B. CAN バス
C. Modbus
D. IoT
Answer: B (メーッセージを残す**)**

説明
コントローラー エリア ネットワーク - CAN バスは、今日の自動車やその他のデバイスに搭載されている電子制御ユニット (ECU) が、信頼性の高い優先順位主導の方法で相互に通信できるように設計されたメッセージ ベースのプロトコルです。メッセージまたは 「フレーム」はネットワーク内のすべてのデバイスによって受信され、ホスト コンピューターは必要ありません。

最新問題: **251**
サイバーセキュリティ アナリストは現在、アクセス制御リストが適用された新しく導入されたサーバーをチェックしています。スキャンを実行すると、アナリストは次の結果のコード スニペットを受け取りました。
このスキャンの出力を説明しているものは次のうちどれですか?
A. アナリストは真陽性を発見しましたが、ステータス コードが正しくないため、禁止されたメッセージが示されています。
B. アナリストが誤検知を発見しました。ステータス コードが正しくないため、OK メッセージが表示されます。
C. アナリストが誤検知を発見しました。ステータス コードが正しくないため、サーバー エラー メッセージが表示されます。
D. アナリストは真陽性を発見しました。ステータス コードは正しく、ファイルが見つからないというエラー メッセージが表示されます。
Answer: D (メーッセージを残す**)**

最新問題: **252**
シミュレーション
開発者は最近、新しいコードを 3 つの Web サーバーにデプロイしました。毎日の自動外部デバイス スキャン レポートには、PCI DSS に基づく障害項目となるサーバーの脆弱性が示されます。
脆弱性が有効でない場合、アナリストは適切な手順を実行してスキャンをクリーンにする必要があります。
脆弱性が有効な場合、アナリストは発見結果を修正する必要があります。
ネットワーク図で提供される情報を確認した後、ステップ 2 タブを選択し、ドロップダウン オプションを使用してリストされた各サーバーの正しい検証結果と修復アクションを選択してシミュレーションを完了します。
説明書
ステップ 1: ネットワーク図に示されている情報を確認します。
ステップ 2: 与えられたシナリオで、脆弱性に対処するためにどの修復アクションが必要かを判断します。
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] ボタンを選択してください。

Answer:
WEB_SERVER01 = 真陽性
WEB_SERVER02 = 真陽性 = HTTP を無効にする
WEB_SERVER03 = 真陽性 = パブリック CA からの証明書を要求する
WEB_SERVER01: 有効 - SSL/TLS を実装します
WEB_SERVER02: 有効 - Cookie を経由して送信するときに安全な属性を設定します
HTTPSのみ
WEB_SERVER03: 有効 - CA 署名証明書を実装してください

最新問題: **253**
セキュリティ アナリストは次の Web サーバー ログを調査しています。
この問題を最もよく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. ディレクトリ トラバーサルのエクスプロイト
C. クロスサイト リクエスト フォージェリ
D. クロスサイト スクリプティング
Answer: B (メーッセージを残す)

最新問題: **254**
オンライン ゲーム会社がランサムウェア攻撃の影響を受けました。従業員が、ネットワークに接続中に会社支給のモバイル デバイスで SMS 攻撃を介して受信した添付ファイルを開いてしまいました。モバイル デバイスのフォレンジック分析中に役立つアクションは次のうちどれですか? (2 つ選択してください)。
A. 電話機を工場出荷時の設定にリセットします
B. 電話機を再起動し、最新のセキュリティ アップデートをインストールします。
C. それぞれの加工過程の文書化
D. 望ましくない可能性のあるプログラムをアンインストールします
E. 分析のためにモバイル デバイスのメモリ ダンプを実行します。
F. eFuse を参照してデバイスのロックを解除する
Answer: (解答を表示する)
保管過程を文書化することは、すべての証拠が正しく収集され、保存されていることを確認するのに役立つため、あらゆるデバイスのフォレンジック分析において重要なステップです。攻撃が発生したときのデバイスの状態に関する情報が得られ、さらなる分析に使用できるため、メモリ ダンプも不可欠です。
それぞれの保管過程を文書化すると、フォレンジック分析中にモバイル デバイスから収集された証拠の完全性と証拠能力を維持するのに役立ちます。保管管理とは、誰が、いつ、どこで、どのように、そしてなぜ証拠を処理、アクセス、または変更したかの記録です。分析のためにモバイル デバイスのメモリ ダンプを実行すると、プロセス、ネットワーク接続、暗号化キーなど、ランサムウェア攻撃に関する貴重な情報が含まれる可能性のある揮発性データをモバイル デバイスから抽出するのに役立ちます。メモリ ダンプは、メモリ (RAM) の内容をファイルまたはストレージ デバイスにコピーするプロセスです。

最新問題: **255**
システム管理者は重要なシステムを保護しようとしています。管理者はシステムをファイアウォールの内側に配置し、強力な認証を有効にし、このシステムのすべての管理者に必須のトレーニングへの参加を要求しました。
実装されているコントロールを最もよく説明しているものは次のうちどれですか?
A. 多層防御
B. 監査修復
C. アクセス制御
D. 多要素認証
Answer: A (メーッセージを残す)

最新問題: **256**
セキュリティ アナリストは定期的なログ レビュー中に、root ユーザーの Bash 履歴ログからは識別できない次のコマンドを発見しました。
アナリストが最初に調査すべきコマンドは次のうちどれですか?
A. 3 行目
B. 5 行目
C. 1 行目
D. 6 行目

E. 2 行目
F. 4 行目
Answer: E (メーッセージを残す**)**

最新問題: **257**
大手製薬会社のセキュリティ アナリストは、脅威インテリジェンス リソース組織から内部ユーザー用の資格情報を受け取りました。これには、企業アカウントのユーザー名と有効なパスワードが含まれています。セキュリティ運用監視の一環としてアナリストが最初に行うべきアクションは次のうちどれですか?
A. すべてのユーザー パスワードを変更して、悪意のある攻撃者がパスワードを使用できないようにします。
B. Mimikatz が使用されたことを示すイベント ID をイベント ログで検索します。
C. すべての従業員のマシンでスケジュールされたウイルス対策スキャンを実行し、悪意のあるプロセスを探します。
D. マルウェア感染の場合に、グループ内のすべてのユーザーのマシンを再イメージ化します。
Answer: B (メーッセージを残す**)**

最新問題: **258**
サイバーセキュリティ アナリストは現在、アクセス制御リストが適用された新しく導入されたサーバーをチェックしています。
スキャンを実行すると、アナリストは次の結果のコード スニペットを受け取りました。
このスキャンの出力を説明しているものは次のうちどれですか?
A. アナリストは真陽性を発見しました。ステータス コードは正しく、ファイルが見つからないというエラー メッセージが表示されます。
B. アナリストは真陽性を発見しましたが、ステータス コードが正しくないため、禁止されたメッセージが示されています。
C. アナリストが誤検知を発見しました。ステータス コードが正しくないため、OK メッセージが表示されます。
D. アナリストが誤検知を発見しました。ステータス コードが正しくないため、サーバー エラー メッセージが表示されます。
Answer: A (メーッセージを残す**)**

最新問題: **259**
オンライン ゲーム会社がランサムウェア攻撃の影響を受けました。従業員が、ネットワークに接続中に会社支給のモバイル デバイスで SMS 攻撃を介して受信した添付ファイルを開いてしまいました。モバイル デバイスのフォレンジック分析中に役立つアクションは次のうちどれですか? (2 つ選択してください)。
A. それぞれの加工過程の文書化
B. 望ましくない可能性のあるプログラムをアンインストールします
C. 分析のためにモバイル デバイスのメモリ ダンプを実行します
D. 電話機を工場出荷時の設定にリセットします
E. 電話機を再起動し、最新のセキュリティ アップデートをインストールします。
F. eFuse を参照してデバイスのロックを解除する
Answer: A,C (メーッセージを残す**)**

最新問題: **260**
数人の会計部門のユーザーが、職場に戻ってログインした後、ワークステーションの閲覧履歴に異常なインターネット トラフィックが記録されていると報告しています。ビルのセキュリティ チームは、会計部門のユーザーが会社に出勤した後、清掃スタッフがシステムを使用しているのが見つかったと IT セキュリティ チームに通知しました。日。この問題が再発するのを防ぐために、IT セキュリティ チームは次のどの手順を実行する必要がありますか? (2つお選びください。)
A. ワークステーションの不正使用を監視するためにカメラを設定します。
B. 会計グループに対して時間ベースの制限を通常の営業時間に設定するように NAC を構成します。
C. 会計部門のユーザーのみがワークステーションにアクセスできるように、必須のアクセス制御を構成します。
D. Web モニター アプリケーションをインストールして、営業時間外のインターネットの使用状況を追跡します。
E. ワークステーション アカウントのタイムアウトを 3 分にするポリシーを構成します。
Answer: B,E (メーッセージを残す)

最新問題: **261**
セキュリティ アナリストは、機密性の高い企業の価格情報が顧客に送信されたインシデントを解決しようとしています。この情報は、従業員が公開マーケティング資料に添付して意図せず送信したものと思われます。このインシデントが繰り返されるリスクを制限するには、次の構成変更のうちどれが最も効果的ですか?
A. マーケティング資料をサニタイズします。
B. 内部関係者の脅威手順を更新します。
C. クライアント アドレスをブロックリストに追加します。
D. DLP ルールとメタデータを更新します。
Answer: (解答を表示する)

最新問題: **262**
セキュリティ アナリストは、公開されている企業サーバーへのアクセスが非常に遅く、断続的に発生するという報告を受けました。
システムが侵害されている可能性があると考え、アナリストは次のコマンドを実行します。
上記のコマンドの出力に基づいて、アナリストが調査を進めるために次に実行すべきことは次のうちどれですか?
A. サーバー ログを調べて、Web アプリケーションの侵害を示すさらなる兆候を確認します。
B. /tmp/.t/tfile は不正な SSHD サーバーである可能性があるため、バイナリ分析を実行します。
C. kill -9 1325 を実行して負荷平均を下げ、サーバーを再び使用できるようにします。
D. crontab -r を実行します。rm -rf /tmp/.tto システム上のマルウェアを削除して無効にします。
Answer: A (メーッセージを残す)

最新問題: **263**
インシデント対応手順中に悪意のあるアーティファクトが収集されました。セキュリティ アナリストは、サンドボックスで実行してその機能や操作方法を理解することはできません。マルウェアの機能をさらに分析するには、次の手順のうちどれが最適ですか?
A. リバースエンジニアリング
B. 文字列の抽出
C. 動的分析
D. 静的解析
Answer: (解答を表示する)

最新問題: **264**

ある医療機関は最近、電話による支払いの受け付けを開始しました。管理者は、さまざまな種類のデータを保存することによる影響を懸念しています。次の種類のデータのうち、最も厳しい規制制約を受けるのはどれですか?
A. IP
B. PCI
C. PHI
D. PII
Answer: B (メーッセージを残す**)**

最新問題: **265**
サイバーセキュリティ アナリストは現在、Nessus を使用して複数の FTP サーバーをスキャンしています。スキャンの結果を受け取ったら、アナリストはさらにテストを行って、見つかった脆弱性が存在するかどうかを確認する必要があります。
アナリストは次のコード スニペットを使用します。
アナリストがチェックしている脆弱性は次のうちどれですか?
A. バッファオーバーフロー
B. SQL インジェクション
C. デフォルトのパスワード
D. フォーマット文字列攻撃
Answer: B (メーッセージを残す**)**

最新問題: **266**
セキュリティ アナリストは、ファイアウォール ログから特定されたプロキシ回避ソフトウェアをダウンロードしようとした内部システムからの悪意のあるトラフィックを調査していますが、宛先 IP はブロックされ、キャプチャされていません。アナリストが行うべきことは次のうちどれですか?
A. コンピュータをシャットダウンします。
B. スナップショットを取得します
C. Wireshark を使用してライブ データをキャプチャする
D. DNS ログが有効かどうかを確認します。
E. ネットワーク ログを確認します。
Answer: (解答を表示する**)**

最新問題: **267**
ホワイトは前夜のインシデント報告書を検討しており、セキュリティアナリストは企業のウェブサイトがpo mcaiのプロパガンダで改ざんされていることに気づきました。このタイプの俳優を最もよく表すのは次のうちどれですか?
A. ハクティビスト
B. 国民国家
C. 内部関係者の脅威
D. 組織犯罪
Answer: A (メーッセージを残す**)**
ハクティビストは、ハッキング技術を使用して政治的または社会的な大義や議題を推進する行為者の一種です。ハクティビストは、自分たちが反対したり反対したりする組織や政府の Web サイトやシステムをターゲットにし、自分たちの目的に関連したメッセージやプロパガンダでそれらを改ざんすることがよくあります。この場合、ハクティビストは企業の Web サイトを政治的プロパガンダで改ざんしました。

最新問題: **268**
サイバーセキュリティ アナリストが調査の前後にフォレンジック イメージの整合性を検証するために使用する必要があるツールは次のうちどれですか?
A. gzip
B. 文字列
C. ファイル
D. sha1sum
E. dd
Answer: (解答を表示する)

最新問題: **269**
ある製造会社は、消費者への自社製品の直接販売に参加することを決定しました。
同社は、既存のクラウド サービス プロバイダーを使用して、メイン サイトのサブドメインを電子商取引のポータルとして使用することにしました。公開後、サイトは安定しており、適切に機能しますが、一日の売上が好調だった後、サイトは競合他社のランディング ページにリダイレクトされ始めます。問題の原因を特定し、影響範囲を最小限に抑えるために、企業のセキュリティ チームが実行すべきアクションは次のうちどれですか?
A. サードパーティと協力して侵入テスト サービスを提供し、エクスプロイトが見つかるかどうかを確認します。
B. クラウド プロバイダーに問い合わせて DNS 攻撃の性質を判断し、影響を受ける他のクライアントを特定します。
C. DNS レコードをチェックして、Cname またはエイリアス レコードがサブドメインに設定されていることを確認します。
D. DNS レコードをチェックして、サブドメインに対して正しい MX レコードが確立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: **270**
セキュリティ アナリストは、クラウド評価の実行中に Prowler スキャンを実行し、レポート内に次の情報が生成されます。
Prowler レポートに基づくと、最も良い推奨事項は次のうちどれですか?
A. BusinessUsr アクセス キー 1 を削除します。
B. アクセスキー 1 を削除します。
C. Cloud Dev アクセス キー 1 を削除します
D. アクセスキー 2 を削除します。
Answer: (解答を表示する)

最新問題: **271**
ある組織は、必須ではないサービスをクラウド コンピューティング環境に移行したいと考えています。管理チームはコストを重視しており、12 時間という復旧時間の目標を達成したいと考えています。望ましい結果を達成するには、次のクラウド回復戦略のうちどれが最も効果的ですか?
A. すべてのサービスを別のインスタンスに複製し、インスタンス間の負荷分散を行います。
B. 同じクラウド プロバイダー内の別のリージョンへのアクティブなレプリケーションを備えたホット サイトを確立します。
C. 別のリージョンにある同じクラウド プロバイダーを使用してウォーム ディザスタ リカバリ サイトをセットアップします。
D. フェールオーバーに使用できる別のクラウド プロバイダーのコールド サイトを使用してシステムを構成します。
Answer: (解答を表示する)
別のリージョンに同じクラウド プロバイダーを使用してウォーム ディザスタ リカバリ サイトをセットアップすると、コストを低く抑えながら 12 時間の目標復旧時間 (RTO) を達成できます。ウォーム ディザスタ リカバリ サイトは、災害発生時にすぐに起動できる必須のハードウェアおよびソフトウェア コンポーネントの一部を備え

た、部分的に構成されたサイトです。ウォーム サイトは、事前構成されたコンポーネントを持たないコールド サイトよりも高速に復旧できますが、完全に構成され複製されたコンポーネントを備えたホット サイトよりもコストが低くなります。同じクラウド プロバイダーを使用すると、移行と同期のプロセスが簡素化され、別のリージョンを使用すると、リージョンの停止や災害を回避できます。

最新問題: **272**
PHI を狙うサイバー攻撃者が増加しているため、数百万の顧客から機密性の高いデータを収集するヘルスケア企業は、顧客のデータが組織の内部および外部で確実に保護されるソリューションを導入しています。次の対策のうち、損失を最もよく防ぐことができるのはどれですか。顧客の機密データについて?
A. 環境にセキュリティ リソースを追加します。
B. 多要素認証を実装する
C. 特権アクセス管理を実装する
D. リスク管理プロセスを実装する
Answer: (解答を表示する**)**

最新問題: **273**
セキュリティ アナリストは、電子メール セキュリティ サービスからの次のログを確認しています。
電子メールがブロックされた理由を最もよく説明しているものは次のうちどれですか?
A. To アドレスが無効です。
B. 電子メールは www.spamfilter.org URL から送信されました。
C. IP アドレスとリモート サーバー名が同じです。
D. IP アドレスはブラックリストに登録されました。
E. From アドレスが無効です。
Answer: (解答を表示する**)**
参考 :https://www.webopediA.com/TERM/R/RBL.html

最新問題: **274**
企業は FTP サーバーを使用して重要なビジネス機能をサポートしています。FTP サーバーは次のように構成されています。
* FTP サービスは、/opt/ftp/data に設定されたデータ ディレクトリで実行されています。
* FTP サーバーは従業員の自宅をホストしており、/home 内のベクトル
* 従業員は機密情報をホーム ディレクトリに保存する場合があります
LoC により、FTP ディレクター/トラバーサル攻撃により機密データが消失したことが明らかになりました。FTP サーバーを標的とした現在および将来のディレクトリトラバーサル攻撃のリスクを軽減するには、サーバー管理者が次のどれを実装する必要がありますか?
A. 機密ファイルのファイルレベルの暗号化を実装します。
B. FTPS をサポートするように FTP サーバーを再構成します
C. FTP サーバーを chroot 環境で実行します。

D. FTP サーバーを最新バージョンにアップグレードします
Answer: C (メーッセージを残す**)**
これにより、FTP サーバーのアクセスが特定のディレクトリ ツリーに制限され、そのツリーの外部のファイルにアクセスする可能性のあるディレクトリ トラバーサル攻撃が防止されます。ファイル レベルの暗号化の実装、FTPS のサポート、または FTP サーバーのアップグレードを行っても、ディレクトリ トラバーサル攻撃は防止できません。

最新問題**: 275**
次の結果を確認してください。
次のうちどれが発生しましたか?
A. 172.29.0.109 はトロイの木馬に感染しています。
B. 172.29.0.109 はワームに感染しています。
C. これは通常のネットワーク トラフィックです。
D. 123.120.110.212 はトロイの木馬に感染しています。
Answer: C (メーッセージを残す**)**

最新問題**: 276**
脅威インテリジェンス部門は最近、システム ルーターを悪用する新種のマルウェアを悪用する高度な永続的脅威を知りました。同社は現在、脅威レポートで言及されているのと同じデバイスを使用しています。次の構成変更のうち、組織のセキュリティ体制を最も改善するのはどれですか?
A. 高度な持続的脅威からの IP アドレスを含む IPS ルールを実装し、脆弱性から保護するためにルーターにパッチを適用します。
B. マルウェア亜種のコンテンツを含む IPS ルールを実装し、脆弱性から保護するためにルーターにパッチを適用します。
C. マルウェア亜種のコンテンツを含む IDS ルールを実装し、脆弱性から保護するためにルーターにパッチを適用します。
D. 高度な持続的脅威からの IP アドレスを含む IDS ルールを実装し、脆弱性から保護するためにルーターにパッチを適用します。
Answer: B (メーッセージを残す**)**

最新問題**: 277**
これを防ぐには、クエリをパラメータ化することが重要です。
A. セキュリティの脆弱性のある古いライブラリを使用したクエリ。
B. データベースに対する不正なアクションの実行。
C. 不正アクセスを許可する Web シェルの確立。
D. 昇格した特権でコードを実行するメモリ オーバーフロー。
Answer: B (メーッセージを残す**)**

最新問題**: 278**
インシデント対応チームは、クレジット カードのデータにアクセスした可能性のある悪意のあるソフトウェアを検出しました
ａ.インシデント対応チームは重大な損害を軽減し、是正措置を講じることができました。インシデント対応メカニズムを整備することによって。学んだ教訓について通知する必要があるのは次のうちどれですか?
A. 会社のリーダーシップ
B. 顧客
C. 法務チーム
D. 人事部

Answer: C (メーッセージを残す)

最新問題: **279**
ヘルプ デスクの技術者が、会社の CRM n の認証情報を平文で従業員の個人電子メール アカウントに誤って送信してしまいました。その後、技術者は適切なプロセスと従業員の会社メールを使用して従業員のアカウントをリセットし、セキュリティ チームにインシデントを通知しました。インシデント対応手順に従って、セキュリティ チームが次に行うべきことは次のうちどれですか?
A. インシデント概要レポートを作成します。
B. CRM ベンダーに問い合わせてください。
C. インシデント対応計画を更新します。
D. 事後データの相関関係を実行します。
Answer: D (メーッセージを残す)

最新問題: **280**
アナリストがエンドユーザー PC でリッスンしているポートを確認するために使用するコマンド ライン ユーティリティは次のうちどれですか?
A. トレースト
B. netstat
C. ping
D. nslookup
Answer: B (メーッセージを残す)

最新問題: **281**
セキュリティ アナリストは、ウイルス感染の症状のあるモバイル デバイスを受け取りました。ウイルスは、分析のためにサンドボックスからサンドボックスへと移動するたびに変化します。分析ライフサイクル全体を通じてバリエーションの数を特定するのに役立つのは次のうちどれですか?
A. ハッシュ ユーティリティ
B. ジャーナリング
C. ログビューア
D. OS とプロセスの分析
Answer: (解答を表示する)

最新問題: **282**
プロジェクト リーダーは、組織の内部および外部のネットワーク インフラストラクチャの潜在的な弱点を特定することに重点を置いた、今後のプロジェクトの作業明細書をレビューしています。
プロジェクトの一環として、外部請負業者のチームが組織に対してさまざまな攻撃を試みます。この作業記述書では、インフラストラクチャの弱点を示す論理図を作成するために、ネットワーク リソースを調査するための自動化ツールの利用について具体的に取り上げています。
作業明細書に記載されている活動範囲は、次の例です。
A. 脆弱性スキャン
B. フレンドリーな DoS
C. 侵入テスト
D. ソーシャル エンジニアリング
E. セッションハイジャック

Answer: C (メーッセージを残す)

最新問題: **283**
攻撃ベクトルを理解し、インテリジェンス ソースを統合することは、以下の重要な要素です。
A. プロアクティブな脅威ハンティング
B. リスク管理コンプライアンス。
C. 脆弱性管理計画。
D. インシデント対応計画。
Answer: (解答を表示する)
脅威ハンティング活動。
1. 仮説を立て、
2. 脅威アクター/活動のプロファイリング、
3. 脅威ハンティング戦術、
4. 攻撃対象領域の削減、
5. 重要なシステム/資産をグループ/保護ゾーンにバンドルします。
6. 攻撃ベクトルを理解、評価、対処する
7. 統合されたインテリジェンス
8. 検出機能の向上。

最新問題: **284**
ある企業は、5 ～ 10 人の従業員をサポートするために小規模なリモート オフィスを設立しています。会社のホーム オフィスは別の都市にあり、そこでビジネス アプリケーションにはクラウド サービス プロバイダーを、データのホストにはローカル サーバーを使用しています。リモート オフィスからローカル サーバーおよびビジネス アプリケーションへの共有アクセスを提供するには、次のうち最も簡単で安全なソリューションはどれですか?
A. VPC を使用して会社のデータをホストし、ビジネス アプリケーションの現在のソリューションを維持します。
B. リモート オフィスに新しいサーバーを使用してデータをホストし、ビジネス アプリケーションの現在のソリューションを維持します。
C. ホーム オフィスには VDI を使用し、ビジネス アプリケーションには現在のソリューションを維持します。
D. VPN を使用してホーム オフィスにある会社のデータにアクセスし、ビジネス アプリケーションの現在のソリューションを維持します。
Answer: (解答を表示する)
正解は D です。VPN を使用してホーム オフィスにある会社のデータにアクセスし、ビジネス アプリケーションの現在のソリューションを維持します。仮想プライベート ネットワーク (VPN) は、インターネットなどのパブリック ネットワーク上に安全で暗号化された接続を作成するテクノロジーです。VPN を使用すると、ユーザーは同じローカル ネットワーク上にいるかのように、サーバーなどのリモート ネットワーク上のリソースにアクセスできます。VPN を使用すると、セキュリティとプライバシーを維持しながら、リモート オフィスからホーム オフィスにある会社のデータへの共有アクセスを提供できます1。

最新問題: **285**
企業は顧客データの侵害の疑いについて知らされました。内部監査チームは法務部門と連携し、サイバーセキュリティ チームと協力して報告書の検証を開始しました。企業は調査中に次のどの対応プロセスに従う必要がありますか?
A. セキュリティ アナリストはシステム オペレーターにインタビューし、その結果を内部監査人に報告する必要があります。
B. セキュリティ アナリストは、インシデントが発生したときに違反の疑いを規制当局に報告する必要があります。
C. セキュリティ アナリストは、調査を実施する信頼できる関係者への通信を制限する必要があります。

D. セキュリティ アナリストは、アクティブな調査中に内部監査リクエストに応答すべきではありません
Answer: C (メーッセージを残す**)**

最新問題: **286**
最近のセキュリティ侵害を受けて、ある企業はアカウントの使用状況を調査して、特権アカウントが通常の営業時間中にのみ使用されていることを確認することにしました。調査の過程で、セキュリティ アナリストは、アカウントが深夜に継続的に使用されていたことを確認しました。
アナリストが次に取るべきアクションは次のうちどれですか?
A. インシデント対応計画を開始します。
B. ユーザーと一緒にアクティビティを確認します。
C. 特権アカウントを無効にします
D. 不一致を人事部に報告します。
Answer: B (メーッセージを残す**)**

最新問題: **287**
金融組織は世界中にオフィスを構えています。組織のポリシーと手順に従って、海外で事業を行うすべての幹部は、帰国時にモバイル デバイスに悪意のあるソフトウェアや改ざんの痕跡がないか検査を受ける必要があります。情報セキュリティ部門がこのプロセスを監督しており、デバイスが侵害された幹部は一人もいない。最高情報セキュリティ責任者は、組織のデータを保護するために追加の保護手段を導入したいと考えています。デバイスが盗難された場合にデータのプライバシーを保護するには、次の制御のうちどれが最も効果的ですか?
A. すべてのモバイル デバイスに暗号化ソリューションをインストールします。
B. DLP ソリューションを今すぐインストールしてデータを追跡します
C. デバイスの紛失または盗難に備えて、モバイル デバイスのワイプ ソリューションを実装します。
D. ラップトップの紛失または盗難を直ちにセキュリティ部門に報告するように従業員をトレーニングします。
Answer: C (メーッセージを残す**)**

最新問題: **288**
脅威フィードでは、ゼロデイ脆弱性の LoC として使用されるファイルのリストが公開されました。サイバーセキュリティ アナリストは、次のメカニズムとして、エンドポイントのログイン スクリプトにこれらのファイルのカスタム ルックアップを含めることを決定しました。
A. マルウェア シグネチャの作成を自動化します。
B. 脅威インテリジェンス サイクル ループを閉じます。
C. TAXII サーバーの STIX オブジェクトを生成します
D. 既存の検出機能を改善します。
Answer: D (メーッセージを残す**)**

アナリストは、ログイン中にこれらのファイルのいずれかがエンドポイントに存在するかどうかを確認することで、既存の検出機能を向上させるメカニズムとして、エンドポイントのログイン スクリプトにこれらのファイルのカスタム ルックアップを含めることにしました。これは、ゼロデイ脆弱性によって感染した可能性がある侵害されたエンドポイントを特定し、アナリストにさらなる調査や対応を促すのに役立ちます。

最新問題: **289**
建物の封鎖されたセクションがインターネットに接続できない セキュリティ アナリスト。セキュリティ アナリストが私の問題を調査しましたが、企業 Web プロキシへの接続は確認されませんでした。ただし、アナリストは、インターネットへのトラフィックがわずかに急増していることに気付きました。ヘルプ デスク技術者は、すべてのユーザーが接続 SSID に接続していることを確認します。しかし、ネットワーク接続には同じ SSID が 2 つリストされています。何が起こってい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. 帯域幅の消費量
B. ビーコン送信
C. サービス拒否
D. ネットワーク上の不正なデバイス
Answer: (解答を表示する**)**

最新問題: **290**
情報セキュリティ アナリストは、サーバー上の脆弱性スキャン結果を確認しているときに、次のことに気づきました。
アナリストが開発者に推奨する最も適切なアクションは、Web サーバーを次のように変更することです。
A. TLSvl 2 のみを受け入れます
B. AES と SHA を使用した暗号スイートのみを受け入れます
C. 脆弱な暗号スイートは受け入れられなくなりました
D. SSL/TLS は WAF とロード バランサーにオフロードされます
Answer: C (メーッセージを残す**)**
暗号スイートは、安全な通信セッション中にデータの暗号化、認証、整合性がどのように実行されるかを定義する一連のアルゴリズムです。一部の暗号スイートは、攻撃者によって簡単に破られたり侵害されたりする可能性がある、時代遅れまたは安全でないアルゴリズムを使用しているため、脆弱または弱いと考えられています。脆弱性スキャンの結果は、Web サーバーが RC4、MD5、DES などのいくつかの脆弱な暗号スイートを受け入れていることを示しています。アナリストが開発者に推奨する最善のアクションは、脆弱な暗号スイートを受け入れず、安全な暗号スイートのみを受け入れるように Web サーバーを変更することです。TLSv1.2 のみを受け入れるように Web サーバーを変更する、AES および SHA を使用する暗号スイートのみを受け入れるようにする、または SSL/TLS を WAF およびロード バランサーにオフロードするなどのアクションも考えられますが、Web サーバーを変更するほど具体的でも効果的でもありません。そのため、脆弱な暗号スイートは受け入れられなくなりました。参考: https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/

最新問題: **291**
ネットワーク セキュリティ アナリストのチームは、ネットワーク トラフィックを調査して、機密データが流出したかどうかを判断しています。さらなる調査の結果、アナリストは機密データが侵害されたと考えています。この種の機密データの漏洩に対して最も効果的に防御できるのは、次の機能のうちどれですか?
A. エッジ ファイアウォールを展開します。
B. DLP を実装する
C. EDR を展開します。
D. ハードドライブを暗号化します
Answer: (解答を表示する**)**

DLP (Data Loss Prevention) は、データ侵害を検出して防止するサイバーセキュリティ ソリューションです。機密データの抽出をブロックし、データの不正または不適切な共有、転送、使用を防ぎます。また、組織がデータ保護規制やポリシーに準拠するのにも役立ちます1。DLP は、ネットワーク、デバイス、アプリケーション、クラウド サービス間のデータ移動を監視および制御することで、機密データの漏洩を防ぐのに役立ちます。DLP は、ユーザーが信頼できない宛先または受信者に機密データを送信またはアップロードすることを警告またはブロックすることもできます。

最新問題: **292**
ある企業は、パッシブなネットワーク監視を可能にする環境を構成したいと考えています。機密性の高いネットワークの中断を避けるために、会社の要求に応えるためにスキャナの NIC でサポートされている必要があるものは次のうちどれですか?
A. 無差別モード
B. 全二重モード
C. ポートミラーリング
D. ポートブリッジング
E. トンネルオールモード
Answer: (解答を表示する**)**

最新問題: **293**
アナリストは、すべての Apache サーバーに対する技術的なセキュリティ コンプライアンス チェックの準備をしています。次のうちどれを使用するのが最適ですか?
A. CIS ベンチマーク
B. カインとアベル
C. ナギオス
D. OWASP
E. 乱雑
Answer: (解答を表示する**)**

最新問題: **294**
セキュリティ アナリストは、異常なアクティビティを特定するために次のログ エントリを調査しています。
次の攻撃タイプのうちどれが発生していますか?
A. バッファオーバーフロー
B. SQL インジェクション
C. ディレクトリ トラバーサル
D. クロスサイト スクリプティング
Answer: (解答を表示する**)**

最新問題: **295**
顧客サイトでの物理的侵入テスト中に、地元の法執行官がテストに遭遇し、チームの正当性に疑問を呈しました。
次の情報のうち、警察官に提示すべき情報はどれですか?
A. タイミング情報
B. 作業範囲
C. チームレポート
D. 婚約書

Answer: D (メーッセージを残す)

最新問題: **296**
企業の変更管理チームは、電子メール サーバーが運用環境にリリースされる前に、電子メール サーバーに対する潜在的な変更をレビューするようセキュリティ アナリストに依頼しました。アナリストは次の変更リクエストをレビューします。
変更の理由として最も考えられるのは次のうちどれですか?
A. ネットワークに対して認証されていないユーザーからの電子メールを拒否します。
B. 会社のドメインへの電子メールを受け入れるため。
C. SPF レコードにリストされていないサーバーからの電子メールを拒否するには
D. デジタル署名されていない電子メール アドレスからの電子メールを拒否します。
Answer: C (メーッセージを残す)

最新問題: **297**
HSM を最もよく説明しているのは次のうちどれですか?
A. 暗号化を管理し、トラフィックを復号化し、ライブラリ呼び出しを維持するコンピューティング デバイス
B. デジタル キーを管理し、暗号化/復号化機能を実行し、その他の暗号化機能を維持するコンピューティング デバイス
C. 物理キーを管理し、デバイスを暗号化し、強力な暗号化機能を作成するコンピューティング デバイス
D. アルゴリズムを管理し、エントロピー関数を実行し、デジタル署名を維持するコンピューティング デバイス
Answer: B (メーッセージを残す)
HSM (ハードウェア セキュリティ モジュール) は、デジタル キーを管理し、暗号化/復号化機能を実行し、その他の暗号化機能を維持するコンピューティング デバイスです2。HSM は、暗号キーのライフサイクルを保護するために特別に設計された専用の暗号プロセッサです。HSM は、暗号化、認証、デジタル署名、その他のセキュリティ機能に使用される暗号キーを保存できます。HSM は、各デバイスに固有でチップから離れることのないランダム キーを生成することもできます。HSM は、ハードウェアの分離と暗号化を使用して、これらのキーを不正アクセスや改ざんから保護できます3。HSM は、アテステーションと呼ばれるプロセスを使用して、デバイス上のオペレーティング システムとファームウェアの整合性を測定および検証することもできます。暗号化は秘密コードを作成および使用する科学または技術であるため、HSM は暗号化 (A) を管理しません。物理キーは何かをロックまたはロック解除するために使用される有形のオブジェクトであるため、HSM は物理キーを管理しません。アルゴリズムは問題を解決したりタスクを実行したりするために使用される一連のルールまたは命令であるため、HSM はアルゴリズム (D) を管理しません。

最新問題: **298**
セキュリティ アナリストは、vhost-paymonts .conf ファイルへの変更に基づくタイル整合性監視イベントについて警告を受けました。既知の正常なバックアップに対する diff コマンドの出力は次のようになります。
次のうち、最も可能性が高いのはどれですか?
A. カードに請求せずに支払いを受け入れるようにファイルが変更されました
B. クレジット カード情報の記録を避けるためにファイルが変更されました
C. カード番号が有効であることを確認するためにファイルが変更されました。
D. クレジット カード番号を収集するためにファイルが変更されました
Answer: B (メーッセージを残す)

最新問題: **299**
セキュリティ アナリストは、重要なシステムの高レベルのメモリ消費に関する SIEM アラートを受け取りました。

問題を修復しようと数回試みた後、システムがダウンしました。根本原因の分析により、悪意のある攻撃者がアプリケーションにメモリを再利用させないよう強制したことが判明しました。これにより、システムのリソースが枯渇してしまいました。
この攻撃を最もよく説明しているのは次のうちどれですか?
A. インジェクション攻撃
B. メモリ破損
C. サービス拒否
D. アレイ攻撃
Answer: C (メーッセージを残す**)**
参照: https://economictimes.indiatimes.com/definition/memory-corruption

最新問題**: 300**
サイバーセキュリティ アナリストは、Web 脆弱性スキャン ログのいくつかの結果を確認するように依頼されました。
次のコードのスニペットがあるとします。
状況と行うべき推奨事項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. セキュリティ アナリストは、ソース IP 65.240.22.1 ネットワークを指す埋め込み iframe を発見しました。
コードにはドメイン名を含める必要があります。ドメイン名を使用してエントリを更新することをお勧めします。
B. セキュリティ アナリストは、Web ページにアクセスするユーザーから隠されている埋め込み iframe を発見しました。このコードは正しいです。これは設計上の設定であり、脆弱性は存在しません。
C. セキュリティ アナリストは、ソース IP 65.240.22.1 ネットワークを指す埋め込み iframe を発見しました。
リンクは隠されており、疑わしいです。Web ページからエントリを削除することをお勧めします。
D. セキュリティ アナリストは、ソース IP 65.240.22.1 ネットワークを指している埋め込み iframe を発見しました。
iframe を表示することをお勧めします。コードを修正すると問題が解決します。
Answer: B (メーッセージを残す**)**

最新問題**: 301**
セキュリティ アナリストはコンピューター犯罪捜査を支援しており、PC を確保して科学捜査研究所に届けるよう依頼されました。PC を保護するために最も役立つものは次のうちどれですか? （3つお選びください。）
A. ドライブイレーザー
B. 書き込みブロッカー
C. 改ざん防止シール
D. マルチメーター
E. ファラデーケージ
F. ネットワークタップ
G. 加工管理フォーム
Answer: C,E,G (メーッセージを残す**)**

最新問題: **302**
ある組織は、Web サーバーを強化し、潜在的な攻撃者によって公開される可能性のある情報を削減しようとしています。セキュリティ アナリストは、最近の Web サーバー スキャンの脆弱性スキャン結果を検討しています。
スキャン結果の一部を以下に示します。
次の行のうち、修復する必要があるホストに関する情報の開示を示しているものはどれですか?
A. 調査結果#5144322
B. 初めて検出 2015 年 11 月 10 日 09:00 GMT-0600
C. アクセス パス: http://myOrg.com/mailingList.htm
D. リクエスト: GET http://myOrg.com/mailingList.aspx?content=volunteer
E. 応答: :\Documents\MarySmith\mailingList.pdf
Answer: E (メーッセージを残す**)**

最新問題: **303**
組織には次のリスク軽減ポリシーがあります。
* 補償制御のないリスクは、nsk 値が 50,000 ドルを超える場合に最初に軽減されます。
※その他のnsk軽減策はリスク値に応じて加算されます。
次のリスクが確認されています。
リスク軽減の優先順位は、高い順から次のどれですか?
A. C、B、A、D
B. D、C、B、A
C. A、C、D、B
D. C、D、A、B
E. B、C、D、A
Answer: D (メーッセージを残す**)**

最新問題: **304**
セキュリティ アナリストは、ランサムウェアが会社のいくつかのワークステーションのディスクを暗号化したというインシデントを処理しています。今後この種のインシデントを防ぐために最も効果的なのは次のうちどれですか?
A. 仮想マシンの毎日のスナップショットを使用してすべてのエンドポイントを仮想化します。
B. ステートフル ファイアウォールの代わりに UTM を実装し、ゲートウェイ ウイルス対策を有効にします。
C. ワークステーションをバックアップして、リカバリを容易にし、ゴールド イメージを作成します。
D. ランサムウェア認識プログラムを確立し、安全で検証可能なバックアップを実装します。
Answer: B (メーッセージを残す**)**

最新問題: **305**

セキュリティ アナリストは定期的なログ レビュー中に、root ユーザーの Bash 履歴ログからは識別できない次のコマンドを発見しました。
アナリストが最初に調査すべきコマンドは次のうちどれですか?
A. 1 行目
B. 3 行目
C. 6 行目
D. 5 行目
E. 2 行目
F. 4 行目
Answer: (解答を表示する**)**

最新問題**: 306**
セキュリティ アナリストは、企業ネットワークから 3 層クラウド環境への安全な接続を開発学習に提供する必要があります。開発者は、さまざまな構成タスクを実行するために、3 つの層すべてのサーバーにアクセスする必要があります。安全なトランスポートを提供するために、アナリストは次のテクノロジーのうちどれを実装する必要がありますか?
A. CASB
B. VPC
C. フェデレーション
D. VPN
Answer: D (メーッセージを残す**)**
VPN と VPC の違いは何ですか?
仮想プライベート ネットワーク (VPN) がパブリック インターネット上で安全なデータ転送を提供するのと同様に、VPC は民間企業とパブリック クラウド プロバイダーの間で安全なデータ転送を提供します。
VPN (Virtual Private Network) は、企業ネットワークからクラウド環境への安全な接続を提供するテクノロジーです。VPN は 2 つのネットワーク間に暗号化されたトンネルを作成し、開発者がトラフィックを傍受や改ざんにさらすことなく、クラウド環境の 3 層すべてのサーバーにアクセスできるようにします。VPN は、開発者の ID と権限を確認するための認証および認可メカニズムも提供します。

最新問題**: 307**
企業はすべてのデータをクラウドに保存します。現在、会社所有のラップトップはすべて管理されておらず、すべてのユーザーが管理者権限を持っています。セキュリティ チームは、環境を保護する方法を特定するのに苦労しています。会社のデータを保護する最善の方法は次のうちどれですか?
A. システムに UEM を実装し、セキュリティ ソフトウェアを導入します。
B. すべてのワークステーションに DLP を実装し、企業データが社外に送信されるのをブロックします。
C. CASB を実装し、特定の種類のデータがワークステーションにダウンロードされないようにする
D. 企業システムの集中監視とログ記録を実装します。
Answer: (解答を表示する**)**
Cloud Access Security Broker (CASB): あらゆる種類のデバイスにわたるユーザーによるクラウド サービスへのアクセスを仲介するように設計されたエンタープライズ管理ソフトウェア

最新問題**: 308**
セキュリティ アナリストは、従業員が退職前にネットワーク上で従業員の PII に関わる悪意のある活動を計画している証拠を示す電子メールを数件受け取ったと警告しました。セキュリティ アナリストの最善の対応は、法務部門と調整して次のことを行うことです。

A. 上級幹部
B. 広報部
C. 法執行機関
D. 人事部
Answer: D (メーッセージを残す)

最新問題: **309**
システムの操作権限 (ATO) は 4 日後に期限切れになるように設定されています。他の活動と限られた人員のため、この組織はこれまで再認証活動の開始を怠ってきました。サイバーセキュリティ グループは脆弱性スキャンを実行し、以下に示す結果の一部を取得しました。
シナリオと脆弱性スキャンの出力に基づいて、セキュリティ チームはこの発見に対して次のどれを行う必要がありますか?
A. 無視します。これは誤検知であり、組織は他の発見に注力する必要があります。
B. サーバーを再起動して、HTTP 検証が有効になっていることを確認します。
C. Web 構成ファイルに移動し、HTTP 検証を強制する設定を検索し、正しい設定に手動で更新することで修復します。
D. これは重大度が 「高」であるため、現時点ではこのリスクを受け入れてください。ただし、テストには利用可能な 4 日以上の時間が必要であり、システム ATO と競合する必要があります。
Answer: (解答を表示する)

最新問題: **310**
ネットワーク インフラストラクチャのレビューを行っているセキュリティ アナリストは、コア スイッチに接続され、机の後ろに隠されているラップトップを発見しました。
アナリストはラップトップの画面に次の情報を表示します。
セキュリティアナリストがとるべき最善の行動は次のうちどれですか?
A. ネットワーク上のデバイスのスキャンを開始して、パスワード解析ツールを見つけます。
B. ドメイン内のすべてのユーザーに次回ログイン時にパスワードの変更を強制します。
C. ラップトップを切断し、ユーザー jsmith と proger にログアウトするように依頼します。
D. FILE-SHARE-A サーバーをオフラインにして、ウイルスをスキャンします。
Answer: D (メーッセージを残す)

最新問題: **311**
システムの操作権限 (ATO) は 4 日後に期限切れになるように設定されています。他の活動と限られた人員のため、この組織はこれまで再認証活動の開始を怠ってきました。サイバーセキュリティ グループは脆弱性スキャンを実行し、以下に示す結果の一部を取得しました。
シナリオと脆弱性スキャンの出力に基づいて、セキュリティ チームはこの発見に対して次のどれを行う必要がありますか?
A. これは重大度が 「高」であるため、現時点ではこのリスクを受け入れてください。ただし、テストには利用可能な 4 日を超える時間が必要であり、システム ATO を競合させる必要があります。
B. 無視します。これは誤検知であり、組織は他の発見に注力する必要があります。
C. Web 構成ファイルに移動し、HTTP 検証を強制する設定を検索し、正しい設定に手動で更新することで修復します。
D. サーバーを再起動して、HTTP 検証が有効になっていることを確認します。
Answer: C (メーッセージを残す)

最新問題: **312**
セキュリティ アナリストは、電子メール セキュリティ サービスからの次のログを確認しています。
電子メールがブロックされた理由を最もよく説明しているものは次のうちどれですか?
A. 電子メールは www.spamfilter.org URL から送信されました。
B. IP アドレスはブラックリストに登録されました。
C. To アドレスが無効です。
D. IP アドレスとリモート サーバー名が同じです。
E. From アドレスが無効です。
Answer: B (メーッセージを残す**)**

最新問題: **313**
SNMP の脆弱性を悪用したネットワーク攻撃が検出されました。
サイバーセキュリティアナリストが最初にすべきことは次のうちどれですか?
A. 脆弱性を修正するために必要なパッチを適用します。
B. インシデントを上級管理者にエスカレーションして指導を求めます。
C. ネットワーク上のすべての特権ユーザー アカウントを無効にします。
D. 攻撃している IP アドレスを一時的にブロックします。
Answer: A (メーッセージを残す**)**
セクション: (なし)
説明

最新問題: **314**
企業のドメインが多数のフィッシング キャンペーンに巻き込まれています。アナリストは、その企業がドメイン スプーフィングの被害者であると判断する必要があります。レコードを確認すると、DMARC に失敗した電子メールを無視するようメールボックス プロバイダーに指示する DMARC レコードがあるにもかかわらず、アナリストは次のことを発見しました。
会社の要件がメールボックス プロバイダーによって正しく処理されない理由を説明する最も適切なものは次のうちどれですか?
A. DMARC レコードの DKIM アラインメント タグが正しく構成されていません。
B. DMARC レコードには SPF アラインメント タグがありません。
C. DMARC レコードのポリシー タグが正しく構成されていません。
D. DMARC レコードのバージョン タグは、現在のバージョン (DMARC3) ではなく DMARC1 に設定されます。
Answer: B (メーッセージを残す**)**

最新問題: **315**
ある大手ソフトウェア会社は、ソース管理および展開パイプラインとしてクラウド コンピューティング環境に移行したいと考えています。ビジネスの性質上、管理者は復旧時間の目標を 1 時間以内にする必要があると判断します。次の戦略のうち、企業が望ましい回復時間を達成するために最も有利な立場に立つのはどれですか?
A. 同じリージョンに重複環境を構成し、両方のインスタンス間の負荷分散を行います。
B. 複製されたコピーと自動スケーリングをオンにして、すべてのクラウド コンポーネントをセットアップします。
C. 他のリージョンへのアクティブなレプリケーションを備えた代替サイトを確立します。
D. 災害時のフェイルオーバーに使用できる複製コピーをオンプレミスで作成します。

Answer: C (メーッセージを残す)

最新問題: **316**
従業員は、Windows ワークステーション上のシステム パフォーマンスの低下を観察しました。従業員はドキュメントにアクセスしようとしたときに、ファイル アイコンが異常に表示され、ファイル拡張子が変更されていることに気付きました。従業員は即座にマシンをシャットダウンし、監督者に警告しました。
これらのアクションの結果、次の法医学的証拠のうちどれが失われますか?
A. マシンをシャットダウンする前のすべてのユーザー アクション
B. マシンのローカル データベースに保存されているすべての情報
C. レジストリに書き込まれるためにキューに入れられているすべてのキャッシュされたアイテム
D. システムのメモリ内の揮発性アーティファクト
Answer: D (メーッセージを残す)
揮発性アーティファクトとは、オープン ネットワーク接続、実行中のプロセス、暗号化キー、インターネット履歴など、コンピュータの実行中に揮発性メモリに保存されるデータです。揮発性アーティファクトは、フォレンジック調査、特にハード ドライブに痕跡を残さないマルウェアや悪意のあるアクティビティの検出と分析に貴重な証拠を提供する可能性があります。ただし、揮発性アーティファクトは電源がオフになるとシステムのメモリから消去されるため、後で復元することはできません。

最新問題: **317**
システム管理者は、実行中のさまざまなサービスの脆弱性を判断するために、企業の外部ネットワークのネットワーク偵察を行っています。いくつかのサンプル トラフィックを外部ホストに送信すると、管理者は次のパケット キャプチャを取得します。
出力に基づいて、次のどのサービスの脆弱性をさらにテストする必要がありますか?
A. SSH
B. HTTPS
C. SMB
D. HTTP
Answer: C (メーッセージを残す)

最新問題: **318**
攻撃ベクトルを理解し、インテリジェンス ソースを統合することは、以下の重要な要素です。
A. プロアクティブな脅威ハンティング
B. リスク管理コンプライアンス。
C. 脆弱性管理計画。
D. インシデント対応計画。
Answer: A (メーッセージを残す)
脅威ハンティング活動。
1. 仮説を立て、

2. 脅威アクター/活動のプロファイリング、
3. 脅威ハンティング戦術、
4. 攻撃対象領域の削減、
5. 重要なシステム/資産をグループ/保護ゾーンにバンドルします。
6. 攻撃ベクトルを理解、評価、対処する
7. 統合されたインテリジェンス
8. 検出機能の向上。

最新問題: **319**
情報セキュリティ アナリストは、最近の侵入テストからデータを収集し、次の出力をレビューしています。
アナリストは、ターゲット上で実行されている Web ベースのサービスに関する詳細情報を取得したいと考えています。
次のコマンドのうち、必要な情報が得られる可能性が最も高いのはどれですか?
A. トレーサート 10.79.95.173
B. ftpd 10.79.95.173.rdns.datacenters.com 443
C. ping -t 10.79.95.173.rdns.datacenters.com
D. Telnet 10.79.95.173 443
Answer: (解答を表示する**)**

最新問題: **320**
サイバーセキュリティ アナリストは現在、アクセス制御リストが適用された新しく導入されたサーバーをチェックしています。
スキャンを実行すると、アナリストは次の結果のコード スニペットを受け取りました。
このスキャンの出力を説明しているものは次のうちどれですか?
A. アナリストは真陽性を発見しました。ステータス コードは正しく、ファイルが見つからないというエラー メッセージが表示されます。
B. アナリストは誤検知を発見しました。ステータス コードが正しくないため、サーバー エラー メッセージが表示されます。
C. アナリストは真陽性を発見しましたが、ステータス コードが正しくないため、禁止されたメッセージが示されています。
D. アナリストが誤検知を発見しました。ステータス コードが正しくないため、OK メッセージが表示されます。
Answer: A (メーッセージを残す**)**

最新問題: **321**
セキュリティ アナリストは、全体的な攻撃対象領域を減らす必要があります。
アナリストが推奨すべきインフラストラクチャの変更は次のうちどれですか?
A. ハニーポットを実装します。
B. エアギャップに敏感なシステム。
C. ネットワークのセグメンテーションを増やします。
D. クラウドベースのアーキテクチャを実装します。
Answer: B (メーッセージを残す**)**
参考: https://www.securitymagazine.com/articles/89283-ways-to-reduce-your- Attack-surface

最新問題: **322**
サイバーセキュリティ アナリストは次の出力をレビューしています。

アナリストは上記の出力から次のどれを推測できますか?
A. リモート ホストはポート 8080 でサービスを実行しています。
B. リモート ホストはポート 80 で Web サーバーを実行しています。
C. リモート ホストはポート 80 をポート 8080 にリダイレクトしています。
D. リモート ホストのファイアウォールがポート 80 のパケットをドロップしています。
Answer: A (メーッセージを残す)

最新問題: **323**
HSM を最も正確に説明しているのは次のうちどれですか?
A. HSM はネットワークベースまたはリムーバブル USB を使用できます。
B. HSM は MFA に明示的に使用されます
C. HSM は、暗号化のための低コストのソリューションです。
D. HSM はソフトウェアより暗号化が遅い
Answer: C (メーッセージを残す)

最新問題: **324**
セキュリティ アナリストは、電子メール セキュリティ サービスからの次のログを確認しています。
電子メールがブロックされた理由を最もよく説明しているものは次のうちどれですか?
A. IP アドレスとリモート サーバー名が同じです。
B. To アドレスが無効です。
C. From アドレスが無効です。
D. 電子メールは www.spamfilter.org URL から送信されました。
E. IP アドレスはブラックリストに登録されました。
Answer: E (メーッセージを残す)

最新問題: **325**
脅威ハンティング チームのセキュリティ アナリストは、ワークステーションの標準 OS 導入の一部として現在実行されている不要な無害なサービスのリストを作成しました。アナリストはこのリストを運用チームに提供し、組織内のすべてのワークステーションのサービスを自動的に無効にするポリシーを作成します。
セキュリティ アナリストの目標を最もよく表しているものは次のうちどれですか?
A. システム ベースラインを作成するには
B. 攻撃対象領域を減らすため
C. システムのパフォーマンスを最適化するため
D. マルウェアの検出を向上させるため
Answer: (解答を表示する)
説明
攻撃対象領域を縮小するということは、攻撃者が利用できる機能を制限することを意味します。たとえば、1 つを除いて施設へのすべてのドアをロックすると、攻撃対象領域が減少します。攻撃対象領域を減らすことを表す別の用語は、システムの強化です。システムの強化には、すべてのシステムが可能な範囲で強化され、機能を提供できるようにすることが含まれます。

最新問題: **326**

Linux サーバーを利用する会社に勤めているセキュリティ アナリストは、脆弱性スキャンから次の結果を受け取りました。
誤検知の可能性が最も高いのは次のうちどれですか?
A. 匿名 FTP が有効になっています
B. \srvsvc による Windows SMB サービスの列挙
C. サポートされていない Web サーバーの検出
D. ICMP タイムスタンプ要求のリモート日付開示
Answer: B (メーッセージを残す**)**

最新問題**: 327**
セキュリティ アナリストは、組織内で使用できる 2 つの脆弱性管理ツールを評価しています。アナリストは、各ベンダーの指示に従って各ツールをセットアップし、同じターゲット サーバーに対して実行される脆弱性のレポートを作成しました。
ツール A は次のことを報告しました。
ツール B は次のことを報告しました。
各ツールで使用される方法を最もよく説明しているものは次のうちどれですか? (2つお選びください。)
A. ツール B はエージェントベースです。
B. ツール B は認証されていません。
C. ツール A はエージェントベースです。
D. ツール A は認証されていません。
E. ツール B は機械学習テクノロジーを利用しました。
F. ツール A はファジング ロジックを使用して脆弱性をテストしました。
Answer: A,D (メーッセージを残す**)**

最新問題**: 328**
組織の内部部門は、大量の機密データを保存するためにクラウド プロバイダーを頻繁に使用します。脅威アクターは、クラウドでホストされているハイパーバイザーを使用するために仮想マシンをデプロイし、アクセス権を昇格させました。脆弱性を修正するには次のアクションのうちどれが最適ですか?
A. 仮想マシンをサンドボックス化します。
B. MFA ソリューションを実装します。
C. 安全なハイパーバイザーのバージョンを更新します。
D. 各顧客に専用のハードウェアを実装します。
Answer: C (メーッセージを残す**)**
MFA を使用すると、攻撃者が VM にアクセスできる可能性を減らすことができますが、シナリオでは攻撃者が権限を昇格できたと具体的に述べており、質問では脆弱性を修復するために何ができるかを尋ねています。この場合の脆弱性は、権利を拡大できることです。

最新問題**: 329**
組織はリスクを評価して、緩和策に優先順位を付けることができます。リスクとその確率および影響は次のとおりです。
リスク軽減の優先順位は、高いものから低いものまで次のうちどれですか?
A. D、A、C、B
B. A、B、C、D
C. C、B、D、A

D. A、D、B、C
E. B、C、A、D
Answer: B (メーッセージを残す)

最新問題: **330**
企業の最高情報セキュリティ責任者 (CISO) は、いくつかの機密性の高いファイルの整合性を懸念しています。これらのファイルへの変更は、特定の許可されたユーザーのアクティビティ セッションに結び付ける必要があります。CISO の懸念に対処するための最良の手法は次のうちどれですか?
A. 事前承認なしでファイルへのすべての変更を拒否するように DLP を構成します。ファイルに不正な変更がないか監視します。
B. 定期的に SHA-256 を使用して、機密情報を含むディレクトリをハッシュします。ファイルに不正な変更がないか監視します。
C. ファイルに法的ホールドを適用します。許可されたユーザーに、厳密な時間コンテキスト アクセス ポリシーに従うことを要求します。ファイルに不正な変更がないか監視します。
D. Wireshark を使用して、ディレクトリとの間のすべてのトラフィックをスキャンします。ファイルに不正な変更がないか監視します。
Answer: B (メーッセージを残す)
定期的に SHA-256 を使用して、機密情報を含むディレクトリをハッシュします。ファイルに不正な変更がないか監視します。このオプションは、ファイルの整合性を確保し、変更を特定のユーザー セッションに結び付けるための最良の手法です。ハッシュは、特定の入力に対して一意の値を生成するプロセスであり、入力を変更すると異なるハッシュ値が生成されます。安全なハッシュ アルゴリズムである SHA-256 を使用することにより、アナリストは各ユーザー セッションの前後でファイルのハッシュ値を比較し、不正な変更を検出できます。

最新問題: **331**
最近、ある組織の戦略がソーシャル メディア Web サイトに投稿されました。Web サイトに投稿されたドキュメントは、組織内の 1 台のサーバーにのみ保存されているドキュメントの正確なコピーです。セキュリティ アナリストは、問題が疑われるサーバー上のコマンド ライン エントリから次の出力を確認します。
最善の行動方針は次のうちどれですか?
A. データ漏洩について確立されたすべての TCP 接続を監視します。
B. どの Firefox プロセスがマルウェアであるかを特定します
C. PID 773 に関連付けられたマルウェアを削除します
D. ファイアウォールですべての TCP 接続をブロックします。
E. PID 123 に関連付けられたマルウェアを調査します
Answer: (解答を表示する)

最新問題: **332**
ある企業は、顧客のネットワーク上のデバイスをリモート管理できるハードウェア セキュリティ アプライアンスを顧客に提供しています。顧客には構成を変更する権限がありません。会社は、アプライアンスへの不正な変更を管理するソフトウェア プロセスを導入し、その変更を記録し、中央管理者に転送します。評価用リポジトリアプライアンスが正規の構成状態から変更されていないことを確認するために、企業は次のプロセスのうちどれを使用していますか?
A. CI/CD

B. ソフトウェア保証
C. 改ざん防止
D. 変更管理
Answer: (解答を表示する**)**
改ざん防止は、システムまたはデバイスを不正な変更や修正から保護するプロセスです。また、システムまたはデバイスを変更しようとする試みをログに記録し、報告することもできます。同社は改ざん防止機能を使用して、アプライアンスが元の構成状態から変更されないようにしています。CI/CD、ソフトウェア アシュアランス、および変更管理は、特に不正な変更に対処するプロセスではありません。参照: https://www.acq.osd.mil/se/briefs/16943-DoD-AT-Overview-Brief.pdf

最新問題**: 333**
セキュリティ アナリストは社内サブネットをスキャンし、次の Nmap 出力を持つホストを発見しました。
この Nmap スキャンの出力に基づいて、アナリストは次のどれを最初に調査する必要がありますか?
A. ポート 135
B. ポート 22
C. ポート 445
D. ポート 3389
Answer: (解答を表示する**)**

最新問題**: 334**
新しいアプリケーションのセキュリティ評価中に、テスターがアプリケーションにログインしようとしましたが、指定されたユーザー名のパスワードが正しくありませんという次のメッセージを受け取りました。悪意のある攻撃者が有益な情報を受け取る可能性を減らすためにテスターが推奨できるのは次のうちどれですか?
A. 間違ったパスワードが入力された場合にアプリケーション サポート ページにリダイレクトするように Web ページを設定します。
B. エラー メッセージでは、認証の正しい要素の確認が提供されないことを認識します。
C. アプリケーションにパスワードベースの認証を使用しないようにします。
D. 認証のエラー メッセージを無効にする
Answer: B (メーッセージを残す**)**

最新問題**: 335**
セキュリティ アナリストは、異常なトラフィック パターンを特定するために、過去 30 分間に生成されたトラフィックを含むファイアウォール使用状況レポートをレビューしています。
アナリストがさらに調査する必要がある送信元 IP アドレスは次のうちどれですか?
A. 10.18.76.179
B. 10.50.180.49
C. 192.168.48.147
D. 192.168.100.5
Answer: B (メーッセージを残す**)**
セキュリティ アナリストは、送信元 IP アドレス 10.50.180.49 をさらに調査する必要があります。この IP アドレスは、インターネット上でルーティングできないプライベート ネットワークに属しています。ただし、ファイアウォール使用状況レポートには、この IP アドレスがポート 443 (HTTPS) 上の外部宛先にトラフィックを送信したことが示されています。これは、攻撃者が IP アドレスを使用してデータを漏洩したり、コマンド アンド コントロール サーバーと通信したりすることによって、IP アドレスがスプーフィングされているか侵害されていることを示している可能性があります。

最新問題: **336**
企業のアプリケーション開発はサードパーティの開発チームに委託されています。SLAに基づきます。開発チームは、安全なコーディングのための業界のベスト プラクティスに従う必要があります。この契約を確認する最善の方法は次のうちどれですか?
A. ストレステスト
B. 入力の検証
C. ユーザー受け入れテスト
D. セキュリティ回帰テスト
E. アプリケーションのファジング
Answer: (解答を表示する**)**

最新問題: **337**
技術者は、ファイアウォールの自動システムから次のセキュリティ警告を受け取ります。
アラートを確認した後、最も優れた分析は次のうちどれですか?
A. このアラートは、ユーザーがダイナミック DNS を使用してセキュリティ対策をバイパスしようとしたことを示します。
B. DNS は通常のネットワーク機能であるため、このアラートは誤検知です。
C. このアラートは、ユーザーが無効なログイン試行を多すぎたため、SIEM によって生成されました。
D. このアラートは、エンドポイントが感染している可能性があり、疑わしいホストに接続している可能性があることを示します。
Answer: D (メーッセージを残す**)**

最新問題: **338**
セキュリティ アナリストがシステム侵害を調査しています。アナリストは、侵害時にシステムの OS パッチが最新のものであったことを確認しました。解消される可能性が最も高い脆弱性の種類は次のうちどれですか?
A. インサイダーの脅威
B. ゼロデイ
C. 高度な持続的脅威
D. バッファオーバーフロー
Answer: (解答を表示する**)**

最新問題: **339**
次のソフトウェア セキュリティのベスト プラクティスのうち、攻撃者が Web アプリケーション内で任意の SQL コマンドを実行できないようにするものはどれですか? (2つお選びください。)
A. 認証
B. 出力エンコーディング
C. 入力の検証
D. データ保護
E. セッション管理
F. パラメータ化されたクエリ
Answer: C,F (メーッセージを残す**)**

最新問題: **340**

システムの操作権限 (ATO) は 4 日後に期限切れになるように設定されています。他の活動と限られた人員のため、この組織はこれまで再認証活動の開始を怠ってきました。サイバーセキュリティ グループは脆弱性スキャンを実行し、以下に示す結果の一部を取得しました。
シナリオと脆弱性スキャンの出力に基づいて、セキュリティ チームはこの発見に対して次のどれを行う必要がありますか?
A. これは重大度が 「高」であるため、現時点ではこのリスクを受け入れてください。ただし、テストには利用可能な 4 日を超える時間が必要であり、システム ATO を競合させる必要があります。
B. 無視します。これは誤検知であり、組織は他の発見に注力する必要があります。
C. サーバーを再起動して、HTTP 検証が有効になっていることを確認します。
D. Web 構成ファイルに移動し、HTTP 検証を強制する設定を検索し、正しい設定に手動で更新することで修復します。
Answer: (解答を表示する**)**

最新問題: **341**
外部ユーザーは、Web アプリケーションが遅く、情報を送信しようとすると頻繁にタイムアウトになると報告しています。
次のソフトウェア開発のベスト プラクティスのうち、この問題を防ぐのに役立つものはどれですか?
A. 回帰テスト
B. ファジング
C. 入力の検証
D. ストレステスト
Answer: D (メーッセージを残す**)**

最新問題: **342**
新製品のセキュリティ機能を評価および検証するために、製品セキュリティ アナリストが割り当てられています。評価の一部には、セキュリティ上の欠陥に対する特定の間隔での設計変更のレビューが含まれます。変更の推奨と次のチェックポイントでの変更の確認が含まれます。実行されるアクティビティを定義するのに最も適したものは次のうちどれですか。?
A. ユーザー受け入れテスト
B. ストレステスト
C. コードレビュー
D. セキュリティ回帰テスト
Answer: C (メーッセージを残す**)**
SDLC が開発段階に達すると、コードの生成が開始されます。つまり、チームが作業しているソフトウェアまたはコンポーネントのバージョンを管理する機能と、チェックイン/チェックアウト機能およびリビジョン履歴を組み合わせることが、ソフトウェア開発時に必要かつ強力なツールであることを意味します。
質問は 「新しい」製品に関するものなので、それが重要だと思います。ただし、それは、製品化される可能性のある製品の開発に関するものであるようにも見えます。
回帰テストは、加えられた変更によって新たな問題が生じていないこと、および新たな脆弱性、構成ミス、その他の問題が導入されていないことを確認するテストに重点を置いています。
コード レビューは、ソフトウェア アプリケーションまたはシステムのソース コードにセキュリティ上の欠陥、エラー、バグ、または脆弱性がないかどうかを調べて評価するプロセスです。コード レビューは、運用上の問題が発生する前に問題を特定して修正することで、ソフトウェア製品の品質とセキュリティを向上させるのに役立ちます。コード レビューは、新製品のセキュリティ機能の評価と検証の一部です。ユーザー受け入れテスト、ストレス テスト、またはセキュリティ回帰テストは、新製品のセキュリティ機能を評価および検証するために使用できる他の種類のテストですが、セキュリティ上の欠陥について特定の間隔で設計変更をレビューすることは含まれません。参考: https://www.synopsys.com/blogs/software-security/code-review/

最新問題: **343**
SOC で働くセキュリティ アナリストは最近、ホストが特定のドメインと IP のセットにアクセスし、マルウェアに感染した Balances m を発見しました。この状況で取るべき最も適切な行動は次のうちどれですか?
A. IP およびドメインとの間のトラフィックを許可しないようにファイアウォール設定への変更リクエストを実装します。
B. マルウェアの IPS シグネチャを実装し、関連するドメインと IP のブラックリストを更新します。
C. マルウェアの IPS 署名と、IP およびドメイン間のトラフィックを許可しないファイアウォール設定の変更リクエストを実装します。
D. マルウェアの IPS 署名と、関連するすべてのドメインと IP をノックするための別の署名リクエストを実装します。
Answer: A (メーッセージを残す**)**

最新問題: **344**
Web アプリケーションの静的解析レポートによると、動的コード評価スクリプト インジェクションの脆弱性が発見されました。ソース コードの脆弱性を修正するための最良のオプションは次のどれですか?
A. コードの脆弱なセクションをすぐに削除します。
B. Web アプリケーション ファイアウォールにカスタム ルールを作成します。
C. 実行および解釈の前にユーザー入力を検証します。
D. パラメータ化されたクエリを使用します。
Answer: (解答を表示する**)**
実行および解釈の前にユーザー入力を検証すると、コードまたはコマンドを含む可能性のあるユーザーからの悪意のある入力をチェックしてフィルタリングすることにより、動的コード評価スクリプト インジェクションの脆弱性を防ぐことができます。動的コード評価スクリプト インジェクションは、アプリケーションがユーザー入力を受け入れ、適切な検証やサニタイズを行わずにそれを独自のコードの一部として実行または解釈した場合に発生する脆弱性の一種です。これにより、攻撃者が任意のコードやコマンドをアプリケーションに挿入し、アプリケーションと同じ権限でそれらを実行することが可能になります。実行および解釈の前にユーザー入力を検証すると、入力が予期された形式、長さ、タイプに準拠していること、およびアプリケーションのロジックや動作を変更する可能性のある悪意のある文字や構文が含まれていないことを確認するのに役立ちます。

最新問題: **345**
セキュリティ アナリストは、重要な Web アプリケーションの停止コールに参加するよう求められました。Web ミドルウェア サポート チームは、Web サーバーが実行されており、リクエストの処理に問題がないことを確認しました。ただし、一部の調査により、ファイアウォールによる Web サーバーへの拒否がその朝の午前 1 時頃から始まったことが判明しました。アクセスを可能にするために緊急の変更が行われましたが、管理者は根本原因の特定を求めています。次のステップとして最適なのは次のうちどれですか?
A. ログ サーバーでルールの変更を検索します。
B. ポート スキャナーを使用して、Web サーバー上のすべてのリスニング ポートを特定します。
C. Web サーバーの近くにパケット アナライザーをインストールし、サンプル トラフィックをキャプチャして異常を検出します。
D. ACL を使用して Web サーバーへのすべてのトラフィックをブロックします。
Answer: (解答を表示する**)**

最新問題: **346**
次のうち、それ自体が PII とみなされるのはどれですか? (2 つ選択してください)。
A. 政府 ID
B. 役職
C. 雇用開始日

D. 出生証明書
E. 雇用主の住所
F. 母親の旧姓
Answer: (解答を表示する**)**
PII (個人識別情報) とは、単独で、または他の情報と組み合わせて、特定の個人を識別、連絡、または特定するために使用できる情報です1。PII は、追加情報がなくても、それ自体で個人を一意に識別できる情報です。PII 自体の例は次のとおりです。
政府ID。政府 ID は、政府当局が識別目的で個人に発行する番号またはコードです。政府 ID の例としては、社会保障番号、パスポート番号、運転免許証番号などが挙げられます。政府 ID は、追加情報がなくても個人を一意に識別できます。
出生証明書。出生証明書は、個人の出生を記録する文書であり、名前、生年月日、出生地、両親の名前などの情報が含まれています。出生証明書は、追加情報がなくても個人を一意に識別できます。
PII 自体の他の例としては、生体認証データ、DNA プロファイル、指紋などが挙げられます。それ自体が PII ではない情報の例は次のとおりです。
役職。役職は、組織内の役職または役割の名前または説明です。多くの個人が同じ役職を持つ可能性があるため、追加情報がなければ役職によって個人を一意に識別することはできません。
雇用開始日。雇用開始日とは、個人が組織で働き始めた日です。多くの個人が同じ雇用開始日を持つ可能性があるため、追加情報がなければ雇用開始日は個人を一意に識別するものではありません。
雇用主の住所。雇用主の住所は、個人が勤務する組織の所在地です。多くの個人が同じ雇用主の住所で働くことができるため、雇用主の住所は追加情報なしで個人を一意に識別するものではありません。
母親の旧姓。母親の旧姓は、女性が結婚する前に持っていた姓です。多くの人が同じ母親の旧姓を持つ可能性があるため、追加情報がなければ母親の旧姓は個人を一意に識別するものではありません。
それ自体は PII ではない情報の他の例としては、性別、人種、民族、年齢などが挙げられます。

最新問題: **347**
セキュリティ分析チームは、潜在的なマルウェア活動について警告を受けています。最初の調査では、影響を受けるワークステーションの 1 つが TCP ポート 80 で 5 つの IP アドレスにビーコンを送信し、ポート 445 を介してネットワーク全体に拡散しようとしていることがわかりました。この応答プロセスの検出段階でチームが次のステップにすべきなのは次のうちどれですか?
A. ネットワーク トラフィックに基づいて SIEM で相関検索を作成し、影響を受ける可能性のあるシステムを特定します。
B. インシデントを管理者にエスカレーションします。その後、管理者がネットワーク インフラストラクチャ チームに連絡して情報を提供します。
C. システムによっては、有線および無線接続を無効にして、影響を受ける各デバイスをネットワークから大幅に削除します
D. エンジニアリング チームと協力して、内部の SMB トラフィックと 5 つの IP アドレスへのアウトバウンド HTTP トラフィックをブロックします。相関関係を作成して、影響を受ける可能性のあるシステムを特定します。
Answer: (解答を表示する**)**

最新問題: **348**

組織は、ユーザーが管理者アカウントにログインすることを禁止しています。ユーザーが昇格されたアクセス許可を必要とする場合。ユーザーのアカウントは管理者グループの一部である必要があり、ユーザーは必要に応じて一時的にのみ権限を昇格する必要があります。組織は、システムアクティビティをレビューする際に次のレポートの優先順位を持っています。
* 成功した管理者ログインのレポート優先度 - 高
* 失敗した管理者ログインのレポート優先度 - 中
* 一時的な昇格されたアクセス許可の失敗 - 低
* 成功した一時的な昇格されたアクセス許可 - 報告不可
セキュリティ アナリストがサーバーの syslog を調査し、次のことを確認しました。
次のイベントのうち、レポートの優先順位が最も高いのはどれですか?
A. オプション C
B. オプション D
C. オプション B
D. オプション A
Answer: D (メーッセージを残す**)**

最新問題**: 349**
開発チームは最近、本番前のテスト用に公開 Web サイトの新しいバージョンをリリースしました。開発チームは、Web サイトの視認性が高いため、Web サイトの機能を検証するためにさまざまなチームの協力を求めています。次のアクティビティのうち、開発チームが開始しているプロセスを最もよく表しているものはどれですか?
A. 静的解析
B. ストレステスト
C. コードレビュー
D. ユーザー受け入れテスト
Answer: (解答を表示する**)**
ユーザー受け入れテストは、ソフトウェア アプリケーションが運用環境にリリースされる前に、エンド ユーザーの要件と期待を満たしていることを検証するプロセスです。ユーザー受け入れテストは、ソフトウェア アプリケーションの機能、使いやすさ、パフォーマンス、および実際のシナリオやフィードバックとの互換性を検証するのに役立ちます。ユーザー受け入れテストには、開発者、テスター、顧客、関係者など、さまざまなチームが関与する場合があります。

最新問題**: 350**
セキュリティ アナリストは、ホストがネットワーク上でアクティブかどうかを判断しようとしています。アナリストはまず次のことを試みます。
次にアナリストは次のコマンドを実行します。
結果の違いを説明できるのは次のうちどれですか?
A. ICMP はファイアウォールによってブロックされています。
B. 元の ping コマンドを実行するには root 権限が必要でした。
C. ping と hping3 のルーティング テーブルが異なりました。
D. hping3 が誤検知を返しています。
Answer: A (メーッセージを残す**)**

最新問題**: 351**
セキュリティ アナリストは、侵害された Linux サーバーを調査しています。アナリストは ps コマンドを発行し、次の出力を受け取ります。
侵害されたシステムをさらに分析するには、管理者が NEXT を実行する必要があるコマンドは次のうちどれですか?

A. /bin/la -1 /proc/1301/exe
B. キル -9 1301
C. strace /proc/1301
D. rpm -V openash-server
Answer: C (メーッセージを残す)

最新問題: **352**
ActiveX コントロールがユーザーの Web アプリケーション上で悪意のあるコードを実行するのを防ぐための最良のセキュリティ対策は次のうちどれですか?
A. ネットワークベースの IPS をインストールして悪意のある ActiveX コードをブロックします
B. HIPS を導入して悪意のある ActiveX コードをブロックする
C. ActiveX コントロールをブロックするように Web ブラウザ設定を調整する
D. ActiveX コントロールを使用するポート上のトラフィックをブロックするようにファイアウォールを構成する
Answer: (解答を表示する)

最新問題: **353**
クライアントは企業の API にアクセスして価格データを取得できません。アナリストは、クライアント以外のソースがデータの API をスクレイピングしており、それが原因でサーバーが利用可能なリソースを超過していることを発見しました。API の可用性を保護するには、次のうちどれが最適ですか?
A. 仮想プライベート ネットワーク
B. IP ホワイトリスト
C. 証明書ベースの認証
D. Web アプリケーション ファイアウォール
Answer: (解答を表示する)

最新問題: **354**
セキュリティ アナリストはジャンプ サーバーにログオンし、システムの構成とステータスを監査します。ジャンプ サーバーへのアクセスと構成に関する組織のポリシーには次のものが含まれます。
* インターネットへのネットワーク アクセスは許可されていません。
※SSHはサーバーの管理のみを目的としています。
* ユーザーは、管理者として直接ログインせずに、自分のアカウントを使用する必要があります。
※不要なサービスは無効化する必要があります。
アナリストは昇格されたアクセス許可で netstar を実行し、次の出力を受け取ります。
サーバーが違反しているポリシーは次のうちどれですか?
A. 不要なサービスを無効にする必要があります。
B. SSH はサーバーの管理のみを目的としています。
C. インターネットへのネットワーク アクセスは許可されません。
D. ユーザーは、管理者として直接ログインせずに、自分のアカウントを使用する必要があります。
Answer: C (メーッセージを残す)
サーバーは、HTTPS トラフィックに使用されるポート 443 で外部 IP アドレス (216.58.194.174) への接続が確立されているため、インターネットへのネットワーク アクセス禁止のポリシーに違反しています。これは、サーバーがインターネット上の Web サーバーと通信していることを示しますが、これはポリシーで許可されていません。SSH はサーバーの管理のみに使用され (他のデバイスへのアクセスには使用されない)、ユーザーは自分のアカウントを使用し (管理者としてログインしていない)、

不要なサービスは有効になっていない (SSH と HTTPS のみ) ため、他のポリシーには違反しません。走っている）。参考資料: CompTIA サイバーセキュリティ アナリスト (CySA+) 認定試験の目的 (CS0-002)、9 ページ。https://en.wikipedia.org/wiki/Jump_server

最新問題: **355**
中小企業では、経理部門に職務を分離するのに十分な人員がいません。管理者はビジネスのために小切手を書き、元帳と照合します。不正行為が発生していないことを確認するために、企業は四半期ごとにレビューを実施し、社内の別の役員がすべての清算された小切手を台帳と比較します。このタイプのコントロールを最もよく説明しているものは次のうちどれですか?
A. 抑止力
B. 予防的
C. 補償中
D. 刑事
Answer: C (メーッセージを残す**)**
代替制御とも呼ばれる補償制御は、現時点では実装が困難または非現実的であると考えられるセキュリティ対策の要件を満たすために導入されるメカニズムです。
補償制御は、根本的な問題を解決せずに脆弱性に対処するために講じる追加のセキュリティ対策です。」補償統制とは、既存または潜在的な統制の弱点のリスクを軽減する統制のことです2。この場合、経理部門における職務分掌の欠如は、不正またはエラーのリスクを高める統制の弱点となります。別の役員による四半期ごとのレビューは、管理者によって記録された取引の独立した検証を提供することにより、このリスクを軽減する補償管理です。

最新問題: **356**
サイバーセキュリティ アナリストは現在、アクセス制御リストが適用された新しく導入されたサーバーをチェックしています。
スキャンを実行すると、アナリストは次の結果のコード スニペットを受け取りました。
このスキャンの出力を説明しているものは次のうちどれですか?
A. アナリストが誤検知を発見しました。ステータス コードが正しくないため、OK メッセージが表示されます。
B. アナリストは真陽性を発見しましたが、ステータス コードが正しくないため、禁止されたメッセージが示されています。
C. アナリストは真陽性を発見しました。ステータス コードは正しく、ファイルが見つからないというエラー メッセージが表示されます。
D. アナリストが誤検知を発見しました。ステータス コードが正しくないため、サーバー エラー メッセージが表示されます。
Answer: C (メーッセージを残す**)**

最新問題: **357**
プロダクト マネージャーはアナリストと協力して、データ分析プラットフォームとして機能し、Web ブラウザーからアクセスできる新しいアプリケーションを設計しています。製品マネージャーは、PaaS プロバイダーを使用してアプリケーションをホストすることを提案します。
PaaS ソリューションを使用する際にセキュリティ上の懸念があるのは次のうちどれですか?
A. 安全でないアプリケーション プログラミング インターフェイスは、データの侵害につながる可能性があります。
B. 基礎となるアプリケーション サーバーへのパッチ適用はクライアントの責任となります。
C. コードとしてのインフラストラクチャ機能を使用すると、攻撃対象領域が増加します。
D. アプリケーションはデータベース レベルで暗号化を使用できません。
Answer: B (メーッセージを残す**)**

最新問題: **358**
アナリストは、従業員のハードドライブの法医学的に健全なコピーを受け取りました。従業員のマネージャーは、不適切な画像がハードドライブから削除された可能性があると疑っています。アナリストが削除された証拠を回復するのに役立つのは次のうちどれですか?

A. ファイル分析ツール
B. ファイルのタイムスタンプ
C. ファイル彫刻ツール
D. ファイルハッシュユーティリティ
Answer: C (メーッセージを残す)

最新問題: **359**
侵入検知アナリストは、複数の内部ホストの VPN サーバーに記録された未知の IP アドレスから発信された受信接続を報告しました。セキュリティ アナリストは調査中に、ホストに関連付けられた識別子が存在しないと判断しました。セキュリティ アナリストが最良の情報を取得するために実施すべきことは次のうちどれですか?
A. 組織の IP テーブルを更新します。
B. ユーザー アクセスのログ記録を有効にします。
C. すべての VPN 接続をシャットダウンします。
D. Active Directory のルールを作成します。
Answer: B (メーッセージを残す)
ユーザー アクセス ログ (UAL) は、ユーザーがサーバー上で実行したリモート アクセスと管理アクティビティの詳細を記録する、Windows Server オペレーティング システムの機能です。UAL は、ユーザー名、送信元 IP アドレス、宛先ホスト名、使用されたプロトコル、接続の時間と継続時間などの情報を提供できます1。VPN サーバーでユーザー アクセス ログを有効にすると、セキュリティ アナリストが不明な IP アドレスから発信された受信接続を特定して調査するための最適な情報を取得するのに役立ちます。

最新問題: **360**
開発チームはオープンソース ソフトウェアを使用し、2 週間のスプリントによるアジャイル手法に従っています。先月、セキュリティ チームは共通ライブラリの安全でないバージョンに関するバグを報告しました。
DevOps チームはサーバー上のライブラリを更新し、その後セキュリティ チームがサーバーを再スキャンして脆弱性がなくなったことを確認しました。今月、セキュリティ チームはサーバー上で同じ脆弱性を発見しました。
脆弱性の原因を修正するには次のどれを行う必要がありますか?
A. ソフトウェア リポジトリ管理ツールを実装します。
B. サーバーに HIPS をインストールします。
C. コード内で入力検証を使用するように開発者に指示します。
D. アプリケーションの前に WAF をデプロイします。
Answer: A (メーッセージを残す)

最新問題: **361**
セキュリティ アナリストは、社内の多くのユーザーが受信したと報告されたフィッシング攻撃を調査しています。電子メールの 1 つの本文を以下に示します。
Office 365 ユーザー。
アカウントがロックアウトされているようです。このリンクをクリックし、手順に従ってアクセスを復元してください。よろしくお願いします。
セキュリティチーム
会社の規模と高いストレージ要件のため、会社は DNS リクエストのログを記録したり、ネットワーク トラフィックのパケット キャプチャを実行したりしませんが、ネットワーク フロー データはログに記録します。アナリストが次に実行する可能性が最も高いコマンドは次のうちどれですか?
A. telnet office365.com 25

B. トレーサート 122.167.40.119
C. http://accountfix-office365.com/login をカールします。php
D. nslookup accountfix-office365.com
Answer: D (メーッセージを残す)
nslookup は、ドメイン ネーム システム (DNS) にクエリを実行し、ドメイン名と IP アドレスに関する情報を表示できるコマンド ライン ツールです。セキュリティ アナリストは、nslookup を使用して、フィッシングの試みに使用された悪意のあるドメイン accountfix-office365.com の IP アドレスを見つけることができます。これは、アナリストが攻撃元をブロックしたり追跡したりするのに役立ちます。Telnet、tracert、curl などのコマンド ライン ツールもありますが、ドメイン名に基づいてフィッシング行為を調査する場合、nslookup ほど役に立ちません。参照: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup

最新問題: **362**
セキュリティ アナリストは、会社のワイヤレス ネットワークを介した認証交換を監視しています。
Wireshark の出力のサンプルを以下に示します。
ワイヤレス ネットワークのセキュリティ体制を向上させるのは次のうちどれですか?
A. LEAP の代わりに PEAP を使用する
B. .jsp の代わりに aspx を使用します。
C. TLSv1.1 の代わりに SSL 2.0 を使用する
D. TCP の代わりに UDP を使用する
Answer: A (メーッセージを残す)

最新問題: **363**
ファイル整合性監視では、次のファイルが書面による要求または承認された変更なしに変更されたことを示します。
次の変更が加えられました。
chmod 777 -Rv /usr
次のうちどれが発生している可能性がありますか?
A. /usr の所有権が root ユーザーに変更されました。
B. 管理機能はユーザーからロックされています。
C. 管理コマンドは誰でも読み取り/書き込み可能になりました。
D. /usr の所有権は現在のユーザーに変更されました。
Answer: C (メーッセージを残す)

最新問題: **364**
インシデント対応手順中に、セキュリティ アナリストが侵害されたサーバーのディスクからバイナリ ファイルを抽出しました。ファイルを実行せずに分析するための最良の方法は次のうちどれですか?
A. メモリ分析

B. ハッシュ署名チェック
C. リバースエンジニアリング
D. 動的分析
Answer: C (メーッセージを残す**)**
リバース エンジニアリングは、逆アセンブラ、デバッガ、逆コンパイラなどのツールを使用して、バイナリ ファイルを実行せずに分析するプロセスです。リバース エンジニアリングは、バイナリ ファイルの機能、動作、目的、およびバイナリ ファイルに含まれる可能性のある悪意のあるコードや脆弱性を特定するのに役立ちます。

最新問題: **365**
企業の最高情報責任者は、CASB ソリューションを使用して、クラウド アクセス中にポリシーが確実に満たされるようにしたいと考えています。会社のビジネスの性質とリスク選好のため、経営チームは財務情報をクラウドに保存しないことを選択しました。セキュリティ アナリストは、クラウドへの財務データ漏洩の脅威を軽減するソリューションを推奨する必要があります。アナリストは次のうちどれを推奨しますか?
A. CASB を利用して、オンプレミスに保存されている財務情報に対して DLP 保存データ保護を適用します。
B. この目的には CASB ソリューションを利用せず、移動中のデータ用にオンプレミスで DLP を追加します。
C. CASB を利用して、クラウドに移動する財務情報に対して DLP データインモーション保護を適用します。
D. この目的には CASB ソリューションを利用せず、保存データ用にオンプレミスの DLP を追加します。
Answer: C (メーッセージを残す**)**
説明
「CASB ソリューションは通常、独自の DLP ポリシー エンジンを提供しており、CASB で DLP ポリシーを構成し、クラウド サービスに適用できます。」
https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solutio

最新問題: **366**
金融機関が自社のセクター専用の安全なフィードで最新の脅威インテリジェンス情報を共有する主な理由は次のうちどれですか?
A. 一般的な悪意のある行為者と侵害の兆候に関する情報を増強するため
B. 悪意のある攻撃者が悪意のある攻撃から防御できることを認識しないようにするため
C. 他の業界が金融機関向けの情報にアクセスできないようにするため
D. 顧客のモバイル アプリケーションを特にターゲットにした攻撃に焦点を当てる
Answer: A (メーッセージを残す**)**
これが、金融機関がその分野専用の安全なフィードで最新の脅威インテリジェンス情報を共有する主な理由です。脅威インテリジェンスとは、組織の資産、業務、または評判に対する現在または潜在的な脅威に関する情報の収集、分析、および配布です。脅威インテリジェンス情報を共有することで、金融機関は同業他社やパートナーの集合的な知識、経験、能力から恩恵を受け、状況認識、脅威の検出、インシデント対応を強化できます。脅威インテリジェンス情報を共有することは、金融機関が一般的な攻撃パターン、傾向、手法に加えて、悪意のある攻撃者やそれらに関連する侵害の痕跡 (IOC) を特定するのにも役立ちます。IOC は、IP アドレス、ドメイン、URL、ファイル ハッシュ、電子メール アドレスなど、ネットワークまたはシステム上の潜在的に悪意のあるアクティビティや侵入を特定するために使用できるフォレンジック データです。

最新問題: **367**
セキュリティ アナリストはサブネットをスキャンするように依頼されました。スキャン中に、次の出力が生成されました。
上記の出力に基づいて、最も可能性が高いのは次のうちどれですか?
A. 両方のホストがメール サーバーです
B. 192.168.100.214 は Web サーバーです
C. 192.168.100.214 は安全な FTP サーバーです

D. 192.168.100.145 は DNS サーバーです
Answer: B (メーッセージを残す**)**

最新問題**: 368**
組織には、サーバーを 1 つの機能専用にし、不要なサービスを無効にすることを要求するポリシーがあります。Web サーバーの Nmap スキャンからの次の出力があるとします。
次のポートのうちどれを閉じる必要がありますか?
A. 22
B. 80
C. 443
D. 1433
Answer: D (メーッセージを残す**)**
サーバーを 1 つの機能専用にする...」http/s と SQL は 2 つの機能です。私は D を選択しますが、質問の内容がひどいものであり、質問を書いた人はおそらく酔っていた可能性が高いという意見には同意します。

最新問題**: 369**
セキュリティ アナリストは、さまざまな種類の脆弱性スキャンを実行します。脆弱性スキャンの結果を確認して、実行されたスキャンの種類と、各デバイスで誤検知が発生したかどうかを判断します。
説明書：
[生成された結果] ドロップダウン オプションを選択して、結果が資格情報付きスキャン、資格情報なしのスキャン、またはコンプライアンス スキャンのいずれから生成されたかを決定します。
認証情報付きスキャンと認証情報なしのスキャンのみについて、誤検知の結果を評価し、誤検知を示す結果を確認します。注: 現在選択されているオプションのチェックを外したい場合は、そのオプションをもう一度クリックします。
最後に、脆弱性スキャンの結果に基づいて、サーバーを結果にドラッグしてサーバーの種類を特定します。
Linux Web サーバー、ファイル プリント サーバー、およびディレクトリ サーバーはドラッグ可能です。
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] ボタンを選択してください。シミュレーションが完了したら、[完了] ボタンを選択して送信してください。シミュレーションが送信されたら、 吹へ」ボタンを選択して続行してください。
Answer:

最新問題**: 370**
サイバーセキュリティ アナリストは、組織のエンドポイントに関するチーム ハントに貢献しています。
アナリストが最初に行うべきことは次のうちどれですか?
A. 仮説を立てます。
B. プロセス分析を実行します。
C. 脅威アクターとアクティビティをプロファイリングします。
D. 書き込み検出ロジック。
Answer: C (メーッセージを残す**)**

最新問題**: 371**

ソフトウェア開発ディレクターは、バックエンド データベース サーバーの侵害成功など、最近の Web アプリケーション セキュリティ インシデントに懸念を抱いています。ディレクターは、セキュリティ チームと協力して、Web アプリケーションとそれをサポートするサービスを設計、構築、テストするための標準化された方法を実装したいと考えています。基準を満たすのは次のうちどれですか?
A. OWASP
B. サンズ
C. PHP
D. Ajax
Answer: A (メーッセージを残す**)**
https://www.synopsys.com/software-integrity/resources/knowledge-database/owasp-top-10.html

最新問題**: 372**
組織は、その施設やシステムにアクセスするベンダーのセキュリティ体制を懸念しています。組織は、ベンダーによって実装されたポリシーが組織のポリシーと一致していることを確認するために、ベンダー レビュー プロセスを実装したいと考えています。コンプライアンスを最も確実に保証できるのは次のうちどれですか?
A. 社内レッドチーム レポート
B. ベンダーの自己評価レポート
C. 独立した第三者の監査レポート
D. 承認されたサードパーティ脆弱性ベンダーによる内部および外部スキャン
Answer: C (メーッセージを残す**)**
独立したサードパーティの監査レポートは、確立された標準と基準に従う外部監査人によるベンダーのセキュリティ体制と実践の客観的で公平な評価を含むため、ベンダーによる組織のポリシーへの準拠を最大限に保証できます。独立したサードパーティの監査レポートは、ベンダーが組織の要件と期待を満たしているかどうかを検証し、対処する必要があるギャップや弱点を特定するのに役立ちます。

最新問題**: 373**
TPM の機能を最もよく説明しているのは次のうちどれですか?
A. セキュリティ測定値を保存することでプラットフォームの機密性を確保します。
B. ハードドライブの暗号化アルゴリズムを実装するには
C. 一意のキーを使用してハードウェアベースのセキュリティ機能を提供します。
D. OS インストールの管理を改善します。
Answer: C (メーッセージを残す**)**

最新問題**: 374**
セキュリティ アナリストは、定期的な監視中に、ローカル ホストと通信しているいくつかの不審な Web サイトを発見しました。アナリストは、24 時間にわたって IP 192.168.50.2 をクエリします。
さらに調査するには、アナリストは SRC 192.168.50.2 の PCAP をリクエストする必要があります。
A. DST 172.10.3.5。
B. 夏時間 175.35.20.5。
C. DST 138.10.2.5。
D. DST 172.10.45.5。
E. 夏時間 138.10.25.5。
Answer: C (メーッセージを残す**)**

最新問題: **375**
複数の脅威インテリジェンスを評価するコンサルタントは、クライアントの潜在的なリスクを評価します。コンサルタントがクライアントの攻撃対象領域をモデル化する際に考慮すべき最良のアプローチは次のうちどれですか?
A. 上級管理チームと会い、推奨されるソリューションに資金が利用可能かどうかを判断します。
B. 同業他社に外部スキャンを依頼し、開いているポートを確認し、クライアントと情報を比較します。
C. 攻撃の可能性を減らすためにクライアントが購入できる潜在的なツールについて話し合います。
D. 同様の業界の同業他社に対する攻撃を調べ、同じ攻撃が発生する確率を評価します。
Answer: D (メーッセージを残す**)**

最新問題: **376**
セキュリティ アナリストは、いくつかのワークステーションがポート 3389 のトラフィック使用量を報告していると判断しました。
パッチレポートによると、すべてのワークステーションで最新の OS パッチが実行されています。ヘルプ デスク マネージャーは、一部のユーザーがワークステーションからログオフされ、ネットワーク アクセスが通常よりも遅くなっていると報告しています。アナリストは、ゼロデイ脅威によりリモート攻撃者がワークステーションにアクセスできるようになったと考えています。すべてのサービスに影響を与えずに脅威を阻止するための最善の手順は次のうちどれですか? (2つお選びください。)
A. APT が一般的なため、パブリック NAT IP アドレスを変更します。
B. RDP アクセスを無効にするようにグループ ポリシーを構成します。
C. パブリック インターネット アクセスを切断し、ワークステーション上のログを確認します。
D. 最新の OS パッチをワークステーションに再適用します。
E. 内部トラフィックをプロキシ サーバー経由でルーティングします。
F. ネットワーク上のユーザーにパスワード変更を強制します。
Answer: B,F (メーッセージを残す**)**

最新問題: **377**
アナリストは Nmap を使用してホストの定期的なスキャンを実行し、次の出力を受け取ります。
アナリストが最初に調査すべきなのは次のうちどれですか?
A. ポート 21
B. ポート 23
C. ポート 22
D. ポート 80
Answer: (解答を表示する**)**

最新問題: **378**

セキュリティ運用チームは模擬フォレンジック調査を実施しています。侵害されたワークステーションを奪取した後、最初に取るべきアクションは次のうちどれですか?
A. エスカレーション チェックリストを有効にする
B. インシデント対応計画を実施します。
C. フォレンジック画像を分析します
D. 証拠の取得を実行します
Answer: D (メーッセージを残す**)**
https://staff.washington.edu/dittrich/misc/forensics/

最新問題**: 379**
セキュリティ アナリストは、定期的な監視中に、ローカル ホストと通信しているいくつかの不審な Web サイトを発見しました。アナリストは、24 時間にわたって IP 192.168.50.2 をクエリします。
さらに調査するには、アナリストは SRC 192.168.50.2 の PCAP をリクエストする必要があります。
A. 夏時間 172.10.45.5。
B. DST 138.10.2.5。
C. DST 172.10.3.5。
D. 夏時間 175.35.20.5。
E. DST 138.10.25.5。
Answer: B (メーッセージを残す**)**

最新問題**: 380**
クライアントは企業の API にアクセスして価格データを取得できません
ａ.アナリストが以下以外の情報源を発見する
クライアントが API をスクレイピングしてデータを取得しているため、サーバーが利用可能なリソースを超過しています。どっち
API の可用性を保護するには、次のことが最善でしょうか?
A. 証明書ベースの認証
B. 仮想プライベート ネットワーク
C. IP ホワイトリスト
D. Web アプリケーション ファイアウォール
Answer: C (メーッセージを残す**)**

最新問題**: 381**
ある企業は、新しいサプライ チェーン管理ソリューションを導入するために、ヨーロッパに拠点を置く世界的なソフトウェア会社を選びました。会社の主な関心事は次のうちどれですか?
A. 知的財産の損失
B. パケットインジェクション
C. 国家安全保障政策への違反
D. 国際労働法
Answer: C (メーッセージを残す**)**

最新問題: **382**
定期的な脆弱性スキャンにより、重要なエンタープライズ Web アプリケーションに既知の脆弱性が検出されました。次のステップとして最適なのは次のうちどれですか?
A. システムにパッチを適用するには、変更リクエストを送信します。
B. リスクと重大度を評価して、さらなる措置が必要であると判断します。
C. 管理者に違反を通知し、緊急手順を開始します。
D. アプリケーションを運用環境から削除し、ユーザーに通知します。
Answer: (解答を表示する**)**
定期的な脆弱性スキャンは、自動ツールまたはソフトウェアを使用して、システムまたはネットワーク内の既知の脆弱性を特定し、評価するプロセスです3。脆弱性スキャンは、必ずしもシステムまたはネットワーク上にアクティブな脅威またはエクスプロイトがあることを意味するわけではなく、むしろ潜在的な脅威やエクスプロイトが存在することを意味します。攻撃者によって悪用される可能性のある弱点。定期的な脆弱性スキャンで重要なエンタープライズ Web アプリケーションの既知の脆弱性が検出された後の最善の次のステップは、脆弱性のリスクと重大度を評価することです。これは、Web アプリケーションに対するエクスプロイトの可能性と影響を評価し、修復アクションの優先順位を付けることを意味します。脆弱性の重大度と緊急性に基づいて。

最新問題: **383**
調査中に、セキュリティ アナリストは、ウイルス対策ソフトが検出できなかったマルウェアに感染しているマシンを特定しました。
データカービングを実行するための証拠を入手するのに最適な場所は次のうちどれですか?
A. システムメモリ
B. ハードドライブ
C. ネットワークパケット
D. Windows レジストリ
Answer: A (メーッセージを残す**)**
参照：
https://resources.infosecinstitute.com/memory-forensics/#gref https://www.computerhope.com/jargon/d/data-carving.htm

最新問題: **384**
アナリストは、複数のフィールド デバイス上のファームウェア バージョンに対する不正な変更に関するアラートを継続監視ソリューションから受け取ります。資産所有者は、ファームウェア バージョンの更新が認定技術者によって実行されていないこと、および顧客からパフォーマンスの問題や機能停止が報告されていないことを確認しています。デバイスをさらなる悪用から保護するために、アナリストが資産所有者に推奨する最善のアクションは次のうちどれですか?
A. デバイスのパスワードを変更します。
B. BIOS パスワードを実装します。
C. 分析のために実稼働ネットワークからアセットを削除します。
D. 調査結果を脅威インテリジェンス コミュニティに報告します。
Answer: (解答を表示する**)**
他のデバイスを指している場合は、はい - BIOS パスワードが侵害される前に実装します。ただし、すでに侵害されているものは、さらなる悪用を避けるためにシステムから削除する必要があります。さらに、そこにパスワードを設定すると、攻撃者があなたのパスワードを入手する可能性があります。

最新問題: **385**
プロアクティブな脅威ハンティング活動を実行する重要な理由は次のうちどれですか7 (2 つ選択)。
A. すべてのアラートが完全に調査されていることを確認するため

B. インシデント対応機能をテストするため
C. 未知の脅威を発見するため
D. アラート ルールをより具体的にできるようにするため
E. 新しいセキュリティ ベースラインを作成するには
F. セキュリティの脅威に対するユーザーの認識を向上させるため
Answer: C,E (メーッセージを残す**)**
プロアクティブな脅威ハンティングとは、アラートや侵害の兆候を待つのではなく、ネットワーク内の未知の脅威を積極的に検索するプロセスです。プロアクティブな脅威ハンティング活動を実行する重要な理由は次のとおりです。
既存のセキュリティ ツールや制御による検出を回避した可能性のある未知の脅威を発見し、損害やデータ損失を引き起こす前に軽減します。
ネットワークの現在の状態を反映する新しいセキュリティ ベースラインを作成し、通常の動作やアクティビティからの異常や逸脱を特定します。

最新問題: **386**
セキュリティ管理者は、root による FTP ログイン試行を警告する IDS ルールを作成する必要があります。次のルールのうち、最良の解決策はどれですか?
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: (解答を表示する**)**

最新問題: **387**
セキュリティ アナリストは、インシデント対応中にマシンからメモリの内容をキャプチャした後、潜在的に悪意のあるプロセスをいくつか特定しました。さらに調査を進めるための次のステップは次の手順のうちどれですか?
A. ファイルのクローン作成
B. タイムラインの構築
C. データカービング
D. リバースエンジニアリング
Answer: (解答を表示する**)**

最新問題: **388**
サイバーセキュリティ アナリストは、Web サーバーの攻撃対象領域を減らす制御を実装する必要があります。最も優れた事前制御は次のうちどれですか?
A. 未使用モジュールの無効化
B. ホストベースの IDS のインストール
C. リモート サーバーへのログの送信
D. 脆弱性スキャンの実行
Answer: A (メーッセージを残す**)**
未使用のモジュールを無効にすることは、攻撃者が悪用できる潜在的なエントリ ポイントや脆弱性の数を最小限に抑えることで、Web サーバーの攻撃対象領域を減らすことができる予防的な制御です。未使用のモジュールを無効にすると、リソースが解放され、複雑さが軽減されるため、Web サーバーのパフォーマンスと安定性が向上します。

最新問題: **389**

次のインシデント対応コンポーネントのうち、複数の事業部門と一般社会の間の連絡役を特定できるものはどれですか?
A. レッドチーム分析
B. エスカレーションのプロセスと手順
C. トリアージと分析
D. 通信計画
Answer: D (メーッセージを残す)
コミュニケーション計画は、インシデント対応プロセス中に情報がどのように伝達されるかを概説した文書です。誰が、どのような情報を、いつ、どのように、誰に伝達するかを定義します4。コミュニケーション計画では、複数の事業部門と一般の人々の間の連絡役となるのが誰であるか、また上級管理職、法律顧問、法執行機関などの他の利害関係者を特定できます。メディア。リエゾンとは、コミュニケーションと調整を促進するために、さまざまな関係者やグループの間のリンクまたは仲介者として機能する人です。

最新問題: **390**
セキュリティ構成管理ポリシーでは、すべてのパッチは運用環境に移行する前にテスト手順を受ける必要があると規定されています。セキュリティ アナリストは、1 つの Web アプリケーション サーバーが営業時間外にテストを行わずにパッチをダウンロードして適用していることに気付きました。明らかな副作用はなく、サーバーの機能には影響がないようで、スキャン後にマルウェアは見つかりませんでした。
アナリストは次のどのアクションをとるべきですか?
A. Web アプリケーション サービスの異常な帯域幅消費を監視します。
B. 異常なアクティビティのインシデント チケットを作成します。
C. 営業時間内に自動パッチ適用が行われるようにスケジュールを変更します。
D. パッチ適用によるサービス中断がないか Web アプリケーションを監視します。
Answer: B (メーッセージを残す)

最新問題: **391**
セキュリティ管理者はアナリストに侵入テストの結果に関するフィードバックを提供するよう依頼しました。結果を確認した後、管理者は脆弱性悪用の可能性に関する情報を要求します。次の情報データ ポイントのうち、アナリストがセキュリティ マネージャーに提供し、セキュリティ マネージャーがリスク要因を上級管理チームに伝えるのに最も役立つものはどれですか? (2 つ選択してください)。
A. 確率
B. 敵対者の能力
C. 攻撃ベクトル
D. 影響
E. 分類
F. 侵害の兆候
Answer: B,D (メーッセージを残す)
説明
CompTIA CySA+ (CS0-002) のベスト プラクティスによると、リスク要因を上級管理者に伝えるためにセキュリティ マネージャーに提供する最も有用な情報データ ポイントは、影響力と攻撃者の能力です。影響とは、データ損失やシステム侵害など、攻撃や脆弱性の悪用が成功した場合の潜在的な影響を指します。敵対者の能力とは、攻撃者の技術的専門知識やリソースなど、脆弱性を悪用する能力を指します。これらのデータ ポイントを組み合わせると、脆弱性に関連するリスクの全体像が得られ、上級管理者がリスクの軽減と修復に関して十分な情報に基づいた意思決定を行えるようになります。確率、攻撃ベクトル、分類、侵害の指標などの他のデータ ポイントも貴重な情報となりますが、リスク軽減の取り組みに優先順位を付けるには、影響力と攻撃者の能力が最も重要であると考えられます。

最新問題: **392**
最近の監査により、いくつかのコーディング エラーと、公開ポータルで使用されている入力検証の欠如が明らかになりました。ポータルの性質とエラーの重大度により、ポータルにパッチを適用することができません。侵害のリスクを軽減するために使用できるツールは次のうちどれですか?
A. Web プロキシ
B. 侵入防止システム
C. ネットワーク ファイアウォール
D. Web アプリケーション ファイアウォール
Answer: (解答を表示する**)**

最新問題: **393**
セキュリティ アナリストは脆弱性スキャンの結果を確認しており、新しいワークステーションに古いウイルス対策シグネチャがあるとしてフラグが立てられていることに気付きました。アナリストは次のプラグイン出力を観察します。
ウイルス対策ソフトウェアはリモート ホストにインストールされます。
インストール パス: C:\Program Files\AVProduct\Win32\
製品エンジン: 14.12.101
エンジンバージョン: 3.5.71
現在、スキャナーには AVProduct のバージョンに関する情報がありません
3.5.71。もうサポートされていない可能性があります。
エンジンのバージョンが古いです。サポートされている最も古いバージョン
ベンダーは 4.2.11 です。
アナリストはベンダーの Web サイトを使用して、サポートされている最も古いバージョンが正しいことを確認します。
状況を最もよく説明しているものは次のうちどれですか?
A. これは偽陰性であり、新しいコンピューターはデスクトップ チームによって更新される必要があります。
B. これは誤検知であり、スキャン プラグインはベンダーによって更新される必要があります。
C. これは真の陽性であり、新しいコンピューターは古いバージョンのソフトウェアでイメージ化されました。
D. これは真の陰性であり、新しいコンピューターには正しいバージョンのソフトウェアがインストールされています。
Answer: A (メーッセージを残す**)**

最新問題: **394**
セキュリティ アナリストがインシデントを調査し、他のインシデントに関連する可能性のあるいくつかの詳細を明らかにしました。セキュリティ アナリストは、他のインシデントが現在のインシデントに関連しているかどうかを判断したいと考えています。次の脅威調査方法のうち、アナリストが使用するのに最も適切なものはどれですか?
A. リスク評価
B. 評判データ

C. 行動分析
D. CVSS スコア
Answer: C (メーッセージを残す**)**