CompTIA.CS0-001.v2019-04-26.q108

試験コード：	CS0-001
試験名称：	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
認証ベンダー：	CompTIA
無料問題の数：	108
バージョン：	v2019-04-26
ページの閲覧量：	905
問題集の閲覧量：	19980

https://www.jpnshiken.com/shiken/CompTIA.CS0-001.v2019-04-26.q108.html

質問: **1**

会社のソフトウェアから脆弱性を取り除くための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、脆弱性が修正されていること、およびアプリケーションがまだ適切に機能していることを確認するためのソフトウェアのテストを担当しています。次のテストのどれがNEXTを実行する必要がありますか？

A. あいまい

B. ユーザー受け入れテスト

C. 回帰テスト

D. 侵入テスト

正解: (正解を表示します)

説明/参照：

Explanation:

参照 :https://en.wikipedia.org/wiki/Regression_testing

質問: **2**

サイバーセキュリティアナリストが次のアウトプットを検討しています。

```
root@kali!# hping3 -S -p 80 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=80 flags=RA seq=0 win=0 rtt=0

root@kali!# hping3 -S -p 8080 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=8080 flags=SA seq=0 win=29200
```

アナリストは上記の出力から次のうちどれを推測できるでしょうか。

A. 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。

B. 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。

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. リモートホストはポート80でWebサーバーを実行しています。

正解: (正解を表示します)

質問: **3**
アナリストは、コマンドラインツールを使用して、ホスト上で開いているポートと実行中のサービスを、それらのサービスとポートに関連付けられているアプリケーションと共に識別します。
アナリストは次のうちどれを使用しますか？
A. Wireshark
B. Qualys
C. netstat
D. nmap
E. ping
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **4**
最近のセキュリティ侵害に続いて、この侵害の背後にある要因を分析するために事後分析が行われました。サイバーセキュリティ分析では、特定の利害関係者に合わせて調整された現在のイベントと新たな脅威ベクトルに基づいて、潜在的な影響、軽減、および修正を検討しました。次のうちどれがこれと見なされますか？
A. 脅威インテリジェンス
B. 高度な持続的脅威
C. 脅威データ
D. 脅威情報
正解: **(**正解を表示します**)**

質問: **5**
ネットワーク管理者が安全なWebサイトの証明書に関する問題のトラブルシューティングを試みています。
トラブルシューティングプロセス中に、ネットワーク管理者は、ローカルネットワーク上のWebゲートウェイプロキシがローカルマシン上のすべての証明書に署名したことに気付きます。
次のうちどれがプロキシが実行するために合法的にプログラムされている攻撃の種類について説明しますか？
A. 中間者
B. リプレイ
C. 推移的アクセス
D. なりすまし
正解: **(**正解を表示します**)**

質問: **6**
ネットワーク内のさまざまな部署が関係するインシデントを解決しながら、未解決の問題に対処するために次のどのアクションを実行する必要がありますか

A. 教訓報告書
B. リバースエンジニアリング工程
C. CoC文書
D. インシデント対応計画
正解: **(**正解を表示します**)**

質問: **7**
組織は脆弱性の修復を優先するためにCommon Vulnerability Scoring System（CVSS）スコアを使用します。
管理者は、システム機能へのリスクが少なくても実装が容易である場合に、CVSSスコアが低い脆弱性が優先されるように、困難要因に基づいて優先順位を変更したいと考えています。
経営陣も優先順位を数値化したいと考えています。次のうちどれが経営者の目的を達成するでしょうか？
A. （CVSSスコア）* 2）/難易度=優先度
CVSSスコアが重み付けされ、難易度が1から5の範囲であり、5が最も簡単で最もリスクが低い実装である場合
B. (CVSSスコア）*難易度=優先度
難易度が0.1から1.0の範囲で、1.0が最も実装が簡単で最もリスクが低い場合
C. （CVSSスコア）/難易度=優先度
難易度が1から10の範囲で、10が最も簡単で最もリスクが低い
D. (CVSSスコア）*難易度=優先度
難易度が1から5の範囲で、1が最も簡単で最もリスクが低い
正解: **C (**コメントを発表する**)**

質問: **8**
次のパケットを確認したところ、サイバーセキュリティアナリストは、不正なサービスが会社のコンピュータで実行されていることを発見しました。

```
16:26:42.943463 IP 192.168.1.10:25 > 10.38.219.20:3389 Flags
[P.], seq 1768:1901, ackl, win 511, options [nop,nop,TS val
271989777 ecr 475239494], length 133
```

次のACLのうちどれが実装されていれば、それ以外のサービスへのさらなるアクセスを防止し、他のサービスに影響を与えないでしょうか。
A. DENY TCP ANY HOST 10.38.219.20 EQ 3389
B. DENY IP HOST 10.38.219.20 ANY EQ 25
C. DENY IP HOST192.168.1.10 HOST 10.38.219.20 EQ 3389
D. DENY TCP ANY HOST 192.168.1.10 EQ 25
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **9**
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。次のうちどれが侵入先のワークステーションを没収した後に最初に取られるべきであるか。
A. エスカレーションチェックリストを有効にします
B. インシデント対応計画を実施する
C. 法医学画像を分析します
D. 証拠取得を行います
正解: (正解を表示します)
説明/参照：
参照 :https://staff.washington.edu/dittrich/misc/forensics/

質問: **10**
ある企業が、複数のボリュームDoS攻撃の犠牲になっています。問題のあるトラフィックのパケット分析は次のことを示しています。

```
09:23:45.058939 IP 192.168.1.1:2562 > 170.43.30.4:0 Flags[], seq 1887775210:188
09:23:45.058940 IP 192.168.1.1:2563 > 170.43.30.4:0 Flags[], seq 1887775211:188
09:23:45.058941 IP 192.168.1.1:2564 > 170.43.30.4:0 Flags[], seq 1887775212:188
09:23:45.058942 IP 192.168.1.1:2565 > 170.43.30.4:0 Flags[], seq 1887775213:188
```

次の緩和策のうちどれが上記の攻撃に対して最も効果的ですか？
A. 会社は、ゲートウェイルーターで192.168.1.1から来るすべてのトラフィックをドロップするために、ネットワークベースのシンクホールを実装する必要があります。
B. 会社は上流ISPに連絡し、RFC1918トラフィックが廃棄されるように頼むべきです。
C. 会社は、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. 会社は、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。
正解: (正解を表示します)

質問: **11**
脅威インテリジェンスフィードが、カーネルに重大な脆弱性があることを示す警告を投稿しました。
残念ながら、同社の資産在庫は最新のものではありません。組織内の影響を受けるすべてのサーバーを見つけるために、サイバーセキュリティアナリストはどのようなテクニックを実行しますか？
A. syslogに送信されたデータからの手動ログレビュー
B. すべてのホストにわたるOSフィンガープリントスキャン
C. サーバーネットワークを通過するデータのパケットキャプチャ
D. ネットワーク上のサービス検出スキャン
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **12**
ネットワークトラフィックを確認するときに、セキュリティアナリストは疑わしい活動を検出します。

```
110 172.150.200.129 TCP    1140 > 443 [SYN] Seq=0 Win=15901 Len=0 MSS=1460 SACK_PERM=1
111 172.150.200.129 TCP    1140 > 443 [ACK] Seq=1 ACK=1 Win=15091 Len=0
112 172.150.200.129 SSLv2  Client Hello
113 172.150.200.129 TCP    [TCP Dup ACK 112#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
114 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
115 172.150.200.129 TCP    [TCP Dup ACK 114#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
120 172.150.200.129 TCP    [TCP Dup ACK 114#2] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
122 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
```

上記のログに基づいて、次の脆弱性攻撃のどれが起こりますか？
A. プードル
B. ゼウス
C. ハートブリード
D. ShellShock
E. DROWN
正解: (正解を表示します)

質問: **13**
新しいポリシーでは、セキュリティチームはWebアプリケーションとOSの脆弱性スキャンを実行する必要があります。同社のWebアプリケーションはすべてフェデレーション認証を使用しており、中央ポータルからアクセスできます。次のうちどれが会社のWebアプリケーションのより徹底的なスキャンを確実にするために実装されるべきであると同時に誤検知を減らしますか？
A. 脆弱性スキャナーは認証スキャンを実行するように設定されている必要があります。
B. 脆弱性スキャナーは、OSとネットワークサービスの検出を実装する必要があります。
C. 脆弱性スキャナーはWebサーバーにインストールされているはずです。
D. 脆弱性スキャナは、既知および未知の脆弱性をスキャンする必要があります。
正解: (正解を表示します)

質問: **14**
セキュリティ管理者は、最初のインスタンスから数か月後に、ローカルの特権ユーザーが "root"として対話的にサーバーにログインし、インターネットを閲覧していると判断します。管理者は、そのサーバーのセキュリティログを年1回見直すことによってこれを判断します。管理者は、次のセキュリティアーキテクチャ分野のうち、レビューと修正を推奨するものがありますか？ 2を選択）
A. パスワードの複雑さ
B. ログ集計と分析
C. 暗号化
D. 利用規定
E. ネットワークの分離と分離

F. ソフトウェアアシュアランス
正解: **(**正解を表示します**)**

質問: **15**
侵害からの相関データは、組織をすべての妥協の指標の共通点として示しているため、法執行機関は企業の弁護士に連絡しました。ある従業員が、弁護士と法執行機関の会話を聞き取り、それについてのコメントをソーシャルメディアに投稿します。それからメディアは、その違反について他の従業員と連絡を取り始めます。違反に関する情報がそれ以上開示されないようにするには、次のうちどれを実行する必要がありますか。
A. インシデントコミュニケーションに関するセキュリティ意識のトレーニングを行います。
B. すべての従業員に対し、違反について口頭でNDAに誓約するよう要求する。
C. 法執行機関に従業員と面会させます。
D. 従業員によるソーシャルメディアへのアクセスを一時的に無効にします
正解: **(**正解を表示します**)**

質問: **16**
インシデントに続いて教訓レポートを作成することは、アナリストが以下の情報のうちどれを伝達するのに役立ちますか？ （2つ選択）
A. IPアドレス、アプリケーション、および資産の一覧
B. 業務上の対応を改善するための方針と慣行の強化
C. インシデントの根本原因分析とそれが組織に及ぼした影響
D. 経営者が見直すための詳細なリバースエンジニアリングステップの概要
E. 影響を受けるサーバーとエンドポイントからの管理に報告するパフォーマンスデータ
正解: **B,C (**コメントを発表する**)**

質問: **17**
この事業は、顧客データの侵害の疑いがあることを知らされています。内部監査チームは、法務部門と連携して、レポートを検証するためにサイバーセキュリティチームと協力し始めました。調査中、企業は次の対応プロセスのどれに従うべきですか。
A. セキュリティアナリストはシステム運用者にインタビューし、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活発な調査中に内部監査要求に応答してはいけません

C. セキュリティアナリストは、調査を行っている信頼できる機関に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、インシデントが発生したときに違反の疑いがあることを規制当局に報告する必要があります。
正解: **C** (コメントを発表する)

質問: **18**
セキュリティアナリストがアクティブホストのネットワークをスキャンしたいと考えています。次のホスト特性のどれが仮想ホストと物理ホストを区別するのに役立ちますか？
A. DNSルーティングテーブル
B. ゲートウェイ設定
C. ホストIP
D. 予約済みMAC
正解: **D** (コメントを発表する)

質問: **19**
重大なApacheの脆弱性に関する警告が情報セキュリティコミュニティ全体に配信されています。次の対策のうちどれが既知の脆弱性を特定するだけですか？
A. 環境内のすべてのサーバーで認証されていない脆弱性スキャンを実行します。
B. すべてのWebサーバー上の特定の脆弱性についてスキャンを実行します。
C. 環境内のすべてのサーバーでWebの脆弱性スキャンを実行します。
D. 環境内のすべてのWebサーバーで認証スキャンを実行します。
正解: **B** (コメントを発表する)
説明/参照：
Explanation:

質問: **20**
次のうちどれが、許可された侵入テストのためのタイムラインと時刻境界の慎重な選択の背後にある推論を表していますか？ 2を選択）
A. 意図しない業務への影響を軽減するため
B. チームのコミュニケーションと報告の頻度を決定する
C. テストが運用にある程度の影響を与えることを確認する
D. テスト活動に必要な人的資源を計画するため
E. 発生する可能性がある実際の侵入との競合を回避するため
正解: (正解を表示します)

質問: **21**
サイバーセキュリティアナリストは、DDoS攻撃の結果として複数のシステムの動作が遅くなっているという報告を受けました。次のうちどれがサイバーセキュリティアナリストが実行するための最良の行動でしょうか？

A. 重要システムの監視を続けます。
B. すべてのサーバインタフェースをシャットダウンします。
C. インシデントの管理者に連絡してください。
D. 影響を受けるシステムについてユーザーに通知します。
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **22**
次の項目のどれが、インシデント対応の有効性および改善が必要なギャップがあるかに加えて、インシデントが検出された時期、インシデントの影響度、および修正方法に関する詳細な情報を含む文書を表します。
A. 法医学分析レポート
B. CoCレポート
C. 動向分析レポート
D. 教訓レポート
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **23**
キーベースの認証を有効にした後、セキュリティアナリストが次のログを確認しています。

上記の情報を考えると、システムを保護するために次のステップのうちどれを実行する必要がありますか。
A. 匿名SSHログインを無効にします。
B. SSHのパスワード認証を無効にします。
C. SSHv1を無効にします。
D. リモートルートSSHログインを無効にします。
正解: **B (**コメントを発表する**)**
説明/参照：

Explanation:

質問: **24**
サイバーセキュリティアナリストは、パブリッククラウドベースのシステムを利用した新しい基幹機能を見つけました。アナリストは、CIAに関してシステムによって処理された情報を分類する必要があります。次のうちどれが情報のCIA分類を提供する必要がありますか？
A. サイバーセキュリティアナリスト
B. システム管理者
C. クラウドプロバイダ
D. データの所有者
正解: **(**正解を表示します**)**

質問: **25**
建物のロビーのATMが危険にさらされています。セキュリティ技術者は、ATMは複数の技術者によって法的に分析される必要があると助言しています。フォレンジックツールキットの次のうちどれが最初に使用される可能性がありますか。 2を選択）
A. ハッシュユーティリティ
B. ブロッカー書き込み
C. ドライブイメージャー
D. ドライブアダプタ
E. 犯罪テープ
F. CoCの形
正解: **(**正解を表示します**)**

質問: **26**
次のうちどれが侵入テストのためのエンゲージメントの規則の中で不可欠な要素ですか？
2を選択）
A. スケジュール
B. 権限
C. 業務上の理由
D. 支払条件
E. システム管理者の一覧
正解: **A,B (**コメントを発表する**)**

質問: **27**
管理者は、アクターがWebサーバーから外部のホストへ機密データを盗用している方法を調査しています。徹底的な法医学的調査の結果、管理者はサーバのBIOSがrootkitのインストールによって変更されたと判断しました。ルートキットを取り外してBIOSを既知の良好な状態にフラッシュした後、別のルートキットがインストールされている場合に備えて、次のうちどれが将来のBIOSへの悪意のあるアクセスから保護するのでしょうか。

A. ホストベースID
B. マルウェア対策アプリケーション
C. ファイルの整合性監視
D. TPMデータシール
正解: **(**正解を表示します**)**

質問: **28**
金融サービス会社に勤務する脅威インテリジェンスアナリストは、次のレポートを受け取りました。
"www.bankfinancecompsoftware.comに常駐する効果的なウォーターホールキャンペーンが行われています。このドメインはランサムウェアを配信しています。このランサムウェア亜種はMBRを上書きすることができるため研究者によって" LockMaster "と呼ばれています。この攻撃経路に関する防御操作を実行してください。」アナリストはクエリを実行し、このトラフィックがネットワーク上で見られたと評価しました。アナリストは次のうちどれをしなければならないのですか。 2を選択）
A. MBRを保護するためにフルディスク暗号化を有効にするようセキュリティ設計者にアドバイスします。
B. 会社に広めるための脅威情報メッセージを作成する
C. セキュリティアナリストに、"LockMaster"という文字列でSIEMに警告を追加するように指示します。
D. ドメインにアクセスして脅威の評価を始めます
E. ファイアウォールエンジニアにドメインのブロックを実装するように指示してください
F. 予防措置としてMBRをフォーマットします
正解: **(**正解を表示します**)**

質問: **29**
ソフトウェアアシュアランスラボでは、さまざまなランダムなデータセットを自動的に生成して入力し、エラー/障害状態を引き起こすことを試みることで、アプリケーションに対して動的な評価を実行しています。次のソフトウェア評価機能のうち、ラボはSDLCのどの段階でANDを実行しますか。 2つ選択してください。）
A. あいまい
B. 行動モデル
C. 静的コード分析
D. 試作フェーズ
E. 所要量フェーズ
F. 計画フェーズ
正解: **(**正解を表示します**)**
説明/参照：
参照先 :http://www.brighthub.com/computing/smb-security/articles/9956.aspx

質問: **30**
セキュリティアナリストがログを確認し、従業員に発行された会社所有のコンピュータが多数の警告や警告を生成していることを発見しました。アナリストはログイベントの確認を続け、異なる、未知のIPアドレスからの企業所有ではないデバイスが同じイベントを生成していることを発見しました。アナリストはこれらの調査結果をマネージャに通知し、マネージャはこれらのアクティビティはすでに知られており、進行中のイベントの一部であると説明します。このシナリオでは、アナリスト、従業員、およびマネージャの担当者は次のうちどれですか。
A. アナリストは赤チームです。
従業員は青いチームです。
マネージャーは白いチームです。
B. アナリストは白いチームです。
従業員は赤いチームです。
マネージャーは青いチームです。
C. アナリストは赤いチームです。
従業員は白いチームです。
マネージャーは青いチームです。
D. アナリストは青いチームです。
従業員は赤いチームです。
マネージャーは白いチームです。
正解: **(**正解を表示します**)**
説明/参照：
参照 :https ://danielmiessler.com/study/red-blue-purple-teams/

質問: **31**
テクノロジー企業に勤務する脅威インテリジェンスアナリストは、ベンダーからこのレポートを受け取りました。
「技術業界の組織に対して知的財産窃盗キャンペーンが実施されてきた。この活動の指標は各侵入に固有のものである。標的にされていると思われる情報はR&Dデータである。この攻撃経路に関する防御操作を実行してください。」次の組み合わせのどれが、どのように脅威を分類する必要があるのか、およびこの活動から保護するのに最も役立つと思われる分析の種類はどれかを示唆していますか。
A. ポリモーフィックマルウェアと安全なコード分析
B. インサイダー脅威と指標の分析
C. APTと行動分析
D. ランサムウェアと暗号化
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **32**
データの漏洩に続いて、サイバーセキュリティアナリストは次の実行されたクエリに気づいた。
ユーザーからのSELECT * WHERE name = rickまたは1 = 1
次の攻撃のうちどれが起こりましたか？そして、次の技術的セキュリティ管理のどれがこの攻撃からの将来の影響の危険性を最もよく減らすでしょうか？　2を選択）
A. クッキーの暗号化
B. XSS攻撃
C. パラメータ検証
D. キャラクターブラックリスト
E. 悪意のあるコードの実行
F. SQLインジェクション
正解: (正解を表示します)
説明/参照：
参照 :https://lwn.net/Articles/177037/

質問: **33**
セキュリティアナリストが、これまでのSIEMアラートの対象となっていたマシンで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を利用しているネットワーク接続、%TEMP%フォルダ内のsvchost.exeおよびcmd.exeのコピー、および外部IPに接続していたRDPファイルに気付いた。セキュリティアナリストが発見した脅威はどれですか。
A. DDoS
B. APT
C. ランサムウェア
D. ソフトウェアの脆弱性
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **34**
PHIの保存に関する規制遵守の目的を達成するためには、脆弱性スキャンを継続的に実施する必要があります。最後に完了したネットワークのスキャンで5,682件の脆弱性が報告されています。

最高情報責任者（CIO）は、すべての既知の問題を解決するための修復計画を立てたいと考えています。次のうちどれが続行するための最良の方法ですか？
A. 誤検知と例外をすべて識別してから、残りのすべての項目を解決します。
B. 現在の脆弱性のリストが解決されるまで、追加のスキャンを延期します。
C. PHIを処理する資産をサンドボックス環境に配置してから、すべての脆弱性を解決します。
D. 資産インベントリで重要と判断されたアイテムにスキャンを減らし、最初にこれらの問題を解決します。
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **35**
最近の監査で、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はできません。
次のツールのうちどれが危険にさらされるリスクを減らすために使用できますか？
A. ネットワークファイアウォール
B. Webプロキシ
C. 侵入防止システム
D. Webアプリケーションファイアウォール
正解: **(**正解を表示します**)**

質問: **36**
脅威インテリジェンスアナリストが検索エンジンの危殆化の指標を調査している間、Webプロキシは同じ指標に関するアラートを生成しました。脅威インテリジェンスアナリストは、関連サイトは訪問されなかったが検索エンジンで検索されたと述べています。次のうちどれがこのような状況で起こった可能性がありますか？
A. アナリストは標準の承認済みブラウザを使用していません。
B. アナリストは誤って指標に関連したリンクをクリックしました。
C. アナリストは使用中のブラウザでプリフェッチを有効にしています。
D. アナリストの検索とは無関係のアラート。
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **37**
技術者は、ユーザーのワークステーションにネットワーク接続がないという報告を受け取ります。技術者は、調査を行い、ユーザーのVoIP電話の背面を走っているパッチケーブルがローリングチェアの下に直接配線されており、時間の経過とともに平らに粉砕されていることに気付きました。

次のうちどれがこの問題の最も可能性の高い原因ですか？
A. 過剰な衝突
B. 分割ペア
C. クロストーク
D. 電磁波障害
正解: **(**正解を表示します**)**

質問: **38**
ヘルプデスクは、セキュリティアナリストに、複数のユーザーから報告された疑わしい電子メールに関して発生し始めている傾向について通知しました。アナリストは、次のファイルを含むinvoice.zipという添付ファイルが電子メールに含まれていると判断しました。
Locky.js
xerty.ini
xerty.lib
さらに分析すると、.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ていることがわかります。NASのデータが感染した機器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どれですか？
A. 会社のVPNへのアクセスを無効にします。
B. 請求書の添付ファイルを開かないように指示する電子メールの従業員。
C. 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。
D. 会社のWebプロキシフィルタに.jsファイルに含まれているURLを追加します。
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **39**
セキュリティアナリストがトラフィック分析を行っており、WebサーバーへのHTTP POSTを監視しています。POSTヘッダーの長さは約1000バイトです。送信中は、10秒ごとに1バイトが配信されます。次の攻撃のうちどれがトラフィックを示していますか？
A. SQLインジェクション
B. ろ過
C. バッファオーバーフロー
D. サービス拒否
正解: **B (**コメントを発表する**)**

質問: **40**
大学は、集中管理されたラップトップと学生/従業員のラップトップの両方の脆弱性スキャンを実装することで、ネットワークのセキュリティ体制を強化したいと考えています。このソリューションは、拡張可能で、誤検知を最小限に抑え、結果の精度を高め、エンタープライズコンソール

を介して集中管理できるようにする必要があります。次のスキャントポロジのうちどれがこの環境に最適ですか？

A. ネットワークインフラストラクチャの中核にあるパッシブスキャンエンジン

B. クラウドベースとサーバーベースのスキャンエンジンの組み合わせ

C. サーバーベースのエージェントとエージェントベースのスキャンエンジンの組み合わせ

D. エンタープライズコンソールにインストールされているアクティブスキャンエンジン

正解: (正解を表示します)

説明/参照：

Explanation:

質問: **41**

OWASP ZAPツールを使用して本社のWebサイトをスキャンした後、サイバーセキュリティアナリストは次の警告を確認しています。

```
The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT
containing password type input. Passwords may be stored in
browsers and retrieved.
```

アナリストは問題のあるコードの断片をレビューします。

```
<form action="authenticate.php">
     Username:<br>
     <input type="text" name="username" value="" autofocus><br>
     Password: <br>
     <input type="password" name="passwword" value="" maxlength="32"><br>
     <input type="submit" value="submit">
</form>
```

次のうちどれが上記の警告とコードスニペットに基づく最良の行動方針ですか？

A. アナリストは、誤検知に対してスキャナー例外を実装する必要があります。

B. システム管理者はSSLを無効にしてTLSを実装する必要があります。

C. 開発者はコードを確認してコードの修正を実装する必要があります。

D. 組織は、問題を解決するためにブラウザのGPOを更新する必要があります。

正解: (正解を表示します)

説明/参照：

Explanation:

質問: **42**

ネットワーク上でパケットアナライザを実行した後、セキュリティアナリストは次の出力に気付きました。

次のうちどれが起こっていますか？

A. pingスイープ

B. ポートスキャン

C. ネットワークマップ

D. サービスの発見

正解: **(**正解を表示します**)**

説明/参照：

Explanation:

質問: **43**

アナリストは、脆弱性スキャナが最新のシグニチャセットを持っていないため、パッチが当てられていないサーバには検出されない脆弱性があることを発見しました。経営陣は、セキュリティチームに、スキャンを実行する少なくとも24時間前に最新のシグネチャでスキャナを更新させるよう指示しましたが、結果は変わりません。次のうちどれが失敗に対処するための最良の論理制御ですか？

A. スキャンツールを自動的にアップデートするようにスクリプトを設定します。

B. 既存の更新プログラムが実行されていることを手動で確認します。

C. 展開する前にサンドボックスで脆弱性の修正をテストします。

D. 認証モードで実行するように脆弱性スキャンを設定します。

正解: **(**正解を表示します**)**

説明/参照：

Explanation:

質問: **44**

ある組織がWebサーバーを強化したいと考えています。この目標の一部として、リーダーシップは脆弱性スキャンが実行されるように指示しました、そしてセキュリティチームは業界のベストプラクティスに従ってサーバを修正するべきです。チームはすでに脆弱性スキャナーを選択し、必

要なスキャンを実行しました。そして今、チームは修正を優先する必要があります。次のうちどれが業界のベストプラクティスに従って修復の脆弱性を優先するのに役立ちますか？
A. SLA
B. ITIL
C. CVSS
D. OpenVAS
E. Qualys
正解: **C** (コメントを発表する)

質問: **45**
プロジェクトリーダーは、組織の内部および外部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焦点を当てた、今後のプロジェクトの作業明細書を検討しています。プロジェクトの一環として、外部の請負業者のチームが組織に対してさまざまな攻撃を仕掛けようとします。この作業明細書は、特に、インフラストラクチャにおける論理図表示の弱点を開発するための試みにおいて、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対処している。
作業明細書に記載されている活動の範囲は、以下の例です。
A. セッションハイジャック
B. 脆弱性スキャン
C. 侵入テスト
D. フレンドリーDoS
E. ソーシャルエンジニアリング
正解: **C** (コメントを発表する)

質問: **46**
アナリストは、社内で開発されたCRMシステムの最新バージョンをテストしていました。アナリストは基本的なユーザーアカウントを作成しました。Kaliの最新版に含まれるいくつかのツールを使用して、アナリストは設定ファイルへのアクセス、フォルダやグループに対する権限の変更、そして新しいシステムオブジェクトの削除と作成を行うことができました。
アナリストは、これらの許可されていない活動を実行するために次の技法のうちどれを使用しましたか？
A. インプットインジェクション
B. 特権の昇格
C. ディレクトリトラバーサル
D. なりすまし
正解: (正解を表示します)

質問: **47**
ビジネスクリティカルなアプリケーションは、特殊文字の使用を許可していないため、現在のパスワードポリシーの要件をサポートできません。管理者は、パスワードの標準が弱いためにセキュリティ上の問題が発生する危険性を受け入れたくありません。次のうちどれがアプリケーションに関連するリスクを制限するための適切な手段ですか？
A. パスワードポリシーを変更する
B. 新しいアカウント管理手順を作成する
C. 認証トラフィックの暗号化
D. 補正コントロール
正解: **C** (コメントを発表する)

質問: **48**
セキュリティアナリストがサーバーの脆弱性を修正するよう依頼されました。アナリストがこの脆弱性に対するパッチを見つけると、次のうちどれがNEXTに起こるはずですか？
A. 変更管理処理を開始します。
B. まだ脆弱性が存在することを確認するために再スキャンします。
C. 継続監視を実施する。
D. インシデント対応プロセスを開始します。
正解: **A** (コメントを発表する)
説明/参照：
Explanation:

質問: **49**
セキュリティの専門家がネットワーク使用率レポートの結果を分析しています。この報告書には以下の情報が含まれています。

IP Address	Server Name	Server Uptime	Historical	Current
172.20.2.58	web.srvr.03	30D 12H 52M 09S	41.3GB	37.2GB
172.20.1.215	dev.web.srvr.01	30D 12H 52M 09S	1.81GB	2.2GB
172.20.1.22	hr.dbprod.01	30D 12H 17M 22S	2.24GB	29.97GB
172.20.1.26	mrktg.file.srvr.02	30D 12H 41M 09S	1.23GB	0.34GB
172.20.1.28	accnt.file.srvr.01	30D 12H 52M 09S	3.62GB	3.57GB
172.20.1.30	R&D.file.srvr.01	1D 4H 22M 01S	1.24GB	0.764GB

次のサーバーのうちどれをさらに調査する必要がありますか？
A. hr.dbprod.01
B. R&D.file.srvr.01
C. mrktg.file.srvr.02

D. web.srvr.03
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **50**
セキュリティアナリストが、ネットワーク上の新しいセグメントに対して脆弱性スキャンを設定しようとしています。資格情報付きスキャンを実行しながら、資格情報がネットワークを通過しないようにするという要件を考えると、次のうちどれが最良の選択ですか？
A. 各エンドポイントに管理者権限を持つスキャナを配置します
B. エンドポイントにエージェントをインストールしてスキャンを実行します
C. 各エンドポイントに脆弱性スキャナの認証情報を提供します
D. スキャナーとエンドポイント間のトラフィックをすべて暗号化します
正解: (正解を表示します)

質問: **51**
技術者が最近いくつかのウイルスとスパイウェアプログラムを搭載したコンピュータを修正し、インターネット設定が未知のプロキシを介してすべてのトラフィックをリダイレクトするように設定されていることに気付きました。このタイプの攻撃は次のうちどれとして知られていますか？
A. ショルダーサーフィン
B. フィッシング
C. 中間者
D. ソーシャルエンジニアリング
正解: (正解を表示します)

質問: **52**
最近の脆弱性スキャンでは、組織の公衆インターネット向けIPアドレスに4つの脆弱性が見つかりました。組織への違反のリスクを減らすために優先順位を付けること。最初に修正されるべきものはどれですか。
A. 暗号的に弱いことが知られている暗号。
B. 自己署名SSL証明書を使用しているWebサイト
C. リモートでコードが実行されることを可能にするバッファオーバーフロー。
D. 内部IPアドレスを明らかにするHTTP応答
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **53**

サイバーセキュリティアナリストは、よく知られている「Call Home」メッセージがネットワーク境界で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アラートを受け取りました。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。アラートが真のポジティブであると判断した後、最も可能性の高い原因は次のうちどれですか？
A. 攻撃者は会社のリソースを偵察しています。
B. 外部の指揮統制システムが感染したシステムに到達しようとしています。
C. インサイダーがリモートネットワークに情報を抽出しようとしています。
D. マルウェアは社内システムで実行されています。
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **54**
今後の顧客のための取り組みの一環として、アナリストは、スキャンがSOWで定義された情報に準拠していることを確認するために侵入テストアプリケーションを設定しています。SOWに伝統的に見られる情報に基づいて、次の種類の情報のうちどれを考慮すべきですか？ （2つ選択してください。）
A. スキャンのタイミング
B. エグゼクティブサマリーレポートの内容
C. 除外されたホスト
D. メンテナンス期間
E. IPS設定
F. インシデント対応方針
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **55**
セキュリティアナリストは、従業員が辞任を申し出る前にデータの漏洩を試みる可能性があることを懸念しています。残念ながら、同社はデータ損失防止（DLP）システムを購入する余裕がありません。
以下の推奨事項のうち、セキュリティアナリストはデータ損失に対する徹底的な防御を提供するためにどのような注意を払うべきですか？ （3つ選択）
A. 社内ネットワークまたはVPN経由で接続されていない限り、ラップトップでインターネットにアクセスできないようにする
B. ユーザーがコピー＆ペースト機能を使用できないようにする
C. ユーザーがワークステーションを変更するときに移動プロファイルを使用できないようにする
D. グループポリシーを使用してフラッシュドライブがUSBポートに接続できないようにする

E. ユーザーがワークステーションからワークステーションにデータをコピーできないようにします
F. ユーザーがWebプロキシ経由で個人の電子メールサイトやファイル共有サイトにアクセスするのを防ぎます。
正解: **A,D,F (**コメントを発表する**)**

質問: **56**
ある会社が年間予算の10%をセキュリティ技術に投資しました。CIO（最高情報責任者は、この投資がなければ、同社が3カ月前に競合他社に経験したのと同じサイバー攻撃の次の犠牲者になる危険性があると確信しています。しかし、この投資にもかかわらず、ユーザーは仕事を終わらせるために同僚とユーザー名とパスワードを共有しています。次のうちどれがこのプラクティスによって導入されたリスクを排除しますか？
A. 自分の資格情報を共有しているすべてのユーザーについてレポートを作成し、それ以上の操作について管理者に警告します。
B. ユーザーに自分の資格情報を共有しないように求める電子メールを送信する
C. 否認防止を確実にするための解決策に投資しそして実行する
D. 毎日パスワードを変更する
正解: **(**正解を表示します**)**

質問: **57**
プロキシログを確認しているときに、セキュリティアナリストは疑わしいトラフィックパターンに気付きました。いくつかの内部ホストが、ポート80を介して常に外部IPアドレスと通信しているのが観察されました。事件が宣言され、調査が開始されました。影響を受けたユーザーにインタビューした後、アナリストは、新しいグラフィックデザインスイートを展開した直後にアクティビティが開始されたと判断しました。この情報に基づいて、次の行動のうちどれが調査における適切なNEXTステップであろうか？
A. 影響を受けるユーザーが認証しているサーバー上のすべてのウイルス対策およびマルウェア対策製品、およびその他すべてのホストベースのセキュリティソフトウェアを更新します。
B. デスクトップサポート担当者に、影響を受けるすべてのワークステーションのイメージを再作成してグラフィックデザインスイートを再インストールするよう依頼してください。ウィルススキャンを実行してウィルスが存在するかどうかを確認します。
C. 宛先IPアドレスとその所有者を特定し、影響を受けるホストで実行中のプロセスを調べて、そのアクティビティが悪意のあるものかどうかを判断します。
D. ネットワークスキャンを実行し、監視対象のトラフィックを生成している可能性がある不正なデバイスを特定します。
それらのデバイスをネットワークから削除してください。
正解: **A (**コメントを発表する**)**

質問: **58**

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、同社のサイバーセキュリティ業務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と業界のベストプラクティスを一致させる必要性を認識しました。次の業界参照のうちどれがこれを達成するのに適切ですか？
A. OSSIM
B. NIST
C. PCI
D. OWASP
正解: **(**正解を表示します**)**
説明/参照：
参照 :https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf

質問: **59**
サイバーセキュリティアナリストは、30のネットワーク資産のハードウェアアドレスを発見するよう依頼されました。コマンドラインから、ARPスキャンを提供し、タスクを達成するための最も効率的な方法を反映するために使用されるツールはどれですか。
A. nmap
B. tracert
C. ping -a
D. nslookup
正解: **(**正解を表示します**)**
説明/参照：
参照 :https://serverfault.com/questions/10590/how-to-get-a-list-of-all-ip-addresses-and-ideally- a-lanのデバイス名

質問: **60**
新しい最高技術責任者（CTO）は、ローカルイントラネットのネットワーク監視サービスに関する推奨事項を求めています。CTOは、ゲートウェイとの間のすべてのトラフィックを監視する機能と、特定のコンテンツをブロックする機能を求めています。次の推奨事項のうち、組織のニーズを満たすものはどれですか。
A. ゲートウェイルータの内部インタフェースと外部インタフェースの両方でIPフィルタリングを設定することを推奨します。
B. ゲートウェイルーターの内部インターフェイスにIDSを、外部インターフェイスにファイアウォールをインストールすることをお勧めします。
C. ゲートウェイルーターの内部インターフェースにファイアウォールを、外部インターフェースにNIDSをインストールすることをお勧めします。
D. ゲートウェイルーターの内部と外部の両方のインターフェイスにIPSをインストールすることをお勧めします。
正解: **(**正解を表示します**)**

説明/参照：
Explanation:

質問: **61**
技術者が集中的な脆弱性スキャンを実行して、どのポートが悪用される可能性があるかを検出します。スキャン中は、いくつかのネットワークサービスが無効になり、運用に影響があります。どのネットワークサービスが中断されたかを評価するために使用されるのは、次のうちどれですか。
A. syslog
B. ネットワークマッピング
C. ファイアウォールログ
D. NIDS
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **62**
何人かのユーザーは、チームのフォルダにドキュメントを保存しようとすると、次のメッセージが表示されると報告しています。
ファイルをコピーまたは移動できません - サービスを利用できません。
さらに調査したところ、syslogサーバーは、ユーザーがファイルのコピーを試みているファイルサーバーからログイベントを取得していないことがわかりました。次のうちどれがこれらの問題を引き起こす可能性が最も高いシナリオですか？
A. ファイルサーバーのCPUとメモリの使用率が高い
B. ファイルサーバの空き容量がすべて消費されています
C. ファイルサーバー上で悪意のあるプロセスが実行されています
D. ネットワークは飽和状態にあり、ネットワークの輻輳が発生しています
正解: **D (**コメントを発表する**)**

質問: **63**
最高情報セキュリティ責任者（CISO）は、セキュリティプログラムの基盤となるフレームワークを特定するようセキュリティスタッフに依頼しました。CISOは、セキュリティプログラムがすべて

の必要なベストプラクティスを満たしていることを示す認証を取得したいと考えています。次のうちどれが最良の選択でしょうか？
A. SDLC
B. OSSIM
C. ISO
D. SANS
正解: **(**正解を表示します**)**

質問: **64**
アナリストがSIEMダッシュボードで異常なアラートを受信しました。アナリストは、業務に影響を与えずにハッカーがターゲットシステムに送信しているペイロードを取得したいと考えています。アナリストは次のうちどれを実装すべきですか？
A. ハニーポット
B. ジャンプボックス
C. サンドボックス
D. 仮想化
正解: **A (**コメントを発表する**)**
説明/参照：
Explanation:

質問: **65**
アプリケーション開発会社がそのソフトウェアの新しいバージョンを一般に公開しました。リリースから数日後、同社はエンドユーザーからアプリケーションの動作が著しく遅くなったことを知らされ、古いセキュリティのバグが新しいリリースで再発しました。開発チームは、報告された問題に対処するために、次の開発サイクルでセキュリティアナリストを含めることを決定しました。セキュリティアナリストは、報告されている既存の問題を解決するために次のうちどれに焦点を当てるべきですか？
A. セキュリティアナリストは、各アプリケーション開発サイクルの間にセキュリティ回帰テストを実行する必要があります。
B. セキュリティアナリストは、各アプリケーション開発サイクルの間にアプリケーションの脆弱性を見つけるためにアプリケーションファジングを実行する必要があります。
C. セキュリティアナリストは、各アプリケーション開発サイクルの間に安全なコーディング方法を実行する必要があります。
D. セキュリティアナリストは、各アプリケーション開発サイクルの間にエンドユーザー承認セキュリティテストを実行する必要があります。
正解: **(**正解を表示します**)**

質問: **66**
あるエグゼクティブがセキュリティアナリストに、特定の攻撃経路に関する過去のログ、トラフィック、アラートを集計するよう依頼しました。その後、アナリストはデータを分析し、この攻

撃ベクトルに関する将来の問題を予測しました。セキュリティアナリストが最も実施している可能性があるのは、次の種類の分析のうちどれですか。
A. 行動分析
B. 利用可能分析
C. トレンド分析
D. 経営分析
正解: **(**正解を表示します**)**

質問: **67**
機密性と整合性を考慮して、サーバーをデスクトップより安全にするのはどれですか。
（3つ選択）
A. 処理能力
B. OS
C. 物理アクセス制限
D. ハードドライブ容量
E. 訓練を受けたオペレータ
F. VLAN
正解: **(**正解を表示します**)**

質問: **68**
セキュリティアナリストがSIEMからの警告に気付いた。ワークステーションが繰り返しポートに接続しようとしています
実稼働ネットワーク上の445のファイルサーバー。試行はすべて無効な認証情報で行われます。次のうちどれが起こっているのか説明しますか？
A. 攻撃者がワークステーションを制御し、SMBセッションを作成してファイルサーバーに移動しようとしています。
B. マルウェアがワークステーションを感染させ、ファイルサーバーの特定のIPアドレスにビーコンアウトしています。
C. 攻撃者がワークステーションを制御し、ネットワークをポートスキャンしています。
D. ファイルサーバーは、SMB経由でマルウェアをワークステーションに転送しようとしています。
正解: **A (**コメントを発表する**)**

質問: **69**
製造業のソフトウェア開発会社が、主力製品のアルファ版を完成させたばかりです。アプリケーションは過去3年間開発中です。SOCは、特定のAPTに関連した指標による侵入の試みを見てきました。同社はCOOPのホットサイトの場所を持っています。次の脅威のうちどれが最も大きな経済的影響を会社にもたらすでしょうか？
A. ICSの破壊
B. IPS回避

C. IPの盗難
D. DDoS
正解: **(**正解を表示します**)**

質問: **70**
Webアプリケーションには、既知の会社のユーザーを検証するために使用される認証方法に新たに発見された脆弱性があります。 「password」というパスワードを持つAdminのユーザーIDは、インターネットを介したアプリケーションへの昇格したアクセスを許可します。次のうちどれが運用展開前に脆弱性を発見するための最良の方法ですか？
A. 入力検証
B. ユーザー受け入れテスト
C. アプリケーションのストレステスト
D. 手動ピアレビュー
正解: **(**正解を表示します**)**

質問: **71**
セキュリティアナリストは、組み込みデバイスのユーザーインターフェイスが一般的なSQLインジェクションに対して脆弱であると判断しました。デバイスを交換できず、ソフトウェアをアップグレードできません。セキュリティアナリストは、このデバイスに追加のセキュリティを追加することをお勧めしますか？
A. セキュリティアナリストは、このデバイスをWAFの背後に配置することをお勧めします。
B. セキュリティアナリストは、このデバイスが定期的にWebログをSIEMシステムにエクスポートすることをお勧めします。
C. セキュリティアナリストは、このデバイスを定期的な脆弱性スキャンに含めることを推奨するべきです。
D. セキュリティアナリストはIDSをネットワークセグメントに配置することを推奨します。
正解: **(**正解を表示します**)**

質問: **72**
SIEMのアナリストは、ゲスト無線ネットワークからいくつかのEHR（Electronic Health Record）システムへの活動の急増に気づいた。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にアップロードされたことを発見しました。アナリストは最初に次の行動のうちどれを行うべきですか？
A. 違反を報告するために公民権局（OCR）に連絡してください
B. ゲートウェイルータにACLを設定
C. インシデント対応計画を有効にする
D. 最高プライバシー責任者（CPO）に通知する
正解: **(**正解を表示します**)**

質問: **73**

セキュリティアナリストがActive Directoryのレビューを実行していて、経理部門で2つの新しいユーザーアカウントを発見しました。どちらのユーザーも昇格した権限を持っていませんが、グループ内のアカウントには、既定で会社の重要な財務管理アプリケーションへのアクセス権が与えられています。次のうちどれが最善の行動方針ですか？
A. インシデント対応計画に従って新規アカウントを導入する
B. アプリケーションからのアウトバウンドトラフィックのデータ流出の兆候を監視します
C. アカウントが有効であることを確認し、ロールベースのアクセス許可が適切であることを確認します。
D. 機密アプリケーションへのアカウントのアクセス権限を削除します
E. ユーザーアカウントを無効にします
正解: **C** (コメントを発表する)

質問: **74**
技術者が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、次のうちどれがBEST分析ですか？
A. このアラートはSIEMによって生成されたものです。ユーザーが無効なログイン試行を多く試みたためです。
B. この警告は、ユーザーが動的DNSを使用してセキュリティ対策を回避しようとしていることを示します。
C. この警告は、エンドポイントが感染している可能性があること、および疑わしいホストに連絡している可能性があることを示します。
D. 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。
正解: (正解を表示します)

質問: **75**
管理は、ネットワークの外部から社内の重要なサーバーへの管理者アクセスに関係しています。具体的には、ファイアウォールの規則により、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。次のうちどれが効果的な解決策でしょうか？

A. マルウェア対策
B. サーバーの強化
C. ハニーポット
D. ジャンプボックス
正解: (正解を表示します)

質問: **76**
会社Aは、会社Bのビジネスパートナーに会社Aの会議室で利用可能なイーサネットポートを利用することを許可します。このアクセスはパートナーがVPNを会社Bのネットワークに確立することを可能にするために提供されます。会社Aのセキュリティアーキテクトは、会社Bのパートナーが利用可能なポートからのみインターネットに直接アクセスできるようにし、会社Aの従業員は同じポートから会社Aの内部ネットワークにアクセスできるようにしたいと考えています。次のうちどれがこれを可能にするために採用することができますか？
A. SIEM
B. ACL
C. SAML
D. MAC
E. NAC
正解: (正解を表示します)

質問: **77**
次のどの修復戦略のうち、組み込みICSがネットワークベースで侵害されるリスクを軽減するのに最も効果的ですか。 2つ選択してください。）
A. パッチ
B. NIDS
C. セグメンテーション
D. 未使用のサービスを無効にする
E. ファイアウォール
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **78**
サイバーセキュリティアナリストは、攻撃を受けたユーザーの資格情報への攻撃の原因を突き止めました。ログ分析の結果、攻撃者は不正な外国からの認証に成功したことを確認しました。経営陣は、セキュリティアナリストに、危殆化したパスワードに基づく攻撃を軽減するための解決策を調査して実装するよう依頼しました。アナリストは次のうちどれを実装すべきですか？
A. セルフサービスパスワードのリセット
B. シングルサインオン
C. コンテキストベース認証
D. パスワードの複雑さ
正解: **C (**コメントを発表する**)**
説明/参照：
Explanation:

質問: **79**
システム管理者が次の出力を確認しました。

```
#nmap server.local
Nmap scan report for server.local (10.10.2.5)
Host is up (0.3452354s latency)
Not shown:997 closed ports

PORT      STATE     Service
22/tcp    open      ssh
80/tcp    open      http

#nc server.local 80
220 server.local Company SMTP server (Postfix/2.3.3)
#nc server.local 22
SSH-2.0-OpenSSH_7.1p2 Debian-2
#
```

次のうちシステム管理者は上記の出力から推測できますか？
A. 会社の電子メールサーバーは標準外のポートを実行しています。
B. 会社の電子メールサーバーが危険にさらされています。
C. 同社は脆弱なSSHサーバーを運営しています。
D. 会社のWebサーバーが危険にさらされています。
正解: **(**正解を表示します**)**
説明/参照：
Explanation:

質問: **80**
次の原則のどれがセキュリティアナリストがインシデントの間にどのようにコミュニケーションをとるべきかについて説明しますか？
A. コミュニケーションはセキュリティスタッフのみに限定されるべきです。
B. コミュニケーションは法執行機関からのものであるべきです。

C. コミュニケーションは経営陣だけに制限されるべきです。
D. コミュニケーションは信頼できる当事者だけに限定されるべきです。
正解: **A** (コメントを発表する)

質問: **81**
Linuxマシンからの次の出力があるとします。
file2cable -i eth0 -f file.pcap
次のうちどれがセキュリティアナリストが達成しようとしていることを説明していますか？
A. アナリストはインターフェイスeth0上のトラフィックをキャプチャしようとしています。
B. アナリストはプロトコルアナライザを使用してネットワークトラフィックを監視しようとしています。
C. アナリストは、インターフェースeth0で帯域利用率を測定しようとしています。
D. アナリストはPCAPファイルのトラフィックをキャプチャしようとしています。
E. アナリストはPCAPファイルからキャプチャしたデータを再生しようとしています。
正解: (正解を表示します)

質問: **82**
SDLCの一環として、ソフトウェア開発者は大量のランダムデータを入力することによって新しいWebアプリケーションのセキュリティをテストしています。次の種類のテストはどれですか。
A. 回帰テスト
B. あいまい
C. 入力検証
D. ストレステスト
正解: (正解を表示します)

質問: **83**
Webアプリケーションの脆弱性スキャン中に、SQLデータベースサーバに接続されたWebフォームに特定のキーフレーズが入力された後、アプリケーションが不適切なデータを表示することが発見されました。次のうちどれが機密データを返すこの種の攻撃の可能性を減らすために使用されるべきですか？
A. アプリケーションファジング
B. 入力検証
C. 静的コード解析
D. ピアレビューコード
正解: (正解を表示します)

質問: **84**
セキュリティ管理策のレビュー中、アナリストはワークステーションから外部の安全でないFTPサーバに接続することができました。アナリストはトラブルシューティングを行い、ワークステーションが接続されているセグメントファイアウォールのACLを確認しました。

Seq	Direction	Source IP/Mask	Dest IP/Mask
1	In	10.1.1.0/255.255.255.0	172.21.50.5/255.25
2	Out	172.21.50.5/255.255.255.255	10.1.1.0/255.255.2
3	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.2
4	Out	10.1.1.0/255.255.255.0	10.1.1.0/255.255.2
5	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.2
6	Out	10.1.1.0/255.255.255.0	10.40.40.0/255.255
7	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.2
8	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0
9	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0
10	Any	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

上記のACLに基づいて、アナリストがFTPサーバーに接続できた理由は次のうちどれですか？

A. FTPはACLのシーケンス8で明示的に許可されていました。

B. FTPはACLのシーケンス10で許可されました。

C. FTPはACLのSeq 3とSeq 4に含まれるものとして許可されていました。

D. FTPはACLのシーケンス9からの送信として許可されていました。

正解: **A** (コメントを発表する)

説明/参照：

質問: **85**

サイバーセキュリティアナリストには、APT活動の可能性を確認するためのSIEMイベントログがいくつかあります。アナリストは、IPアドレスとドメインの両方の指標のリストを含むいくつかの項目を与えられました。アナリストが実行するための最善のアプローチは次のうちどれですか。

A. IPアドレスを使ってイベントログを検索します。

B. 手動でレビューしながらイベントの傾向を分析して、いずれかの指標が一致するかどうかを確認します。

C. すべての指標を含む高度なクエリを作成し、一致するものをすべて確認します。

D. APTによって使用されたことが知られているエクスプロイトで脆弱性をスキャンします。

正解: (正解を表示します)

説明/参照：

Explanation:

質問: **86**

同様の3つの運用サーバーが脆弱性スキャンを受けました。スキャンの結果、3台のサーバーに 探刻」と評価された2つの異なる脆弱性があることが明らかになりました。

管理者は、3つのサーバーについて次のことを確認しました。

サーバーはインターネットからアクセスできない

- AVプログラムは、2週間前と同じくらい最近サーバーがマルウェアを持っていたことを示します
- SIEMは、過去20日間で異常なトラフィックを示しています
- システムファイルの整合性検証は不正な変更を示しています

次の評価のどれが有効であり、最も適切なNEXTステップは何ですか？ 2を選択）
A. サーバー上で脆弱性スキャンを定期的にスケジュールします。
B. サーバーは改ざんされている可能性があります
C. サーバーが矛盾して構築された可能性があります
D. サーバーがSIEM経由で誤検知を生成している可能性があります
E. すぐに既知の良い設定からサーバーを再構築
F. インシデント対応計画を有効にする
正解: **E,F** (コメントを発表する)

質問: **87**
ある組織が、そのWebサーバーに関連する脆弱性を修正したいと考えています。最初の脆弱性スキャンが実行され、アナリストが結果を確認しています。修正を開始する前に、アナリストは、実際の脆弱性ではない問題に時間を費やすことを避けるために、誤検知を取り除きたいと考えています。
次のうちどれが偽陽性の可能性があるの指標でしょうか？
A. スキャナーコンプライアンスプラグインが古いことをレポートが示しています。
B. 「低」と表示された項目は情報提供のみを目的としています。
C. スキャン結果のバージョンは自動資産インベントリとは異なります。
D. 'HTTPS'エントリはWebページが安全に暗号化されていることを示します。
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **88**
電子メールの添付ファイルを開こうとした後、人事部の従業員がデバイスが応答しなくなるという問題を抱え始めました。知らされると、セキュリティアナリストは、IDSに異常な動作やウイルス対策ソフトウェアからのアラートが発生していなくても、状況に疑いを抱くようになりました。次のうちどれがこの状況での脅威の種類を説明しますか？
A. 死の包み
B. ゼロデイマルウェア
C. PIIの抽出
D. 既知のウイルス
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **89**
次のようなアクセスログがあるとします。

次のうちどれが正確にこのログが表示するものを説明しますか？

A. jQueryの脆弱性

B. Javascriptの脆弱性

C. インターネットから実行された脆弱性スキャン

D. 外部でホストされているデータベースとのアプリケーション統合

正解: **C** (コメントを発表する)

質問: **90**

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
- wordpad.exe
- notepad.exe

アナリストは不正なプロセスを判断するために次のツールのうちどれを利用すべきですか？

A. ping 127.0.0.1。

B. grepto検索を使います。

C. Nessusを使います。

D. Netstatを使用してください。

正解: **D** (コメントを発表する)

質問: **91**

次のうちどれが脅威管理のためのログによる相関分析に有効ですか？

A. SIEM

B. SCAP

C. IPS

D. PCAP

正解: (正解を表示します)

質問: **92**
セキュリティアナリストは、特定のサーバーがその月の間に1TBを超える帯域幅を消費したことに気付きました。ポート3333が開いています。ただし、サーバーまたはその活動に関するアラートや通知はありません。アナリストは次のうちどれを発見しましたか。
A. 誤検知
B. APT
C. DDoS
D. ゼロデイ
正解: **(**正解を表示します**)**

質問: **93**
データセンターへのアクセスは、すべてのデータセンターへの出入りを記録する近接バッジで制御されます。
アクセス記録は、機器の盗難の際にどのスタッフがデータセンターにアクセスしたかを識別するために使用されます。
このポリシーを有効にするために、次のうちどれを防ぐ必要がありますか？
A. 共連れ
B. ソーシャルエンジニアリング
C. フィッシング
D. パスワード再利用
正解: **A (**コメントを発表する**)**

質問: **94**
悪意のあるユーザーが次の出力を確認しています。
root :~#ping 192.168.1.137
192.168.2.1から64バイトicmp_seq = 1 ttl = 63 time = 1.58 ms
192.168.2.1から64バイトicmp_seq = 2 ttl = 63 time = 1.45 ms
root :~#
上記の出力に基づいて、悪意のあるユーザーとターゲットの間のデバイスはどれですか？
A. ハブ
B. アクセスポイント
C. スイッチ
D. プロキシ

正解: **D** (コメントを発表する)

質問: **95**
本番Webサーバーでパフォーマンスの問題が発生しています。調査の結果、未承認の新しいアプリケーションがインストールされ、不審なトラフィックが未使用のポートを介して送信されました。エンドポイントセキュリティは、マルウェアやウイルスを検出していません。次の種類の脅威のうちどれがこのMOSTに分類される可能性がありますか？
A. バッファオーバーフローの脆弱性
B. ボットネット
C. 高度な持続的脅威
D. ゼロデイ
正解: (正解を表示します)

質問: **96**
ある企業が、訪問者が使用する共通の領域内の多数のネットワークドロップの1つを介してネットワークリソースにアクセスしている不正なデバイスを発見しました。
会社は、許可されていないデバイスがネットワークにアクセスするのを迅速に防止したいが、接続しているすべてのクライアントに対して会社が変更を加えることを防止することを決定します。
次のうちどれを実装する必要がありますか？
A. 強制アクセス制御
B. ネットワーク侵入防止
C. WPA2
D. ポートセキュリティ
正解: (正解を表示します)

質問: **97**
ファイアウォールログの定期的な見直しの間に、アナリストは、組織のサーバーサブネットからのIPアドレスが夜間に外部IPアドレスに接続し、毎回150から500メガバイトのデータを送信していたことを確認しました。これは約1週間継続しており、影響を受けるサーバーはフォレンジックレビューのためにオフラインにされました。次のうちどれがインシデントの影響評価を促進する可能性が最も高いですか？
A. 会社の従業員と顧客のPIIが抽出されました。
B. 会社に関する生の財務情報にアクセスしました。
C. サーバーのフォレンジックレビューには、効率の悪いサービスへのフォールバックが必要でした。
D. IPアドレスとその他のネットワーク関連の設定が抽出されました。
E. 影響を受けるサーバーのローカルルートパスワードが危険にさらされました。
正解: **A** (コメントを発表する)
説明/参照：

Explanation:

質問: **98**
次のポリシーのどれがデータ所有権ポリシーの目的を最もよく説明していますか？
A. ポリシーは、承認されたユーザーが適切なデータにアクセスするための組織によるアカウントの管理を概説する必要があります。
B. このポリシーは、企業ネットワークまたはインターネット上のデータにアクセスするためにユーザーが従う必要がある慣行を文書化する必要があります。
C. ポリシーは、ユーザーと管理者間の役割と責任、および特定のデータタイプの管理について説明する必要があります。
D. ポリシーは、規制上またはビジネス上のニーズに基づいて情報タイプを保持するためのプロトコルを確立する必要があります。
正解: **(**正解を表示します**)**

質問: **99**
セキュリティアナリストがフォレンジック用のイメージのコピーを作成するために使用するコマンドはどれですか。
A. dd
B. rm
C. 触れる
D. wget
正解: **(**正解を表示します**)**

質問: **100**
アナリストは、ワークステーションからの異常なネットワークトラフィックを観察しています。ワークステーションは、暗号化されたトンネルを介して既知の悪質なサイトと通信しています。更新されたアンチウイルスシグネチャファイルを使用したフルアンチウイルススキャンでは、感染の兆候は見られません。次のうちどれがワークステーションで発生しましたか？
A. ゼロデイ攻撃
B. 既知のマルウェア攻撃
C. セッションハイジャック
D. クッキーを盗む
正解: **A (**コメントを発表する**)**
説明/参照：
Explanation:

質問: **101**
次のどれが、モバイルアプリケーションが、同じモバイルデバイス上の別のアプリケーション（ソーシャルメディア上でそのデバイスで再生している現在の曲の名前を投稿する音楽アプリ

ケーションなど)によってのみ利用可能であるべき情報にアクセスして操作できるようにするコントロールです。サイト）？
A. 二重認証
B. 相互排他アクセス
C. 推移的な信頼
D. 共同ホストアプリケーション
正解: **(**正解を表示します**)**

質問: **102**
組織は、重要なサービスの質の低下と重要な外部リソースの可用性を経験しています。次のうちどれが問題の調査に使用できますか？
A. 脆弱性分析
B. リスク分析
C. 行動分析
D. Netflow分析
正解: **D (**コメントを発表する**)**

質問: **103**
一連のIPアドレスに対するNmapスキャンの結果、"cpe :/ o :"で始まり、その後に会社名、製品名、およびバージョンが続く1行以上が返されました。次のうちどれがこの文字列が管理者の識別に役立ちますか？
A. オペレーティングシステム
B. インストールされているハードウェア
C. 稼働中のサービス
D. インストールソフトウェア
正解: **(**正解を表示します**)**

質問: **104**
さまざまなデバイスがネットワーク内の単一の邪悪な双子に接続し、認証しています。次のうちどれが最もターゲットにされている可能性がありますか？
A. 携帯端末
B. すべてのエンドポイント
C. VPN
D. ネットワーク基盤
E. 有線SCADA機器
正解: **(**正解を表示します**)**
説明/参照：
参照先 :http://www.corecom.com/external/livesecurity/eviltwin1.htm

質問: **105**

サイバーセキュリティアナリストが組織の脆弱性レポートを完成させており、それに資産を正確に反映させたいと考えています。次の項目のどれがレポートに含まれるべきですか？
A. プロセッサ使用率
B. 仮想ホスト
C. 組織統治
D. ログ処理
E. 資産の隔離
正解: (正解を表示します)
説明/参照：
Explanation:

質問: **106**
コンピュータがウイルスに感染しており、未知のサービスを介してサーバを指揮統制するためのビーコンを送信しています。セキュリティ技術者は、Command and Controlサーバーへのトラフィックをドロップしても、ファイアウォールログを介して感染したホストを識別できるようにするために、次のうちどれを実装する必要がありますか？
A. シンクホール
B. ポートとサービスをブロックする
C. パッチ
D. エンドポイントセキュリティ
正解: (正解を表示します)
説明/参照：
参照 :https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/tap / 58891

質問: **107**
サイバーセキュリティコンサルタントは、1週間以内に運用に入る予定の新しくインストールされたMS SQL Server 2012に対する脆弱性スキャンの次の出力を確認しています。

Summary
The remote MS SQL server is vulnerable to the Hello overflow

Solution
Install Microsoft Patch Q316333 or disable the Microsoft SQL Server service or use a firewall to protect the MS SQL port

References
MSB: MS02-043, MS02-056, MS02-061
CVE: CVE-2002-1123
BID: 5411
Other: IAVA 2002-B-0007

上記の情報に基づいて、システム管理者は次のうちどれをすべきですか？ (2を選択)
A. マイクロソフトのパッチQ316333をインストールして、提案された解決策を実施してください。
B. MS SQLポートを保護するために境界ファイアウォールでネットワークベースのACLを設定します。
C. 結果を誤検知としてマークし、以降のスキャンで表示されるようにします。
D. 参照を確認して、この脆弱性がリモートから悪用される可能性があるかどうかを判断します。
E. 侵入テストツールまたは概念実証のエクスプロイトを使用して脆弱性を確認します。
正解: **(**正解を表示します**)**

質問: **108**
ヒューリスティックシステムを使用してコンピュータのベースラインの異常を検出すると、システム管理者はIDSとウイルス対策をベースにしたシグネチャがそれを検出しなくても攻撃を検出することができました。さらに分析したところ、攻撃者は実行可能ファイルをUSBポートから会社のPCにダウンロードし、それを実行して特権の昇格の欠陥を引き起こすことが判明しました。次の攻撃のうちどれが最も起こりそうでしたか？
A. ディレクトリトラバーサル
B. クッキーを盗む
C. XMLインジェクション
D. ゼロデイ
正解: **D (**コメントを発表する**)**