CompTIA.SY0-601-JPN.v2022-10-22.q121

試験コード：	SY0-601-JPN
試験名称：	CompTIA Security+ Certification Exam (SY0-601日本語版)
認証ベンダー：	CompTIA
無料問題の数：	121
バージョン：	v2022-10-22
ページの閲覧量：	523
問題集の閲覧量：	9982

https://www.jpnshiken.com/shiken/CompTIA.SY0-601-JPN.v2022-10-22.q121.html

質問: **1**
組織は、ホストされている Web サーバーが最新バージョンのソフトウェアを実行していないことを懸念しています。潜在的な脆弱性を特定するのに最も役立つのは次のうちどれですか?
A. Hping3 -s comptia, org -p 80
B. Nc -1 -v comptia, org -p 80
C. nmp comptia, org -p 80 -aV
D. nslookup -port=80 comtia.org
正解: **(**正解を表示します**)**
Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

質問: **2**
ランサムウェア攻撃により、Web サーバーが侵害されました。さらに調査を進めると、ランサムウェアが過去 72 時間にわたってサーバーに存在していたことが明らかになりました。システム管理者は、サービスをできるだけ早く元に戻す必要があります。管理者がサービスを安全な状態に復元するために使用する必要があるのは、次のうちどれですか?
A. 72 時間前に実行された最後の増分バックアップ 最も投票された
B. 最も投票された最後の既知の良好な構成
C. 7 日前に実行された最後の完全バックアップ
D. ベースライン OS 構成
正解: **(**正解を表示します**)**
Ransomware will most likely render the web server unusable and must be isolated for forensic investigation. This will leave the only option to start a new web server from scratch and restore the last full backup, plus any differential or incremental backups which are sure to be clean from ransomware (if available).

質問: **3**
DBAは、週末にいくつかの実稼働サーバーのハードドライブがワイプされたと報告しています。DBAは、システムファイルが予期せず削除されたために、いくつかのLinuxサーバーが使用できなくなったことも報告しています。セキュリティアナリストは、ソフトウェアがこれらのサーバーから意図的にデータを削除するように構成されていることを確認しました。サーバーへのバックドアは見つかりませんでした。次の攻撃のうち、データトスを引き起こすために最も使用された可能性が高いのはどれですか？
A. リモートアクセス型トロイの木馬

B. ルートキット
C. ランサムウェア
D. ファイルレスウイルス
E. 論理爆弾
正解: **(**正解を表示します**)**

質問: **4**
会社は、Webアクセスを制限し、従業員がアクセスするWebサイトを監視する機能を望んでいます。次のうち、これらの要件を最もよく満たすのはどれですか？
A. WAF
B. VPN
C. ファイアウォール
D. インターネットプロキシ
正解: **(**正解を表示します**)**

質問: **5**
システム管理者は、オブジェクトのアクセス ポリシーをその所有者が決定できるようにするアクセス制御スキームを実装する必要があります。次のアクセス制御スキームのうち、要件に最も適しているのはどれですか?
A. ロールベースのアクセス制御
B. 任意アクセス制御
C. 強制アクセス制御
D. 属性ベースのアクセス制御
正解: **(**正解を表示します**)**
Discretionary access control (DAC) is a model of access control based on access being determined "by the owner" of the resource in question. The owner of the resource can decide who does and does not have access, and exactly what access they are allowed to have.

質問: **6**
ある企業は、利用可能なストレージが限られており、オンライン プレゼンスが 4 時間を超えることはできません。障害が発生した場合に最速のデータベース復元時間を可能にするために会社が実装する必要があるバックアップ方法論は、次のうちどれですか?
A. 毎週日曜日の午後 8:00 に完全バックアップを実施し、夜間の差分バックアップを午後 8:00 に実施します。
B. 毎週日曜日の午後 8:00 に、夜間のフル バックアップを実装します。
C. 毎週日曜日の 8:00 に異なるバックアップを実装し、午後 8:00 に夜間の増分バックアップを実装します。
D. 毎週日曜日の午後 8:00 に完全なテープ バックアップを実装し、毎晩テープ ローテーションを実行します。
正解: **(**正解を表示します**)**

質問: **7**
ユーザーが秘密鍵を使用して電子メールに署名するときに保証されるのは、次のうちどれですか？
A. 利用可能
B. 認証
C. 守秘義務

D. 否認防止
正解: **(**正解を表示します**)**

質問: **8**
スタートアップ企業は、複数の SaaS および IaaS プラットフォームを使用して、企業インフラストラクチャを立ち上げ、顧客向けの Web アプリケーションを構築しています。セキュリティ、管理性、およびプラットフォームへの可視性を提供するのに最適なソリューションは次のうちどれですか?
A. シェム
B. DLP
C. CASB
D. SWG
正解: **(**正解を表示します**)**
A cloud access security broker is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies A CASB has a separate, and more distinctive role. Differing from the use case for SWG, which focuses on the broader filtering and protection against inbound threats and filtering illegitimate web traffic, a CASB is more deeply integrated and has control over your cloud application usage. It can be tied into an applications API to scan data at rest or can be used with a proxy based deployment to enforce inline policies for more real time protection.

質問: **9**
最近のセキュリティ評価中に、一般的な OS に脆弱性が発見されました。OS ベンダーはこの問題を認識しておらず、次の四半期内にパッチをリリースすると約束しました。
A. レガシー オペレーティング システム
B. サプライチェーン
C. 構成が弱い
D. ゼロデイ
正解: **D (**コメントを発表する**)**

質問: **10**
ユーザーは、Webポータルのログイン画面でユーザー名とパスワードを入力します。数秒後、次のメッセージが画面に表示されます。パスワードフィールドには、数字、特殊文字、文字の組み合わせを使用してください。このメッセージが説明している概念は次のうちどれですか？
A. パスワード履歴
B. パスワードの使用期間
C. パスワードの再利用
D. パスワードの複雑さ
正解: **D (**コメントを発表する**)**

質問: **11**
次のコンポーネントのうち、単一のファイアウォールを介してインバウンドインターネットトラフィックを統合して複数のクラウド環境に転送するために使用できるのはどれですか？
A. エッジコンピューティング
B. クラウドホットサイト

C. DNSシンクホール
D. トランジットゲートウェイ
正解: **(**正解を表示します**)**

質問: **12**
ユーザーはパスワードを入力してワークステーションにログインすると、認証コードの入力を求められます。次の MFA 要素または属性のうち、認証プロセスで使用されているものはどれですか? (2 つ選択)。
A. 知っていること
B. できること
C. 持っているもの
D. あなたの何か
E. どこかで
F. あなたは誰か
正解: **A,C (**コメントを発表する**)**

質問: **13**
ある会社は、すべてのラップトップにワイヤレスを使用し、その資産の非常に詳細な記録と、ワイヤレス ネットワーク上での使用が許可されているデバイスの包括的なリストを保持しています。最高情報責任者 (CIO) は、無許可のデバイスを使用してワイヤレス PSK をブルート フォースし、内部ネットワークへのアクセスを取得する可能性のあるスクリプト キディーを懸念しています。これを防ぐために会社が実施すべきことは次のうちどれですか?
A. BPDU ガード
B. WPA-EAP
C. IP フィルタリング
D. A WIDS
正解: **B (**コメントを発表する**)**
"EAP is in wide use. For example, in IEEE 802.11 (WiFi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism." https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol The Wi-Fi Alliance added EAP-FAST (along with EAP-TLS and EAP-TTLS) to its list of supported protocols for WPA/WPA2 in 2010. Source: https://jaimelightfoot.com/blog/comptia-security-wireless-security/ "EAP has been expanded into multiple versions." * "The Wi-Fi Alliance added PEAP to its list of supported protocols for WPA/WPA2/WPA3." * "The Wi-Fi Alliance added EAP-FAST to its list of supported protocols for WPA/WPA2/WPA3." * "The Wi-Fi Alliance added EAP-TTLS to its list of supported protocols for WPA/WPA2/WPA3." Excerpt From: Wm. Arthur Conklin. "CompTIA Security+ All-in-One Exam Guide (Exam SY0-601))."

質問: **14**
次のうち、制限されたエリアにアクセスするためのインタラクティブなプロセスの活用について説明しているのはどれですか？
A. 永続性
B. バッファオーバーフロー
C. 特権の昇格
D. ファーミング
正解: **(**正解を表示します**)**

https://en.wikipedia.org/wiki/Privilege_escalation#:~:text=Privilege%20escalation%20is%20the%20act,from%20an%20application%20or%20user

質問: **15**
セキュリティ アナリストは、進行中のビジネス オペレーションに影響が及ぶ前に発生する可能性のあるデータ損失の最大量を特定する任務を負っています。次の用語のうち、この指標を最もよく定義しているのはどれですか?
A. MTTR
B. RPO
C. MTBF
D. RTO
正解: **(**正解を表示します**)**

質問: **16**
公開Webサイトの資格情報データベースがインターネット上で漏洩した数日後に複数のビジネスアカウントが侵害されました。侵害でビジネスメールは特定されませんでしたが、セキュリティチームは、公開されたパスワードのリストが後でビジネスアカウントを侵害するために使用されたと考えています。次の問題は軽減されますか？
A. パスワード履歴
B. 複雑さの要件
C. 利用規定
D. 共有アカウント
正解: **C (**コメントを発表する**)**

質問: **17**
最高セキュリティ責任者は、システムが予期せずオフラインになったときに、顧客がバックエンド インフラストラクチャからエラーを受信する発生を減らすことができるソリューションを探しています。セキュリティ アーキテクトは、ソリューションがセッションの持続性を維持するのに役立つことを望んでいます。次のうち、要件を最もよく満たすのはどれですか?
A. NIC チーミング
B. リバース プロキシ
C. フォワード プロキシ
D. ロードバランサー
正解: **A (**コメントを発表する**)**

質問: **18**

ある組織が停止し、重要なシステムがオンラインに戻るまでに 90 分かかりました。停止中にデータが失われることはありませんでしたが、重要なシステムが 60 分以内に再び使用可能になることが期待されていました。
A. MTBF
B. RPO
C. MTTR
D. RTO
正解: **(**正解を表示します**)**
https://www.enterprisestorageforum.com/management/rpo-and-rto-understanding-the-differences/

質問: **19**
セキュリティ アナリストがマルウェアを特定し、企業ネットワークを介して拡散していることを確認し、CSIRT を起動しました。アナリストが次に行うべきことは次のうちどれですか? あ
A. 感染したすべてのホストを隔離して、さらなる拡散を制限しようとする
B. 感染したシステムのイメージを再作成するためのヘルプ デスク チケットを作成する
C. すべてのエンドポイント ウイルス対策ソリューションを最新の更新プログラムで更新します。
D. マルウェアがネットワークにどのように導入されたかを確認します。
正解: **(**正解を表示します**)**

質問: **20**
攻撃者は、オンライン システムからいくつかのソルト化されていないパスワード ハッシュを盗み出すことに成功しました。以下のログを考えると：

```
Session          : hashcat
Status           : cracked
Hash.Type        : MD5
Hash.Target      : b3b81d1b7a41[illegible]ab3a507d0a586a0
Time.Started     : Fri Mar 10 10:18:45 2020
Recovered        : 1/1 (100%) Digests
Progress         : 28756845 / 450365879 (6.38%) hashes
Time.Stopped     : Fri Mar 10 10:20:12 2020
Password found   : Th3B3stP@55w0rd!
```

次のうち、攻撃者が実行しているパスワード攻撃のタイプを最もよく表しているのはどれですか?
A. ブルートフォース
B. パスザハッシュ
C. パスワード スプレー
D. 辞書
正解: **D (**コメントを発表する**)**

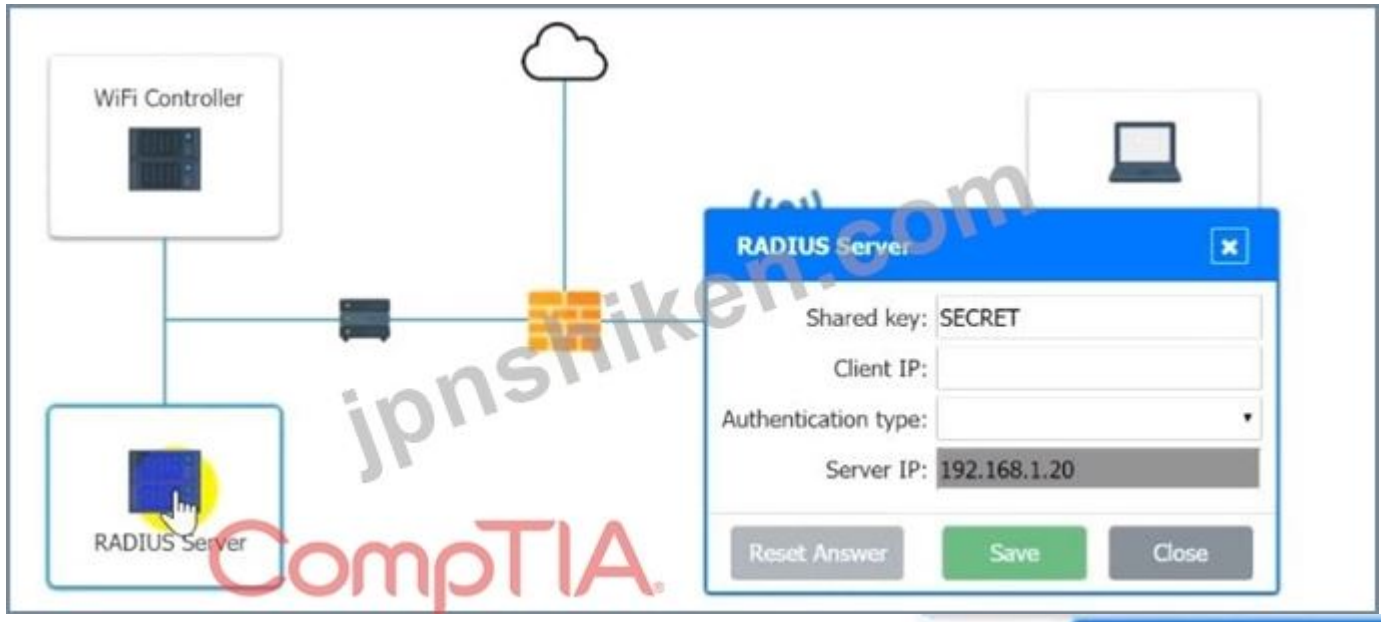
質問: **21**
銀行の最高コンプライアンス責任者は、すべての新入社員の身元調査ポリシーを承認しました。次のうち、最も保護する可能性が高いポリシーはどれですか。
A. 履歴書に虚偽の情報を追加して、より適格であるように見えるようにした応募者

B. 業界のコンプライアンスを遵守するために盗難で有罪判決を受けた従業員を雇用する
C. 縁故主義を防ぐために、現在の従業員の兄弟が銀行で働くのを防ぐ
D. 顧客情報を盗もうとしている可能性のある他の銀行で新入社員が働いていないことを確認する
正解: **(**正解を表示します**)**

質問: **22**
SOC オペレーターは、機能しているユーザー ID への SSH 試行が短期間のうちに各 Linux システムで失敗したことを示す複数の Linux システムから継続的にアラートを受信しています。次のうち、この動作を最もよく説明しているのはどれですか?
A. レインボーテーブルアタック
B. パスワード スプレー
C. ロジックボム
D. マルウェアボット
正解: **(**正解を表示します**)**
Password Spraying is a variant of what is known as a brute force attack. In a traditional brute force attack, the perpetrator attempts to gain unauthorized access to a single account by guessing the password "repeatedly" in a very short period of time.

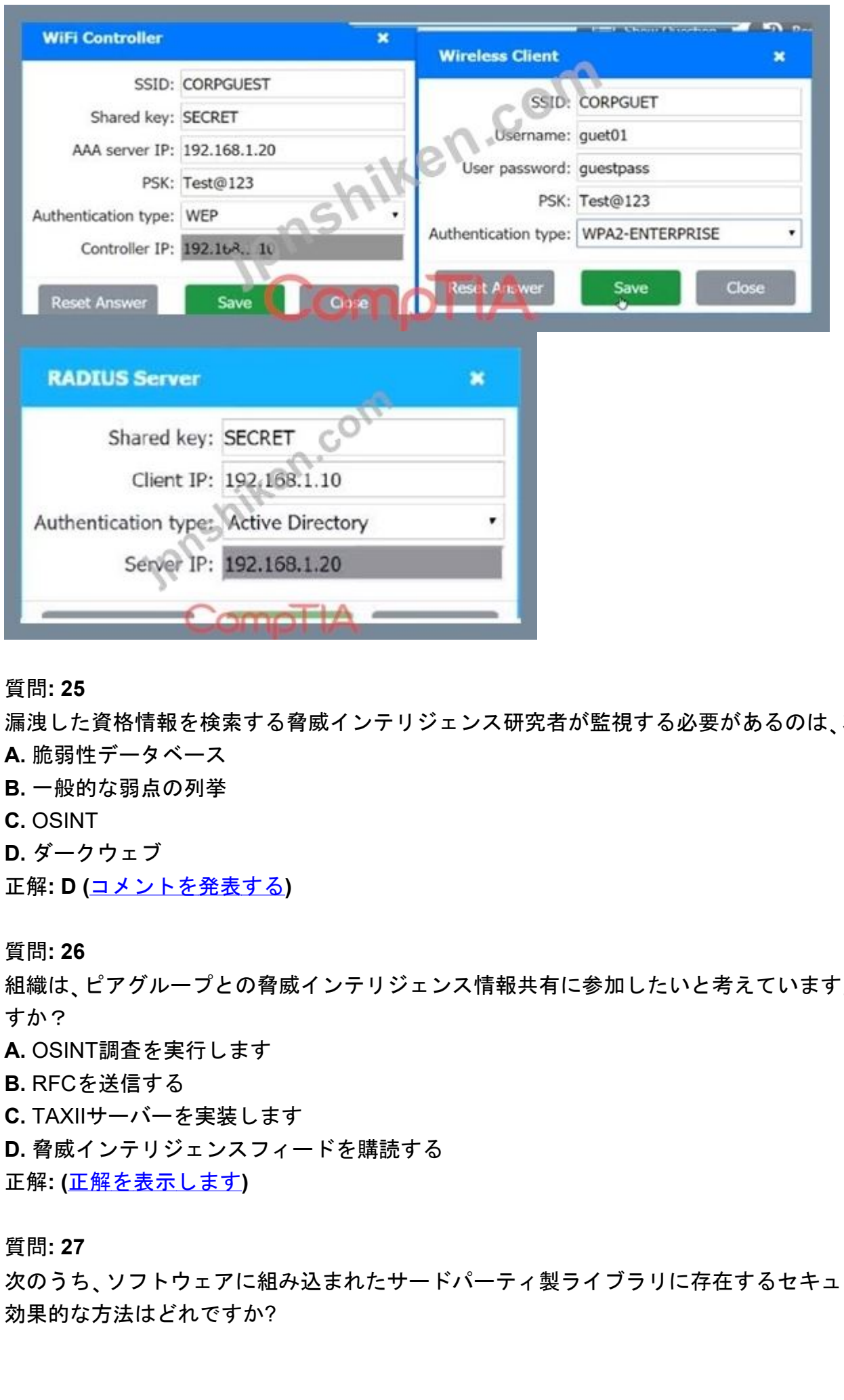
質問: **23**
セキュリティコンプライアンス評価の一環として、監査人は自動化された脆弱性スキャンを実行します。さらに、監査人は評価を完了するために次のうちどれを行う必要がありますか？
A. ログ分析
B. 構成レビュー
C. パケットキャプチャ
D. ユーザー行動分析
正解: **(**正解を表示します**)**

質問: **24**
システム管理者は、認証されたゲストアクセス用に新しいワイヤレスネットワークをインストールする必要があります。ワイヤレスネットワークは、利用可能な最も安全な暗号化とプロトコルを使用して802.IXをサポートする必要があります。
次の手順を実行します。
1.RADIUSサーバーを構成します。
2.WiFiコントローラーを構成します。
3.着信ゲスト用にクライアントを事前設定します。ゲストADの資格情報は次のとおりです。
ユーザー :guest01
パスワード :guestpass



正解:

Use the same settings as describe in below images.



質問: **25**
漏洩した資格情報を検索する脅威インテリジェンス研究者が監視する必要があるのは、次のうちどれですか？
A. 脆弱性データベース
B. 一般的な弱点の列挙
C. OSINT
D. ダークウェブ
正解: **D** (コメントを発表する)

質問: **26**
組織は、ピアグループとの脅威インテリジェンス情報共有に参加したいと考えています。次のうち、組織の要件を最も満たす可能性が高いのはどれですか？
A. OSINT調査を実行します
B. RFCを送信する
C. TAXIIサーバーを実装します
D. 脅威インテリジェンスフィードを購読する
正解: (正解を表示します)

質問: **27**
次のうち、ソフトウェアに組み込まれたサードパーティ製ライブラリに存在するセキュリティ上の欠陥を、本番環境にリリースする前に検出する最も効果的な方法はどれですか?

A. ソフトウェアリリース前の侵入テストの回数を増やします。
B. 脆弱性スキャンを実装して、SDLC の依存関係を早期に評価します。
C. サーバー側とクライアント側の検証に異なる手法を採用します。
D. サードパーティ ライブラリには別のバージョン管理システムを使用します。
正解: **(**正解を表示します**)**

質問: **28**
インシデント対応プロセスの次のうち、特定フェーズの速度を改善するための最良のアプローチはどれですか?
A. 誤検知率を減らすために監視を調整します。
B. すべてのイベントを複数の syslog サーバーにリダイレクトします。
C. 環境に存在するセンサーの数を増やします。
D. すべての重要なアセットで詳細ログを有効にします。
正解: **D (**コメントを発表する**)**

質問: **29**
次の組織のうち、システムの最適なセキュリティ構成のためのフレームワークと制御を設定しているのはどれですか？
A. NIST
B. PCI DSS
C. GDPR
D. ISO
正解: **A (**コメントを発表する**)**

質問: **30**
ペネトレーションテスターは内部サーバーを危険にさらすことができ、現在のセッションをネットワークの横方向の動きでピボットしようとしています。サーバーで利用できる場合、次の評価ステップに最も役立つ情報を提供するツールは次のうちどれですか。
A. Memdump
B. Nmap
C. 剖検
D. カッコウ
正解: **C (**コメントを発表する**)**

質問: **31**
従業員は、電子メールの添付ファイルとして配信されたワードプロセッシングファイルを受け取りました。件名と電子メールの内容により、従業員は添付ファイルを開くようになりました。次の攻撃ベクトルのうち、このマルウェアに最もよく一致するものはどれですか？
A. 埋め込まれたPythonコード
B. Bashスクリプト
C. マクロ対応ファイル
D. クレデンシャル収集Webサイト
正解: **C (**コメントを発表する**)**

質問: **32**
セキュリティアナリストは、会社のWebサイトの公的にアクセス可能なセクションで発生した潜在的な攻撃を評価するように依頼されました。悪意のある攻撃者は、ユーザーをだまして次のように攻撃しようとしてエントリを投稿しました。

```
https://www.c0mptia.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E
```

次のうち、最も観察された可能性が高いのはどれですか？
A. XSS
B. セッションのリプレイ
C. SOLI
D. DLLインジェクション
正解: **B** (コメントを発表する)

質問: **33**
アナリストは、ネットワーク上のホストのビーコン アクティビティに関する複数のアラートを受け取ります。アクティビティを分析した後、アナリストは次のアクティビティを観察します。
* ユーザーが comptia.org を Web ブラウザーに入力します。
※表示されるウェブサイトはcomptia.orgのサイトではありません。
* Web サイトは、攻撃者からの悪質なサイトです。
* 別のオフィスのユーザーには、この問題はありません。
観測された攻撃の種類は次のうちどれですか?
A. DNS poisoning
B. Domain hijacking
C. On-path attack
D. Locator (URL) redirection
正解: **D** (コメントを発表する)

質問: **34**
組織の最高経営責任者 (CEO) は、従業員が営業時間中いつでも在宅勤務できるようにすることを望んでいます。休暇中にリスクの高い国から柔軟に働き、別の国のサードパーティ組織に働きかけます。最高情報責任者 (CIO) は、リスクの大部分を軽減するために、会社がいくつかの基本を実装できると考えています。CEOの懸念を軽減するのに最適なのは次のうちどれですか? (2 つ選択)。
A. 役割ベースのアクセス制御
B. ジオタグ
C. 位置情報
D. 証明書

E. 時間帯制限
F. トークン
正解: **(**正解を表示します**)**

質問: **35**
次のベストのうち、ベンダーサポートの有効期限が切れてすぐに交換できないシステムを実行しているときに発生するセキュリティリスクを軽減するのはどれですか？
A. バグバウンティプログラムを開始する
B. システムをシャドーITとして分類します。
C. 脆弱性スキャンの頻度を増やします
D. 適切なネットワークアクセス制限を実装する
正解: **(**正解を表示します**)**

質問: **36**
次の ISO 規格のうち、プライバシーについて認定されているのはどれですか?
A. ISO 9001
B. ISO27002
C. ISO 27701
D. ISO 31000
正解: **C (**コメントを発表する**)**
ISO 27701 also abbreviated as PIMS (Privacy Information Management System) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy. Privacy information management systems are sometimes referred to as personal information management systems.
https://pecb.com/whitepaper/the-future-of-privacy-with-isoiec-27701

質問: **37**
組織は、運用ステータスに展開される前にパッチが開発およびテストされるいくつかの環境を維持しています。運用状態になる直前にパッチが展開される環境は次のうちどれですか？
A. 生産
B. 開発
C. ステージング
D. テスト
正解: **(**正解を表示します**)**

質問: **38**
アナリストが攻撃に関連するログを確認しています。ログは、AV ソリューションによって隔離された悪意のあるファイルを攻撃者がダウンロードしたことを示しています。攻撃者はローカルの非管理者アカウントを利用して、悪意のあるファイルを新しい場所に復元しました。このファイルは、ペイロードを実行するために別のプロセスによって使用されました。アナリストが観測した攻撃は次のうちどれですか?
A. 権限昇格
B. リクエスト偽造

C. インジェクション
D. リプレイアタック
正解: **(**正解を表示します**)**
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf[1]) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.[2] There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.[3] In a CSRF attack, an innocent end user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

質問: **39**
フォレンジック調査中に否認防止を提供するのは、次のうちどれですか?
A. dd によるドライブの複製
B. 揮発性メモリの内容を先にダンプ
C. 機密データの暗号化
D. ドライブ イメージの SHA-2 署名を使用する
E. 証拠に接触した全員を記録する
正解: **D (**コメントを発表する**)**

質問: **40**
ある企業がクラウドへの移行を検討しています。同社は、世界中のさまざまな場所から個人を雇用しています。同社は、オンプレミスインフラストラクチャの青写真を増やしたくはなく、必要な追加の計算能力に対してのみ支払いをしたいと考えています。次のソリューションのうち、会社のニーズに最適なものはどれですか？
A. プライベートクラウド
B. ホットバックアップサイト
C. マネージドセキュリティサービスプロバイダー
D. ハイブリッド環境
正解: **(**正解を表示します**)**

質問: **41**
インターネット向けアプリケーションのコード開発をサードパーティの請負業者にアウトソーシングする場合のセキュリティ上の最大の懸念事項は次のうちどれですか？
A. 不明なバックドア
B. 知的財産の盗難
C. 昇格された特権
D. 品質保証
正解: **(**正解を表示します**)**

質問: **42**

次のうち、組織全体に深い知識を提供するポリシーはどれですか?
A. 職務分離ポリシー
B. 資産管理ポリシー
C. ジョブ ローテーション ポリシー
D. 利用規定
正解: **(**正解を表示します**)**

質問: **43**
次のうち、潜在的な攻撃者の手法をエミュレートすることにより、組織のセキュリティ プログラムの有効性をテストする専門チームはどれですか?
A. 赤チーム
B. チーム中
C. 青チーム
D. 紫チーム
正解: **(**正解を表示します**)**
Red team-performs the offensive role to try to infiltrate the target.

質問: **44**
ある会社がヨーロッパの顧客の個人情報の取り扱い方法を監査している会社は次のうちどれに相談すべきですか？
A. GDPR
B. PCI DSS
C. ISO
D. NIST
正解: **(**正解を表示します**)**

質問: **45**
ワークステーションにログインするたびに、ユーザーにバナーが表示されます。バナーには、ユーザーがプライバシーを合理的に期待する権利はなく、アクセスは許可された担当者のみであることが記載されています。
そのバナーを越えて進むために。ユーザーは [OK] ボタンをクリックする必要があります。これは次の例のどれですか?
A. SLA
B. MOU
C. AUP
D. 秘密保持契約
正解: **C (**コメントを発表する**)**

質問: **46**
A
ユーザーがデスクトップを使用して企業ネットワーク内からWebサイトに移動しようとしています。ユーザーがURLを入力したとき。https://www.site.comの場合、ブラウザから証明書の不一致の警告が表示されます。http://www.anothersite.comにアクセスしても、ユーザーは警告を受け取りません。この攻撃について説明しているのは次のうちどれですか？
A. DNSポイズニング

B. 邪悪な双子
C. オンパス
D. ドメインハイジャック
正解: **(**正解を表示します**)**

質問: **47**
SIEM 内の集約されたログ ファイルの整合性を保証するセキュリティのベスト プラクティスは次のうちどれですか?
A. 集約されたログ ファイルを少なくとも 1 日に 2 回、または現地の規制要件に従ってバックアップします。
B. 集約されたログ ファイルを書き込み保護し、アクセスが制限された隔離されたサーバーに移動します。
C. ソース ログ ファイルをバックアップし、少なくとも 6 年間、または地域の規制要件に従ってアーカイブします。
D. 現地の規制要件に準拠するソース ログ ファイル サーバーでハッシュを設定します。
正解: **D (**コメントを発表する**)**

質問: **48**
最近のフィッシング キャンペーンにより、複数のユーザー アカウントが侵害されました。セキュリティ インシデント対応チームは、すべてのフィッシング メールを受信時にフィルタリングし、送信者のメール アドレスをブロックするという手作業を削減するとともに、その他の時間のかかる軽減措置を講じる任務を負っています。これらのタスクを合理化するために構成できるのは、次のうちどれですか?
A. ファイアウォール ルール
B. SIEM データ収集
C. URL フィルター
D. MOM ポリシー
E. SOAR プレイブック
正解: **(**正解を表示します**)**

質問: **49**
最高セキュリティ責任者は、バックエンド インフラストラクチャのスケーラビリティと柔軟性を向上させ、サービスを中断することなく更新および変更できるソリューションを探しています。セキュリティ アーキテクトは、バックエンド サーバーのリソースを削減するソリューションを選択することを望んでおり、バックエンド サーバーで実行されるアプリケーションにとってセッションの永続性は重要ではないことを強調しました。次のうち、要件を最もよく満たすのはどれですか?
A. リバース プロキシ
B. 自動パッチ管理
C. スナップショット
D. NIC チーミング

正解: **A** (コメントを発表する)
A reverse proxy would be the best solution for increased scalability and flexibility for back-end infrastructure.

質問: **50**
組織は VPN を介してすべてのトラフィックをルーティングします ほとんどのユーザーはリモートであり、機密情報を格納する企業のデータセンターに接続します インターネット境界にはファイアウォールがあり、その後に DIP アプライアンス、VPN サーバー、およびデータセンター自体が続きます。次のうち、最も弱い設計要素はどれですか?
A. VPN トンネルに 2 つのホップを追加すると、リモート接続が遅くなる場合があります
B. 分割トンネル接続は、DLP アプライアンスのパフォーマンスに悪影響を及ぼす可能性があります
C. 暗号化された VPN トラフィックは、ネットワークに出入りするときに検査されません。
D. DLP アプライアンスは NGFW に統合する必要があります。
正解: (正解を表示します)

質問: **51**
新しい会社は、WLANを構築するときにチャネル干渉を回避したいと考えています。会社は、無線周波数の動作を知り、デッドゾーンを特定し、アクセスポイントに最適な場所を決定する必要があります。次のうちどれを最初に行う必要がありますか？
A. ヒートマップを構成します。
B. キャプティブポータルを利用します。
C. 現地調査を実施します。
D. Wi-Fiアナライザーをインストールします。
正解: (正解を表示します)

質問: **52**
ネットワークからのデータの流出を阻止または防止する効果的なツールは次のうちどれですか?
A. TPM
B. FDE
C. DLP
D. NIDS
正解: **C** (コメントを発表する)

質問: **53**
広報チームは、大規模な電子商取引会社の施設を巡るツアーにゲストのグループを連れて行きます。ツアーの前日に、会社は従業員に電子メールを送信して、すべてのホワイトボードを掃除し、すべてのデスクを片付けていることを確認します。同社は、防御しようとしている可能性が最も高いです。
A. 専有情報の損失
B. 会社の名誉毀損
C. ソーシャル エンジニアリング
D. 資格情報の公開
正解: (正解を表示します)

In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information think phishing, spoofing. That is not being demonstrated in this question. The company is protecting themselves from loss of proprietary information by clearing it all out. so that if anyone in the tour is looking to take it they will be out of luck

質問: **54**
セキュリティアナリストは、最高情報セキュリティ責任者から次のように依頼されました。
*インフラストラクチャの集中管理を提供する安全な方法を開発する
*老朽化したエンドユーザーのマシンを絶えず交換する必要性を減らします
*一貫したユーザーデスクトップの費用を提供する
次のBESTのうち、これらの要件を満たすものはどれですか？
A. コンテナ化
B. モバイルデバイス管理
C. BYOD
D. VDI
正解: **(**正解を表示します**)**

質問: **55**
いくつかの大学が共同研究プロジェクトに参加しており、コンピューティングリソースとストレージリソースを共有する必要があります。次のクラウド導入戦略のうち、このニーズに最適なものはどれですか。
A. コミュニティ
B. プライベート
C. 公開
D. ハイブリッド
正解: **(**正解を表示します**)**
Community cloud storage is a variation of the private cloud storage model, which offers cloud solutions for specific businesses or communities. In this model, cloud storage providers offer their cloud architecture, software and other development tools to meet the requirements of the community. A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

質問: **56**
SOC は、最近のインシデントの後、プロセスと手順を見直しています。このレビューでは、感染したホストを隔離することが最善の方法であると判断するのに 30 分以上かかったことが示されています。これにより、マルウェアが封じ込められる前に、追加のホストに拡散することができました。インシデント対応プロセスを改善するには、次のうちどれが最適ですか?
A. 許容される使用法に関する追加のエンドユーザー トレーニングを提供する
B. 感染したホストの手動検疫の実装
C. ネットワークを信頼できるゾーンと信頼できないゾーンに分割する
D. より良い意思決定ポイントでプレイブックを更新する
正解: **(**正解を表示します**)**

質問: **57**

次のうち、パブリック クラウドでのアプリケーションのホスティングに特に関連するリスクはどれですか?
A. ゼロデイ
B. 内部脅威
C. 保護されていない root アカウント
D. 共有テナンシー
正解: **(**正解を表示します**)**

質問: **58**
ネットワーク管理者は、Web ページの読み込み時間が長いという警告を受けました。ルーティングまたは DNS の問題ではないと判断した後、管理者はルーターにログインしてコマンドを実行し、次の出力を受け取ります。

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

ルーターで発生しているのは次のうちどれですか?
A. DDoS 攻撃
B. リソース枯渇
C. バッファオーバーフロー
D. メモリリーク
正解: **(**正解を表示します**)**

質問: **59**
最近のセキュリティ インシデントを調査しているときに、セキュリティ アナリストは、特定のサーバー上のすべてのネットワーク接続を表示することにしました。必要な情報を提供するのは次のうちどれですか?
A. nslookup
B. ネット統計
C. nmap
D. arp
正解: **(**正解を表示します**)**

質問: **60**
ファイルのハッシュを公開する理由は次のうちどれですか?
A. ファイルの整合性を検証するには
B. ハッシュを復号化パスフレーズとして使用するには
C. ハッシュをソフトウェア アクティベーション キーとして使用するには
D. ソフトウェアがデジタル署名されているかどうかを確認するには
正解: **D (**コメントを発表する**)**

質問: **61**

組織のアカウントのユーザー名とパスワードが 3 人目に発見された後、セキュリティ エンジニアがログ ファイルを確認しています。エンジニアは、ベンダーの Web サイトの IP アドレスが 1 つ前に変更されたことに気付きました。この変化は8時間続きました。次の攻撃のうち、使用された可能性が最も高いのはどれですか?

A. 中間者
B. スピアフィッシング
C. 悪の双子
D. DNS ポイズング

正解: **D** (コメントを発表する)

DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer). https://en.wikipedia.org/wiki/DNS_spoofing

質問: **62**

最近のセキュリティ違反の後、セキュリティアナリストは、prot 23を介してネットワークデバイスにアクセスするために、ネットワークを介してcieartextを介していくつかのadmimstratrveusemamesとパスワードが送信されていると報告しています。ネットワークデバイスを構成しますか？

A. FTP
B. SNMPv3
C. SFTP
D. Telnet
E. SSH

正解: (正解を表示します)

質問: **63**

次のうち、従業員が不適切な Web サイトにアクセスしている同僚に会うのを防いでいるのはどれですか?

A. AUP
B. 秘密保持契約
C. ジョブ ローレーション ポリシー
D. 職務分離ポリシー

正解: (正解を表示します)

質問: **64**

ユーザーは、週末に仕事を片付けたいと考えていましたが、VPN を使用して企業ネットワークにログインする際に問題がありました。月曜日に、ユーザーはこの問題のチケットをオープンしましたが、正常にログインできました。次のうち、実施されているポリシーを最もよく表しているのはどれですか?
A. 時間ベースのログイン
B. ジオフェンシング
C. パスワード履歴
D. ネットワークの場所
正解: **(**正解を表示します**)**

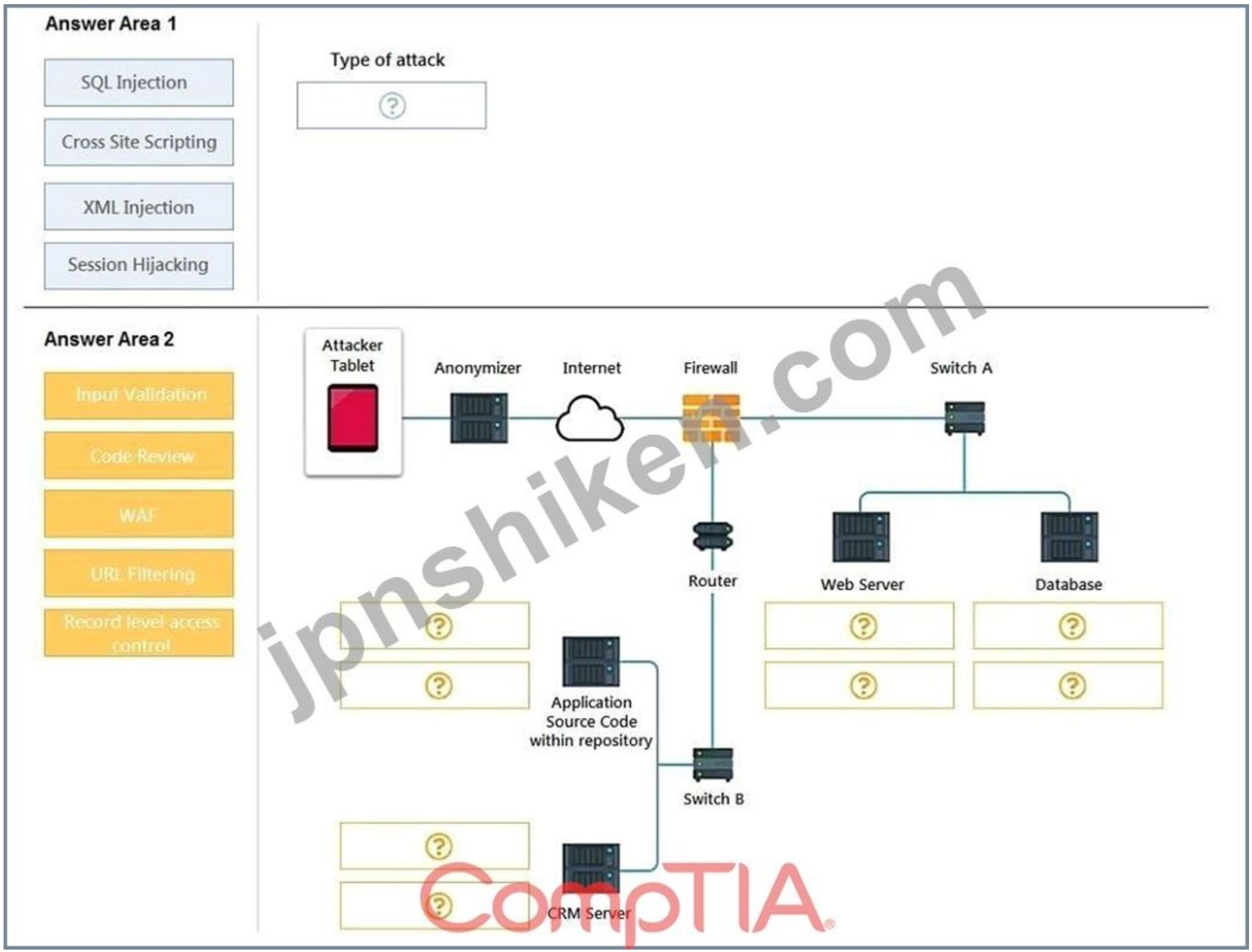
質問: **65**
ソフトウェア インベントリ レポートを作成しているときに、セキュリティ アナリストは、会社のほとんどのサーバーにインストールされている不正なプログラムを発見しました。このプログラムは、経理チームのみに展開されるアプリケーションと同じコード署名証明書を利用します。次の緩和策のうち、サーバー環境を最も安全に保護できるのはどれですか?
A. アカウンティング アプリケーション ファイルのハッシュを許可リストに追加します。
B. 承認されたアプリケーションのコード署名証明書を更新します。
C. 両方のプログラムで使用されているコード署名証明書を取り消します。
D. 承認されていないすべてのファイル ハッシュのインストールをブロックします。
正解: **(**正解を表示します**)**

質問: **66**
セキュリティ アナリストは、電子メールで送信されたアラートを受け取りました。アナリストの最高情報セキュリティ責任者 (CISO) は、PII は細心の注意を払って処理する必要があることを明らかにしました。次のうち、アラートが発生した可能性が最も高いのはどれですか?
A. S/MIME
B. DLP
C. IMAP
D. HIDS
正解: **B (**コメントを発表する**)**
Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

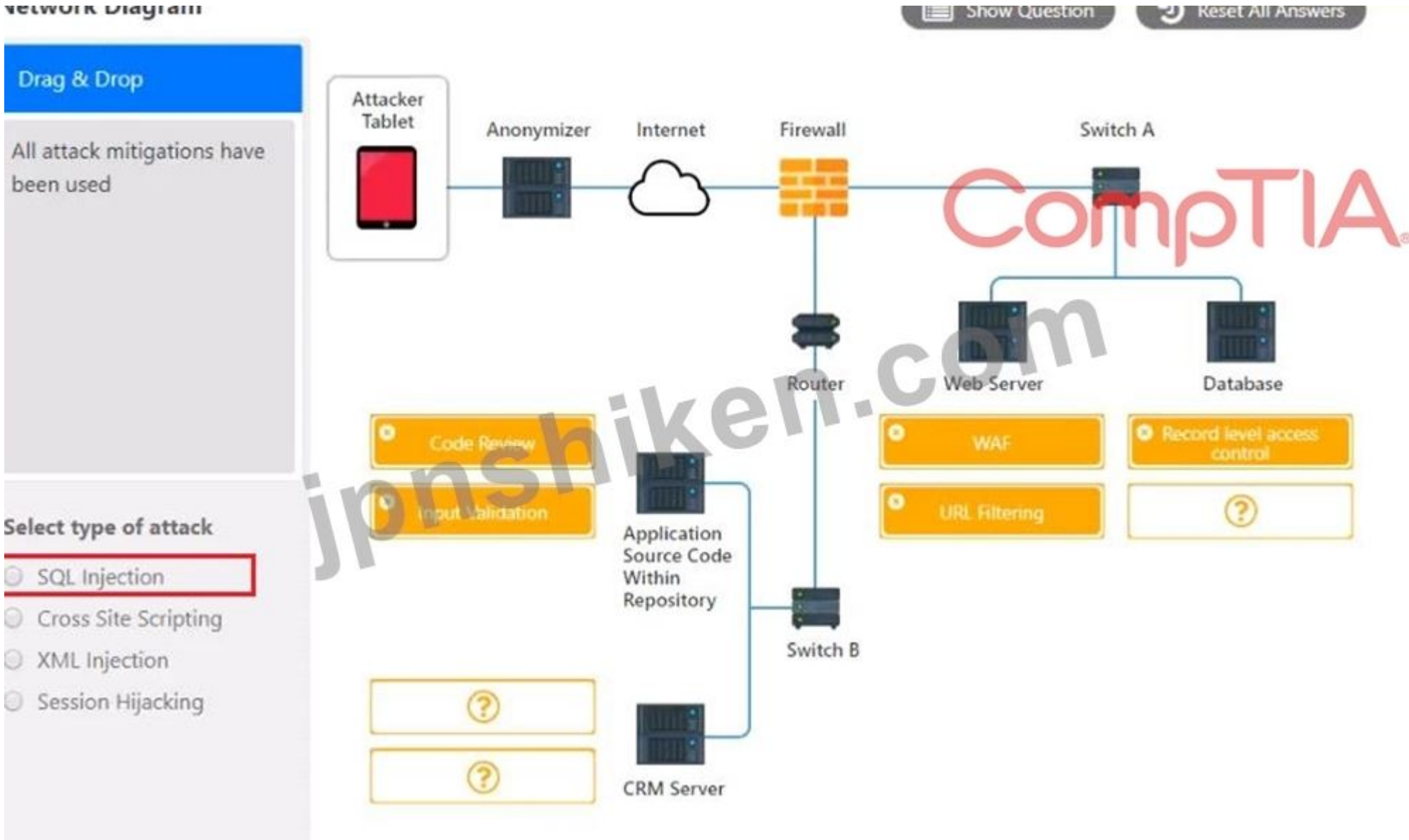
質問: **67**
組織が緩和手順に優先順位を付けることができるように、既知の脆弱性の計算値を提供するのは次のうちどれですか？
A. SIEM
B. CVSS
C. CVE
D. SOAR
正解: **(**正解を表示します**)**

質問: **68**
ドラッグドロップ

会社に対して攻撃が発生しました。
手順
あなたは次のことを任されています。
攻撃者のタブレットをクリックして出力を確認することで、ネットワークで発生している攻撃の種類を特定します。(回答領域 1)。
資産を適切なサーバーにドラッグして将来の攻撃の有効性を減らすために、どの補償制御を資産に実装する必要があるかを特定します。
(回答エリア 2) すべてのオブジェクトが使用されますが、すべてのプレースホルダーが埋められるわけではありません。オブジェクトは一度しか使用できません。
いつでもシミュレーションを初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。


Answer Area 1
SQL Injection
Cross Site Scripting
XML Injection
Session Hijacking
Type of attack
Answer Area 2
Input Validation
Code Review
WAF
URL Filtering
Record level access control
Attacker Tablet
Anonymizer
Internet
Firewall
Switch A
Router
Web Server
Database
Application Source Code within repository
Switch B
CRM Server

正解:



質問: **69**
サーバー管理者が password.txt という名前のドキュメントをサーバーの管理者アカウントのデスクトップに配置する理由を最もよく説明しているのは、次のうちどれですか?
A. システムを回復する必要がある場合、ドキュメントはバックアップ ファイルです。
B. この文書はハニーファイルであり、サイバー侵入者の注意を引くことを目的としています。
C. ドキュメントは、OS がログイン資格情報を検証するために必要な標準ファイルです。
D. このドキュメントは、アカウントが危険にさらされた場合に備えて、すべてのキーストロークを保存するキーロガーです。
正解: **(**正解を表示します**)**

質問: **70**
セキュリティ アナリストは、企業のサーバーに格納されるデータを分類する任務を負っています。次のうち、専有物として分類する必要があるのはどれですか?
A. マーケティング戦略
B. お客様のメールアドレス
C. 従業員の給与

D. お客様の生年月日
正解: **(**正解を表示します**)**

質問: **71**
次のリスク管理戦略のうち、運用目的で既知のリスクを持つレガシーシステムを維持するために組織が使用するのはどれですか？
A. 転移
B. 緩和
C. 回避
D. 受け入れ
正解: **D (**コメントを発表する**)**

質問: **72**
最高情報セキュリティ責任者は、シャドーITのnsk削減を指示し、認可されていないすべての高nskSaaSアプリケーションをユーザーアクセスからブロックすることを要求するポリシーを作成しました。このリスクを軽減するための最良のセキュリティソリューションは次のうちどれですか。
A. VPNコンセントレーター
B. MFA
C. CASB
D. VPCエンドポイント
正解: **(**正解を表示します**)**

質問: **73**
最近の監査では、企業顧客との通信に使用される Web アプリケーションでの特定の暗号化標準の使用に関する重要な調査結果が明らかになりました。顧客の技術的な制限により、同社は暗号化標準をアップグレードできません。このシナリオによって生じるリスクを軽減するために使用する必要があるコントロールの種類は次のうちどれですか?
A. 補正中
B. 探偵
C. 物理
D. 予防
正解: **(**正解を表示します**)**

質問: **74**
RTO が BIA に含まれる理由を説明しているのは、次のうちどれですか?
A. 組織がデータを既知の時点に回復できるように、バックアップ アプローチを通知します。
B. 資産の損失を収益化し、リスク軽減のための損益分岐点を決定します。
C. アプリケーションまたはシステムの許容ダウンタイムを特定します。
D. リスクに優先順位を付けて、組織がリソースを適切に割り当てられるようにします。
正解: **(**正解を表示します**)**

質問: **75**

地理的に分散した2つのデータセンターを持つ大銀行は、両方の場所での大規模な停電を懸念しています。毎日、各場所で数秒間続く非常に大きな停電が発生しています。ただし、夏の間は、特に最大1時間続く意図的な電圧低下のリスクが高くなります。jndustnal製錬所の近くの場所の1つで。データ損失のリスクを軽減するための最良の解決策は次のうちどれですか？
A. ジェネレーター
B. 二重供給
C. PDU
D. 毎日のバックアップ
E. UPS
正解: **(**正解を表示します**)**

質問: **76**
ラップトップが関与するインシデント対応プロセス中に、マルウェアのエントリポイントとしてホストが特定されました。
管理チームは、ラップトップを復元してユーザーに返却してもらいたいと考えています。サイバーセキュリティアナリストは、ホストへの侵入を引き続き調査したいと考えています。アナリストが調査を続行し、ラップトップをできるだけ早くユーザーに返却できるようにするのは、次のうちどれですか？
A. dd
B. 頭
C. tcpdump
D. memdump
正解: **C (**コメントを発表する**)**

質問: **77**
組織は、許可されていないユーザーがアクセスを拒否される可能性が最も高い生体認証システムを実装したいと考えています。組織が生体認証ソリューションを比較するために使用する必要があるのは次のうちどれですか？
A. 遠い
B. 使いやすさ
C. FRR
D. CER
E. コスト
正解: **(**正解を表示します**)**

質問: **78**
エアギャップのある実験室の HVAC システムを保護する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. 監視ログを保護するため
B. 可用性を確保するため
C. データ漏洩を防ぐため
D. サードパーティのアクセスを容易にするため
正解: **C** (コメントを発表する)

質問: **79**
ソフトウェアとインフラストラクチャのコストを削減および制限するために、最高情報責任者は電子メールサービスをクラウドに移行することを要求しました。クラウドプロバイダーと組織は、機密データを保護するためのセキュリティ制御を備えている必要があります。次のクラウドサービスのうち、リクエストに最適なものはどれですか？
A. SaaS
B. ダース
C. ラース
D. Paas
正解: **D** (コメントを発表する)

質問: **80**
ネットワーク管理者は、回復力とアップタイムに重点を置いて、新しいデータセンターを構築する必要があります。この目的を最もよく満たすのは次のうちどれですか？ 2つ選んでください。）
A. デュアル電源
B. オフサイト バックアップ
C. 自動 OS アップグレード
D. NIC チーミング
E. 定期侵入テスト
F. ネットワーク接続ストレージ
正解: **A,B** (コメントを発表する)
https://searchdatacenter.techtarget.com/definition/resiliency

質問: **81**
企業は、重要なサービスをサポートするためにレガシー ソフトウェアを引き続き使用する必要があります。次のうち、この行為のリスクを最もよく説明しているのはどれですか?
A. 安全でないプロトコル
B. ベンダー サポートの欠如
C. 弱い暗号化
D. デフォルトのシステム構成
正解: **A** (コメントを発表する)

質問: **82**

セキュリティ アナリストは、セキュリティ評価のために一連の SOAP HTTP 要求でパケット キャプチャを実行しています。アナリストは出力をファイルにリダイレクトします。キャプチャが完了した後、アナリストは最初のトランザクションをすばやく確認し、一連のリクエスト全体から特定の文字列を検索する必要があります。タスクを完了するために使用するのに最適なのは、次のうちどれですか? (2 つ選択)。
A. head
B. Tcpdump
C. grep
D. rail
E. curl
F. openssi
G. dd
正解: **A,C** (コメントを発表する)
A - "analyst needs to review the first transactions quickly"
C - "search the entire series of requests for a particular string"

質問: **83**
セキュリティ アナリストが Web アプリケーションのログを調べていると、次のログが見つかりました。

```
https://www.comptia.org/contact-us/%3Ffile%3D..%2F..%2F..%2Fetc%2Fpasswd
```

観測されている攻撃は次のうちどれですか?
A. XSS
B. ディレクトリトラバーサル
C. オンパス攻撃
D. CSRF
正解: (正解を表示します)

質問: **84**
会社の医師会は、組織の責任を制限するために保険会社と契約しました。
次のリスク管理慣行のうち、最もよく説明しているのはどれですか？
A. 回避
B. 謝辞
C. 緩和
D. 転移
正解: **D** (コメントを発表する)

質問: **85**
Web サイトの開発者が新しい e コマース Web サイトに取り組んでおり、簡単な再注文プロセスを作成するためにクレジット カード番号を保存する最も適切な方法について、情報セキュリティの専門家に尋ねました。この目標を達成するのに最適な方法は次のうちどれですか?
A. 入力時にクレジット カード番号をハッシュ化します。
B. 磁気ストリップ情報のソルティング
C. データベース内のクレジット カードのトークン化

D. 転送中のクレジット カード情報を暗号化します。
正解: **(**正解を表示します**)**

質問: **86**
デバイスのファームウェアの脆弱性を悪用してデュアルホーム（有線および無線）多機能デバイスにアクセスした後、侵入テスターは別のネットワーク資産へのシェルアクセスを取得します。この手法は次の例です。
A. 特権の昇格
B. フットプリント
C. ピボット。
D. 永続性
正解: **(**正解を表示します**)**

質問: **87**
最近の外部監査の後、コンプライアンス チームは、保管中のカード会員データを暗号化していない、準拠していない範囲内のいくつかのホストのリストを提供しました。次のコンプライアンス フレームワークのうち、コンプライアンス チームの最大の懸念に対処するものはどれですか?
A. ISO27001
B. GDPR
C. PCI DSS
D. NIST CSF
正解: **C (**コメントを発表する**)**

質問: **88**
北アメンカに拠点を置くソーシャルメディア企業は、新しいグローバル市場への拡大を目指しており、国際基準への準拠を維持する必要があります。同社のデータ保護責任者が最も懸念しているのは次のうちどれですか？」
A. ISO 27001
B. NISTフレームワーク
C. PCI-DSS
D. GDPR
正解: **(**正解を表示します**)**

質問: **89**
何人かのユーザーがヘルプデスクでチケットを開いています。ヘルプデスクは、さらなるレビューのためにチケットをセキュリティアナリストに再割り当てしました。セキュリティアナリストは、次のメトリックをレビューします。

Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

次のうち、セキュリティアナリストのレビューの結果である可能性が最も高いのはどれですか？
A. Sales-PCのユーザーがフィッシング攻撃に陥った

B. PCとルーターの間でオンパス攻撃が発生しています
C. 企業のPCがボットネットになりました
D. ISPがアウトバウンド接続をドロップしています
正解: **B** (コメントを発表する)

質問: **90**
最近、悪意のあるアクターが企業のネットワークに侵入し、データセンターに横移動しました。調査の結果、フォレンジック企業は侵害されたサーバーのメモリにあったことを知りたがっています。次のファイルのうち、フォレンジック会社に提出する必要があるのはどれですか?
A. セキュリティ
B. アプリケーション
C. ダンプ
D. シスログ
正解: **(**正解を表示します**)**
Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated by Windows or by the apps that crash, but you can also manually generate them
https://www.digitalcitizen.life/view-contents-dump-file/

質問: **91**
ユーザーには、建物への物理的なアクセスを提供するスマート カードが発行されています。カードには、情報システムへのアクセスに使用できるトークンも含まれています。ユーザーは、建物全体に配置された任意のシン クライアントにログインして、毎回同じデスクトップを表示できます。これらの機能を提供するために利用されているテクノロジは次のうちどれですか? (2 つ選択)
A. RFID
B. GPS
C. VDI
D. TOTP
E. BYOD
F. 対処
正解: **(**正解を表示します**)**

質問: **92**
ある会社は、一部の企業アカウントが侵害された疑いがあります。ユーザーに認識されない場所からの不審なログインの数は増加しています。旅行する従業員は、新しいサインインプロパティに対して行われる可能性のある正当なログイン要求をブロックすることなく、アカウントを保護する必要があります。次のセキュリティ制御のどれを実装できますか？

A. アカウントリクエストがnskしきい値に達したときにMFAを適用します
B. アクセス制御スキームを随意アクセス制御にシフトする
C. 本社からのアクセスのみを許可するようにジオフェンスを実装します
D. 営業時間に合わせた時間ベースのログインリクエストを実施する
正解: **C** (コメントを発表する)

質問: **93**
セキュリティ エンジニアは、ビジネス パートナーにファイルを送信するためのファイル転送ソリューションを構築しています。ユーザーは、ファイルを特定のディレクトリにドロップして、サーバーからビジネス パートナーに送信したいと考えています。ビジネス パートナーへの接続はインターネット経由であり、安全である必要があります。次のどれを使用できますか?
A. SRTP
B. S/MIME
C. LDAPS
D. SSH
正解: (正解を表示します)

質問: **94**
侵入テスターは、アプリケーションをファジングして、スタックの EIP がメモリ上のどこにあるかを特定しています。侵入テスターが実行を計画している攻撃は、次のうちどれですか?
A. レースコンディション
B. XSS
C. パスザハッシュ
D. バッファオーバーフロー
正解: (正解を表示します)

質問: **95**
次のうち、組織がクラウド プロバイダーのすぐに使用できるアプリケーションを利用する場合を最もよく表しているのはどれですか?
A. IaaS
B. SaaS
C. パス
D. XaaS
正解: (正解を表示します)
SaaS, or software as a service, is on-demand access to ready-to-use, cloud-hosted application software.
https://www.ibm.com/cloud/learn/iaas-paas-saas

質問: **96**
システム管理者は、仮想サーバーのパフォーマンスの低下を報告します。管理者は仮想メモリの割り当てを増やして状態を改善しますが、数日後にパフォーマンスが再び低下します。管理者は分析ツールを実行し、次の出力を確認します。

```
==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 82116 bytes
==3214== definitely lost: 4608 bytes in 18 blocks.
```

管理者はtimeAttend.exeを終了し、次の数日間のシステムパフォーマンスを監視し、システムパフォーマンスが低下しないことに気付きます。次の問題のうち、最も発生しやすいものはどれですか。

A. DLLインジェクション
B. バッファoveiflow
C. メモリリーク
D. API攻撃
正解: **B** (コメントを発表する)

質問: **97**
データ流出分析は、攻撃者がWebサーバーからシステム構成ノートをダウンロードすることに成功したことを示しています。Webサーバーのログは削除されましたが、アナリストは、システム構成のメモがWebサーバーのデータベース管理者のフォルダーに保存されていると判断しました。次の攻撃のうち、何が発生したかを説明するものはどれですか。 2つ選択）
A. SQLインジェクション
B. ディレクトリトラバーサル
C. 特権の昇格
D. クロスサイトスキャプティング
E. パスザハッシュ
F. 偽造を要求する
正解: (正解を表示します)

質問: **98**
セキュリティアナリストは、コンテナ内で実行されている一部のアプリケーションで検出された重大な脆弱性を懸念しています。次のうち、最善の修復戦略はどれですか。
A. 実行中の各コンテナーに個別にパッチを適用し、アプリケーションをテストします
B. ベースコンテナイメージを更新し、環境を再デプロイします
C. サーバーの通常のパッチ適用スケジュールにコンテナーを含めます
D. コンテナが実行されているホストを更新します
正解: **A** (コメントを発表する)

質問: **99**
企業は、日常業務を中断することなく、意思決定ポイントと関連するインシデント対応アクションをテストする実際のシナリオを使用して、更新されたインシデント対応計画を検証する必要があります。次のうち、会社の要件を最もよく満たすのはどれですか？
A. レッドチームの練習
B. キャプチャーザフラッグ演習
C. フィッシング詐欺
D. 卓上運動
正解: **D** (コメントを発表する)

質問: **100**
最高情報セキュリティ責任者（CISO）は、顧客データを保護するための適切な管理が実施されていることを示すサポートドキュメントをサードパーティベンダーが提供するように要求しました。サードパーティベンダーがCISOに提供するのに最適なのは次のうちどれですか？
A. GDPRコンプライアンスの証明
B. SOC2タイプ2レポート
C. NISTRMFワークブック
D. クラウドセキュリティアライアンスの資料
正解: **(**正解を表示します**)**

質問: **101**
ある企業は最近、専有情報が競合他社に漏洩したときに重大なデータ損失を経験しました。会社は適切なラベルを使用して特別な予防措置を講じました。ただし、電子メールフィルターログにはインシデントの記録はありません。調査の結果、企業ネットワークが侵害されていないことが確認されましたが、ドキュメントは従業員のCOPEタブレットからダウンロードされ、クラウドストレージを介して競合他社に渡されました。
このデータ漏洩の最善の改善策は次のうちどれですか？
A. ユーザートレーニング
B. CASB
C. DLP
D. MDM
正解: **C (**コメントを発表する**)**

質問: **102**
USBリムーバブルメディア制限ポリシーを実施するための費用対効果の高い物理的制御の最良の例は次のうちどれですか？
A. USBとリムーバブルメディアの接続を検出するためのエンドポイントエージェントのインストール
B. USBポートにセキュリティ/アンチタンパーテープを貼り付けて、ポート番号を記録し、定期的にポートを検査します
C. 許可されたUSBリムーバブルメディアへのアクセスを制限するGPOを実装し、それが実施されていることを定期的に確認します
D. USBポートにアクセスできない、ロックされたキー制御コンテナにシステムを配置する
正解: **(**正解を表示します**)**

質問: **103**
ネットワーク エンジニアは、運用サーバーと開発サーバーに使用される 2 つのサブネットを作成しました。セキュリティ ポリシーに従って、運用サーバーと開発サーバーにはそれぞれ、互いに直接通信できない専用ネットワークが必要です。サーバー管理者がこれらのデバイスにアクセスできるようにするには、次のうちどれを展開する必要がありますか?
A. インターネット プロキシ サーバー
B. ジャンプサーバー
C. NIDS
D. VLAN
正解: **B (**コメントを発表する**)**

質問: **104**

リスク評価により、リスクを是正するためのコストが保険契約の5年間のコストよりも大きいと判断されたため、ofgantzationは保険契約を購入することを決定しました。組織はリスクを可能にしています
A. 回避
B. 転移
C. 緩和
D. 受け入れ
正解: **B** (コメントを発表する)

質問: **105**
最近のセキュリティ違反により、ファイアウォールおよびネットワーク管理ソリューション内のソフトウェアの脆弱性が悪用されました。各デバイスで違反が発生した時期を特定するために最もよく使用されるのは、次のうちどれですか？
A. SIEM相関ダッシュボード
B. ファイアウォールのsyslogイベントログ
C. ネットワーク管理ソリューションのログイン監査ログ
D. 帯域幅モニターとインターフェースセンサー
正解: **A** (コメントを発表する)

質問: **106**
ある会社は最近、製品をオンラインで販売するために e コマース ポータルを立ち上げました。同社は、セキュリティ基準への準拠を必要とする支払いにクレジット カードの受け入れを開始したいと考えています。電子商取引プラットフォームでクレジット カードを受け入れる前に、会社が準拠する必要がある基準は次のうちどれですか?
A. PCI DSS
B. ISO22301
C. ISO27001
D. NIST CSF
正解: **A** (コメントを発表する)
Additionally, many organizations should abide by certain standards. For example, organizations handling credit card information need to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS includes six control objectives and 12 specific requirementsthat help prevent fraud

質問: **107**
最高情報セキュリティ責任者は、新しいデータセンターアーキテクチャの復元力要件を定義しました。要件は次のとおりです。
*重要なファイル共有は、自然災害の最中およびその後も引き続きアクセス可能です

*ハードディスクの5%は、データに影響を与えることなく、いつでも障害が発生する可能性があります。
*バッテリーレベルが20%を下回ると、システムは正常にシャットダウンするように強制されます。これらの目標を最もよく達成するために必要なものは次のうちどれですか。 3つ選択）
A. RAID
B. ファイバースイッチング
C. UPS
D. スナップショット
E. 負荷分散
F. 冗長電源
G. NAS
H. 地理的分散
I. laC
正解: **B,G,H (**コメントを発表する**)**

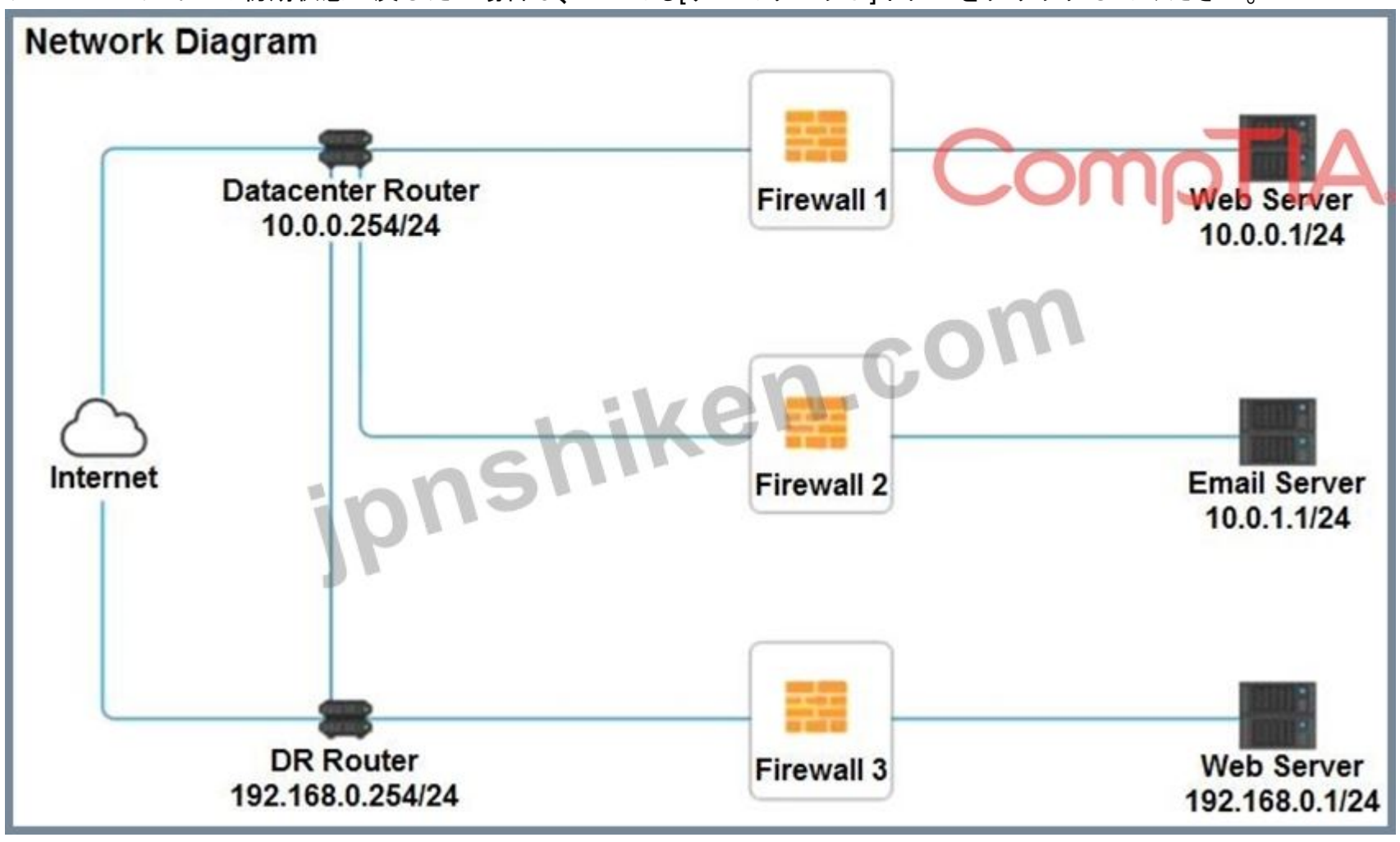
質問: **108**
会社は、会社のWebサイトのアドレスとコンテンツに非常によく似たフィッシングサイトへのリンクが記載された電子メールを受信しています。会社がこの攻撃を軽減するための最良の方法は次のうちどれですか？
A. 会社独自のドメインと同様のドメインのリストを生成し、それぞれにDNSシンクホールを実装します。
B. 自動化されたツールを使用して、フィッシングWebサイトを偽のユーザー名とパスワードで溢れさせます。
C. フィッシングで取得した資格情報を使用してVPNにアクセスする攻撃者をトラップするハニーネットを作成します。
D. インターネットに接続しているすべての電子メールサーバーでPOPとIMAPを無効にし、SMTPSを実装します。
正解: **(**正解を表示します**)**

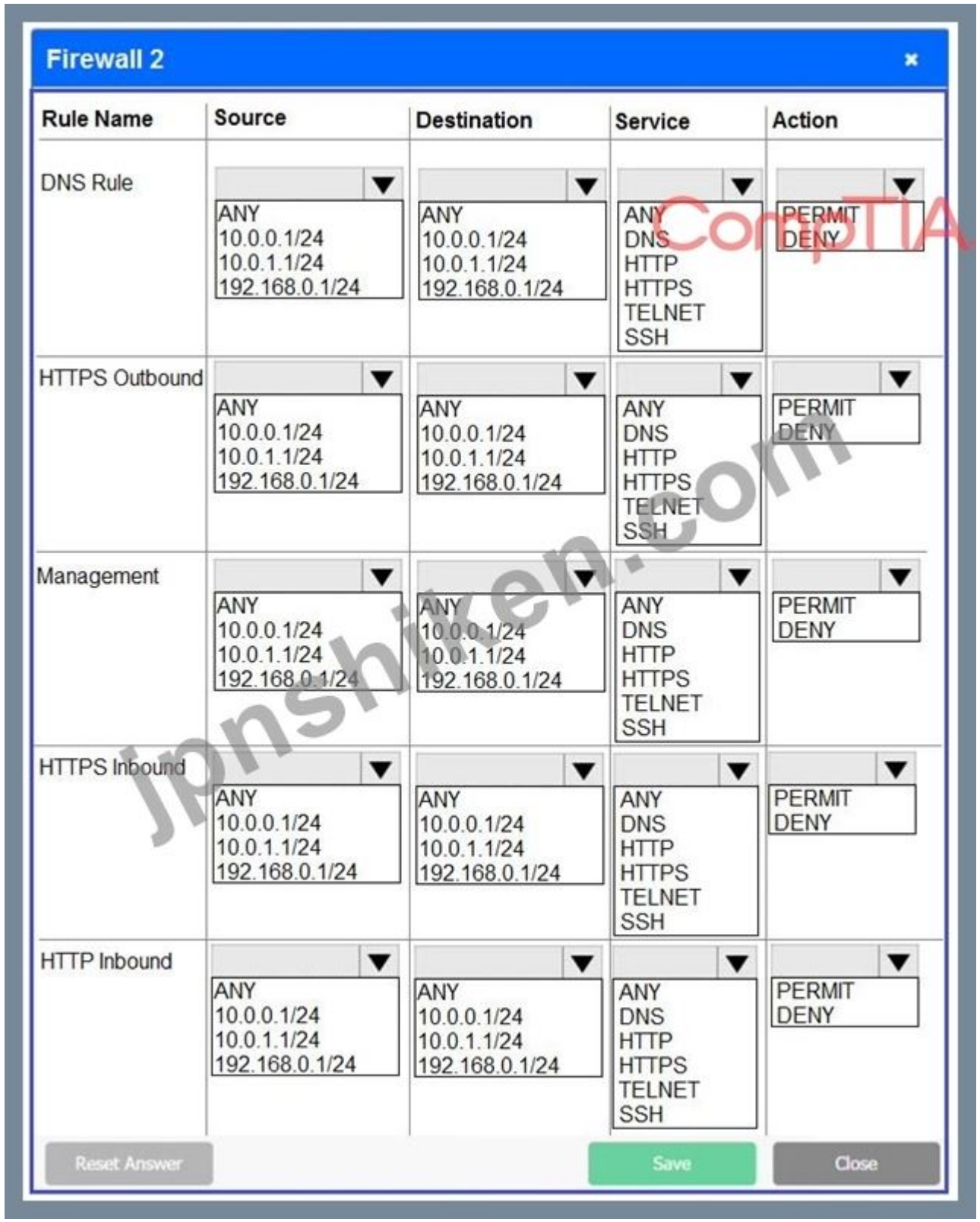
質問: **109**
フラッド ゾーンにある組織は、IT 運用の復旧に関連する懸念事項を次のように文書化する可能性が最も高くなります。
A. 通信計画。
B. 事業継続計画
C. 事業継続計画
D. 災害復旧計画。
正解: **(**正解を表示します**)**

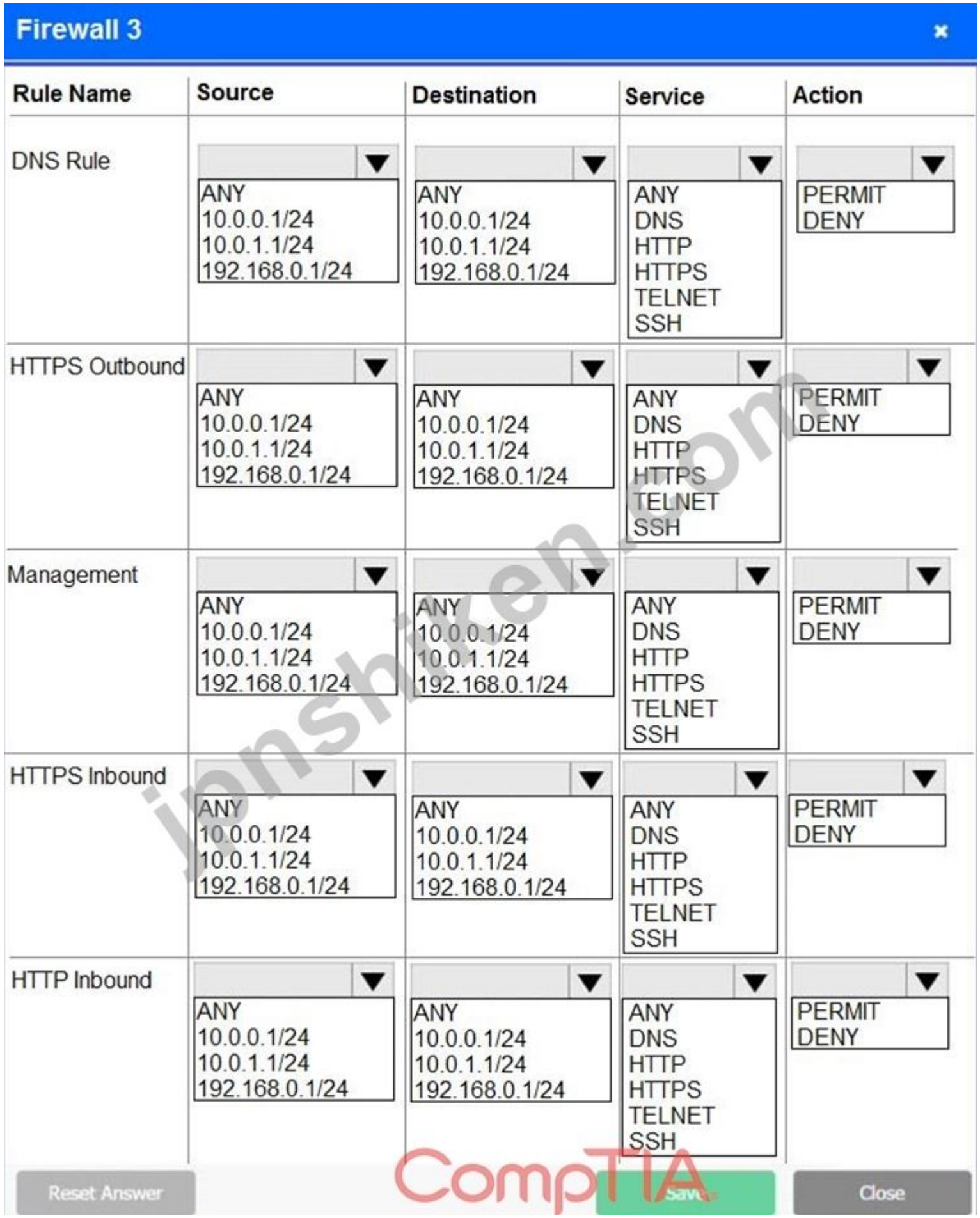
質問: **110**
セキュリティ アナリストは、企業の実行を標的にする可能性のある攻撃の種類を積極的に理解する必要があります。次のインテリジェンス ソースのうち、セキュリティ アナリストがレビューする必要があるのはどれですか?
A. 脆弱性フィード
B. 構造化された脅威情報表現
C. 指標情報の信頼できる自動交換
D. 業界情報共有およびコラボレーション グループ
正解: **(**正解を表示します**)**

質問: **111**
最高情報セキュリティ責任者は、公共のUSB充電ステーションを使用する際に、従業員の携帯電話から機密情報が漏洩するのを防ぎたいと考えています。次のうち、実装するのに最適なソリューションはどれですか？
A. DLP
B. USB OTG
C. USBポートを無効にする
D. USBデータブロッカー
正解: **(**正解を表示します**)**

質問: **112**
ある会社が最近DRサイトを追加し、ネットワークを再設計しています。DRサイトのユーザーは、Webサイトの閲覧に問題があります。
手順
各ファイアウォールをクリックして、以下を実行します。
*クリアテキストのWebトラフィックを拒否します。
*安全な管理プロトコルが使用されていることを確認してください。DRサイトで問題を解決してください。
外部の制約により、ルールセットの順序を変更することはできません。
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[すべてリセット]ボタンをクリックしてください。




Firewall 2
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close


Firewall 3
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Close

正解:

Firewall 1:
DNS Rule - ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound - 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT
Management - ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound - ANY --> ANY --> HTTPS --> PERMIT
HTTP Inbound - ANY --> ANY --> HTTP --> DENY
Firewall 2: No changes should be made to this firewall

Firewall 3:
DNS Rule - ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound - 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT
Management - ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound - ANY --> ANY --> HTTPS --> PERMIT
HTTP Inbound - ANY --> ANY --> HTTP --> DENY

質問: 113

ヘルプデスクの技術者は、組織のサイバーセキュリティモデム応答チームの一員であると主張する誰かから電話を受け取ります。発信者は技術者にネットワークの内部ファイアウォールIPアドレスを確認するように依頼します。技術者の最善の行動方針は次のうちどれですか。
A. 発信者に本人確認のための電子メールを送信するように要求し、要求された情報を電子メールで発信者に提供します
B. 発信者の名前を尋ね、電子メールディレクトリで個人の身元を確認し、要求された情報を電話で提供します
C. 発信者に直接ヘルプデスクに立ち寄り、電話を切り、発信者からのそれ以上の要求を拒否するように指示します。
D. 可能であれば、カーターの電話番号を書き留めてください。情報を要求している人の名前が電話を切ります。組織のサイバーセキュリティ担当者に通知します
正解: **A** (コメントを発表する)

質問: **114**
次のうち、継続的デリバリーソフトウェア開発方法論について説明しているのはどれですか？
A. V字型
B. アジャイル
C. スパイラル
D. 滝
正解: (正解を表示します)

質問: **115**
IT セキュリティ マネージャーは、公開されている会社情報に関するレポートを要求します。管理者の懸念は、悪意のあるアクターが積極的な偵察を行わずにデータにアクセスできるようになることです。分析を実行するための最も効率的なアプローチは次のうちどれですか?
A. オプションを使用して nmap を実行します: すべてのポートをスキャンし、卑劣なモード。
B. dnsenum を使用してパブリック DNS エントリを確認します。
C. 上場企業の IR を対象とした脆弱性スキャンを実行する
D. ツールにドメイン パラメータを指定します。
正解: (正解を表示します)

質問: **116**
サイバーセキュリティ管理者のチームは縮小されており、オンプレミスのネットワークとセキュリティ インフラストラクチャを効率的に運用する必要があります。この状況を解決するために、管理者はサービス プロバイダーを雇うことにしました。管理者は次のうちどれを使用する必要がありますか?
A. SDP
B. AAA
C. IaaS
D. MSSP
E. マイクロサービス
正解: **D** (コメントを発表する)
https://www.techtarget.com/searchitchannel/definition/MSSP

質問: **117**

会社の新しい最高情報セキュリティ責任者は、セキュリティ チームに、より強力なユーザー アカウント ポリシーを実装するように依頼しました。新しいポリシーでは、次のことが必要です。
* ユーザーは、過去 10 個のパスワードから一意のパスワードを選択できます
* 特定のリスクの高い国からのユーザーはログインできません
セキュリティ チームは次のうちどれを実装する必要がありますか? (2 つ選択)。
A. ジオタグ
B. ジオフェンシング
C. パスワードの再利用
D. パスワードの複雑さ
E. 位置情報
F. パスワード履歴
正解: **(**正解を表示します**)**

質問: **118**
ユーザーの共通のサインインプロパティのベースラインを作成することにより、リモートアクセスの要求を追跡するためのセキュリティ提案が設定されました。ベースラインの逸脱が検出されると、lv1FAチャレンジがトリガーされます。提案を展開するために構成する必要があるのは次のうちどれですか？
A. 広範な認証プロトコル
B. 等価認証の同時認証
C. エージェントレスネットワークアクセス制御
D. コンテキストアウェア認証
正解: **(**正解を表示します**)**

質問: **119**
次のうち、認証方法として、また不正アクセス試行の警告メカニズムとして機能するのはどれですか?
A. HMAC ベースのワンタイム パスワード
B. 認証サービス
C. プッシュ通知
D. スマートカード
正解: **(**正解を表示します**)**

質問: **120**
脆弱性が発見されましたが、脆弱性に対処する既知のパッチは存在しません。適切な修正がリリースされるまで、次のコントロールのうちどれが最もうまく機能しますか?
A. 修正
B. 探偵
C. 抑止力
D. 補正中
正解: **B (**コメントを発表する**)**

質問: **121**
地方銀行の社長は、潜在的な投資家に SOC ツアーを頻繁に提供することを好みます。次のポリシーのうち、ツアー後に発生する悪意のあるアクティビティのリスクを最も軽減するのはどれですか?
A. アクセス制御
B. パスワードの複雑さ
C. 使用可
D. クリーンデスク
正解: **A** (コメントを発表する)

有効的な**SY0-601-JPN**問題集はJPNTest.com提供され、**SY0-601-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**SY0-601-JPN**試験問題集を提供します。JPNTest.com SY0-601-JPN試験問題集はもう更新されました。ここで**SY0-601-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SY0-601-JPN-mondaishu ¶**1061**問、３０%ディスカウント、特別な割引コード:
JPNshiken」