サイバーセキュリティ シナリオのインタラクティブな EBOOK

現実的なシナリオ。よりスマートな意思決定。より強固な防御。

セキュリティに対する Dell の取り組みは、当社のあらゆる活動の中核をなすものです。この e-book では、インサイト、ベスト プラクティス、革新的なテクノロジーを共有することで、新たなサイバー リスクに先手を打つために必要なツールと知識をご紹介します。

攻撃シナリオの選択

サイバーセキュリティの脅威は常に進化しており、組織にはデータを保護するための効果的な対応が求められます。組織に最適な準備を整えるために、実際のシミュレーション演習に参加して、サイバー攻撃に対抗するためのサイバーセキュリティ戦略を確認していきましょう。

国や地方自治体、金融サービス、医療など、さまざまなセクターにおける攻撃タイプと業界固有の課題について説明します。その過程で、ノートパソコンやデスクトップからエンタープライズ システムまで、Dell の統合セキュリティ ソリューションが、これらの脅威からの保護のためにどのように構築されているかをご紹介します。

- バックアップへの侵入 →
- ランサムウェア →
- 分散型サービス拒否 (DDoS) →
- サプライ チェーン ハードウェア →
- 悪意のある内部関係者 →
- サプライ チェーン ソフトウェア →
- 中間者攻撃 (MITM) →
- ゼロデイ →
- プロンプト /SQL インジェクション →

攻撃タイプ：バックアップへの侵入

クラウド バックアップ サービス プロバイダーのマネージャーは、ある晩、失われたデータをリストアしようとしているクライアントから電話を受けました。

そのクライアントは、クラウドからのリカバリーを何度も試みましたが、リカバリーは常に失敗しています。

マネージャーがクライアントのオフィスに出向くと、すべてのコンピューター画面に全データは暗号化されており、データにアクセスするには身代金を支払う必要があると表示されています。

理解度テスト →

攻撃タイプ：バックアップへの侵入

1：攻撃対象領域を縮小　2　3　4

どのバックアップ システムまたは顧客が影響を受けたかは不明です。最初に何をすべきですか？

- [ ] 関係当局に通知する
- [ ] すべてのシステムをシャットダウンする
- [ ] 脅威を封じ込めて隔離する
- [ ] リストアできるクリーンなバックアップがあるかどうかを確認する

正解を見る →

攻撃タイプ：バックアップへの侵入

1：攻撃対象領域を縮小 — 2 — 3 — 4

どのバックアップ システムまたは顧客が影響を受けたかは不明です。最初に何をすべきですか？

- ✗ 関係当局に通知する
- ✗ すべてのシステムをシャットダウンする
- ✓ 脅威を封じ込めて隔離する
- ✗ リストアできるクリーンなバックアップがあるかどうかを確認する

脅威を直ちに封じ込めて隔離することで、さらなる拡散や被害を防ぎ、インシデントの範囲を評価する時間を確保できるため、AI を含むあらゆるタイプのサイバー攻撃による影響を最小限に抑えることができます。

次の質問 →

攻撃タイプ：バックアップへの侵入

1 — 2：サイバー脅威の検出と対処 — 3 — 4

顧客のデータを迅速に利用できるようにすることを優先します。どのような方法で対処しますか？

- [ ] 身代金を支払う
- [ ] ランサムウェアの種類を特定する
- [ ] 関係当局に通知する
- [ ] 侵害されたデータを特定する

正解を見る →

攻撃タイプ：バックアップへの侵入

1 — 2：サイバー脅威の検出と対処 — 3 — 4

顧客のデータを迅速に利用できるようにすることを優先します。どのような方法で対処しますか？

- ✗ 身代金を支払う
- ✗ ランサムウェアの種類を特定する
- ✗ 関係当局に通知する
- ✓ 侵害されたデータを特定する

侵害されたデータを特定することで、最も重要な顧客情報のリカバリーに集中し、データを迅速に利用できるようにして、影響を受けていないシステムでの不要な作業を回避できます。

次の質問 →

攻撃タイプ：バックアップへの侵入

1 — 2 — 3：サイバー攻撃からのリカバリー — 4

リカバリーできるバックアップを確認しました。プロセスの最初のステップは何ですか？

- [ ] まずは重要なシステムの復旧を優先する
- [ ] フォレンジック分析を使用して、攻撃が完全に封じ込められていることを確認する
- [ ] すべてのパスワードを変更し、侵害された認証情報を取り消す
- [ ] ゼロトラスト原則を実施する

正解を見る →

攻撃タイプ：バックアップへの侵入

1 — 2 — 3：サイバー攻撃からのリカバリー — 4

リカバリーできるバックアップを確認しました。プロセスの最初のステップは何ですか？

- ✗ まずは重要なシステムの復旧を優先する
- ✓ フォレンジック分析を使用して、攻撃が完全に封じ込められていることを確認する
- ✗ すべてのパスワードを変更し、侵害された認証情報を取り消す
- ✗ ゼロトラスト原則を実施する

システムを復元する前に、攻撃が完全に封じ込められていることを確認して、偶発的な再感染やさらなる被害を防ぎ、環境内での脅威の永続化や拡大を回避する必要があります。

次の質問 →

攻撃タイプ：バックアップへの侵入

1 2 3 4：全体的なベストプラクティス

今後発生するリスクを軽減するために、どのような方法が考えられますか？

- [ ] ゼロトラストの原則を利用する
- [ ] エンドポイントでの検出および対応 (EDR) 機能を活用する
- [ ] エアギャップの不変バックアップを実装する
- [ ] 上記すべて

正解を見る →

攻撃タイプ：バックアップへの侵入

1 2 3 4：全体的なベストプラクティス

今後発生するリスクを軽減するために、どのような方法が考えられますか？

- ゼロトラストの原則を利用する
- エンドポイントでの検出および対応 (EDR) 機能を活用する
- エアギャップの不変バックアップを実装する
- 上記すべて

多層防御戦略を使用することで、リスクを軽減し、被害を最小限に抑え、組織のレジリエンスを高めることができます。単一の対策だけでは不十分です。

ソリューションを見る →

攻撃タイプ：バックアップへの侵入

まとめ

バックアップ侵入とは、サイバー犯罪者がバックアップ システムの脆弱性を悪用して、重要なリカバリー データを侵害、破壊、暗号化することです。この高度な攻撃は、他のインシデント（ランサムウェアやマルウェアの導入など）と同時に行われるか、またはその後に行われる可能性があり、運用面と財務面での影響が深刻化します。

Dell は、進化するサイバー脅威に直面しても組織がレジリエンスを維持できるよう支援することが重要だと考えています。最先端のソリューション、エキスパート サービス、信頼できるパートナーシップを通じて、最も重要なものを守るお手伝いをいたします。

当社のソリューションと、今日の最も困難なサイバー課題への取り組み方について、詳細をご覧ください。

バックアップへの侵入の概要を見る →

⌂ シナリオに戻る

PowerProtect ポートフォリオ ›

AI 主導の CyberSense 分析を活用した、暗号化されエアギャップされた不変バックアップ ヴォールトで、迅速な検出とリカバリーが可能になり、レジリエンスを維持できます。

PowerEdge サーバー ›

Dell は、セキュア ブート、ハードウェア ルート オブ トラスト、システム ロックダウン機能でバックアップを保護する、信頼性の高いインフラストラクチャを用意しています。

信頼できるワークスペース ›

SafeBIOS や SafeData の保護機能は、リスクを軽減し、バックアップ システムが改ざんされることなく、必要なときに迅速に利用できるようにします。

セキュリティとレジリエンスに関するサービス ›

安全な導入からプロアクティブなインシデント対応まで、当社のエキスパートとパートナーがレジリエンスの構築と迅速なリカバリーを支援します。

ネットワーク ソリューション ›

Dell は、ネットワーク セグメンテーション、多要素認証 (MFA)、最小限の権限構成で、アクセスをロック ダウンし、重要なデータを保護できるよう支援します。

攻撃タイプ：分散型サービス拒否 (DDoS)

大雪が予想される火曜日の午後、ある州政府機関での出来事です。

運輸省の IT チームには、どのシステムにもアクセスできず、以下の処理ができないというエージェントからの問い合わせが殺到しています。

- 運転免許証の更新
- 道路使用許可の取得
- 税金の支払い
- 道路状況の確認
- 緊急対応システムを起動し、道路作業員による雪道や凍結路面の除雪作業を遅らせる

すべてシステムがタイムアウトしたことが原因です。

理解度テスト →

攻撃タイプ：分散型サービス拒否 (DDoS)

1：攻撃対象領域を縮小　2　3　4

発生状況を把握するために、まず何をしますか？

- [ ] インバウンド トラフィックに突然、原因不明の急増が発生していないかネットワーク デバイスで確認する
- [ ] 単一または限られた数の IP アドレスからの異常なトラフィックがないか、ネットワーク デバイスで確認する
- [ ] 過剰な接続失敗やトラフィックのブロック イベントがないか、ファイアウォールやネットワーク可視化ツールのログを確認する
- [ ] 上記すべて

正解を見る →

攻撃タイプ：分散型サービス拒否 (DDoS)

1：攻撃対象領域を縮小 2 3 4

発生状況を把握するために、まず何をしますか？

- [x] インバウンド トラフィックに突然、原因不明の急増が発生していないかネットワーク デバイスで確認する
- [x] 単一または限られた数の IP アドレスからの異常なトラフィックがないか、ネットワーク デバイスで確認する
- [x] 過剰な接続失敗やトラフィックのブロック イベントがないか、ファイアウォールやネットワーク可視化ツールのログを確認する
- [x] 上記すべて

広範囲にわたるシステム アウテージを適切に診断するには、ネットワーク デバイスのアクティビティとファイアウォールや可視化ツールのログを同時に確認して、異常なパターンやブロック イベントを迅速に検出する必要があります。そうすることで、サイバー インシデントとインフラストラクチャの問題を区別できるため、より迅速で正確なインシデント対応が可能になります。

次の質問 →

攻撃タイプ：分散型サービス拒否 (DDoS)

1 — 2：サイバー脅威の検出と対処 — 3 — 4

これは、DDoS 攻撃の可能性があると思われます。最初にするべきことは何ですか？

- [ ] すべてのネットワーク トラフィックを DDoS 緩和サービス経由でリダイレクトする
- [ ] Web アプリケーション ファイアウォール (WAF) ルールを有効にして、悪意のあるパターンを除去する
- [ ] トラフィックの急増が正当なソースによるものかどうかを確認する
- [ ] 発生状況を社内外に伝える

正解を見る →

攻撃タイプ：分散型サービス拒否 (DDoS)

1 — 2：サイバー脅威の検出と対処 — 3 — 4

これは、DDoS 攻撃の可能性があると思われます。最初にするべきことは何ですか？

- ✗ すべてのネットワーク トラフィックを DDoS 緩和サービス経由でリダイレクトする
- ✗ Web アプリケーション ファイアウォール (WAF) ルールを有効にして、悪意のあるパターンを除去する
- ✓ トラフィックの急増が正当なソースによるものかどうかを確認する
- ✗ 発生状況を社内外に伝える

DDoS 対策を有効にする前に、トラフィック急増の正当性を確認することが不可欠です。そうすることで、正規のユーザーを誤ってブロックすることを回避し、重要なステークホルダーの混乱を防ぎ、適切かつ正確にターゲットを絞った保護措置を講じることができるため、公共事業や全体的な事業継続性への悪影響を最小限に抑えることができます。

次の質問 →

攻撃タイプ：分散型サービス拒否 (DDoS)

1 2 3：サイバー攻撃からのリカバリー 4

今後、DDoS 攻撃を回避するために、どのような対策を講じることができますか？

- [ ] 問題のある IP アドレスをブロックする
- [ ] DDoS シミュレーションによる定期的な侵入テストを実施する
- [ ] クラウド プロバイダーは通常 DDoS 攻撃を受けないため、すべてのアプリケーションをクラウドに移行する
- [ ] ゼロトラスト原則を実施する

正解を見る →

攻撃タイプ：分散型サービス拒否 (DDoS)

1 2 3：サイバー攻撃からのリカバリー 4

今後、DDoS 攻撃を回避するために、どのような対策を講じることができますか？

- ✗ 問題のある IP アドレスをブロックする
- ✓ DDoS シミュレーションによる定期的な侵入テストを実施する
- ✗ クラウド プロバイダーは通常 DDoS 攻撃を受けないため、すべてのアプリケーションをクラウドに移行する
- ✓ ゼロトラスト原則を実施する

DDoS シミュレーションによるプロアクティブな侵入テストでは、防御のギャップを特定して強化します。一方、ゼロトラストの原則では、常に最小限のアクセス権限を適用することでリスクを最小限に抑えることに重点を置いています。そのため、緊急時の対応調整やリアルタイムのトラフィック信号制御など、攻撃中も機能を維持する必要がある重要なシステムが中断されるリスクを軽減できます。

次の質問 →

攻撃タイプ：分散型サービス拒否 (DDoS)

1 2 3 4：全体的なベストプラクティス

全体的なインシデント対応とリカバリー計画 (IRR) の一環として、誰に通知すべきですか？

- [ ] 法務チーム
- [ ] サイバー保険ベンダー
- [ ] CISA（サイバーセキュリティ・社会基盤安全保障庁）、FBI、MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [ ] 上記すべて

正解を見る →

攻撃タイプ：分散型サービス拒否 (DDoS)

1 2 3 4：全体的なベストプラクティス

全体的なインシデント対応とリカバリー計画 (IRR) の一環として、誰に通知すべきですか？

- [x] 法務チーム
- [x] サイバー保険ベンダー
- [x] CISA（サイバーセキュリティ・社会基盤安全保障庁）、FBI、MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [x] 上記すべて

大規模なサイバー インシデントが発生した場合は、コンプライアンス、請求、法執行に関して、法務、保険、政府機関との調整を検討します。すべての規制要件が満たされていることを確認した後、組織はインシデントを効果的に封じ込め、解決し、リカバリーできます。

ソリューションを見る →

攻撃タイプ：分散型サービス拒否 (DDOS)

まとめ

DDoS 攻撃は、ネットワーク、サービス、サーバーの通常の機能を停止させることを目的に、複数のソースから大量のトラフィックを送りつけるサイバー攻撃です。この攻撃はボットネットを悪用して実行されます。ボットネットとは、感染したデバイスで構成されるネットワークであり、攻撃者は感染デバイスを遠隔操作で制御します。

Dell では、高度な検出および軽減テクノロジーとエキスパート サービス、ゼロトラスト アプローチを組み合わせることで、組織が DDoS 攻撃に対するレジリエンスを維持できるよう支援しており、組織では迅速な対応、中断の最小化、防御の強化が可能になります。

高度なサイバー レジリエンス戦略の詳細をご覧になり、DDoS から組織を保護するために Dell がどのように支援できるかをご確認ください。

DDoS 攻撃の概要を見る →

シナリオに戻る

ネットワーク ソリューション ›

ネットワーク セグメンテーション、マイクロセグメンテーション、最小限の権限適用を行うことで、重要な資産を隔離し、攻撃の拡散を制限し、DDoS 攻撃を迅速に封じ込めます。

PowerEdge サーバー ›

Dell は、ハードウェア ルート オブ トラスト、セキュア ブート、システム ロックダウン、リアルタイムの改ざん防止機能により、レジリエンスに優れたハイパフォーマンスの DDoS 保護と迅速なリカバリーを可能にします。

信頼できるデバイス ›

SafeBIOS、SecureData、検出と対応の自動化を統合することで、エンドポイントの攻撃対象領域が最大 70% 縮小され、DDoS による妨害が侵害ベクトルとなるのを防止します。

PowerProtect ポートフォリオ ›

AI 主導の脅威分析を活用して暗号化された不変的なエアギャップ バックアップ環境では、DDoS 攻撃による中断時に迅速で検証済みのリストアを保証し、ビジネス継続性を維持します。

セキュリティとレジリエンスに関するサービス ›

Managed Detection and Response (MDR)、インシデント対応とリカバリー (IRR)、脅威ハンティング、レジリエンスに優れたアーキテクチャ ガイダンスを活用することで、DDoS への対応を高め、防御機能を強化できます。

攻撃タイプ：悪意のある内部関係者

火曜日の午前 8 時です。米国のヘルスケア企業の従業員にとって、1 日の業務は始まったばかりです。

機密性の高い患者データを扱うシニアレベルの従業員が、 夜遅くまでオフィスで仕事をした後にログインしました。

彼女は、 前の晩に作業していたフォルダーに変更があったことに気付きました。 チームに報告した後、 彼女は IT 部門に問い合わせました。

調査の結果、 犯罪組織とつながりのある IT 部門の若手社員が、 シニアレベルの従業員を騙して USB ラバー ダッキーをデバイスに挿入させ、 BIOS（基本入出力システム）を脆弱なバージョンにダウングレードさせてシステムを侵害したことが判明しました。

理解度テスト →

攻撃タイプ：悪意のある内部関係者

1：攻撃対象領域を縮小　2　3　4　5

悪意のある内部関係者は、MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) フレームワークによって追跡された 2 つの手法を使用して、この攻撃を開始しました。概要

- [ ] 信頼できる関係 + リムーバブル メディアを介したレプリケーション
- [ ] ソーシャル エンジニアリング + リムーバブル メディアによるレプリケーション
- [ ] ソーシャル エンジニアリング + 外部リモート サービス
- [ ] 信頼関係 + ハードウェアの追加

正解を見る →

攻撃タイプ：悪意のある内部関係者

1：攻撃対象領域を縮小 2 3 4 5

悪意のある内部関係者は、MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) フレームワークによって追跡された 2 つの手法を使用して、この攻撃を開始しました。概要

- ✗ 信頼できる関係 + リムーバブル メディアを介したレプリケーション
- ✓ ソーシャル エンジニアリング + リムーバブル メディアによるレプリケーション
- ✗ ソーシャル エンジニアリング + 外部リモート サービス
- ✗ 信頼関係 + ハードウェアの追加

攻撃者は、MITRE ATT&CK の人為的な操作とポータブル ストレージを介したレプリケーションという 2 つの手法を駆使し、ソーシャル エンジニアリングを活用してシニアレベルの従業員を騙し、USB ラバー ダッキーを接続させ、リムーバブル メディアを介して侵害されたデータを配信しました。

次の質問 →

攻撃タイプ：悪意のある内部関係者

1 — 2：サイバー脅威の検出と対処 — 3 — 4 — 5

攻撃者が 2 つの手法を使用する必要があったのはなぜですか？

- [ ] グローバル管理者としてネットワークにアクセスし、BIOS をダウングレードするため
- [ ] 管理者を装い、BIOS をダウングレードできるようにするため
- [ ] デバイスのドメイン ネーム システム (DNS) プロバイダーを変更して、1 回限りのネットワーク アクセスに必要な認証情報を取得するため
- [ ] デバイスにマルウェアをインストールして、継続的なネットワーク アクセスに必要な認証情報を取得するため

正解を見る →

攻撃タイプ：悪意のある内部関係者

1 — 2：サイバー脅威の検出と対処 — 3 — 4 — 5

攻撃者が 2 つの手法を使用する必要があったのはなぜですか？

- ✗ グローバル管理者としてネットワークにアクセスし、BIOS をダウングレードするため
- ✗ 管理者を装い、BIOS をダウングレードできるようにするため
- ✗ デバイスのドメイン ネーム システム (DNS) プロバイダーを変更して、1 回限りのネットワーク アクセスに必要な認証情報を取得するため
- ✓ デバイスにマルウェアをインストールして、継続的なネットワーク アクセスに必要な認証情報を取得するため

攻撃者は、USB ラバー ダッキーを介したマルウェアのインストールによるデバイスの侵害と、継続的なネットワーク アクセスを可能にする認証情報の取得という 2 つの方法を使用して、ターゲット環境に対する永続的で不正な制御を確立する必要がありました。

次の質問 →

攻撃タイプ：悪意のある内部関係者

1 2 3：サイバー脅威の検出と対処 4 5

不規則なネットワーク アクティビティを検出する方法の 1 つは何ですか？

- [ ] アプリケーション制御
- [ ] Extended Detection and Response (XDR)
- [ ] 次世代アンチウイルス (NGAV)
- [ ] エンドポイント ジオフェンシング

正解を見る →

攻撃タイプ：悪意のある内部関係者

1 2 3：サイバー脅威の検出と対処 4 5

不規則なネットワーク アクティビティを検出する方法の 1 つは何ですか？

- ✗ アプリケーション制御
- ✓ Extended Detection and Response (XDR)
- ✗ 次世代アンチウイルス (NGAV)
- ✗ エンドポイント ジオフェンシング

脅威を迅速に検出するための広範で相関性のある可視性という点で、XDR は疑わしいネットワーク アクティビティの検出に最適です。エンドポイント、ネットワーク、クラウド環境全体のアクティビティを継続的に監視して分析できることが、その理由です。

次の質問 →

攻撃タイプ：悪意のある内部関係者

1 2 3 4：サイバー攻撃からのリカバリー 5

キル チェーンの初期段階で不審なアクティビティを検出できる、パソコンに組み込みのセキュリティは何ですか？

- [ ] Security Information and Event Management (SIEM)
- [ ] Extended Detection and Response (XDR)
- [ ] Indicators of Attach (IOA)
- [ ] ロールベース アクセス制御 (RBAC)

正解を見る →

攻撃タイプ：悪意のある内部関係者

1 2 3 4：サイバー攻撃からのリカバリー 5

キル チェーンの初期段階で不審なアクティビティを検出できる、パソコンに組み込みのセキュリティは何ですか？

- ✗ Security Information and Event Management (SIEM)
- ✗ Extended Detection and Response (XDR)
- ✓ Indicators of Attach (IOA)
- ✗ ロールベース アクセス制御 (RBAC)

IOA は、攻撃者の行動や疑わしいアクティビティ パターンが発生したときに検出することに重点を置いています。そのため、セキュリティ チームは、シグネチャ ベースの方法より早期に脅威を特定し、重大な被害が発生する前に介入できます。

次の質問 →

攻撃タイプ：悪意のある内部関係者

1 2 3 4 5：全体的なベスト プラクティス

最初のアクセス方法を特定した後、今後同様の侵害からリカバリーし、阻止するために、どのような対策を講じることができますか？

- [ ] BIOS を最新バージョンにアップデートします
- [ ] BIOS のダウングレード オプションを無効化する
- [ ] USB ポートを無効にする
- [ ] USB デバイスの安全な使用とマルウェアの拡散を防止するためのきめ細かい制御を実装する
- [ ] 上記すべて

正解を見る →

攻撃タイプ：悪意のある内部関係者

1 2 3 4 5：全体的なベスト プラクティス

最初のアクセス方法を特定した後、今後同様の侵害からリカバリーし、阻止するために、どのような対策を講じることができますか？

- [x] BIOS を最新バージョンにアップデートします
- [x] BIOS のダウングレード オプションを無効化する
- [x] USB ポートを無効にする
- [x] USB デバイスの安全な使用とマルウェアの拡散を防止するためのきめ細かい制御を実装する
- [x] 上記すべて

ハードウェアの安全性を確保し、ダウングレードをブロックするための明確な攻撃ベクトルに対処することで、USB ベースの脅威を封じ込め、マルウェアの拡散を複数のポイントで阻止できます。これは、影響を受けたシステムをリカバリーし、将来の侵害から保護するための包括的で重層的な防御を構築するうえで役立ちます。

ソリューションを見る →

攻撃タイプ：悪意のある内部関係者

まとめ

悪意のある内部関係者による攻撃とは、組織内の個人が、個人的な目的、金銭的な目的、または競争上の目的のために、アクセス権を悪用してデータを侵害したり、業務を中断したり、機密情報を抽出したりする攻撃です。この個人は、従業員、請負業者、パートナー、または会社のシステムやネットワークへの正当なアクセス権を持つ人物である可能性があります。

Dell は、高度なテクノロジーと厳格なセキュリティ プロトコルを組み合わせて、悪意のある内部関係者によるサイバー攻撃を防御します。

高度なサイバー レジリエンス戦略の詳細をご覧になり、悪意のある内部関係者による攻撃から組織を保護するために Dell がどのように支援できるかをご確認ください。

悪意のある内部関係者の概要を見る →

⌂ シナリオに戻る

信頼できるデバイスとインフラストラクチャ ›

最小限の権限、多要素認証 (MFA)、ロールベースのアクセス制御 (RBAC)、二重認証、ゼロトラスト保護を組み込むことで、エンドポイントとインフラストラクチャを保護し、内部関係者による脅威のリスクを軽減できます。

PowerEdge サーバー ›

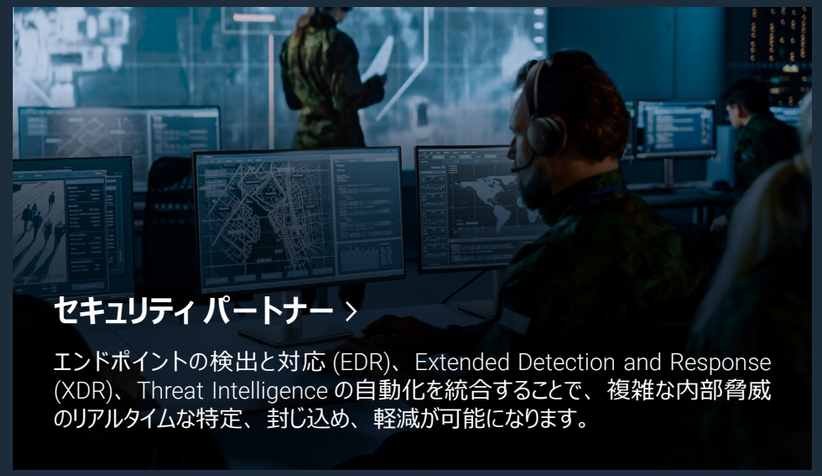
ハードウェア ルート オブ トラスト、セキュア ブート、動的 USB ポート管理、システム ロックダウンを活用して、物理的またはファームウェアベースの内部攻撃からの改ざんや停止を防止します。

PowerProtect ポートフォリオ ›

変更不可能な分離されたバックアップにより、データの整合性、迅速なリストア、データ操作の試行の早期検出が保証され、内部関係者によるインシデントからのリカバリーを可能にします。

セキュリティとレジリエンスに関するサービス ›

エキスパート主導のトレーニング、侵入テスト、脅威ハンティング、インシデント対応、侵害リカバリー サービスを通じて、内部関係者主導のイベントに対する準備とレジリエンスが強化されます。



セキュリティ パートナー ›

エンドポイントの検出と対応 (EDR)、Extended Detection and Response (XDR)、Threat Intelligence の自動化を統合することで、複雑な内部脅威のリアルタイムな特定、封じ込め、軽減が可能になります。

攻撃タイプ：中間者 (MITM)

あるカフェで、疑うことを知らない一人の客が、セキュリティ対策が施されていない無料の Wi-Fi に接続し、チーム共有文書の更新を土壇場で行います。

その後、IT 部門は、従業員のアカウントからの異常なログイン試行と、世界中の複数の場所からの不正なデータアクセスに関する通知を受け取ります。

調査の結果、攻撃者がワイヤレス接続を傍受して操作し、機密情報にアクセスしていることが確認されました。

理解度テスト →

攻撃タイプ：中間者 (MITM)

1：攻撃対象領域を縮小　2　3　4

異常なログイン試行を検出した後、IT チームが最初に調査すべき場所はどこですか？

- [ ] ファイアウォール、侵入検出システム (IDS)、侵入防止システム (IPS) のログ、Extended Detection and Response (XDR)
- [ ] 影響を受ける従業員のノートパソコン
- [ ] カフェのセキュリティ保護されていない Wi-Fi 上のネットワーク トラフィック
- [ ] 会社のシステムからの認証ログ

正解を見る →

攻撃タイプ：中間者 (MITM)

1：攻撃対象領域を縮小 2 3 4

異常なログイン試行を検出した後、IT チームが最初に調査すべき場所はどこですか？

- ✓ ファイアウォール、侵入検出システム (IDS)、侵入防止システム (IPS) のログ、Extended Detection and Response (XDR)
- ✗ 影響を受ける従業員のノートパソコン
- ✗ カフェのセキュリティ保護されていない Wi-Fi 上のネットワーク トラフィック
- ✓ 会社のシステムからの認証ログ

IT チームは、ファイアウォール、IDS/IPS、認証ログを分析することで、不正アクセスの試行を追跡し、侵害されたアカウントを評価して、インシデントの範囲をより深く理解することができます。

次の質問 →

攻撃タイプ：中間者 (MITM)

1 — 2：サイバー脅威の検出と対処 — 3 — 4

MITM 攻撃を確認した後、IT チームはただちにどのような対応を取る必要がありますか？

- [ ] 侵害された従業員のデバイスをネットワークから直ちに切断し、分析のために隔離する
- [ ] ファイアウォール ルールとネットワーク構成をアップデートして、さらなる不正アクセスを防止する
- [ ] 全従業員アカウントのパスワードをリセットする
- [ ] 影響を受けるシステムを無効にしてデータの流出を防止する

正解を見る →

攻撃タイプ：中間者 (MITM)

1 — 2：サイバー脅威の検出と対処 — 3 — 4

MITM 攻撃を確認した後、IT チームはただちにどのような対応を取る必要がありますか？

- ✓ 侵害された従業員のデバイスをネットワークから直ちに切断し、分析のために隔離する
- ✓ ファイアウォール ルールとネットワーク構成をアップデートして、さらなる不正アクセスを防止する
- ✗ 全従業員アカウントのパスワードをリセットする
- ✗ 影響を受けるシステムを無効にしてデータの流出を防止する

侵害されたデバイスを直ちに切断して隔離すると、攻撃者のアクセスが停止し、フォレンジック証拠が保持されます。一方、ファイアウォールとネットワーク ルールをアップデートすると、悪意のある接続がさらにブロックされ、より広範なネットワークが継続的な侵害から保護されます。

次の質問 →

攻撃タイプ：中間者 (MITM)

1 2 3：サイバー攻撃からのリカバリー 4

MITM 攻撃に対する脆弱性を軽減するには、どのような予防策を講じればよいですか？

- [ ] 全従業員に仮想プライベート ネットワーク (VPN) の使用を強制する
- [ ] 多要素認証 (MFA) などのゼロトラスト セキュリティ原則を実装する
- [ ] パブリック Wi-Fi の使用を避ける
- [ ] E メールで共有される機密ファイルを暗号化する

正解を見る →

攻撃タイプ：中間者 (MITM)

1 2 3：サイバー攻撃からのリカバリー 4

MITM 攻撃に対する脆弱性を軽減するには、どのような予防策を講じればよいですか？

- ✓ 全従業員に仮想プライベート ネットワーク (VPN) の使用を強制する
- ✓ 多要素認証 (MFA) などのゼロトラスト セキュリティ原則を実装する
- ✗ パブリック Wi-Fi の使用を避ける
- ✗ E メールで共有される機密ファイルを暗号化する

安全でないネットワークでの VPN 利用を強制することで、従業員のインターネットトラフィックを暗号化し、傍受を防止します。同時に、ゼロトラスト セキュリティと MFA を実装することで、 すべてのアクセス リクエストが継続的に検証されるようになります。

次の質問 →

攻撃タイプ：中間者 (MITM)

1 — 2 — 3 — 4：全体的なベストプラクティス

侵害に対処した後、組織はどのような長期戦略を実施すべきですか？

- [ ] システムの監査とパッチ適用を定期的に実施する
- [ ] ネットワーク セグメンテーションを強化して機密データとシステムを隔離する
- [ ] エンドポイントの検出と対応 (EDR) ソリューションと Managed Detection and Response (MDR) ソリューションを導入する
- [ ] 従業員向けの堅牢で定期的なトレーニングを実施する
- [ ] 上記すべて

正解を見る →

攻撃タイプ：中間者 (MITM)

1 — 2 — 3 — 4：全体的なベストプラクティス

侵害に対処した後、組織はどのような長期戦略を実施すべきですか？

- [x] システムの監査とパッチ適用を定期的に実施する
- [x] ネットワーク セグメンテーションを強化して機密データとシステムを隔離する
- [x] エンドポイントの検出と対応 (EDR) ソリューションと Managed Detection and Response (MDR) ソリューションを導入する
- [x] 従業員向けの堅牢で定期的なトレーニングを実施する
- [x] 上記すべて

さまざまな脅威から保護するために、こうした長期的な戦略を組み合わせることで、攻撃者がギャップを悪用するのを防ぎ、侵害に迅速かつ効果的に対応できるような、包括的でレジリエンスに優れたセキュリティ体制を構築できます。

ソリューションを見る →

攻撃タイプ：中間者 (MITM)

まとめ

MITM 攻撃では、サイバー犯罪者が 2 者間（従業員と企業のサーバー間、顧客とビジネス Web サイト間など）の通信を密かに傍受します。攻撃者の目的はさまざまですが、結果は同じです。つまり、信頼とセキュリティの侵害です。

Dell の革新的で拡張性のあるセキュリティ ソリューションを導入することで、組織は、検出、対応、リカバリーを確実に行うために必要なツールと専門技術を使用して、MITM の脅威を無力化し、資産を保護し、ビジネスの整合性を維持できるようになります。

高度なサイバー レジリエンス戦略の詳細をご覧になり、MITM 攻撃から組織を保護するために Dell がどのように支援できるかをご確認ください。

MITM 攻撃の概要を読む →

⌂ シナリオに戻る

信頼できるデバイス ›

Dell は、ハードウェア認証、SafeBIOS や SafeID などのファームウェア保護、堅牢な暗号化、ゼロトラスト フレームワークを活用して、エンドポイントと転送中のデータを保護します。

PowerEdge サーバー ›

セキュア ブート、シリコン ルート オブ トラスト、動的 USB ポート管理、システム ロックダウンを利用して、ハードウェアの整合性を確保し、重要なワークロードをネットワークベースの脅威から保護します。

ストレージ ソリューション ›

静止データや転送中のデータを暗号化し、隔離されたスナップショットと迅速なリカバリー機能を組み合わせることで、ファイルの安全性を確保し、MITM 攻撃後も迅速にリストアできるようにします。

PowerProtect ポートフォリオ ›

変更不可能で隔離されたバックアップと AI 主導の CyberSense 分析は、MITM 攻撃の発生時に迅速なリカバリーと信頼できるデータ リストアを可能にします。

セキュリティとレジリエンスに関するサービス ›

脆弱性評価やユーザー トレーニングから、侵入テストやインシデント対応にいたるまで、Dell のエキスパートとパートナーによる包括的なサポートで、防御を強化します。

攻撃タイプ：プロンプト /SQL インジェクション

主にチャット ボットを介してサービスを実施する航空会社のカスタマー サービス部門で働いています。

あなたと同僚のもとに、顧客からマイレージ アカウントにログインできないという電話が殺到していることに気づきます。ログインしてみると、マイレージ アカウントのマイルがすべて消えていることがわかります。

理解度テスト →

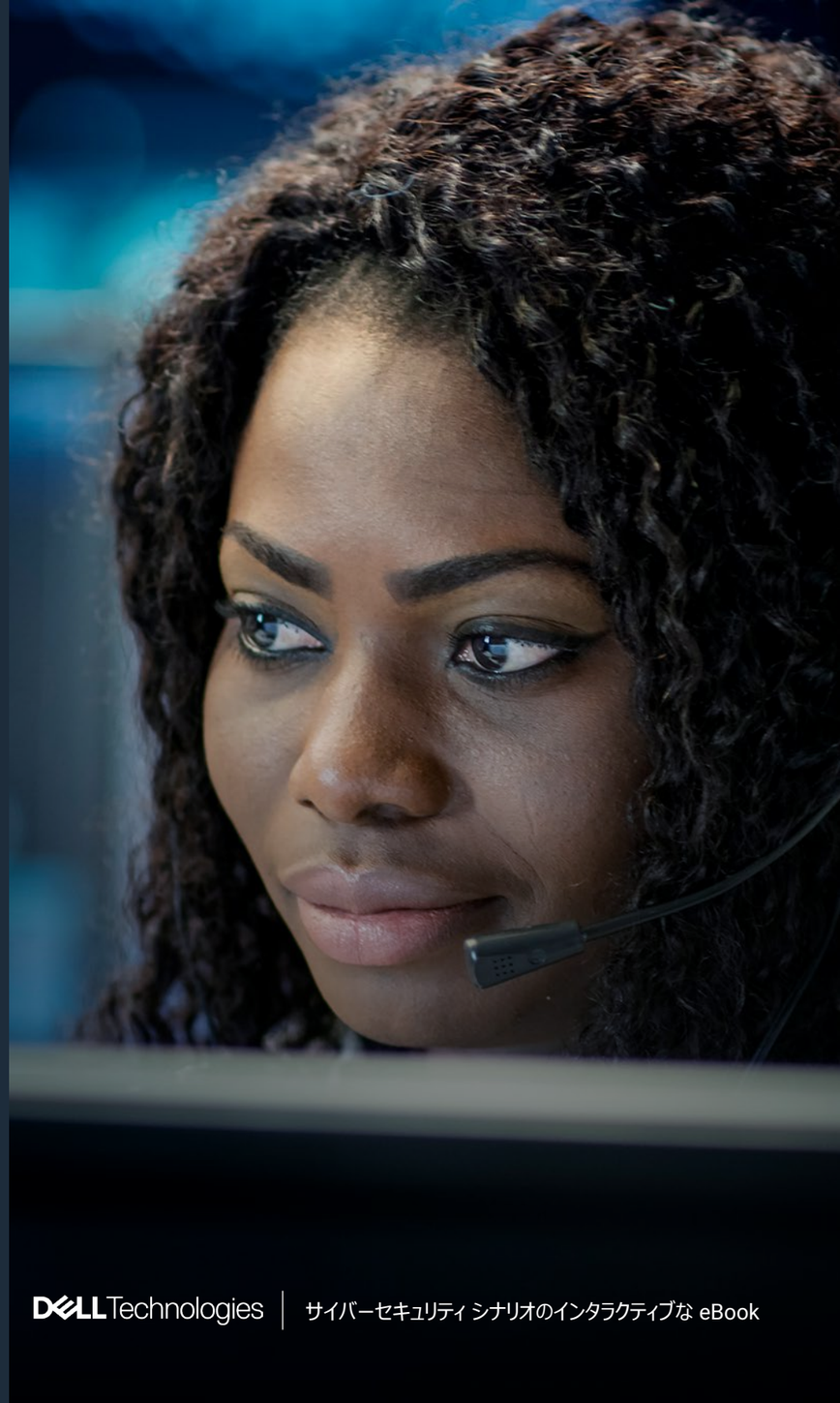
攻撃タイプ：プロンプト /SQL インジェクション

1：攻撃対象領域を縮小　2　3　4

調査すると、ログにいくつかのエラーが見つかります。*構造化クエリー言語 (SQL) ステートメントの構文エラーまたは無効な列名「admin」*です。これはどのようなタイプのサイバー インシデントですか？

- [ ] 認証情報の盗難
- [ ] プロンプトまたは SQL インジェクション
- [ ] 中間者攻撃
- [ ] フィッシング

正解を見る →



攻撃タイプ：プロンプト /SQL インジェクション

1：攻撃対象領域を縮小 2 3 4

調査すると、ログにいくつかのエラーが見つかります。*構造化クエリー言語 (SQL) ステートメントの構文エラーまたは無効な列名「admin」です。*これはどのようなタイプのサイバー インシデントですか？

- ✗ 認証情報の盗難
- ✓ プロンプトまたは SQL インジェクション
- ✗ 中間者攻撃
- ✗ フィッシング

「プロンプトまたは SQL インジェクション」が正解です。「SQL ステートメントの構文エラー」や「無効な列名「admin」」などのログエラーから、攻撃者が悪意のある SQL コードを使用してチャットボットの入力フィールドを悪用し、顧客のアカウント データにアクセスしたり、変更したりしたことがわかります。これは明らかに SQL インジェクション攻撃の兆候であり、上述の疑わしいアクティビティに一致します。

次の質問 →

攻撃タイプ：プロンプト /SQL インジェクション

1 — 2：サイバー脅威の検出と対処 — 3 — 4

カスタマー サービス チャットボットを介してプロンプト /SQL インジェクションが発生したことに気付きました。どうすべきでしょうか？

- [ ] ボットをオフラインにする
- [ ] データベース ログを調査して、不正アクセスや盗難、変更、削除されたデータについて調べる
- [ ] すべてのデータ侵害開示法を遵守する
- [ ] 上記すべて

正解を見る →

攻撃タイプ：プロンプト /SQL インジェクション

1 — 2：サイバー脅威の検出と対処 — 3 — 4

カスタマー サービス チャットボットを介してプロンプト /SQL インジェクションが発生したことに気付きました。どうすべきでしょうか？

- [x] ボットをオフラインにする
- [x] データベース ログを調査して、不正アクセスや盗難、変更、削除されたデータについて調べる
- [x] すべてのデータ侵害開示法を遵守する
- [x] 上記すべて

プロンプト /SQL インジェクション攻撃に対応するには、チャットボットをオフラインにして、不正アクセスがないかデータベース ログを調査し、開示法を遵守する必要があります。これらの手順は、悪用を阻止し、被害を評価し、規制上や倫理上の義務を果たすのに不可欠です。

次の質問 →

攻撃タイプ：プロンプト /SQL インジェクション

1 — 2 — 3：サイバー攻撃からのリカバリー — 4

プロンプト /SQL インジェクションを阻止するために、どのような機能を導入すべきですか？

- [ ] コーディングの実践として、準備されたステートメントやパラメーター化されたクエリーを使用するように開発チームを教育する
- [ ] Managed Detection and Response (MDR) ツール
- [ ] 多要素認証 (MFA)、ロールベースのアクセス制御 (RBAC)、Web アプリケーション ファイアウォール (WAF) など、最小権限アクセスを実装する
- [ ] バックエンド データベース / ナレッジベースをセグメント化する

正解を見る →

攻撃タイプ：プロンプト /SQL インジェクション

1 — 2 — 3：サイバー攻撃からのリカバリー — 4

プロンプト /SQL インジェクションを阻止するために、どのような機能を導入すべきですか？

- ✓ コーディングの実践として、準備されたステートメントやパラメーター化されたクエリーを使用するように開発チームを教育する
- ✗ Managed Detection and Response (MDR) ツール
- ✓ 多要素認証 (MFA)、ロールベースのアクセス制御 (RBAC)、Web アプリケーション ファイアウォール (WAF) など、最小権限アクセスを実装する
- ✗ バックエンド データベース / ナレッジベースをセグメント化する

準備されたステートメントやパラメーター化されたクエリーを使用するよう開発チームをトレーニングすることで、ソースでの SQL インジェクション攻撃をブロックします。一方、MFA、RBAC、WAF などの最小限のアクセス権限による制御を適用することで、攻撃者による権限の昇格や横方向への移動を防ぐことができ、インジェクションの試みの影響を抑制します。

次の質問 →

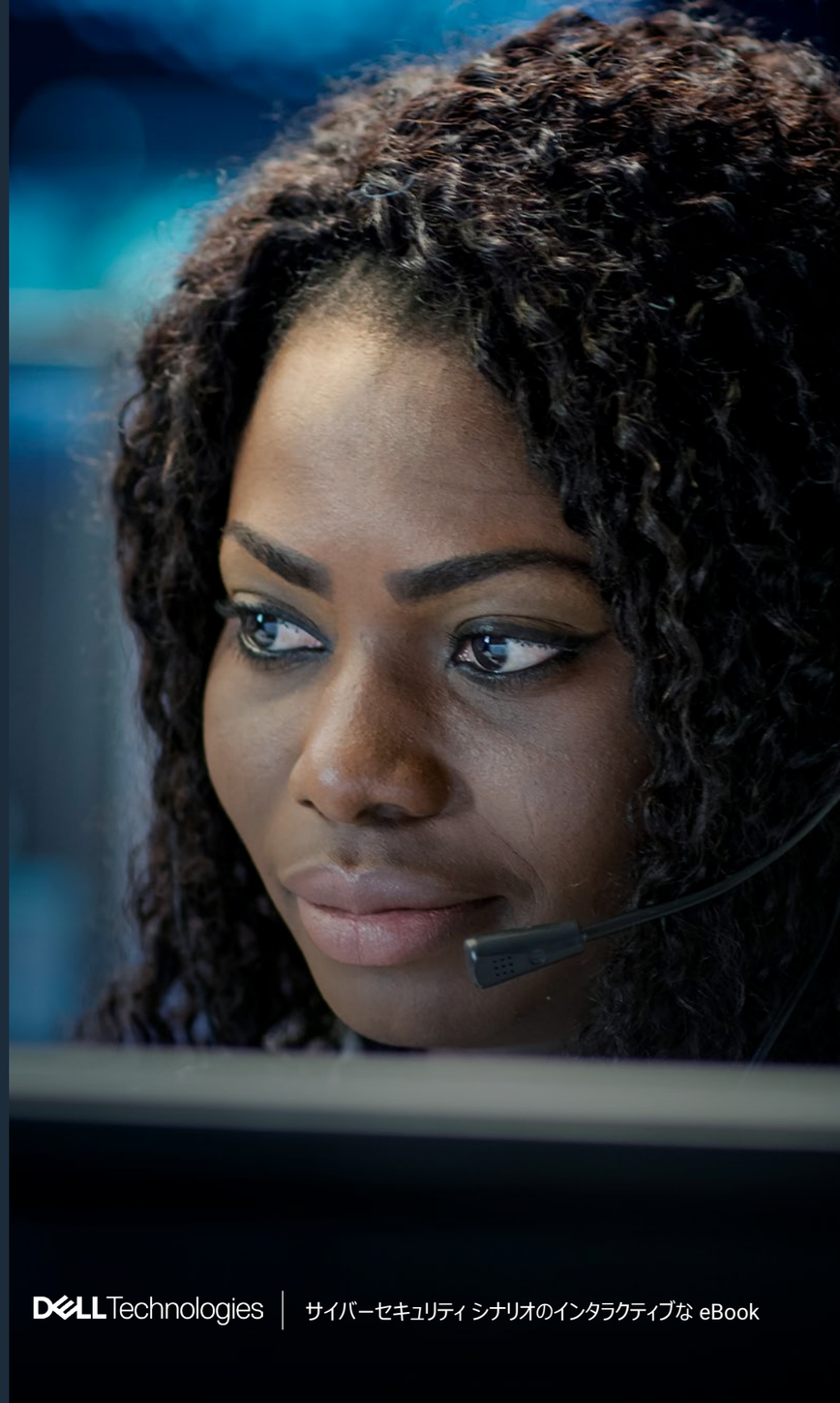
攻撃タイプ：プロンプト /SQL インジェクション

1 2 3 4：全体的なベストプラクティス

航空会社の顧客データを取り戻すために、どのような手段を取りますか？

- [ ] 盗まれたデータを追跡する
- [ ] 顧客にプロフィールを作りなおしてもらう
- [ ] サイバー攻撃者から買い戻す
- [ ] 最新の侵害されていないバックアップからリストアしてマイレージを復元し、顧客にパスワードの変更とクレジット カードの確認を行うよう通知する

正解を見る →



攻撃タイプ：プロンプト /SQL インジェクション

1 2 3 4：全体的なベスト プラクティス

航空会社の顧客データを取り戻すために、どのような手段を取りますか？

- ✗ 盗まれたデータを追跡する
- ✗ 顧客にプロフィールを作りなおしてもらう
- ✗ サイバー攻撃者から買い戻す
- ✓ 最新の侵害されていないバックアップからリストアしてマイレージを復元し、顧客にパスワードの変更とクレジット カードの確認を行うよう通知する

失われたアカウントデータを、最新の侵害されていないバックアップからリカバリーすることで、データの整合性を維持し、ダウンタイムを短縮するパスワードをリセットし、クレジット カードの使用状況を監視するよう顧客に迅速に通知することで、破壊的なインジェクション攻撃後の法令遵守をさらにサポートする

ソリューションを見る →

攻撃タイプ：プロンプト /SQL インジェクション

まとめ

プロンプト インジェクション攻撃と SQL インジェクション攻撃は、サイバー犯罪者が使用するサイバー攻撃手法の中で、最も被害が大きく広範に及ぶことが幾度となく証明されてきました。これらの攻撃は、ユーザー クエリーやデータベース システムの脆弱性を悪用するもので、サイバー攻撃者にサーバーの操作、データの窃取、ワークフローの妨害を行う余地を与えます。

進化するプロンプト /SQL インジェクションによる脅威や攻撃から組織を保護することは、Dell のサイバーセキュリティに対する継続的な取り組みの一環であり、当社は検出、対応、リカバリーに必要なツールと専門技術を提供します。

高度なサイバー レジリエンス戦略についてお読みになり、プロンプト攻撃や SQL インジェクション攻撃からの防御を Dell がどのように支援できるかをご確認ください。

プロンプト /SQL インジェクションの概要を見る →

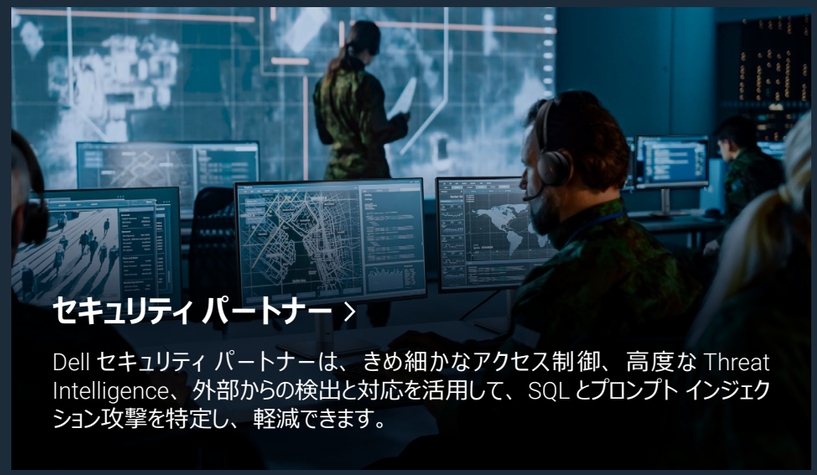
⌂ シナリオに戻る

信頼できるワークスペースと信頼できるインフラストラクチャ ›

エンドポイントを保護し、侵害された認証情報がインジェクション攻撃で悪用されるリスクを軽減します。

PowerEdge サーバー ›

Dell PowerEdge サーバーは、ハードウェア ルート オブ トラスト、セキュア ブート、シリコンベースのセキュリティ、リアルタイムの構成検証を備えており、信頼できるコードのみを実行する改ざん防止インフラストラクチャを保証します。



セキュリティ パートナー ›

Dell セキュリティ パートナーは、きめ細かなアクセス制御、高度な Threat Intelligence、外部からの検出と対応を活用して、SQL とプロンプト インジェクション攻撃を特定し、軽減できます。

PowerProtect ポートフォリオ ›

Dell の変更不可能なエアギャップ バックアップと高度な Cyber Recovery 分析は、信頼できるリストア ポイントを特定し、データの破損や流出からの迅速なリカバリーを可能にします。

セキュリティとレジリエンスに関するサービス ›

Dell のエキスパートとパートナーは、セキュアな開発のトレーニングや侵入テストから、脅威の追跡やインシデント対応まで、インジェクション攻撃に対する保護の検証と迅速な修復を支援します。

攻撃タイプ：ランサムウェア

電子カルテ (EHR)、スマート点滴ポンプ、放射線画像診断など、すべてが一元管理のネットワークに接続された医療システムで知られる、地方の中核病院で IT 担当者として勤務しています。

昨夜、いくつかのシステムが同時にクラッシュし始めました。朝までに、臨床スタッフは患者記録から締め出されたと報告しています。

複数の端末に次のような身代金要求メモが表示されています。

「ファイルは暗号化されています。72 時間以内に 20 ビットコインを支払わないと、患者データを公開します」

理解度テスト →

攻撃タイプ：ランサムウェア

1：攻撃対象領域を縮小　2　3　4

ヘルプ デスクには、ファイル暗号化やアプリケーション エラーに関する報告が 100 件以上寄せられています。セキュリティ ログには、内部ドメイン アカウントからの異常なファイル名の変更が記録されています。最初にするべきことは何ですか？

- [ ] 身代金を直ちに支払い、重要なサービスをリストアする
- [ ] 法執行機関と法務担当者に通知する
- [ ] 影響を受けるすべてのエンドポイントの再イメージ化を開始する
- [ ] 感染したシステムをネットワークから切り離す

正解を見る →

攻撃タイプ：ランサムウェア

1：攻撃対象領域を縮小 — 2 — 3 — 4

ヘルプ デスクには、ファイル暗号化やアプリケーション エラーに関する報告が 100 件以上寄せられています。セキュリティ ログには、内部ドメイン アカウントからの異常なファイル名の変更が記録されています。最初にするべきことは何ですか？

- ✗ 身代金を直ちに支払い、重要なサービスをリストアする
- ✗ 法執行機関と法務担当者に通知する
- ✗ 影響を受けるすべてのエンドポイントの再イメージ化を開始する
- ✓ 感染したシステムをネットワークから切り離す

感染した病院システムを直ちに切断して隔離することで、ランサムウェアの拡散を阻止し、重要な医療機器と機密性の高い患者データを保護します。また、調査のための証拠を保全して、連携の取れた対応とリカバリーのための重要な時間を確保します。

次の質問 →

攻撃タイプ：ランサムウェア

1 — 2：サイバー脅威の検出と対処 — 3 — 4

インシデント対応チームは、多要素認証 (MFA) を使用していないサーバーへのアクセスに使用された、侵害されたアカウントから攻撃が開始された可能性が高いことを発見しました。攻撃に最も直接的に貢献したのは次のうちどれですか？

- [ ] 古いウイルス対策定義
- [ ] 公開された電子カルテ (EHR) データベース
- [ ] リモート アクセスにおける MFA の欠如
- [ ] 脆弱な E メール フィルタリング

正解を見る →

攻撃タイプ：ランサムウェア

1 — 2：サイバー脅威の検出と対処 — 3 — 4

インシデント対応チームは、多要素認証 (MFA) を使用していないサーバーへのアクセスに使用された、侵害されたアカウントから攻撃が開始された可能性が高いことを発見しました。攻撃に最も直接的に貢献したのは次のうちどれですか？

- ✗ 古いウイルス対策定義
- ✗ 公開された電子カルテ (EHR) データベース
- ✓ リモート アクセスにおける MFA の欠如
- ✗ 脆弱な E メール フィルタリング

リモート アクセスにおける MFA の欠如は、攻撃者が追加の検証手順を踏むことなく、盗難または推測された認証情報でログインできるようにすることで、サーバー侵害を可能にしました。MFA を使用すると、侵害されたアカウントでも 2 つ目の認証が必要になり、不正アクセスのリスクが大幅に軽減されます。

次の質問 →

攻撃タイプ：ランサムウェア

1 2 3：サイバー攻撃からのリカバリー 4

医療スタッフは、現在、紙ベースのワークフローに依存しています。そのため、本日手術が予定されている患者をシステムで確認することができません。病院の運営をサポートするのに最適な短期的アクションは何ですか？

- [ ] コア データベース サーバーを再起動して再初期化を行う
- [ ] たとえ 6 か月前のものであっても、すべての古いバックアップを有効にする
- [ ] 病院の手動によるダウンタイム手順を有効化し、緊急対応チームにエスカレーションする
- [ ] ケースバイケースで、どのように進めるかをスタッフに判断させる

正解を見る →

攻撃タイプ：ランサムウェア

1 — 2 — 3：サイバー攻撃からのリカバリー — 4

医療スタッフは、現在、紙ベースのワークフローに依存しています。そのため、本日手術が予定されている患者をシステムで確認することができません。病院の運営をサポートするのに最適な短期的アクションは何ですか？

- ✗ コア データベース サーバーを再起動して再初期化を行う
- ✗ たとえ 6 か月前のものであっても、すべての古いバックアップを有効にする
- ✓ 病院の手動によるダウンタイム手順を有効化し、緊急対応チームにエスカレーションする
- ✗ ケースバイケースで、どのように進めるかをスタッフに判断させる

手動のダウンタイム手順を有効化し、緊急対応チームにエスカレーションすることで、重要な臨床ワークフローを即座に継続し、患者の安全を守り、ケアを検証して文書化するための標準化されたプロセスを確立できます。このアプローチは、エラーを最小限に抑え、リスクとリソースを効率的に管理し、専門家がデジタル システムを安全に復元できるようサポートします。

次の質問 →

攻撃タイプ：ランサムウェア

1 2 3 4：全体的なベストプラクティス

地元メディアがこのニュースを取り上げています。経営陣は、公式声明を出すべきかどうかを知りたがっており、法務部からは HIPAA（医療保険の相互運用性と説明責任に関する法律）の義務について問い合わせがありました。次のステップとして最も適切なものはどれですか？

- [ ] 詳細な情報が入手できるまで、事件を公に否定する
- [ ] サードパーティーの IT ベンダーを非難するプレスリリースを発表する
- [ ] 規制当局に通知し、内部侵害の通知手続きを開始する
- [ ] ただちに身代金を支払い、世間の注目を避ける

正解を見る →

攻撃タイプ：ランサムウェア

1 — 2 — 3 — 4：全体的なベストプラクティス

地元メディアがこのニュースを取り上げています。経営陣は、公式声明を出すべきかどうかを知りたがっており、法務部からは HIPAA（医療保険の相互運用性と説明責任に関する法律）の義務について問い合わせがありました。次のステップとして最も適切なものはどれですか？

- ✗ 詳細な情報が入手できるまで、事件を公に否定する
- ✗ サードパーティーの IT ベンダーを非難するプレスリリースを発表する
- ✓ 規制当局に通知し、内部侵害の通知手続きを開始する
- ✗ ただちに身代金を支払い、世間の注目を避ける

HIPAA と州法で義務付けられている通り、保護されるべき医療情報の侵害を当局と影響を受ける個人にすみやかに報告することで、法令遵守、法的保護、ベストプラクティスの透明性を確保し、法的損害や風評被害を防ぎ、開示義務の責任を果たして、患者、スタッフ、ステークホルダーとの適切なコミュニケーションを確立することができます。

ソリューションを見る →

攻撃タイプ：ランサムウェア

まとめ

ランサムウェアは、身代金が支払われるまでコンピューター システムやデータへのアクセスを遮断するマルウェアの一種です。深刻な問題を引き起こすサイバー攻撃の 1 つに数えられます。世界の組織の 50% が過去 1 年間に少なくとも 1 回ランサムウェアの被害を受けています。ランサムウェア攻撃に伴う平均ダウンタイムは 3 週間に及び、深刻な業務中断を招いています。

Dell では、ゼロトラスト フレームワーク、エンドポイント保護、ネットワーク セグメンテーションで組織を保護し、ランサムウェアの侵入を阻止して、その拡散を抑えることを優先しています。エキスパート主導のインシデント対応計画は、レジリエンスの維持や攻撃からの迅速なリカバリーに役立ちます。

高度なサイバー レジリエンス戦略の詳細をご覧になり、ランサムウェア攻撃から組織を保護するために Dell がどのように支援できるかをご確認ください。

ランサムウェア攻撃の概要を見る →

⌂ シナリオに戻る

信頼できるインフラストラクチャ ›

ハードウェア認証、多要素認証 (MFA)、ロールベースのアクセス制御 (RBAC)、ゼロトラスト フレームワークは、インフラストラクチャ レベルでランサムウェアを阻止します。

ネットワーキングと PowerEdge サーバー ›

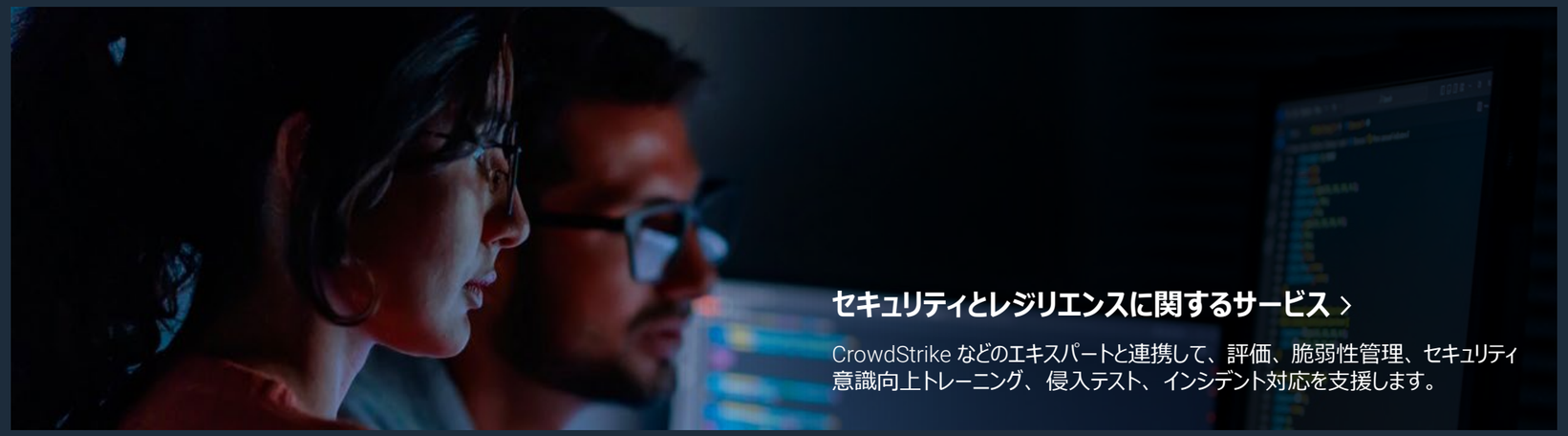
ランサムウェアの動きを制限します。ネットワーク セグメンテーション、セキュア ブート、シリコン ルート オブ トラスト、動的 USB ポート管理、システム ロックダウンの機能を備えています。

信頼できるワークスペース ›

SafeBIOS、SafeID、SafeData、エンドポイントの検出と対応 (EDR) ツールを統合することで、プロアクティブな Threat Intelligence の利用、リアルタイム検出、マルウェアの自動封じ込めがデバイス レベルで可能になります。

PowerProtect ポートフォリオ ›

変更不可能なエアギャップ バックアップ、インテリジェントな Cyber Recovery 分析、迅速なリストア機能により、重要なデータを保護し、恐喝を防止してレジリエンスを高めます。



セキュリティとレジリエンスに関するサービス ›

CrowdStrike などのエキスパートと連携して、評価、脆弱性管理、セキュリティ意識向上トレーニング、侵入テスト、インシデント対応を支援します。

攻撃タイプ：サプライ チェーン ハードウェア

ある会社では、世界中のオフィス全体に 500 台の新しいノートパソコンを導入します。導入を迅速化するために、イメージングとハードウェアの準備をサードパーティーの IT ロジスティクス ベンダーに委託しました。ベンダーは、事前構成済みのマシンを従業員に直接出荷します。

数日もしないうちに、現場から次のような電話が何本もかかってきます。

- 多要素認証 (MFA) の要求がバイパスされ、正しく機能していない
- セキュリティ チームは、不規則な時間帯に多数の不正な管理者ログインを確認している
- また、オフラインであると思われるユーザーからの仮想プライベート ネットワーク (VPN) トラフィックも確認している

理解度テスト →

攻撃タイプ：サプライ チェーン ハードウェア

1：攻撃対象領域を縮小　2　3　4

従業員は、ログインしていないのに多要素認証 (MFA) のプッシュ通知を受信したと報告しています。組織のセキュリティ ダッシュボードには、会社発行の資産タグが付いたデバイスからログインされたことが表示されます。セキュリティ オペレーション センター (SOC) チームにとって、最も論理的な最初のステップは何ですか？

- [ ] ユーザーのアカウントを無効にし、リモートでノートパソコンを消去する
- [ ] ログイン IP とデバイスの指紋を他の既知の侵害されたユーザーと比較する
- [ ] ユーザーに障害が発生していると仮定して HR にエスカレーションする
- [ ] パスワードをただちに変更するよう全社的に警告を発する

正解を見る →

攻撃タイプ：サプライ チェーン ハードウェア

1：攻撃対象領域を縮小 2 3 4

従業員は、ログインしていないのに多要素認証 (MFA) のプッシュ通知を受信したと報告しています。組織のセキュリティ ダッシュボードには、会社発行の資産タグが付いたデバイスからログインされたことが表示されます。セキュリティ オペレーション センター (SOC) チームにとって、最も論理的な最初のステップは何ですか？

- ✗ ユーザーのアカウントを無効にし、リモートでノートパソコンを消去する
- ✓ ログイン IP とデバイスの指紋を他の既知の侵害されたユーザーと比較する
- ✗ ユーザーに障害が発生していると仮定して HR にエスカレーションする
- ✗ パスワードをただちに変更するよう全社的に警告を発する

SOC チームが、不審なアクティビティが広範な攻撃の一部であるか、単独の攻撃であるかを判断して、パターン認識を迅速に行う場合、サプライ チェーン ハードウェア攻撃を特定する際の最初のステップは、対象を絞ったインシデント対応とさらなるリスクの封じ込めになります。

次の質問 →

攻撃タイプ：サプライ チェーン ハードウェア

1 — 2：サイバー脅威の検出と対処 — 3 — 4

インシデント対応チームは、影響を受けた複数のノートパソコンが、ベンダーの公式リリース ノートと一致しない SSD ファームウェア バージョンを実行していることを確認しました。エンドポイント検出応答 (EDR) には、 悪意のあるプロセスは表示されていません。これは何を示している可能性が最も高いですか？

- [ ] IT ベンダーからの構成エラー
- [ ] 自ら削除する新しいタイプのランサムウェア
- [ ] ファームウェアレベルでのサプライ チェーンへの侵害
- [ ] イメージング中の正常な動作

正解を見る →

攻撃タイプ：サプライ チェーン ハードウェア

1 — 2：サイバー脅威の検出と対処 — 3 — 4

インシデント対応チームは、影響を受けた複数のノートパソコンが、ベンダーの公式リリース ノートと一致しない SSD ファームウェア バージョンを実行していることを確認しました。エンドポイント検出応答 (EDR) には、 悪意のあるプロセスは表示されていません。これは何を示している可能性が最も高いですか？

- ✗ IT ベンダーからの構成エラー
- ✗ 自ら削除する新しいタイプのランサムウェア
- ✓ ファームウェアレベルでのサプライ チェーンへの侵害
- ✗ イメージング中の正常な動作

複数のノートパソコンで見られた不正な SSD ファームウェアは、EDR では検出されず、公式リリースとも一致しないことから、ハードウェアまたはファームウェアの意図的な改ざんを示しています。これは、 ファームウェアレベルでのサプライ チェーンへの侵害の特徴です。

次の質問 →

攻撃タイプ：サプライ チェーン ハードウェア

1 2 3：サイバー攻撃からのリカバリー 4

不正な SSD ファームウェアが搭載されている疑いのあるデバイス 100 台を隔離しました。リモート アクセスできる攻撃者に気づかれずに、対処する方法を決定する必要があります。次にとるべき最善の行動は何ですか？

- [ ] すべてのデバイスの電源を切り、フォレンジックに送る
- [ ] システムの稼動中にライブでメモリー ダンプを行い、調査する
- [ ] 侵害されたことをサードパーティー ベンダーに通知する
- [ ] すべてのデバイスを消去し、世界中の全ユーザーに新しいノートパソコンを再配布する

正解を見る →

攻撃タイプ：サプライ チェーン ハードウェア

1 — 2 — 3：サイバー攻撃からのリカバリー — 4

不正な SSD ファームウェアが搭載されている疑いのあるデバイス 100 台を隔離しました。リモート アクセスできる攻撃者に気づかれずに、対処する方法を決定する必要があります。次にとるべき最善の行動は何ですか？

- ✗ すべてのデバイスの電源を切り、フォレンジックに送る
- ✓ システムの稼動中にライブでメモリー ダンプを行い、調査する
- ✗ 侵害されたことをサードパーティー ベンダーに通知する
- ✗ すべてのデバイスを消去し、世界中の全ユーザーに新しいノートパソコンを再配布する

ライブ メモリー ダンプは、アクティブなマルウェアやルートキットなどの不安定な証拠を保全するために重要であり、隠れた脅威やアクセス ポイントが失われたり、攻撃者に警告されたりする前に発見することで、対象を絞ったインシデント対応を可能にします。

次の質問 →

攻撃タイプ：サプライ チェーン ハードウェア

1 2 3 4：全体的なベスト プラクティス

最高情報セキュリティ責任者から、この攻撃がどのようにして環境に侵入したかについて概要をたずねられました。エグゼクティブ チームに簡潔な説明を行う必要があります。攻撃についてどのように説明すべきですか？

- [ ] フィッシング リンクから誤ってウイルスがダウンロードされた
- [ ] ネットワークの設定ミスで外部からのアクセスを許可してしまった
- [ ] ノートパソコンのプロビジョニング中に、侵害されたハードウェア ベンダーを通じて悪意のあるファームウェアが導入された
- [ ] 開発者の 1 人が安全でないコードを本番環境にプッシュした

正解を見る →

攻撃タイプ：サプライ チェーン ハードウェア

1 — 2 — 3 — 4：全体的なベスト プラクティス

最高情報セキュリティ責任者から、この攻撃がどのようにして環境に侵入したかについて概要をたずねられました。エグゼクティブ チームに簡潔な説明を行う必要があります。攻撃についてどのように説明すべきですか？

- ✗ フィッシング リンクから誤ってウイルスがダウンロードされた
- ✗ ネットワークの設定ミスで外部からのアクセスを許可してしまった
- ✓ ノートパソコンのプロビジョニング中に、侵害されたハードウェア ベンダーを通じて悪意のあるファームウェアが導入された
- ✗ 開発者の 1 人が安全でないコードを本番環境にプッシュした

ファームウェア バージョンが一致しておらず、アクティブなマルウェアがないことから、これはユーザーのミスや設定ミスではなく、ベンダーに起因するファームウェアレベルの攻撃であることが確実です。

ソリューションを見る →

攻撃タイプ：サプライ チェーン ハードウェア

まとめ

サプライ チェーン攻撃は、近年大幅に増加しています。攻撃者は、製造、出荷、導入の過程で物理デバイスを改ざんしたり、ソフトウェア プロバイダーの弱点を探し出したりすることで、悪意のあるコンポーネントやコードを注入する手段や、システムを破壊する手段、機密データを引き出す手段を得ます。被害の範囲は、小規模企業からグローバル企業まで多岐にわたることがあります。この攻撃の被害を受けると、深刻な経済的損失、顧客の信頼の低下、法的な制裁などの結果を招きます。

Dell は、厳格なベンダー リスク アセスメントを統合し、ゼロトラストの原則を組み込み、継続的なデバイス検証と独立した整合性チェックを行うことで、サプライ チェーン ハードウェア攻撃を軽減します。ライフサイクル全体を通じてハードウェアの整合性を強化します。

高度なサイバー レジリエンス戦略の詳細をご覧いただき、サプライ チェーン ハードウェア攻撃から組織を保護するために Dell がどのように支援できるかをご確認ください。

サプライ チェーン ハードウェア攻撃の概要を見る →

シナリオに戻る

サプライ チェーン保証 ›

Dell のサプライ チェーンは、高度な出所特定、改ざん防止ロジスティクス、透明性の高い調達を通じて、ハードウェア、ファームウェア、サプライヤーが組織に到着する前に厳格に検証されるようにします。

セキュアなコンポーネント検証 (SCV) ›

工場出荷時と設置時にパソコン コンポーネントを暗号形式で検証することで、真正性を確保し、隠れた改変を検出して、サプライ チェーンの改ざんリスクを軽減します。

信頼できるワークスペースと信頼できるインフラストラクチャ ›

ハードウェアベースの認証と継続的なファームウェア整合性チェックでエンドポイントを保護し、不正な変更や悪意のある埋め込みが脅威となる前に警告を発します。

資産追跡と ProSupport Suite with SupportAssist ›

包括的な資産追跡、デバイスの出所に関するリアルタイム モニタリング、プロアクティブな整合性検証で、迅速な異常検出を確実に行い全デバイスのセキュリティを確保します。

セキュリティ パートナー：AI を活用した検出と対応 ›

AI 主導のセキュリティ ツールは、継続的なモニタリング、フォレンジック調査、改ざんや異常なデバイス動作の自動封じ込めを可能にし、サプライ チェーンの脅威に対する迅速な対応が可能になります。

攻撃タイプ：サプライ チェーン ソフトウェア

ある会社は、病院で使用されるクラウドベースの分析ソフトウェアを開発しています。バックエンド サービスは、信頼できるサードパーティー開発者が GitHub で管理している、広く使用されている オープンソースのログ ライブラリーに依存しています。

開発チームが知らないうちに、攻撃者は GitHub アカウントを侵害し、次の目的で設計された隠れたコードを含む悪意のあるアップデートを挿入しました。

- アプリケーション プログラミング インターフェイス (API) キーや JavaScript オブジェクト表記 Web トークン (JWT) シークレットなどの環境変数を抽出する
- 特定の IP アドレスからリクエストがあった場合に、リバース シェルを生成する
- リモートでトリガーされない限り、休止状態のままにする

理解度テスト →

攻撃タイプ：サプライ チェーン ソフトウェア

1：攻撃対象領域を縮小　2　3　4

API が突然、500 件のエラーを主要なクライアントに返し始めます。クラウド モニタリングは、コンテナ化されたサービスから、以前に確認されていないドメインへのアウトバウンド接続にフラグを設定します。まずどのような対応をしますか？

- [ ] コンテナからのすべてのアウトバウンド ネットワーク トラフィックを無効にする
- [ ] 影響を受けるサービスを再起動して、メモリーの問題を解決する
- [ ] GitHub リポジトリーで最近のコード コミットを確認する
- [ ] ドメインのホスティング プロバイダーに連絡する

正解を見る →

攻撃タイプ：サプライ チェーン ソフトウェア

1：攻撃対象領域を縮小 2 3 4

API が突然、500 件のエラーを主要なクライアントに返し始めます。クラウド モニタリングは、コンテナ化されたサービスから、以前に確認されていないドメインへのアウトバウンド接続にフラグを設定します。まずどのような対応をしますか？

- ✓ コンテナからのすべてのアウトバウンド ネットワーク トラフィックを無効にする
- ✗ 影響を受けるサービスを再起動して、メモリーの問題を解決する
- ✗ GitHub リポジトリーで最近のコード コミットを確認する
- ✗ ドメインのホスティング プロバイダーに連絡する

コンテナからのアウトバウンド ネットワーク トラフィックをすべて無効にすることで、攻撃者による機密データの流出や、侵害されたログ ライブラリーを介したリモート アクセスの確立をただちに阻止できます。リアルタイムで環境を隔離することで、調査のための重要な時間を確保し、API キーとシークレットを保護し、休止状態の攻撃メカニズムの活性化を防ぎます。

次の質問 →

攻撃タイプ：サプライ チェーン ソフトウェア

1 — 2：サイバー脅威の検出と対処 — 3 — 4

エンジニアリング リードは、問題が発生する 3 日前にアプリケーションが GitHub から自動的にコードを取得したことを確認しています。そのバージョンは、まだどの公開データベースでも悪意があるものとしてマークされていません。最も責任のある即時のアクションは何ですか？

- [ ] GitHub を介してライブラリーのメンテナンス担当者に直接連絡する
- [ ] すべてのローカル プロジェクトの依存関係を削除して再構築する
- [ ] 共通脆弱性識別子 (CVE) を待ってから、さらにアクションを実行する
- [ ] 最後に確認された安全なバージョンのコードまでロールバックする

正解を見る →

攻撃タイプ：サプライ チェーン ソフトウェア

1 — 2：サイバー脅威の検出と対処 — 3 — 4

エンジニアリング リードは、問題が発生する 3 日前にアプリケーションが GitHub から自動的にコードを取得したことを確認しています。そのバージョンは、まだどの公開データベースでも悪意があるものとしてマークされていません。最も責任のある即時のアクションは何ですか？

- ✗ GitHub を介してライブラリーのメンテナンス担当者に直接連絡する
- ✗ すべてのローカル プロジェクトの依存関係を削除して再構築する
- ✗ 共通脆弱性識別子 (CVE) を待ってから、さらにアクションを実行する
- ✓ 最後に確認された安全なバージョンのコードまでロールバックする

最後に確認された安全なバージョンのコードまでロールバックすることで、侵害されたアップデートがただちに削除され、攻撃者の足がかりをなくし、運用の整合性がリストアされるため、リスクをプロアクティブに封じ込め、機密データを保護できます。

次の質問 →

攻撃タイプ：サプライ チェーン ソフトウェア

1 — 2 — 3：サイバー攻撃からのリカバリー — 4

分析の結果、ライブラリーから API キーとクラウド認証情報が流出していたことが判明しました。侵害されたバージョンで構築された複数のコンテナを特定しました。封じ込め戦略において最も重要なステップはどれですか？

- [ ] 影響を受ける環境全体ですべての認証情報を取り消してローテーションする
- [ ] 更新されたオペレーティング システム (OS) イメージを使用してコンテナを再イメージ化する
- [ ] 開発チームのノートパソコンを消去する
- [ ] GitHub リポジトリーの削除通知を提出する

正解を見る →

攻撃タイプ：サプライ チェーン ソフトウェア

1 — 2 — 3：サイバー攻撃からのリカバリー — 4

分析の結果、ライブラリーから API キーとクラウド認証情報が流出していたことが判明しました。侵害されたバージョンで構築された複数のコンテナを特定しました。封じ込め戦略において最も重要なステップはどれですか？

- ✓ 影響を受ける環境全体ですべての認証情報を取り消してローテーションする
- ✗ 更新されたオペレーティング システム (OS) イメージを使用してコンテナを再イメージ化する
- ✗ 開発チームのノートパソコンを消去する
- ✗ GitHub リポジトリーの削除通知を提出する

認証情報の取り消しとローテーションは、クラウド侵害後の最初の重要なステップであり、侵害の範囲に関係なく、攻撃者によるサービスへのアクセスをブロックし、データの盗難を阻止して、システムを保護します。

次の質問 →

攻撃タイプ：サプライ チェーン ソフトウェア

1 2 3 4：全体的なベスト プラクティス

最高技術責任者と法務 / コンプライアンスチームに、何が起こったかを説明するよう求められています。最も正確で明確な説明は何ですか？インシデントをどのように要約しますか？

- [ ] 社内の継続的な統合と継続的な導入 / デリバリー (CI/CD) ツールが失敗し、不正なコードの導入を許した
- [ ] サードパーティー製ソフトウェアの依存関係が侵害され、自動化によって本番環境に導入された
- [ ] 開発者が緊急リリースにテストされていないコードを含めた
- [ ] 攻撃者が GitHub リポジトリーをブルート フォースした

正解を見る →

攻撃タイプ：サプライ チェーン ソフトウェア

1 2 3 4：全体的なベスト プラクティス

最高技術責任者と法務 / コンプライアンスチームに、何が起こったかを説明するよう求められています。最も正確で明確な説明は何ですか？インシデントをどのように要約しますか？

- ✗ 社内の継続的な統合と継続的な導入 / デリバリー (CI/CD) ツールが失敗し、不正なコードの導入を許した
- ✓ サードパーティー製ソフトウェアの依存関係が侵害され、自動化によって本番環境に導入された
- ✗ 開発者が緊急リリースにテストされていないコードを含めた
- ✗ 攻撃者が GitHub リポジトリーをブルート フォースした

根本原因はサプライ チェーン攻撃でした。攻撃者がサードパーティー製ソフトウェアの依存関係を侵害し、自動化されたビルド プロセスによって悪意のあるアップデートが本番環境に直接取り込まれ、アプリケーションの整合性と機密性の高い環境に影響を与え、信頼できる外部依存関係における悪意のあるアップデートのリスクが浮き彫りになりました。

ソリューションを見る →

攻撃タイプ：サプライ チェーン ソフトウェア

まとめ

サプライ チェーン ソフトウェアのサイバー攻撃は、ソフトウェアのアップデートやサードパーティーの統合、開発環境の脆弱性を悪用し、ネットワーク全体に悪意のあるコードを埋め込むことで、被害を拡大させます。このような攻撃は、広範なデータ侵害、業務の中断、エコシステム全体の侵害を引き起こし、あらゆる規模の企業に影響を与える可能性があります。

Dell は、透明性、安全な開発、継続的なモニタリングを重視しながら、迅速なリカバリーとステークホルダーとのコミュニケーションを確保するための堅牢なインシデント対応計画を維持することで、サイバー レジリエンスの強化に取り組んでいます。

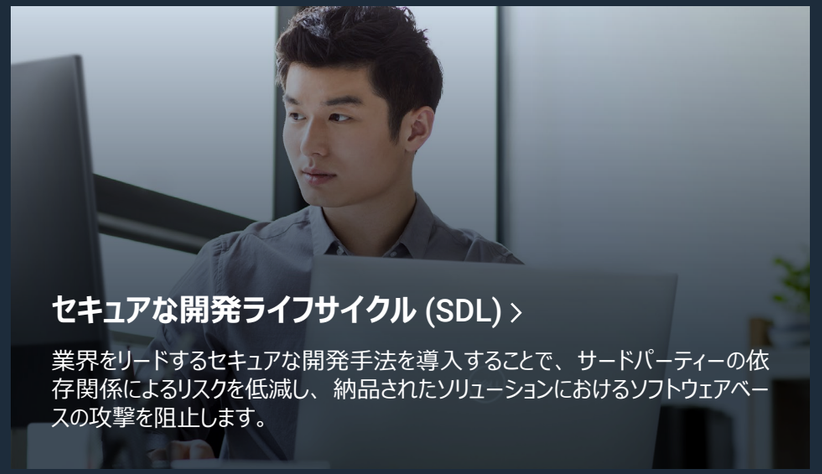
高度なサイバー レジリエンス戦略の詳細をご覧になり、サプライ チェーン ソフトウェア攻撃から組織を保護するために Dell がどのように支援できるかをご覧ください。

サプライ チェーン ソフトウェア攻撃の概要を見る →

⌂ シナリオに戻る

サプライ チェーン保証 ›

Dell のサプライ チェーンは、高度な出所特定、改ざん防止ロジスティクス、透明性の高い調達を通じて、ハードウェア、ファームウェア、サプライヤーが組織に到着する前に厳格に検証されるようにします。



セキュアな開発ライフサイクル (SDL) ›

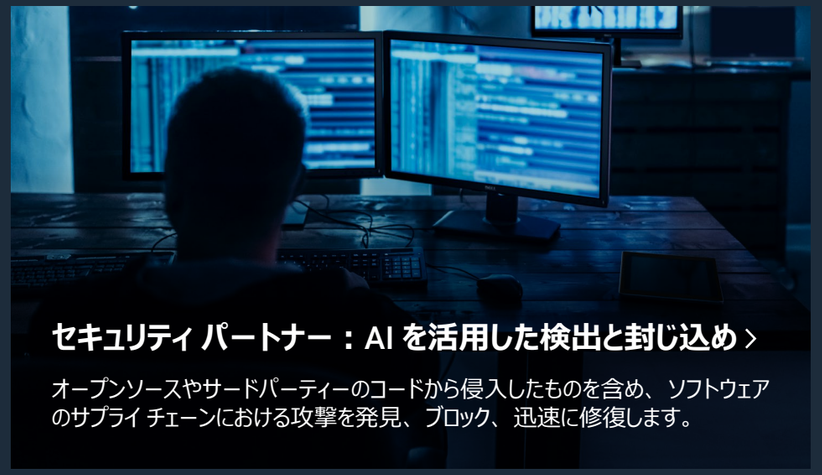
業界をリードするセキュアな開発手法を導入することで、サードパーティーの依存関係によるリスクを低減し、納品されたソリューションにおけるソフトウェアベースの攻撃を阻止します。

信頼できるワークスペースと信頼できるインフラストラクチャ ›

SafeBIOS、SafeID、SafeData によるハードウェア認証により、エンドポイントでは信頼されたコードのみが実行され、不正または悪意のあるソフトウェア改変を迅速に検出できます。

資産追跡と ProSupport Suite with SupportAssist ›

デバイスとソフトウェアをリアルタイムで監視することで、サプライチェーンを通じてもたらされる異常を迅速に検出して対応できます。



セキュリティ パートナー：AI を活用した検出と封じ込め ›

オープンソースやサードパーティーのコードから侵入したものを含め、ソフトウェアのサプライ チェーンにおける攻撃を発見、ブロック、迅速に修復します。

攻撃タイプ：ゼロデイ

企業の認証ログを監視するセキュリティ アナリストのケースです。最近、ユーザーが認証情報を共有していないにもかかわらず、アカウントへの不正アクセスが報告されています。

ログを調べたところ、次のようなアクティビティが見つかりました。

```
[INFO] 2025-04-02 14:05:12 - User Login - UserID: 1023 - IP: 192.168.1.15 - JWT Token Issued
[INFO] 2025-04-02 14:07:35 - User Login - UserID: 1023 - IP: 5.62.60.12 - JWT Token Reused
[INFO] 2025-04-02 14:08:00 - User Login - UserID: 1023 - IP: 203.0.113.45 - JWT Token Reused
```

同時に、セキュリティ研究者は、次に挙げるアプリケーション プログラミング インターフェイス (API) の脆弱性を特定しました。

- JavaScript オブジェクト表記 Web トークン (JWT) には、有効期限がありません。
- トークンは、HTTP 専用 Cookie ではなく、ローカル ストレージに保存されます。
- 多要素認証 (MFA) は、実施されません。

理解度テスト →

攻撃タイプ：ゼロデイ

1：攻撃対象領域を縮小　2　3　4

警告ベルが鳴らなかったため、セキュリティ チームとしては、これがゼロデイ攻撃であると疑っていますが、それをどのように確認しますか？

- [ ] すべてのユーザーをシステムからログオフする
- [ ] ログから異常な認証動作の主なものを特定する
- [ ] 他社の友人に電話して、同じ問題が発生しているかどうかを確認する
- [ ] 他のセキュリティ異常アクティビティとの相関関係を調べる

正解を見る →

攻撃タイプ：ゼロデイ

1：攻撃対象領域を縮小 — 2 — 3 — 4

警告ベルが鳴らなかったため、セキュリティ チームとしては、これがゼロデイ攻撃であると疑っていますが、それをどのように確認しますか？

- ✗ すべてのユーザーをシステムからログオフする
- ✓ ログから異常な認証動作の主なものを特定する
- ✗ 他社の友人に電話して、同じ問題が発生しているかどうかを確認する
- ✓ 他のセキュリティ異常アクティビティとの相関関係を調べる

異常な認証動作（異常なログイン時間、認証情報の再利用、非定型デバイスからのアクセスなど）を特定し、それをデータ アクセスの異常や権限の昇格などの他の異常なセキュリティ アクティビティと関連付けることで、組織的なゼロデイ攻撃であることを確認できます。

次の質問 →

攻撃タイプ：ゼロデイ

1 — 2：サイバー脅威の検出と対処 — 3 — 4

この脆弱性は未知のものであるため、セキュリティ チームは被害を抑えながら調査を進めなければなりません。これをどのように行いますか？

- [ ] システム全体のすべての認証セッションを無効にする
- [ ] 攻撃のエントリーポイントにすべてのリソースを集中させる
- [ ] 多要素認証 (MFA) ログインのみを強制する
- [ ] 現在の静的ファイアウォールまたは Web アプリケーション ファイアウォール (WAF) ルールに依存する

正解を見る →

攻撃タイプ：ゼロデイ

1 — 2：サイバー脅威の検出と対処 — 3 — 4

この脆弱性は未知のものであるため、セキュリティ チームは被害を抑えながら調査を進めなければなりません。これをどのように行いますか？

- ✓ システム全体のすべての認証セッションを無効にする
- ✗ 攻撃のエントリーポイントにすべてのリソースを集中させる
- ✓ 多要素認証 (MFA) ログインのみを強制する
- ✗ 現在の静的ファイアウォールまたは Web アプリケーション ファイアウォール (WAF) ルールに依存する

これらのアクションを組み合わせることで、セキュリティが強化され、リスクが最小限に抑えられると同時に、攻撃者のアクセスを遮断することで、セキュリティ チームは根本的な脆弱性を調査して解決できます。

次の質問 →

攻撃タイプ：ゼロデイ

1 2 3：サイバー攻撃からのリカバリー 4

Dell のパソコンには、セキュア ブート、トラステッド プラットフォーム モジュール (TPM)、基本入出力システム (BIOS) パスワード保護、SafeBIOS などのテクノロジーが搭載されています。これらは、ゼロデイ攻撃にどのように役立ちますか？

- [ ] アプリケーション プログラミング インターフェイス (API) トークンを盗む認証情報ダンプ攻撃から保護する
- [ ] 物理的なアクセス権を持つ攻撃者がオペレーティング システム (OS) のセキュリティを迂回して、認証トークンを盗むマルウェアをインストールするのを防ぐ
- [ ] 攻撃者が BIOS 設定を操作して OS のセキュリティを弱め、API セッションの乗っ取りにつながるのを防ぐ
- [ ] 上記すべて

正解を見る →

攻撃タイプ：ゼロデイ

1 — 2 — 3：サイバー攻撃からのリカバリー — 4

Dell のパソコンには、セキュア ブート、トラステッド プラットフォーム モジュール (TPM)、基本入出力システム (BIOS) パスワード保護、SafeBIOS などのテクノロジーが搭載されています。これらは、ゼロデイ攻撃にどのように役立ちますか？

- [x] アプリケーション プログラミング インターフェイス (API) トークンを盗む認証情報ダンプ攻撃から保護する
- [x] 物理的なアクセス権を持つ攻撃者がオペレーティング システム (OS) のセキュリティを迂回して、認証トークンを盗むマルウェアをインストールするのを防ぐ
- [x] 攻撃者が BIOS 設定を操作して OS のセキュリティを弱め、API セッションの乗っ取りにつながるのを防ぐ
- [x] 上記すべて

この階層型アプローチは、BIOS、ファームウェア、認証情報、システム構成を対象としたゼロデイ攻撃に包括的な保護で対応します。これらのテクノロジーは、改ざん、不正アクセス、認証情報の盗難を防止することで、攻撃者によって新たな脆弱性が発見された場合でも効果を維持します。

次の質問 →

攻撃タイプ：ゼロデイ

1 2 3 4：全体的なベストプラクティス

ゼロデイ攻撃の発生を防ぐための最善の方法は何ですか？

- [ ] オープンソース ソフトウェアを使用しない
- [ ] ゼロトラスト原則を活用する
- [ ] オペレーティング システム (OS)、ファームウェア、アプリケーション プログラミング インターフェイス (API)、ライブラリー、コンテナなど、すべてをパッチが適用された状態に保つ
- [ ] 会社の周囲に電気ゲートを設置して、攻撃者の侵入を防ぐ

正解を見る →

攻撃タイプ：ゼロデイ

1 2 3 4：全体的なベストプラクティス

ゼロデイ攻撃の発生を防ぐための最善の方法は何ですか？

- ✗ オープンソース ソフトウェアを使用しない
- ✓ ゼロトラスト原則を活用する
- ✗ オペレーティング システム (OS)、ファームウェア、アプリケーション プログラミング インターフェイス (API)、ライブラリー、コンテナなど、すべてをパッチが適用された状態に保つ
- ✗ 会社の周囲に電気ゲートを設置して、攻撃者の侵入を防ぐ

未知の脆弱性やパッチが適用されていないシステムが存在する場合、ゼロトラスト原則は、ユーザーやデバイスからの暗黙的な信頼を排除し、継続的な認証を実施し、必要な情報のみへのアクセスに制限し、攻撃者の動きを封じ込めることで、ゼロデイ攻撃を防ぎ、未確認の脅威による組織のリスクを大幅に軽減します。

ソリューションを見る →

攻撃タイプ：ゼロデイ

まとめ

ゼロデイ攻撃は、ソフトウェアやハードウェアのまだ明らかになっていないセキュリティ脆弱性を、パッチまたは修正が利用可能になる前に悪用します。攻撃者は、時間的に有利となるチャンスを利用し、脆弱性が検出され対処される前に、往々にして広範囲のシステム停止を引き起こします。

Dell は、ゼロトラストの制御、ネットワーク セグメンテーション、迅速な封じ込め、ユーザー教育を通じて、ゼロデイ攻撃に対処し、新たな脅威に対する防御をさらに強化します。

高度なサイバー レジリエンス戦略の詳細をご覧になり、ゼロデイ攻撃から組織を保護するために Dell がどのように支援できるかをご確認ください。

ゼロデイ攻撃の概要を見る →

⌂ シナリオに戻る

信頼できるワークスペースと信頼できるインフラストラクチャ ›

エンドポイントとインフラストラクチャを保護します。Dell は、SafeBIOS、SafeID、SafeData などの保護機能と、多要素認証 (MFA) やロールベースのアクセス制御 (RBAC) などのゼロトラスト フレームワークを組み合わせることで、多層防御によりパスの悪用を制限し、ハードウェア認証を確実にします。

PowerEdge サーバー ›

セキュア ブート、シリコン ルート オブ トラスト、SmartFabric ネットワーク セグメンテーションを使用することで、横方向の移動が制限され、信頼できるコードのみがインフラストラクチャ上で実行されるようになります。

セキュリティ パートナー ›

高度な Threat Intelligence、Managed Detection and Response (MDR)、Extended Detection and Response (XDR)、きめ細かなアクセス制御を使用して、ゼロデイ攻撃が拡散する前に検出、追跡、封じ込めができます。

PowerProtect ポートフォリオ ›

不変的なバックアップ、隔離された Cyber Recovery ヴォールト、AI 主導の CyberSense 分析を使用して、ゼロデイ侵害後の迅速なリストアとレジリエンスを確保します。

セキュリティとレジリエンスに関するサービス ›

Dell のエキスパートは、パッチ管理からインシデント対応まで、迅速な封じ込め、フォレンジック調査、レジリエンス計画でゼロデイ脅威に対抗します。


DELL Technologies