CompTIA.SY0-601-JPN.v2021-12-01.q139

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：	139
バージョン：	v2021-12-01
ページの閲覧量：	600
問題集の閲覧量：	14538

https://www.jpnshiken.com/shiken/CompTIA.SY0-601-JPN.v2021-12-01.q139.html

質問: **1**
組織は、既存の多要素認証に3番目の要素を実装したいと考えています。組織はすでにスマートカードとパスワードを使用しています。次のうち、3番目の要素に対する組織のニーズを満たすのはどれですか？
A. 指紋
B. PIN
C. 生年月日
D. TPM
正解: **A** (コメントを発表する)

質問: **2**
重大な停止またはインシデントへの対応の適時性について新しいベンダーと交渉する場合、次のうちどれを実施する必要がありますか？
A. MOU
B. NDA
C. MTTR
D. SLA
正解: (正解を表示します)

質問: **3**
会社のユーザーであるジョーは、自分のワークステーションに感染したWebサイトにつながる電子メールリンクをクリックしました。ジョーはネットワークに接続され、ウイルスはネットワーク共有に広がりました。保護対策はこのウイルスを阻止することができず、検出を回避し続けています。このマルウェアから環境を保護するために、管理者は次のうちどれを実装する必要がありますか？
A. ヒューリスティックな動作検出ソリューションを実装します。
B. ネットワーク共有を保護するためにCASBを実装します。
C. IDS / IPSを実装する
D. 定義ベースのアンチウイルスをインストールします。
正解: **A** (コメントを発表する)

質問: **4**
会社の最高情報責任者（CIO）は、最高情報セキュリティ責任者（CISO）と会って、会社の開発者のスキルレベルを向上させるためのいくつかの活動を計画しています。開発者のトレーニングに最も適しているのは次のうちどれですか？
A. バスト意識トレーニング
B. キャプチャーザフラッグコンペティション
C. 物理的セキュリティトレーニング
D. フィッシングシミュレーション
正解: **(**正解を表示します**)**

質問: **5**
セキュリティ評価により、最近展開された運用サーバーでまだ使用されているDESと3DESが決定されます。評価で特定されたのは次のうちどれですか？
A. Unsecmeプロトコル
B. オープンパーミッション
C. 弱い暗号化
D. デフォルト設定
正解: **C (**コメントを発表する**)**

質問: **6**
組織は、管理者/ルートの資格情報とサービスアカウントに対してより厳格な制御を実装する必要があります。プロジェクトの要件は次のとおりです。
クレデンシャルのチェックイン/チェックアウト
パスワードを使用するが知らない能力
パスワードの自動変更
資格情報へのアクセスのログ
次のソリューションのどれが要件を満たしますか？
A. OAuth 2.0
B. 特権アクセス管理システム
C. OpenIDConnect認証システム
D. セキュアエンクレーブ
正解: **(**正解を表示します**)**

質問: **7**
小売業の幹部は最近、主要な競合他社との仕事を受け入れました。翌週、セキュリティアナリストはセキュリティログを確認し、離れたエグゼクティブのアカウントにアクセスするためのログオン試行が成功したことを確認します。次のセキュリティ慣行のどれが問題に対処したでしょうか？
A. 秘密保持契約

B. 利用規定
C. オフボーディング
D. 最小特権
正解: **C** (コメントを発表する)

質問: **8**
ある会社が、外部ストレージデバイスの使用を禁止する内部脅威ポリシーを起草しました。リムーバブルメディアを介したデータの漏えいから会社を最もよく保護するのは次のうちどれですか？
A. ホストベースのセキュリティツールを使用したリムーバブルメディアデバイスと書き込み機能のブロック
B. システムファイルへのユーザーアクセスをブロックするグループポリシーの実装
C. ファイアウォールログでの大規模なデータ転送トランザクションの監視
D. リムーバブルメディアポリシーについて従業員を教育するための必須トレーニングの開発
正解: (正解を表示します)

質問: **9**
ある会社は、コンピューターベースの製造が12時間連続して機能しない場合、機器の保守にかかる費用よりも多くのお金を失うことになると判断しました。正の総所有コストを維持するには、次のうちどれが12時間未満でなければなりませんか？
A. MTBF
B. MTTR
C. RPO
D. RTO
正解: (正解を表示します)

質問: **10**
ソフトウェア会社の最終的なソフトウェアリリースに脆弱なコードが不正に含まれている可能性が最も高いのは、次のうちどれですか？　2つ選択してください。）
A. 古いマルウェア対策ソフトウェア
B. ベンダー/サプライチェーン
C. 侵入テストユーティリティの使用
D. 含まれているサードパーティライブラリ
E. 弱いパスワード
F. 安全でないプロトコル
正解: (正解を表示します)

質問: **11**
セキュリティ研究者は、機密性の高いユーザーデータがWebサイトで販売されていることが判明したことを組織に警告しました。

影響を受ける当事者に通知するために組織が使用する必要があるのは次のうちどれですか？
A. コミュニケーション計画
B. インシデント対応計画
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: **12**
アナリストは、サーバーにパッチが適用されておらず、外部のアクターがポート139でデータを盗み出したと判断しました。アナリストは、インシデントをどのように防止できたかを最もよく確認するために、次のソースのどれを確認する必要がありますか？
A. セキュリティログ
B. イベントの相関関係
C. ベースラインレポート
D. 脆弱性スキャン出力
正解: **(**正解を表示します**)**

質問: **13**
セキュリティエンジニアは、企業のモバイルデバイスポリシーに準拠するMDMソリューションを実装する必要があります。ポリシーでは、モバイルユーザーがデバイス上の企業リソースにアクセスするには、次の要件を満たす必要があると規定されています。
*モバイルデバイスOSは最新リリースにパッチを適用する必要があります
*画面ロックを有効にする必要があります（パスコードまたは生体認証）
*デバイスの紛失または盗難が報告された場合は、企業データを削除する必要があります。セキュリティエンジニアが構成する必要があるコントロールは次のうちどれですか。（2つ選択してください）
A. リモートワイプ
B. ストレージセグメンテーション
C. 姿勢
D. ジオフェンス
E. フルデバイス暗号化
F. コンテナ化
正解: **(**正解を表示します**)**

質問: **14**
最高セキュリティ責任者（CSO）は、組織と第三者の間で電子メールを介して交換される機密情報の量と整合性について懸念しています。CSOは、2つの組織間で転送中の情報を傍受している無許可の当事者を特に懸念しています。次のうちどれがCSOの懸念に対処しますか？
A. SPF
B. TLS

C. SSL
D. DMARC
E. DKIM
正解: (正解を表示します)

質問: **15**
新興企業は、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。プラットフォームにセキュリティ、管理性、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. CASB
B. SIEM
C. DLP
D. SWG
正解: (正解を表示します)

質問: **16**
大学のIT部門は、教授がセキュリティ制御を回避するために大学のネットワークにサーバーを配置することを懸念しています。次のBESTのうち、このタイプの脅威を表すものはどれですか？
A. ハクティビズム
B. ホワイトハット
C. シャドーIT
D. スクリプトキディ
正解: (正解を表示します)

質問: **17**
最近、eコマース会社のWebサイトでいくつかの大量の商品が購入されました。各トランザクションの合計は負の値であり、顧客のアカウントにクレジットが発生しました。将来同様の状況を防ぐために、次のうちどれを実装する必要がありますか？
A. 加算される可能性のあるすべての値を計算し、コードで適切な整数が使用されていることを確認します。
B. 非常に短い期間内に送信されたトランザクションが処理されないようにしてください。

C. セッションリプレイ攻撃を探してブロックするようにWebアプリケーションファイアウォールを構成します。
D. 無効な文字や値の使用を防ぐために、入力の検証が行われていることを確認してください。
正解: **D** (コメントを発表する)

質問: **18**
企業は、電子メールやエンタープライズアプリケーションへのアクセスを許可するために、ユーザーにモバイルデバイスを提供しています。同社は最近、ユーザーがいくつかの異なるベンダーやデバイスモデルから選択できるようにしました。MDMを構成する場合、この異種デバイスアプローチのセキュリティへの重要な影響は次のうちどれですか。
A. 特定のデバイスは本質的に他のデバイスよりも安全性が低いため、デバイスベンダー間の差異に対処するために補償的な制御が必要になります。
B. 最も一般的なMDM構成のセットは、エンタープライズモバイルセキュリティコントロールの効果的なセットになります。
C. すべてのデバイスがSCEPベースの登録をサポートする必要があります。したがって、選択したアーキテクチャの異質性により、秘密鍵が攻撃者に不必要に公開される可能性があります。
D. MDMは通常、異種の展開環境をサポートしないため、複数のMDMをインストールして構成する必要があります。
正解: (正解を表示します)

質問: **19**
次のうち、内部からハイパーバイザーをターゲットにするコードの機能について説明しているのはどれですか
A. フォグコンピューティング
B. コンテナブレイクアウト
C. 画像の偽造
D. ソフトウェア定義ネットワーク
E. VMエスケープ
正解: (正解を表示します)

質問: **20**
ある会社が最近、機密性の高いビデオをオンプレミス間で移動しました。会社所有のウェブサイト。その後、同社はビデオがアップロードされ、インターネットに共有されたことを知りました。次のうち、会社が原因を見つけることを最も可能性が高いのはどれですか？
A. ボラティリティのオーダー
B. 監査権条項
C. 透かし
D. ログ分析
E. チェックサム
正解: **D** (コメントを発表する)

質問: **21**
法医学捜査官は、会社のWebサイトで報告された不正な支払いの数を調べています。一部の異常なログエントリは、ユーザーが不要なメーリングリストの電子メールを受信し、リンクをクリックして登録解除を試みたことを示しています。ユーザーの1人が電子メールをフィッシングチームに報告し、転送された電子メールは次のリンクを明らかにしました。
フォレンジック調査員が最も発生したと判断する可能性が高いのは、次のうちどれですか？
A. XSRF
B. CSRF
C. XSS
D. SQLインジェクション
正解: **B (**コメントを発表する**)**

質問: **22**
@movable mediaのコストとデータ転送のセキュリティリスクは、研究室にとっては高すぎるものになっています。研究所は、データ転送をより簡単かつ安全にするために、パートナー研究所と相互接続することを決定しました。最高セキュリティ責任者（CSO）は、相互接続が確立されると、専有データが公開されることについていくつかの懸念を抱いています。ネットワーク管理者は、パートナーラボのユーザーへの不要なデータの漏洩を防ぐために、次のセキュリティ機能のどれを実装する必要がありますか？
A. データ転送エージェントのみがネットワーク間でデータを移動できるようにするNAC
B. 外部向けゾーンのファイル転送サーバーを使用したVLANゾーニング
C. ネットワーク間のファイル転送を防ぐためにホスト上で実行されているDLP
D. ActiveDirectoryを介した完全なトンネリングとNAS認証を備えたVPN
正解: **(**正解を表示します**)**

質問: **23**
ある会社が、最適な環境温度になるように新しいデータセンターのレイアウトを設計しています。次のうちどれを含める必要がありますか？ （2つ選択してください）
A. IoTサーモスタット
B. コールドアイル
C. 湿度モニター
D. ホットアイル
E. 取り外し可能なドア
F. エアギャップ
正解: **(**正解を表示します**)**

質問: **24**
コストとオーバーヘッドを削減するために、組織はオンプレミスの電子メールソリューションからクラウドベースの電子メールソリューションに移行したいと考えています。現時点では、他の

サービスは移動しません。次のクラウドモデルのうち、組織のニーズに最適なものはどれですか？
A. SaaS
B. MaaS
C. PaaS
D. laaS
正解: **C** (コメントを発表する)

質問: **25**
原子力発電所は最近の攻撃の犠牲者であり、すべてのネットワークはエアギャップされていました。その後の調査で、問題の原因としてワームが明らかになりました。次のベストのうち、何が起こったのかを説明しているのはどれですか？
A. HVACはメンテナンスベンダーに接続されていました。
B. ICSファームウェアが古くなっていました
C. ローカルマシンにRATがインストールされています。
D. 無防備な従業員によって悪意のあるUSBが導入されました。
正解: **D** (コメントを発表する)

質問: **26**
次の環境のうち、エンドユーザーの混乱を最小限に抑え、コードの最終バージョンを使用してデータベースの移行や主要なシステム変更の影響を評価するために使用される可能性が最も高いのはどれですか？
A. 生産
B. 開発
C. テスト
D. ステージング
正解: (正解を表示します)

質問: **27**
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って組織のセキュリティプログラムの有効性をテストすることに専念している人々のチームはどれですか？
A. レッドチーム
B. ブルーチーム
C. チーム中
D. パープルチーム
正解: (正解を表示します)

質問: **28**
次のアルゴリズムのうち、キーサイズが最も小さいものはどれですか？
A. AES

B. RSA
C. DES
D. Twofish
正解: (正解を表示します)

質問: **29**
企業は、ネットワークとアプリケーションの侵入テストを実施するために外部のセキュリティ会社を雇っています。会社には、アプリケーションの顧客が利用できるドキュメントのみが提供されています。次のBESTのうち、発生するテストのタイプを表すものはどれですか？
A. グレーボックス
B. ブラックボックス
C. ホワイトボックス
D. バグバウンティ
正解: (正解を表示します)

質問: **30**
LoTデバイスで自動化を実装する場合、ネットワークを安全に保つために最初に考慮すべきものは次のうちどれですか？
A. 2波の互換性
B. ネットワーク範囲
C. 通信プロトコル
D. Zigbee構成
正解: (正解を表示します)

質問: **31**
各当事者の責任を定義し、主要な成果物の概要を示し、第三者のリスクを管理するための違反に対する罰金を含めるために、組織間で確立するのに最適なのは次のうちどれですか？
A. BPA
B. SLA
C. ARO
D. 覚書
正解: (正解を表示します)

質問: **32**
セキュリティ管理者は、サーバーがさまざまな攻撃に対して脆弱であるかどうかを判断しようとしています。ツールを使用した後、管理者は次の出力を取得します。

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s0fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```


出力に基づいて、次の攻撃のどれが正常に実装されましたか？
A. ディレクトリトラバーサル
B. SQLインジェクション
C. 競合状態
D. メモリリーク
正解: **(**正解を表示します**)**

質問: **33**
ある会社は最近、自社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設定しました。同社は、セキュリティ基準への準拠を必要とする支払い用の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。eコマース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、会社が準拠しなければならない基準は次のうちどれですか？
A. PCI DSS
B. NIST CSF
C. ISO 27001
D. ISO 22301
正解: **(**正解を表示します**)**

質問: **34**
セキュリティアナリストが脆弱性スキャンを実行して、疑わしいセキュリティ齧歯動物の間に欠落しているパッチをチェックしています。応答プロセスの次のフェーズのうち、このアクティビティが最も発生する可能性が高いのはどれですか。
A. 回復
B. 準備
C. 封じ込め
D. 識別
正解: **B (**コメントを発表する**)**

質問: **35**
現在、セキュリティ管理者は、レポートの生成、フィッシング調査、ユーザーのプロビジョニングとプロビジョニング解除などの一般的なセキュリティタスクに多くの時間を費やしています。これにより、管理者は他のセキュリティプロジェクトに時間を費やすことができなくなります。この企業には、スタッフを追加する予算がありません。管理者は次のうちどれを実装する必要がありますか？
A. SCAP
B. DAC
C. SOAR
D. ABAC
正解: **(**正解を表示します**)**

質問: **36**
最高セキュリティ責任者（CSO）は、顧客が一般的に使用されるファイル共有サービスで社内の機密ファイルにアクセスできることを通知されました。ファイル共有サービスは、承認されたサードパーティアプリケーションの1つとして会社のスタッフが使用するものと同じです。
さらに調査した後、セキュリティチーム
機密ファイルの共有が偶発的であり、悪意のないものであると判断します。ただし、CSOは、このタイプのインシデントの再発を最小限に抑えるための変更を実装したいと考えていますが、既存のビジネスプロセスに影響を与えたくはありません。次のうち、CSOの目的を最もよく満たすのはどれですか？
A. CASB
B. 仮想ネットワークのセグメンテーション
C. コンテナのセキュリティ
D. DLP
E. SWG
正解: **(**正解を表示します**)**

質問: **37**
セキュリティ管理者が企業のワイヤレスネットワークを分析しています。ネットワークには、チャネル1と11で実行されている2つのアクセスポイントしかありません。airodump-ngを使用している間。管理者は、他のアクセスポイントが、使用可能なすべてのチャネルで同じ企業ESSIDを使用し、正当なアクセスポートの1つの同じBSSIDを使用して実行されていることに気付きます。
A. ジャミング
B. 邪悪な双子
C. 分離
D. 不正なアクセスポイント
E. 中間者
正解: **(**正解を表示します**)**

質問: **38**
次のうちどれが侵入者を阻止するための最良の物理的セキュリティ対策を提供しますか？ 2つ選択してください。）
A. フェンシング
B. アラーム
C. マントラップ
D. センサー
E. サイネージ
F. 照明
正解: **(**正解を表示します**)**

質問: **39**
会社のヘルプデスクは、Mimikatzがリモートシステムで実行しようとしたことを示すいくつかのAVアラートを受信しました。何人かのユーザーはまた、休憩室で拾った新会社のフラッシュドライブには512KBのストレージしかないことを報告しました。次のうちどれが原因である可能性が最も高いですか？
A. 新しいフラッシュドライブが正しくパーティション化されておらず、システムは承認されていないアプリケーションを使用してドライブを再パーティション化しようと自動的に試みています。
B. 新しいフラッシュドライブには、フラッシュドライブがアプリケーションの許可リストにないため、AVソフトウェアによってブロックされているドライバーが必要です。これにより、ドライブは一時的に512KBのストレージに制限されます。
C. GPOは、フラッシュドライブの使用を防止します。これにより、誤検知のAV表示がトリガーされ、ドライブは512KBのストレージのみに制限されます。
D. フラッシュドライブをブロックしているGPOは、メモリからプレーンテキストのクレデンシャルを取得しようとしている悪意のあるフラッシュドライブによってバイパスされています。
正解: **D (**コメントを発表する**)**

質問: **40**
組織はすべてのトラフィックをVPN経由でルーティングします。ほとんどのユーザーはリモートで、機密情報を格納する企業データセンターに接続します。インターネットの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、データセンター自体が続きます。次のうち、最も弱いデザイン要素はどれですか？
A. 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
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与える可能性があります
C. DLPアプライアンスはNGFWに統合する必要があります。
D. 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可能性があります
正解: **A (**コメントを発表する**)**

質問: **41**
システムアナリストは、新しいデジタルフォレンジックのCoCフォームを生成する責任があります。アナリストがこのドキュメントに含める必要があるのは次のうちどれですか。 2つ選択してください)。
A. 日時
B. ベンダーの名前
C. ボラティリティの順序
D. 警告バナー
E. チェックサム
F. アーティファクトの場所
正解: **A,C (**コメントを発表する**)**

質問: **42**
脆弱性評価レポートには、発見された脆弱性のCVSSスコアが含まれます。これは、スコアによって組織が改善できるためです。
A. 脆弱性データベースで適切な緩和手法を調査する
B. 侵入テストを通じて組織のネットワークに脆弱性が存在することを検証します
C. 考えられる影響に基づいて、脆弱性の修正に優先順位を付けます。
D. 脆弱性を軽減するために必要なソフトウェアパッチを見つける
正解: **C (**コメントを発表する**)**

質問: **43**
中小企業は、攻撃者から復号化キーを購入することにより、ファイルサーバーに対するランサムウェア攻撃から回復したばかりです。この問題はフィッシングメールによって引き起こされたものであり、IT管理者はそれが二度と起こらないようにしたいと考えています。IT管理者が回復後に最初に行うべきことは次のうちどれですか？
A. すべてのワークステーションを再構築し、新しいウイルス対策ソフトウェアをインストールします
B. NASをスキャンして、残存するマルウェアまたは休止状態のマルウェアを探し、頻繁にテストされる新しい毎日のバックアップを作成します
C. 管理者権限を制限し、すべてのシステムとアプリケーションにパッチを適用します。
D. アプリケーションのホワイトリストを実装し、ユーザーアプリケーションの強化を実行します
正解: **(**正解を表示します**)**

質問: **44**
データセットを担当するマネージャーは、セキュリティエンジニアに、ハードディスク上のデータに暗号化を適用するように依頼しました。セキュリティエンジニアは次の例です。
A. データ管理者。
B. データプロセッサ

C. データコントローラー。
D. データ所有者
正解: **B** (コメントを発表する)

質問: **45**
次のインシデント対応ステップのうち、業務を維持しながら重要なシステムを保護するためのアクションを伴うものはどれですか？
A. 回復
B. 封じ込め
C. 学んだ教訓
D. 調査
正解: **B** (コメントを発表する)

質問: **46**
ネットワーク技術者がコーヒーショップにゲストワイヤレスネットワークを設置しています。顧客がアイテムを購入すると、ワイヤレスネットワークのパスワードが最近印刷され、顧客がログインできるようになります。技術者が最も高いレベルのセキュリティを最小限のオーバーヘッドで提供するように構成する可能性が最も高いのは次のうちどれですか。
A. WPS-PIN
B. WPA-PSK
C. WEP-TKIP
D. WPA-EAP
正解: (正解を表示します)

質問: **47**
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次のうちどれですか？
A. 内部脅威
B. 保護されていないルートアカウント
C. 共有テナンシー
D. ゼロデイ
正解: **C** (コメントを発表する)

質問: **48**
セキュリティアナリストLinuxワークステーションを強化しており、安全なログインのために公開鍵がリモートシステムに転送されていることを確認する必要がありますこれらの要件を満たすために、アナリストは次のどの手順を実行する必要がありますか？ 2つ選択してください)。
A. ash-iを使用してキーを転送します。
B. openssl-sを使用してキーを転送します。
C. ssh-copy-idを使用してキーを転送します。
D. scpを使用してキーを転送します。
E. ssh-keygerを使用してキーを転送します。
正解: **(**正解を表示します**)**

質問: **49**
セキュリティアナリストがインシデントを調査して、攻撃者が侵入先のラップトップで何ができたかを判断しています。アナリストは、次のSIEMログを確認します。
ラップトップを危険にさらすために使用された方法を説明しているのは次のうちどれですか？
A. 攻撃者はOutlookユーザープロファイルからユーザー資格情報を正常にフィッシングできました
B. 攻撃者は、パスザハッシュ攻撃を使用してPC1からPC2に横方向に移動することができました
C. 攻撃者は、マルウェアをCAasdf234フォルダーにインストールし、それを使用して管理者の夜をゲームし、Outlookを起動することができました。
D. 攻撃者は、ファイルにPowerShellが埋め込まれたスプレッドシートの添付ファイルを電子メールで送信することにより、アプリケーションのホワイトリストを回避できました。
正解: **(**正解を表示します**)**

質問: **50**
次のうち、アプリケーションパッチを展開するための最良のアプローチを説明しているのはどれですか？
A. ステージング環境でパッチをテストし、開発環境でパッチに対して開発してから、本番システムに適用します。
B. テスト環境でパッチをテストし、それらを本番システムに適用してから、ステージング環境に適用します。
C. 本番システムにパッチを適用し、ステージング環境でパッチを適用してから、テスト環境ですべてをテストします。
D. パッチをテスト環境のシステムに適用し、次にステージング環境のシステムに適用し、最後に本番システムに適用します。
正解: **D (**コメントを発表する**)**

質問: **51**
次のうち、データ所有者とデータ管理者の違いを最もよく説明しているのはどれですか？

A. データ所有者はデータを管理する責任があり、データ管理者はデータを処理する際の管理過程を維持する責任があります。
B. データ所有者はデータの使用方法を決定する責任があり、データ管理者はデータの保護を実装する責任があります
C. データ所有者はデータの使用規則を順守する責任があり、データ管理者はデータに関するコーポレートガバナンスを決定する責任があります。
D. データ所有者はデータアクセスの技術的権限を付与し、データ管理者はデータへのデータベースアクセス制御を維持します
正解: **B** (コメントを発表する)

質問: **52**
保険会社の最高財務責任者 (CFO) は、会社の最高経営責任者 (CEO) であるアンからアカウントへの10,000ドルの送金を要求する電子メールを受け取りました。メールには、アンが休暇中で、現金とクレジットカードが入った財布をなくしたことが記載されています。攻撃者が使用しているソーシャルエンジニアリング手法は次のうちどれですか？
A. ファーミング
B. 捕鯨
C. タイプミスのしゃがみ
D. フィッシング
正解: **B** (コメントを発表する)

質問: **53**
ランサムウェア攻撃の後、フォレンジック会社は被害者と攻撃者の間の暗号通貨取引を確認する必要があります。この取引を追跡するために、会社が最も検討する可能性が高いのは次のうちどれですか？
A. NetFlowデータ
B. パブリックレジャー
C. チェックサム
D. イベントログ
正解: (正解を表示します)

質問: **54**
金融アナリストは、クライアントからの機密情報を含む電子メールを期待しています。電子メールが到着すると、アナリストはエラーを受け取り、暗号化されたメッセージを開くことができません。この問題の原因として最も可能性が高いのは次のうちどれですか？
A. S / MMEプラグインが有効になっていません。
B. セキュアIMAPは実装されていません
C. POP3Sはサポートされていません。
D. SLL証明書の有効期限が切れています。
正解: (正解を表示します)

質問: **55**
次のリスク管理戦略のうち、サイバーセキュリティ保険が使用されるのはどれですか？
A. 緩和策
B. 転移
C. 受け入れ
D. 回避
正解: **B** (コメントを発表する)

質問: **56**
サイバー攻撃を開始する前に受動的に情報を収集するプロセスは、次のように呼ばれます。
A. テールゲーティング
B. 先頭に追加
C. ファーミング
D. 偵察
正解: (正解を表示します)

質問: **57**
単一のVMが同じハイパーバイザー上の別のVMによって侵害される影響を軽減するために、管理者は技術的な制御を利用してトラフィックをさらに分離したいと考えています。次のソリューションのうち、この目的を最もよく達成するのはどれですか？
A. ゼロトラストポリシーを実装し、ハイパーバイザーサーバーを物理的に分離します。
B. 公開されたVMまたは脆弱なVMをDMZに移動します。
C. ハイパーバイザーファイアウォールをインストールして、東西のトラフィックをフィルタリングします。
D. ハイパーバイザーネットワークスイッチにVLANを追加します。
正解: **D** (コメントを発表する)

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くなっていることを警告されています。管理者は、ルーティングまたはDNSの問題ではないと判断した後、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。
次のうち、ルーターで発生しているのはどれですか？
A. リソースの枯渇
B. DDoS攻撃
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**

セキュリティアナリストが、デフォルトのファイル権限が誤って設定されている脆弱性を調査しています。同社は、脆弱性管理に資格のないスキャンを使用しています。
アナリストが権限を確認するために使用できるツールは次のうちどれですか？
A. chmod
B. nc
C. 1秒
D. setuid
E. ssh
F. nessus
正解: **(**正解を表示します**)**

質問: **60**
次のうち、データ管理者とデータ処理者の役割と責任を概説する可能性が最も高いのはどれですか？
A. GDPR
B. ISO 31000
C. PCI DSS
D. SSAE SOC 2
正解: **(**正解を表示します**)**

質問: **61**
セキュリティエンジニアは、会社のサーバーに対して最近攻撃を実行した脅威インテリジェンスソースから次の出力を取得しました。
この種の攻撃を最もよく表しているのは次のうちどれですか？
A. API
B. 偽造を要求する
C. ディレクトリトラバーサル
D. SQLインジェクション
正解: **(**正解を表示します**)**

質問: **62**
セキュリティアナリストは、Webログを確認しているときに、次のログ出力を確認します。

この攻撃が成功するのを防ぐには、次の緩和戦略のどれが最善でしょうか？
A. コード署名
B. ストアドプロシージャ
C. 入力検証
D. 安全なCookie
正解: **(**正解を表示します**)**

質問: **63**
全国的な企業が1日中いつでも不正ログインを経験しています。ログインは、会社に従業員がいない国から発信されているようです。次のコントロールのどれ。
会社はIAM戦略の一部として使用することを検討する必要がありますか？　2つ選択してください）。
A. ジオフェンス
B. 複雑なパスワードポリシー
C. セルフサービスパスワードのリセット
D. ジオロケーション
E. 不可能な旅行ポリシー
F. 時間ベースのログイン
正解: **(**正解を表示します**)**

質問: **64**
ホストがマルウェアに感染しました。インシデント対応中に、ユーザーのジョーは、リンクが記載された電子メールを受信しなかったと報告しましたが、彼は一日中インターネットを閲覧していました。次のうち、マルウェアがどこで発生したかを示す可能性が最も高いのはどれですか？
A. DNSログ
B. SNMPログ
C. SIPトラフィックログ
D. Webサーバーのログ
正解: **(**正解を表示します**)**

質問: **65**
最近のセキュリティ評価では、攻撃者が組織内の脆弱なワークステーションを悪用し、ネットワーク上で数か月間存続していることが明らかになりました。組織は、セキュリティを再評価する必要性を認識しています。
境界内のリスクを軽減するための戦略次のソリューションのうち、組織の戦略を最もよくサポートするのはどれですか？
A. EDR
B. DLP
C. UTM
D. FIM

正解: **(**正解を表示します**)**

質問: **66**
組織は、国境の入口および出口ポートで使用するための認証サービスを開発しています。このサービスは、パスポートシステムから取得したデータフィード、乗客マニフェスト、および港にあるCCTVシステムからの高解像度ビデオフィードを使用します。このサービスには機械学習技術が組み込まれており、生体認証の登録プロセスを排除すると同時に、当局が時間の経過とともにより正確に乗客を識別できるようにします。乗客が頻繁に旅行するほど、サービスは乗客をより正確に識別します。次のバイオメトリクスのうち、登録を必要とせずに使用される可能性が最も高いのはどれですか？　2つ選択してください。）
A. フェイシャル
B. 網膜
C. 歩行
D. 声
E. 指紋
F. 静脈
正解: **A,C (**コメントを発表する**)**

質問: **67**
Webサイトの開発者は、新しいeコマースWebサイトに取り組んでおり、情報セキュリティの専門家に、クレジットカード番号を保存して簡単な再注文プロセスを作成するための最も適切な方法を求めています。次の方法のうち、この目標を最もよく達成するのはどれですか？
A. データベース内のクレジットカードをトークン化する
B. 入力時にクレジットカード番号をハッシュします。
C. 磁気ストライプ情報の塩漬け
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: **68**
数十のシステムに影響を及ぼしているインシデントには、ルールと更新のためにインターネットサービスに到達するマルウェアが含まれます。インターネットホストのIPアドレスは、それぞれの場合で異なるように見えます。組織は、対応と復旧のアクションをサポートするための共通のIoCを決定したいと考えています。次の情報源のうち、このソリューションを最もよくサポートするのはどれですか？
A. ブラウザキャッシュ
B. アンチウイルス
C. DNSクエリログ
D. Webログファイル
正解: **C (**コメントを発表する**)**

質問: **69**
業界見本に参加した翌日、数人の従業員が職場に復帰します。その同じ日に、セキュリティマネージャは、従業員の各ワークステーションから送信されるいくつかのマルウェアアラートに気づきます。セキュリティマネージャは調査しますが、境界ファイアウォールまたはNIDSへの攻撃の兆候は見つかりません。次のうち、マルウェアアラートを引き起こす可能性が最も高いのはどれですか？
A. プレゼンテーションメディアによって開始された、イントラネット全体に伝播したワーム
B. 攻撃を実行しようとしているvCardに含まれているファイルレスウイルス
C. 悪意のあるコードを実行しようとしているが、ホストファイアウォールによってブロックされているUSBフラッシュドライブ
D. ホスト上で悪意のあるコードを通過して実行したトロイの木馬
正解: **(**正解を表示します**)**

質問: **70**
組織は定期的にインフラストラクチャをスキャンしてセキュリティパッチが欠落していないかどうかを確認しますが、ハッカーがスキャナーのアカウントにアクセスすることを懸念しています。このリスクを最小限に抑えるには、次のうちどれが最適ですか？
A. リスクの高いサーバーに対して非クレデンシャルスキャンを使用します。
B. 90日ごとに更新される複雑な8文字のパスワードが必要です。
C. 異常なスキャナーアカウントのログオン時間にログを記録して警告します。
D. ワークステーションの非侵入型スキャンのみを実行します。
正解: **C (**コメントを発表する**)**

質問: **71**
オフラインの政府施設のセキュリティエンジニアは、SSL証明書の有効性を懸念しています。エンジニアは、証明書が取り消されているかどうかを判断するために、最小の遅延で最速のチェックを実行したいと考えています。次のうちどれがこれらの要件に最適ですか？
A. RA
B. CSR
C. CRL
D. OCSP
正解: **(**正解を表示します**)**

質問: **72**
セキュリティ運用アナリストは、会社のSIEMソリューションを使用してアラートを相互に関連付けています。インシデント対応プロセスの次のどの段階がこの例ですか？
A. 根絶
B. 識別
C. 回復
D. 準備

正解: **B** (コメントを発表する)

質問: **73**
脆弱性評価レポートには、発見された脆弱性のCVSSスコアが含まれます。これは、スコアによって組織が改善できるためです。
A. 考えられる影響に基づいて、脆弱性の修正に優先順位を付けます。
B. 侵入テストを通じて組織のネットワークに脆弱性が存在することを検証します
C. 脆弱性を軽減するために必要なソフトウェアパッチを見つける
D. 脆弱性データベースで適切な緩和手法を調査する
正解: (正解を表示します)

質問: **74**
次のうち、投票機の整合性をサポートする可能性が最も高いのはどれですか？
A. 完全転送秘密
B. トランスポート層のセキュリティ
C. 非対称暗号化
D. ブロックチェーン
正解: (正解を表示します)

質問: **75**
職場全体の製造会社で、電子メールアカウントが侵害されています。ある事件では、ユーザーがフランスの本社からログインしましたが、数秒後、同じユーザーアカウントがブラジルからのログインを試みました。次のアカウントポリシーのうち、このタイプの攻撃を最もよく防ぐのはどれですか？
A. ジオフェンス
B. 不可能な移動時間
C. ジオロケーション
D. ネットワークの場所
正解: (正解を表示します)

質問: **76**
会社は、Tier0およびTier1システムへの管理者特権を必要とするすべての作業に特別に構成されたワークステーションを使用します。同社は厳格なプロセスに従って、納品後すぐにシステムを強化します。これらの厳格なセキュリティ対策を講じていても、ワークステーションの1つからインシデントが発生しました。根本的な原因は、SoCが改ざんまたは交換されたことにあるようです。次のうち、最も発生した可能性が高いのはどれですか？
A. ダウングレード攻撃
B. 論理爆弾
C. ファイルレスマルウェア
D. BIOSの構成が間違っています

E. サプライチェーン攻撃
正解: (正解を表示します)

質問: **77**
エンドユーザーは、コンピューターの動作が数週間通常よりも遅いと報告しています。調査中に、アナリストは、システムがユーザーの電子メールアドレスと10桁の番号を1日1回IPアドレスに送信していると判断しました。ユーザーのコンピューターに関する最近のログエントリは次のとおりです。
この問題の原因として最も可能性が高いのは次のうちどれですか？
A. ランサムウェアはコマンドアンドコントロールサーバーと通信しています。
B. エンドユーザーがWebブラウザからPUPを購入してインストールしました
C. ハッカーが機密データを盗み出そうとしています
D. コンピューター上のボットがWebサイトに対してブルートフォースパスワードを実行しています
正解: (正解を表示します)

質問: **78**
エンジニアは、企業所有のモバイルデバイスから機密データにアクセスしたいと考えています。個人データはデバイス上で許可されていません。エンジニアが出張する際に考慮しなければならないMDM構成は次のうちどれですか？
A. アプリケーション管理
B. コンテナ化
C. ジオフェンス
D. 画面ロック
正解: (正解を表示します)

質問: **79**
次のうち、実際のデータのサブセットを利用し、システムの特徴と機能、および定義されたテストケースに対してエンドユーザーの観点からシステムがどのように相互作用または実行するかを評価するために使用される可能性が最も高いのはどれですか？ 2つ選択してください)。
A. テスト
B. 生産

C. SDLC
D. PoC
E. 研究開発
F. UAT
正解: **(**正解を表示します**)**

質問: **80**
セキュリティ評価中に、セキュリティは過度に許容的なアクセス許可を持つファイルを見つけます。次のツールのうち、アナリストが既存のユーザーとグループの権限を減らし、ファイルからset-user-IDを削除できるようにするのはどれですか？
A. setuid
B. chmod
C. 1a
D. leof
E. chflags
正解: **D (**コメントを発表する**)**

質問: **81**
セキュリティ監査人は、内部セキュリティチームから提供された脆弱性スキャンデータを確認しています。次のBESTのうち、有効な資格情報が使用されたことを示すものはどれですか？
A. スキャン結果には、ターゲットホストで公開されている開いているポート、プロトコル、およびサービスが表示されます
B. インストールされたプログラムのソフトウェアバージョンを列挙したスキャン
C. スキャンにより、ターゲットホストの脆弱性のリストが生成されました
D. スキャンにより、期限切れのSSL証明書が特定されました
正解: **B (**コメントを発表する**)**

質問: **82**
次の状況のうち、緩和のために探偵制御タイプを使用するのが最善でしょうか？
A. ある会社がIPSシステムを購入しましたが、要件を確認した後、アプライアンスはトラフィックをブロックするのではなく、監視することになりました。
B. ある会社がネットワークロードバランサーを実装して、Webアプリケーションの99.999%の可用性を確保しました。
C. ある会社が、経理部門と情報技術部門の間のトラフィックを分離するために、アプリケーションレベルのファイアウォールを購入しました。
D. ある会社がすべての資本資産の洪水防御のために賠償責任保険を購入しました。
E. ある会社は、自然災害が発生した場合にサービスを復元する可能性を高めるためのバックアップソリューションを設計しました。
正解: **A (**コメントを発表する**)**

質問: **83**
攻撃者は、利用可能なパッチがない脆弱性を悪用しています。攻撃者が悪用しているのは次のうちどれですか？
A. 安全でないルートアカウント
B. デフォルトの権限
C. 弱い暗号化
D. ゼロデイ
正解: **D (**コメントを発表する**)**

質問: **84**
洪水地帯にある組織は、IT運用の復旧に関連する懸念を次のように文書化する可能性が最も高いです。
A. コミュニケーション計画。
B. 事業継続計画
C. 運用計画の継続性
D. 災害復旧計画。
正解: **D (**コメントを発表する**)**

質問: **85**
WindowsシステムのSMBプロトコルに新しい脆弱性が最近発見されましたが、現在、この問題を解決するためのパッチはありません。セキュリティ管理者は、会社のDMZ内のサーバーが外部からの攻撃に対して脆弱になることを懸念しています。ただし、SMBはLAN上の多数の内部システムおよびアプリケーションによって使用されるため、管理者はサーバー上のサービスを無効にすることはできません。DMZへのすべての外部インバウンド接続に対して、次のTCPポートのどれをブロックして、サーバー？　2つ選択してください）。
A. 443
B. 161
C. 445
D. 143
E. 139
F. 135
正解: **(**正解を表示します**)**

質問: **86**
最高経営責任者（CEO）の個人情報がソーシャルエンジニアリング攻撃で盗まれました。次の情報源のうち、CEOの個人情報が売りに出されているかどうかを明らかにするのはどれですか？
A. 自動化された情報共有
B. オープンソースインテリジェンス
C. ダークウェブ
D. 脆弱性データベース

正解: **(**正解を表示します**)**

質問: **87**
新しく設置されたインターネットアクセス可能な4K監視カメラに関して最高情報セキュリティ責任者（CISO）が最も懸念するのは、次のうちどれですか？
A. タイムリーにパッチを適用しないと、カメラが危険にさらされる可能性があります。
B. 施設の物理的セキュリティでは、カメラを盗難から保護できない場合があります。
C. すべての施設を100%監視できないと、会社が不必要なリスクにさらされる可能性があります。
D. エクスポートされたビデオは、ファイルサーバー上で過剰なスペースを占める可能性があります。
正解: **(**正解を表示します**)**

質問: **88**
以下は、マルウェアの実行の発生を減らすために最も効果的な管理制御です。
A. 変更管理手順
B. NIDS更新の頻度
C. セキュリティ意識向上トレーニング
D. EDRレポートサイクル
正解: **C (**コメントを発表する**)**

質問: **89**
ユーザーがヘルプデスクに連絡して、次のことを報告します。
2日前、企業のワイヤレスSSIDに接続した後、ポップアップブラウザウィンドウがユーザーに名前とパスワードの入力を求めました。これはこれまでに一度も起こったことはありませんでしたが、ユーザーは要求に応じて情報を入力しました。
ユーザーはインターネットにアクセスできましたが、翌日まで部門共有にアクセスできませんでした。
ユーザーは現在、銀行から不正取引に関する通知を受け取っています。
このシナリオで最も使用された可能性が高い攻撃ベクトルは次のうちどれですか？
A. DNSポイズニング
B. ARP中毒
C. 邪悪な双子
D. 不正なアクセスポイント
正解: **D (**コメントを発表する**)**

質問: **90**
SOCは、最近のインシデントの後、プロセスと手順を検討しています。このレビューでは、感染したホストの検疫が最善の行動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。マルウェアが封じ込められる前に、マルウェアが追加のホストに拡散することを許可しました。インシデント対応プロセスを改善するのに最適なのは次のうちどれですか？

A. より良い意思決定ポイントでプレイブックを更新する
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. 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
正解: **(**正解を表示します**)**

質問: **91**
Webベースの販売に影響を与えたデータセンターの長期停止に続いて、企業は業務をプライベートクラウドソリューションに移行することを決定しました。セキュリティチームは、次の要件を満たしています。
*チームがクラウドベースのサービスをどのように使用しているかを可視化する必要があります。
*会社は、支払いカードに関連するデータがいつクラウドに送信されているかを識別できる必要があります。
*エンドユーザーの地理的な場所に関係なくデータが利用可能である必要があります
*管理者は、トラフィックとトレンドを一目で確認できる必要があります。
セキュリティアナリストが推奨するのは次のうちどれですか？
A. CASBソリューションを実装します。
B. 他のクラウドサービスプロバイダーへのトラフィックを制限するファイアウォールルールを作成します。
C. Webベースのコンテンツフィルターを構成します。
D. 転送中のデータを監視するためのDLPソリューションをインストールします。
正解: **D (**コメントを発表する**)**

質問: **92**
組織がAUPを定義する理由は次のうちどれですか？
A. ITプロバイダーとコンシューマー間の可用性と信頼性の特性を定義する
B. 組織のリソースへのアクセスと使用に必要な最低レベルの特権を定義する
C. 2つの組織間の意図されたパートナーシップを定義する
D. 組織のITシステムのユーザー向けの一連のルールと動作を定義する
正解: **D (**コメントを発表する**)**

質問: **93**

セキュリティエンジニアは、次の要件を実装する必要があります。
*すべてのレイヤー2スイッチは、ActiveDirectoryのTor認証を利用する必要があります。
* Active Directoryがオフラインの場合、すべてのレイヤー2スイッチはローカルフォールバック認証を使用する必要があります。
*すべてのレイヤー2スイッチは同じではなく、複数のベンダーによって製造されています。
これらの要件を満たすためにエンジニアが取るべき行動は次のうちどれですか？ 2つ選択してください)。
A. RADIUSを実装します。
B. TACACS +を実装します
C. セカンダリログイン方式でスイッチのポートセキュリティを設定します。
D. ローカルログインをセカンダリとしてスイッチにAAAを設定します。
E. ActiveDirectoryサーバーでローカルファイアウォールを有効にします。
F. DHCPサーバーを実装します。
正解: (正解を表示します)

質問: **94**
セキュリティアナリストは、午前2時から午前4時の時間帯に外部IPアドレスと通信している複数のホストを調査しています。このマルウェアは、従来のウイルス対策ソフトウェアによる検出を回避しました。次の種類のマルウェアのうち、ホストに感染する可能性が最も高いのはどれですか？
A. ワーム
B. ランサムウェア
C. ラット
D. ポリモフィック
正解: (正解を表示します)

質問: **95**
グローバル企業では、ブルートフォース攻撃によるクレデンシャルの盗難やアカウントのロックアウトが原因で、不正なログ記録が発生しています。同社は、これらの攻撃を軽減するために、サードパーティのIDプロバイダーの実装を検討しています。次のうちどれが、会社が将来のベンダーに要求するのに最適なコントロールでしょうか？
A. IP制限
B. 複雑なパスワードポリシー
C. 多要素認証
D. 禁止されているパスワードリスト
正解: (正解を表示します)

質問: **96**

Windowsサーバーをインストールした後、サイバーセキュリティ管理者はセキュリティのベストプラクティスに従ってサーバーを強化する必要があります。次のうち、管理者の目標を達成するのはどれですか？ （2つ選択してください）。
A. サービスアカウントを無効にする
B. ゲストアカウントを無効にする
C. ネットワーク共有を有効にする
D. NetBIOS over TCP / IPを無効にする
E. LANManagerハッシュ値の保存
F. NTLMを有効にする
正解: **(**正解を表示します**)**

質問: **97**
ある会社は最近、紛失または破損した企業所有のモバイルデバイスを交換するコストのために、厳密なBYOD文化に移行しました。BYOD文化のバランスを取りながら、会社のデータを保護するのに最適なテクノロジーは次のうちどれですか？
A. リモートワイプ
B. コンテナ化
C. ジオフェンス
D. フルディスク暗号化
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、まもなく公開される新しいWebサイトを検討しています。アナリストは、URLに次の情報を表示します。
http://dev-site.comptia.org/home/show.php?sessionID=77276554
次に、アナリストは内部ユーザーにテスト目的で新しいWebサイトへのリンクを送信し、ユーザーがリンクをクリックすると、アナリストは次のURLでWebサイトを閲覧できます。
http://dev-site.comptia.org/home/show.php?sessionID=98988475
次のアプリケーション攻撃のどれがテストされていますか？
A. Cross-site request forgery
B. Session replay
C. Pass-the-hash
D. Object deference
正解: **B (**コメントを発表する**)**

質問: **99**
セキュリティアナリストは、誰かがappadminテストアカウントにログインしたというSIEMアラートを受信します。これは、攻撃の早期検出にのみ使用されます。次に、セキュリティアナリストは、次のアプリケーションログを確認します。
セキュリティアナリストは、次のうちどれを結論付けることができますか？

A. サービスアカウントのパスワードが変更された可能性があり、その結果、アプリケーション内でログインが継続的に失敗します。
B. アプリケーションに対してリプレイ攻撃が行われています。
C. ユーザー認証システムに対してインジェクション攻撃が行われています。
D. 認定された脆弱性スキャナー攻撃は、アプリケーションに対していくつかのCVEをテストしています。
正解: **(**正解を表示します**)**

質問: **100**
次のうち、Webアプリケーションの安全なコーディング手法を改善しようとしているソフトウェア開発者にとって最良のリソースはどれですか？
A. NIST CSF
B. OWASP
C. サードパーティライブラリ
D. 脆弱性スキャンの結果
正解: **(**正解を表示します**)**

質問: **101**
WindowsシステムのSMBプロトコルに新しい脆弱性が最近発見されましたが、現在、この問題を解決するためのパッチはありません。セキュリティ管理者は、会社のDMZ内のサーバーが外部からの攻撃に対して脆弱になることを懸念しています。ただし、SMBはLAN上の多くの内部システムおよびアプリケーションによって使用されるため、管理者はサーバー上のサービスを無効にすることはできません。サーバーを保護するための回避策として、DMZへのすべての外部インバウンド接続でブロックする必要があるTCPポートは次のうちどれですか？　2つ選択してください）。
A. 443
B. 161
C. 143
D. 135
E. 445
F. 139
正解: **E,F (**コメントを発表する**)**

質問: **102**
ネットワーク管理者は、組織のセキュリティ体制を改善するためにIDSをインストールするように依頼されました。次のコントロールタイプのうち、IDSはどれですか？
A. 物理的
B. 管理
C. 修正
D. 探偵

正解: **(**正解を表示します**)**

質問: **103**
ユーザーがワークステーションにログインするためのパスワードを入力すると、認証コードの入力を求められます。次のMFA要素または属性のどれが認証プロセスで利用されていますか？ 2つ選択してください)。
A. あなたが持っているもの
B. あなたが知っていること
C. あなたにできること
D. あなたは何か
E. あなたは誰か
F. どこかにいる
正解: **(**正解を表示します**)**

質問: **104**
アナリストがインターネットフォーラムにアクセスして、ツールに関する情報を探します。アナリストは、関連情報が含まれていると思われる脅威を見つけました。投稿の1つは次のように述べています。
次のうち、フォーラムの読者に対して試みられた攻撃を最もよく表しているのはどれですか？
A. XSS攻撃
B. API攻撃
C. SOU攻撃
D. DLL攻撃
正解: **A (**コメントを発表する**)**

質問: **105**
ログを確認しているときに、セキュリティエンジニアは、多くのエンドユーザーが突然ファイルをダウンロードしていることに気付きます。
.tar.gz拡張子。ファイルを詳しく調べると、それらがPE32ファイルであることがわかります。エンドユーザーは、ダウンロードを開始しなかったと述べています。さらなる調査により、エンドユーザーはすべて、1週間前にhrefリンクを含む感染したMHTファイルを含む外部の電子メールをクリックしたことが明らかになりました。次のうち、最も発生する可能性が高いのはどれですか？
A. ファイアレスウイルスがローカルネットワーク環境に拡散しています。
B. ワークステーションはコマンドアンドコントロールサーバーにビーコンを送信しています。
C. RATがインストールされ、追加のエクスプロイトツールを転送しています。
D. 論理爆弾が実行され、データ転送を担当します。
正解: **C (**コメントを発表する**)**

質問: **106**

次のうちどれがノード間でデータを分散し、ダウンタイムを最小限に抑えながらデータの操作をより困難にしますか？
A. Hybrid cloud
B. Public cloud
C. Fog computing
D. MSSP
正解: **A** (コメントを発表する)

質問: **107**
セキュリティ管理者は、異なるグローバルインスタンスとワークロード間で発生する異常なアクティビティに気づき、異常なトラフィックのソースを特定する必要があります。次のログソースのうち、異常なトラフィックのソースを示すのに最適なものはどれですか？
A. HIDS
B. CASB
C. VPC
D. UEBA
正解: (正解を表示します)

質問: **108**
ある会社が、クライアント向けに新しいインターネットプラットフォームを立ち上げています。同社は独自の承認ソリューションを実装することを望んでいませんが、代わりに別のプラットフォームによって提供される承認に依存したいと考えています。目的のソリューションを実装するための最良のアプローチは次のうちどれですか？
A. OAuth
B. TACACS +
C. RADIUS
D. SAML
正解: (正解を表示します)

質問: **109**
GDPRの下で、プライバシーとWebサイトのユーザー権利の保護に最も責任があるのは次のうちどれですか？

A. データ所有者
B. データプロセッサ
C. データ保護責任者
D. データコントローラー
正解: (正解を表示します)

質問: **110**
金融機関は、顧客の融資プロセスを支援するために、新しい安全な暗号化されたドキュメント共有アプリケーションを採用しました。この新しいプラットフォーム全体でいくつかの重要なPIIを共有する必要がありますが、DLPシステムによってブロックされています。組織のセキュリティ体制を損なうことなく、PIIを安全なアプリケーションと共有するのに最適なアクションは次のうちどれですか？
A. すべてのPIIを許可するようにDLPポリシーを構成します
B. 特定のPIIでこのアプリケーションをホワイトリストに登録するようにDLPポリシーを構成します
C. このアプリケーションで使用されるすべてのポートを許可するようにファイアウォールを構成します
D. アプリケーションを許可するようにウイルス対策ソフトウェアを構成します
E. PIIを暗号化するようにアプリケーションを構成します
正解: (正解を表示します)

質問: **111**
次のクラウドモデルのうち、クライアントにサーバー、ストレージ、ネットワークを提供しますが、それ以外は提供しませんか？
A. PaaS
B. IaaS
C. DaaS
D. SaaS
正解: (正解を表示します)

質問: **112**
組織は、日常業務を行うためにサードパーティのビデオ会議に依存しています。最近のセキュリティの変更により、すべてのリモートワーカーが企業リソースへのVPNを利用する必要があります。VPNに接続したときの遅延を最小限に抑えながら、高品質のビデオ会議を維持するのに最適なのは次のうちどれですか？
A. VPNアクセラレータでQoSを適切に構成する
B. スプリットトンネリングを利用して、企業リソースのトラフィックのみを暗号化する
C. 需要の増加に対応するために高帯域幅の接続を購入する
D. 地理的多様性を使用してVPNターミネーターをエンドユーザーに近づける
正解: (正解を表示します)

質問: **113**
セキュリティアナリストは、最近リリースされたセキュリティアドバイザリを使用して履歴ログを確認し、アドバイザリで概説されている特定のアクティビティを探しています。アナリストは次のうちどれを行っていますか？
A. 脅威ハンティング
B. パケットキャプチャ
C. 認定された脆弱性スキャン
D. ユーザー行動分析
正解: **(正解を表示します)**

質問: **114**
研究者は過去10か月間大規模なデータセットを分析してきました。研究者は他の機関の同僚と協力し、通常はSSH経由で接続して追加のデータを取得します。歴史的に、この設定は問題なく機能していましたが、研究者は最近、次のメッセージを受け取り始めました。
次のネットワーク攻撃のうち、研究者が最も経験している可能性が高いのはどれですか？
A. 邪悪な双子
B. MACクローニング
C. 中間者
D. ARP中毒
正解: **(正解を表示します)**

質問: **115**
セキュリティアナリストは、次のコマンドライン出力を確認しています。
アナリストは次のうちどれを観察していますか？
A. IGMPスプーフィング
B. URLリダイレクト
C. DNSポイズニング
D. MACアドレスのクローン作成
正解: **(正解を表示します)**

質問: **116**
次のベストのうち、事前定義された固定電話でのコールバックを必要とするMFA属性を説明しているのはどれですか？
A. あなたが知っている誰か
B. あなたが展示しているもの
C. どこかにいる
D. あなたにできること
正解: **C (コメントを発表する)**

質問: **117**
攻撃者は、オンラインシステムから無塩のパスワードハッシュをいくつか盗み出すことに成功しました。以下のログを考えると：
次のうち、攻撃者が実行しているパスワード攻撃の種類を最もよく表しているのはどれですか？
A. 辞書
B. パスワードスプレー
C. ブルートフォース
D. パスザハッシュ
正解: **A** (コメントを発表する)

質問: **118**
システム管理者は、同じX.509証明書を複数のサーバーにインストールする必要があります。管理者は次のうちどれを使用する必要がありますか？
A. キーエスクロー
B. 拡張検証証明書
C. 自己署名証明書
D. 証明書の連鎖
正解: (正解を表示します)

質問: **119**
ユーザーは、安全なコンピューターに対して認証するためにパスワードとUSBキーを導入する必要があり、認証は会社が存在する州に限定されます。次の認証概念のどれが使用されていますか？
A. あなたが知っていること、あなたが持っていること、そしてあなたがいる場所
B. あなたが持っているもの、あなたがいる場所、そしてあなたが知っている誰か
C. あなたが何か、あなたが知っている何か、そしてあなたが展示できる何か
D. あなたが知っていること、あなたができること、そしてあなたがいる場所
正解: (正解を表示します)

質問: **120**
組織は、侵入テストを実行するためにセキュリティアナリストを雇いました。アナリストは、サーバーへの1Gb相当のインバウンドネットワークトラフィックをキャプチャし、分析のためにpcapをマシンに転送します。アナリストがpcapをさらに確認するために使用する必要があるツールは、次のうちどれですか？
A. Nmap
B. Wireshark
C. cURL
D. Netcat
正解: **B** (コメントを発表する)

質問: **121**
商用のサイバー脅威インテリジェンス組織は、関係のないさまざまな顧客のIoCを監視しています。特定の脅威インテリジェンスを他の有料サブスクライバーにリリースする前に、組織は次の契約によって義務付けられている可能性が最も高いです。
A. IoCデータ内で観察されたPIIを匿名化します。
B. 観察されたデータに基づく影響評価で企業を支援します。
C. 脅威インテリジェンスレポートの使用率を追跡するためのメタデータを追加します。
D. 特定のAPTおよび国民国家のアクターへの帰属を実行します。
正解: **(**正解を表示します**)**

質問: **122**
有名な組織がAPIからの攻撃を経験しています。組織は、カスタムマルウェアが作成されて会社に電子メールで送信されたり、駐車場にドロップされたUSBスティックにインストールされたりすることを懸念しています。このシナリオに対する最善の防御策は次のうちどれですか？
A. 署名ベースのアンチウイルスioアップデートを30分ごとに構成する
B. 不明なソフトウェアのサンドボックスにアプリケーションの実行を実装します。
C. デジタル署名されていない場合の脆弱性のためのファジング新しいファイル
D. 電子メールにS / MIMEを適用し、挿入時にUSBドライブを自動的に暗号化します。
正解: **(**正解を表示します**)**

質問: **123**
アナリストが内部ネットワークで実行されている安全でないサービスを特定しようとしていますポートスキャンを実行した後、アナリストはサーバーでデフォルトのポートでいくつかの安全でないサービスが有効になっていることを特定します次のベストのどれが現在実行されているサービスと安全な代替手段を説明しますそれらを交換するために」3つ選択）
A. SNMPv2 SNMPv3
B. TLS、SSL
C. TFTP FTP
D. SFTP FTPS
E. HTTP、HTTPS
F. POP、IMAP
G. ログイン、rlogin

H. SNMPv1、SNMPv2
I. Telnet SSH
正解: **A,E,I (**コメントを発表する**)**

質問: **124**
組織の最高経営責任者（CEO）は、スタッフが営業時間中、パンデミックまたは危機時のインシデントの際にいつでも自宅で仕事ができるようにしたいと考えていますが、CEOは、一部のスタッフが休暇中のリスクの高い国からの柔軟性と仕事は、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、会社がリスクの大部分を軽減するためにいくつかの基本を実装できると信じています。CEOの懸念を緩和するのに最適なのは次のうちどれですか？（2つ選択してください）。
A. ジオロケーション
B. ジオタグ
C. トークン
D. 証明書
E. 時間帯の制限
F. 役割ベースのアクセス制御
正解: **(**正解を表示します**)**

質問: **125**
企業は、暗号化キーを安全な方法で保持する必要があります。次のネットワークアプライアンスのうち、この目標を達成できるのはどれですか？
A. TPM
B. DLP
C. HSM
D. CASB
正解: **(**正解を表示します**)**

質問: **126**
最高セキュリティ責任者（CSO）は、各営業担当者のラップトップにローカルに保存されているPIIの量を懸念しています。営業部門では、機器の紛失率が平均よりも高くなっています。次の推奨事項のうち、CSOの懸念に最もよく対処するのはどれですか？
A. すべてのハードドライブをSEDに交換します。
B. MDMソリューションを展開します。
C. 各ラップトップにDLPエージェントをインストールします。
D. マネージドFDEを実装します。
正解: **(**正解を表示します**)**

質問: **127**

セキュリティアナリストは、データリンク層セキュリティのみを使用して、ネットワークの特定のセグメントへのアクセスを制限することを推奨する必要があります。アナリストが最も推奨する可能性が高いコントロールは次のうちどれですか？
A. BPDU
B. ARP
C. ACL
D. MAC
正解: **(**正解を表示します**)**

質問: **128**
セキュリティエンジニアは、SSLを介した悪意のあるWebリクエストから会社のWebサイトを保護するためにWAFをインストールしています。目的を達成するために必要なものは次のうちどれですか？
A. スプリットトンネルVPN
B. リバースプロキシ
C. 復号化証明書
D. 負荷分散サーバー
正解: **C (**コメントを発表する**)**

質問: **129**
従業員は詐欺の罪で起訴され、企業資産を使用した疑いがあります。当局が証拠を収集し、証拠の許容性を維持するために、次の法医学的手法のどれを使用する必要がありますか？
A. CoC
B. 否認防止
C. データ回復
D. ボラティリティの順序
正解: **(**正解を表示します**)**

質問: **130**
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。次のうち、潜在的な脆弱性を特定するのに最も役立つのはどれですか？
A. nmp comptia、org -p 80 -aV
B. Nc -1 -v comptia、org -p 80
C. Hping3 -s comptia、org -p 80
D. nslookup -port = 80 comtia.org
正解: **(**正解を表示します**)**

質問: **131**
ユーザーの不便に対する許容度が低い組織は、ラップトップのハードドライブを紛失やデータの盗難から保護したいと考えています。次のうちどれが最も受け入れられるでしょうか？

A. DLP
B. SED
C. HSM
D. TPM
正解: **(**正解を表示します**)**

質問: **132**
地元のコーヒーショップは、WPA2-PSKを利用する顧客向けの小さなWiFiホットスポットを運営しています。コーヒーショップは、セキュリティのトレンドを常に把握し、WiFiをさらに安全にするためにWPA3を実装したいと考えています。コーヒーショップがPSKの代わりに使用する可能性が最も高いテクノロジーは次のうちどれですか？
A. MSCHAP
B. SAE
C. WEP
D. WPS
正解: **(**正解を表示します**)**

質問: **133**
次の一般的な使用例のうち、ステガノグラフィが採用されるのはどれですか？
A. 否認防止
B. 難読化
C. ブロックチェーン
D. 整合性
正解: **B (**コメントを発表する**)**

質問: **134**
監査人は、最後の2つの評価中に脆弱であった組み込みOSを備えたセキュリティアプライアンスの評価を実行しています。次のベストのうち、アプライアンスの脆弱な状態を説明しているのはどれですか？
A. アプライアンスには、評価のための管理者の資格情報が必要です。
B. ベンダーはアプライアンスのパッチを提供していません。
C. デバイスは弱い暗号化暗号を使用します。
D. システムは弱いデフォルトのセキュリティ設定で構成されました。
正解: **(**正解を表示します**)**

質問: **135**
多数のモバイルデバイスを所有しているAn ..は、デバイスの紛失や盗難が発生した場合に不正アクセスを管理するための強化されたセキュリティ制御を模索しています。具体的には、モバイルデバイスが建物から3マイル（4.8 km）以上離れている場合、管理チームはセキュリティチームに警

告を発し、それらのデバイスのサーバーリソースを制限する必要があります。組織は次のどのコントロールを実装する必要がありますか？
A. ジオフェンス
B. 近距離無線通信
C. GPSタグ付け
D. ロックアウト
正解: (正解を表示します)

質問: **136**
重要なシステムに対する組織のRPOは2時間です。このシステムは、月曜日から金曜日の午前9時から午後5時まで使用されます。現在、組織は毎週土曜日に完全バックアップを実行しており、完了するまでに4時間かかります。次の追加のバックアップ実装のうち、アナリストがビジネス要件を満たすための最良の方法はどれですか？
A. 月曜日から金曜日の午後6時の完全バックアップと1時間ごとの差分バックアップ。
B. 月曜日から金曜日の午後6時の増分バックアップと1時間ごとの差分バックアップ
C. 月曜日から金曜日の午後6時の増分バックアップと1時間ごとの完全バックアップ。
D. 月曜日から金曜日の午後6時の完全バックアップと、1時間ごとの増分バックアップ。
正解: (正解を表示します)

質問: **137**
組織のユーザーは、最初の適切な許可なしに、インターネットからワークステーションにプログラムをインストールしています。組織は、ユーザーが標準化されたプログラムをインストールできるポータルを維持しています。ただし、一部のユーザーは、レガシープログラムがプロパティを機能できるようにするために、ワークステーションの管理アクセス権を持っています。この問題に対処するために、セキュリティ管理者が実装を検討する必要があるのは次のうちどれですか？
A. データ損失防止
B. アプリケーションのホワイトリング
C. アプリケーションコード署名
D. Webアプリケーションファイアウォール
正解: (正解を表示します)

質問: **138**

企業は、ログを一元化してベースラインを作成し、セキュリティイベントを可視化する必要があります。次のテクノロジーのどれがこの目的を達成しますか？
A. Webアプリケーションファイアウォール
B. セキュリティ情報とイベント管理
C. 次世代ファイアウォール
D. 脆弱性スキャナー
正解: **B** (コメントを発表する)

質問: **139**
選挙日に新しいウイルスが発生したことをめぐる誤った情報の拡散は、投票に行くリスクを冒さないことを選択した有権者に向けられました。これは次の例です。
A. intimidation
B. an influence campaign
C. prepending.
D. information elicitation
E. a watering-hole attack
正解: (正解を表示します)