VMware.250-605.v2026-06-26.q54

試験コード： 250-605
試験名称： Symantec Endpoint Protection 14.x Admin R2 Technical Specialist
認証ベンダー： VMware
無料問題の数： 54
バージョン： v2026-06-26
ページの閲覧量： 102
問題集の閲覧量： 540
https://www.jpnshiken.com/shiken/VMware.250-605.v2026-06-26.q54.html

質問: **1**
SEDRは、セキュリティチームが疑わしい活動と確認済みの悪意のある活動を区別するのにどのように役立ちますか？
A. インシデント名を脅威インテリジェンスフィードと比較する
B. IPアドレスごとにトリガーされたファイアウォールブロックの数をカウントします
C. 各エンドポイントを特定の調査チームに割り当てることで
D. イベントをMITRE ATT&CKステージにマッピングし、アーティファクトを関連付ける
正解: **(**正解を表示します**)**

質問: **2**
組織がSEPで位置情報に基づくポリシーを使用する理由は何ですか？
A. クラウド環境でのみグループ更新プロバイダーの役割を適用する
B. クライアントのネットワーク状況に基づいてセキュリティポリシーをカスタマイズする
C. オフライン時に保護機能を自動的に無効にする
D. 企業ネットワーク上で管理対象外のデバイスを許可する
正解: **(**正解を表示します**)**

質問: **3**
Symantec Endpoint Protectionの導入において、グループアップデートプロバイダ（GUP）はどのような役割を果たしますか？
A. 複数のSEPMサイトにわたるファイアウォールルールを管理します。
B. Syslogトラフィックを外部ログコレクターに転送します
C. ライセンスキーとポリシーのバックアップをホストします
D. 近くのクライアントにコンテンツの更新を提供する代替サーバーとして機能します。
正解: **(**正解を表示します**)**

質問: **4**
SEPのどの機能を使えば、管理者はWindowsとMacの両方のクライアントでUSBストレージデバイスをブロックできるのでしょうか？

A. デバイス制御
B. アプリケーション制御
C. ソナー保護
D. ホストの完全性
正解: **A** (コメントを発表する)

質問: **5**
SEPMのどの2種類のレポートが、Windowsクライアント全体におけるウイルスやスパイウェアの活動を監視するのに役立ちますか？
（2つ選択）
A. ログオン失敗レポート
B. デバイス制御イベント
C. 感染ファイル（ソース別）
D. リスク分布概要
正解: **C,D** (コメントを発表する)

質問: **6**
システムロックダウンを有効にする際、許可されるアプリケーションのセットを定義するために不可欠なファイルはどれですか？
A. ホスト整合性チェックファイル
B. 除外ポリシーファイル
C. セキュリティ証明書ファイル
D. ファイル指紋リスト
正解: (正解を表示します)

質問: **7**
SEPのどのコンポーネントが、アプリケーションの動作をリアルタイムで分析してゼロデイ脅威を検出しますか？
A. インサイトルックアップ
B. 侵入防止システム
C. SONAR（Symantec Online Network for Advanced Response）
D. 自動保護
正解: (正解を表示します)

質問: **8**
数千ものエンドポイントを抱える大規模企業向けにSEDR導入の規模を決定する際に、最も重要な考慮事項は何ですか？
A. SEPMと統合するエンドポイントの数
B. テレメトリデータの保存および保持のためのディスク容量
C. インターネット接続可能な物理的な拠点の数

D. DNS伝播遅延
正解: **(**正解を表示します**)**

質問: **9**
SEPMクライアントグループ内でのポリシー継承は、デフォルトではどのように機能しますか？
A. 子グループは継承されたポリシーをすべて自動的に上書きします
B. ポリシーは、クライアントが管理されていない場合にのみ継承されます。
C. ポリシーの継承は手動で有効にするまで無効になっています。
D. ポリシーは明示的に上書きされない限り、親グループから継承されます。
正解: **D (**コメントを発表する**)**

質問: **10**
SEP管理者が組織固有の侵入防止ルールを作成できる機能は何ですか？
A. ログ相関エンジン
B. ホストルックアップオーバーライド
C. Symantec Insight
D. カスタム署名設定
正解: **D (**コメントを発表する**)**

質問: **11**
SEPMとActive Directoryを統合することで得られる2つのメリットは何ですか？
（2つ選択）
A. 既存のOU構造に基づいた、より容易なポリシー割り当て
B. SEPMへのログイン用ユーザー認証情報の自動同期
C. SEPM内での手動クライアントグループ作成の削減
D. Active Directoryにおける不正デバイスのリアルタイム検出
正解: **(**正解を表示します**)**

質問: **12**
SEDRは、環境全体における脅威の根絶をどのように促進するのでしょうか？
A. 管理者がリモートで悪意のあるファイルを削除できるようにすることで
B. SEPライセンスを自動的に更新することで
C. メールベースのフィッシングシミュレーターを導入することで
D. Windowsイベントログ転送を有効にすることで
正解: **(**正解を表示します**)**

質問: **13**
EARデータをレビューする際、どのような行動が認証情報窃盗の強い兆候とみなされるでしょうか？

A. プロセスインジェクションでlsass.exeにアクセスする実行ファイル
B. アプリケーションがローカルの PDF ファイルを繰り返し開く
C. 一時インターネットキャッシュへのファイル作成
D. 勤務時間外にログインするユーザー
正解: **(**正解を表示します**)**

質問: **14**
SEPクライアントは、デフォルトではどのような方法でSEPMとの通信を開始しますか？
A. UDPベースのブロードキャスト
B. SEPMからのプッシュ通信
C. LiveUpdateによる手動同期
D. HTTPS経由のクライアント主導型ポーリング
正解: **(**正解を表示します**)**

質問: **15**
SEDRアプライアンスの設置における主要な考慮事項を最もよく表しているのはどれですか？
A. SEPクライアントからの遅延を最小限に抑えるようにサイズと配置を調整する必要があります。
B. SEPMと同じマシンにインストールする必要があります
C. インターネット経由での直接アップデートにはパブリックIPアドレスが必要です
D. Windows Server 2022にのみインストール可能です
正解: **(**正解を表示します**)**

質問: **16**
エンドポイント数を増やすことは、SEDRアーキテクチャ設計にどのような影響を与えるか？
A. SEPMとの統合を簡素化します
B. エンドポイント通信に必要なネットワークホップ数が少ない
C. CPU、RAM、ディスクI/Oなどのバックエンドリソースのスケーリングが必要です
D. クライアントマシンでより多くのメモリとCPUが必要になります
正解: **(**正解を表示します**)**

質問: **17**
SEDRのインシデント報告において、インシデントタイムラインはどのような役割を果たしますか？
A. ネットワークのパフォーマンスを時系列で表示します。
B. 日々のSEPポリシー遵守状況を表示します
C. 古いセキュリティ定義を強調表示します
D. 関連するすべての脅威イベントを時系列順に表示します
正解: **(**正解を表示します**)**

質問: **18**
Symantec Endpoint Detection and Response (SEDR) をインストールする前に必須となる前提条件はどれですか？
A. システムにはIntel vProテクノロジーが搭載されている必要があります。
B. Microsoft SQL Serverがインストールされている必要があります
C. ドメイングループポリシーオブジェクトを無効にする必要があります
D. SEPMサーバーが既に導入され、統合されている必要があります。
正解: **D (**コメントを発表する**)**

質問: **19**
セキュリティインシデントへの迅速かつ確実な対応を可能にする相関エンジンとは何ですか？
A. 懐疑論者
B. インサイト
C. シナプス
D. ソナー
正解: **(**正解を表示します**)**

質問: **20**
セキュリティイベントを分析する際、SEPMのログページの主な役割は何ですか？
A. スキャンスケジュールとポリシーを設定する
B. 管理対象クライアントすべてからのリアルタイムのインシデントデータを表示する
C. ライセンスとキャパシティプランニングを示す
D. 古いバックアップとスキャン定義をアーカイブする
正解: **(**正解を表示します**)**

質問: **21**

SEPMは、クライアントビューにおいてエンドポイントの健全性をどのように判断するのですか？
A. クライアントのスキャン結果をグローバル脅威データベースと比較することによって
B. クライアントデバイスのファイアウォールポートスキャンによる
C. LiveUpdateサーバーの応答に基づく
D. 定義、リスク検出、ポリシー遵守に関する情報を使用する
正解: **D** (コメントを発表する)

質問: **22**
SEDR環境において、ユーザー管理証明書はどのような役割を果たしますか？
A. SEDRと外部システム間の安全な通信を保証します。
B. デフォルトのSEPアンチウイルス署名を置き換えます
C. SEPMで管理者ロールを有効化します
D. ログアーカイブを安全に保管します
正解: (正解を表示します)

質問: **23**
SEDRによる効果的な脅威検出を確実にするために、SEPMではどのような設定を行う必要がありますか？
A. ログとテレメトリデータをSEDRアプライアンスに転送する
B. 自動保護スキャンのみを有効にする
C. デフォルトのドメイン管理者ロールを割り当てる
D. クライアントの整合性チェックを無効にする
正解: (正解を表示します)

質問: **24**
感染したメールメッセージに警告メッセージを挿入できる機能はどれですか？
A. インターネットメールのマルウェア対策
B. Microsoft Outlook 自動保護
C. Microsoft Exchange アンチマルウェア
D. インターネットメール自動保護
正解: (正解を表示します)

質問: **25**
SEDRインシデントレポートには通常、どのような重要なデータポイントが含まれますか？
A. SEPライセンスキー
B. エンドポイントのメモリ使用状況ログ
C. 関連するエンドポイント、脅威の深刻度、および推奨される対策
D. SEPMパッチバージョンの履歴

正解: **(**正解を表示します**)**

質問: **26**
SEP環境内のどのコンポーネントが、デフォルトでウイルス定義ファイルやその他のコンテンツをクライアントにダウンロードして配布する役割を担っていますか？
A. グループアップデートプロバイダー (GUP)
B. LiveUpdate管理者（LUA）
C. インサイトクラウド
D. SEPM
正解: **(**正解を表示します**)**

質問: **27**
Symantec Endpoint Detection and Responseソリューションの主要な構成要素を2つ挙げてください。
（2つ選択）
A. インシデントマネージャー
B. シマンテックメールセキュリティクラウド
C. エンドポイントアクティビティレコーダー
D. Active Directory フェデレーション サービス
正解: **(**正解を表示します**)**

質問: **28**
SEPエミュレータは脅威検出にどのように貢献するのでしょうか？
A. 安全な環境でファイル実行をシミュレートすることにより、難読化されたマルウェアを検出します。
B. インストール前にシステムドライバを確認する
C. 未知のアプリケーションをすべてブロックすることで
D. 毎日フルシステムスキャンを実行する
正解: **(**正解を表示します**)**

質問: **29**
SEDRのどのコンポーネントが、インシデント対応のために脅威関連の活動やシステム動作に関する詳細な情報を提供しますか？
A. 事件詳細ページ
B. SEPポリシー検査官
C. エンドポイントヘルスダッシュボード
D. SEPコンテンツマネージャー
正解: **A (**コメントを発表する**)**

質問: **30**

SEDRのどの機能を使えば、セキュリティチームは時間の経過とともに検出精度を向上させることができますか？
A. 定期ライセンス監査
B. ルール設定とノイズ低減による環境調整
C. MACアドレスのホワイトリスト登録
D. オンデマンドSEPポリシー再生
正解: **B** (コメントを発表する)

質問: **31**
事業に影響を与える可能性のある事案は、どの程度の優先順位で対応されるべきでしょうか？
A. 低
B. 高
C. 中
D. クリティカル
正解: (正解を表示します)

質問: **32**
管理者は、システムロックダウンで使用するファイルフィンガープリントリストをどのように生成できますか？
A. SEPクライアントから指紋エクスポートを実行する
B. 「SymDiag」ツールを使用するSEPクライアントから
C. SEPMからスキャンログをエクスポートする
D. クライアント展開ウィザードの使用
正解: (正解を表示します)

質問: **33**
大規模環境におけるコンテンツ配信時の帯域幅消費量を削減するために、管理者はどのような2つの方法を利用できますか？
（2つ選択）
A. 差分コンテンツアップデートを展開する
B. グループ更新プロバイダー（GUP）を使用する

C. クライアントがインターネットから直接アップデートを取得するように設定する
D. 保存されているコンテンツの改訂回数を増やす
正解: **(**正解を表示します**)**

質問: **34**
スキャンが日常業務に支障をきたさないように、特定のファイルやフォルダを様々なスキャン対象から除外する機能はどれですか？
A. スキャンオーバーライド
B. 例外
C. 許可リスト
D. セキュリティオーバーライド
正解: **(**正解を表示します**)**

質問: **35**
SEPMのどの機能を使用すると、管理者は脅威活動、ポリシー遵守状況、およびシステムステータスのグラフによる要約を生成できますか？
A. レポートページ
B. コマンドステータス
C. 概要ダッシュボード
D. システムログ
正解: **(**正解を表示します**)**

質問: **36**
SEDRにおけるファイル削除コマンドのタイムアウト時間はどれくらいですか？
A. 2日間
B. 72時間
C. 7日間
D. 5日間
正解: **(**正解を表示します**)**

質問: **37**
Splunkとの連携によるイベント分析を可能にするには、SEDRでどのような設定を行う必要がありますか？
A. カスタムDNSルール
B. SEPコンテンツレプリケーター
C. syslog転送プロファイル
D. ネットワークパケットスニファ
正解: **C (**コメントを発表する**)**

質問: **38**

SEDRは、脅威対応能力を強化するために、どのような2つの利点を提供しますか？
（2つ選択）
A. イベントタイムラインの再構築
B. リモートデバイスのパッチ適用
C. メールスパムフィルタリング
D. 横方向の動きの検出
正解: **A,D** (コメントを発表する)

質問: **39**
SEPMがコンテンツ更新プロセスの一環として定期的にダウンロードおよび配信するコンテンツの種類は何ですか？
A. Windowsのアップデートとシステムドライバー
B. ライセンスデータとユーザー認証ログ
C. アプリケーションインストーラーとエージェントバイナリ
D. ウイルス定義、IPSシグネチャ、およびレピュテーションデータ
正解: (正解を表示します)

質問: **40**
SEP管理者は、顧客が別の地域ベースのポリシーに切り替えるべきタイミングをどのように定義すればよいのでしょうか？
A. SEPMでロケーション切り替え条件を設定することにより
B. LiveUpdateポリシーを更新することにより
C. クライアントを新しいグループに割り当てることで
D. ユーザーの役割を変更することによって
正解: (正解を表示します)

質問: **41**
SEPMで、ヘルスレポートやリスクレポートを定期的に自動送信するには、どのような設定が必要ですか？
A. レポートデータベースのインデックス作成
B. ロールベースのアクセス制御
C. 定期レポート
D. 日次サマリーログローテーション
正解: (正解を表示します)

質問: **42**
監視対象のエンドポイントで不審な活動が行われている可能性を示す条件はどれですか？
A. ファイアウォールログを無効化
B. 記憶における予期せぬ親子関係
C. ポリシーのダウンロードが多数繰り返されている

D. SEPMへの認証に失敗しました
正解: **B** (コメントを発表する)

質問: **43**
どのオプションを使用すると、SEP管理者は特別なネットワークアクセスルールを必要とするアプリケーションに対して例外を設定できますか？
A. 位置情報認識設定
B. ホスト整合性チェック
C. 適用規則条件
D. Insight Overridesをダウンロード
正解: **C** (コメントを発表する)

質問: **44**
SEPは、Windowsエンドポイントにダウンロードされたファイルに含まれるゼロデイ脅威をどのように検出し、修復するのですか？
A. すべてのファイルをSEPM隔離環境に転送します
B. ファイル拡張子フィルターのみを使用します
C. SONAR、Insight Reputation、およびDownload Insightを組み合わせてリスクを評価します。
D. 不明なソースからダウンロードされたすべてのファイルをブロックします。
正解: (正解を表示します)

質問: **45**
企業セキュリティ戦略において、SEPデバイス制御を使用する2つの利点は何ですか？
（2つ選択）
A. USBストレージを介した不正なデータ流出を防止します
B. データ保護ポリシーへの準拠を保証します
C. ハードウェアレベルの証明書を使用してUSBデバイスを暗号化します。
D. 悪意のあるURLを自動的にブロックします
正解: (正解を表示します)

質問: **46**
SEPMでコンテンツ配信を監視する際に確認できる情報は、次のうちどれですか？
（2つ選択）
A. クライアントのスケジュール済みスキャン履歴
B. クライアントマシンの総ストレージ容量
C. クライアントの最終コンテンツ更新成功時刻
D. クライアント上のウイルス定義ファイルのバージョン番号
正解: **C,D** (コメントを発表する)

質問: **47**
SEPのどの機能を使用すると、管理者は特定のファイル、フォルダ、またはアプリケーションを保護技術によるスキャンやブロックから除外できますか？
A. アプリケーション制御
B. ライブアップデートコンテンツの例外
C. セキュリティ例外
D. ホスト整合性ポリシー
正解: **(**正解を表示します**)**

質問: **48**
SEPのメモリエクスプロイト対策によって一般的に検出および軽減されるエクスプロイト手法はどれですか？ 2つ挙げてください）
2つ選択）
A. 山積みスプレー
B. DNSトンネリング
C. メールフィッシング
D. シェルコードインジェクション
正解: **(**正解を表示します**)**

質問: **49**
SEPMのどの機能が、感染拡大の検出やポリシー違反などの特定のセキュリティイベントについて管理者に警告するために使用されますか？
A. リスクログ
B. 通知条件
C. 複製スケジュール
D. コマンドキュー
正解: **(**正解を表示します**)**

質問: **50**
ウイルス定義を含む.jdbファイルを処理するために、SEPMサーバー上のどのディレクトリが使用されますか？

A. \Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\content\incoming
B. /ProgramData/Symantec/SEPM/LiveUpdate/Temp
C. /SEPM/Logs/Upload
D. \Symantec\Tools\Backup\LiveDef
正解: **(**正解を表示します**)**

質問: **51**
SEPMにウイルス定義ファイルを手動でインストールする際によく使用されるファイル拡張子は何ですか？
A. .sar
B. .vdb
C. .jdb
D. .zip
正解: **C (**コメントを発表する**)**

質問: **52**
Symantec Endpoint Detection and Response (SEDR) は、データ処理とインシデント管理にどのようなアーキテクチャモデルを使用していますか？
A. 分散型ログ記録を備えたピアツーピアアーキテクチャ
B. エンドポイントキャッシングを備えたハブアンドスポークアーキテクチャ
C. ストレージノードを統合したクライアント/サーバーモデル
D. 分散エージェントを備えた集中型データレイク
正解: **D (**コメントを発表する**)**

質問: **53**
SEDR環境におけるデータ保持期間に最も影響を与える要因は何ですか？
A. システムイメージのサイズ
B. LiveUpdate定義の頻度
C. 展開されたポリシーの数
D. エンドポイントごとに生成されるテレメトリデータの量
正解: **(**正解を表示します**)**

質問: **54**
SEDRとSEPMの統合が成功した場合、EDR機能を強化するために共有される2つのデータストリームはどれですか？
（2つ選択）
A. エンドポイントスキャンログ
B. ポリシー遵守違反
C. テレメトリデータとイベントメタデータ

D. パッチ展開スケジュール
正解: **(**正解を表示します**)**