CompTIA.SY0-601-JPN.v2022-01-14.q162

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：	162
バージョン：	v2022-01-14
ページの閲覧量：	1019
問題集の閲覧量：	42466

https://www.jpnshiken.com/shiken/CompTIA.SY0-601-JPN.v2022-01-14.q162.html

質問: **1**
セキュリティ研究者は、ゼロデイエクスプロイトの広範な使用に関するデータを収集しようとしています。研究者がこのデータを収集するために最も使用する可能性が高いのは次のうちどれですか？
A. cvss
B. ハニーポット
C. DNSシンクホール
D. 脆弱性スキャン
正解: **B** (コメントを発表する)

質問: **2**
組織がAUPを定義する理由は次のうちどれですか？
A. 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
B. 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
C. 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
D. 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
正解: (正解を表示します)

質問: **3**
インシデント対応中に、セキュリティアナリストはWebサーバー上の次のログエントリを監視します。
次のうち、アナリストが経験している攻撃の種類を最もよく表しているのはどれですか？
A. SQLインジェクション
B. ディレクトリトラバーサル
C. クロスサイトスクリプティング
D. パスザハッシュ
正解: (正解を表示します)

質問: **4**

A500は、内部脅威検出プログラムを実装しています。主な懸念事項は、ユーザーが許可なく機密データにアクセスしている可能性があることです。潜在的な内部脅威を検出するために、どの休耕地を展開する必要がありますか？
A. ファイルの整合性の監視
B. ハニーファイル
C. DMZ
D. ULF
正解: **(**正解を表示します**)**

質問: **5**
Webサイトhttp://companywebsite.comでは、ユーザーは登録のために、セキュリティの質問への回答を含む個人情報を提供する必要があります。次のうち、データ侵害を引き起こす可能性が最も高いのはどれですか？
A. 安全でないプロトコル
B. パッチがありません
C. オープンパーミッション
D. 入力検証の欠如
正解: **(**正解を表示します**)**

質問: **6**
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. 論理爆弾
B. BIOSの構成が間違っています
C. サプライチェーン攻撃
D. ダウングレード攻撃
E. ファイルレスマルウェア
正解: **(**正解を表示します**)**

質問: **7**
適切に作成されたBCPに含める必要があるコントロールセットは次のうちどれですか？　3つ選択）
A. 修正
B. 回復
C. 探偵
D. フィジカル
E. 補償

F. 抑止力
G. 予防
正解: **(**正解を表示します**)**

質問: **8**
次のうち、揮発性が最も高いものから最も低いものへの正しい順序はどれですか？
A. メモリ、ディスク、一時ファイルシステム、キャッシュ、アーカイブメディア
B. キャッシュ、メモリ、一時ファイルシステム、ディスク、アーカイブメディア
C. メモリ、一時ファイルシステム、ルーティングテーブル、ディスク、ネットワークストレージ
D. キャッシュ、ディスク、一時ファイルシステム、ネットワークストレージ、アーカイブメディア
正解: **(**正解を表示します**)**

質問: **9**
次のうちどれが、パッチが適用されていない従来のプログラマブルロジックコントローラーの操作に悪影響を与える可能性が最も高く、バックエンドLAMPサーバーとWebインターフェイスを介してインターネット経由でアクセス可能な人的管理インターフェイスを備えたOTシステムを実行しますか？　2つ選択してください。）
A. SQLインジェクション
B. サーバー側のリクエストの偽造
C. データの漏えい
D. 弱い暗号化
E. クロスサイトスクリプティング
F. システムログが不十分
正解: **B,D (**コメントを発表する**)**

質問: **10**
企業が懸念しているのは、レッドチーム演習後のセキュリティです。レポートは、SMBがインターネットに公開され、NTLMV1を実行しているため、チームが重要なサーバーに到達できたことを示しています。調査結果を最もよく説明しているのは次のうちどれですか。
A. 開いているポートとサービス
B. 弱いデータ暗号化
C. サーバーのデフォルト設定
D. セキュリティで保護されていない管理者アカウント
正解: **A (**コメントを発表する**)**

質問: **11**
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. 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
B. 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
C. 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
D. VPNアクセラレータでQoSを適切に構成する
正解: **(**正解を表示します**)**

質問: **12**
地域のガイドラインでは、すべての情報システムが準拠するための最小セキュリティベースラインを満たす必要があります。セキュリティ管理者がベースラインに対してシステム構成を評価するために使用できるのは、次のうちどれですか？
A. SOARプレイブック
B. リスク管理フレームワーク
C. セキュリティ管理マトリックス
D. ベンチマーク
正解: **D (**コメントを発表する**)**

質問: **13**
SOCは、インサイダー脅威検出プログラムを実装しています。主な懸念事項は、ユーザーが許可なく機密データにアクセスしている可能性があることです。潜在的な内部脅威を検出するために展開する必要があるのは次のうちどれですか？
A. ハニーファイル
B. DLP
C. ADMZ
D. ファイルの整合性の監視
正解: **(**正解を表示します**)**

質問: **14**
攻撃者は、クライアントのWebサイトでユーザーの資格情報を取得しようとしています。セキュリティアナリストは、ランダムなユーザー名とパスワードが何度も試行されていることに気づきました。アナリストがランダムなユーザー名とパスワードを入力したとき。
ログオン画面に次のメッセージが表示されます。
アナリストが推奨する有効にする必要があるのは次のうちどれですか？
A. 入力検証
B. 難読化
C. ユーザー名のロックアウト
D. エラー処理
正解: **(**正解を表示します**)**

質問: **15**
新しく購入した企業のWAPは、可能な限り最も安全な方法で設定する必要があります。

手順
ネットワーク図の以下の項目をクリックして、それに応じて構成してください。
WAP
DHCPサーバー
AAAサーバー
ワイヤレスコントローラー
LDAPサーバー
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。
正解:

質問: **16**
ある会社が、暗号化されたプロトコルと暗号化されていないWebブラウジングプロトコルの両方を利用するWebサーバーをインターネット上にセットアップしています。セキュリティエンジニアは、インターネットからサーバーに対してポートスキャンを実行し、次の出力を確認します。
次のステップのうち、セキュリティエンジニアがNEXTを実行するのに最適なのはどれですか？
A. インターネットからのDNSアクセスを許可します。
B. インターネットからのHTTPSアクセスをブロックする
C. インターネットからのSSHアクセスをブロックします。
D. インターネットからのSMTPアクセスをブロックする
正解: **(**正解を表示します**)**

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**」

質問: **17**
ユーザーは、過去2週間以内にいくつかの疑わしいアクティビティを報告し、その結果、いくつかの不正なトランザクションが発生しました。調査の結果、セキュリティアナリストは次のことを発見しました。
*その期間内に違反した資格情報の複数のレポート
*ネットワークの特定の部分でリダイレクトされているトラフィック
*さまざまな内部ユーザーが同意なしに送信する不正な電子メール次のタイプの攻撃のうち、最も使用された可能性が高いのはどれですか？
A. リプレイアタック
B. 偽造をリクエストする

C. 競合状態
D. クロスサイトスクリプティング
正解: **D** (コメントを発表する)

質問: **18**
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. 生年月日
B. 指紋
C. PIN
D. TPM
正解: **B** (コメントを発表する)

質問: **19**
最高経営責任者（CEO）は、同社の新しいサービスプロバイダーからのサービスのレベルに不満を持っています。サービスプロバイダーはCEOを阻止しています。
仕事用アカウントから個人用アカウントにメールを送信することから。次のタイプのサービスプロバイダーのどれが使用されていますか？
A. マスターマネージドサービスプロバイダー
B. クラウドサービスプロバイダー
C. 電気通信サービスプロバイダー
D. マネージドセキュリティサービスプロバイダー
正解: (正解を表示します)

質問: **20**
否認防止を実装する際にセキュリティエンジニアが利用する暗号化の概念は次のうちどれですか？　2つ選択してください）
A. 秘密鍵
B. 塩漬け
C. 完全転送秘密
D. 対称鍵
E. ブロック暗号
F. ハッシュ
正解: (正解を表示します)

質問: **21**
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. アラーム

B. 照明
C. サイネージ
D. マントラップ
E. センサー
F. フェンシング
正解: **D,F** (コメントを発表する)

質問: **22**
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. 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。
B. 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。
C. 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。
D. 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。
正解: (正解を表示します)

質問: **23**
会社の特権ユーザーがサーバーからいくつかの専有文書を盗んだ。また、ユーザーはログファイルにアクセスし、インシデントのすべてのレコードを削除しました。システム管理者は、他のログファイルを確認できることを調査員に通知しました。管理者が調査員を支援するために構成した可能性が最も高いのは次のうちどれですか？
A. メモリダンプ
B. アプリケーションログ
C. syslogサーバー
D. ログ保持ポリシー
正解: (正解を表示します)

質問: **24**
クレジットカード取引会社の情報セキュリティ責任者は、内部統制を使用してフレームワークマッピングの演習を行っています。同社は最近、ヨーロッパに新しいオフィスを設立しました。セキュリティ担当者は、次のフレームワークのどれに既存のコントロールをマッピングする必要がありますか？ (2つ選択してください)。

A. SOC
B. CSA
C. GDPR
D. PCI DSS
E. NIST
F. ISO
正解: **C,D** (コメントを発表する)

質問: **25**
次のシナリオのうち、リスク削減手法を最もよく表しているのはどれですか？
A. 技術的な変更ではセキュリティ管理の目的を達成できないため、会社は保険を購入し、データ侵害による損失を心配しなくなりました。
B. 技術的な変更ではセキュリティ管理の目的を達成できないため、会社はより安全な操作方法についてユーザーをトレーニングするポリシーを実装しています。
C. 技術的な変更ではセキュリティ管理の目的を達成できないため、最高情報責任者（CIO）がリスクを承認することを決定します。
D. 技術的な変更ではセキュリティ管理の目的を達成できないため、運用方法に応じて会社が変更されます
正解: (正解を表示します)

質問: **26**
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. エアギャップ
B. コールドアイル
C. 取り外し可能なドア
D. ホットアイル
E. IoTサーモスタット
F. 湿度モニター
正解: (正解を表示します)
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/secure-areas/

質問: **27**
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. 最小特権
B. 利用規定
C. オフボーディング

D. 秘密保持契約
正解: **(**正解を表示します**)**

質問: **28**
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. 証明書の連鎖
B. 自己署名証明書
C. キーエスクロー
D. 拡張検証証明書
正解: **(**正解を表示します**)**

質問: **29**
サイバーセキュリティアナリストは、Webサーバーからのログファイルを確認し、ディレクトリトラバーサル攻撃が発生したことを示す一連のファイルを確認します。アナリストが最もよく目にするのは次のうちどれですか？
A）
B）
C）
D）
A. オプションB
B. オプションC
C. オプションD
D. オプションA
正解: **A (**コメントを発表する**)**

質問: **30**
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. ゼロデイ
B. 弱い暗号化
C. 安全でないルートアカウント
D. デフォルトの権限
正解: **A (**コメントを発表する**)**

質問: **31**
セキュリティエンジニアは、信頼できないネットワークからの接続を必要とするサーバーに使用できるネットワークセグメントを作成する必要があります。エンジニアは次のうちどれを実装する必要がありますか？
A. エアギャップ

B. ホットサイト
C. スクリーニングされたサブネット
D. AVLAN
正解: **C** (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**」

質問: **32**
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. 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
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. 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。
D. 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
正解: **B** (コメントを発表する)

質問: **33**
次のうち、同意または承認なしに組織内で使用されるアプリケーションとシステムに言及しているのはどれですか？
A. 内部脅威
B. ダークウェブ
C. シャドーIT
D. OSINT
正解: (正解を表示します)

質問: **34**
会社のエンジニアは、業界全体の他のエンジニアと定期的に公開インターネットフォーラムに参加しています。このシナリオで攻撃者が最も使用する可能性が高い戦術は次のうちどれですか？
A. ファーミング
B. クレデンシャルの収集
C. ハイブリッド戦争
D. 水飲み場型攻撃
正解: (正解を表示します)

質問: **35**
最高セキュリティ責任者（CSO）は、実行可能ファイルとデータファイルの両方でOSからの不正な実行特権を検出し、プロキシまたはUTMと連携して機能するソリューションを考案するよう技術者に依頼しました。次のうち、CSOの要件を最もよく満たすのはどれですか？
A. サンドボックス
B. ファジング
C. コードレビュー
D. 静的コード分析
正解: **(**正解を表示します**)**

質問: **36**
次のうち、3要素認証を満たすのはどれですか？
A. パスワード、ハードトークン、NFCカード
B. パスワード、網膜スキャナー、NFCカード
C. 指紋スキャナー、ハードトークン、網膜スキャナー
D. パスワード、指紋スキャナー、網膜スキャナー
正解: **(**正解を表示します**)**

質問: **37**
セキュリティアナリストは、内部Webアプリケーションの問題に関するいくつかのレポートを受け取りました。ユーザーは、ログイン時に2回クレデンシャルを提供する必要があることを失効させます。アナリストはアプリケーションチームに確認し、これは予期された動作ではないことに注意します。アナリストがゲートウェイでいくつかのコマンドを実行し、次の出力インターネットアドレスを取得するために数十年を調べた後
次のうち、会社が経験している攻撃を最もよく表しているのはどれですか？
A. ARP中毒
B. DNSハイジャック
C. URLリダイレクト
D. MACフラッディング
正解: **(**正解を表示します**)**

質問: **38**
次の職務のうち、ビジネス要件と規制要件が確実に満たされるようにするデータ品質とデータ入力のイニシアチブを後援するのはどれですか？
A. データプロセッサ
B. データ所有者
C. データプライバシーオフィサー。
D. データスチュワード
正解: **(**正解を表示します**)**

質問: **39**
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. ポリモフィック
B. ランサムウェア
C. ラット
D. ワーム
正解: **(**正解を表示します**)**

質問: **40**
最近、リモートユーザーが海外で2週間の休暇を取り、会社所有のラップトップを持ってきました。仕事に戻ったとき、ユーザーはラップトップをVPNに接続できませんでした。ユーザーがラップトップをVPNに接続できない最も可能性の高い理由は次のうちどれですか？
A. ユーザーのアカウントは法的に保留されました。
B. ユーザーのラップトップは、最新のパス更新を見逃したため、隔離されました。
C. VPNクライアントはブラックリストに登録されました。
D. 海外旅行のため、ユーザーのラップトップはネットワークから分離されました。
正解: **D (**コメントを発表する**)**

質問: **41**
ある会社が最近、メインのWebサイトが攻撃者のWebサーバーに誘導され、攻撃者が疑いを持たない顧客から資格情報を取得できるようにする攻撃を経験しました。この種の攻撃が将来発生するのを防ぐために、会社は次のうちどれを実装する必要がありますか？
A. IPSec
B. S / MIME
C. SSL / TLS
D. DNSSEC
正解: **(**正解を表示します**)**

質問: **42**
ソフトウェア開発者は、新製品の一般リリースの前に、コード実行テスト、ブラックボックステスト、および非機能テストを実行する必要があります。次のうち、開発者が実行しているタスクを最もよく表しているのはどれですか？
A. 正規化
B. ステージング
C. 検証
D. 検証

正解: (正解を表示します)

質問: **43**
セキュリティ管理者は、次の出力を示すネットワークスイッチのテーブルを確認します。
このスイッチで発生しているのは次のうちどれですか？
A. MACフラッディング
B. DNSポイズニング
C. MACクローニング
D. ARP中毒
正解: (正解を表示します)

質問: **44**
セキュリティアナリストが、サードパーティの請負業者からの侵入テストレポートを確認しています。侵入テスターは、組織の新しいAPIを使用してドライバーをバイパスし、組織のWebサーバーで権限昇格を実行しました。APIを見ると、セキュリティアナリストは、特定のAPI呼び出しが古いOSを実行しているレガシーシステムに対するものであることに気付きます。次のうち、最も可能性の高い攻撃タイプはどれですか？
A. セッションのリプレイ
B. 偽造をリクエストする
C. DLLインジェクション
D. シミング
正解: (正解を表示します)

質問: **45**
ある会社では、利用可能なストレージが限られており、オンラインでのプレゼンスは4時間以上はできません。限られた使用可能なストレージスペースを維持している障害が発生した場合に、データベースの復元時間を最速にするために、会社が実装する必要があるバックアップ方法は次のうちどれですか？
A. 毎週日曜日の午後8時にフル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。
B. 毎週日曜日の午後8時に毎晩完全バックアップを実装する
C. 毎週日曜日の午後8時に完全バックアップを実装し、毎晩8:00に差分バックアップを実装します。
D. 毎週日曜日の午後8時に異なるバックアップを実装し、午後8時に毎晩増分バックアップを実装します。
正解: (正解を表示します)

質問: **46**
ネットワーク管理者は、復元力と稼働時間に重点を置いて、新しいデータセンターを構築する必要があります。次のうちどれがこの目的を最もよく満たすでしょうか？ （2つ選択してください。）

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. 定期的な侵入テスト
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

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**」

質問: **47**
セキュリティ管理者は、高い読み取り速度とフォールトトレランスに重点を置いたRAIS構成を作成する必要があります。複数のドライバーが同時に失敗する可能性はほとんどありません。管理者が使用する必要があるRAID構成は次のうちどれですか？
A. RA1D 0
B. RAID1
C. RAID 5
D. RAID 10
正解: **(**正解を表示します**)**
https://techgenix.com/raid-10-vs-raid-5/

質問: **48**
サイバーセキュリティの最中に、セキュリティエンジニアが感染したデバイスをネットワークから削除し、侵害されたすべてのアカウントをロックダウンします。次のインシデント対応フェーズのうち、セキュリティエンジニアが現在運用しているのはどれですか？
A. 準備
B. 根絶
C. 回復
D. 封じ込め
E. 識別
正解: **(**正解を表示します**)**

質問: **49**

攻撃者は、特定のカメラブランドとモデルのセットアップガイドをオンラインで簡単に検索することで、企業のセキュリティカメラに簡単にログインできました。次のうち、攻撃者が悪用した構成を最もよく表しているのはどれですか？
A. デフォルト設定
B. オープンパーミッション
C. 弱い暗号化
D. 安全でないプロトコル
正解: **(**正解を表示します**)**

質問: **50**
製造業者は、政府の規制によって保護および管理する必要がある非常にセキュリティの高い製品の設計を作成します。これらのデザインには、企業ネットワークやインターネットからはアクセスできません。これらの設計を保護するための最良の解決策は次のうちどれですか？
A. 非武装地帯
B. ファラデーケージ
C. エアギャップ
D. シールドケーブル
正解: **(**正解を表示します**)**

質問: **51**
多数の資産を持つ大企業でのデータ侵害を調査するために、外部の科学捜査官が雇われました。侵害はDMZで始まり、機密情報に移動し、攻撃者がネットワークを通過したときに複数のログを生成することが知られています。この調査に最も役立つのは次のうちどれですか？
A. パケットアナライザを使用してNetFlowトラフィックを調査します。
B. SIEMをチェックして、相関ログを確認します。
C. 現在のセッションを表示するには、ルーターへのアクセスが必要です。
D. 脆弱性スキャンを実行して、弱点を特定します。
正解: **(**正解を表示します**)**

質問: **52**
組織は、地理的に多様な場所にバックアップサーバーママを構築しています。最高情報セキュリティ責任者は、新しいハードウェアが既存の下水道室の同じ脆弱性の影響を受けにくいという要件をプロジェクトに実装しました。システムエンジニアは次のうちどれを考慮する必要がありますか？
A. ワークロードをパブリッククラウドインフラストラクチャに移行する
B. 新しい探偵セキュリティコントロールの設計
C. 堅牢なパッチ管理ソリューションの実装
D. さまざまなベンダーからハードウェアを購入する
正解: **(**正解を表示します**)**

質問: **53**
攻撃者は、URLwww.validwebsite.comで偽のWebサイトを作成することにより、ユーザーを悪用しようとしています。攻撃者の意図は、正当なWebサイトのルックアンドフィールを模倣して、疑いを持たないユーザーから個人情報を取得することです。次のソーシャルエンジニアリング攻撃のうち、これが説明しているのはどれですか？
A. タイプミスのしゃがみ
B. 情報の引き出し
C. 水飲み場型攻撃
D. なりすまし
正解: **C (**コメントを発表する**)**

質問: **54**
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. NIST CSF
B. ISO 22301
C. PCI DSS
D. ISO 27001
正解: **(**正解を表示します**)**

質問: **55**
サードパーティのWebベースのサービスとファイル共有プラットフォームを使用している企業でデータ損失イベントを特定して修正するのに最適なのは次のうちどれですか？
A. UTM
B. DLP
C. CASB
D. SIEM
正解: **(**正解を表示します**)**

質問: **56**
ネットワーク管理者は、iPSecを利用してサイト間VPNを構成したいと考えています。管理者は、データ整合性の暗号化、認証、および再生防止機能を使用してトンネルを確立することを望んでいます。管理者がVPNを構成するときに使用する必要があるのは、次のうちどれですか。
A. AH
B. EDR
C. ESP
D. DNSSEC
正解: **(**正解を表示します**)**

https://www.hypr.com/encapsulating-security-payload-esp/
Encapsulating Security Payload (ESP) is a member of the Internet Protocol Security (IPsec) set of protocols that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely.

質問: **57**
主要な政党がサーバーの侵害を経験しました。その後、ハッカーは野党に有利なキャンペーン戦略に関する盗まれた内部通信を公に投稿しました。次のうち、これらの脅威アクターを最もよく表しているのはどれですか？
A. 高度な持続的脅威
B. スクリプトキディ
C. 半承認のハッカー
D. 州の関係者
正解: **(**正解を表示します**)**

質問: **58**
サイバーセキュリティ管理者は、iptablesをエンタープライズファイアウォールとして使用しています。管理者がいくつかのルールを作成しましたが、ネットワークが応答していないようです。すべての接続がファイアウォールによってドロップされています。ルールを削除するのに最適なオプションは次のうちどれですか？
A. #iptables -Z
B. #iptables -P INPUT -j DROP
C. #iptables -t mangle -X
D. #iptables -F
正解: **(**正解を表示します**)**

質問: **59**
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. Zigbee構成
B. ネットワーク範囲
C. 通信プロトコル
D. Z-Waveの互換性
正解: **(**正解を表示します**)**

質問: **60**
最近、一部のラップトップは、キーレスRFID対応ロックで保護されているロックされたストレージ領域から失われました。物理的な空間に明らかな損傷はありません。セキュリティマネージャーは誰がドアのロックを解除したかを特定しますが、人事部は従業員が事件の時点で休暇中

であったことを確認します。次のうち、最も発生する可能性が高いものを説明しているのはどれですか？
A. 従業員の物理アクセスカードのクローンが作成されました。
B. 従業員の生体認証が収集されました
C. 犯罪者がドアを開けるためにピッキングツールを使用しました。
D. 従業員が人的資源と共謀している
正解: **(**正解を表示します**)**

質問: **61**
セキュリティアナリストは、侵害されたシステムに関連するフォレンジック調査中に、携帯電話からいくつかの.jpg写真を発見しました。アナリストは、フォレンジックツールを実行してファイルメタデータを収集します。すべてのメタデータがまだ無傷である場合、次のうちどれが画像の一部になりますか？
A. 印刷ジョブの総数
B. GPS位置
C. 作成されたコピーの数
D. ファイルが削除されたとき
正解: **(**正解を表示します**)**

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**」

質問: **62**
会社の電子メールシステムをさらに保護するために、管理者は会社のドメインのDNSレコードに公開鍵を追加しています。次のうちどれが使用されていますか？
A. PFS
B. DMARC
C. SPF
D. DNSSEC
正解: **(**正解を表示します**)**

質問: **63**
最近の事件から得られた教訓の分析は、管理事務員が技術サポートからであると主張する誰かから電話を受けたことを明らかにしています。発信者は、サラリーマンにWebサイトにアクセスし、ウイルス対策パッケージを装ったプログラムをダウンロードしてインストールするように説得し

ました。このプログラムは実際には、攻撃者が後でワーカーのPCをリモートコントロールするために使用できるバックドアでした。将来この種の攻撃を防ぐのに役立つのは、次のうちどれですか？
A. 検疫
B. セグメンテーション
C. アプリケーションのホワイトリスト
D. データ損失防止
正解: **(**正解を表示します**)**

質問: **64**
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. TLS
B. SSL
C. SPF
D. DMARC
E. DKIM
正解: **(**正解を表示します**)**

質問: **65**
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. パケットキャプチャ
B. ユーザー行動分析
C. 脅威ハンティング
D. 認定された脆弱性スキャン
正解: **C (**コメントを発表する**)**
https://www.comptia.org/blog/your-next-move-threat-hunter#:~:text=Threat%20hunters%20are%20IT%20professionals%20who%20proactively%20find,that%20might%20evade%20the%20security%20operations%20center%20%28SOC%29.

質問: **66**
新しいセキュリティエンジニアがシステムの強化を開始しました。エンジニアが使用している強化手法の1つは、NASへのリモートログインを無効にすることです。ユーザーは、データがユーザーのPCからまだ表示可能であるにもかかわらず、SCPを使用してファイルをNASに転送できないことを報告しています。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. ネットワークサービスはNASで実行されなくなりました
B. ローカルホストでTFTPが無効になっています

C. sshd.confを使用する代わりに、networkd.configでリモートログインが無効になりました
D. 構成ファイルを変更する代わりにSSHがオフになりました
正解: **(**正解を表示します**)**

質問: **67**
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. 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
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. PIIを暗号化するようにアプリケーションを構成します
E. すべてのPIIを許可するようにDLPポリシーを構成します
正解: **B (**コメントを発表する**)**

質問: **68**
セキュリティアナリストは、ネットワーク共有とインターネットへの接続の問題として最初に報告されたインシデントを調査しています。ログとツールの出力を確認しているときに、アナリストは次のことを確認します。
次の攻撃のどれが発生しましたか？
A. IPの競合
B. パスザハッシュ
C. MACフラッディング
D. ディレクトリトラバーサル
E. ARP中毒
正解: **(**正解を表示します**)**
https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning

質問: **69**
次のうち、ハードウェアとソフトウェアのインベントリ、脆弱性管理、およびすべてのネットワーク環境でのリスクを最小限に抑えるための継続的な監視を含めることにより、システムセキュリティの基本的な制御を提供する6つの初期ステップを使用するのはどれですか？
A. ISO 27701
B. SSAE SOC 2
C. インターネットセキュリティセンター
D. NISTリスク管理フレームワーク

正解: (正解を表示します)

質問: **70**
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. 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
B. 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
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. 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
正解: **D** (コメントを発表する)

質問: **71**
オンライン買い物客向けに同社の製品ラインやその他の情報を紹介するために新しいWebサイトを立ち上げている小売企業は、次のURLを登録しました。
会社が利便性とコストに関心を持っている場合、会社がWebサイトを保護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. ワイルドカード証明書
B. 拡張検証証明書
C. 自己署名証明書
D. ルート証明書
E. コード署名証明書
正解: (正解を表示します)

質問: **72**
金融アナリストは会社のAUPに違反していると非難されており、その主張を立証する法医学的証拠があります。アナリストの無実の主張に異議を唱えるのは次のうちどれですか？
A. ボラティリティの順序
B. 否認防止
C. CoC
D. 法的保留
正解: (正解を表示します)

質問: **73**
組織は、重要なサブネットでの侵入検知および防止技術を異常ベースのシステムに移行することを計画しています。これを成功させるために、組織は次のうちどれを決定する必要がありますか？

A. IPS署名
B. エンドポイント構成
C. ベースライン
D. 敵の行動プロファイル
正解: **(**正解を表示します**)**

質問: **74**
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. パブリックレジャー
B. NetFlowデータ
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: **75**
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. OpenIDConnect認証システム
B. OAuth 2.0
C. セキュアエンクレーブ
D. 特権アクセス管理システム
正解: **(**正解を表示します**)**

質問: **76**
次の環境のうち、ハードウェアレベルとソフトウェアレベルの両方でシステムのコンポーネント部分の実行を評価し、パフォーマンス特性を測定するために最もよく使用されるのはどれですか？
A. プロダクション
B. ステージング
C. テスト
D. 開発
正解: **(**正解を表示します**)**

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**」

質問: **77**
次の技術的制御のうち、ホストでのバッファオーバーフローの検出と防止に最適なものはどれですか？
A. NIPS
B. HIDS
C. DLP
D. EDR
正解: **(**正解を表示します**)**

質問: **78**
IT部門のオンサイト開発者は、長年にわたってチームに所属しています。アプリケーションがリリースされるたびに、セキュリティチームは複数の脆弱性を特定できます。チームがアプリケーションを本番環境にリリースする準備ができていることを確認するのに最も役立つのは、次のうちどれですか？
A. データ公開クエリを防止します。
B. アプリケーションをリリースする前にQAに提出してください。
C. サードパーティライブラリの使用を制限します。
D. ソースコードを難読化します。
正解: **(**正解を表示します**)**

質問: **79**
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. ジオフェンス
B. 姿勢
C. フルデバイス暗号化

D. リモートワイプ
E. コンテナ化
F. ストレージセグメンテーション
正解: **C,D (**コメントを発表する**)**

質問: **80**
セキュリティアナリストが最近の脆弱性に関する情報を確認しています。アナリストが最も影響を受けているプラットフォームを検証するために相談する可能性が高いのは、次のうちどれですか？
A. OSINT
B. SIEM
C. CVSS
D. CVE
正解: **(**正解を表示します**)**
CVE entries are brief. They don't include technical data, or information about risks, impacts, and fixes. Those details appear in other databases, including the U.S. National Vulnerability Database (NVD), the CERT/CC Vulnerability Notes Database, and various lists maintained by vendors and other organizations. Across these different systems, CVE IDs give users a reliable way to tell one unique security flaw from another.

質問: **81**
ユーザーのPCが最近マルウェアに感染しました。ユーザーはベンダーサポートのないレガシープリンターを使用しており、ユーザーのOSには完全にパッチが適用されています。ユーザーはインターネットからドライバーパッケージをダウンロードしました。ダウンロードしたファイルに脅威は見つかりませんでしたが、ファイルのインストール中に、悪意のあるランタイムの脅威が検出されました。次のうちどれが感染の最も可能性の高い原因ですか？
A. ユーザーのウイルス対策ソフトウェアの定義が古く、ドライバーのインストールによって破損していました
B. ドライバーにはマルウェアがインストールされており、検出を回避するためにダウンロード時にリファクタリングされました。
C. ユーザーのコンピューターにはルートキットがインストールされており、新しいドライバーがキーファイルを上書きするまで検出を回避していました。
D. ユーザーのコンピューターは、新しいドライバーがインストールされたときに実行するように設定された論理爆弾に感染しています。
正解: **(**正解を表示します**)**

質問: **82**
セキュリティアナリストは、BYODユーザー向けのMDMソリューションを実装する必要があります。これにより、企業はデバイスに存在する企業の電子メールを引き続き制御し、デバイスの紛失

や盗難が発生した場合に発生する可能性のあるデータの漏えいを制限できます。次のうちどれがこれらの要件を最もよく満たしますか？ (2つ選択してください)。
A. フルデバイス暗号化
B. アプリケーションのホワイトリスト
C. ネットワーク使用規則
D. リモコン
E. コンテナ化
F. ジオフェンス
正解: **(**正解を表示します**)**

質問: **83**
最近発見されたゼロデイエクスプロイトは、SMBネットワークプロトコルの未知の脆弱性を利用して、コンピューターに迅速に感染します。感染すると、コンピューターは暗号化され、身代金を要求されます。この攻撃の再発を防ぐのに最適なのは次のうちどれですか？
A. SMBポートへのインバウンド外部接続を拒否するように境界ファイアウォールを構成します。
B. エンドポイント検出および応答システムが疑わしいSMB接続について警告していることを確認します。
C. コンピューターが毎月のオペレーティングシステムをインストールするように設定されていることを確認し、自動的に更新します。
D. 認証されていないユーザーによる共有ネットワークフォルダーへのアクセスを拒否します。
正解: **(**正解を表示します**)**

質問: **84**
会社はすべてのラップトップでワイヤレスを使用し、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とともに、資産の非常に詳細な記録を保持しています。最高情報責任者 (CIO)は、許可されていないデバイスを使用してワイヤレスPSKをブルートフォース攻撃し、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を懸念しています。これを防ぐために、会社は次のうちどれを実装する必要がありますか？
A. BPDUガード
B. WPA-EAP
C. IPフィルタリング
D. WIDS
正解: **(**正解を表示します**)**
"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: **85**
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. chflags
B. chmod
C. 1a
D. setuid
E. leof
正解: **(**正解を表示します**)**

質問: **86**
会社が最近侵害された会社の新しいサイバーセキュリティ戦略の一部は、すべてのセキュリティデバイスからのログを一元化することです。次のコンポーネントのどれがログを中央ソースに転送しますか？
A. ログ集計
B. ログコレクター
C. ログパーサー
D. ログの強化
正解: **(**正解を表示します**)**

質問: **87**
ハードウェアインシデントの後、問題を修正するために計画外の緊急メンテナンス活動が実施されました。
この期間中に、SIEMで複数のアラートが生成されました。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. SIEMはルールを相互に関連付けることができず、アラートをトリガーしました。
B. 同時に発生した攻撃により、複数のアラートが生成されました。
C. 予期しないトラフィックが複数のルールと相関し、複数のアラートを生成しました。
D. 相関ルールのエラーが複数のアラートをトリガーしました。
正解: **(**正解を表示します**)**

質問: **88**
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. MAC
B. ACL
C. BPDU
D. ARP
正解**: A (**コメントを発表する**)**
MAC operates at layer 2 which is the data link layer.

質問**: 89**
読み取られたデータを保護するためのテストおよびトレーニングの目的で、機能テストデータを新しいシステムで使用できるようにするのは次のうちどれですか？
A. データの暗号化
B. データマスキング
C. データの重複排除
D. データの最小化
正解**: (**正解を表示します**)**
https://ktechproducts.com/Data-mask#:~:text=Data%20Masking%20is%20a%20method%20of%20creating%20a,partial%20data%20based%20on%20the%20user%E2%80%99s%20security%20permissions.
The main reason for applying masking to a data field is to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data. However, the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. It is more common to have masking applied to data that is represented outside of a corporate production system. In other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles https://en.wikipedia.org/wiki/Data_masking

質問**: 90**
システム管理者は、ハッカーがOAuthアプリケーションを利用して、ユーザーをだまして企業のクレデンシャルの使用を許可させないようにするソリューションを探しています。次のうち、このソリューションを最もよく表しているのはどれですか？
A. UEM
B. VPC
C. CASB
D. WAF
正解**: (**正解を表示します**)**

質問**: 91**
大規模なデータ侵害の後にアプリケーションを保護するために、eコマースサイトはすべてのユーザーの資格情報をリセットします。リセット後にサイトのユーザーが危険にさらされないようにするのに最適なのは、次のうちどれですか？

A. 3回失敗した後のアカウントのロックアウト
B. 転送中の暗号化されたクレデンシャル
C. パスワード再利用ポリシー
D. ログイン履歴に基づくジオフェンスポリシー
正解: **(**正解を表示します**)**

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**」

質問: **92**
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、建物全体にある任意のシンクライアントにログを記録し、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ーは次のうちどれですか？　2つ選択してください）
A. BYOD
B. COPE
C. TOTP
D. RFID
E. GPS
F. VDI
正解: **D,F (**コメントを発表する**)**

質問: **93**
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. 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。
B. 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。
C. 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。

D. 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。
正解: **(**正解を表示します**)**

質問: **94**
重要なシステムとデータが完全に失われた場合に備えて、組織は計画を策定しています。次の計画のうち、組織が最も開発しそうなものはどれですか？
A. コミュニケーション
B. インシデント対応
C. ディザスタリカバリ
D. データ保持
正解: **(**正解を表示します**)**

質問: **95**
アナリストが管理チームのセキュリティレポートを生成しています。セキュリティガイドラインでは、暗号化されていないすべてのリスニングサービスを無効にすることを推奨しています。
Nmapからのこの出力を考えると：
アナリストが無効にすることを推奨するのは次のうちどれですか？
A. 21 / tcp
B. 443 / tcp
C. 23 / tcp
D. 22 / tcp
正解: **B (**コメントを発表する**)**

質問: **96**
アナリストは、電源ボタンを押したままにして、ユーザーが実行しているアプリケーションと、ユーザーのコンピューターがシャットダウンされる前に開いていたファイルを特定する必要があります。次のうち、その情報が含まれている可能性が最も高いのはどれですか？
A. RAM
B. ページファイル
C. NGFW
D. NetFlow
正解: **(**正解を表示します**)**

質問: **97**
セキュリティアナリストは、指紋スキャナーのデータセンターアクセスログを確認し、施設へのアクセスに関するユーザーの報告に関連するエラーが豊富にあることに気付きます。アクセス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. 誤った拒否
B. 証明

C. 有効性のルール
D. クロスオーバーエラー率
正解: **(**正解を表示します**)**

質問: **98**
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. データ保護責任者
B. データ所有者
C. データプロセッサ
D. データコントローラー
正解: **B (**コメントを発表する**)**

質問: **99**
技術者は、実験室でのデータ損失を防ぐ必要があります。研究室は外部ネットワークに接続されていません。次の方法のうち、データの漏えいを防ぐのに最適な方法はどれですか？　2つ選択してください)。
A. ファイルレベルの暗号化
B. MFA
C. ドライブの暗号化
D. ネットワークファイアウォール
E. USBブロッカー
F. VPN
正解: **(**正解を表示します**)**

質問: **100**
セキュリティアナリストは、システムからの次の出力を確認しています。
次のうち、最も観察される可能性が高いのはどれですか？
A. DNSポイズニング
B. ARPパーソニング
C. サービス拒否
D. 中間者
正解: **(**正解を表示します**)**

質問: **101**
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. サードパーティライブラリ
B. NIST CSF
C. OWASP

D. 脆弱性スキャンの結果
正解: **(**正解を表示します**)**

質問: **102**
セキュリティアナリストは、企業でのマルウェアインシデントを調査しています。マルウェアは、www.comptia.comのコマンドアンドコントロールWebサイトにアクセスしています。すべてのアウトバウンドインターネットトラフィックはsyslogサーバーに記録され、/ logfiles / messagesに保存されます。
アナリストがsyslogサーバーでコマンドアンドコントロールWebサイトへの最近のトラフィックを検索するために使用するのに最適なコマンドは次のうちどれですか？
A. オプションD
B. オプションB
C. オプションA
D. オプションC
正解: **D (**コメントを発表する**)**

質問: **103**
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。次のベストのどれがこの慣行のリスクを説明しますか？
A. 弱い暗号化
B. 安全でないプロトコル
C. ベンダーサポートの欠如
D. デフォルトのシステム構成
正解: **(**正解を表示します**)**

質問: **104**
最近の監査では、ビジネス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発見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、次のタイプのコントロールのどれを使用する必要がありますか？
A. 補償
B. 物理的
C. 予防
D. 探偵
正解: **A (**コメントを発表する**)**

質問: **105**
ネットワークエンジニアは、倉庫内の複数のワイヤレスバーコードスキャナーとワイヤレスコンピューターが出荷サーバーに断続的に接続している理由を調査するように依頼されました。バーコードスキャナーとコンピューターはすべてフォークリフトに搭載されており、通常の使用中に

倉庫内を移動します。問題を特定するためにエンジニアは次のうちどれを行う必要がありますか？ （2つ選択してください。）
A. 現地調査を実施する
B. FTKイメージャをデプロイします
C. ヒートマップを作成する
D. 不正なアクセスポイントをスキャンします
E. セキュリティプロトコルをアップグレードする
F. キャプティブポータルをインストールする
正解: **(**正解を表示します**)**
heat map and site survey will provide the wifi strength and identify the weakness areas..this will give the opportunity if we need to increase WiFI strength or give suggestion to the forklift drivers about the movement

質問: **106**
セキュリティアナリストは、MOMインフラストラクチャを強化するためのポリシーを適用する必要があります。要件は次のとおりです
*モバイルデバイスを取引してワイプできることを確認します。
*モバイルデバイスが暗号化されていることを確認します。
アナリストがこれらの要件を満たすために、すべてのデバイスで有効にする必要があるのは次のうちどれですか？
A. 生体認証
B. ジオタグ
C. ジオフェンス
D. ジオロケーション
正解: **(**正解を表示します**)**

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**」

質問: **107**
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. バッファオーバーフロー

B. DDoS攻撃
C. メモリリーク
D. リソースの枯渇
正解: **(**正解を表示します**)**

質問: **108**
最高情報セキュリティ責任者（CISO）は、データベースリソースを消費するローカルデータセンターへのDDoS攻撃が長引く場合に、組織が事業運営を継続できるかどうかを懸念しています。CISOがこのリスクを軽減するために最も推奨するのは次のうちどれですか？
A. データセンターで利用可能な帯域幅をアップグレードします
B. ホットサイトフェイルオーバーの場所を実装する
C. 顧客への完全なSaaSオファリングに切り替えます
D. すべてのエンドユーザークエリにチャレンジレスポンステストを実装します
正解: **D (**コメントを発表する**)**
creating a whole new hot sire just because of DDoS seems extremely expensive. Instead, deploying a countermeasure like challenge response would mitigate the DDoS.
https://www.radware.com/security/ddos-knowledge-center/ddospedia/http-challenge
https://www.nexusguard.com/hubfs/Nexusguard_Whitepaper_DDoS_Mitigation_EN_A4.pdf?t=1487581897757

質問: **109**
現在の秘密鍵が危険にさらされている場合、すべての履歴データを復号化するためにそれを使用できないことを保証するのは次のうちどれですか？
A. 準同型暗号化
B. 完全転送秘密
C. 楕円曲線暗号
D. キーストレッチ
正解: **C (**コメントを発表する**)**

質問: **110**
組織のヘルプデスクには、特定のWebサイトにアクセスできなくなったというユーザーからの電話が殺到しています。これらのWebサイトは前日にアクセス可能だったため、ヘルプデスクは問題をセキュリティチームにエスカレーションします。セキュリティアナリストは次のコマンドを実行します :ipconfig / flushdnsが、問題は解決しません。最後に、アナリストが影響を受けるマシンのDNSサーバーを変更すると、問題は解決します。次の攻撃のうち、元のDNSサーバーで発生した可能性が最も高いのはどれですか？
A. ドメインハイジャック
B. DNSトンネリング
C. DNSキャッシュポイズニング
D. 分散型サービス拒否

正解: (正解を表示します)

質問: **111**
組織の労働力は増加しており、そのほとんどは営業部門への追加によって推進されています。新しく雇用された各営業担当者は、ビジネスを行うためにモバイルデバイスに依存しています。最高情報責任者（CIO）は、組織がスケールアップするのと同じくらい迅速にスケールダウンする必要があるのではないかと考えています。CIOは、組織のセキュリティと顧客のプライバシーについても懸念しています。次のうち、CIOの懸念に対処するのに最適なものはどれですか？
A. 新入社員がモバイルデバイスを6か月間使用することを禁止する
B. COPE方法論を使用してモバイルデバイスを展開する
C. MDMを活用しながら、状態部門にBYODを実装する
D. CYODモデルで使用する営業部門のデバイスを4つ選択します
正解: (正解を表示します)

質問: **112**
大規模な産業用システムのスマートジェネレーターは、システムステータスを監視し、重大な障害が発生したときにサードパーティの保守担当者にアラートを送信します。ネットワークログを確認しているときに、会社のセキュリティマネージャは、ジェネレータのIPが内部ファイルサーバーのIPにパケットを送信していることに気付きます。アラート機能を維持しながらセキュリティマネージャが実装するのに最適な緩和策は次のうちどれですか？
A. 分離
B. 封じ込め
C. ファイアウォールのホワイトリスト
D. セグメンテーション
正解: (正解を表示します)

質問: **113**
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. 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。
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. 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。
正解: (正解を表示します)

質問: **114**

次のうち、サービスリポジトリとして機能するクライアントサーバーアーキテクチャで動作することが多いのはどれですか。企業の消費者に構造化された脅威インテリジェンスデータへのアクセスを提供しますか？
A. STIX
B. TAXII
C. OSINT
D. CIRT
正解: **D** (コメントを発表する)

質問: **115**
重要なファイルサーバーがアップグレードされており、システム管理者は、新しいサーバーがパリティを達成し、2つの同時ディスク障害を処理するために必要なRAIDレベルを決定する必要があります。次のRAIDレベルのどれがこの要件を満たしていますか？
A. RAID 0 + 1
B. RAID 6
C. RAID 5
D. RAID 2
正解: **B** (コメントを発表する)

質問: **116**
セキュリティチームは、リラ企業ネットワークのIPスペースから著作権侵害の報告を受けました。レポートには、インシデントの正確なタイムスタンプと、著作権で保護されたファイルの名前が記載されていました。アナリストは、侵害元のマシンを特定する任務を負っており、このようなインシデントの再発を防ぐための対策を実施するように指示されています。次のうち、MOSTが両方のタスクを実行できるのはどれですか？
A. 許可リスト
B. HIDS
C. NGFW
D. TPM
正解: **C** (コメントを発表する)

質問: **117**
Webサーバー管理者には冗長サーバーがあり、プライマリサーバーがダウンしたときにセカンダリサーバーへのフェイルオーバーを確保する必要があります。混乱を避けるために、管理者は次のうちどれを実装する必要がありますか？
A. 高可用性
B. NICチーミング
C. デュアル電源
D. laaS
正解: (正解を表示します)

質問: **118**
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. スクリプトキディ
B. シャドーIT
C. ハクティビズム
D. ホワイトハット
正解: **(**正解を表示します**)**
Shadow IT solutions increase risks with organizational requirements for control, documentation, security, reliability, etc - https://en.wikipedia.org/wiki/Shadow_IT

質問: **119**
セキュリティエンジニアは、すべてのワークステーションで2要素認証を有効にしました。次のアプローチのうち、最も安全なものはどれですか？　2つ選択してください）。
A. パスワードとCAPTCHA
B. パスワードとセキュリティの質問
C. パスワードとワンタイムトークン
D. パスワードと指紋
E. パスワードと音声
F. パスワードとスマートカード
正解: **(**正解を表示します**)**

質問: **120**
ザ・
ウェブサイトhttp://companywebsite.comでは、ユーザーは登録のためにセキュリティ応答を含む個人情報を提供する必要があります。次のうち、日付違反を引き起こす可能性が最も高いのはどれですか？
A. 不確かなプロトコル
B. オープンパーミッション
C. 入力検証の欠如
D. パッチがありません
正解: **(**正解を表示します**)**

質問: **121**
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. 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。
D. 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。
正解: **C** (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**」

質問: **122**
CSIRTは、最近の事件から学んだ教訓を検討しています。ワームはネットワーク全体に妨げられることなく拡散し、多数のコンピューターやサーバーに感染する可能性がありました。次の推奨事項のうち、将来同様のインシデントの影響を軽減するのに最適なものはどれですか？
A. すべてのウイルス対策シグネチャを毎日更新します。
B. アプリケーションのブラックリストを実装します。
C. ファイアウォールでネットワークをセグメント化します。
D. 境界にNIDSデバイスをインストールします。
正解: **C** (コメントを発表する)

質問: **123**
ある会社は、過去数か月にわたって公益事業会社からの非常に短い停電を経験しています。
これらの停止は、毎回1秒間しか続きません。公益事業会社はこの問題を認識しており、故障した変圧器の交換に取り組んでいます。重要なサーバーとネットワークデバイスをオンラインに保つために会社が何を購入すべきかを説明しているのは、次のうちどれですか。
A. A UPS
B. Dual power supplies
C. APDU
D. A generator
正解: **A** (コメントを発表する)

質問: **124**
次の環境のうち、ダミーデータを利用し、コードを直接評価してビルドごとに簡単に変更できるシステムにローカルにインストールされる可能性が最も高いのはどれですか？

A. 生産
B. ステージング
C. テスト
D. 開発
正解: **(**正解を表示します**)**

質問: **125**
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3がユーザーに電子メールアドレスと10桁の数字を1日1回IPアドレスで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唯一の再送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. ハッカーが機密データを盗み出そうとしています。
B. 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。
C. コンピューター上の4つのボットは、Webサイトに対してパスワードを強制するルールです。
D. エンドユーザーはWebブラウザから2つのPUPを購入してインストールしました。
正解: **(**正解を表示します**)**

質問: **126**
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. LANManagerハッシュ値の保存
B. NetBIOS over TCP / IPを無効にする
C. ネットワーク共有を有効にする
D. サービスアカウントを無効にする
E. ゲストアカウントを無効にする
F. NTLMを有効にする
正解: **(**正解を表示します**)**

質問: **127**
ある組織が積極的な攻撃を支援するためにコンサルタントを雇い、コンサルタントは侵害されたアカウントとコンピューターを特定することができました。コンサルタントが根絶の準備をすることを最も推奨する可能性が高いのは次のうちどれですか？
A. 攻撃者に警告しないように、侵害されたアカウントとコンピューターをハニーネットに分割します。
B. 攻撃者のアクセスを排除するために、侵害されたアカウントとコンピューターをログオフして削除します。
C. 侵害されたアカウントとコンピューターを隔離し、ネットワークアクセスのみを提供する

D. 侵害されたアカウントとコンピューターを隔離し、すべてのネットワークとインターネットアクセスを遮断します。
正解: **A** (コメントを発表する)

質問: **128**
次のうち、許可されていない人員を護衛する際にスタッフに説明責任を負わせるのはどれですか？
A. バッジ
B. カメラ
C. ロック
D. 訪問者ログ
正解: (正解を表示します)

質問: **129**
ある企業は、ウイルス対策およびWebコンテンツフィルターによって悪意のあるアクティビティがブロックされた場合にアラートをログに記録して送信するための新しいSIEMを実装しています。このシナリオの主な使用例は次のうちどれですか？
A. 抑止制御の実施
B. 是正管理の実施
C. 予防管理の実施
D. 探偵コントロールの実装
正解: (正解を表示します)

質問: **130**
企業はBYODポリシーを採用しており、ユーザーデバイス上の企業情報を保護するための包括的なソリューションを探しています。次のソリューションのうち、ポリシーを最もよくサポートするのはどれですか？
A. バイオメトリクス
B. フルデバイス暗号化
C. モバイルデバイス管理
D. リモートワイプ
正解: (正解を表示します)

質問: **131**
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. 災害復旧計画。
C. 運用計画の継続性
D. 事業継続計画

正解: (正解を表示します)

質問: **132**
フィッシングおよびスピアフィッシング攻撃は、企業のスタッフに対してより頻繁に発生しています。次のうちどれがこの問題を軽減するのに最も役立つと思われますか？
A. DNSクエリログ
B. DNSSECとDMARC
C. DNS内の正確なメールエクスチェンジャーレコード
D. DNS条件付きフォワーダーの追加
正解: (正解を表示します)

質問: **133**
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。
次のスロップを実行します。
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: **134**
組織のSIEMは、内部ネットワークのワークステーションからの疑わしいトラフィックを検出しました。ワークステーションのSOCのアナリストが、ボットネットに関連付けられているマルウェアがデバイスにインストールされていることを発見しました。ワークステーションのログを確認すると、ローカルアカウントの特権がローカル管理者にエスカレーションされていることがわかります。アナリストがこの現実の出来事を報告する必要があるのは、次のどのグループですか？
A. NOCチーム
B. 脆弱性管理チーム
C. CIRT
D. リードチーム
正解: (正解を表示します)

質問: **135**
次世代ファイアウォールでのみ利用できる2つの機能はどれですか？ (2つ選択してください)
A. 仮想プライベートネットワーク
B. パケットフィルタリング

C. ディープパケットインスペクション
D. ステートフルインスペクション
E. アプリケーションの認識
正解: **A,D** (コメントを発表する)

質問: **136**
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. 準備
B. 封じ込め
C. 識別
D. 回復
正解: (正解を表示します)

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**」

質問: **137**
次のコントロールのうち、悪意のあるインサイダー活動を最もよく特定して報告するのはどれですか？
A. 侵入検知システム
B. プロキシ
C. 監査証跡
D. 強力な認証
正解: (正解を表示します)
An intrusion detection system (IDS; also intrusion protection system or IPS) is a device or software application that monitors a network or systems for malicious activity or policy violations. [1] Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

質問: **138**

故障した機器のトラブルシューティングと復元に必要な平均時間を測定するメンテナンス指標について説明しているのは次のうちどれですか？
A. RTO
B. MTBF
C. MTTR
D. RPO
正解: (正解を表示します)
Mean time to repair (MTTR) is a measure of the maintainability of a repairable item, which tells the average time required to repair a specific item or component and return it to working status. It is a basic measure of the maintainability of equipment and parts. This includes the notification time, diagnosis and the time spent on actual repair as well as other activities required before the equipment can be used again. Mean time to repair is also known as mean repair time.
https://www.techopedia.com/definition/2719/mean-time-to-repair-mttr

質問: **139**
ネットワークエンジニアは、大規模オフィスのワイヤレスインフラストラクチャをアップグレードするための計画を作成する必要があります。現在遅延と接続の問題が発生しているエリアを優先する必要があります。次のうち、優先順位を決定するための最良のリソースはどれですか？
A. Nmapn
B. ヒートマップ
C. ネットワーク図
D. Wireshark
正解: (正解を表示します)
engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently.
Site surveys and heat maps provide the following benefits: Identify trouble areas to help eliminate slows speeds and poor performance

質問: **140**
銀行の遅延を要求した携帯電話のSMSを最近使用したユーザー。この場合、次のソーシャルエンジニアリング手法のどれが使用されましたか？
A. SPIM
B. スミッシング
C. ビッシング
D. スピアフィッシング
正解: (正解を表示します)

質問: **141**
セキュリティアナリストは、セキュリティインシデントがどのように発生したか、回復のために実行された手順、および将来のインシデントを回避する方法を詳しく説明したドキュメントを作

成する必要があります。応答プロセスの次のどの段階で、このアクティビティが実行されますか？
A. 識別
B. 準備
C. 回復
D. 学んだ教訓
正解: **D** (コメントを発表する)

質問: **142**
DRPとBCPの違いは次のうちどれですか？
A. BCPは災害時に操作を実行し続けますが、DRPは実行しません。
B. BCPは正式に作成および承認されていますが、DRPはそうではありません。
C. BCPは運用の中断に備え、DRPは自然災害に備えます
D. BCPは、DRPの運用中の災害に対する技術的な対応です。
正解: (正解を表示します)

質問: **143**
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. 161
B. 139
C. 135
D. 143
E. 443
F. 445
正解: **C,E** (コメントを発表する)

質問: **144**
セキュリティアナリストは、会社が発行した多数の新しいラップトップを構成しています。アナリストは次の要件を受け取りました。
*デバイスは、広範囲に旅行するスタッフによって国際的に使用されます。
*旅行の要件により、時折の個人的な使用は許容されます。
*ユーザーは、認可されたプログラムと生産性スイートをインストールして構成できる必要があります。
*デバイスは暗号化する必要があります
*デバイスは、低帯域幅環境で動作できる必要があります。

次のうち、デバイスのセキュリティ体制に最大のメリットをもたらすのはどれですか？
A. 常時接続VPNの構成
B. アプリケーションのホワイトリストの実装
C. オンプレミスコンテンツフィルターを通過するためにWebトラフィックを要求する
D. ウイルス対策DATの更新スケジュールを毎週に設定する
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/always-on-vpn-technology-overview

質問: **145**
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. 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
B. 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
C. 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
D. 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
正解: **(**正解を表示します**)**

質問: **146**
ある会社が、業務をクラウドに移行することを決定しました。ユーザーが個人的な使用のために会社のアプリケーションをダウンロードするのを防ぎ、アップロードされるデータを制限し、会社全体でどのアプリケーションが使用されているかを可視化するテクノロジーを利用したいと考えています。次のソリューションのうち、これらの要件を最もよく満たすのはどれですか？
A. CASB
B. NG-SWG
C. アプリケーションのホワイトリスト
D. NGFW
正解: **(**正解を表示します**)**

質問: **147**
組織は、可能性のあるデータに保存されているデータへのユーザーアクセスを保護するために、2段階の検証プロセスを実装しました。各従業員は、携帯電話番号の電子メールアドレスとコードを使用してデータにアクセスするようになりました。組織が実装した認証方法は次のうちどれですか？
A. 静的コード
B. プッシュ通知

C. トークンキー
D. HOTP
正解: **(**正解を表示します**)**

質問: **148**
サードパーティのWebベースのサービスとファイル共有プラットフォームを使用している企業でデータ損失イベントを特定して修正するのに最適なのは次のうちどれですか？
A. EDR
B. SIEM
C. UTM
D. CASB
正解: **(**正解を表示します**)**

質問: **149**
セキュリティアナリストは、攻撃者がUser3を使用して企業のネットワーク内に足場を築く方法を決定する必要があります。会社のロックアウトポリシーでは、3回の試行が失敗した後、アカウントを最低15分間ロックアウトする必要があります。ログファイルを確認しているときに、アナリストは次のことを発見しました。
次の攻撃のうち、最も発生した可能性が高いのはどれですか？
A. 辞書
B. 資格情報の詰め込み
C. パスワードスプレー
D. ブルートフォース
正解: **(**正解を表示します**)**
"Brute force attack in which stolen user account names and passwords are tested against multiple websites." CompTIA SY0-601 Official Study Guide Page 690 This is a poorly worded question and while credential stuffing is a type of brute force attack, the information given does not indicate multiple websites. At best, this looks like a password spraying attack, but it is more likely a brute-force attack. Also note the output reads "unsername" and not "username" - perhaps irrelevant but the little things can and do matter

質問: **150**
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
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、期限切れのSSL証明書が特定されました
D. 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
正解: **B (**コメントを発表する**)**

質問: **151**
次のうち、リスク回避の例はどれですか？
A. 機器の盗難を防止するための予防措置を講じていない
B. 脆弱性の修正を促進するために、セキュリティ更新プログラムを本番環境に直接インストールする
C. エクスプロイトに関連する経済的損失に備えるための保険の購入
D. 互換性エラーを防ぐために新しいソフトウェアをインストールしない
正解: (正解を表示します)

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**」

質問: **152**
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. 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。
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. 論理爆弾が実行され、データ転送を担当します。
D. 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。
正解: (正解を表示します)
https://www.howtogeek.com/362203/what-is-a-tar.gz-file-and-how-do-i-open-it/

質問: **153**
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. 複雑なパスワードポリシー
B. 禁止されているパスワードリスト
C. 多要素認証

D. IP制限
正解: **(**正解を表示します**)**

質問: **154**
組織内のリモートワーカーは、ローカルにインストールされたアプリケーションとローカルに保存されたデータを備えた会社提供のラップトップを使用します。ユーザーは暗号化された接続を使用してリモートサーバーにデータを保存できます。組織は、ラップトップに保存されたデータが一般に公開されていることを発見しました。次のセキュリティソリューションのうち、将来のデータ開示のリスクを軽減するのはどれですか？
A. VPN
B. FDE
C. TPM
D. HIDS
正解: **(**正解を表示します**)**

質問: **155**
インシデント対応技術者は、調査中にモバイルデバイスを収集しました。技術者は、CoCを維持するために次のうちどれを行う必要がありますか？
A. コレクションを文書化し、所有権が変更されたときにサインオフを要求します。
B. コレクションをブロックチェーンで保護されたパブリック元帳に記録します。
C. 盗難や改ざんを防ぐために、デバイスを安全な場所またはその他の安全な場所にロックします。
D. データの破損を防ぐために、デバイスをファラデーケージに入れます。
正解: **A (**コメントを発表する**)**

質問: **156**
セキュリティエンジニアは、建物内の機密エリアへのMFAアクセスを強化する必要があります。キーカードと指紋スキャンはすでに使用されています。次のうちどれが認証の別の要素を追加しますか？
A. SMSテキスト
B. 網膜スキャン
C. ハードトークン
D. キーパッドPIN
正解: **(**正解を表示します**)**

質問: **157**
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. 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
C. DLPアプライアンスはNGFWに統合する必要があります。
D. 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
正解: **A (**コメントを発表する**)**

質問: **158**
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。
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。
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: **(**正解を表示します**)**
Data Owner - the administrator/CEO/board/president of a company Data custodian - the ones taking care of the actual data - like IT staff (generally) or HR staff (for HR-related data) https://security.stackexchange.com/questions/218049/what-is-the-difference-between-data-owner-data-custodian-and-system-owner https://www.nicolaaskham.com/blog/2019/4/12/whats-the-difference-between-data-owners-and-data-custodians

質問: **159**
次のポリシーのうち、組織が企業のIT /セキュリティ運用における潜在的な単一障害点を特定して軽減するのに役立つのはどれですか？
A. 最小特権
B. 意識向上トレーニング
C. 職務の分離
D. 必須の休暇
正解: **(**正解を表示します**)**
Separation of duties - is a means of establishing checks and balances against the possibility that critical system or procedures can be compromised by insider threats. Duties and responsibilities should be divided among individuals to prevent ethical conflicts or abuse of powers.

質問: **160**
セキュリティアナリストがサーバー上のログを確認し、次の出力を確認しています。
セキュリティアナリストが観察しているのは次のうちどれですか？
A. レインボーテーブル攻撃

B. パスワードスプレー攻撃
C. キーロガー攻撃
D. 辞書攻撃
正解: (正解を表示します)

質問: **161**
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. 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
C. 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
D. 感染したホストの手動検疫の実装
正解: (正解を表示します)

質問: **162**
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. 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。
B. 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。
C. 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。
D. デバイスは弱い暗号化暗号を使用します。
正解: (正解を表示します)

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**」