Symantec.250-580.v2025-04-07.q56

試験コード:	250-580
試験名称:	Endpoint Security Complete - Administration R2
認定資格:	Symantec
無料問題数:	56
バージョン:	v2025-04-07
アクセス数:	472
ページビュー数:	560
https://www.jpnpdf.com/Symantec.250-580.v2025-04-07.q56-mondaishu.html	

最新問題: **1**
ネットワーク整合性を構成するときに、信頼できる証明書を追加することが必要なのはなぜですか?
A. セキュリティスキャンのためのエンタープライズSSL復号化を許可する
B. ICDmへの接続を保護するため
C. 信頼できるVPN接続を許可する
D. 攻撃者のMITMプロキシを回避する
Answer: (解答を表示する**)**
Symantec Endpoint Security でネットワーク整合性を構成する場合、セキュリティ スキャン用のエンタープライズ SSL 復号化を許可するために信頼できる証明書を追加することが不可欠です。これにより、暗号化されたトラフィックの検査が可能になり、SSL/TLS 通信における脅威や異常を識別するために重要になります。
* 信頼できる証明書の目的:
* 信頼できる証明書を追加すると SSL 復号化が容易になり、セキュリティ警告や接続の問題を引き起こすことなく、セキュリティ システムが暗号化されたデータ ストリームを分析することで潜在的な脅威を検出できるようになります。
* 他のオプションがあまり適用されない理由:
* ICDm への接続のセキュリティ保護 (オプション B) と VPN 接続のセキュリティ保護 (オプション C) は、Network Integrity の SSL 復号化への重点とは直接関係ありません。
* 攻撃者の MITM プロキシをバイパスする (オプション D) だけでは、ネットワーク整合性内の信頼できる証明書の機能には直接対応できません。
参考資料: SSL 復号化を有効にするには、信頼できる証明書を追加することが必要です。これは、Network Integrity での包括的なセキュリティ スキャンにとって重要です。

最新問題: **2**
SEDR 内でイベントはいつ生成されますか?

A. インシデントが選択された場合
B. アクティビティが発生したとき
C. いずれかのイベントが開かれたとき
D. エンティティが表示されるとき
Answer: B (メーッセージを残す)
Symantec Endpoint Detection and Response (SEDR) では、アクティビティが発生するとイベントが生成されます。これには、ファイルの変更、ネットワーク接続、潜在的な脅威を示す可能性のあるプロセスの起動など、システムによって検出されたすべてのアクションや動作が含まれます。アクティビティに応じてイベントが生成されることで、SEDR は、効果的な脅威の検出と対応に不可欠なリアルタイムの監視とログ記録を提供できます。

最新問題**: 3**
会社の管理者は、Symantec Endpoint Protection を構成するために 1 台の端末を共有しています。管理者は、コンソールを使用する各管理者が、各自の資格情報を使用して認証するようにしたいと考えています。管理者が端末からログオフするのを忘れると、他のユーザーが簡単に Symantec Endpoint Protection Manager (SEPM) コンソールにアクセスできるようになることを懸念しています。
権限のないユーザーが SEPM コンソールにログインするリスクを最小限に抑えるために、管理者はどの設定を無効にする必要がありますか?
A. ユーザーがログオン時に資格情報を保存できるようにする
B. 指定された時間接続されていないクライアントを削除します
C. 指定された回数のログオン失敗後にアカウントをロックします
D. 管理者がパスワードをリセットできるようにする
Answer: A (メーッセージを残す)
管理者がログオフを忘れた場合の不正アクセスのリスクを軽減するには、Symantec Endpoint Protection Manager (SEPM) で 「ログオン時にユーザーが資格情報を保存できるようにする」設定を無効にする必要があります。
このオプションを無効にすると、管理者は SEPM コンソールにアクセスするたびに資格情報を入力する必要があり、自動ログインが防止され、他のユーザーが許可なくアクセスする可能性が低くなります。
* 保存された資格情報を無効にする目的:
* 資格情報の保存を防止することで、SEPM は各管理者にセッションごとに手動で認証することを強制し、セキュリティを向上させます。
* この設定は、管理者がログアウトに失敗した場合にコンソールがログイン情報を保持しないようにするため、共有環境で特に役立ちます。
* 他のオプションがあまり重要でない理由:
* 接続されていないクライアントを削除する (オプション B) は、管理者ログインではなくエンドポイント クライアントに関係します。

* 失敗した後にアカウントをロックする (オプション C) は、ブルート フォース攻撃から保護しますが、保存された資格情報には対処しません。
* 管理者がパスワードをリセットできるようにする (オプション D) は、ログインの永続性ではなく、パスワード管理に関連しています。
参考: 保存された資格情報を無効にすることは、各セッションに固有のログインを強制し、共有コンソール環境のセキュリティを強化するためのベスト プラクティスです。

最新問題: **4**
Symantec Endpoint Protection クライアント マシンで生成されたボットネット コマンド アンド コントロール トラフィックを検出できる保護テクノロジはどれですか?
A. 洞察力
B. ソナー
C. リスクトレーサー
D. 侵入防止
Answer: (解答を表示する**)**
侵入防止は、Symantec Endpoint Protection 内の保護技術であり、ボットネットのコマンド アンド コントロール (C&C) トラフィックを検出できます。侵入防止は、ネットワーク トラフィック パターンを分析し、既知の C&C 通信特性を識別することで、ボットネット アクティビティを示す疑わしいネットワーク接続をブロックできます。
* 侵入防止がボットネットトラフィックを検出する方法:
* 侵入防止機能は、ボットネット C&C プロトコルに関連付けられたシグネチャの送信トラフィックと受信トラフィックを監視します。
* 既知の悪意のある IP またはドメインへの接続をブロックし、ボットネット クライアントとそのコントローラー間の通信を効果的に妨害します。
* 他のオプションが間違っている理由:
* Insight(オプション A) は、ネットワーク トラフィックではなくファイルのレピュテーションに重点を置いています。
* SONAR (オプション B) は、エンドポイント上の動作ベースの脅威を検出しますが、C&C トラフィックは特に検出しません。
* リスク トレーサー (オプション C) は検出された脅威のソースを特定しますが、ボットネット ネットワーク トラフィックを直接検出することはありません。
参考資料: 侵入防止は、ボットネットの C&C トラフィックを検出してブロックし、侵害されたエンドポイントが攻撃者と通信するのを防ぐための重要なコンポーネントです。

最新問題: **5**
ストレージ要件を計算するにはどのような情報が必要ですか?
A. エンドポイントの数、使用可能な帯域幅、使用可能なディスク容量、エンドポイント ダンプの数、ダンプ サイズ
B. エンドポイントの数、エンドポイントあたりの EAR データ数 (1 日あたり)、保持日数、エンドポイント ダンプの数、ダンプ サイズ

C. エンドポイントの数、使用可能な帯域幅、保持日数、エンドポイントダンプの数、ダンプサイズ
D. エンドポイントの数、エンドポイントあたりの EAR データ数 (1 日あたり)、使用可能なディスク容量、エンドポイント ダンプの数、ダンプ サイズ
Answer: (解答を表示する**)**
Symantec Endpoint Security (SES) のストレージ要件を計算するには、データ保持とイベント ストレージのニーズに関連する特定の情報を収集する必要があります。必要な情報は次のとおりです。
* エンドポイントの数:管理するデータの規模を決定します。
* 1 日あたりのエンドポイントあたりの EAR データ: 各エンドポイントによって毎日生成され、ストレージ使用量に影響するエンドポイント アクティビティ レコーダー (EAR) データを指します。
* 保持日数: 保存されるデータの総量に影響するデータ保持期間を示します。
* エンドポイント ダンプの数とダンプ サイズ: これらのパラメーターは、フォレンジック分析とトラブルシューティングに不可欠なメモリ ダンプのサイズと数を定義します。
この情報により、ストレージのニーズを正確に計算し、ログ、ダンプ、アクティビティ データに十分な容量を確保できます。

最新問題**: 6**
トラフィックの悪意のある通信パターンを検査するためにパケット レベルで実行されるセキュリティ制御はどれですか。
A. ネットワーク保護
B. 侵入防止
C. エクスプロイトの緩和
D. ファイアウォール
Answer: (解答を表示する**)**
侵入防止システム (IPS) はパケット レベルで動作し、トラフィックに悪意のある通信パターンがないか検査します。IPS はネットワーク パケットをリアルタイムで分析し、事前に定義されたシグネチャと動作ルールに基づいて潜在的に有害なトラフィックを識別してブロックします。
* パケットレベルでのIPSの機能:
* IPS は、ネットワークに入るパケットを検査し、既知の攻撃シグネチャや疑わしい動作のパターンと比較します。このパケット レベルの検査は、SQL インジェクションやクロスサイト スクリプティングなどのさまざまな攻撃を防ぐのに役立ちます。
* 他のオプションが間違っている理由:
* ネットワーク保護 (オプション A) はより広いカテゴリであり、必ずしもパケット検査に固有のものではありません。
* エクスプロイト緩和 (オプション C) は、パケット レベルのトラフィック分析ではなく、アプリケーションのエクスプロイトの防止に重点を置いています。

* ファイアウォール (オプション D) はルールに基づいてトラフィック フローを制御しますが、IPS ほど包括的にパケットの悪意のあるパターンを検査しません。
参照: 侵入防止機能は、シマンテックのセキュリティ フレームワークに不可欠なパケット レベルの保護を提供し、ネットワークベースの攻撃から保護します。

最新問題: **7**
クライアントが指定されたソースからコンテンツをダウンロードしていることを示すクライアント ログはどれですか?
A. リスクログ
B. システムログ
C. SesmLu.log
D. ログ.ライブアップデート
Answer: D (メーッセージを残す**)**
Log.LiveUpdate ログには、Symantec Endpoint Protection (SEP) クライアントのコンテンツのダウンロードに関連する詳細が表示されます。このログには、次のような更新に関連するアクティビティが記録されます。
* コンテンツ ソース情報: クライアントが更新をダウンロードするソース (SEPM、グループ更新プロバイダ (GUP)、または LiveUpdate サーバーから直接) を記録します。
* ダウンロードの進行状況とステータス: このログは、ダウンロードの成功または失敗、およびダウンロードされたコンテンツのバージョンの詳細を管理者が監視するのに役立ちます。
Log.LiveUpdate を確認することで、管理者はクライアントが指定されたソースからコンテンツを正しくダウンロードしているかどうかを確認できます。

最新問題: **8**
IPS を補完し、ネットワーク攻撃に対する第 2 層の保護を提供するセキュリティ制御はどれですか。
A. ファイアウォール
B. ホスト整合性
C. ネットワーク保護
D. マルウェア対策
Answer: A (メーッセージを残す**)**

最新問題: **9**
発行されたデバイス コマンドの進行状況を追跡するには、管理者はどのデバイス ページを表示する必要がありますか?
A. コマンド履歴
B. アクティビティの更新
C. コマンドステータス
D. 最近のアクティビティ

Answer: (解答を表示する**)**
コマンド ステータス ページは、管理者が Symantec Endpoint Security で発行されたデバイス コマンドの進行状況を追跡する場所です。このページには次の情報が表示されます。
* リアルタイムコマンド更新: 保留中」などのコマンドの現在のステータスを表示します。 完了」または 失敗」と表示され、コマンドの実行に関する即時の洞察が提供されます。
* 詳細な進行状況の追跡: コマンド ステータス ログには各コマンドの詳細が記載されているため、管理者はスキャン、更新、再起動などのアクションがエンドポイントによって正常に処理されたことを確認できます。
コマンド ステータス ページは、管理者が発行したコマンドの結果を監視および検証するのに役立つため、効果的なデバイス管理に不可欠です。

最新問題**: 10**
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. 好機を狙った攻撃
B. ファイルレス攻撃
C. スクリプトキディ
D. 土地で暮らす
Answer: D (メーッセージを残す**)**
Living off the land (LOTL) は、攻撃者が環境内の既存のツールやリソースを悪意のある目的で利用する戦術です。このアプローチでは、新しい検出可能なマルウェアを導入する必要性が最小限に抑えられ、代わりにネットワーク上にすでに存在する信頼できるシステム ユーティリティとソフトウェアが使用されます。
* 土地で暮らすことの特徴:
* LOTL 攻撃は、PowerShell や Windows Management Instrumentation (WMI) などの組み込みユーティリティを利用して、従来のマルウェア防御をトリガーせずに悪意のある操作を実行します。
* この方法はステルス性が高く、使用されるツールがオペレーティング システムの正規のコンポーネントであるため、署名ベースの検出を回避できる場合が多くあります。
* 他のオプションが間違っている理由:
* 機会主義的攻撃 (オプション A) とは、内部リソースを使用するのではなく、簡単にアクセスできる脆弱性を悪用する攻撃を指します。
* ファイルレス攻撃 (オプション B) は、LOTL テクニックを含むがこれに限定されない、より広範なカテゴリです。
* スクリプト キディ (オプション C) は、環境固有の高度な戦術ではなく、事前に作成されたスクリプトを使用する経験の浅い攻撃者を指します。
参考資料: Living off the land 戦術では、環境独自のツールが活用されるため、従来のマルウェア対策戦略を使用して検出および防止することが困難になります。

最新問題: **11**
ダウンロードしたプログラムによるブラウザ プラグインのインストールをブロックする Symantec Endpoint Protection テクノロジーはどれですか?
A. 侵入防止
B. ソナー
C. アプリケーションとデバイスの制御
D. 改ざん防止
Answer: C (メーッセージを残す**)**
Symantec Endpoint Protection (SEP) のアプリケーションとデバイス制御テクノロジは、ダウンロードしたプログラムがブラウザ プラグインをインストールしないようにするなど、不正なソフトウェア動作をブロックする役割を担っています。この機能は、プログラムのインストール動作、特定のシステム コンポーネントへのアクセス、ブラウザ設定とのやり取りの制御など、アプリケーションによる特定のアクションを制限するポリシーを適用するように設計されています。アプリケーションとデバイス制御は、ブラウザに対する潜在的に望ましくない、または悪意のある変更を阻止することでエンドポイントを効果的に保護し、未検証または有害なプラグインから発生する可能性のある脅威からユーザーを保護します。

最新問題: **12**
リアルタイム管理を実現するために SES 内で利用される通信方法はどれですか?
A. ロングポーリング
B. 標準ポーリング
C. プッシュ通知
D. ハートビート
Answer: C (メーッセージを残す**)**
プッシュ通知は、Symantec Endpoint Security (SES) 内でリアルタイム管理を容易にするために使用される通信方法です。この方法により、次のことが可能になります。
* 即時更新: SES は、標準のポーリング間隔を待たずに、ポリシーの変更、更新、またはコマンドをエンドポイントに即座にプッシュできます。
* 脅威への効率的な対応: プッシュ通知により、指示がエンドポイントに即座に配信されるため、新たな脅威への対応時間が短縮されます。
* リソース使用量の削減:継続的なポーリングとは異なり、プッシュ通知は必要に応じてトリガーされるため、ネットワークとシステムのリソース需要が削減されます。
プッシュ通知は、SES でリアルタイム管理を実現し、タイムリーな応答と更新を提供してエンドポイントのセキュリティを強化するために不可欠です。

最新問題: **13**
中間者攻撃に遭遇した場合に、データ漏洩からユーザーを保護する SES セキュリティ制御はどれですか?
A. IPv6 トンネリング

B. IPS
C. ファイアウォール
D. VPN
Answer: (解答を表示する**)**
Symantec Endpoint Security (SES) の侵入防止システム (IPS) は、中間者 (MITM) 攻撃中のデータ漏洩を防ぐ上で重要な役割を果たします。このようなシナリオで IPS がどのように保護するかを次に示します。
* 脅威検出:IPS はネットワーク トラフィックをリアルタイムで監視し、不正アクセスの試みや異常なパケット パターンなど、MITM 攻撃の兆候となる疑わしいパターンを識別してブロックします。
* データ傍受の防止: IPS はこれらの脅威をブロックすることで、悪意のある行為者がユーザー データを傍受またはリダイレクトするのを防ぎ、データ漏洩を防ぎます。
* 自動応答:IPS は即座に応答するように設計されており、機密データが侵害される前に攻撃を検出して軽減します。
IPS はプロアクティブな保護を提供することで、潜在的な MITM 脅威が発生した場合でもデータの安全性を確保します。

最新問題**: 14**
管理者は Mac 上のデバイスを識別するために何を利用すべきでしょうか?
A. デバイスが接続されている場合はDevViewerを使用します。
B. デバイスが接続されている場合は DeviceInfo を使用します。
C. デバイスが接続されたらデバイス マネージャーを使用します。
D. デバイスが接続されたときにGatherSymantecInfoを使用します。
Answer: D (メーッセージを残す**)**
Mac 上のデバイスを識別するには、デバイスが接続されているときに管理者は GatherSymantecInfo ツールを使用できます。このツールは、Symantec Endpoint Protection に固有のシステム情報と診断データを収集し、管理者がデバイスを正確に識別してトラブルシューティングできるようにします。GatherSymantecInfo を使用すると、Mac 環境でエンドポイントを管理およびサポートするために不可欠な包括的なデータ収集が保証されます。

最新問題**: 15**
ログオン試行が数回失敗した後、Symantec Endpoint Protection Manager (SEPM) はデフォルトの管理者アカウントをロックしました。管理者は、感染拡大に対処するためにできるだけ早くシステムを変更する必要がありますが、管理者アカウントが唯一のアカウントです。
既存の環境への影響を最小限に抑えながら問題を修正するには、管理者はどのようなアクションを実行する必要がありますか?
A. 15分待ってから再度ログオンしてください
B. バックアップからSEPMを復元する

C. 管理サーバーと構成ウィザードを実行してサーバーを再構成します
D. SEPMを再インストールする
Answer: A (メーッセージを残す**)**
Symantec Endpoint Protection Manager (SEPM) のデフォルトの管理者アカウントが、ログイン試行に数回失敗してロックされている場合、管理者にとって最善の対応策は、15 分待ってから再度ログオンを試行することです。このアプローチが推奨される理由は次のとおりです。
* アカウント ロックアウト ポリシー: SEPM を含むほとんどのシステムは、ログイン試行に一定回数失敗するとアカウントを一時的に無効にするアカウント ロックアウト ポリシーを備えています。通常、これらのポリシーにはリセット時間 (通常は約 15 分) が含まれており、リセット時間が過ぎるとアカウントは再びアクティブになります。
* 中断を最小限に抑える: アカウントが自動的にロック解除されるまで待つことで、既存の環境への中断を最小限に抑えることができます。これにより、複雑になる可能性のある回復プロセスや、追加の複雑さやデータ損失を引き起こす可能性のあるバックアップからの復元の必要性を回避できます。
* システム変更の回避: バックアップからの SEPM の復元、サーバーの再構成、再インストールなどのアクションを実行すると、構成に大きな変更が生じ、特に感染拡大に対処するために即時の対応が必要な場合に、さらに複雑な問題が発生する可能性があります。
* 脅威への対応の優先順位付け: セキュリティ インシデントに迅速に対応することは重要ですが、SEPM 構成の整合性を維持し、スムーズな回復を確保することも重要です。
ロックアウト期間を待つことで、システムのセキュリティ プロトコルが尊重され、管理者は最小限のリスクでアクセスを回復できるようになります。
要約すると、ロックアウトの期限が切れるのを待つのが最も簡単で混乱の少ない解決策であり、管理者は SEPM 環境に不必要なリスクを与えることなく重要な機能を再開できます。

最新問題**: 16**
ハイブリッド環境を使用しており、SEPM で管理されているエンドポイントが SEPM に接続できない場合、エンドポイントがパブリック ホットスポットを使用している場合、管理者はどのくらい早くセキュリティ警告を受信できますか?
A. ネットワーク整合性でVPNが有効化された後
B. クライアントがSEPMに接続するとき
C. 次のハートビートで
D. すぐに
Answer: D (メーッセージを残す**)**
ハイブリッド環境では、SEPM で管理されているエンドポイントが SEPM に接続できず、パブリック ホットスポットを使用している場合、管理者は ICDm (Integrated Cyber Defense Manager) を通じてセキュリティ アラートをすぐに受信できます。手順は次のとおりです。

* クラウドベースのアラート:ICDm は、エンドポイントの SEPM への直接接続に依存しないリアルタイムの監視およびアラート機能を提供します。
* ネットワークの独立性:エンドポイントはクラウド (ICDm) に接続するため、ネットワークの種類や VPN の状態に関係なく、イベントやアラートが発生するとすぐに報告できます。
* 応答性の強化: この設定により、管理者はエンドポイントがネットワークに接続されていない場合でもセキュリティ インシデントに迅速に対応できます。これは、モバイルおよびリモート ワークのシナリオでの脅威の封じ込めに不可欠です。
ハイブリッド環境における ICDm の即時アラート機能により、継続的な監視と潜在的なセキュリティ脅威への迅速な対応が可能になります。

最新問題**: 17**
LiveShell を使用するにはどの ICDm ロールが必要ですか?
A. セキュリティアナリスト
B. 管理者
C. 閲覧者
D. 任意
Answer: (解答を表示する**)**
Symantec の Integrated Cyber Defense Manager (ICDm) で Live Shell を使用するには、管理者ロールが必要です。
LiveShell を使用すると、管理者はエンドポイントでコマンドライン インターフェイスを開き、トラブルシューティングやインシデント対応に直接アクセスできるようになります。
* 管理者ロールが必要な理由:
* LiveShell はエンドポイントへの高レベルのアクセスを許可するため、不正使用を防ぎ、許可された担当者だけがエンドポイントでコマンドライン セッションを開始できるように、管理者権限を持つユーザーに限定されています。
* 他の役割が間違っている理由:
* セキュリティアナリスト (オプション A) とビューアー (オプション C) には、エンドポイントでコマンドを実行するために必要な権限がありません。

* セキュリティ上の理由により、LiveShell へのアクセスは管理者ロールに制限されているため、任意 (オプション D) は正しくありません。
参照: LiveShell を使用するには管理者権限が必要であり、トラブルシューティングや対応のためにエンドポイント コマンド インターフェイスにアクセスできるのは承認されたユーザーのみであることを保証します。

最新問題**: 18**
IPS はカスタム署名をどのようにチェックしますか?
A. IPS は、表にリストされているシグネチャをチェックします。検出結果が受信または送信トラフィック パケットと一致すると、IPS エンジンは他のシグネチャのチェックを続行します。
B. IPS は、テーブルにリストされているシグネチャをチェックします。検出が受信または送信トラフィック パケットと一致すると、IPS エンジンはシグネチャのチェックを再開します。
C. IPS は、テーブルにリストされているシグネチャをチェックします。検出が受信または送信トラフィック パケットと一致すると、IPS エンジンは他のシグネチャのチェックを停止します。
D. IPS は、テーブルにリストされているシグネチャをチェックします。検出が受信または送信トラフィック パケットと一致すると、IPS エンジンは他のシグネチャをログに記録します。
Answer: C (メーッセージを残す**)**
Symantec Endpoint Protection の侵入防止システム (IPS) は、定義されたシグネチャのリストに対して受信および送信トラフィック パケットをスキャンすることによって動作します。このプロセスは、潜在的なセキュリティ脅威を示す既知の攻撃パターンまたは異常を特定することを目的としています。
IPS がこれらのカスタム シグネチャに基づいてトラフィック パケット内で一致を検出すると、次のシーケンスが発生します。
* 初期検出と一致:IPS エンジンは、シグネチャ テーブルを参照して、トラフィックをリアルタイムでアクティブに監視します。一致が見つかるまで、各パケットが順番にチェックされます。
* さらなるチェックの停止: 署名が受信または送信トラフィックと一致すると、IPS エンジンは同じトラフィック パケット内の他の署名のさらなるチェックを終了します。この設計により、脅威が特定された後の冗長な処理を回避することで、システム リソースが節約され、パフォーマンスが最適化されます。
* 検出時のアクション: 一致したシグネチャに基づいて脅威を識別して確認した後、IPS エンジンは、パケットのブロック、管理者への警告、イベントのログ記録などの構成された応答を適用します。

このアプローチでは、最初に検出されたシグネチャのみに焦点を当てることで効率的な脅威検出が保証され、不要な処理オーバーヘッドが防止され、迅速なインシデント対応が保証されます。

最新問題: **19**
バイナリ実行可能ファイルを評価するために Symantec Insight が使用する基準を 2 つ選択してください。
A. 感度
B. 普及率
C. 機密性
D. コンテンツ
E. 年齢
Answer: B,E (メーッセージを残す**)**
Symantec Insight は、普及度と年齢という 2 つの主要な基準を使用してバイナリ実行ファイルを評価します。これらのメトリックは、広範なユーザー ベースでのファイルの動作に基づいて、ファイルが無害か悪質かを判断するのに役立ちます。
* 普及度: この指標は、シマンテックのグローバルコミュニティ全体でファイルがどの程度広く使用されているかを評価します。普及度が高いファイルは一般的に安全である可能性が高くなりますが、まれなファイルはリスクが高くなります。
* 年齢: ファイルの年齢も考慮されます。評判が安定している古いファイルは悪意のあるファイルである可能性が低くなりますが、新しい未検証のファイルはより厳密に精査されます。
Symantec Insight はこれらの基準を使用してバイナリ ファイルの信頼性の高い評価を提供し、潜在的な脅威を事前に特定することでエンドポイントのセキュリティを強化します。

最新問題: **20**
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. 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
B. 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
C. 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。
D. 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
Answer: B (メーッセージを残す**)**
Symantec Endpoint Protection のセキュリティ アナリスト ロールには、エンドポイントの検索、ダンプのトリガー、ファイルの取得と隔離を行う権限があります。これらの権限により、セキュリティ アナリストは潜在的な脅威を調査し、さらに分析するためのデータを収集し、必要に応じて悪意のあるファイルを隔離できます。
* セキュリティアナリストの役割の機能:
* エンドポイントの検索: アナリストはエンドポイント全体で検索を実行し、疑わしいファイルやアーティファクトを見つけることができます。

* トリガー ダンプ: これにより、アナリストは詳細な調査のためにメモリ ダンプやその他のフォレンジック データを作成できます。
* ファイルの取得と隔離: アナリストはエンドポイントから直接ファイルを隔離できるため、脅威を軽減し、さらなる拡散を防ぐことができます。
* 他のオプションが間違っている理由:
* 新しいサイトの登録 (オプション A) とデバイス グループまたはポリシーの作成 (オプション C および D) は、通常、セキュリティ アナリストではなく、より広範なアクセス権を持つ管理者向けに予約されています。
参考資料: セキュリティ アナリストの役割は、ファイルの検索、ダンプ、隔離などの調査および対応アクションに重点を置いています。

最新問題**: 21**
ドメインの誤った構成や隠れたバックドアが検出された後、Active Directory の脅威防御アラームのどのような種類が表示されますか?
A. コンピュータ情報収集
B. パス ・ザ ・チケット
C. 資格情報の盗難
D. 暗い隅
Answer: (解答を表示する**)**
Dark Corners アラームは、Active Directory の脅威防御機能の一部であり、ディレクトリ環境内でドメインの誤った構成や隠れたバックドアが検出されたときにトリガーされます。このアラームの機能は次のとおりです。
* 隠れた脅威の検出:Dark Corners は、不正アクセス パスや悪用される可能性のある誤った構成など、Active Directory 内の隠れた脆弱性を識別し、管理者に警告します。
* セキュリティ保証:これらの問題を特定することで、管理者は、検出が難しい潜在的なリスクに積極的に対処し、修正することができます。
* Active Directory セキュリティの強化:Dark Corners アラームは、バックドアや誤った構成によって攻撃者に隠れたアクセス ポイントが提供されないようにし、Active Directory の全体的なセキュリティ体制を強化します。
この機能により、Active Directory 内でより詳細なレベルの検査が可能になり、微妙ながらも重大なセキュリティ リスクから保護されます。

最新問題**: 22**
ある企業は、単一の ESXi ホスト上で実行されている 50 台の仮想マシンに Symantec Endpoint Protection (SEP) を導入しています。
各 SEP エンドポイントが Symantec Endpoint Protection Manager と通信している間に、ESXi サーバーへの突然の IOPS の影響を最小限に抑えるために、管理者はどのような構成変更を行うことができますか?
A. ダウンロードインサイトの感度レベルを上げる
B. ハートビート間隔を短縮する

C. ダウンロードのランダム化ウィンドウを増やす
D. 保存するコンテンツのリビジョン数を減らす
Answer: (解答を表示する**)**
SEP エンドポイント通信による ESXi サーバーへの突然の IOPS への影響を最小限に抑えるには、管理者はダウンロードのランダム化ウィンドウを増やす必要があります。この構成変更により、仮想マシン間で SEP 更新のタイミングが分散され、サーバーの同時 I/O 負荷が軽減されます。
* ダウンロードのランダム化の効果:
* ランダム化ウィンドウを増やすと、更新は一度にダウンロードされるのではなく、間隔をあけてダウンロードされるため、バースト IOPS の需要が低下します。
* これは、高 IOPS アクティビティによるパフォーマンスの低下を防ぐため、複数の VM が単一の ESXi サーバー上でホストされている仮想化環境で特に役立ちます。
* 他の選択肢があまり効果的でない理由:
* ダウンロード インサイトの感度を上げる (オプション A) と、IOPS には影響しません。
* ハートビート間隔を短くすると (オプション B)、通信頻度が増加し、IOPS が向上する可能性があります。
* コンテンツ リビジョンの削減 (オプション D) はストレージ サイズに影響しますが、更新 IOPS は制御されません。
参考資料: 仮想環境では、SEP 更新サイクル中の IOPS 需要を管理するために、ダウンロードのランダム化ウィンドウを増やすことが推奨されます。

最新問題**: 23**
デバイスがホスト整合性チェックに失敗した場合はどうなりますか?
A. マルウェア対策スキャンが開始されます
B. デバイスが再起動されました
C. デバイスは隔離されています
D. 管理通知が記録されます
Answer: (解答を表示する**)**
デバイスが Symantec Endpoint Protection (SEP) のホスト整合性チェックに失敗すると、隔離されます。つまり、ネットワーク内で潜在的なセキュリティ リスクが広がるのを防ぐために、デバイスのネットワーク リソースへのアクセスが制限される可能性があります。隔離により、構成されたセキュリティ標準を満たしていないデバイスを封じ込め、ネットワーク全体の整合性を保護することができます。
* ホスト整合性エラー時の隔離の目的:
* ホスト整合性チェックにより、エンドポイント デバイスが最新のウイルス対策シグネチャや必要なパッチなどのセキュリティ ポリシーに準拠していることを確認します。
* デバイスがこのチェックに失敗した場合、検疫によってネットワーク接続が制限され、非準拠デバイスによる潜在的なリスクにネットワークをさらすことなく修復アクションが可能になります。
* 他のオプションがあまり適していない理由:

* マルウェア対策スキャン (オプション A) とデバイスの再起動 (オプション B) は、整合性チェックの失敗に対するデフォルトの応答ではありません。
* 管理通知 (オプション D) はログに記録される場合がありますが、検疫のように封じ込めは提供されません。
参照: 非準拠デバイスを隔離することは、ホスト整合性チェックの失敗に対する標準的な対応であり、修復中にネットワーク保護を確保します。

最新問題: **24**
SEDR の分離ボタンをクリックしてエンドポイントを分離すると、どのタイプの通信がブロックされますか?
A. すべての非SEPおよび非SEDRネットワーク通信
B. すべてのネットワーク通信
C. SEPおよびSEDRネットワーク通信のみ
D. WebおよびUNCネットワーク通信のみ
Answer: A (メーッセージを残す**)**
Symantec Endpoint Detection and Response (SEDR) でエンドポイントが隔離されると、隔離により SEP および SEDR 関連のトラフィックを除くすべてのネットワーク通信がブロックされます。この選択的なブロックにより、SEP および SEDR 管理者はエンドポイントを管理できる状態を維持しながら、その他の潜在的に有害なネットワーク通信を遮断できます。
* 隔離の仕組み:
* 分離により、SEP および SEDR 以外のすべてのネットワーク通信がブロックされ、エンドポイントが他のネットワーク エンティティに接続したり、他のネットワーク エンティティからアクセスされたりするのを効果的に防止します。
* この方法は、監視やさらなる対応アクションのためにエンドポイントを管理サーバーに接続したまま脅威を封じ込めるのに役立ちます。
* 他のオプションが間違っている理由:
* すべてのネットワーク通信 (オプション B) は SEP/SEDR 管理トラフィックを防止しますが、これは設計に反します。
* SEP と SEDR のネットワーク通信のみ (オプション C) は誤りです。これは、SEP と SEDR のみがブロックされていることを示していますが、実際には他のすべてのトラフィックがブロックされています。
* Web および UNC ネットワーク通信のみ (オプション D) では、分離機能の全範囲がカバーされません。
参考資料: SEDR の分離機能は、脅威を封じ込めながら安全な管理アクセスを可能にする制御された応答メカニズムを提供します。

最新問題: **25**
SEPM のパフォーマンスが予想を下回り、断続的にエラーが発生します。システム管理者にパフォーマンスの問題を通知するにはどうすればよいでしょうか?

A. システム イベント アラートを追加し、通知を発行する頻度を指定します。通知する必要がある電子メール アドレスと、サーバーの健全性が低下した場合のアクションを指定します。
B. 認証アラートを追加し、通知を発行する頻度を指定します。通知する必要がある電子メール アドレスと、サーバーの健全性が低下した場合のアクションを指定します。
C. クライアント セキュリティ アラートを追加し、通知を発行する頻度を指定します。通知する必要がある電子メール アドレスと、サーバーの健全性が低下した場合のアクションを指定します。
D. サーバー ヘルス アラートを追加し、通知を発行する頻度を指定します。通知する必要がある電子メール アドレスと、サーバー ヘルスが悪化した場合のアクションを指定します。
Answer: D (メーッセージを残す**)**
SEPM のパフォーマンスの問題を管理者に通知するには、サーバー ヘルス アラートを追加する必要があります。このタイプのアラートは、SEPM のヘルスを監視するように特別に設計されており、パフォーマンスの低下やエラーの発生時に通知をトリガーします。
* 設定手順:
* SEPM でサーバー ヘルス アラートを設定し、サーバーのヘルス状態が悪いことを示す条件を指定します。
* アラートの頻度を設定し、通知用の電子メール アドレスを指定して、管理者がタイムリーな更新を受信できるようにします。
* 他のオプションが間違っている理由:
* システム イベント アラート (オプション A) は一般的なシステム イベントをカバーしますが、パフォーマンスにはあまり特化していません。
* 認証アラート (オプション B) は、ログインとアクセスの問題に焦点を当てます。
* クライアント セキュリティ アラート (オプション C) は、SEPM サーバーのパフォーマンスではなく、エンドポイント セキュリティに関連しています。
参考資料: サーバー ヘルス アラートは SEPM のパフォーマンスを監視するためにカスタマイズされており、サーバー ヘルスを追跡するのに最適な選択肢です。

最新問題**: 26**
管理者は、Windows の起動時に発生する可能性のある脅威を調査しています。Microsoft によってデジタル署名されていないファイルが確認されました。このファイルの脅威をスキャンするには、管理者はどのマルウェア対策機能を有効にする必要がありますか?
A. 早期起動マルウェア対策を有効にする
B. 自動保護を有効にする
C. 行動分析を有効にする
D. Microsoft ELAM を有効にする
Answer: A (メーッセージを残す**)**
起動時マルウェア対策 (ELAM) は、Windows の起動の初期段階でマルウェア対策保護を提供するように設計された機能です。ELAM を有効にすると、起動時に読み込まれるドライ

バーとファイル、特に Microsoft などの信頼できるソースによってデジタル署名されていないドライバーとファイルがスキャンされます。
* ELAM の仕組み:
* ELAM は起動時に他のドライバーの前に読み込まれ、重要なファイルとドライバーをスキャンして、他のセキュリティ レイヤーが完全に動作する前に実行を試みる可能性のある潜在的なマルウェアを特定します。
* 観察されたファイルは Microsoft によってデジタル署名されていないため、ELAM は起動時にそれを検出して分析し、潜在的な脅威が初期化されるのを防ぎます。
* ELAMの利点:
* Windows の起動プロセス中に読み込まれてシステムに永続的に侵入しようとするルートキットやその他の脅威に対して、プロアクティブな防御を提供します。
* 他のオプションがあまり適していない理由:
* 自動保護と動作分析は有効ですが、システムの起動後に動作します。
* Microsoft ELAM は Windows で既にデフォルトで有効になっていますが、SEP の ELAM 機能と同じカスタマイズ性は提供されません。
参考資料: ELAM を有効にすることは、署名されていないファイルや疑わしいファイルに対して最も初期の起動段階を保護するための SEP の重要なベスト プラクティスです。

最新問題**: 27**
関連するセキュリティ イベントの親子関係を表示するインシデント ビュー ウィジェットはどれですか?
A. インシデント概要ウィジェット
B. プロセス系統ウィジェット
C. イベントウィジェット
D. インシデントグラフウィジェット
Answer: (解答を表示する**)**
Symantec Endpoint Security のインシデント ビューのプロセス リネージ ウィジェットは、主要な悪意のあるアクションから生じるプロセスやアクティビティなど、関連するセキュリティ イベント間の親子関係を視覚的に表現します。このウィジェットは、システム内の潜在的な脅威の起源と伝播経路を追跡するのに役立ち、セキュリティ チームは後続のアクションをトリガーした最初のプロセスを特定できます。この階層関係を表示することで、プロセス リネージ ウィジェットは詳細なフォレンジック分析をサポートし、管理者がインシデントがどのように展開したかを理解し、関連する各セキュリティ イベントの影響を状況に応じて評価するのに役立ちます。

最新問題**: 28**
ビジネスに影響を及ぼす可能性のあるインシデントはどの程度の優先順位で考慮されますか?
A. 低い
B. クリティカル

C. 高
D. 中
Answer: (解答を表示する**)**
ビジネスに影響を及ぼす可能性のあるインシデントは、通常、サイバーセキュリティ フレームワークとインシデント対応プロトコルで優先度の高いものとして分類されます。この分類の詳細な根拠は次のとおりです。
* 潜在的な業務中断: 間接的であっても業務運営に影響を与える、または影響を与える恐れのあるインシデントには、迅速な対応を確実にするために高い優先度が割り当てられます。この分類では、直ちに重大ではないが、迅速に対処しないとエスカレートする可能性のあるインシデントが優先されます。
* エスカレーションのリスク: 優先度の高いインシデントは、壊滅的ではないものの、重要なシステムに影響を与えたり、機密データを危険にさらしたりする可能性があるため、深刻なビジネスへの影響につながる前に注意を払う必要がある状況です。
* 迅速な対応要件: 優先度が高いとラベル付けされたインシデントは、ビジネスへのさらなる影響や運用停止を防ぐために、即時の調査と封じ込め措置のためにフラグが付けられます。
このコンテキストでは、重大なインシデントには即時の重大な影響を伴う緊急の脅威 (アクティブなデータ侵害など) が含まれますが、高い優先度は重大なリスクまたはビジネスへの影響の可能性があるインシデントに適用されます。この優先順位付けは、効果的なインシデント管理に不可欠であり、リソースをビジネス継続性に対する潜在的なリスクに集中させることができます。

最新問題**: 29**
Integrated Cyber Defense Manager で最も権限が制限されているデフォルト ロールはどれですか?
A. エンドポイント コンソール ドメイン管理者
B. サーバー管理者
C. 制限付き管理者
D. 限定管理者
Answer: C (メッセージを残す**)**
統合サイバー防御マネージャー (ICDm) の制限付き管理者ロールは、デフォルト ロールの中で最も権限が制限されています。このロールは、重要な管理機能や高度な管理機能なしで基本機能にアクセスする必要があるユーザーを対象としており、偶発的または不正な変更のリスクが低くなります。
* 制限付き管理者の役割:
* 制限付き管理者はアクセスが厳しく制限されており、通常は特定の情報の表示と最小限のアクションの実行に制限されます。
* 他の役割が間違っている理由:

* エンドポイント コンソール ドメイン管理者 (オプション A) とサーバー管理者 (オプション B) には、エンドポイント設定とサーバー構成を管理するためのより広範な権限があります。
* 制限付き管理者 (オプション D) には制限付き管理者よりも多くの権限がありますが、完全なアクセス権はありません。
参照: 制限付き管理者ロールは最小限の権限を提供し、システム アクセスを制限し、より特権のあるロールに関連するセキュリティ リスクを軽減します。

最新問題: **30**
収集されたアプリケーション動作データに基づいてカスタム動作分離ポリシーを作成するために管理者が使用できるツールは何ですか?
A. 行動の蔓延チェック
B. 行動ヒートマップ
C. アプリケーションカタログ
D. アプリケーション頻度マップ
Answer: (解答を表示する**)**
管理者は、Symantec Endpoint Security のアプリケーション カタログを使用して、カスタムの動作分離ポリシーを作成できます。このツールは、アプリケーションの動作に関するデータをコンパイルし、管理者が環境内で観察された特定の動作に対処する分離ポリシーを定義できるようにします。アプリケーション カタログを活用することで、管理者はアプリケーションの動作に基づいてポリシーをカスタマイズし、潜在的に悪質なアクティビティの制御と封じ込めを強化できます。

最新問題: **31**
Cynic の特徴は何ですか?
A. ローカルサンドボックス
B. イベントデータをセキュリティ情報およびイベント管理 (SIEM) に転送する
C. クラウドサンドボックス
D. カスタマイズ可能な OS イメージ
Answer: (解答を表示する**)**
Cynic は、クラウド サンドボックス機能を提供する Symantec Endpoint Security の機能です。クラウド サンドボックスにより、Cynic は安全で隔離されたクラウド環境で疑わしいファイルや動作を分析し、内部ネットワークに危害を与えることなく潜在的な脅威を特定できます。仕組みは次のとおりです。
* クラウドへのファイル送信: 疑わしいファイルはクラウドベースのサンドボックスに送信され、さらに詳しく分析されます。
* 動作分析: クラウド環境内で、Cynic はさまざまな条件をシミュレートしてファイルの動作を観察し、マルウェアやその他の有害なアクションを効果的に検出します。
* リアルタイムの脅威インテリジェンス: 検出結果はすぐに報告されるため、Symantec Endpoint Protection は分析に基づいて迅速に対処できます。

Cynic のクラウド サンドボックスは、高度な脅威検出に対してスケーラブルで安全かつ非常に効果的なアプローチを提供します。

最新問題: **32**
攻撃者が脆弱なアプリケーションを悪用するために使用するセキュリティ脅威の種類は何ですか?
A. 横方向の移動
B. 権限昇格
C. 資格情報アクセス
D. コマンドとコントロール
Answer: (解答を表示する**)**
ラテラルムーブメントは、攻撃者が脆弱なアプリケーションを悪用し、ネットワーク内のシステム間を移動するために使用するセキュリティ脅威の一種です。この手法により、攻撃者はアプリケーションの脆弱性を悪用して複数のシステムにアクセスし、ネットワークの奥深くまで進むことができます。
* 横方向の移動を理解する:
* 横方向の移動では、ソフトウェアの脆弱性を悪用して追加のシステムやデータ リソースにアクセスします。
* 攻撃者はこの方法を使用して、侵害されたネットワーク内で影響力を拡大し、多くの場合、アプリケーションの脆弱性を利用して他のシステムに移動します。
* 他のオプションが間違っている理由:
* 権限昇格 (オプション B) は、単一のシステムでより高いアクセス権を取得することに重点を置いています。
* 資格情報アクセス (オプション C) では、アプリケーションを悪用するのではなく、ログイン資格情報を盗みます。
* コマンド アンド コントロール (オプション D) は、アプリケーションの悪用ではなく、侵害されたデバイスと攻撃者のサーバー間の通信を指します。
参考資料: ラテラルムーブメントは、アプリケーションの脆弱性を利用して組織のネットワーク内での攻撃者のアクセスを拡大するため、標的型攻撃における一般的な脅威ベクトルとなります。

最新問題: **33**
Symantec ファイアウォールの次に、第 2 層の防御を提供するポリシーの種類は何ですか?
A. ウイルスとスパイウェア
B. ホスト整合性
C. 侵入防止
D. システムロックダウン
Answer: C (メーッセージを残す**)**
侵入防止システム (IPS) は、Symantec ファイアウォールに続く第 2 層の防御を提供します。ファイアウォールがネットワーク境界でのアクセスとトラフィック フローを制御する一方で、IPS は、悪意のあるアクティビティ (エクスプロイトの試みや疑わしいネットワーク パターンなど) の兆候がないか、着信トラフィックと発信トラフィックを積極的に監視および検査します。
* IPS がファイアウォールを補完する方法:
* ファイアウォールは防御の第一層として機能し、ルールとポリシーに基づいて不正アクセスをブロックします。
* IPS は許可されたトラフィックをリアルタイムで検査し、既知のエクスプロイトや異常なネットワーク動作など、基本的なファイアウォール ルールを回避する可能性のある攻撃を識別してブロックします。
* 他の選択肢があまり効果的でない理由:
* ウイルスとスパイウェア (オプション A) は、ネットワーク防御ではなく、ファイルとプログラム内のマルウェア検出に重点を置いています。
* ホスト整合性 (オプション B) はコンプライアンスに関連し、システム ロックダウン (オプション D) はアプリケーションの実行を制御しますが、ネットワーク トラフィックを監視しません。
参照: 侵入防止機能は、シマンテックのネットワーク セキュリティ スタックに重要な防御層を追加し、ファイアウォールと連携して包括的な保護を実現します。

最新問題: **34**
SEP for Mac を実行しているクライアントの通信を復元するには、管理者はどのような方法を使用する必要がありますか?
A. クライアント展開ウィザードを使用して通信パッケージをプッシュアウトします。
B. SEPM で Sylink Drop Tool を使用します。
C. SSH を使用して次のコマンドを実行します。
D. sudo launchct1 load /Library/LaunchDaemons/eom.Symantec.symdaemon.'plist
E. サードパーティのデプロイメントを使用して通信パッケージをプッシュアウトします。
Answer: (解答を表示する**)**
Symantec Endpoint Protection (SEP) for Mac を実行しているクライアントの通信を復元するには、管理者はクライアント展開ウィザードを使用して通信パッケージをプッシュする必要があります。このパッケージは、Symantec Endpoint Protection Manager (SEPM) との通信設定を再確立し、クライアントが管理サーバーに接続できるようにします。

* クライアント展開ウィザードを使用する理由:
* クライアント展開ウィザードを使用すると、管理者は SEP クライアントが SEPM に再接続して適切な通信チャネルを再確立するために必要な通信設定 (Sylink.xml) を展開できます。
* 他のオプションがあまり適していない理由:
* Sylink Drop Tool (オプション B) は主に Windows で使用され、macOS では使用されません。
* SSH コマンド (オプション C) は、SEPM 通信設定の復元には関係ありません。
* クライアント展開ウィザードが使用可能な場合、サードパーティ展開 (オプション D) は不要です。
参考: クライアント展開ウィザードは、SEP for Mac クライアントの通信設定を復元するための推奨される方法です。

最新問題**: 35**
Symantec Endpoint Protection (SEP) 管理者は、マシンでパフォーマンスの問題が発生しているという複数のレポートを受け取ります。管理者は、レポートがスケジュールされた LiveUpdate とほぼ同時に発生していることを発見しました。
LiveUpdate が発生したときに I/O を最小限に抑えるために、SEP 管理者はどの設定を構成する必要がありますか?
A. LiveUpdate スケジュールを変更する
B. 管理者定義のスキャンスケジュールを変更する
C. スキャン作成者がログオフしているときにユーザー定義のスキャンの実行を許可するを無効にする
D. 新しい定義が届いたときにアクティブスキャンを実行するのを無効にする
Answer: A (メーッセージを残す**)**
LiveUpdate が発生したときの I/O の影響を最小限に抑えるには、LiveUpdate スケジュールを調整する必要があります。このソリューションが効果的な理由は次のとおりです。
* ピーク時のシステムへの影響を軽減: オフピーク時に LiveUpdate をスケジュールすることで、使用率の高い期間にシステム リソースが解放され、パフォーマンスの問題が発生する可能性が軽減されます。
* 効率的なリソース割り当て: スケジュールを調整することで、ユーザー アクティビティにエンドポイント リソースが必要になる可能性が低い時間に LiveUpdate を実行できるため、パフォーマンスへの影響が最小限に抑えられます。
* 定期的な更新の維持: このアプローチにより、勤務時間中にエンドポイントのパフォーマンスに影響を与えることなく、定期的に更新が行われます。
この方法は、リソース負荷を管理し、スケジュールされた更新中にスムーズなパフォーマンスを維持するのに最適です。

最新問題**: 36**

ある組織では、バックアップと復元ウィザードを使用して毎週バックアップを実行しています。今週は、ディスク容量不足のため、プロセスを完了できませんでした。
SEP 管理者は SEPM バックアップ ファイルの場所をどのように変更しますか?
A. 管理サーバー構成ウィザードで SEPM を再構成して、データ ディレクトリを移動します。
B. 管理サーバー構成ウィザードで SEPM を再構成して、バックアップ ディレクトリを移動します。
C. 管理サーバー構成ウィザードで SEPM を再構成して、インストール ディレクトリを移動します。
D. 管理サーバー構成ウィザードで SEPM を再構成して、データベース ディレクトリを移動します。
Answer: B (メーッセージを残す**)**
ディスク容量不足のためにバックアップが失敗した場合、Symantec Endpoint Protection Manager (SEPM) 管理者はバックアップ ファイルの場所を変更してプライマリ ドライブの容量を解放できます。これを行うには、次の手順を実行します。
* 管理サーバー構成ウィザード:
* SEPM には、管理サーバー構成ウィザードを使用して、バックアップ ディレクトリを含む特定のディレクトリを再構成するオプションが用意されています。
* バックアップ ディレクトリを移動するオプションを選択すると、管理者は、デフォルトのデータ ディレクトリやインストール ディレクトリを混乱させることなく、バックアップ ファイルを保存するのに十分なスペースがある新しい場所を指定できます。
* バックアップディレクトリの場所を変更する手順:
* SEPM 管理サーバー構成ウィザードを起動します。
* バックアップ ディレクトリを具体的に再設定または移動するオプションを選択します。この手順は、コア SEPM インストールまたはデータベース ディレクトリには影響しません。
* 将来の障害を防ぐために、十分なストレージが利用できるバックアップ ディレクトリの新しいパスを指定します。
* 選択の理由:
* オプション A、C、および D では、データ、インストール、またはデータベース ディレクトリの移動が行われますが、これはバックアップ ストレージの問題とは関係ありません。バックアップ ディレクトリの再配置によってのみ、バックアップ プロセス中のディスク容量不足の問題が解決されます。
参考資料: このソリューションは、Symantec Endpoint Protection 14.x のドキュメントに記載されている Symantec Endpoint Protection Manager の構成ガイドラインに従います。

最新問題**: 37**
管理者は、疑わしいファイルの影響を受けるすべてのデバイスをどのように確認すればよいでしょうか?

A. [アラートとイベント] リストから [ファイル] を選択し、ファイル リストから [デバイス] を選択します。
B. 検出されたアイテムのリストからデバイスを選択します。
C. [検出された項目] リストからファイルを選択し、[詳細] ページで [デバイス] を選択します。
D. アラートとイベント リストからデバイスを選択します。
Answer: C (メーッセージを残す**)**
疑わしいファイルの影響を受けるすべてのデバイスを表示するには、管理者は [検出されたアイテム] リストに移動し、特定のファイルを選択して、[詳細] ページから影響を受けるデバイスを表示する必要があります。
* 影響を受けるデバイスを表示する手順:
* 管理コンソール内の 検出されたアイテム」リストに移動します。
* 問題の疑わしいファイルを見つけて選択し、その詳細ページを開きます。
* [詳細] ページには、ファイルに関連付けられているデバイスのリストが表示され、疑わしいアクティビティによって影響を受ける可能性のあるエンドポイントに関する情報が提供されます。
* 他のオプションがあまり適していない理由:
* オプション A と B では、選択したファイルの特定のデバイス リストは提供されません。
* オプション D は、疑わしいファイルではなくデバイスを最初に選択することを意味するため、正しくありません。
参考: 検出されたアイテムのリストとファイル固有の詳細ページを使用すると、管理者は複数のデバイスにわたるファイルのフットプリントを追跡できます。

最新問題**: 38**
単一の管理プラットフォームが接続できる SEPM の最大数はいくつですか?
A. 50
B. 10
C. 5,000
D. 500
Answer: A (メーッセージを残す**)**
単一の管理プラットフォームが接続できる Symantec Endpoint Protection Manager (SEPM) の最大数は 50 です。この制限により、管理プラットフォームは、システムに過負荷をかけることなく、接続された SEPM 間で通信、ポリシー配布、レポートを処理できるようになります。
* 50 SEPM制限の重要性:
* この制限は、特に広範な環境をサポートするために複数の SEPM が必要となる大規模な展開において、安定したパフォーマンスと効果的な管理を確保するために設けられています。
* 大企業における関連性:

* 複数の場所にまたがるエンドポイントを管理する組織では、多くの場合、複数の SEPM を使用します。プラットフォームの 50 マネージャーの制限により、集中管理を維持しながら拡張性が実現されます。
参考資料: SEPM 接続制限は、Symantec Endpoint Protection のアーキテクチャ仕様の一部として文書化されています。

最新問題: **39**
ある組織では最近、感染が発生し、環境のヘルス チェックを実施しています。SEP チームは、アプリケーションの動作を制御および監視するためにどのような保護テクノロジーを有効にできますか?
A. ホスト整合性
B. システムロックダウン
C. アプリケーション制御
D. 動作監視 (SONAR)
Answer: C (メーッセージを残す**)**
Symantec Endpoint Protection (SEP) のアプリケーション制御により、SEP チームにはアプリケーションの動作を制御および監視する機能が提供されます。このテクノロジにより、管理者は特定のアプリケーションの動作を制限または許可するポリシーを設定でき、環境を効果的に制御し、許可されていないアプリケーションや有害なアプリケーションによるリスクを軽減できます。仕組みは次のとおりです。
* ポリシーベースの制御:管理者は、許可または制限されるアプリケーションを定義するポリシーを作成し、許可されていないアプリケーションの実行を防ぐことができます。
* 動作監視: アプリケーション制御は、アプリケーションのアクションを監視し、異常な動作や潜在的に有害な動作を検出して管理者に警告します。
* 強化されたセキュリティ: アプリケーションの動作を制御することで、SEP は疑わしいアプリケーションが環境に影響を与えるのを防ぎ、脅威を軽減するのに役立ちます。これは、感染後の回復や継続的なヘルス チェックに特に役立ちます。
アプリケーション制御は、アプリケーションの動作をリアルタイムで管理できるようにすることで、エンドポイントの防御を強化します。

最新問題: **40**
Active Directory がほぼすべての標的型攻撃の一部となっているのはなぜですか?
A. AD 管理は、弱いレガシー API によって管理されます。
B. ADは、設計上、簡単にアクセスできるフラットなファイル名空間ディレクトリデータベースです。
C. ADは、ネットワーク内のすべてのエンドポイントにすべてのID、アプリケーション、リソースを公開します。
D. AD ユーザーの属性には、非表示の昇格された管理者権限が含まれます
Answer: C (メーッセージを残す**)**

Active Directory (AD) は、ネットワーク全体でアクセス可能なユーザー ID、アプリケーション、リソースの中央ディレクトリとして機能するため、攻撃の標的となることがよくあります。この可視性により、攻撃者は AD を横方向の移動、権限の昇格、偵察に悪用する魅力的なターゲットとしています。AD が侵害されると、攻撃者は組織の内部構造に関する重要な情報を入手し、機密データへのさらなる悪用やアクセスが可能になります。

最新問題: **41**
管理者は、SES Complete ハイブリッド環境を完全にクラウド管理された環境に移行することを決定します。
オンプレミスのグループ構造とポリシーをクリーンアップした後、移行の次の推奨手順は何ですか?
A. SEPMから固有のポリシーをエクスポートする
B. SEPMをICDmに登録する
C. ICDmからエージェントを移行する
D. ICDm に固有のポリシーをインポートする
Answer: A (メーッセージを残す**)**
SES Complete ハイブリッド環境を完全なクラウド管理セットアップに移行する場合、オンプレミスのグループ構造とポリシーをクリーンアップした後の次の推奨手順は、SEPM から固有のポリシーをエクスポートすることです。これにより、次のことが保証されます。
* ポリシーの継続性: SEPM からポリシーをエクスポートすると、クラウド環境で複製または適応する必要がある固有の構成が保持されます。
* ICDm へのインポートの準備: エクスポートされたポリシーは ICDm にインポートできるため、特定のポリシーのカスタマイズを失うことなく、よりスムーズな移行が可能になります。
このステップは、環境がクラウド管理に移行する際に一貫したセキュリティ ポリシーの適用を維持するために重要です。

最新問題: **42**
LiveShell はどのプラットフォームで利用できますか?
A. ウィンドウ
B. すべて
C. Linux
D. マック
Answer: (解答を表示する**)**
LiveShell は、Windows、Linux、Mac など複数のプラットフォームで利用できるシマンテックのツールです。管理者は、エンドポイントでライブ コマンドライン シェルを開いて、オペレーティング システムに関係なくリモート トラブルシューティングと応答機能を提供できます。
* クロスプラットフォームの可用性:

* LiveShell のクロスプラットフォーム サポートにより、管理者は Windows、Linux、または macOS を実行しているエンドポイントでインシデントに対応し、問題をトラブルシューティングし、コマンドを実行できます。
* LiveShellの使用例:
* このツールは、コマンドやスクリプトのエンドポイントにすばやくアクセスする必要があるインシデント対応チームにとって便利であり、さまざまな環境にわたる脅威の管理と軽減に役立ちます。
参考資料: LiveShell はすべての主要プラットフォームで利用できるため、異機種環境全体で Symantec のエンドポイント管理および応答機能が強化されます。

最新問題: **43**
管理者が特定のエンドポイント プロファイルに基づいてポリシーを適用するのに役立つ SES 機能はどれですか?
A. ポリシーバンドル
B. デバイスプロファイル
C. ポリシーグループ
D. デバイスグループ
Answer: D (メッセージを残す**)**
Symantec Endpoint Security (SES) では、デバイス グループにより、管理者は特定のエンドポイント プロファイルに基づいてポリシーを適用できます。デバイス グループは、部門、場所、デバイスの種類などの特性に従ってエンドポイントを分類し、各グループの特定のセキュリティ ニーズを満たすカスタマイズされたポリシーの適用を可能にします。デバイス グループを使用することで、管理者はセキュリティ ポリシーを効率的に管理し、エンドポイントのプロファイルに基づいて適切な保護を適用できます。

最新問題: **44**
ある組織には、開発者のグループがテスト用に利用する仮想化環境があります。この組織は、スケジュールされたスキャンを実行するときにパフォーマンスを最適化するためにどの機能を利用できますか?
A. 早期マルウェア対策 (ELAM) 検出を無効にする
B. 仮想化環境で共有インサイトキャッシュを使用する
C. スケジュールされたスキャンをランダム化する
D. 自動保護設定を調整する
Answer: B (メッセージを残す**)**
仮想化環境では、Symantec Endpoint Protection (SEP) は、冗長なスキャンを削減してパフォーマンスを向上させる機能として Shared Insight Cache (SIC) を提供します。
* 共有インサイトキャッシュ機能:
* SIC を使用すると、仮想環境内の SEP クライアントはスキャン結果を共有できます。ファイルがスキャンされて安全であると判断されると、その結果はキャッシュされ、他の

SEP クライアント間で共有されるため、異なる仮想マシン (VM) 上で同じファイルが重複してスキャンされるのを防ぐことができます。
* このキャッシュ メカニズムは、ソフトウェア ライブラリやシステム ファイルなど、複数の VM が同一のファイルを頻繁に使用する環境で特に役立ちます。
* 最適化されたパフォーマンス:
* SIC は繰り返しのスキャンを減らすことで CPU とディスクの使用を最小限に抑え、スケジュールされたスキャン中でも仮想化環境のパフォーマンスを維持できるようにします。
* このアプローチは、VM の効率性が生産性にとって非常に重要となる開発環境やテスト環境に最適です。
* 他のオプションがあまり適していない理由:
* ELAM を無効にしたり、Auto-Protect 設定を調整したりすると、セキュリティが低下したり、仮想化環境の全体的なパフォーマンスに限られた影響しか与えなかったりする可能性があります。
* スケジュールされたスキャンをランダム化すると、リソース負荷を分散するのに役立ちますが、VM 間での冗長なスキャンを防ぐことはできません。
参考資料: Shared Insight Cache は、仮想環境に関する SEP のベスト プラクティスで説明されているように、仮想化セットアップで SEP のパフォーマンスを最適化するように特別に設計されています。

最新問題**: 45**
ウイルスおよびスパイウェア対策ポリシーで、管理者は最初のアクションを 『クリーニング」リスクに設定し、最初のアクションが失敗した場合は 『削除」リスクに設定します。管理者が考慮すべき要素はどれですか (2 つ選択してください)。
A. 削除されたファイルがまだごみ箱に残っている可能性があります。
B. IT Analytics は調査のためにファイルのコピーを保持する場合があります。
C. 誤検知により正当なファイルが削除される可能性があります。
D. Insight は、Symantec に送信する前にファイルをバックアップする場合があります。
E. 脅威のコピーがまだ隔離されている可能性があります。
Answer: (解答を表示する**)**
最初に 『リスクをクリーンアップ」し、クリーンアップが失敗した場合は 『リスクを削除」するアクションでウイルスおよびスパイウェア対策ポリシーを構成する場合、次の 2 つの重要な考慮事項があります。
* 誤検知 (C): クリーニング アクションが失敗すると、正当なファイルが誤って脅威として識別され、削除されるリスクがあります。この結果は、重要なファイルの損失を回避するために、ポリシーを慎重に構成することの重要性を強調しています。
* 隔離コピー (E): ファイルが削除された場合でも、隔離コピーが残っている場合があります。このバックアップにより、削除が誤検知であった場合や、調査のためにファイルのさらなる分析が必要な場合に、ファイルを取得できます。

これらの考慮事項は、管理者が意図しないデータ損失を回避し、隔離された脅威を将来的に確認するための柔軟性を維持するのに役立ちます。

最新問題: **46**
Symantec Insight の機能は何ですか?
A. 構造化データの評判評価を提供します
B. グループ更新プロバイダー (GUP) の機能を強化します。
C. LiveUpdateの効率と効果を高めます
D. バイナリ実行ファイルの評価を提供します
Answer: (解答を表示する**)**
Symantec Insight は、バイナリ実行ファイルの評判評価を提供するテクノロジです。このシステムは、世界中の何百万ものユーザーからの情報を集約する Symantec の Global Intelligence Network のデータを活用します。仕組みは次のとおりです。
* ファイル レピュテーション データベース:Symantec Insight は、普及度、発生元、動作などのさまざまな要素に基づいて、各実行ファイルにレピュテーション スコアを割り当てます。
* 動的な意思決定: これらの評価を参照することで、SEP はファイルが安全か潜在的に有害かを動的に判断し、それに応じてファイルを許可またはブロックできます。
* 誤検知の削減:Insight は、広く使用されている正当なファイルと、まれで潜在的にリスクのあるファイルを区別できるため、誤検知を削減するのに役立ちます。
このレピュテーションベースのアプローチは、従来のシグネチャベースの検出だけに頼ることなく、疑わしいファイルを事前に識別することで保護を強化します。

最新問題: **47**
管理者は、特定のグループのウイルスおよびスパイウェア対策ポリシーを変更し、Auto-Protect を無効にします。管理者はポリシーを割り当て、クライアント システムは対応するポリシー シリアル番号を適用します。物理的なクライアント システムを目視で検査すると、ポリシー シリアル番号は正しいです。ただし、クライアント システムでは Auto-Protect がまだ有効になっています。
クライアントに必要な設定が確実に行われるようにするには、管理者はどのようなアクションを実行する必要がありますか?

A. クライアントシステムを再起動します
B. コンピュータ上でコマンドを実行してコンテンツを更新する
C. ポリシーの設定の横にある南京錠を有効にする
D. ウイルスおよびスパイウェア対策ポリシーを撤回する
Answer: (解答を表示する**)**
管理者がウイルスとスパイウェア対策ポリシーを変更して Auto-Protect を無効にしたにもかかわらず、クライアントで Auto-Protect がまだ有効になっている場合、設定がロックされていないことが原因である可能性があります。Symantec Endpoint Protection ポリシーでは、設定の横にある南京錠アイコンを有効にすると、ポリシーが厳密に適用され、ローカルクライアント設定が上書きされます。このロックがないと、クライアントは新しいポリシーにもかかわらず以前の設定を保持する可能性があります。設定をロックすると、指定したグループ内のすべてのクライアントに、必要な設定が一貫して適用されることが保証されます。

最新問題**: 48**
エンドポイント通信チャネル (ECC) 2.0 により、Symantec EDR は直接何に接続できるようになりますか?
A. SEDR クラウド コンソール
B. シナプス
C. SEP エンドポイント
D. セプム
Answer: D (メーッセージを残す**)**
エンドポイント通信チャネル (ECC) 2.0 により、Symantec Endpoint Detection and Response (EDR) は Symantec Endpoint Protection Manager (SEPM) と直接接続できるようになります。この接続により、次のことが可能になります。
* 効率的なデータ交換:ECC 2.0 は、SEPM と Symantec EDR 間のリアルタイム通信とデータ交換を容易にします。
* エンドポイントの可視性の強化: SEPM に直接接続することで、Symantec EDR はエンドポイントのアクティビティをより詳細に監視し、脅威の検出と対応を改善できます。
* 統合脅威管理:ECC 2.0 は、SEPM と EDR 間の協調的な取り組みをサポートし、脅威のより効果的な封じ込めと軽減を可能にします。
SEPM との直接通信により、EDR のエンドポイントを効果的に管理および保護する機能が強化されます。

最新問題**: 49**
SEDR Isolate 機能を使用するにはどの SEP 機能が必要ですか?
A. ホスト分離ポリシー
B. アプリケーション制御
C. ホスト整合性ポリシー
D. アプリケーション検出

Answer: (解答を表示する**)**
Symantec Endpoint Protection (SEP) のホスト整合性ポリシーは、Symantec Endpoint Detection and Response (SEDR) の分離機能を使用するために必要です。ホスト整合性により、管理者はエンドポイントでセキュリティ コンプライアンスを強制することができ、分離機能に不可欠で、非準拠または侵害されたシステムがネットワークと通信できないようにします。
* ホスト整合性ポリシーが分離をサポートする方法:
* ホスト整合性を適用することで、SEP はエンドポイントがネットワーク アクセスを許可する前にセキュリティ要件に準拠していることを保証し、準拠していない場合は隔離することができます。
* このポリシーは、応答性の高い脅威の封じ込めのために SEDR の分離機能と統合するフレームワークを提供します。
* 他のオプションが適さない理由:
* ホスト分離ポリシー (オプション A) は実際の SEP 機能ではありません。
* アプリケーション制御 (オプション B) はアプリケーションの動作を管理しますが、エンドポイントの分離には結び付けられません。
* アプリケーション検出 (オプション D) はアプリケーションを識別しますが、分離は処理しません。
参考資料: SEP のホスト整合性ポリシーは、SEDR と組み合わせて分離機能を実装する上で不可欠です。

最新問題**: 50**
環境でアプリケーション学習を有効にする際に管理者が考慮する必要がある 2 つの考慮事項はどれですか? (2 つ選択してください。)
A. アプリケーション学習により誤検知が増加する可能性があります。
B. アプリケーション ラーニングは、企業内の少数のシステムに導入する必要があります。
C. アプリケーション学習により、Symantec Endpoint Protection Manager で CPU またはメモリの使用量が大幅に増加する可能性があります。
D. アプリケーション学習では、事前にファイル フィンガープリント リストを作成する必要があります。
E. E.Application Learning は Insight に依存します。
Answer: (解答を表示する**)**
Symantec Endpoint Protection (SEP) でアプリケーション学習を有効にする場合、管理者は次の点を考慮する必要があります。
* 誤検知の増加: アプリケーション学習では、必ずしも脅威とは限らない、なじみのないアプリケーションや珍しいアプリケーションが識別されるため、誤検知が増加する可能性があります。
* パイロット展開の推奨: 潜在的な混乱を軽減するために、アプリケーション ラーニングは最初はシステムの小さなサブセットに展開する必要があります。このアプローチにより、

管理者は、その影響を観察し、ポリシーを調整し、収集された学習データを制御してから、企業全体に展開することができます。
これらの考慮事項は、リソースの影響を管理し、アプリケーション学習の正確性を確保するのに役立ちます。

最新問題: **51**
組織内で断片的なテレメトリ収集方法を使用すると、どのような結果になるでしょうか?
A. 調査員は詳細な可視性に欠けている
B. コントロール間のオーケストレーションの背後
C. 誤検知が見られる
D. 調査中も攻撃は拡大し続けている
Answer: (解答を表示する**)**
組織内でテレメトリ収集が断片化されると、調査担当者が詳細な可視性を得られない可能性があります。これが問題となる理由は次のとおりです。
* 不完全なデータ: 収集方法が断片化されるとデータが断片化され、セキュリティ チームがインシデントの全体像を把握することが難しくなります。
* 調査効率の低下: きめ細かくまとまったテレメトリがないと、調査員は攻撃の経路を正確に追跡することが難しくなり、対応時間が遅くなります。
* 重要な指標を見逃すリスクの増加: 侵害の重要な指標が見落とされ、環境内で脅威が存続したり再発したりする可能性があります。
統合テレメトリは、脅威を完全に理解して軽減するために必要な詳細な洞察を提供するため、徹底的かつ効率的な調査に不可欠です。

最新問題: **52**
デバイスが会社のセキュリティ標準に準拠していることを確認するのに役立つ SES 機能はどれですか?
A. ホスト整合性
B. 集中防御
C. 信頼できるアップデーター
D. 適応型保護
Answer: (解答を表示する**)**
ホスト インテグリティは、デバイスが企業のセキュリティ標準に準拠していることを確認する Symantec Endpoint Security (SES) の機能です。この機能は、システム構成の検証、必要なソフトウェア (ウイルス対策やファイアウォールの設定など) の確認、組織が指定したその他のコンプライアンス基準の検証によって実行されます。
* ホストインテグリティの機能:
* ホスト整合性チェックは、ネットワーク アクセスを許可する前に、各エンドポイントが必要なセキュリティ構成を満たしていることを確認するように設計されています。
* デバイスが非準拠の場合、ホスト整合性は、ソフトウェアの更新や管理者への警告などの修復手順を強制して、デバイスを準拠状態にすることができます。

* 他のオプションがあまり適していない理由:
* 集中保護 (オプション B) と適応型保護 (オプション D) は、アクティブな脅威の検出に重点を置いていますが、コンプライアンスの強制には重点を置いていません。
* 信頼できるアップデーター (オプション C) は、全体的なコンプライアンス チェック用ではなく、アラートをトリガーせずに特定のソフトウェア更新を許可するためのものです。
参考資料: ホスト整合性は、デバイス間でのセキュリティ ポリシーの遵守を促進し、ネットワーク全体のコンプライアンスを確保する SES の重要な機能です。

最新問題: **53**
Symantec Endpoint Protection Manager と Active Directory の統合を設定するときに推奨される Symantec のベストプラクティスは何ですか?
A. サーバー プロパティに複数の Active Directory サーバーがリストされていることを確認します。
B. 組み込みの管理者アカウントを Active Directory アカウントにリンクします。
C. 既存の AD 構造をインポートして、ユーザー モードでクライアントを整理します。
D. 特定のコンピュータへのアクセスを拒否して管理コンソールを保護します。
Answer: C (メーッセージを残す**)**
Symantec Endpoint Protection Manager (SEPM) との Active Directory (AD) 統合を設定する場合、Symantec のベスト プラクティスは、既存の AD 構造をインポートして、ユーザー モードでクライアントを管理することです。このアプローチには、次のようないくつかの利点があります。
* 簡素化されたクライアント管理: AD 構造をインポートすることで、SEPM は AD で既に定義されている組織構造をミラーリングできるため、グループまたは組織単位へのポリシーの管理と割り当てが容易になります。
* ユーザーベースのポリシー: クライアントをユーザー モードで整理すると、ポリシーがデバイス間でユーザーを追跡できるようになり、ユーザーがログインする場所に関係なく一貫した保護が提供されます。
* 合理化された更新と権限: AD との統合により、ユーザー アカウントまたはグループの変更が SEPM 内で自動的に反映され、クライアント組織における管理作業と潜在的なエラーが削減されます。
このベスト プラクティスは、AD で確立された構造を活用して SEPM の機能を強化します。

最新問題: **54**
クラウド コンソールに関して生成されるイベントが含まれるアラート ルール カテゴリはどれですか?
A. セキュリティ
B. システム
C. 診断
D. アプリケーションアクティビティ

Answer: B (メーッセージを残す)
システムアラート ルール カテゴリには、クラウド コンソールに関して生成されたイベントが含まれます。これらのアラートは、管理アクション、システム ヘルス チェック、コンソール操作に関連するその他の重要な通知など、管理コンソール内のシステム レベルのアクティビティに関連しています。
* システムカテゴリのアラートの種類:
* システムアラートは、コンソールとインフラストラクチャに直接関連するアクティビティをカバーし、管理プラットフォーム自体に影響する重要な変更や問題について管理者に通知します。
* 他のオプションが間違っている理由:
* セキュリティ (オプション A) は、潜在的な脅威とセキュリティ イベントに重点を置いています。
* 診断 (オプション C) にはトラブルシューティング情報が含まれますが、コンソール イベントは具体的にはカバーされません。
* アプリケーション アクティビティ (オプション D) は、コンソール レベルの通知ではなく、アプリケーション固有のイベントに関係します。
参考: システム アラートは、コンソールの運用整合性を管理および維持するために重要な、クラウド コンソール関連のイベントの可視性を提供します。

最新問題**: 55**
カスタム侵入防止シグネチャを作成する前に、Symantec Endpoint Protection 管理者が実行する必要があるアクションは何ですか?
A. カスタム署名の順序を変更する
B. カスタム侵入防止シグネチャライブラリを作成する
C. シグネチャ変数を定義する
D. 署名ログを有効にする
Answer: C (メーッセージを残す)
カスタム侵入防止シグネチャを作成する前に、Symantec Endpoint Protection (SEP) 管理者はシグネチャ変数を定義する必要があります。これらの変数を定義すると、カスタム シグネチャ内で使用される特定の値 (IP アドレスやポート番号など) をカスタマイズできるようになり、脅威検出の柔軟性と精度が向上します。
* 署名変数の役割:
* 署名変数を使用すると、管理者は複数の署名で再利用できるパラメータを定義して、カスタム署名を特定のニーズに合わせて調整できます。
* この最初のステップは、カスタム シグネチャが正しく機能し、目的の脅威またはネットワーク動作をターゲットにしていることを確認するために重要です。
* 他のオプションが間違っている理由:
* カスタム署名の順序の変更 (オプション A) は、署名の作成後に実行されます。
* 事前のアクションとして、カスタム侵入防止シグネチャ ライブラリ (オプション B) を作成する必要はありません。

* 署名ログの有効化 (オプション D) は監視目的ではオプションですが、カスタム署名を作成するための前提条件ではありません。
参考資料: シグネチャ変数の定義は、SEP で効果的なカスタム侵入防止シグネチャを作成するための重要な準備手順です。

最新問題: **56**
ICDm からファイルをダウンロードする前に何を入力する必要がありますか?
A. 名前
B. パスワード
C. ハッシュ
D. 日付
Answer: C (メーッセージを残す**)**
統合サイバー防御マネージャー (ICDm) からファイルをダウンロードする前に、ファイルのハッシュを入力する必要があります。ハッシュはファイルの一意の識別子として機能し、正しいファイルがダウンロードされたことを確認し、その整合性を検証します。これが必要な理由は次のとおりです。
* ファイル検証:ハッシュを入力することで、ユーザーは正しいファイルにアクセスしていることを確認し、無関係なファイルや潜在的に有害なファイルを誤ってダウンロードすることを防ぎます。
* セキュリティ対策:ハッシュ要件によりセキュリティがさらに強化され、機密ファイルの不正ダウンロードや配布を防ぐことができます。
この方法により、ICDm 内での正確かつ安全なファイル管理が保証されます。