CompTIA.CS0-001.v2019-05-21.q157

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：	157
バージョン：	v2019-05-21
ページの閲覧量：	1102
問題集の閲覧量：	28070

https://www.jpnshiken.com/shiken/CompTIA.CS0-001.v2019-05-21.q157.html

質問: **1**
次のうちどれが仮想マシンのホストOSとしてWindowsを使用する場合の脆弱性ですか？
A. Windowsは頻繁に修正プログラムを適用する必要があります。
B. Windowsは、動作するために何百ものファイアウォールポートを開く必要があります。
C. Windowsは "ping of death"に対して脆弱です。
D. Windowsの仮想化環境は通常不安定です。
正解: **(**正解を表示します**)**

質問: **2**
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。数日後
このリリースでは、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いこと、および古いセキュリティについての通知を受けました。
新しいリリースではバグが再現されています。開発チームはセキュリティを含めることを決定しました
次の開発サイクル中にアナリストが報告された問題に対処するのに役立ちます。次のうちどれセキュリティアナリストは、現在報告されている問題を解決するため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中に安全なコーディング方法を実行する必要があります。
サイクル。
B. セキュリティアナリストは、アプリケーションごとにエンドユーザー承認のセキュリティテストを実行する必要があります。
開発サイクル
C. セキュリティアナリストはそれぞれ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。
アプリケーション開発サイクル
D. セキュリティアナリストは、各アプリケーション開発中にセキュリティ回帰テストを実行する必要があります。

サイクル。
正解: **D** (コメントを発表する)

質問: **3**
セキュリティ調査のフォレンジック段階で、攻撃者が発見できることが判明しました。
安全性の低いチーム共有ドライブ上の秘密鍵。攻撃者はこれらの鍵を使って傍受し、復号化しました
Webサーバー上の機密トラフィック。次のうちどれが、この種の悪用とその可能性について説明しています
修復？
A. 中間者。秘密鍵の適切に管理された保管
B. セッションハイジャックネットワーク侵入検知センサー
C. クロスサイトスクリプティング暗号化キーサイズの増加
D. ルートキット公開鍵の管理された保管
正解: **A** (コメントを発表する)

質問: **4**
コンピュータがウイルスに感染しており、サーバを指揮統制するためのビーコンを送信している未知のサービスを通じて。セキュリティ技術者は、次のうちどれを削除する必要があります。
Command and Controlサーバーに送信され、それでも感染ホストを識別できるトラフィック
ファイアウォールログ？
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/ta-
p / 58891

質問: **5**
サイバーセキュリティアナリストがログデータを確認しているところ、以下のような出力が表示されます。

次のうちどれがこのログを生成した可能性がありますか。
A. ホスト型侵入検知システム
B. Webアプリケーションファイアウォール
C. ステートフルインスペクションファイアウォール
D. ネットワークベースの侵入検知システム
正解: **B** (コメントを発表する)

質問: **6**
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が与えられた。どっち
次のアクションはアナリストが実行するための最善のアプローチですか？
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: **7**
会社のコンピュータが犯罪を犯すために使用されました。システムは押収され、さらに撤去されました
分析。次のどれが差し押さえ時にケーブルと接続にラベルを付ける目的です
コンピューターシステム？
A. コンピュータシステムとの通信を攻撃から遮断する
B. 監護の連鎖を維持する
C. 削除された時点のシステム構成をキャプチャします
D. 接続されているケーブルのモデル、製造元、および種類を文書化する
正解: **C** (コメントを発表する)

質問: **8**
ヘルプデスクは、セキュリティアナリストに、疑わしいものに関して発展し始めている傾向について通知しました。
複数のユーザーによって報告された電子メール。アナリストは、電子メールに次のものが含まれていると判断しました
次のファイルを含むinvoice.zipという名前の添付ファイル：
Locky.js
xerty.ini
xerty.lib
さらに分析すると、.zipファイルが開かれると、新しいバージョンのランサムウェアをインストールしていることがわかります。
デバイスNASのデータが漏洩するのを防ぐために、最初に行うべきことは次のうちどれですか。
感染したデバイスで暗号化されていますか？
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: **9**
至るところで使用されている基本的なスクリーンキャプチャアプリケーション内に新しいゼロデイ脆弱性が発見されました
環境この脆弱性を発見してから2日後、ソフトウェアの製造元はその脆弱性を発見していません。修正を発表したか、この新たに発見された脆弱性に対する修正があるかどうか。傷つきやすいアプリケーションはそれほど重要ではありませんが、管理者や経営者によって使用されることがあります。
管理チームこの脆弱性により、リモートでコードが実行され、次のコードへの特権アクセスが可能になります。
システム。次のうちどれが、この脅威を軽減するための最善策ですか？
A. 製造者が許可するまでアプリケーションを使用しないことをエンドユーザーに伝えます。
脆弱性を解決しました。
B. 製造元と協力して修正プログラムの期間を決定します。
C. アプリケーションを削除し、それと同等の脆弱性のないアプリケーションと置き換えます。
D. ファイアウォールで脆弱なアプリケーショントラフィックをブロックし、それぞれのアプリケーションサービスを無効にします。
コンピューター。
正解: **(**正解を表示します**)**

質問: **10**
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
常にポート80を介して外部IPアドレスと通信しているのが観察されました。事件は
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、アナリストは決定しました
この活動は、新しいグラフィックデザインスイートを導入した直後に始まりました。この情報に基づいて、
以下の行動は、調査における適切な次のステップであろうか？
A. 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変更してグラフィックデザインを再インストールするよう依頼する
スイート。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。
B. 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。
C. 送信先IPアドレスとその所有者を特定し、実行中のプロセスを調べます。
活動が悪意のあるかどうかを判断するために影響を受けるホスト
D. すべてのウイルス対策製品とマルウェア対策製品、およびその他のすべてのホストベースのセキュリティソフトウェアをアップデートする。
影響を受けるユーザーが認証するサーバー。
正解: **(**正解を表示します**)**

質問: **11**
セキュリティアナリストが、ビジネスクリティカルをサポートするサーバーの脆弱性スキャンを完了しました。
外部のベンダーによって管理されているアプリケーション。スキャンの結果は、デバイスが見つからないことを示しています
重要なパッチ次のうちどれがこれらの脆弱性の修正を妨げることができますか？　を選択してください
ニ。）
A. 業務プロセスの中断
B. 補助仕入先とのSLA
C. 必要なサンドボックステスト
D. 不適切なデータ分類
E. 不完全な資産在庫
正解: **A,C (**コメントを発表する**)**

質問: **12**
ネットワーク技術者は、攻撃者がネットワークに侵入しようとしており、攻撃を仕掛けようとしていることを懸念しています。

攻撃者がネットワーク上でどのIPアドレスが有効であるかを知ることを防ぐためのファイアウォールに関する規則。
次のプロトコルのどれを拒否する必要がありますか？
A. ARP
B. ICMP
C. SMTP
D. TCP
正解: **B** (コメントを発表する)

質問: **13**
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、同社のメインWebへのHTTP POSTを観察している
サーバ。POSTヘッダーの長さは約1000バイトです。送信中、1バイトが配信されます
10秒ごと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. サービス拒否
C. ろ過
D. バッファオーバーフロー
正解: (正解を表示します)

質問: **14**
赤いチームアクターは、携帯電話が会社のコンピュータで充電できるようにするのが一般的なやり方であることを認めています、
ただし、メモリストレージへのアクセスはブロックされています。次のうちどれが一般的な攻撃手法です。
この慣習を利用する？ 2つ選んでください。）
A. 接続されているデバイスを、設定されたデバイスを偽装する不正なアクセスポイントに変えるUSB攻撃
ワイヤレスSSID
B. ブロックされているデバイスタイプでBluetooth接続を可能にする「Snarfing」と呼ばれるBluetoothピアリング攻撃
USBポートに物理的に接続されている場合
C. コンピュータをだまして、接続されているデバイスがキーボードであると判断させ、その後送信するUSB攻撃
攻撃を開始するためのキーボードとして1文字ずつ（事前に記録された一連のキーストローク）
D. システムを悪用してネットワークアダプタであると判断させ、その後ユーザーパスワードを実行するUSB攻撃
オフラインパスワードクラッキングのためのハッシュ収集ユーティリティ
E. デバイスのレジストリを変更して（Windows PCのみ）、フラッシュドライブに以下のことを許可するBluetooth攻撃。

マウントしてからJavaアプレット攻撃を仕掛ける
正解: **B,E** (コメントを発表する)

質問: **15**
ビジネスクリティカルなアプリケーションは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
特殊文字の使用が許可されていないためです。経営陣は、リスクを負うことを受け入れたくありません。
弱いパスワード標準によるセキュリティ上の問題の可能性。次のうちどれが適切ですか
アプリケーションに関連するリスクを制限するための手段ですか？
A. パスワードポリシーの変更
B. 認証トラフィックの暗号化
C. 補正コントロール
D. 新しいアカウント管理手順を作成する
正解: (正解を表示します)

質問: **16**
セキュリティアナリストが、次のものを含むと疑われる特定のサーバーのパケットキャプチャを確認しています
マルウェアを発見し、次のパケットを発見します。

```
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [SYN] Seq=0 Win=4128 Len=0 MSS=146
73.252.34.101 138.23.45.201 TCP dns (53) -> 56712 [SYN, ACK] Seq=0 Ack=1 Win=4128 Le
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [ACK] Seq=1 Ack=1 Win=4128 Len=0
73.252.34.101 138.23.45.201 SSH Server: Protocol (SSH-2.0-Cisco-1.25)
138.23.45.201 73.252.34.101 SSH Client: Protocol (SSH-1.99-Cisco-1.25)
73.252.34.101 138.23.45.201 SSHv2 Server: Key Exchange Init
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [SYN] Seq=0 Win=65535 Len=0
73.252.34.101 103.34.243.12 TCP ftp (21) -> 62014 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [ACK] Seq=1 Ack=1 Win=65535 Len=0
73.252.34.101 103.34.243.12 FTP Response: 220 ProFTPD 1.3.0a Server
103.34.243.12 73.252.34.101 FTP Request: User FTP
73.252.34.101 103.34.243.12 FTP Response: 331 Anonymous login ok, send your complete
as your password.
103.34.243.12 73.252.34.101 FTP Request: Pass ftp
73.252.34.101 103.34.243.12 FTP Response: 230 Anonymous access granted, restrictions
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[SYN] Seq=0 Win=5840 Len=0 MSS=1460 SAC
835172936 TSecr=2216538 WS=64
73.252.34.101 202.53.245.78 TCP 8080 -> 57678[SYN, ACK] Seq=1 Ack=1 Win=5888 Len=0 T
TSecr=835172936
202.53.245.78 73.252.34.101 HTTP GET /images/layout/logo.png HTTP/1.0
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[ACK] Seq=135 Ack=2897 Win=11648 Len=0
TSecr=835172936
```

次のトラフィックパターンまたはデータのうち、セキュリティアナリストにとって最も重要なものはどれですか。
A. 202.53.245.78からのHTTPトラフィックに使用されるポート
B. 103.34.243.12によって付与された匿名アクセス
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
正解: (正解を表示します)

質問: **17**
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: **18**
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、不正なサービスが不正であることを発見しました。
会社のコンピュータで実行されています。

```
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、それは不正なサービスへのさらなるアクセスのみを妨げるでしょう。
そして他のサービスに影響を与えませんか？
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: **19**
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。
どっち
次のうち何が起こっているのか？
A. 攻撃者がワークステーションを制御し、作成してファイルサーバーに移動しようとしていますSMBセッション
B. 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。
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. 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。
正解: (正解を表示します)

質問: **20**
セキュリティアナリストが、歴史的な問題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。
SIEMアラートアナリストは、非共通ポートでSSLを利用しているネットワーク接続に気付いた。
%TEMP%フォルダ内のsvchost.exeとcmd.exe、および外部IPに接続していたRDPファイル。どれの
セキュリティアナリストは次の脅威を発見しましたか？
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: **21**
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管理者だけに制限されるべきです。
B. 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。
C. 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。
D. コミュニケーションは法執行機関から来るべきです。
正解: **(**正解を表示します**)**

質問: **22**
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。の
技術者が調査し、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配線されていることに気付く
ローリングチェアの真下にあり、時間の経過とともに平らに粉砕されています。
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. クロストーク
B. 過剰な衝突
C. 電磁波障害
D. 分割ペア
正解: **(**正解を表示します**)**

質問: **23**
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。与えられた
認証情報を実行しながら、認証情報がネットワークを通過するのを防ぐという要件
スキャン、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. スキャナーとエンドポイント間のすべてのトラフィックを暗号化します
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. 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
正解: **D (**コメントを発表する**)**

質問: **24**
サイバーセキュリティコンサルタントは、新たな攻撃者に対する脆弱性スキャンの次の出力を確認しています
1週間以内に運用開始予定のMS SQL Server 2012をインストールしました。

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. 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。
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. 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てください。
D. 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。
E. 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。
正解: **B,D** (コメントを発表する)

質問: **25**
次の修復戦略のどれが、ネットワークベースのリスクを減らすのに最も効果的ですか
組み込みICSの妥協 (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: **C,D** (コメントを発表する)
説明/参照：
Explanation:

質問: **26**
店舗の場所とIPスペースが広く分散している小売企業は、PCIの要件を満たす必要があります。
脆弱性スキャンに関する。組織はこの機能を第三者に外部委託することを計画しています。
コストを削減。
次のうちどれがスキャンの実行に関連する期待を伝えるために使用されるべきですか？
A. 覚書
B. 教訓として文書化
C. 脆弱性評価報告書
D. SLA

正解: **D** (コメントを発表する)

質問: **27**
何人かのユーザーは、チームフォルダにドキュメントを保存しようとすると、次のように報告しています。
メッセージが受信されます。
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。
ユーザーがファイルをコピーしようとしている場所。次のうちどれが最も起こりそうなシナリオです
これらの問題？
A. ファイルサーバーのCPUとメモリの使用率が高い
B. ファイルサーバー上で悪意のあるプロセスが実行されています
C. ファイルサーバの空き容量がすべて消費されています
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: **28**
重要なApache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。
脆弱性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: **29**
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。調査の際、新しい未承認
アプリケーションがインストールされ、疑わしい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
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になりますか
として分類？
A. ゼロデイ
B. ボットネット
C. バッファオーバーフローの脆弱性
D. 高度な持続的脅威

正解: **D** (コメントを発表する)

質問: **30**
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、次の場合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。
機器の盗難
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. フィッシング
B. 共連れ
C. ソーシャルエンジニアリング
D. パスワード再利用
正解: **B** (コメントを発表する)

質問: **31**
脆弱性アナリストは、10.1.1.0 / 24に未承認のWebサーバーを持つすべてのシステムを特定する必要があります。
ネットワーク。アナリストは次のデフォルトのNmapスキャンを使用します。
nmap -sV -p 1-65535 10.1.1.0/24
次のうちどれが上記のコマンドを実行した結果でしょうか？
A. このスキャンはすべてのTCPポートをチェックします。
B. このスキャンは不正なサーバーを識別します。
C. このスキャンはすべてのポートを調べ、開いているポートを返します。
D. このスキャンはすべてのTCPポートをチェックしてバージョンを返します。
正解: (正解を表示します)

質問: **32**
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. 訓練を受けたオペレーター
B. OS

C. VLAN
D. 物理アクセス制限
E. ハードドライブ容量
F. 処理能力
正解: **A,B,D (**コメントを発表する**)**

質問: **33**
セキュリティアナリストは、境界ファイアウォール上にある着信パケットを拒否するACLを作成しています。
内部アドレス、反転外部アドレス、およびマルチキャストアドレス。次のどれが
アナリストが防止しようとしていますか？
A. なりすまし攻撃
B. DDoS攻撃
C. ブロードキャストストーム
D. 中間者攻撃
正解: **(**正解を表示します**)**

質問: **34**
次のうちどれが直接vSphere ESXiのパッチ未適用の脆弱性によって影響を受ける可能性がありますか？
A. 組織の仮想インフラ
B. 組織のモバイル機器
C. 組織の物理ルーター
D. 組織のVPN
正解: **(**正解を表示します**)**

質問: **35**
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
脆弱性が修正されたことを確認するためにソフトウェアをテストすることを課題としています。
アプリケーションはまだ正しく機能しています。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: **36**
組織のポリシーでは、1週間以内に重大度7以上の脆弱性修正が必要です。なんでも
重大度が7未満の場合、30日以内に修復する必要があります。組織にもセキュリティが必要
修復を実行する前に、脆弱性の詳細を調査するチーム。調査の場合
検出結果が誤検知であることを確認し、修復は実行されず、脆弱性スキャナーを実行します。
今後のスキャンから誤検知を除外するように設定が更新されました。
この組織には3つのApache Webサーバーがあります。

192.168.1.20 - Apache v2.4.1
192.168.1.21 - Apache v2.4.0
192.168.1.22 - Apache v2.4.0

最近の脆弱性スキャンの結果は以下のとおりです。

```
---
Scan Host: 192.168.1.22

15-Feb-16 10:12:10.1 CDT

Vulnerability CVE-2006-5752

Cross-site scripting (XSS) vulnerability in the mod_status module of Apache server
(httpd), when ExtendedStatus is enabled and a public-server-status page is used,
allows remote attackers to inject arbitrary web script or HTML.

Severity: 4.3 (medium)

---
```


チームは調査を行い、Apacheからの発言を見つけます。

```
"Fixed in Apache HTTP server 2.4.1 and later"
```

セキュリティチームは次のどの行動を実行する必要がありますか？
A. 30日以内に192.168.1.22を修正
B. 192.168.1.22の誤検知を無視します
C. 30日以内に192.168.1.20を修正
D. 192.168.1.20の誤検知を調査する
正解: **A** (コメントを発表する)

質問: **37**
アナリストは、今後のクライアントの参加の一環として、侵入テストアプリケーションを設定しています。
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します。次の種類のうちどれ
情報はSOWに伝統的に見られる情報に基づいて考慮されるべきですか？ 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: **A,C** (コメントを発表する)
説明/参照：
Explanation:

質問: **38**
企業が、多数のネットワークのうちの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た
訪問者が使用する一般的な場所に落ちます。
同社は、不正な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と考えています。
しかし、ポリシーによって、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が妨げられています。
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. WPA2
C. ポートセキュリティ
D. ネットワーク侵入防止
正解: (正解を表示します)

質問: **39**
サイバーセキュリティの専門家は、Webサーバーが IPを持つリモートホスト上で実行されているかどうかを判断したいと考えています。
アドレス192.168.1.100。次のうちどれがこのタスクを実行するために使用することができますか？
A. dig www 192.168.1.100を掘る
B. ping -p 80 192.168.1.100
C. nc 192.168.1.100 -1 80
D. nmap 192.168.1.100 -p 80 -A
E. ps aux 192.168.1.100
正解: (正解を表示します)

質問: **40**
ポリシーにより、実稼働時間中に脆弱性をスキャンすることができますが、実
ジュニアテクニシャンによる不正なスキャンにより最近クラッシュしました。次のどれが
この種のスキャンによる本番サーバーのダウンタイムを回避するための最良の方法は？
A. 集中スキャンからエージェントベーススキャンへの移行。
B. 訓練を受けた担当者による脆弱性スキャンの実施を要求してください。
C. 各スキャンの結果を分析するためにサンドボックスを実装します。
D. 毎日自動化された詳細な脆弱性レポートを設定します。
正解: **B** (コメントを発表する)

質問: **41**
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電子医療への活動の急増に気づいた
レコード（EHR）システムさらに分析した結果、アナリストは大量のデータが収集されたことを発見しました。
過去6か月以内にクラウドプロバイダにアップロードしました。アナリストは次のどの行動をとるべきか
最初？
A. インシデント対応計画を有効にする
B. 違反を報告するために公民権局（OCR）に連絡する
C. 最高プライバシー責任者（CPO）に通知する
D. ゲートウェイルータにACLを設定します
正解: **(**正解を表示します**)**

質問: **42**
アナリストは、脆弱性スキャナが原因で、パッチが当てられていないサーバが検出された脆弱性を発見した。
最新の署名セットはありません。経営陣はセキュリティチームに要員を配置するよう指示しました
スキャンを実行する少なくとも24時間前にスキャナを最新のシグネチャでアップデートします。
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: **43**
A社のセキュリティポリシーでは、すべてのSSHアカウントにPKI認証のみを使用するように規定されています。A
A社のセキュリティアナリストは、次のauth.logと構成設定を確認しています。

```
Nov 1 09:53:12 comptia sshd[16269]: Connection from 192.168.2.6 port 53349 on 192

Nov 1 09:53:12 comptia sshd[16269]: Failed publickey for dev from 192.168.2.6 por
SHA256:66c5a96384aa8ba16a71da278317edf4e62eda2c6453a736759186da3a2f7697
Nov 1 09:53:15 comptia sshd[16269]: Accepted password for dev from 192.168.2.6 pc
Nov 1 09:53:15 comptia sshd[16269]: pam_unix(sshd:session): session opened for us
Nov 1 09:53:15 comptia systemd-logind[590]: New session 499 of user dev.
Nov 1 09:53:15 comptia sshd[16269]: User child is on pid 16271
Nov 1 09:53:15 comptia sshd[16271]: Starting session: shell on pts/5 for dev from

Strict Modes no

RSAAuthentication yes

PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shots files

IgnoreRhosts yes

# For this to work you will also need host keys in /etc/ssh_known_hosts

RhostsRSSAuthentication no

# similar for protocol version 2

HostbasedAuthentication no

#Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication

# Ignore User KnownHost yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)

PermitEmptyPasswords no

# Change to yes to enable challenge-resposnse passwords (beware issues with

# some PAM modules and threads);

ChallengeResponseAuthentication no

# Change to no to disable tunneled clear text passwords

PasswordAuthentication yes
```

準拠を確立するために、次のsshd_configファイルに加えるべき変更は次のうちどれですか。
ポリシーと？

A. PermitRootLoginnotoを変更します。#PermitRootLoginyes

B. ChallengeResponseAuthenticationをChallangeResponseAuthenticationに変更します。
いいえ

C. PubkeyAuthenticationをyesに変更します。#PubkeyAuthentication yes

D. #AuthorizedKeysFile sh / .ssh / authorized_keystをAuthorizedKeysFile sh /に変更します。
.ssh / authorized_keys

E. PassworAuthenticationをPasswordAuthenticationに変更します。no

正解: **(**正解を表示します**)**

説明/参照：

質問: **44**

組織は、Common Vulnerability Scoring System（CVSS）スコアを使用して、の修復を優先します。脆弱性
経営陣は、難易度の低い脆弱性を回避するために、難易度に基づいて優先順位を変更したいと考えています。
CVSSスコアは、システム機能へのリスクが少なくても実装が簡単な場合は、優先順位が高くなる可能性があります。
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標を達成するでしょう
目的？
A. (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
B. (（CVSSスコア)* 2)/難易度=優先度
CVSSスコアが加重され、難易度が1から5の範囲で、5が最も簡単で最も低い場合
実施するリスク
C. (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
D. （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
正解: **D** (コメントを発表する)

質問: **45**
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. 業務上の理由
B. 権限
C. 支払条件
D. スケジュール
E. システム管理者の一覧
正解: (正解を表示します)

質問: **46**
ネットワーク管理者が、Webトラフィックの数を増やすことなくWebトラフィックの量を増やす場合
金融取引では、同社は次の攻撃のうちどれを経験しているのでしょうか。
A. サービス拒否
B. フィッシング
C. ブルージャック
D. ARPキャッシュポイズニング
正解: **A** (コメントを発表する)

質問: **47**
インシデントの後に教訓報告書を作成することは、アナリストがどの報告書を伝えるのに役立つかを示します。
以下の情報は？　2つ選択）
A. 業務上の対応を改善するための方針と慣行の強化
B. 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
C. IPアドレス、アプリケーション、および資産の一覧
D. 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
E. 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
正解: **(**正解を表示します**)**

質問: **48**
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
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。
B. 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。
C. 会社は、192.168.1.1からのトラフィックをすべて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。
彼らのゲートウェイルータ。
D. 会社はゲートウェイの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。
正解: **A (**コメントを発表する**)**

質問: **49**
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。
B. アナリストは、インターフェイスeth0の帯域利用率を測定しようとしています。
C. アナリストはインターフェイスeth0でトラフィックをキャプチャしようとしています。
D. 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。
E. 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。
正解: **E** (コメントを発表する)

質問: **50**
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。主な情報
役員（CIO）は、この投資がなければ、会社が次の被害者になる危険性があると確信しています。
同じサイバー攻撃が3か月前に経験した競合他社を攻撃します。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。どっち
次のようにすれば、このプラクティスによってもたらされるリスクを排除できますか？
A. 否認防止を確実にするためのソリューションに投資し、それを実行する
B. 毎日パスワードを変更する
C. ユーザーに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
D. 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。
正解: (正解を表示します)

質問: **51**
ファイアウォールログを定期的に見直している間に、アナリストは組織のIPアドレスが
サーバーのサブネットは、夜間に外部IPアドレスに接続していて、送信していました。
毎回150～500メガバイトのデータ。これは約1週間続いていました、
そして影響を受けた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。次のうちどれが運転する可能性が最も高いです
インシデントの影響評価をアップしますか？
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: **52**
小規模な地方銀行のセキュリティアナリストが、国家が国家の権利を行使しようとしているという警告を受けました
フィッシングキャンペーンを介して金融機関に侵入する。以下の手法のうちどれをアナリストが使うべきか
この種の脅威から防御するための予防策として推奨しますか。
A. 強制アクセス制御
B. ロケーションベースのNAC
C. 要塞ホスト
D. システムの分離
E. ハニーポット
正解: **(**正解を表示します**)**

質問: **53**
Webアプリケーションには、検証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。
知られている会社のユーザー。 「password」というパスワードを持つAdminのユーザーIDは、
インターネット上のアプリケーション。次のうちどれが以前に脆弱性を発見するための最良の方法です
本番展開ですか？
A. 入力検証
B. ユーザー受け入れテスト
C. 手動ピアレビュー
D. アプリケーションのストレステスト
正解: **(**正解を表示します**)**

質問: **54**
最近の監査では、以下のような多くの発見がありました。

192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable OS: Microsoft Windows Server 2012 R2 Vulnerable software installed: Adobe Flash 20.0.0.272
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Microsoft SharePoint Foundation 2010 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Word Server is running an affected version - 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\Patches\602FDAF466AB90540ADE467809F449F5 - key does not existPatch {4FADF206-BA66-4509-A0ED-6487904F945F} is not installed
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2007 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Office Excel Services is running an affected version - 12.0.6612.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\Patches\F6A389258DE016A46B54137BE227809A - key does not existPatch {52983A6F-0ED8-4A61-B645-31B72E7208A9} is not installed
192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2010 Based On the following 2 results: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109510190400100000000F01FEC\Patches\FC0008A30BA17544EB340C8942E98787 - key does not

次のうちどれがこれらの調査結果を修正し、類似の調査結果を最小にするための最良の方法でしょう。

未来？

A. 自動パッチ管理ソリューションを使用してください。

B. すべてのサーバーでMicrosoft Baseline Security Analyzerを実行します。

C. 影響を受けるソフトウェアプログラムをサーバーから削除します。

D. ネットワーク上のすべてのサーバーに対して定期的な脆弱性スキャンをスケジュールします。

正解: (正解を表示します)

質問: **55**
ある企業が、WPA2、20文字以上のWiFiパスフレーズ、および新しいWiFiを実装しました。
30日ごとにパスフレーズを設定し、すべてのワイヤレスアクセスポイントでSSIDブロードキャストを無効にしました。どっち
以下は、軽減しようとしている会社ですか？
A. ダウングレード攻撃
B. 強制認証解除
C. レインボーテーブル
D. SSL固定
正解: (正解を表示します)

質問: **56**
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、それに資産を反映させたいと考えています
正確に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: **57**
次のユーティリティのうちどれが、IPアドレスをドメイン名に解決するために使用される可能性があります。
アドレスにPTRレコードがありますか？
A. nbtstat
B. ifconfig
C. ping
D. arp
正解: (正解を表示します)

質問: **58**
サイバーセキュリティアナリストが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べきツールはどれですか。
調査の前後に？

A. 文字列
B. ファイル
C. gzip
D. sha1sum
E. dd
正解: (正解を表示します)

質問: **59**
次の行動のうちどれが未解決の問題に対処するために起こるべきか
ネットワーク内のさまざまな部門？
A. 教訓レポート
B. インシデント対応計画
C. CoC文書
D. リバースエンジニアリング工程
正解: (正解を表示します)

質問: **60**
システム管理者が重要なシステムを保護しようとしています。管理者がシステムを配置しましたファイアウォールの内側で強力な認証を有効にし、このシステムのすべての管理者が出席することを要求した
必須のトレーニング
次のBESTのどれが実装されているコントロールを説明しますか？
A. 深層防御
B. 監査修正
C. アクセス制御
D. 多要素認証
正解: (正解を表示します)

質問: **61**
最近の監査で、いくつかのコーディングエラーと、公衆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。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. Webプロキシ
B. ネットワークファイアウォール
C. Webアプリケーションファイアウォール
D. 侵入防止システム
正解: (正解を表示します)

質問: **62**
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. SCAP
B. PCAP
C. IPS
D. SIEM
正解: **D (**コメントを発表する**)**

質問: **63**
セキュリティアナリストは、シンクホールからのCPU使用率が急上昇し始めたことに気付き始めました。どっち
何が起こっている可能性があります説明します？
A. 誰かがシンクホールにログオンし、デバイスを使用しています。
B. 陥没穴が疑わしいまたは悪意のあるトラフィックをブロックし始めました。
C. 何かがシンクホールを制御し、悪意のある利用によるCPUスパイクを引き起こしています。
D. シンクホールが不正なトラフィックの再ルーティングを開始しました。
正解: **(**正解を表示します**)**

質問: **64**
次のうちどれが組織のデータ保持ポリシーに最も大きな影響を与えましたか？
A. 各データに割り当てられているCIA分類マトリックス
B. データセットに関する規制要件
C. データ所有者によって設定されたデータの機密性のレベル
D. データを保存するために使われた技術の技術的制約
正解: **(**正解を表示します**)**

質問: **65**
開発チームは現在、それぞれ特定の分野に特化した3人の開発者で構成されています。
プログラミング言語
開発者1 - C ++ / C#
開発者2 - Python
開発者3 - アセンブリ

次のSDLCベストプラクティスのうち、現在利用可能なものを使用して実装するのが難しいものはどれか
スタッフ？
A. ストレステスト
B. あいまい
C. ピアレビュー
D. 回帰テスト
正解: **(**正解を表示します**)**

質問: **66**
次の組織リソースのうち、有効なパスワードまたはPINがないのが一般的です。
脆弱性
A. VDIシステム
B. 携帯端末
C. VPN
D. VoIP電話
E. エンタープライズサーバOss
正解: **B (**コメントを発表する**)**

質問: **67**
最高情報セキュリティ責任者（CISO）は、トポロジーディスカバリーの実施および検証を求めました
資産インベントリに対して。発見は失敗し、信頼できるデータや完全なデータを提供していません。syslog
以下の情報を表示します。

```
Mar 16 14:58:31 myhost nslcd [16637]   :  [0e0f76] LDAP result  ( )  failed unable to authenticate
Mar 16 14:58:32 myhost nslcd [52255a]  :  [0e0f76] LDAP result  ( )  failed unable to contact
Mar 16 14:58:40 myhost nslcd [16637]   :  [0e0f76] LDAP result  ( )  failed to authenticate
Mar 16 14:58:42 myhost nslcd [52255a]  :  [0e0f76] LDAP result  ( )  failed unable to contact
```

次のうちどれが発見が失敗している理由を説明しますか？
A. LDAPを実行しているサーバーにウイルス対策ソフトウェアが展開されています。
B. LDAPサーバーへの接続がタイムアウトしました。
C. LDAPサーバーが間違ったポートに設定されています。
D. スキャンツールに有効なLDAP認証情報がありません。
E. スキャンはLDAPエラーコード52255aを返しています。
正解: **D (**コメントを発表する**)**

質問: **68**
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。初期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。修復を開始する前に、

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: **B** (コメントを発表する)
説明/参照：
Explanation:

質問: **69**
A社は、従業員がUSBメモリを介してPIIを盗用していると疑っています。アナリストが任務ドライブ上の情報を見つけようとしています。問題のPIIには以下が含まれます。

comp@mail.com	564-23-4765
tia@mail.com	754-09-3276
puter@mail.com	143-32-2323
sam@mail.com	545-11-0192
jim@mail.com	093-45-3748

アナリストに割り当てられたタスクを最もよく達成するのはどれですか？
A. \ d [9] 'XXX-XX-XX'
B. 3 [0-9] \ d-2 [0-9] \ d-4 [0-9] \ d
C. ？[3] - ？[2] - ？[3]
D. \ d {3} - d {2} - \ d {4}
正解: (正解を表示します)

質問: **70**
次のNISTのリスク管理の枠組みのステップのどれが情報システムになりますか
セキュリティエンジニアは、継承されたセキュリティ管理策を識別し、それらの管理策をシステムに合わせて調整しますか。
A. 実装する
B. 分類する
C. アクセス
D. 選択
正解: (正解を表示します)

質問: **71**
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
基本ユーザーアカウントKaliの最新版に含まれるいくつかのツールを使用して、アナリストは次のものにアクセスすることができました。
設定ファイル、フォルダとグループのアクセス許可の変更、および新しいシステムオブジェクトの削除と作成を行います。
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. なりすまし
C. 権限昇格
D. ディレクトリトラバーサル
正解: **D** (コメントを発表する)

質問: **72**
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. ShellShock
B. ゼウス
C. プードル
D. DROWN
E. ハートブリード
正解: (正解を表示します)

質問: **73**
最高情報セキュリティ責任者（CISO）は、セキュリティスタッフに、そのための枠組みを特定するよう依頼しました。
セキュリティプログラムの基盤となります。CISOはセキュリティプログラムを示す認証を取得したい
すべての必要なベストプラクティスを満たしています。次のうちどれが最良の選択でしょうか？
A. SDLC

B. ISO
C. OSSIM
D. SANS
正解: **B (**コメントを発表する**)**

質問: **74**
セキュリティアナリストは、許可されていないユーザーが自分のコンピュータに保存されている機密データにアクセスできることを懸念しています。
実動サーバー環境特定のネットワークセグメント上のすべてのワークステーションは、特定のネットワークセグメントに完全にアクセスできます。
実稼働中のサーバー。以下のうちどれを防止するために本番環境にデプロイする必要があります。
不正アクセス？　2つ選んでください。）
A. DLPシステム
B. ハニーポット
C. IPS
D. ジャンプボックス
E. ファイアウォール
正解: **D,E (**コメントを発表する**)**

質問: **75**
最近、Linuxベースのファイル暗号化マルウェアが発見されました。マルウェアを実行する前にその動作を分析するために事前設定されたサンドボックス、セキュリティ専門家は次のコマンドを実行します。
umount -a -t cifs、nfs
上記のコマンドを実行する主な理由はどれですか？
A. マルウェアがリモートシステムに影響を与えるかどうかをテストする
B. ネットワーク経由で重要なファイルをバックアップする
C. マルウェアがメモリ制限されていることを確認します。
D. マルウェアがローカルホストに到達するのを制限します。
正解: **(**正解を表示します**)**

質問: **76**
セキュリティアナリストがコンピュータ犯罪捜査を支援しており、PCを保護するよう求められています。
フォレンジックラボに届けます。次の項目のうちどれがPCを保護するのに最も役立ちますか？
3つ選んでください。）
A. 耐タンパーシール
B. ドライブ消しゴム
C. CoCの形

D. 書き込みブロッカー
E. ファラデー箱
F. マルチメータ
G. ネットワークタップ
正解: **A,C,E** (コメントを発表する)

質問: **77**
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、システム管理者は次のことができました。
会社のシグネチャベースのIDSとウイルス対策では検出されていないにもかかわらず、攻撃を検出します。さらに
分析の結果、攻撃者はUSBから会社のPCに実行可能ファイルをダウンロードしたことが判明しました。
そして、権限昇格の欠陥を引き起こすためにそれを実行しました。次の攻撃のどれが最も可能性があります
発生した？
A. クッキー窃盗
B. ゼロデイ
C. XMLインジェクション
D. ディレクトリトラバーサル
正解: **B** (コメントを発表する)

質問: **78**
ある会社がクレジットカード取引を直接処理することにしました。次のうちどれが満たすでしょう
このタイプのデータをスキャンするための要件
A. 毎月
B. 隔年
C. 四半期ごと
D. 毎年
正解: (正解を表示します)

質問: **79**
未知のソフトウェアの動作をテストして観察するために孤立した環境を作成することも
として知られている：
A. 硬化する
B. サンドボックス化
C. ハッシュ
D. 盗聴
正解: **(**正解を表示します**)**

質問: **80**
人事部の従業員が、機器を開けようとした後に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。
電子メールの添付ファイル。知らされると、セキュリティアナリストは状況に懐疑的になりました。
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はありませんでした。どっち
次のBESTは、この状況における脅威の種類を説明していますか
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: **81**
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は、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ました。この種の攻撃は、
次のうちどれ？
A. フィッシング
B. 中間者
C. ショルダーサーフィン
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: **82**
セキュリティアナリストが会社の次期監査の準備をしています。同社の最新の見直し時に
脆弱性スキャンの結果、セキュリティアナリストは次の未解決の問題を発見しました。

CVE ID	CVSS Base	Name
CVE-1999-0524	1.0	ICMP timestamp request remote date disclosure
CVE-1999-0497	6.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Microsoft WindowsSMB service enumeration via \srvsvc

次の脆弱性のうちどれが最初に改善のために優先されるべきですか？
A. \ srvsvcによるMicrosoft Windows SMBサービスの列挙
B. サポートされていないWebサーバーの検出
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
正解: **B** (コメントを発表する)

質問: **83**
インシデント中にメディアと対話することに関して、許可されているのはどれがベストプラクティスですか？
A. インシデントについては、インシデントについてメディアと話し合うことは絶対にしないでください。
B. インシデントについての知識がある上級管理職レベルの担当者には、それについて話し合うことを許可します。
C. インシデントによる損害の影響に関する財務情報を公開します。
D. 連絡先を1つ指定し、メディアとの連絡用に少なくとも1つのバックアップを指定します。
正解: (正解を表示します)

質問: **84**
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
以下の攻撃のうちどれが起こりましたか？
この攻撃による将来の影響のリスクを軽減しますか？ 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: **85**
一連のIPアドレスに対するNmapスキャンの結果、"cpe :/ o :"で始まりその後に続く1行以上の行が返されました。
会社名、製品名、およびバージョン次のうちどれがこの文字列に役立ちますか
管理者を識別するために？
A. オペレーティングシステム
B. 搭載ハードウェア
C. インストールソフトウェア
D. 稼働中のサービス
正解: **(**正解を表示します**)**

質問: **86**
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ます。
経理部。どちらのユーザーも昇格された権限を持っていませんが、グループ内のアカウントは与えられています
デフォルトでは、会社の重要な財務管理アプリケーションにアクセスします。次のどれが
最高の行動方針は？
A. 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する
B. 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
C. 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
D. 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
E. ユーザーアカウントを無効にします
正解: **(**正解を表示します**)**

質問: **87**
最近のセキュリティ侵害に続いて、事件の背後にある推進要因を分析するために死後の調査が行われました
違反サイバーセキュリティ分析では、以下に基づいて潜在的な影響、軽減策、および是正策について説明しました。
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。次のどれがこれです
と見なされる？
A. 脅威情報
B. 高度な持続的脅威
C. 脅威データ
D. 脅威インテリジェンス
正解: **(**正解を表示します**)**

質問: **88**

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。以下のテクニックのどれが
サイバーセキュリティアナリストは、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: **89**
次の項目のうちどれが、いつインシデントが発生したかに関する詳細情報を含む文書を表している。
インシデント対応に加えて、検出されたこと、インシデントがどれほど影響を受けたか、およびどのように修正されたか
有効性と改善が必要なギャップが見つかりましたか？
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: **D (**コメントを発表する**)**
説明/参照：
Explanation:

質問: **90**
技術者は、エンドポイントが疑わしいダイナミックDNSドメインにビーコン送信していることを示すアラートを受信します。
これに対応して、ネットワークを最もよく保護するためには、次の対策のうちどれを使用すべきです。
アラート？　2つ選んでください。）
A. 悪意のあるトラフィックを捉えて追跡するための内部ハニーポットを実装します。
B. エンドポイントが存在するネットワークセグメントでIDSがアクティブになっていることを確認します。
C. 通信を防ぐためにその動的DNSドメイン用のシンクホールを設定します。
D. リスクアセスメントを実施し、代償統制を実施する。
E. 感染したエンドポイントを隔離して、悪意のある活動が広まるのを防ぎます。
正解: **(**正解を表示します**)**

質問: **91**
サイバーセキュリティコンサルタントは、複数の企業で使用されている次のサービスに共通の脆弱性を発見しました。
組織内のサーバー :VPN、SSH、およびHTTPS。次のうちどれが最も可能性の高い理由です
発見された脆弱性
A. 漏洩したPKI秘密鍵
B. OpenSSLの脆弱なバージョン
C. PEAPの脆弱な実装
D. 弱いレベルの暗号化エントロピー
E. 共通の初期化ベクタ
正解: **(**正解を表示します**)**

質問: **92**
管理は、ネットワークの外部からネットワーク内のキーサーバへの管理者アクセスに関係します。
会社。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。どれの
次は効果的な解決策でしょうか？
A. サーバの強化
B. マルウェア対策
C. ジャンプボックス
D. ハニーポット
正解: **(**正解を表示します**)**

質問: **93**
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に4つの脆弱性が見つかりました
アドレス組織への侵害のリスクを軽減するための優先順位付け
最初に修正する必要がありますか？
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: **94**
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Webゲートウェイプロキシがローカルネットワークはローカルマシン上のすべての証明書に署名しました。
次のうちどれが、プロキシが正当にプログラムされている攻撃の種類について説明しています実行しますか？
A. 中間者
B. なりすまし
C. リプレイ
D. 推移的アクセス
正解: **A (**コメントを発表する**)**

質問: **95**
A社は、B社のビジネスパートナーを訪問することで、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。
A社の会議室このアクセスは、パートナーがVPNを確立できるようにするために提供されています。
B社のネットワークに戻る。A社のセキュリティアーキテクトは、
会社Bの従業員は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ます。
同じポートからA社の内部ネットワークにアクセスできます。次のうちどれができる
これを許可するために採用？
A. MAC
B. SAML
C. ACL
D. NAC
E. SIEM
正解: **D (**コメントを発表する**)**

質問: **96**
サイバーセキュリティアナリストは、管理に使用される企業プロセスに従うよう求められています
組織の脆弱性アナリストは、この方針が3年間で更新されていないことに気付いた。
次のうちどれがポリシーがまだ正確であることを確認するためにアナリストがチェックすべきですか？

A. 脅威インテリジェンスレポート
B. 準拠法
C. 会社の議事録
D. 技術的制約
正解: **(**正解を表示します**)**

質問: **97**
汎用目的で見つかった特定された脆弱性の修正における懸念の主な違い
ITネットワークサーバーとSCADAシステムのそれは、次のとおりです。
A. SCADAシステムを再起動して変更を有効にすることはできません。
B. 変更および構成管理プロセスはSCADAシステムに対応していません。
C. SCADAシステムへのパッチのインストールは確認できません。
D. そうすることで、SCADAシステムに運用上の影響を与える可能性が高くなります。
正解: **(**正解を表示します**)**

質問: **98**
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。間に
スキャンすると、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。次のうちどれ
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ますか。
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: **99**
合併の提案が完了する予定の数週間前に、セキュリティアナリストは異常なことに気付いていました
財務情報を含むファイルサーバー上のトラフィックパターン。定期的なスキャンでは検出されません
既知のエクスプロイトまたはマルウェアの署名次のエントリがftpサーバログに表示されます。
tftp -I 10.1.1.1 GET fourquarterreport.xlsを取得します。
次のうちどれが最善の行動方針ですか？
A. ツールを使用して既知の攻撃をスキャンすることで状況の監視を続けます。
B. データ漏洩を防ぐために境界ファイアウォールにACLを実装します。
C. 財務情報を含むサーバーにクレジットカード情報が含まれているかどうかを確認します。

D. 業務上重要なデータの損失に関連するインシデント対応手順に従う。
正解: (正解を表示します)

質問: **100**
最高セキュリティ責任者（CSO）は、ドメイン上のシステムの脆弱性報告を要求しています。
古くなったOSを実行している人。自動スキャンレポートにはOSのバージョンの詳細が表示されないため、
CSOは、脆弱なシステムからリスクエクスポージャーレベルを決定することはできません。次のどれが
サイバーセキュリティアナリストは、脆弱性スキャンプロセスの一部としてOS情報を列挙します。
最も効率的な方法は？
A. Wiresharkを使ってリストをエクスポートする
B. 認証情報設定を使用
C. nmap -pコマンドを実行
D. コマンドを実行する
正解: (正解を表示します)

質問: **101**
新しく発見されたマルウェアは、アウトバウンドを外部の宛先に接続するという既知の動作をしています。
データを抽出するためのポート27500。以下は、netstatを実行して得られた4つの断片です。
- 別のWindowsワークステーションは使用しないでください。

Workstation A:

Proto	Local Address	Foreign Address	State
TCP	10.1.2.3:49321	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49321	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49323	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49324	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49325	EXTERNALIP:27500	ESTABLISHED

Workstation B:

Proto	Local Address	Foreign Address	State
TCP	[::]:135	[::]:0	Listening
TCP	[::]:445	[::]:0	Listening
TCP	[::]:27500	[::]:0	Listening

上記の情報に基づいて、次のうちどれがこのマルウェアにさらされる可能性がありますか？

A. ワークステーションB

B. ワークステーションA

C. ワークステーションC

D. ワークステーションD

正解: **(**正解を表示します**)**

質問: **102**

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に効果的なウォーターホールキャンペーンがあります。これは

ドメインが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、研究者によって "LockMaster"と呼ばれています。

MBRを上書きする機能のためですが、この用語はマルウェアのシグネチャではありません。防御を実行してください

この攻撃経路に関する操作」

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。どっち

アナリストは次の行動をとるべきですか？ 2を選択）

A. 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。

B. 予防措置としてMBRをフォーマットします

C. ドメインにアクセスして脅威の評価を始めます

D. 会社に広めるための脅威情報メッセージを作成する

E. ドメインにブロックを実装するようにファイアウォールエンジニアにアドバイスする

F. 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する

正解: **(**正解を表示します**)**

質問: **103**

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つの
サーバーには 緊急」と評価された2つの異なる脆弱性がありました。
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. インシデント対応計画を有効にする
B. 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
C. 既知の適切な構成から直ちにサーバーを再構築します
D. サーバー上で脆弱性スキャンの定期的なスケジュールを設定する
E. サーバーが改ざんされた可能性があります
F. サーバーが矛盾して構築された可能性があります
正解: **(**正解を表示します**)**

質問: **104**
ペネトレーションテスターは、セキュリティのセキュリティに影響を与える可能性がある重要な
システムの監査の準備をしています。
環境。これには、環境の外周と内周が含まれます。の間に
次のプロセスのうち、このタイプの情報は通常収集されますか。
A. スコープ
B. タイミング
C. 列挙
D. 権限
正解: **A (**コメントを発表する**)**

質問: **105**
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: **106**

何人かの経理部門のユーザーが彼らの閲覧履歴で異常なインターネットトラフィックを報告しています

職場に戻ってログインした後のワークステーション。建物のセキュリティチームはITセキュリティチームに通知します。

会計部門のユーザーがその日のために出発した後、清掃スタッフがシステムの使用に巻き込まれたこと。

ITセキュリティチームは、これが再発するのを防ぐために次のどのステップを踏むべきですか。（2つ選んでください。）

A. 数時間後にインターネットの使用状況を追跡するためのWebモニタアプリケーションをインストールします。

B. 経理グループに対する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. 経理部門のユーザーだけがにアクセスできるように必須アクセス制御を設定します。ワークステーション

D. 不正使用のためにワークステーションを監視するようにカメラを設定します。

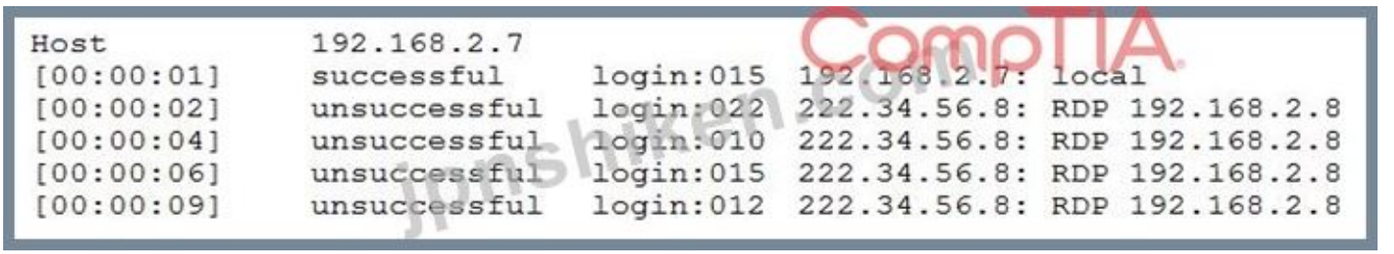
E. ワークステーションアカウントのタイムアウトを3分にするためのポリシーを設定します。

正解: (正解を表示します)

質問: **107**
次のうちどれが、モバイルアプリケーションが情報にアクセスして操作することを可能にするコントロールです。
これは、同じモバイルデバイス上の別のアプリケーション（音楽アプリケーションなど)によってのみ利用可能になります。
ソーシャルメディアサイトのデバイスで再生している現在の曲の名前を投稿しますか？）
A. 二重認証
B. 共同ホストアプリケーション
C. 推移的な信頼
D. 相互排他アクセス
正解: (正解を表示します)

質問: **108**
データベース管理者がセキュリティ管理者に連絡して、ファイアウォールへの接続の変更を要求します。
新しい内部アプリケーション
セキュリティ管理者は、新しいアプリケーションが通常ウイルスによって独占されているポートを使用していることに気付きました。
セキュリティ管理者は要求を拒否し、新しいポートまたはサービスを使用して要求を完了させるよう提案します。
アプリケーションのタスク
次のうちどれがセキュリティ管理者がこの例で実践していますか？
A. 明示的な拒否
B. アクセス制御リスト
C. 暗黙の拒否
D. ポートセキュリティ
正解: (正解を表示します)

質問: **109**
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行動を取るべきであると判断しました。



次のうちどれがシステムのセキュリティ姿勢を改善するために使用されるべきですか？

A. パスワードの複雑さの要件を増やします。

B. 失敗したログイン試行回数を制限します。

C. ファイアウォールをアップグレードします。

D. ログインアカウントの監査を有効にします。

正解: **B** (コメントを発表する)

質問: **110**

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でトラフィックの使用状況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、ワークステーションは最新のOSパッチを実行しています。ヘルプデスクマネージャー

一部のユーザーが自分のワークステーションからログオフしていて、ネットワークアクセスの実行速度が

普通です。アナリストは、ゼロデイ脅威がリモートの攻撃者にアクセスを許可したと考えています。

ワークステーション次のうちどれが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良のステップですか？

2つ選んでください。）

A. パブリックインターネットアクセスを切断してワークステーションのログを確認します。

B. 最新のOSパッチをワークステーションに再適用してください。

C. ネットワーク上のユーザーにパスワードの変更を強制します。

D. プロキシサーバーを介して内部トラフィックをルーティングします。

E. APTが一般的なので、パブリックNAT IPアドレスを変更します。

F. RDPアクセスを無効にするようにグループポリシーを設定します。

正解: (正解を表示します)

質問: **111**

セキュリティ管理者は、最初のインスタンスから数カ月後にローカル特権ユーザーが持っていると判断します。

「foot」として対話的にサーバーに日常的にログインし、インターネットを閲覧している。管理者そのサーバー上のセキュリティログを年1回見直すことでこれを判断します。のどれのために次のセキュリティアーキテクチャの分野で、管理者はレビューと修正を推奨しますか（選択二）。

A. ネットワークの分離と分離
B. 暗号化
C. 利用規定
D. ソフトウェアアシュアランス
E. ログ集計と分析
F. パスワードの複雑さ
正解: **C,E (**コメントを発表する**)**

質問: **112**
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呼び出し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サーバーが稼働しており、リクエストの処理に問題がないことを確認しました。しかしながら、
ある調査では、ファイアウォールが、午前1時頃に始まったWebサーバーを拒否していることを明らかにしました。
朝。アクセスを有効にするために緊急の変更が加えられましたが、管理者はルートを要求しました
原因を特定します。次のうち最良の次のステップはどれですか？
A. Webサーバーの近くにパケットアナライザをインストールして、サンプルトラフィックをキャプチャして異常を見つけます。
B. WebサーバーへのすべてのトラフィックをACLでブロックします。
C. ポートスキャナーを使ってWebサーバー上のすべての待機ポートを調べます。
D. ロギングサーバーでルールの変更を検索します。
正解: **(**正解を表示します**)**

質問: **113**
SIEMからアラートが受信されました。これは、複数のコンピュータへの感染を示しています。脅威に基づいて
特徴として、これらのファイルはホストベースのウイルス対策プログラムによって隔離されました。同時に、
SIEMの追加のアラートは、感染したコンピュータのアドレスからの複数のブロックされたURLを表示します。の
URLは未分類として分類されました。だったURLのIPアドレスのドメインの場所
ブロックされたものはチェックされ、ロシアのISPに登録されます。次のどの手順を実行する必要があります
次？
A. 次のパスサイクルで脆弱性スキャンを実行し、発見した脆弱性にパッチを適用します。ユーザーがいます
コンピュータを再起動してください。SIEMでユースケースを作成し、感染したユーザーのログイン失敗を監視する

コンピュータ
B. ハニーポットとして使用するには、感染したコンピューターと同じ設定のコンピューターをDMZにインストールします。
そのホストとの間で未分類として分類されたURLを許可します。
C. すべてのコンピュータで完全なウイルス対策スキャンを実行し、Splunkを使用して疑わしい活動を探します。
アラートがSIEMで受信される直前に発生しました。
D. ネットワークからそれらのコンピュータを取り外し、ハードドライブを交換してください。感染したハードドライブを送る
調査のために出ます。
正解: **(**正解を表示します**)**

質問: **114**
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、ペイロードを取得したいと考えています。
ハッカーは、業務に影響を与えずにターゲットシステムに送信しています。どっち
アナリストはどのように実装する必要がありますか？
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: **115**
最高情報セキュリティ責任者（CISO）は、セキュリティアナリストに新しいSIEM検索ルールを作成するよう依頼します。
クレジットカード番号がログファイルに書き込まれているかどうかを確認します。CISOとセキュリティアナリストの容疑者
次のログスニペットには、実際の顧客カードデータが含まれています。

```
RecordError - dumping affected entry:
CustomerName: John Doe
Card1RawString: 0413555577814399
Card2RawString: 0444719465780100
CVV: not-stored
CustomerID: 1234-5678
```

次の式のどれが、に一致する形式で潜在的なクレジットカード番号を見つけるでしょうログスニペット？
A. （0-9）×16

B. "04 *"
C. "1234-5678"
D. ^ [0-9] ⑯$
正解: **(**正解を表示します**)**

質問: **116**
セキュリティアナリストがネットワークへの侵入を発見し、未使用のポートを閉じることで問題を迅速に解決します。
次のうちどれを完成させるべきですか？
A. リバースエンジニアリングインシデントレポート
B. 合意のメモ
C. 教訓報告書
D. 脆弱性レポート
正解: **C (**コメントを発表する**)**

質問: **117**
ある医療機関が最近電話で支払いを受け取るようになりました。マネージャーが心配しているさまざまな種類のデータの格納の影響について。次の種類のデータのどれが発生します
最高の規制上の制約
A. PII
B. PCI
C. IP
D. PHI
正解: **(**正解を表示します**)**

質問: **118**
セキュリティアナリストは、PIIが顧客データベースから匿名FTPサーバーにコピーされたことに気付いた
DMZで。ファイアウォールログは、顧客データベースが匿名FTPからアクセスされていないことを示しています
サーバ。次のどの部門がさらに調査を進めることについて決定を下すべきですか？
（2つ選んでください。）
A. 法務
B. IT管理
C. 人事
D. 広報
E. 経営管理
正解: **(**正解を表示します**)**

質問: **119**

脅威インテリジェンスアナリストが検索エンジンの妥協の指標を調査していた間、
Webプロキシが同じインジケータ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次のように述べています。
関連サイトは訪れられなかったが検索エンジンで検索された。次のどれがありそう
このような状況で起こりましたか？
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**: 120**
ある企業が、承認されたスキャンベンダーから外部の脆弱性スキャンの結果を受け取りました。当社は、承認後72時間以内に、これらの脆弱性をクライアントに修正することを求められています。
スキャン結果
以下の契約違反のうちどれがこの是正が内のクライアントに提供されないならば起こります
時間枠？
A. 覚書
B. サービスレベル契約
C. 組織統治
D. 規制遵守
正解**: (**正解を表示します**)**

質問**: 121**
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通信しています
暗号化されたトンネルを介した既知の悪質なサイト。更新されたウイルス対策シグネチャを使用した完全ウイルス対策スキャン
ファイルは感染の兆候を示していません。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**: (**正解を表示します**)**
説明/参照：
Explanation:

質問: **122**
ある大学は、次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。
集中管理と学生/従業員の両方のラップトップ。ソリューションは拡張可能であるべきである
誤検知を最小限に抑え、結果の精度を高め、企業全体で一元管理する
コンソール。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: **123**
次のログスニペットがあるとします。

```
Mar 20 10:08:47 superman sshd[1876]: fatal: Unable to negotiate with
no matching host key type found. Their offer: ssh-dss [preauth]

Mar 20 10:08:47 superman sshd[1888]: Connection closed by 192.168.1.1

Mar 20 10:08:47 superman sshd[1895]: Connection closed by 192.168.1.1

Mar 20 10:08:48 superman sshd[1888]: Connection closed by 192.168.1.1

Mar 20 10:08:48 superman sshd[1902]: fatal: Unable to negotiate with
no matching host key type found. Their offer: ecdsa-sha2-nistp384 [pr
```

次のうちどれが発生したイベントについて説明しますか？
A. パスワードを使って、未知のIPアドレスからSSH接続しようとしました。
B. 192.168.1.166からSSH接続しようとしましたが、PKIを使用していました。
C. ネットワークの外部からSSH接続を試みましたが、PKIを使用して行われました。
D. "スーパーマン"からSSH接続を試みましたが、パスワードを使用して行いました。

正解: (正解を表示します)

質問: **124**
ある組織が最近データ侵害を経験しました。フォレンジック分析により、攻撃者が見つけたことが確認されました
1年以上使用されておらず、定期的にパッチが適用されていなかった従来のWebサーバー。の後セキュリティチームとの議論、経営陣はネットワーク偵察のプログラムを開始することを決めたそして侵入テスト。彼らは活動的なホストを探してネットワークをスキャンしてプロセスを開始したいと考えています。
ポート次のツールのうちどれがこの仕事に最適ですか？
A. Nmap
B. Netstat
C. L0phtCrack
D. ping
E. Wireshark
F. ifconfig
正解: (正解を表示します)

質問: **125**
最近のセキュリティ侵害の後、開発者が書かれたコードを宣伝したことが発見されました
の問題を引き起こしていたユーザーナビゲーションの問題を解決するための修正プログラムとして運用環境にインストールする
複数の顧客このコードは、誤ってすべてのユーザーに管理者権限を付与していました。
機密データおよびレポートへの不適切なアクセス次のうちどれがこのコードを妨げた可能性があります
実稼働環境にリリースされることから？
A. 後任計画
B. 自動報告
C. クロストレーニング
D. 職務分離
正解: (正解を表示します)

質問: **126**
原子力施設管理者は、施設内の水の利用を監視する必要があると判断した。スタートアップビジネス統合の必要性に取り組むための最先端のソリューションを発表したばかりです。
ICSネットワークこのソリューションでは、非常に小さなエージェントをICS機器にインストールする必要があります。どっち
以下は、施設を保護するために投資家が投資するための最も重要なセキュリティ管理策です。
A. インストールされているエージェントに対して侵入テストを実行します。
B. 管理者とユーザーにスルーガイドを要求します。

C. テストシステムにエージェントを1週間インストールしてアクティビティを監視します。
D. ソリューションプロバイダがエージェントのソースコードを分析可能にすることを要求します。
正解: (正解を表示します)

質問: **127**
あるセキュリティアナリストが、企業の店頭Webサイトが Webサイトではないことを報告するサービスチケットをいくつか受け取りました
内部ドメインユーザーがアクセスできます。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。
次のうちどれがこの動作の最も可能性の高い理由ですか？
A. 証明書は期限切れです。
B. FQDNが正しくありません。
C. DNSサーバーが壊れています。
D. 時刻同期サーバーが壊れています。
正解: (正解を表示します)

質問: **128**
SDLCの一環として、ソフトウェア開発者は次のように入力して新しい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。
大量のランダムデータ。次の種類のテストはどれですか。
A. あいまい
B. 入力検証
C. ストレステスト
D. 回帰テスト
正解: (正解を表示します)

質問: **129**
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。レポートには以下の情報

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: **130**
サイバーセキュリティアナリストは、ドメインコントローラ内に実装されているセキュリティ対策を確認するために雇われています
会社の。見直すと、サイバーセキュリティアナリストは、ブルートフォース攻撃が仕掛けられることに気付いた
Windowsプラットフォーム上で動作するドメインコントローラ。によって実装された最初の修復ステップ
サイバーセキュリティアナリストは、アカウントのパスワードをより複雑にすることです。次のどれがNEXTです
サイバーセキュリティアナリストが実装する必要がある修復ステップ
A. 管理者アカウントを新しいセキュリティグループに移動します。
B. より頻繁にポートスキャンを実行します。
C. 別のウイルス対策ソフトウェアをインストールしてください。
D. 脆弱性検索ツールを配置します。
E. LAN Managerのハッシュを保存する機能を無効にします。
正解: **A** (コメントを発表する)

質問: **131**
Webアプリケーションの脆弱性スキャン中に、アプリケーションが表示されることが発見されました
SQLデータベースに接続されたWebフォームに特定のキーフレーズが入力された後の不適切なデータ
サーバ。このタイプの攻撃が戻る可能性を減らすために、次のうちどれを使用するべきか
機密データ？
A. 入力検証
B. アプリケーションファジング
C. 静的コード分析
D. ピアレビューコード
正解: (正解を表示します)

質問: **132**
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が
複数の技術者による法医学的分析が必要です。フォレンジックツールキット内の以下の項目のうちどれ
おそらく最初に使用されるでしょうか？ 2を選択）
A. ドライブアダプタ

B. 犯罪テープ
C. CoCの形
D. ドライブイメージャー
E. ハッシュユーティリティ
F. 書き込みブロッカー
正解: **C,F** (コメントを発表する)

質問: **133**
次のうちどれがタイムラインと時刻の慎重な選択の背後にある推論を表している
許可された侵入テストの境界 2を選択）
A. 意図しない業務への影響を軽減するため
B. 起こり得る本当の侵入との衝突を避けるため
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
D. テスト活動に必要な人的資源を計画するため
E. 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
正解: (正解を表示します)

質問: **134**
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。
「この技術の組織に対して行われた知的財産窃盗キャンペーンが行われました。
業界。このアクティビティの指標は侵入ごとに異なります。あるように思われる情報
研究開発データがターゲットです。データの漏出は、一様なTTPによって数ヶ月にわたって発生するようです。お願いします
この攻撃経路に関して防御操作を実行してください。」
次の組み合わせのどれが、どのように脅威が分類される可能性が最も高いか、またその種類は
この活動から保護するために最も役立つと思われる分析について
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: **135**
ある保険会社が、企業が発行したモバイルデバイスを携帯する迅速な対応のチームドライバーを採用しています
保険会社のアプリがインストールされています。デバイスはMDMによって構成が強化されています。

最新の状態に保った。従業員は保険金請求情報を収集し、支払いを処理するためにアプリを使用します。
最近、多くの顧客が保険会社に対してクレジットカード詐欺の苦情を申し立てました。
彼らの支払いがモバイルアプリを介して処理された直後に発生しました。サイバーインシデント対応チームに調査を依頼しました。最も可能性が高い原因は次のうちどれですか？
A. USBテザリングが有効になります。
B. MDMサーバの設定が誤っています。
C. アプリはTLSを採用していません。
D. 3G以降の安全性が低いセルラーテクノロジは制限されていません。
正解: **(**正解を表示します**)**

質問: **136**
セキュリティイベントを整理し、それらの応答と解決を管理するための集中管理ツールは、次のとおりです。
A. SIEM
B. Wireshark
C. syslog
D. ヒップス
正解: **A (**コメントを発表する**)**

質問: **137**
以下のコマンドのうち、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
つかいます？
A. wget
B. rm
C. dd
D. 触れる
正解: **(**正解を表示します**)**

質問: **138**
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。初期の脆弱性

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。修復を開始する前に、
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. '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。
B. 「低」と表示されている項目は情報提供のみを目的としています。
C. 報告によると、調査結果は情報提供を目的としています。
D. スキャン結果のバージョンが自動資産インベントリと異なります。
正解: **B** (コメントを発表する)

質問: **139**
セキュリティアナリストは、アウトバウンドSFTPプロセスが次の時間帯に発生していることを発見しました。
過去数日。これが発見された時点では、大量のビジネスクリティカルデータが
配信しました。このプロセスの認証は、適切な資格情報を持つサービスアカウントを使用して行われました。
セキュリティアナリストはこの転送の宛先IPを調査し、この新しいプロセスが
変更管理ログに記録されていません。次のどれがベストコースになるでしょう
アナリストが取るべき行動は？
A. 起こりうる事件を調査する。
B. ユーザー権限を確認してください。
C. 脆弱性スキャンを実行します。
D. クラウドプロバイダとSLAを確認します。
正解: (正解を表示します)

質問: **140**
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
攻撃者は不正な外国からの認証に成功したことを明らかにしました。管理
に基づいて攻撃を軽減するためのソリューションを調査し、実装するようにセキュリティアナリストに依頼しました。
危険にさらされたパスワード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: (正解を表示します)
説明/参照：
Explanation:

質問: **141**
サーバーには、機密性の高いワークステーションに定期的に展開されるベースラインイメージが含まれています。の
画像はパッチ適用やその他の修正のために月に一度評価されますが、それ以外は変更されません。どれの
ファイルサーバーを保護し、イメージが保護されていないことを確認するために、次のコントロールを実行する必要があります。
かわった？
A. に接続する必要がある管理者またはユーザーには、2要素認証を使用する必要があります。
サーバ。
B. ベースラインイメージが危険にさらされる前に、攻撃を識別するためのハニーポットをインストールします。
C. ファイルの整合性監視ツールをサーバーにインストールして構成し、それぞれのイメージを更新できるようにします。
月。
D. イメージが更新される前に、少なくとも月に1回サーバーの脆弱性スキャンをスケジュールしてください。
正解: **C (**コメントを発表する**)**

質問: **142**
あるアナリストが、企業の金融アプリケーションサーバーに関する最近の脆弱性の報告をレビューしています。どれの
アナリストは、会社の環境にとって最も重要であると次のように考えますか。
A. 古い暗号化アルゴリズムの使用
B. リモートコード実行
C. SQLインジェクション
D. バナー掴み
E. XSSに対する感受性
正解: **(**正解を表示します**)**

質問: **143**
最近の監査では、60日前にリリースされた重要なパッチがそうではないことが判明した脆弱性スキャンが含まれていました
環境内のサーバーに適用されます。インフラストラクチャチームは問題を特定し、決定しました。
自動パッチ管理アプリケーションを実行しているサーバーでサービスが無効になっていたためです。
次のうちどれが将来同様の監査結果を避けるための最も効率的な方法でしょうか？
A. 起動時に自動的に実行されるようにパッチ管理サーバーのサービスを設定します。
B. 手動によるパッチ管理アプリケーションパッケージを実装して、
プロセス。

C. パッチの適用後30日以内にすべてのサーバーに修正プログラムを適用することを要求する修正プログラム管理ポリシーを作成します。
リリース。
D. サービス監視を実装して、ツールが正しく機能していることを確認します。
正解: (正解を表示します)

質問: **144**
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」メッセージが継続的に送信されているという警告を受けました。
ネットワーク境界でネットワークセンサーによって観察された。プロキシファイアウォールは正常に
メッセージアラートが真のポジティブであると判断した後、次のどれがMOSTを表します
可能性がありますか？
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: **145**
セキュリティアナリストが、ネットワーキング部門からの増加を説明するレポートをレビューしています。
一部のシステムでネットワークパフォーマンスの問題が発生しています。トップトーカーレポート
5分以上のサンプルが含まれています。

Source	Destination	Application	Packets	Volume(Kbps)
8.4.4.100	172.16.1.25	SMTP	4386	6141
96.23.114.14	172.16.1.1	IPSec	7734	10827
172.16.1.101	100.15.25.34	HTTP	3412	4776
96.23.114.18	172.16.1.1	IPSec	2723	3812
172.16.1.101	100.15.25.34	SSL	8697	12176
172.16.1.222	203.67.121.12	Quicktime	1302	1822
172.16.1.197	113.121.12.15	8180/tcp	6045	8463
172.16.1.131	172.16.1.67	DHCP	25	35
172.16.1.25	172.16.1.53	DNS	66	93

上記のサンプルの出力を考えると、セキュリティアナリストは次のうちどれを最初に達成する必要があります。
パフォーマンスの問題を追跡するのに役立ちますか？
A. 表示されている各IPアドレスで逆引きを実行して、トラフィックが必要かどうかを判断します。
B. ランダムまたはデフォルト以外のアプリケーションポート宛てのトラフィックを制限するためにACLを配置します。

C. ネットワーク上のトップトーカーを隔離し、それによって引き起こされた潜在的な脅威の調査を開始します。
過剰なトラフィック
D. ネットワークの一部を整理するために、Quicktimeなどの不要なプロトコルをネットワークでブロックすることをお勧めします。
渋滞
正解: (正解を表示します)

質問: **146**
あるスタッフは、ノートパソコンのパフォーマンスが低下していると報告しました。セキュリティアナリストが調査しました
問題を発見し、CPU使用率、メモリ使用率、およびアウトバウンドネットワークトラフィックがラップトップのリソースを消費します。次のうちどれを解決するための最良の行動方針です。
問題？
A. ノートパソコンのOSに正しくパッチが適用されていることを確認してください。
B. ウィルススキャンを一時停止します。
C. ノートパソコンのメモリを増やします。
D. 悪意のあるプロセスを特定して削除します。
E. スケジュールされたタスクを無効にします。
正解: (正解を表示します)

質問: **147**
新しい最高技術責任者（CTO）は、ネットワーク監視サービスの推奨事項を求めています。
ローカルイントラネットCTOは、ゲートウェイとの間で送受信されるすべてのトラフィックも監視できることを望んでいます。
特定のコンテンツをブロックする機能として。次の推奨事項のどれがニーズを満たすでしょうか組織の？
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. 内部インタフェースにIDSを、外部インタフェー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。
ゲートウェイルータ
C. 内部インタフェースにファイアウォールを、外部インタフェースにNIDSをインストールすることをお勧めします。
ゲートウェイルータ
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: **148**
最近発行された監査報告書は、機密データのエンドユーザー処理に関する例外を強調しています。
資格情報にアクセスします。セキュリティマネージャが調査結果に対処しています。次の活動のどれをすべきですか
実装される？
A. グループポリシーオブジェクトを展開する
B. シングルサインオンプラットフォームを展開する
C. パスワードポリシーを更新します
D. トレーニング要件を増やす
正解: (正解を表示します)

質問: **149**
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. インターネットから実行された脆弱性スキャン
B. Javascriptの脆弱性
C. jQueryの脆弱性
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: (正解を表示します)

質問: **150**
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。どっち次は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: **151**
セキュリティアナリストが組織のソフトウェア開発ライフサイクルのレビューを行いました。アナリスト
チームメンバーが評価して重要な情報を提供する段階にライフサイクルが含まれていないことを報告します。
他の開発者のコードに関するフィードバック。次の評価方法のどれが最適ですか
アナリストのレポートを説明しますか？
A. 滝
B. ピアレビュー
C. 建築評価
D. ホワイトボックステスト
正解: (正解を表示します)

質問: **152**
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脆弱性であると判断しました
SQLインジェクション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。どっち
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。
C. 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。
D. 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。
正解: (正解を表示します)

質問: **153**
以下の対策のうちどれがセキュリティ管理者がMOSTに効果的に適用すべきか
Bootkitレベルの組織のワークステーションデバイスへの感染を軽減しますか？

A. 各デバイスの再起動後にシステム状態の回復を強制します。
B. デバイスのBIOSレベルのパスワードを設定します。
C. ローカル管理者権限を削除します。
D. 二次ウイルス対策アプリケーションをインストールします。
正解: **(**正解を表示します**)**

質問: **154**
調査中に、コンピュータが押収されています。次のうちどれがアナリストの最初のステップです。
取るべきだ？
A. コンピュータの電源を切り、ネットワークから取り外します。
B. CoC文書の作成を開始します。
C. 物理ハードディスクイメージを実行します。
D. ネットワークケーブルを抜き、デスクトップのスクリーンショットを撮ります。
正解: **(**正解を表示します**)**

質問: **155**
プロジェクトリーダーは、次のプロジェクトの作業明細書を確認しています。
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における潜在的な弱点。の一部として
プロジェクト、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採用しようとします。
の
作業明細書では、特にネットワークリソースを調査するための自動ツールの利用について取り上げています。
インフラストラクチャーの弱点を示す論理図を作成する試み。
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. 脆弱性スキャン
B. ソーシャルエンジニアリング
C. フレンドリーDoS
D. 侵入テスト
E. セッションハイジャック
正解: **D (**コメントを発表する**)**

質問: **156**
本社のWebサイトをOWASP ZAPツールでスキャンした後、サイバーセキュリティアナリストがレビューを行っています。
次の警告

```
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: **157**
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、規制または事業に基づいて情報の種類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
ニーズ。
B. このポリシーは、ユーザーがインターネット上のデータにアクセスするために従う必要がある慣行を文書化する必要があります。
企業ネットワークまたはインターネット
C. このポリシーは、承認されたユーザーがアクセスするための組織のアカウント管理の概要を説明するものです。
適切なデータ
D. ポリシーは、ユーザーと管理者間の役割と責任を記述するべきです。
特定のデータタイプの管理
正解: **C (**コメントを発表する**)**