Cisco.300-745.v2026-11-11.q48

試験コード：	300-745
試験名称：	Designing Cisco Security Infrastructure
認証ベンダー：	Cisco
無料問題の数：	48
バージョン：	v2026-11-11
ページの閲覧量：	109
問題集の閲覧量：	536

https://www.jpnshiken.com/shiken/Cisco.300-745.v2026-11-11.q48.html

質問: **1**
企業内のネットワーク機器、エンドポイント、その他のソースからログを収集、分析、視覚化するために使用されるツールはどれですか？
A. Cisco Email Security Appliance
B. クラウドの可観測性
C. Cisco Web Security Appliance
D. Splunk
正解: **D** (コメントを発表する)
Splunkは、ネットワーク機器、エンドポイント、アプリケーションなど、さまざまなソースからのログを収集、分析、視覚化するために使用されるSIEM（セキュリティ情報イベント管理）およびログ管理ツールです。セキュリティ監視とインシデント対応のための集中管理された可視性を提供します。

質問: **2**
インシデント対応とコンプライアンスの目標に合致するベストプラクティスを2つ選択してください。
A. 不変ログを維持する
B. リアルタイム監視を実施する
C. 共有管理者認証情報を使用する
D. 監査を無効にしてパフォーマンスを向上させる
正解: (正解を表示します)
改ざん不可能なログは証拠の完全性を維持し、リアルタイム監視はより迅速な検出と対応を可能にする。これらはどちらも、インシデント対応と規制遵守にとって不可欠である。

質問: **3**
ある銀行は、侵害されたエンドポイントが内部ネットワークにアクセスするという問題に直面しました。セキュリティを強化するため、銀行はすべてのエンドポイントがネットワークへのアクセスを許可される前に、コンプライアンスチェックのためにスキャンされることを保証したいと考えています。どの対策が、このレベルのセキュリティと制御を実現しますか？
A. Cisco DUOを使用してMFAを使用します。
B. Cisco ISEを使用してTrustSecを設定します。
C. データ損失防止ポリシーを設定する。

D. Cisco ISEを使用して姿勢検証を実装します。
正解: **D** (コメントを発表する)
Cisco ISEによるポスチャ検証では、ネットワークアクセスを許可する前にエンドポイントのコンプライアンス（ウイルス対策の状態、パッチ適用状況、セキュリティ設定など）を確認します。これにより、侵害されたエンドポイントやコンプライアンス違反のエンドポイントへのアクセスが拒否され、銀行のセキュリティ上の懸念に直接対処できます。

質問: **4**
ある私立大学のネットワークセキュリティチームは、ネットワークインフラ全体のセキュリティ体制を評価するため、包括的な監査を実施しています。監査中に、セキュリティチームは、信頼できるベンダーから、大学のCI/CDパイプラインにおいて重要な役割を担う製品に重大な脆弱性が発見されたことを知りました。セキュリティチームは、これらの脆弱性によって生じる潜在的なリスクを軽減するために、迅速に対応する必要があります。セキュリティチームは、この情報開示を受けて、まずどのような対応を取るべきでしょうか？
A. IDSを活用して脆弱性の影響を測定する。
B. 顧客にその影響と原因を通知する
C. 企業環境における製品の存在を検証することで、影響を確認する
D. 影響を受けた製品をできるだけ早く修理してください。
正解: (正解を表示します)
脆弱性が開示された後の最初のステップは、影響を受ける製品が組織の環境に存在するかどうかを確認することです。これにより、パッチを適用したり関係者に通知したりする前に、脆弱性が関連性のあるものかどうかが確実になり、無駄な労力を省き、実際の脆弱性への対応に集中することができます。

質問: **5**
大規模大学の管理者は、新入社員がオンボーディング時に適切なアクセス権限を持つようにしたいと考えています。管理者はチームに対し、クラウド環境を設定し、新入社員の役割と責任に基づいて適切なアクセス権限が付与されるようにするよう依頼しました。適切なアクセス権限を確保するために推奨される手法はどれでしょうか？
A. IDアクセス管理
B. セキュリティグループ
C. VPN
D. ネットワークアクセス制御リスト
正解: **A** (コメントを発表する)
IDアクセス管理（IAM）は、役割ベースのアクセス制御を強制し、新入社員がその役割と責任に応じた適切な権限を自動的に付与されるようにします。このアプローチにより、過剰または不適切なアクセスが防止され、クラウド環境のセキュリティが確保されます。

質問: **6**
あるテクノロジー企業には、さまざまな場所から企業リソースにアクセスするリモートワーカーが多数います。同社は、セキュリティポリシーがエンドポイント上で直接管理および適用され、場所に関係なくエンドポイントが脅威から保護されることを保証する必要があります。どのファイアウォールアーキテクチャがこれらの要件を満たしますか？
A. 次世代ファイアウォール
B. ホストベースファイアウォール

C. Webアプリケーションファイアウォール
D. 従来のファイアウォール
正解: **B** (コメントを発表する)
ホストベースのファイアウォールは、エンドポイントに直接セキュリティポリシーを適用することで、場所に関係なくエンドポイントを保護します。このアーキテクチャは、従来のネットワーク境界外から企業リソースにアクセスするリモートワーカーに対し、一貫した防御を提供します。

質問: **7**
コンテナ化されたマイクロサービスアーキテクチャにおいて、安全な通信をサポートする2つのアプローチはどれですか？ 2つ選択してください。）
A. サービス間の相互TLS
B. 共有サービスアカウントの認証情報
C. ポリシー適用機能を備えたサービスメッシュ
D. 静的NATエントリ
正解: (正解を表示します)
相互TLS（mTLS）は、サービス間の暗号化された通信と相互認証を提供します。サービスメッシュは、集中管理されたセキュリティポリシーを適用し、マイクロサービス間の安全な通信を自動化します。

質問: **8**
ある通信会社が最近、ハイブリッド勤務モデルを導入しました。この新しい方針に基づき、従業員は会社の機器を使用すれば週2日間リモートワークを行うことができます。IT部門は、リモートワーク期間中にユーザーをサポートするために、会社のノートパソコンを準備しています。ノートパソコンが盗難された場合でも、会社のリソースへの安全な接続を提供し、機密性の高い企業データを保護するには、IT部門はどのようなソリューションを導入すべきでしょうか？
A. セキュアクライアント
B. シスコデュオ
C. ISE姿勢
D. 傘
正解: (正解を表示します)
Cisco Secure Client（旧称AnyConnect）は、ハイブリッドワークフォースの複雑な環境に対応するために設計された包括的なソリューションです。Secure Clientは、企業の要件を満たすために、リモートラップトップと企業リソース間のすべてのトラフィックが暗号化および認証される安全なVPNトンネル（SSLまたはIPsec）を提供します。
特に、ノートパソコンが盗難された場合、Secure Clientは様々なエンドポイントセキュリティモジュールと連携します。Secure Clientは主にセキュアな接続を管理しますが、常時接続VPNやディスク暗号化ステータスの管理といった機能も提供するプラットフォームです。Cisco Security Infrastructureの設計原則によれば、Secure Clientはエンドポイント上の統合エージェントとして機能し、ユーザーの場所に関係なくセキュリティ体制と接続性を維持します。
Cisco Duo（オプションB）は、ユーザーの身元を確認するための必須の多要素認証（MFA）を提供しますが、データ転送用の暗号化トンネルは提供しません。ISE Posture（オプションC）は、デバイスの状態をチェックする機能（多くの場合、セキュアクライアント経由で提供されます）ですが、接続自体は提供しません。
アンブレラ（オプションD）は、悪意のあるサイトからユーザーを保護し、DNS/Webセキュリティのためのローミングクライアントを提供しますが、企業のプライベートリソースへのセキュアトンネルの必要性を代替するものではありませ

ん。したがって、セキュアクライアントは、リモートユーザーと企業データセンター間のギャップを埋め、デバイスが組織のセキュリティ傘下に留まることを保証する包括的なソリューションです。

質問: **9**
どのデザインポリシーが、生成型AIによる有害コンテンツの作成に対処していますか？
A. 量子耐性暗号化
B. 透かし
C. 検索拡張生成
D. 人間がループに参加する
正解: **(**正解を表示します**)**
ウォーターマーキングとは、AIが生成したコンテンツに隠された識別子を埋め込む、生成型AIの設計ポリシーです。これにより、追跡可能性と説明責任が確保され、悪意のある、あるいは誤解を招くAI出力の検出と規制が容易になるため、有害なコンテンツ作成のリスクに対処するのに役立ちます。

質問: **10**
あるエンジニアリング会社の最高財務責任者（CFO）が、緊急メールに返信したことでフィッシング詐欺の被害に遭いました。そのメールは信頼できるビジネスパートナーからのものに見せかけ、機密性の高い税務情報を要求していました。この事件により、会社は深刻な金銭的損害と評判の低下を被りました。今後同様の事態を防ぐため、セキュリティチームは効果的な対策を講じる必要があります。セキュリティチームは、今後同様の事態を防ぐために、どのような対策を講じるべきでしょうか？
A. 上流トラフィックフィルタ
B. 対象を絞った教育キャンペーン
C. データ損失防止戦略
D. きめ細かな港湾セキュリティ戦略
正解: **(**正解を表示します**)**
ターゲットを絞った教育キャンペーンは、従業員、特に経営幹部などの重要人物に対し、ソーシャルエンジニアリングの試みを認識できるよう訓練することで、フィッシングに直接対処します。技術的な対策も有効ですが、フィッシングは主に人間の行動を悪用するため、意識向上と訓練が最も効果的な予防策となります。

質問: **11**
生成型AIはネットワークのセキュリティ確保にどのように活用されているのか？
A. リアルタイムの負荷分散を提供する
B. 資源消費を改善する
C. 規制遵守を確保するためにリアルタイム監査を実施する
D. ネットワークトラフィックの異常なパターンを検出する
正解: **D (**コメントを発表する**)**
生成型AIは、トラフィックパターンの異常を特定することでネットワークセキュリティを強化します。通常のネットワーク動作を学習し、侵入やデータ漏洩の試みなど、脅威を示唆する可能性のある逸脱を検出します。

質問: **12**

マルチクラウドワークロード全体で一貫したポリシー適用を確保するのに役立つ2つのソリューションはどれですか？（2つ選択してください。）
A. Cisco Secure Workload（テスト）
B. SNMPトラップ
C. クラウド型ファイアウォール（CDFW）
D. 静的IPルーティング
正解: **(**正解を表示します**)**
Cisco Secure Workloadは、環境全体にわたるワークロードの可視化とポリシーの適用を提供し、クラウドベースのファイアウォールは、複数のクラウドプラットフォームにわたって一貫したセキュリティポリシーを適用します。

質問: **13**
製薬会社がハブアンドスポーク型のVPNトポロジーを必要としています。設計では、部分メッシュ型またはフルメッシュ型のオーバーレイネットワークを構築できる必要があります。この環境にはどのVPNソリューションを実装すべきでしょうか？
A. DMVPN
B. L2TP
C. 暗号マップ
D. SSL VPN
正解: **(**正解を表示します**)**
ダイナミックマルチポイントVPN（DMVPN）は、ハブアンドスポーク型のトポロジーをサポートしつつ、必要に応じて部分的なメッシュオーバーレイやフルメッシュオーバーレイを柔軟に構築できます。静的な設定を必要とせず、拡張性と動的なVPNトンネルを提供するため、この要件に最適です。

質問: **14**
製薬会社の従業員が誤ってAWSシークレットキーを含むコードをパブリックGitHubリポジトリにチェックインしてしまい、本番環境のリソースが攻撃者に晒される事態が発生した。セキュリティエンジニアは、このような事態の再発を防ぐために、どのような対策を推奨すべきか？
A. Webアプリケーションファイアウォールを追加します。
B. よりきめ細かな港湾セキュリティ戦略を実施する。
C. フィッシングに関する啓発キャンペーンを実施する。
D. SCMのプリコミットフックを設定します。
正解: **(**正解を表示します**)**
APIキーやAWSシークレットなどの機密情報が誤って漏洩することは、現代のDevOps環境における大きなリスクです。このような事態を防ぐための最も効果的な技術的対策は、ソースコード管理（SCM）のプリコミットフックを実装することです。プリコミットフックとは、コミットが確定してリモートリポジトリにプッシュされる前に、開発者のマシン上でローカルに実行されるスクリプトです。
CiscoのDevSecOps設計原則によれば、プリコミットフックを設定することで、コードをスキャンして機密情報に類似した特定のパターン（例えば、AWSアクセスキーIDの正規表現）を検出できます。スキャナーが機密情報を検出すると、コミットが自動的に中止され、開発者はコードがローカルマシンから送信される前に、機密データを削除するか適切に

暗号化する必要があります。これにより、情報漏洩を発生源で阻止する即時的な「シフトレフト」セーフティネットが実現します。
Webアプリケーションファイアウォール（WAF）（オプションA）は外部からの攻撃を防ぎ、ポートセキュリティ（オプションB）はレイヤ2アクセスを管理しますが、どちらも開発者がGitHubにコードをプッシュすることを阻止することはできません。フィッシング対策教育キャンペーン（オプションC）は一般的なセキュリティ意識向上には役立ちますが、認証情報の漏洩を阻止するために必要な自動化された技術的な対策は提供しません。製薬会社はプリコミットフックを設定することで、認証情報漏洩のリスクを大幅に軽減し、Cisco SDSIカリキュラムの自動化目標に合致する、積極的な防御メカニズムを確立します。

質問: **15**
ある石油・ガス会社は最近、従業員のメモ帳から重要なログイン認証情報が盗まれ、セキュリティ侵害に見舞われた。この事件によりユーザーアカウントへの不正アクセスが発生し、機密性の高い企業データと業務に重大なリスクが生じた。同社はユーザーアカウントの保護を強化するセキュリティ対策を導入したいと考えている。今後このような侵害を防ぐためには、どのような対策を講じるべきだろうか？
A. MFAを実装する
B. シングルサインオンを実装する。
C. RADIUSサーバーを更新します。
D. パスワード有効期限ポリシーを設定します。
正解: (正解を表示します)
多要素認証（MFA）は、パスワードに加えてトークンや生体認証などの追加の認証要素を要求することで、ユーザーアカウントのセキュリティを強化します。認証情報が盗まれた場合でも、MFAは不正アクセスを防止し、情報漏洩のシナリオに直接対処します。

質問: **16**
自動化されたセキュリティ対応ワークフローのパフォーマンスを評価する上で重要な指標はどれですか？（2つ選択してください。）
A. 平均検出時間（MTTD）
B. CPU温度
C. VLAN伝播速度
D. 平均応答時間（MTTR）
正解: (正解を表示します)
MTTDはインシデントが検知されるまでの速さを、MTTRはインシデントが解決されるまでの速さを測定する指標です。これら2つを合わせると、自動化されたセキュリティ対応ワークフローの有効性を示す指標となります。

有効的な**300-745**問題集はJPNTest.com提供され、**300-745**試験に合格することに役に立ちます！JPNTest.comは今最新**300-745**試験問題集を提供します。JPNTest.com 300-745試験問題集はもう更新されました。ここで**300-745**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/300-745-mondaishu
773問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
あるビデオゲーム会社は、オンラインゲームサービスを中断させ、ユーザーエクスペリエンスに影響を与える可能性のあるSYNフラッド攻撃の潜在的な脅威を特定しました。この攻撃はTCPハンドシェイクプロセスを悪用することでネットワークリソースを過負荷状態にし、サーバーの利用不能やパフォーマンスの低下を引き起こす可能性があります。会社のインフラストラクチャを保護し、サービスの中断を防ぐためには、既存のセキュリティ対策を強化することが不可欠です。同社は、このようなネットワークベースの攻撃のリスクを管理および軽減するソリューションを導入する必要があります。同様のリスクを軽減するために導入すべきセキュリティ製品はどれでしょうか？
A. シスコウェブセキュリティアプライアンス
B. シスコ傘
C. Cisco Secure Endpoint
D. シスコセキュアファイアウォール
正解: **(**正解を表示します**)**
SYNフラッド攻撃は、TCPの3ウェイハンドシェイクを悪用する古典的なサービス拒否（DoS）攻撃手法です。攻撃者は、ハンドシェイクを完了せずに大量のSYNパケットを送信することで、ターゲットサーバーの接続テーブルを枯渇させます。Cisco Secure Firewall（旧Firepower）は、このようなネットワーク層の脅威を軽減するために設計されたアーキテクチャコンポーネントです。
Cisco Secure Firewallは、TCPインターセプトやSYN Cookieなどの機能を利用して、これらの攻撃から防御します。SYNフラッドが検出されると、ファイアウォールはハンドシェイクのプロキシとして機能し、3ウェイハンドシェイクが検証された後にのみ、完了した接続をバックエンドサーバーに渡します。これにより、サーバーのリソースが「半開」接続によって過負荷になるのを防ぎます。
一方、Cisco Web Security Appliance（オプションA）は、Webベース（HTTP/HTTPS）の脅威とプロキシ処理に重点を置いており、低レベルのTCPフラッド攻撃の緩和には対応していません。Cisco Umbrella（オプションB）は主にDNSレイヤーのセキュリティとSecure Internet Gateway（SIG）サービスを提供しますが、オンプレミスまたはクラウドホスト型のゲームサーバーを標的とした直接的なSYNフラッド攻撃には効果がありません。Cisco Secure Endpoint（オプションC）は個々のホストをマルウェアから保護しますが、ネットワークインフラストラクチャやサーバーのTCPスタックが大量のフラッドトラフィックによって飽和状態になるのを防ぐことはできません。したがって、Cisco Secure Firewallは、これらのインフラストラクチャレベルのネットワーク攻撃を管理および緩和するための必須製品です。

質問: **18**
企業内のネットワーク機器、エンドポイント、その他のソースからログを収集、分析、視覚化するために使用されるツールはどれですか？
A. Cisco Email Security Appliance
B. クラウドの可観測性
C. Cisco Web Security Appliance
D. Splunk
正解: **D (**コメントを発表する**)**

最新のセキュリティオペレーションセンター（SOC）のアーキテクチャ設計において、可視性は最重要事項です。Splunkは、企業全体のさまざまなソースからデータを集約するために使用される、主要なセキュリティ情報およびイベント管理（SIEM）およびログ管理プラットフォームです。Cisco SDSI v1.0の目標、特に「リスク、イベント、要件」の領域では、インシデント対応と脅威ハンティングのために、テレメトリの中央リポジトリが不可欠です。
Splunkは、ネットワーク機器（ファイアウォール、スイッチ、ルーター）、エンドポイント（ノートパソコン、サーバー）、クラウドアプリケーションからログ、メトリクス、その他のデータを収集します。そして、これらのデータをインデックス化することで、セキュリティアナリストが複雑な検索を実行したり、視覚化を作成したり、組織のセキュリティ状況をリアルタイムで把握できるダッシュボードを構築したりできるようにします。
Ciscoは、特定のクラウドおよびアプリケーションのパフォーマンス監視のためにCisco Secure Cloud AnalyticsやCloud Observability（オプションB）などのネイティブツールを提供していますが、Splunkはインフラストラクチャ全体を包括的に把握できる「シングルペインオブグラス」として機能します。Cisco Email Security Appliance（オプションA）とCisco Web Security Appliance（オプションC）は、ログを生成する専用のセキュリティエンジンですが、企業全体の包括的な収集および分析プラットフォームとしては機能しません。Ciscoのセキュリティ製品をSplunkと統合することで、組織はWSAからのWebリクエストのブロックやセキュアエンドポイントからのマルウェアアラートなどのイベントを関連付けて、連携攻撃を特定し、Cisco SAFEの要件である包括的な可視性を満たすことができます。

質問: **19**
セキュリティインシデント発生後に根本原因分析を実施する主なメリットは何ですか？
A. OSIモデルへの準拠を検証する
B. NTP規格への準拠を有効にする
C. 再発防止のため設計改善を推進する
D. FTPスループットの向上
正解: **(**正解を表示します**)**
根本原因分析は、セキュリティインシデントの根本原因を特定することに重点を置いています。これにより、組織は症状を一時的に修正するだけでなく、システム設計、制御、またはプロセスを改善して、同様のインシデントが再発しないようにすることができます。

質問: **20**
あるソフトウェア開発会社は、複数のクラウドプロバイダーを利用してアプリケーションをホストしています。同社は、以下の要件を満たす拡張性の高いファイアウォールソリューションを設計しています。
複数のクラウド環境にわたる一貫したセキュリティポリシー。
* 一元化された可視性と管理。
* さまざまなクラウドプラットフォームに対応できる拡張性。
どのタイプのファイアウォールが要件を満たしますか？
A. 従来のファイアウォール
B. ゾーンベースファイアウォール
C. 分散ファイアウォール
D. ホストベースファイアウォール
正解: **(**正解を表示します**)**

マルチクラウドアーキテクチャでは、従来の境界型ファイアウォールはしばしば 「ボトルネック」となり、異なるプロバイダ間のマイクロサービス間の東西トラフィックに必要なきめ細かな制御を提供できません。分散型ファイアウォールは、こうした最新の要件を満たすように設計されたアーキテクチャソリューションです。集中型アプライアンスとは異なり、分散型ファイアウォールはソフトウェア定義レイヤーとして実装され、ワークロードの近く（多くの場合、ハイパーバイザ内、またはサービスメッシュの一部として）に配置されます。
Cisco Security Infrastructure の目標によれば、分散ファイアウォールは、ワークロードが AWS、Azure、オンプレミスのデータセンターのいずれにあるかに関わらず、すべての適用ポイントに展開される統一ポリシーの一元管理を可能にします。これにより、フットプリント全体で一貫したセキュリティ ポリシーが保証されます。適用が分散化されているため、新しいクラウド プラットフォームやワークロードが追加されると、ソリューションは自動的に拡張されます。従来のファイアウォール (オプション A) はマルチ クラウドの俊敏性に欠け、ゾーン ベースのファイアウォール (オプション B) は通常、ルータ上の特定の物理インターフェイスまたは論理インターフェイスに結び付けられ、ホスト ベースのファイアウォール (オプション D) は個々の OS レベルで管理されるため、大規模になると一元的に調整することが困難になります。分散ファイアウォール モデルは、高度に動的で異種混在のクラウド 環境における遍在的なセキュリティと簡素化された運用という Cisco SAFE アーキテクチャの目標に合致しています。

質問: **21**
あるIT企業は、ユーザー端末間で悪意のあるコンテンツが拡散し、業務上重要なリソースに影響が出たという事態に直面しました。同社は、ネットワーク上の個々の端末間の通信を制御するソリューションを導入したいと考えています。どの方法が目的を達成できるでしょうか？
A. 半径
B. TrustSec
C. 姿勢
D. プロファイリング
正解: **(**正解を表示します**)**
Cisco TrustSecは、エンドポイントにセキュリティグループタグ（SGT）を割り当て、通信ポリシーを適用することで、ソフトウェア定義のセグメンテーションを実現します。これにより、個々のエンドポイント間のトラフィックをきめ細かく制御し、ネットワーク全体への悪意のあるコンテンツの拡散を防ぐことができます。

質問: **22**
製薬会社がハブアンドスポーク型のVPNトポロジーを必要としています。設計では、部分メッシュまたはフルメッシュのオーバーレイネットワークを構築できる必要があります。この環境にはどのVPNソリューションを実装すべきでしょうか？
A. DMVPN
B. L2TP
C. 暗号マップ
D. SSL VPN
正解: **A (**コメントを発表する**)**
Cisco Security Infrastructureの設計（300-745 SDSI）ブループリントにおいて、ダイナミックマルチポイントVPN（DMVPN）は、部分的なメッシュオーバーレイまたは完全なメッシュオーバーレイへと柔軟に進化できる、拡張性の高いハブアンドスポークトポロジー向けに設計された特殊なアーキテクチャソリューションです。DMVPNは、マル

チポイントGRE（mGRE）トンネル、ネクストホップ解決プロトコル（NHRP）、およびIPsec暗号化を組み合わせて、動的な環境を構築します。
DMVPNの主な利点は、スポークサイト間でオンデマンドのトンネルを確立できることです。従来のハブアンドスポークモデルでは、2つのスポーク間のトラフィックはハブを経由する必要があり、遅延が発生し、ハブのリソース消費が増加します。DMVPNでは、スポークはNHRPを使用して他のスポークのパブリックIPアドレスを検出し、それらの間に直接トンネルを自動的に構築できます。これにより、製薬会社はシンプルなハブアンドスポーク管理モデルを維持しながら、トラフィックパターンに応じてフルメッシュのパフォーマンスを活用できます。
SSL VPN（オプションD）とL2TP（オプションB）は個々のリモートアクセスには最適ですが、サイト間メッシュのスケーラビリティには対応していません。クリプトマップ（オプションC）はIPsecトンネルを構築する従来の方法であり、ピア間の関係を静的かつ手動で設定する必要があるため、フルメッシュを大規模に管理することは事実上不可能です。DMVPNは、大規模なトンネル管理の複雑さを自動化することで、高可用性と柔軟性を備えたセキュアなインフラストラクチャを設計するというCisco SDSIの目標を実現します。

質問: **23**
SOCアナリストがエンドポイントを隔離するために使用するツールはどれですか？
A. フローコレクター
B. syslog
C. ロードバランサー
D. Cisco XDR
正解: **D (**コメントを発表する**)**
侵害が確認された場合、SOCアナリストは迅速に対応して横方向への拡散を防ぐ必要があります。Cisco XDR（Extended Detection and Response）は、ネットワーク、エンドポイント、クラウド全体にわたるクロスレイヤーの検出と自動応答アクションを提供するように設計された統合セキュリティプラットフォームです。XDRにおける最も重要な応答アクションの1つは、エンドポイントを隔離または隔離する機能です。
Cisco XDR は、エンドポイント セキュリティ エージェント (Cisco Secure Client など) およびネットワーク インフラストラクチャ (Cisco ISE など) と統合されます。アナリストは、単一のインターフェイスから「ホスト分離」コマンドをトリガーできます。このコマンドは、エンドポイント エージェントにセキュリティ コンソールとの通信以外のすべてのネットワーク トラフィックをブロックするように指示し、デバイスをデジタル隔離状態にします。これは、デバイスを手動で追跡するよりもはるかに高速で効果的です。フロー コレクタ (オプション A) と syslog (オプション B) は、可視性とログ記録に使用される診断ツールであり、アクティブな強制措置を実行することはできません。ロード バランサー (オプション C) は、アプリケーションのトラフィック分散を管理し、エンドポイントの封じ込めとは無関係です。Cisco XDR は、SDSI の目標である「自動化によるインフラストラクチャの保護」を実現し、SOC チームが連携した対応ワークフローを通じて大規模な脅威を軽減できるようにします。

質問: **24**
ある金融会社は、すべてのトラフィックをセキュアなトンネル経由でルーティングするリモートアクセスソリューションを使用しています。同社は最近、本社から高額なインターネットサービスプロバイダ（ISP）の請求書を受け取りました。調査中のトラフィック分析によると、ネットワークトラフィックの大部分は、従業員がSaaSコラボレーション企業

が提供するビデオ会議に多くの時間を費やしたことが原因でした。セキュリティや従業員エクスペリエンスに悪影響を与えることなくコストを削減するために、同社はどのような変更を行うべきでしょうか？
A. SaaSアプリケーション内で許可されているビデオ解像度サイズを小さくします。
B. 動画SaaSアプリケーションをVPNから分割除外します。
C. VPN接続時にビデオ会議アプリをブロックします。
D. ビデオ通話中はVPNから切断することをユーザーに推奨します。
正解: (正解を表示します)
フルトンネルVPN構成では、リモートクライアントからのすべてのトラフィックは、最終宛先にルーティングされる前にVPNヘッドエンドに送信されます。このため、ビデオ会議などの高帯域幅で遅延に敏感なトラフィックが、企業のデータセンターを経由してインターネットに送り返されるという「ヘアピン現象」が発生し、本社ISP回線の帯域幅消費量が倍増することがよくあります。
この問題を解決するには、企業はスプリットエクスクルードトンネルを導入する必要があります。この構成により、VPN管理者は、セキュアトンネルをバイパスしてユーザーのローカルISP経由で直接インターネットに接続する特定のアプリケーションまたはIPアドレス範囲（この場合はSaaSビデオプラットフォーム）を定義できます。これにより、本社インターネット接続の負荷が大幅に軽減され、ビデオストリームの遅延が短縮されることで「従業員エクスペリエンス」が向上することがよくあります。品質が低下するオプションAや、ワークフローとセキュリティ体制を阻害するオプションC/Dとは異なり、信頼できるSaaSトラフィックをスプリットエクスクルードすることで、インフラストラクチャコストを最適化しながら、社内リソースの高いセキュリティ基準を維持できます。これは、Cisco Secure Client（AnyConnect）およびFirepower Threat Defense（FTD）ポリシーを使用して、拡張性とコスト効率に優れたリモートアクセスソリューションを設計するというCisco SDSIの目標と一致しています。

質問: **25**
ある製造会社は、スマートファクトリー全体にIoTデバイスを導入しており、以下の要件を満たすセキュリティソリューションを必要としています。
- IoTデバイスをネットワークベースの攻撃から保護します。
コミュニケーションパターンの可視化。
- IoTトラフィックの異常検知。
どのファイアウォール技術または機能を推奨すべきでしょうか？
A. ゾーンベースファイアウォール
B. 透過型ファイアウォール
C. 従来のファイアウォール
D. IPS/IDS
正解: (正解を表示します)
侵入防止・検知システム（IPS/IDS）は、IoT通信パターンを可視化し、ネットワークベースの攻撃から保護するとともに、異常検知機能を用いて異常なIoTトラフィック動作を特定します。そのため、スマートファクトリーにおけるIoTデバイスのセキュリティ確保に最も効果的なソリューションと言えます。

質問: **26**

ある製造会社は、スマートファクトリー全体にIoTデバイスを導入しており、以下の要件を満たすセキュリティソリューションを必要としています。
* IoTデバイスをネットワークベースの攻撃から保護します。
* コミュニケーションパターンの可視化。
* IoTトラフィックの異常検知。
どのファイアウォール技術または機能を推奨すべきでしょうか？
A. ゾーンベースファイアウォール
B. 透過型ファイアウォール
C. 従来のファイアウォール
D. IPS/IDS
正解: **D** (コメントを発表する)
スマートファクトリー環境では、IoTデバイスは多くの場合、Modbus、PROFINET、EtherNet/IPなどの特殊な産業用プロトコルを使用し、セキュリティ機能が限定されています。これらのデバイスをネットワークベースの攻撃から保護しつつ、通信パターンを可視化し、異常を検出するという要件を満たすには、IPS/IDS（侵入防止検知システム）が最も効果的なソリューションです。
最新のCisco Secure Firewall（NGFW）システムは、単純なポートベースのフィルタリングを超えた高度なIPS/IDS機能を統合しています。これらのシステムは、ディープパケットインスペクション（DPI）によって特定のIoTプロトコルとベースラインとなる「正常な」動作を識別します。IoTデバイスが突然未知の外部IPアドレスとの通信を開始したり、これまで使用したことのないコマンドを使用しようとしたりすると、IPS/IDSはアラートを発したり、トラフィックを異常としてブロックしたりできます。
ゾーンベースファイアウォール（オプションA）や従来型ファイアウォール（オプションC）はトラフィックをセグメント化し、ゾーン間のアクセスを制御できますが、一般的にIoTセキュリティに必要なきめ細かな可視性と行動ベースの異常検知機能が不足しています。透過型ファイアウォール（オプションB）は、ファイアウォールを透過的にする展開モードです。
レイヤ2では「目に見えない」ため、既存のネットワークへの組み込みには便利ですが、必要な異常検知機能は本来備えていません。そのため、IPS/IDSは、特殊なIoTトラフィックに対するシグネチャベースの保護と挙動の可視化を組み合わせたニーズに対応する、Ciscoセキュリティインフラストラクチャの中核となるテクノロジーです。

質問: **27**
あるIT企業は、ユーザー端末間で悪意のあるコンテンツが拡散し、業務上重要なリソースに影響が出たという事態に直面しました。同社は、ネットワーク上の個々の端末間の通信を制御するソリューションを導入したいと考えています。
どの方法が目的を達成できるでしょうか？
A. 半径
B. TrustSec
C. 姿勢
D. プロファイリング
正解: (正解を表示します)
エンドポイント間での悪意のあるコンテンツの拡散は、典型的な横方向移動の事例です。エンドポイントの物理的な場所やIPアドレスに関係なく、個々のエンドポイント間の通信を制御および制限するには、Cisco TrustSecが推奨される

アーキテクチャアプローチです。TrustSecは、管理や拡張が難しい従来のIPベースのアクセス制御リスト（ACL）から脱却し、代わりにスケーラブルグループタグ（SGT）を使用します。
TrustSec では、すべてのエンドポイントに、その役割またはセキュリティ コンテキスト (例: 「従業員」、「契約業者」または「人事部」)。セキュリティ ポリシーは、どの SGT が相互に通信できるかを規定する中央集中型マトリックス (送信ポリシー マトリックス) で定義されます。たとえば、ポリシーは、エンドポイントが「開発者」グループは「営業」グループのエンドポイントと直接通信できないため、マルウェアがマシン間を移動するのを効果的に防ぐことができます。RADIUS（オプションA）は認証に使用されるプロトコルですが、セグメンテーション自体は実行しません。ポスチャ（オプションC）はデバイスの状態をチェックし、プロファイリング（オプションD）はデバイスの種類を識別しますが、どちらもTrustSecのようなポリシーベースのトラフィック制御は提供しません。TrustSecを導入することで、同社はマイクロセグメンテーションを実現し、内部攻撃対象領域を大幅に縮小し、潜在的な侵害を単一グループ内に封じ込めることができます。これは、現代のセキュアなインフラストラクチャ設計における重要な目標です。

質問: **28**
人間参加型設計ポリシーは、生成型AIのどの影響に対処するものか？
A. フィッシング
B. スケールの変化
C. AIの幻覚
D. ディープフェイク
正解: **(**正解を表示します**)**

質問: **29**
ある小売企業が、ウェブサーバーを標的とした一連のサイバー攻撃に直面しており、その結果、オンラインサービスに支障が生じています。調査の結果、セキュリティチームは、これらの攻撃が不正なHTTPリクエストヘッダーを用いてウェブアプリケーションの脆弱性を悪用したものであることを突き止めました。今後同様の脅威から同社のウェブサイトを保護するため、セキュリティチームは、このような悪意のあるウェブトラフィックを検知・ブロックするように特別に設計されたセキュリティソリューションを導入する必要があります。同様の攻撃からウェブサイトを保護するために使用すべきセキュリティ製品はどれでしょうか？
A. ウイルス対策ソフト
B. 従来型のファイアウォール
C. Webアプリケーションファイアウォール
D. ホストベースファイアウォール
正解: **(**正解を表示します**)**
ここで説明するサイバー攻撃は、アプリケーション層（レイヤー7）を標的とし、特に不正なHTTPヘッダーを介した脆弱性を悪用します。これらの脅威を軽減するために必要なセキュリティソリューションは、Webアプリケーションファイアウォール（WAF）です。ネットワーク層とトランスポート層（IPアドレスとポート）のトラフィックを検査する標準的なファイアウォールとは異なり、WAFはHTTP/HTTPSトラフィックを詳細に検査します。
Cisco Secure Firewall に統合されている WAF やクラウドネイティブ WAF サービスなどは、Web リクエストの構造を理解します。SQL インジェクション、クロスサイトスクリプティング (XSS)、シナリオで言及されている特定の「無効な

HTTP リクエスト ヘッダー」などの高度な攻撃を識別してブロックできます。WAF は、一連のルール (多くの場合 OWASP Top 10 に基づく) を適用することで、悪意のあるリクエストが Web サーバーに到達する前にフィルタリングします。アンチウイルス ソフトウェア (オプション A) とホスト ベースのファイアウォール (オプション D) は、サーバーのオペレーティングシステムをマルウェアや不正な接続から保護しますが、Web リクエストのロジックを検査することはできません。従来のファイアウォール (オプション B) は、ポート 443 のトラフィックを単に「許可」として認識し、通過させます。
WAFの実装は、Cisco SDSIの「アプリケーション」ドメインにおいて、顧客向けWebサービスを悪用から保護するための重要なアーキテクチャ要件です。

質問: **30**
ある企業は最近、競合他社に転職した元従業員が、退職後数週間にわたり機密データにアクセスし、持ち出しを続けていたことを発見しました。この情報漏洩は、組織のデータセキュリティおよびアクセス管理における脆弱性を浮き彫りにしました。今後このような事態を防ぐため、組織は不正なデータアクセスと転送を検知・制限する対策を講じる必要があります。この問題に対処するために、どのような緩和策を実施すべきでしょうか？
A. Webアプリケーションファイアウォールを実装する。
B. ネットワークポリシーのアクセス権限をアップグレードします。
C. データ損失防止戦略を実施する。
D. 監査ログ記録および監視ソリューションを導入する。
正解: **(**正解を表示します**)**
このシナリオは、データ漏洩を伴う典型的な「内部脅威」を描写しています。最初の失敗はおそらく退職手続き（ID管理）にあったと考えられますが、特に「不正なデータアクセスと転送を検知・制限する」ために必要な技術的制御は、データ損失防止（DLP）戦略です。DLPソリューションは、機密データが組織の管理下から流出するのを監視、検知、阻止するように設計されています。
CiscoのEmail Security（ESA）、Web Security（WSA）、Cisco Umbrellaなどのプラットフォーム全体に統合された堅牢なDLP戦略は、フィンガープリンティングやキーワードマッチングなどの技術を使用して、顧客リスト、独自のコード、財務データなどの機密コンテンツを識別することで機能します。このデータを個人のクラウドドライブにアップロードしたり、電子メールで送信したりする不正な試みがあった場合、DLPエンジンが転送を傍受してブロックします。監査ログ（オプションD）は事後的なフォレンジック調査に不可欠ですが、
リアルタイムで転送を「制限」します。WAF（オプションA）はWebサーバーへの外部攻撃から保護し、ネットワークポリシー（オプションB）はトラフィックフローを制御しますが、一般的に機密性の高いビジネスデータを識別するために必要なコンテンツ認識機能が不足しています。DLPを実装することで、アカウントがアクティブな状態であったり、ユーザーが正当なネットワークアクセス権を持っていたりしても、組織の知的財産が保護され続けます。

質問: **31**
ある金融会社は、デバイスに保存されている機密データを積極的に保護することに注力している。
同社は、紛失または盗難されたデバイスに関連する潜在的なリスクを認識しており、不正ユーザーがデバイスにアクセスした場合でも、デバイス内のデータにアクセスしたり悪用したりできないようにするソリューションを求めている。
このソリューションには、ユーザー認証なしではデータを読み取れないようにする戦略の実装が含まれる。どのソリューションがこの要件を満たすか？

A. ケンジントンロックを取り付けます。
B. BIOSパスワードを使用します。
C. ディスク上のデータ暗号化を実装します。
D. GPS追跡を適用する。
正解: **(**正解を表示します**)**
ディスク暗号化は、適切な認証なしにはデバイスに保存されたデータを読み取れないことを保証します。
デバイスが紛失または盗難された場合でも、暗号化によってコンテンツが保護されているため、正規のユーザーが認証情報を提供するまで、不正なユーザーがデータにアクセスしたり悪用したりすることはできません。

有効的な**300-745**問題集はJPNTest.com提供され、**300-745**試験に合格することに役に立ちます！JPNTest.comは今最新**300-745**試験問題集を提供します。JPNTest.com 300-745試験問題集はもう更新されました。ここで**300-745**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/300-745-mondaishu
73問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
ある家具会社は最近、エンドポイント検出 ･対応 (EDR)の設定により、社内管理のノートパソコン上に複数の悪意のあるファイルが存在することが判明した。同社は、既知の悪意のあるファイルがネットワークやエンドポイントに配信されるのを防ぐため、セキュリティを強化する必要がある。新たなソリューションは、受信トラフィックを効果的に検査・フィルタリングする同社の能力を向上させるものでなければならない。
この目標を達成するには、どのセキュリティ製品を使用する必要がありますか？
A. 次世代ファイアウォール
B. 従来型のファイアウォール
C. ホストベースファイアウォール
D. eBPF
正解: **A (**コメントを発表する**)**
次世代ファイアウォール (NGFW)は、ディープパケットインスペクション、侵入防御、高度なマルウェアフィルタリング機能により、受信トラフィックを検査・フィルタリングします。これにより、既知の悪意のあるファイルがネットワークやエンドポイントに到達するのを防ぎ、同社のEDRソリューションを補完します。

質問: **33**
世界的なホテルチェーンが、Cisco ISEとCiscoスイッチを使用してネットワークを管理しています。このホテル会社は、ユーザーとエンドポイントをセグメント化することでネットワークセキュリティを強化したいと考えています。同じVLAN内のデバイス同士が通信できないようにする必要があります。目標は、動的アクセス制御リストを使用せずに相互通信を防止することです。この要件を満たすために、Cisco ISEを使用してどのような対策を講じる必要がありますか？
A. デバイスの位置制御を実装します。
B. エンドポイントプロファイリングを設定します。

C. IDグループを有効にする。
D. TrustSecを設定します。
正解: (正解を表示します)
Cisco TrustSecは、セキュリティグループタグ（SGT）をユーザーとデバイスに割り当てることで、ソフトウェア定義のセグメンテーションを提供します。これにより、動的ACLを使用することなく、同じVLAN内のデバイス間の通信を防止するポリシーを適用できます。これは、このシナリオにおいて安全なセグメンテーションを実現するための適切なアプローチです。

質問: **34**
金属製造会社は、間近に迫ったセキュリティ監査に備え、Kubernetes環境で稼働するコンテナベースサービスのセキュリティ強化を決定しました。同社は、アプリケーションとサービス間のすべての通信が暗号化されることを保証したいと考えています。管理者は、データ交換を保護するために、アプリケーションとサービス間でmTLSサービスを実装する予定です。大規模な暗号化管理とクラスタ全体での効率的な通信維持という要件を考慮すると、どのネットワークトランスポート技術を採用すべきでしょうか？
A. イングレスコントローラー
B. 負荷分散
C. Kubernetesネットワークポリシー
D. サービスメッシュ
正解: (正解を表示します)
サービスメッシュは、マイクロサービス間の相互TLS（mTLS）を標準でサポートしており、Kubernetes環境における大規模な暗号化通信を保証します。また、証明書、鍵、セキュリティポリシーの管理を一元化するため、クラスタ全体でのデータ交換を保護するのに最適な選択肢となります。

質問: **35**
ある企業は、app01、app02などの命名規則を用いて、Kubernetes環境で複数のアプリケーションをホストしていました。セキュリティ対策が講じられていなかったため、app01のユーザーはapp02のデータにアクセスできてしまいました。そこで、管理者は各アプリケーションを個別の名前空間に配置し、名前空間が完全に分離され、相互に通信できないようにすることにしました。この目的を達成するには、どのソリューションを使用すべきでしょうか？
A. HTTPルート
B. ロールバインディング
C. ネットワークポリシー
D. ゲートウェイ
正解: (正解を表示します)
Kubernetesでは、NetworkPolicyによってPodと名前空間間の通信が制御されます。名前空間間のトラフィックを拒否するポリシーを適用することで、管理者は各アプリケーション（例app01、app02）が隔離され、他の名前空間のデータにアクセスできないようにすることができます。

質問: **36**
ネットワークインフラのセキュリティ確保において、AIはどのような用途に活用できるのでしょうか？
A. 既知のゼロ日目攻撃の検出

B. 負荷分散
C. 交通シェーピング
D. サービス品質
正解: **(**正解を表示します**)**
現代のセキュリティアーキテクチャでは、人工知能（AI）と機械学習（ML）を活用して、事後対応型のシグネチャベースの防御を超越しています。ネットワークインフラストラクチャのセキュリティ確保におけるAIの最も重要な用途の1つは、ゼロデイ攻撃（試験の文脈では「デイゼロ」攻撃と呼ばれることが多い）の検出です。ゼロデイ攻撃は、ソフトウェアベンダーや一般には知られていない脆弱性を悪用するため、従来のファイアウォールやウイルス対策ソフトウェアではブロックするためのシグネチャが存在しません。
AIは、行動分析と異常検知を通じてこれらの脅威を特定します。フローの方向、パケットサイズ、パケット間の到着時間、プロトコル動作など、「正常な」ネットワークトラフィックパターンの非常に詳細なベースラインを確立することで、AIモデルは悪意のある攻撃を示す微妙な逸脱を検出できます。
例えば、Cisco Secure Network Analytics（旧称Stealthwatch）と Encrypted Threat Analytics（ETA）は、機械学習を使用して、復号化を必要とせずに、暗号化されたトラフィック内であってもマルウェアの暗号化「フィンガープリント」を識別します。これにより、セキュリティインフラストラクチャは、ベンダーがシグネチャをリリースするのを待つことなく、脅威が発生した瞬間に脅威を特定して軽減できます。ロードバランシング（オプション B）、トラフィックシェーピング（オプション C）、およびサービス品質（オプション D）は、ネットワークのパフォーマンスと可用性にとって重要ですが、これらは従来のトラフィックエンジニアリング機能であり、AI 駆動型セキュリティモデルが提供する高度な脅威検出機能を本質的に提供するものではありません。Cisco SDSI の目標では、AI は、プロアクティブな可視性を実現し、これまで見つからなかった脆弱性の「検出までの平均時間」（MTTD）を短縮するための主要なテクノロジーとして位置付けられています。

質問: **37**
AIが生成したコンテンツに透かしを入れることで、何が防止できるのでしょうか？
A. 膨大な資源消費
B. ディープフェイク
C. 有害物質
D. スケールの変化
正解: **(**正解を表示します**)**
人工知能（AI）とDevSecOpsの分野において、ウォーターマーキングは合成メディアの出所を特定するために使用される重要なセキュリティ技術です。生成型AIモデルが高度化するにつれ、非常にリアルな画像、動画、音声クリップ（ディープフェイクと呼ばれることが多い）を作成できるようになりました。これらのディープフェイクは、ビジネスメール詐欺（BEC）シナリオで経営幹部になりすましたり、誤情報を拡散したりするなど、高度なソーシャルエンジニアリング攻撃に悪用される可能性があるため、組織のセキュリティと社会の信頼に重大なリスクをもたらします。
AI生成コンテンツに暗号化または可視透かしを埋め込むことで、セキュリティシステムとユーザーはメディアの真正性と出所を検証できます。この予防措置は、有効な「署名」のない合成コンテンツを自動セキュリティツールが容易に検出できるようにすることで、ディープフェイクの拡散を阻止するのに役立ちます。透かしは、有害なコンテンツの作成（オプションC）やリソース消費の削減（オプションA）を本質的に阻止するものではありませんが、説明責任と検証の層を提供します。同様に、スケール変更（オプションD）は、透かしでは防止できない技術的な画像操作です。Cisco SDSIフレー

ムワークでは、透かしはAIセキュリティライフサイクルの不可欠な要素とみなされており、生成技術が責任を持って使用され、合成コンテンツが本物のデータと区別できることを保証します。

質問: **38**
あるソフトウェア開発会社は、複数のクラウドプロバイダーを利用してアプリケーションをホストしています。同社は、以下の要件を満たす拡張性の高いファイアウォールソリューションを設計しています。
複数のクラウド環境にわたる一貫したセキュリティポリシー。
- 一元化された可視性と管理。
- 様々なクラウドプラットフォームに対応できる拡張性。
どのタイプのファイアウォールが要件を満たしますか？
A. 従来のファイアウォール
B. ゾーンベースファイアウォール
C. 分散ファイアウォール
D. ホストベースファイアウォール
正解: **(**正解を表示します**)**
分散型ファイアウォールは、マルチクラウドおよびハイブリッド環境向けに設計されています。複数のプラットフォーム間で一貫したセキュリティポリシーを確保し、一元化された可視性と管理機能を提供するとともに、異なるクラウドプロバイダー間でワークロードに合わせてシームレスに拡張できます。これは、複数のクラウドにわたる一元的な拡張性を持たない従来型ソリューションやホスト型ソリューションとは異なり、シナリオの要件を直接満たします。

質問: **39**
ある企業がセキュリティ上の脆弱性を抱えたソフトウェアを公開し、攻撃者がその脆弱性を悪用して環境から重要な情報を盗み出した。この問題はセキュリティチームによって報告され、管理者はソフトウェア公開前にシフトレフトセキュリティテストを実行するよう指示された。ソフトウェア開発パイプラインのどのコンポーネントでテストを実行することを推奨すべきか？
A. 継続的展開
B. クラウドセキュリティ態勢管理
C. ソフトウェア部品表分析
D. ソースコード管理
正解: **D (**コメントを発表する**)**
Cisco SDSI v1.0ブループリントにおいて、「シフトレフト」とは、ソフトウェア開発ライフサイクル（SDLC）の可能な限り早い段階でセキュリティテストを統合する手法を指します。こうした早期テストを実行するためのパイプラインの中で最も効果的な要素は、ソースコード管理（SCM）です。セキュリティツールをSCMシステム（GitHub、GitLab、Bitbucketなど）に直接統合することで、開発者はコード作成中、あるいは最初のコミット段階で脆弱性を特定できます。
静的アプリケーションセキュリティテスト (SAST) やシークレットスキャンなどの手法は、通常、プルリクエストやコミットフックを介して SCM レベルで実行されます。これにより、セキュリティチームは、コードがコンパイルされる前、またはビルドステージに移動される前に、欠陥のあるロジックやハードコードされた認証情報を特定できます。継続的デプロイメント (オプション A) はソフトウェアの最終リリースを処理しますが、パイプラインのこの段階では「シフトレフト」アプローチが最も効果的になるには遅すぎます。ソフトウェア部品表 (SBOM) 分析 (オプション C) は依存

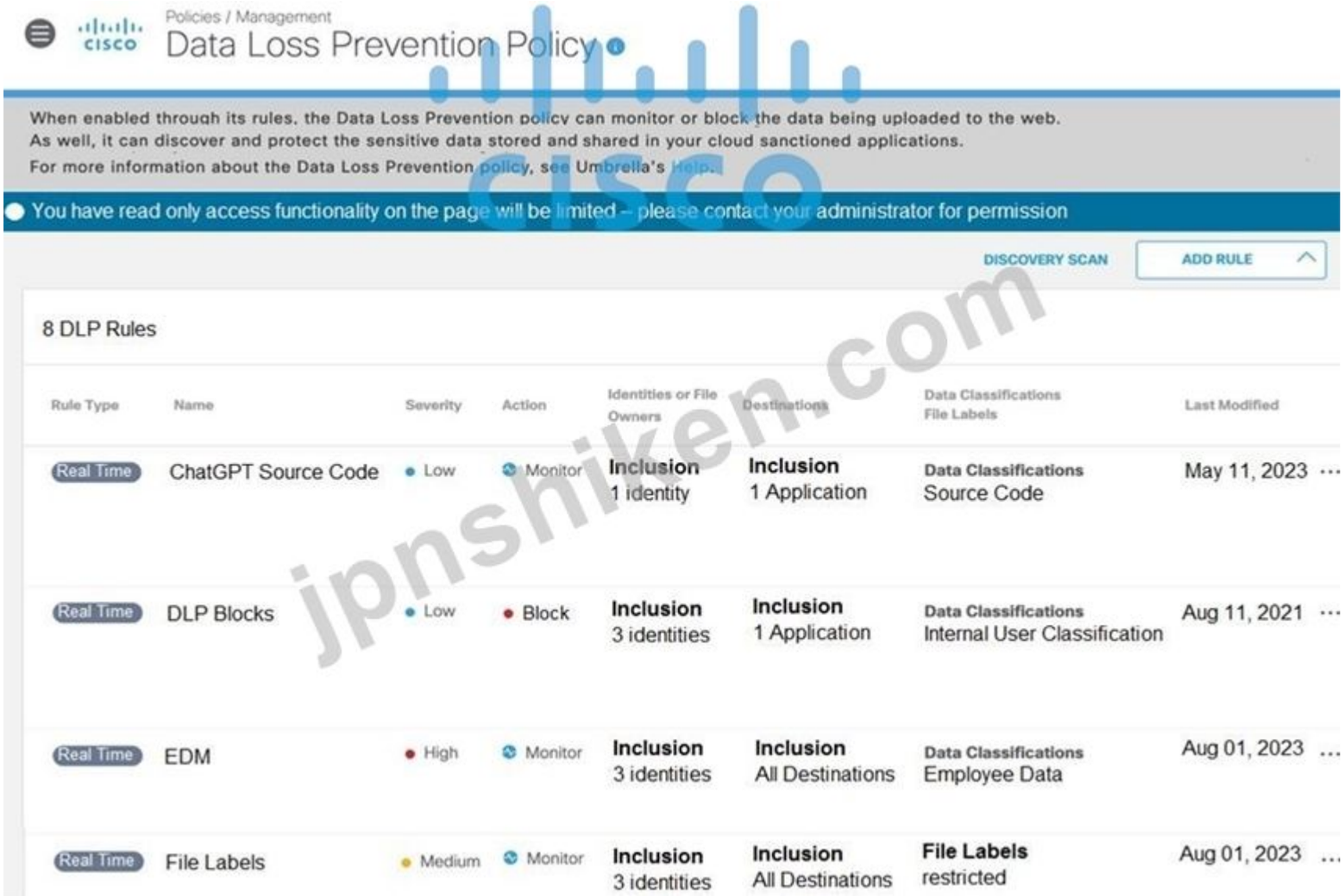
関係管理に焦点を当てた特定のタスクであり、クラウドセキュリティ態勢管理 (CSPM) (オプション B) はアプリケーションコード自体ではなくランタイム環境に焦点を当てています。SCM を主要なチェックポイントとして使用することで、セキュリティが開発プロセスの基盤となり、脆弱なソフトウェアが本番環境に到達するリスクが軽減されます。

質問: **40**
SOCがインシデントの優先順位付けを行うために使用すべきツールはどれですか？
A. SIEM
B. エンドポイント検出と応答
C. CloudWatch
D. エンドポイント保護プラットフォーム
正解: (正解を表示します)
セキュリティオペレーションセンター（SOC）は、さまざまなセキュリティツールからの何千ものアラートによって、しばしば処理能力を超えてしまう。
これらのインシデントを集約、関連付け、そして最も重要な優先順位付けを行うための主要ツールは、セキュリティ情報およびイベント管理（SIEM）システムです。シスコのSDSIドメイン「リスク、イベント、要件」によれば、SIEMはSOCの中枢として機能します。
SIEM（SplunkやCisco Secure Cloud Analyticsなど）は、ファイアウォール、エンドポイント、クラウドサービスからログを取り込み、相関ルールとリスクスコアリングアルゴリズムを使用して、優先度の低い「ノイズ」と重大なセキュリティインシデントを区別します。たとえば、1回のログイン失敗は無視される可能性がありますが、10回のログイン失敗の後に1回のログイン成功と大量のデータ転送が発生した場合は、優先度の高いインシデントとしてエスカレーションされます。エンドポイント検出および対応（EDR）（オプションB）とエンドポイント保護プラットフォーム（EPP）（オプションD）は、個々のホストに対して詳細な可視性と保護を提供しますが、組織のリスクを優先順位付けするために必要なクロスプラットフォーム相関がありません。CloudWatch（オプションC）はAWSリソースの監視サービスですが、マルチソースセキュリティ相関エンジンとしては機能しません。SIEMを使用することで、SOCアナリストは限られた時間を最も影響の大きい脅威に集中させることができ、より効率的で効果的なインシデント対応プロセスを確保できます。

質問: **41**
ある製造会社は最近、管理ネットワーク上でマルウェアが拡散したことが原因でネットワークダウンが発生しました。同社は、今後同様の脅威を検知・軽減し、ネットワーク全体を保護するためのソリューションを導入したいと考えています。どのソリューションが要件を満たしますか？
A. エンドポイント検出と応答
B. 半径
C. 暗号化された脅威分析
D. IPsec VPN
正解: (正解を表示します)
エンドポイント検出・対応（EDR）は、エンドポイントレベルでマルウェアの継続的な監視、検出、および自動的な軽減策を提供します。EDRは、脅威が管理ネットワーク全体に拡散する前に阻止することで、将来同様のネットワークダウンシナリオからインフラストラクチャ全体を保護します。

質問: **42**
あるIT企業は、SaaSモデルでアプリケーションを運用しています。顧客オンボーディングなどの管理タスクは、社内ネットワーク上のユーザーのみに制限する必要があり、管理者はWebブラウザまたはスマートフォンアプリ経由でこれらの機能にアクセスできます。機能に基づいたきめ細かな制御を実現するには、どのアプリケーション技術を使用すべきでしょうか？
A. VPC
B. RBAC
C. セキュリティグループ
D. サービスメッシュ
正解: **B** (コメントを発表する)
顧客オンボーディングなどの管理業務を、職務に基づいて特定のユーザーに限定する必要性は、ロールベースアクセス制御（RBAC）の典型的なユースケースです。アプリケーションセキュリティ設計の文脈において、RBACはユーザーのIDをアプリケーション内の特定の権限セットにマッピングするメカニズムです。
Cisco Security Infrastructure の原則によれば、RBAC は「Admin」ロールがオンボーディング機能にアクセスできる一方、「Support」ロールや「Standard User」ロールはアクセスできないようにすることで、最小権限の原則を保証します。この制御はネットワーク層とは独立しており、アプリケーションまたは ID プロバイダのレベルで適用されます。VPC (オプション A) やセキュリティ グループ (オプション C) はネットワーク層の分離を提供し、(IP 範囲をフィルタリングすることで) ユーザーが企業ネットワーク上にいることを保証できますが、接続が確立された後にアプリケーション内で実行されるさまざまな機能やアクションを区別することはできません。サービス メッシュ (オプション D) はマイクロ サービス間の通信に使用され、ある程度の認可を提供できますが、アプリケーション インターフェイス内で「誰が何を実行できるか」を定義する主要なアーキテクチャ アプローチは RBAC です。
RBACを導入することで、SaaSプロバイダーは機密性の高い管理ワークフローを保護し、承認された担当者のみが顧客データやシステム構成を変更できるようにすることができます。

質問: **43**
図を参照してください。あるソフトウェア開発者が、アプリケーションのソースコードがインターネット上で発見されたことに気づきました。このような事態の再発を防ぐため、開発者はChatGPTのような生成型AIツールへのソースコードのアップロードを防止するDLPポリシーを適用しました。しかし、ポリシーをテストしたところ、ソースコードのアップロードが依然として可能であることが判明しました。
この問題を回避するために、開発者はどのような対策を講じるべきでしょうか？



A. ルールを有効にします。
B. ChatGPTソースコードルールを一番下に移動します。
C. データ分類を変更します。
D. DLPアクションをモニターからブロックに変更します。
正解: **(**正解を表示します**)**
展示されているChatGPTソースコードルールは、アクションが 監視」に設定されています。これはアクティビティをログに記録するだけで、停止させるものではありません。ソースコードのアップロードを防止するには、アクションを ブロック」に変更する必要があります。これによりポリシーが適用され、生成型AIツールへのデータ漏洩が確実に阻止されます。

質問: **44**
生成型AIはネットワークのセキュリティ確保にどのように活用されているのか？
A. リアルタイムの負荷分散を提供する
B. 資源消費を改善する
C. 規制遵守を確保するためにリアルタイム監査を実施する
D. ネットワークトラフィックの異常なパターンを検出する

正解: **D** (コメントを発表する)
人工知能（AI）と生成型AI（GenAI）のネットワークセキュリティへの統合は、Cisco SDSI v1.0ブループリントの重要な要素です。従来のセキュリティメカニズムは決定論的なルールと静的なシグネチャに依存していますが、GenAIは大規模なテレメトリデータを活用して、特定のネットワーク環境のベースライン動作を理解します。AIモデルは、膨大な量のフローログ、パケットメタデータ、およびユーザーアクティビティを処理することで、ゼロデイ攻撃、横方向の移動、低速かつ低量のデータ漏洩といった高度な脅威を示す異常なパターン（しばしば異常と呼ばれる）を検出できます。
最新のセキュリティアーキテクチャにおいて、GenAIは人間のアナリストには見えない逸脱を特定することで、「可視性と監視」の領域を強化します。たとえば、アプリケーションが突然通信頻度を変更したり、これまで知られていなかった内部セグメントに接続したりした場合、AIはこれを潜在的な侵害としてフラグ付けできます。運用効率とパフォーマンスに焦点を当てたオプションAまたはB、あるいはレポート作成とコンプライアンス機能であるオプションCとは異なり、行動分析にAIを使用することで、脅威検出ライフサイクルが直接強化されます。Secure Network Analytics（Stealthwatch）やCognitive IntelligenceなどのCisco製品は、これらのAI機能を使用して、受動的な防御から能動的な姿勢へと移行し、攻撃者にとっての機会を減らし、継続的な監視と遍在的な可視性というCisco SAFE原則に合致させます。

質問: **45**
ある製造会社は最近、管理ネットワーク上でマルウェアが拡散したことが原因でネットワークダウンが発生しました。同社は、今後同様の脅威を検知・軽減し、ネットワーク全体を保護するためのソリューションを導入したいと考えています。どのソリューションが要件を満たしますか？
A. エンドポイント検出と応答
B. 半径
C. 暗号化された脅威分析
D. IPsec VPN
正解: (正解を表示します)
管理ネットワークのような機密性の高いセグメントにマルウェアが拡散することは、ホストレベルのセキュリティと内部可視性の欠如を浮き彫りにします。このような脅威の拡散を検知・軽減し、ネットワーク全体を保護するには、エンドポイント検出・対応（EDR）が最も効果的な選択肢です。シスコのセキュリティエコシステムにおいて、エンドポイントは多くの場合、最後の防衛線であり、マルウェアインシデントに関する最も重要なテレメトリ情報源となります。
Cisco Secure EndpointのようなEDRソリューションを導入することで、製造会社は感染の「最初の感染者」を特定できるようになります。EDRは、デバイストラバーサルやラテラルムーブメント検出などの高度な機能を使用して、マルウェアが管理ネットワークを介してあるマシンから別のマシンへとどのように移動するかを把握します。
セキュリティチームは、感染が検出されると、EDRプラットフォームを使用して「ホスト隔離」コマンドを開始し、物理的に電源を抜くことなく、感染したデバイスとネットワークの他の部分との通信を効果的に遮断することができます。暗号化脅威分析（ETA）（オプションC）は、暗号化されたトラフィック内のマルウェアを復号化せずに検出する強力なネットワークベースの機能ですが、EDRは、ホスト上に存在し、ホスト間で拡散するマルウェアに対して、最もきめ細かな制御と対応機能を提供します。RADIUS（オプションB）とIPsec VPN（オプションD）は、それぞれアクセス制御と転送中のデータの暗号化に重点を置いていますが、ネットワークへのアクセスが既に発生した後に、実行中のマルウェアの蔓延を阻止するために必要な行動分析は提供しません。

質問: **46**
ある農業企業は、多形性マルウェアの脅威から保護するために、多層防御戦略を導入することでサイバーセキュリティ体制を強化したいと考えている。現在、同社のセキュリティインフラは、マルウェアの亜種に対する十分な保護を提供しないステートフルな従来型エッジファイアウォールのみに依存している。この目標を達成するために、同社のセキュリティアーキテクチャにどのような技術を追加する必要があるだろうか？
A. Webアプリケーションファイアウォール
B. 物理的セキュリティ管理
C. ネットワークパフォーマンスモニター
D. ヒューリスティクスに基づくIPS
正解: **(**正解を表示します**)**
ヒューリスティックに基づく侵入防御システム（IPS）は、トラフィックの挙動とパターンを分析し、従来の防御策を回避するためにシグネチャを絶えず変化させるポリモーフィックマルウェアを検出してブロックします。この技術を追加することで、ステートフルファイアウォールの限界を超え、同社の多層防御戦略が強化されます。

有効的な**300-745**問題集はJPNTest.com提供され、**300-745**試験に合格することに役に立ちます！JPNTest.comは今最新**300-745**試験問題集を提供します。JPNTest.com 300-745試験問題集はもう更新されました。ここで**300-745**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/300-745-mondaishu
73問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
ある家具会社が最近、エンドポイント検出・対応（EDR）の設定により、社内管理のノートパソコンに複数の悪意のあるファイルが存在することが判明しました。同社は、既知の悪意のあるファイルがネットワークやエンドポイントに配信されるのを防ぐため、セキュリティを強化する必要があります。新たなソリューションは、受信トラフィックを効果的に検査・フィルタリングする同社の能力を向上させるものでなければなりません。この目標を達成するために、どのセキュリティ製品を使用すべきでしょうか？
A. 次世代ファイアウォール
B. 従来型のファイアウォール
C. ホストベースファイアウォール
D. eBPF
正解: **A (**コメントを発表する**)**
エンドポイント検出・対応（EDR）は、既にデバイスに到達した脅威を検出するのに非常に優れていますが、ここでの目的は、受信トラフィックの検査を強化することで、そもそもそのようなファイルが配信されるのを防ぐことです。次世代ファイアウォール（NGFW）は、ネットワーク境界（またはセグメント間）で動作し、従来のファイアウォールの機能をはるかに超えるディープパケットインスペクション（DPI）を提供するため、この要件を満たす適切なアーキテクチャです。
Cisco Secure Firewall（NGFW）は、侵入防御システム（IPS）、アプリケーション可視化および制御（AVC）、高度マルウェア対策（AMP）など、複数のセキュリティサービスを単一のプラットフォームに統合しています。悪意のあるファイルがネットワークに送信されると、NGFWはシグネチャや動作に基づいてファイルを識別し、内部インフラストラクチャや

エンドポイントに到達する前に転送をブロックします。これにより、トラフィックストリームを効果的に「ゲート」で「クリーンアップ」できます。
従来のファイアウォール（オプションB）は、主にIPアドレスとポートに基づいてフィルタリングするため、悪意のあるファイル コンテンツを識別するために必要なアプリケーション レイヤーの可視性がありません。ホスト ベースのファイアウォール（オプションC）は、個々のデバイス レベルでトラフィックをフィルタリングしますが、これはネットワーク配信防止ツールではなく、最終段階の防御です。eBPF（オプションD）は、可視性と分散フィルタリングに使用される高性能カーネル テクノロジーですが、このコンテキストでは境界トラフィック検査に使用されるスタンドアロンの「セキュリティ 製品」ではありません。NGFWを実装することは、脅威を重要な資産からできるだけ遠く離れた場所でブロックする階層型防御を提供するというCisco SAFEの原則に合致しています。

質問: **48**
金属製造会社は、間近に迫ったセキュリティ監査に備え、Kubernetes環境で稼働するコンテナベースサービスのセキュリティ強化を決定しました。同社は、アプリケーションとサービス間のすべての通信が暗号化されることを保証したいと考えています。管理者は、データ交換を保護するために、アプリケーションとサービス間でmTLSサービスを実装する予定です。大規模な暗号化管理とクラスタ全体での効率的な通信維持という要件を考慮すると、どのネットワークトランスポート技術を採用すべきでしょうか？
A. イングレスコントローラー
B. 負荷分散
C. Kubernetesネットワークポリシー
D. サービスメッシュ
正解: **D** (コメントを発表する)
最新のクラウドネイティブアーキテクチャでは、数百ものマイクロサービスのセキュリティを手動で管理することは現実的ではありません。Kubernetesクラスタ内で相互TLS（mTLS）を大規模に実装するには、サービスメッシュ（IstioやCisco Service Mesh Managerなど）が最適なアーキテクチャソリューションとなります。サービスメッシュは、アプリケーションコード自体を変更することなく、サービス間の通信を処理するための専用のインフラストラクチャレイヤーを提供します。
サービスメッシュは、各サービスインスタンスの横に「サイドカー」プロキシをデプロイすることで動作します。これらのプロキシは、ID検証、証明書のローテーション、暗号化トンネルの確立といった重い処理を担当します。これにより、すべてのデータ交換が暗号化され、サービスは認証されたピアとのみ通信することが保証されます。Ingress Controller（オプションA）はクラスタに入るトラフィックを管理し、Load Balancing（オプションB）はトラフィックを分散しますが、どちらもPod間mTLSに必要なきめ細かな内部暗号化フレームワークを提供しません。Kubernetes Network Policies（オプションC）は、IP/ポートに基づいてトラフィックを許可または拒否する分散ファイアウォールとして機能しますが、暗号化や暗号IDは処理しません。サービスメッシュを選択することで、同社はエンドツーエンド暗号化とアプリケーションの通信フローに対する包括的な可視性に関する監査要件を満たし、Ciscoの安全でスケーラブルなマイクロサービスの設計原則に合致しています。

有効的な**300-745**問題集はJPNTest.com提供され、**300-745**試験に合格することに役に立ちます！JPNTest.comは今最新**300-745**試験問題集を提供します。JPNTest.com 300-745試験問題集はもう更新されました。ここで**300-745**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/300-745-mondaishu
73問、３０%ディスカウント、特別な割引コード: **JPNshiken**」