Symantec.250-586.v2025-01-07.q27

試験コード:	250-586
試験名称:	Endpoint Security Complete Implementation - Technical Specialist
認定資格:	Symantec
無料問題数:	27
バージョン:	v2025-01-07
アクセス数:	333
ページビュー数:	270
https://www.jpnpdf.com/Symantec.250-586.v2025-01-07.q27-mondaishu.html	

最新問題: **1**
敵対者が環境内の既存のツールを活用するときに使用される用語または表現はどれですか?
A. 土地で暮らす
B. 好機を狙った攻撃
C. ファイルレス攻撃
D. スクリプトキディ
Answer: A (メーッセージを残す**)**
サイバーセキュリティにおいて、「living off the land (LOTL)」という用語は、攻撃者がターゲットの環境内にすでに存在する正当なツールやソフトウェアを使用して悪意のあるアクティビティを実行することを指します。このアプローチにより、攻撃者はエンドポイントセキュリティ ソリューションによってフラグが付けられる可能性のある新しい疑わしいファイルを持ち込む代わりに、信頼できるアプリケーションを使用して検出を回避できます。
* 定義と使用状況コンテキスト「living off the land」とは、通常、管理目的または正当な目的でインストールされるツール、ユーティリティ、およびスクリプト環境を活用する方法です。攻撃者は、可視性を最小限に抑え、外部または悪意のある実行可能ファイルの認識に依存するエンドポイント検出メカニズムのトリガーを回避するために、このアプローチを好みます。PowerShell、Windows Management Instrumentation (WMI)、およびコマンドライン ユーティリティ (例: cmd.exe) などのツールは、この戦略を使用する攻撃者によく使用されます。
* エンドポイント セキュリティの完全な実装における戦術エンドポイント セキュリティの完全な実装フレームワークでは、エンドポイント ソリューションが標準管理ツールの正当な使用と誤用を監視して区別する必要があるコンテキストで、LOTL が特に認識されています。このアプローチは、エンドポイント セキュリティ実装の検出および防止フェーズで

文書化されることが多く、コマンドライン アクティビティの監視、PowerShell の使用の監査、およびこれらのツールに関連する異常な動作の特定に特に重点が置かれています。
* 影響と軽減LOTL は、セキュリティ ソリューションが既存のツールの正当な使用と悪意のある使用を区別する必要があるため、検出作業を複雑にする可能性があります。Symantec Endpoint Security Complete は、動作ベースの分析、異常検出、機械学習モデルを使用して、新しいファイルが導入されていない場合でも異常なパターンにフラグを立てることで、これに対処します。
* SES Complete ドキュメントの関連リファレンスSymantec Endpoint Security Complete 内での LOTL 戦術への対処に関する詳細なガイダンスは、脅威ハンティングと動作分析に関するドキュメントのセクションによく記載されています。これらのリソースでは、ネイティブ OS ツール内の疑わしい使用パターンにフラグを立て、テレメトリ データと既知の侵害指標 (IoC) を活用して早期検出を行うようにプラットフォームがどのように設計されているかを概説しています。

最新問題: **2**
Symantec Communities プラットフォームは何を提供しますか?
A. 専門家、エキスパート、愛好家にアクセスして、議論、協力、知識の共有が可能
B. 最新の製品ドキュメント、ダウンロード、サポート情報へのアクセス
C. マイエンタイトルメントリストへのアクセス
D. カスタマーサポートインシデントへのアクセス
Answer: A (メーッセージを残す**)**
Symantec Communities プラットフォームは、専門家、エキスパート、愛好家が議論、協力、知識の共有を行えるようにアクセスを提供します。このプラットフォームでは、ユーザーはサイバーセキュリティ分野の他のユーザーとつながり、Symantec 製品に関する洞察、ベスト プラクティス、ソリューションを交換できます。このプラットフォームは、ユーザーが支援を受け、経験を共有し、最新の開発状況を把握できる共同作業環境を促進します。
Symantec Endpoint Security ドキュメントでは、トラブルシューティング、ネットワーキング、サイバーセキュリティのトピックと Symantec ツールに関する知識の拡大に役立つ共同フォーラムとしての Symantec コミュニティについて説明しています。

最新問題: **3**
実装フェーズで SES Complete Base アーキテクチャを実装した後の次のステップは何ですか?
A. 論理設計を実装する
B. Symantec Security Cloud ページにサインイン
C. 管理者アカウントを作成する
D. エンドポイントの登録と配布
Answer: (解答を表示する**)**
実装フェーズで SES Complete ベース アーキテクチャを実装した後、次の重要なステップはエンドポイントの登録と配布です。このステップでは、エンドポイント デバイスをセ

キュリティ環境に登録し、必要なセキュリティ エージェントをデバイス全体に配布します。適切な登録と配布により、エンドポイントが登録され、ポリシーが適用され、SES Complete ソリューションによる保護が開始されます。
SES 完全実装カリキュラムでは、エンドポイントを管理下に置き、完全なポリシー適用と脅威保護機能を有効にするために、基本アーキテクチャのセットアップに従う構造化されたプロセスとしてこれを説明しています。

最新問題: **4**
Symantec Endpoint Protection Manager (SEPM) 実装でホスト グループを使用できる 2 つの領域はどれですか? (2 つ選択してください。)
A. アプリケーションとデバイスの制御
B. ファイアウォール
C. 場所
D. IPS
E. Insight をダウンロード
Answer: B,D (メッセージを残す**)**
Symantec Endpoint Protection Manager (SEPM) 実装では、ファイアウォールおよび侵入防止システム (IPS) 内でホスト グループを使用できます。ホスト グループを使用すると、管理者はファイアウォールおよび IPS ポリシーで参照できる IP アドレスまたはドメインのセットを定義できるため、指定されたホストまたはネットワーク全体に一貫したセキュリティ制御を適用しやすくなります。
Symantec Endpoint Protection ドキュメントでは、ホスト グループの使用法を指定してポリシー管理を効率化し、SEPM のファイアウォールおよび IPS 構成内でネットワーク セキュリティ対策のためのルールを効率的かつ組織的に適用できるようにします。

最新問題: **5**
セキュリティアナリストロールにはどのような権限がありますか?
A. エンドポイントを検索し、ダンプをトリガーし、ポリシーを作成します
B. ダンプをトリガーし、ファイルを取得して隔離し、新しいサイトを登録する
C. エンドポイントを検索し、ダンプをトリガーし、ファイルを取得して隔離する
D. ダンプをトリガーし、ファイルを取得して隔離し、デバイス グループを作成します。
Answer: C (メッセージを残す**)**
Endpoint Security Complete 実装では、セキュリティ アナリスト ロールには通常、ポリシー作成やデバイス グループ管理などの管理機能ではなく、セキュリティ脅威の監視、調査、対応に重点を置いた権限が与えられます。オプション C がベスト プラクティスと一致する理由を次に示します。
* エンドポイントの検索: セキュリティ アナリストは、セキュリティ警告や異常の調査を担当することがよくあります。
これをサポートするには、通常、潜在的な脅威の影響を受ける特定のデバイスを見つけるためにエンドポイント検索機能にアクセスする必要があります。

* トリガー ダンプ: エンドポイントでメモリまたはシステム ダンプをトリガーすることは、詳細なフォレンジック分析に不可欠です。これにより、アナリストはセキュリティ インシデント発生中または発生後にシステムの状態のスナップショットをキャプチャし、包括的な調査を行うことができます。
* ファイルの取得と隔離: セキュリティ アナリストは、疑わしい、または悪意があると判断されたファイルを隔離または隔離する権限を与えられることがよくあります。このアクションは、潜在的な脅威を封じ込め、ネットワーク内でのマルウェアやその他の有害なアクティビティの拡散を防ぐのに役立ちます。この権限は、脅威をできるだけ早く軽減するというセキュリティ アナリストの役割と一致しています。
他の選択肢の可能性が低い理由の説明:
* オプション A (ポリシーの作成): ポリシーを作成するには、通常、セキュリティ アナリストではなく、セキュリティ管理者やエンドポイント マネージャーに割り当てられるような、より高い管理権限が必要です。
アナリストは、ポリシーの設計よりも、脅威の検出と対応に主に焦点を当てます。
* オプション B (新しいサイトの登録): 新しいサイトの登録は通常、インフラストラクチャのセットアップと拡張に関連する管理タスクであり、セキュリティ アナリストの責任範囲外です。
* オプション D (デバイス グループの作成): デバイス グループの作成と管理は、エンドポイント管理システムの組織構造の構成を伴うため、通常はシステム管理者またはエンドポイント管理者の役割の範囲内です。
要約すると、オプション C は、脅威の調査と対応に重点を置くセキュリティ アナリストの中心的な責任と一致します。その権限は、管理構成やセットアップ タスクにまで及ぶことなく、これらの目的を直接サポートするアクションに重点を置いています。

最新問題**: 6**
シマンテック製品で検出されないマルウェアの証拠はどこに提出できますか?
A. SymProtect ケース ページ
B. ウイルス定義とセキュリティ更新ページ
C. SymSubmit ページ
D. シマンテック脆弱性対応ページ
Answer: C (メーッセージを残す**)**
SymSubmit ページは、シマンテック製品で検出されなかったマルウェアの証拠を送信するための専用プラットフォームです。このプロセスにより、シマンテックは送信内容を分析し、定義や検出技術を更新できる可能性があります。
* SymSubmit の目的: このページは、新しい脅威や未検出の脅威となる可能性のある、顧客が送信したファイルを処理する目的で特別に設定されており、これによりシマンテックはマルウェア検出機能を向上させることができます。

* 提出プロセス: ユーザーは、疑わしいマルウェアのファイル、URL、または詳細な説明を提出することができ、シマンテックのセキュリティ チームがこれらの提出内容を確認して、将来のアップデートに含めるかどうかを検討します。
* 検出の改善: 検出されていないマルウェアを提出することで、組織はシマンテックが最新の脅威インテリジェンスを維持するのに協力し、すべてのユーザーの保護を強化できます。
他の選択肢の可能性が低い理由の説明:
* オプション A (SymProtect ケース ページ) は、マルウェアの提出を目的としたものではありません。
* オプション B (ウイルス定義およびセキュリティ更新ページ) は、送信プラットフォームではなく、更新を提供します。
* オプション D (Symantec 脆弱性対応ページ) は、マルウェアではなくソフトウェアの脆弱性の報告に重点を置いています。
検出されていないマルウェアを送信する正しい場所は、SymSubmit ページです。

最新問題: **7**
Symantec Security クラウドコンソールで複数のドメインを使用する目的は何ですか?
A. 複数のドメインにまたがるデータを結合する
B. 管理者が他のドメインのデータを閲覧または管理できないようにする
C. データを物理的に分離したまま複数の独立したエンティティを管理する
D. 共通のユーザーグループに 1 つ以上の Symantec クラウド製品へのアクセスを提供する
Answer: (解答を表示する**)**
Symantec Security Cloud Console では、複数のドメインを使用することで、組織はデータの分離と独立性を確保しながら、単一の環境内で個別のエンティティを管理できます。この構造は、個別の管理制御とデータ境界を必要とする、明確な業務部門、子会社、または独立した部門を持つ組織にとって有益です。
Symantec Endpoint Security ドキュメントでは、複数のドメインがエンティティ間でデータのプライバシーを維持し、アクセス管理を安全に行う方法、各ドメインがクロスオーバーすることなく独立して動作し、データ分離ポリシーに準拠できるようにする方法について説明しています。

最新問題: **8**
Symantec Endpoint Security 実装における LiveUpdate Administrator (LUA) サーバーの目的は何ですか?
A. クラウドコンソールからクライアントにコンテンツを直接ダウンロードする
B. エージェントとセキュリティコンテンツの更新の負荷を軽減する
C. ネットワーク内の他のピアにポリシーコンテンツを配布する
D. イベント更新のフェイルオーバーサポートを提供する
Answer: B (メーッセージを残す**)**

Symantec Endpoint Security 実装における LiveUpdate Administrator (LUA) サーバーの目的は、エージェントとセキュリティ コンテンツの更新をプライマリ管理サーバーからオフロードすることです。LUA サーバーは、Symantec のクラウドから更新とコンテンツ (ウイルス定義やセキュリティ パッチなど) をダウンロードし、ネットワーク内のエンドポイントに配布します。このアプローチにより、管理サーバーの帯域幅と負荷が軽減され、エンドポイントが大規模または分散している環境での全体的な効率が向上します。
Symantec Endpoint Protection のドキュメントでは、特に最適化された帯域幅と集中的な更新制御を必要とする複雑なネットワーク環境でコンテンツ更新を管理するための重要なコンポーネントとして LUA について説明しています。

最新問題: **9**
信頼できるアプリケーションによって実行される疑わしい動作を管理することで、攻撃対象領域を減らすように設計された機能はどれですか?
A. マルウェア防止設定
B. 適応型保護
C. ホスト整合性構成
D. ネットワーク整合性構成
Answer: B (メーッセージを残す**)**

最新問題: **10**
SEP マネージャーの Microsoft SQL データベースが復元された直後に実行する必要があることは何ですか?
A. SEPマネージャでSymantecサービスを再起動します
B. SQLデータベースを消去する
C. 管理対象クライアントのフェイルオーバーをトリガーする
D. SQLデータベースを複製する
Answer: A (メーッセージを残す**)**
Symantec Endpoint Protection (SEP) マネージャの Microsoft SQL データベースを復元した後は、SEP マネージャで Symantec サービスをすぐに再起動することが重要です。この手順により、SEP マネージャはデータベースへの接続を再確立し、通常の操作を再開します。サービスの再起動は、SEP マネージャが新しく復元されたデータベースを認識して使用できるようにするために重要であり、すべてのエンドポイントが引き続き正しく機能し、保護状態を維持できるようにします。
Symantec Endpoint Protection のドキュメントでは、潜在的なデータ同期の問題を回避し、シームレスな操作の継続性を確保するために、データベースの復元後に必要なアクションとしてサービスを再起動することが指定されています。

最新問題: **11**
Active Directory の不正アカウントに対する脅威防御の目的は何ですか?

A. ワークステーションのメモリから認証情報を収集しようとする攻撃者を危険にさらします。
B. 攻撃者がAD宝の地図を作成しようとするときに、ハニーポットとして機能します。
C. 攻撃者がドメイン管理者グループの内容を読み取ることを防ぎます
D. AdminCount 属性が割り当てられたユーザーに偽の NTLM パスワード ハッシュ値を割り当てます。
Answer: A (メーッセージを残す)
Active Directory の偽アカウントに対する脅威防御の目的は、ワークステーションのメモリから資格情報を収集しようとする攻撃者を摘発することです。これらの偽アカウントは、正当な資格情報に似せて作られていますが、実際には、管理者に悪意のあるアクティビティを警告する罠です。攻撃者がこれらの偽の資格情報にアクセスしようとすると、資格情報を収集しようとする不正な試みの可能性が示され、セキュリティ チームがこれらの侵入を積極的に検出して対応できるようになります。
SES の完全なドキュメントでは、プロアクティブな防御戦略の一環として偽のアカウントを使用する方法について説明します。偽の認証情報が脆弱な領域に埋め込まれ、ネットワーク内での攻撃者の動きを捕捉して追跡します。

最新問題: **12**
SES 完全ソリューション設計のどのセクションに、実装される機能の概要が記載されていますか?
A. インフラストラクチャ設計
B. 構成設計
C. 初期テスト計画
D. 概要
Answer: D (メーッセージを残す)
SES Complete ソリューション設計のエグゼクティブ サマリー セクションでは、実装する機能の概要を示します。このサマリーは、利害関係者と意思決定者向けにカスタマイズされており、技術的な詳細には触れずに、ソリューションの機能、主要な機能、および意図する成果の概要を示します。これは、SES Complete ソリューションの価値と戦略的メリットを組織に伝えるのに役立ちます。
SES の完全な実装ドキュメントでは、ソリューションの範囲と予想される影響を経営陣や非技術系の利害関係者に伝えるための重要なセクションとして、エグゼクティブ サマリーが強調されています。

最新問題: **13**
インフラストラクチャ設計の基本アーキテクチャ セクションでは何を提供しますか?
A. 選択された実装モデルのマッピング
B. エージェントインストールパッケージを一貫して確実に配信する方法
C. エンドポイント登録またはエージェントのインストールへのアプローチ
D. ソリューションのトポロジとコンポーネントの配置の図

Answer: (解答を表示する**)**
SES Complete のインフラストラクチャ設計の 基本アーキテクチャ」セクションでは、ソリューション トポロジとコンポーネント配置の視覚的なレイアウトが提供されます。このセクションは、ソリューションのさまざまなコンポーネントが環境全体にどのように分散されているかを理解するために不可欠であり、各コンポーネントの配置場所と相互接続方法を詳しく説明しています。この概要により、アーキテクチャの各部分が全体的なセキュリティ要件と展開モデルに一致するようにすることができます。
Symantec Endpoint Security ドキュメントの参照では、エンドポイント セキュリティ インフラストラクチャの効果的な導入、保守、および拡張性には、コンポーネントの配置とソリューション トポロジを明確に示すことが重要であると説明されています。

最新問題**: 14**
SEP Manager 管理のグループとポリシーをクラウド管理のグループとポリシーに永続的に変換するための最初の手順は何ですか?
A. クラウド コンソールからグループをクラウド管理に切り替えるコマンドを実行します。
B. グループがMy Company親グループからDefault親グループに移動したことを確認します。
C. エンドポイントの整理方法に基づいてデバイス グループを再作成します。
D. Symantec Endpoint Security からパッケージをインストールします
Answer: A (メーッセージを残す**)**
SEP マネージャー管理のグループとポリシーをクラウド管理に永続的に変換する最初の手順は、クラウド コンソールから グループをクラウド管理に切り替え」コマンドを実行することです。このコマンドは転送プロセスを開始し、以前は SEP マネージャーによってオンプレミスで管理されていたグループとポリシーをクラウド インターフェイスから制御できるようにします。この手順は、クラウド管理インフラストラクチャのプラクティスに合わせて管理責任をクラウドに移行するために重要です。
SES の完全なドキュメントの参照では、グループとポリシーをクラウド管理に移行する際の最初のアクションとしてのこのコマンドの重要性が強調されており、完全にクラウドベースの管理アプローチへのスムーズな移行を促進します。

最新問題**: 15**
SES Complete アーキテクチャにおけるテクノロジーのベストプラクティスに反する説得力のある理由は何でしょうか?
A. 分散管理モデルを実装する
B. SES完全コンポーネント制約を遵守する
C. IT管理チームの分布とポリシーを理解する
D. 強力なビジネス要件を満たすため
Answer: (解答を表示する**)**
状況によっては、SES Complete アーキテクチャのテクノロジのベスト プラクティスから逸脱することが、切実なビジネス要件を満たすために正当化される場合があります。これ

らの要件には、カスタム構成や従来とは異なる実装方法を必要とする特定のコンプライアンス要件、独自の運用ニーズ、または規制上の義務が含まれる場合があります。ベスト プラクティスは堅牢な基盤を提供しますが、重要なビジネス ニーズが標準的なテクノロジの推奨事項を上回る場合は、調整が必要になることがあります。
SES 完全実装カリキュラムでは、重要なビジネス目標を達成するために推奨アーキテクチャをカスタマイズして調整する必要がある場合でも、テクノロジ ソリューションをビジネス目標に合わせることの重要性を強調しています。

最新問題: **16**
プロジェクト終了会議中の最終タスクは何ですか?
A. チームの成果を認める
B. 最終文書を引き渡す
C. 契約の正式な承認を得る
D. 未解決のサポート活動とインシデントの詳細について話し合う
Answer: C (メーッセージを残す**)**
プロジェクト終了会議の最終タスクは、契約の正式な承認を得ることです。このステップは、プロジェクトの完了を正式に示し、すべての成果物が顧客の満足に応えたことを確認します。
* 正式な終了: 承認を得ることで、プロジェクトが合意どおりに実施されたことが文書で確認され、契約が正式に終了し、完了に関する相互合意が示されます。
* サポートへの移行: 承認を受け取ると、顧客は標準サポート サービスに移行され、プロジェクト チームの責任は正式に終了します。
他の選択肢の可能性が低い理由の説明:
* オプション A (成果の認識) とオプション D (サポート活動の議論) は貴重ですが、プロジェクトを確定させるものではありません。
* オプション B (ドキュメントの引き渡し) は、ラップアップの一部ですが、契約を正式に終了するものではありません。
したがって、正式な承認を得ることは、プロジェクト完了会議を終了するための最終かつ重要なタスクです。

最新問題: **17**

テスト プランにおける Active Directory 防御テストの焦点は何ですか?
A. AD ドメイン設定の難読化係数の検証
B. マルウェア防止の強度レベルのテスト
C. アプリケーション起動ルールがエンドポイントでのアプリケーションの実行と動作をブロックまたは許可していることを確認する
D. ネットワーク整合性構成のネットワーク脅威に対する保護を検証する
Answer: C (メーッセージを残す)
テスト プラン内の Active Directory 防御テストの焦点は、エンドポイント保護メカニズム、特にアプリケーション起動ルールの検証です。このテストでは、承認されたアプリケーションのみが実行を許可され、リスクのあるアプリケーションや疑わしいアプリケーションの動作がブロックされ、不正アクセスや悪意のあるソフトウェア アクティビティに対する Active Directory (AD) 防御がサポートされることを確認することに重点を置いています。テストの構成は次のとおりです。
* アプリケーション起動ルール: これらのルールは、エンドポイントで許可されるアプリケーションを規定し、許可されていないアプリケーションの実行を防止します。これらのルールを設定およびテストすることで、組織はアプリケーション レベルで攻撃ベクトルを制限し、AD リソースを防御できます。
* エンドポイントの動作制御: エンドポイントが AD ポリシーに従っていることを確認することが重要です。テストにより、AD 防御メカニズムがアプリケーションの動作を効果的に制御し、危険な操作に逸脱したりセキュリティ ポリシーに違反したりしないようにすることができます。
* AD 防御における役割: この特定のテストは、ディレクトリ サービスの整合性を保護するアプリケーション制御手段に重点を置くことで、AD 防御をサポートします。
他の選択肢の可能性が低い理由の説明:
* オプション A (AD ドメイン設定の難読化係数) は、通常、エンドポイント セキュリティ テストでは重点的に考慮されません。
* オプション B (マルウェア防止の強度レベル) は脅威防止に関連していますが、AD 防御とは特に関連していません。
* オプション D (ネットワーク整合性構成のネットワーク脅威) は、AD 防御ではなくネットワークに重点を置いています。
この領域におけるテスト プランの焦点は、アプリケーションの実行と動作を制御して、不正なアプリケーションや危険なアプリケーションから Active Directory を保護することにあります。

最新問題**: 18**
管理フェーズ中に使用中の機能の検証に関する情報はどこで確認できますか?
A. ソリューション インフラストラクチャ設計
B. ソリューション構成設計
C. テスト計画
D. ビジネスまたは技術目標

Answer: C (メーッセージを残す)
管理フェーズでは、使用中の機能の検証に関する情報はテスト プランに記載されています。このドキュメントでは、ソリューションの機能が期待どおりに動作していることを確認するための特定のテスト、基準、および方法について概説しています。
* テスト プランの検証目的: テスト プランでは、構成された各機能が正しく実行され、意図した目的を満たしていることを検証する手順を指定します。
* テスト結果のドキュメント: 結果のドキュメントも含まれており、これにより、すべての機能が機能し続け、運用環境の要件に準拠していることを確認できます。
他の選択肢の可能性が低い理由の説明:
* オプション A (ソリューション インフラストラクチャ設計) とオプション B (ソリューション構成設計) は、検証ではなくセットアップと構成に重点を置いています。
* オプション D (ビジネスまたは技術目標) は、機能の検証ではなく、目標の設定に使用されます。
したがって、テスト プランは、管理フェーズ中に使用中の機能/機能を検証するための正しい情報源となります。

最新問題: **19**
評価フェーズの計画段階での内部計画コールの目的は何ですか?
A. 最近の課題を確認する
B. 重要な項目について議論する
C. 顧客情報を収集するため
D. クライアントの期待とコンサルタントの期待を一致させる
Answer: (解答を表示する)
評価フェーズの計画段階での内部計画コールの目的は、クライアントの期待とコンサルタントの期待を一致させることです。この一致は、コンサルティング チームとクライアントの両方がプロジェクトの目標、成果物、タイムライン、および潜在的な制約について相互理解を持つために不可欠です。明確な期待を設定することで誤解を最小限に抑え、範囲と目的がすべての関係者に完全に理解されていることを確認して、契約を成功させる基盤を提供します。
SES 完全実装カリキュラムでは、協力的で透明性のある作業関係を確立するためのこのステップの重要性を強調し、それによって実装のその後のフェーズの有効性を高めます。

最新問題: **20**
そもそもセキュリティ侵害の発生を防ぐために設計されたテクノロジーはどれですか?
A. ネットワークファイアウォールと侵入防止
B. ホスト整合性の防止
C. エンドポイント検出と応答
D. 脅威ハンター
Answer: A (メーッセージを残す)

ネットワーク ファイアウォールと侵入防止テクノロジーは、保護バリアを作成し、ネットワーク トラフィックを積極的に監視して潜在的な脅威を検出することで、セキュリティ侵害が最初から発生しないようにするように設計されています。ファイアウォールは不正アクセスを制限し、侵入防止システム (IPS) は悪意のあるアクティビティをリアルタイムで検出してブロックします。これらを組み合わせることで、攻撃がネットワークに侵入する前に阻止するプロアクティブな防御が実現します。
Symantec Endpoint Security ドキュメントは、さまざまな種類のセキュリティ侵害を防ぎ、ネットワーク レベルで重要な保護を提供する最前線の防御としてのファイアウォールと IPS の役割をサポートします。

最新問題: **21**
実装フェーズにおけるパイロット展開の主な目的は何ですか?
A. 顧客の環境におけるソリューション設計の有効性を検証する
B. 主要コンポーネント間の通信パスが確立されていることを確認する
C. 潜在的な未解決の活動やタスクが適切な人に割り当てられていることを確認する
D. すべてのアカウントに割り当てられた権限と割り当てが設定されていることを確認する
Answer: A (メーッセージを残す**)**
実装フェーズにおけるパイロット展開の主な目的は、顧客の環境でソリューション設計の有効性を検証することです。この段階は、実際の設定でソリューションをテストするために重要であり、実装チームは、展開が計画された目的を満たしていることを確認できます。
* 実際の条件での検証: パイロット展開では、実際の動作条件下でソリューションがどのように機能するかをテストし、完全な展開の前に必要なギャップや調整を特定します。
* ソリューションの微調整: パイロットからのフィードバックとパフォーマンス メトリックは、設定、ポリシー、構成を調整して、最適なセキュリティと使いやすさを確保するのに役立ちます。
* ユーザー受け入れテスト: このフェーズでは、エンド ユーザーと管理者がシステムを操作して、使いやすさや必要なトレーニングや調整についての洞察を得ることができます。
他の選択肢の可能性が低い理由の説明:
* オプション B (通信パスの確立) とオプション D (アカウント権限の設定) は予備的なタスクです。
* オプション C (タスクの割り当て) は、パイロット展開の主なテスト目的と一致しない管理手順です。
したがって、ソリューション設計の有効性を検証することが、パイロット展開の主な目的となります。

最新問題: **22**
SEP オンプレミス アーキテクチャに単一サイト設計を選択する理由は何ですか?
A. 地理的範囲
B. ログ保存に関する法的制約

C. 遅延のない集中レポート
D. WAN の使用を制御する
Answer: (解答を表示する**)**
SEP オンプレミス アーキテクチャの単一サイト設計は、遅延のない集中レポートが主な要件である場合によく選択されます。この設計では、すべてのデータ処理が単一の集中サーバー環境内で行われるため、データとレポートへのリアルタイム アクセスが可能になります。
* 集中データ アクセス: 単一サイトの設計により、複数サイトのレプリケーションや分散環境で発生する可能性のある遅延がなく、データがすぐに利用できるようになります。
* 効率的なレポート: すべてのログ、アラート、レポートが一元化されているため、管理者は迅速な対応と監視に不可欠なリアルタイム情報にすばやくアクセスできます。
他の選択肢の可能性が低い理由の説明:
* オプション A (地理的範囲) では、通常、複数のサイトの設定が優先されます。
* オプション B (ログ保持に関する法的制約) では、単一サイト設計によるメリットは特に得られません。
* オプション D (WAN 使用の制御) は、WAN トラフィック管理が必要な分散環境に適しています。
したがって、遅延のない集中レポートは、単一サイト設計を選択する主な理由です。

最新問題**: 23**
統合サイバー防御マネージャー (ICDm) は、顧客の物理的な住所に基づいて何を自動的に作成しますか?
A. サブワークスペース
B. テナント
C. ドメイン
D. LiveUpdate サーバー
Answer: (解答を表示する**)**
統合サイバー防御マネージャー (ICDm) は、顧客の物理的な住所に基づいてドメインを自動的に作成します。この自動ドメイン作成により、地理的または運用上の境界に従ってリソースを整理し、ポリシーを管理し、管理プロセスを合理化し、顧客の構造に合わせることができます。ドメインは、セキュリティ ポリシーと構成を管理するための ICDm 内の論理的な区分を提供します。
Symantec Endpoint Security ドキュメントでは、この自動ドメイン設定を ICDm の組織機能の一部として説明し、物理的または地域的な区別に基づいてリソース管理を強化します。

最新問題**: 24**
SES Complete は、展開オプションに関して顧客に何を提供しますか?
A. クラウドベースのみ
B. オンプレミスのみ

C. ハイブリッド、クラウドベース、オンプレミス
D. ハイブリッドまたはオンプレミスのみ
Answer: (解答を表示する**)**
SES Complete は、ハイブリッド、クラウドベース、オンプレミスの導入オプションをお客様に提供します。この柔軟性により、組織はインフラストラクチャ、セキュリティ ポリシー、運用上のニーズに最適な導入モデルを選択できます。ハイブリッド導入により、組織はオンプレミスとクラウドの両方のリソースを活用できますが、特定の要件や規制上の考慮事項に基づいて、完全にクラウドベースのモデルまたは完全にオンプレミスのモデルが優先される場合があります。
Symantec Endpoint Security ドキュメントでは、インフラストラクチャに関係なく最適化されたセキュリティ ソリューションを実現し、多様な顧客環境に適応できる導入オプションについて詳しく説明しています。

最新問題**: 25**
SES 完全ハイブリッド アーキテクチャにおける Cloud Bridge Connector の役割は何ですか?
A. TCP ポート 1443 を介して SQL Server データベースに接続するすべてのオンプレミス クライアントを管理します。
B. オンプレミスの SEP マネージャーと統合サイバー セキュリティ マネージャー間の通信を TCP ポート 443 経由で安全に同期します。
C. HTTP トラフィックの場合は TCP ポート 7070、SSL トラフィックの場合は 7078 で通信するエージェントおよびセキュリティ コンテンツの更新をオフロードします。
D. SEP クライアント上で保護スタックを構築するすべてのエンジンにコンテンツ更新を提供します。
Answer: B (メッセージを残す**)**
SES 完全ハイブリッド アーキテクチャでは、クラウド ブリッジ コネクタがオンプレミスとクラウド コンポーネント間の安全な通信を可能にする上で重要な役割を果たします。
* 同期ロール: Cloud Bridge コネクタにより、オンプレミスの Symantec Endpoint Protection (SEP) Manager はクラウド環境内の Integrated Cyber Security Manager と安全に通信し、データを同期できるようになります。
* TCP ポート 443 経由の安全な通信: コネクタは、機密性の高いセキュリティ データを送信し、オンプレミス環境とクラウド環境間の同期を維持するために不可欠な、安全な HTTPS 通信に TCP ポート 443 を使用します。
* ハイブリッド アーキテクチャのサポート: この同期機能は、オンプレミス リソースとクラウド リソースを組み合わせて連携し、統合されたセキュリティ ソリューションを提供するハイブリッド アーキテクチャでは不可欠です。
他の選択肢の可能性が低い理由の説明:
* オプション A (SQL Server を介してオンプレミス クライアントを管理する) は、Cloud Bridge Connector の機能とは無関係です。

* オプション C (TCP ポート 7070 および 7078 経由で更新をオフロードする) は、同期ではなく更新の配布に関係します。
* オプション D (SEP クライアントでコンテンツ更新を提供する) も、Cloud Bridge Connector の主な役割の範囲外です。
正解は、Cloud Bridge Connector は、オンプレミスの SEP Manager と Integrated Cyber Security Manager 間の通信を TCP ポート 443 経由で同期するために使用されます。

最新問題**: 26**
SE5 Complete の機能に必要な採用レベルを定義する際の主な焦点は何ですか?
A. 顧客の要件
B. 技術仕様
C. 規制遵守
D. 競合分析
Answer: A (メーッセージを残す**)**
SES Complete の機能に必要な採用レベルを定義する際の主な焦点は、顧客の要件です。このアプローチにより、セキュリティ機能の展開が顧客の特定のニーズと優先順位と一致することが保証されます。
* ビジネス ニーズとの整合: 顧客の要件に重点を置くことで、セキュリティ目標、運用上のニーズ、顧客の特定の環境に基づいて採用レベルが設定されます。
* カスタマイズされた実装: 導入レベルは、組織のリスク許容度、技術的状況、および戦略目標によって異なります。これらの固有の要件を満たすことで、ソリューションから最大限の価値を引き出すことができます。
他の選択肢の可能性が低い理由の説明:
* オプション B (技術仕様) とオプション C (規制遵守) は考慮事項ですが、採用レベルを定義するのではなくサポートします。
* オプション D (競合分析) は、通常、実装フレームワーク内の採用レベルの決定には関係ありません。
したがって、SES Complete で採用レベルを定義する際は、顧客の要件が主な焦点となります。

最新問題**: 27**
実装フェーズにおけるテスト計画の目的は何ですか?
A. 顧客の環境でSESCソリューション設計を評価する
B. SESの実装の完了を監視する
C. 実装フェーズでSES Completeの導入とテストをガイドする
D. SESC実施フレームワークの次のフェーズの承認を求める
Answer: C (メーッセージを残す**)**
Symantec Endpoint Security Complete (SESC) の実装フェーズでは、テスト プランは主に、顧客の環境内で SES Complete の導入を採用および検証するための構造化されたガイダンスを提供するように設計されています。手順を順を追って説明します。

* テスト プランの目的: テスト プランは、展開後にすべてのセキュリティ機能と構成が期待どおりに機能していることを確認します。ソリューションが意図したセキュリティ目標を満たし、顧客のインフラストラクチャと適切に統合されていることを確認するテスト手順を示します。
* SES Complete の導入: このフェーズには、多くの場合、SES Complete が顧客の既存の環境にどの程度統合されるかを評価し、問題に対処し、ユーザーと関係者が移行に備えていることを確認することが含まれます。
* 実装中の構造化テスト: テスト プランは、ソリューションを完全に運用する前にその機能をテストおよび検証するために不可欠です。これには、ソリューションを構成、テスト、微調整して顧客のセキュリティ要件に合わせ、次のフェーズへの準備を確実にすることが含まれます。
他の選択肢の可能性が低い理由の説明:
* オプションは、より広範なソリューション設計評価を指します。通常は、実装フェーズではなく設計フェーズで実行されます。
* オプション B は、テストのガイドではなく、実装後の監視に適しています。
* オプション D (次のフェーズの承認を求める) は、このフェーズのテスト プランの主な機能以外のプロジェクト管理タスクに関連します。
テスト プランの目的は、導入とテストのロードマップとして機能し、SES Complete ソリューションが要求どおりに機能することを保証することです。