SOPHOS

ソフォスのインシデント対応計画ガイド

目次

はじめに

本書は、インシデント対応のベストプラクティスを包括的かつ簡潔に解説し、サイバー脅威への対応を技術的および組織的な両方の側面から検討するときの指針となり、効果の高いインシデント対応プロセスを策定するときの一助となることを目的としています。

本書はインシデント対応の入門書として参照いただけますが、サイバーセキュリティの実務経験がない方だけではなく、技術的または組織的な対策について責任がある情報セキュリティのプロフェショナルの方にも有用な内容になっています。本書は、情報セキュリティ管理に関する法規制についての包括的な参考書ではありません。本書は、各企業が策定している情報漏えいインシデント発生時における開示および対応に関するガイドラインと合わせて利用すべき、補足的な資料です。また、保険契約には、本インシデント対応ガイドの推奨事項とは関係しないガイドラインが含まれる場合もありますので、サイバー保険の役割については別途検討する必要があります。

サイバーインシデントに効果的に対応するための準備を進めておくと、信頼できる対応手順を確立でき、迅速に対応し、必要なリソースを割り当てて、リスクを封じ込めることが可能になります。本書の目的は、インシデント管理ライフサイクルの準備段階におけるインシデント対応プロセスの指針となることであり、最終的には、サイバーインシデントを迅速に封じ込めて、企業や組織への財務および運用への影響を最小限に抑えることです。

セキュリティプロフェショナルの方は、本書で説明している概念や調査方法を参照して、自社のインシデント対応計画やプロセスに取り入れてください。このガイドは、最初から最後まで順番に読み進めることもできますが、最も関心のある章を選んで読むこともできます。本書は、サイバーインシデントに対応するための明確な計画を手順を追って解説しているわけではありません。組織のセキュリティチームがインシデント発生時の対策について準備し、効果的なプロセスを確立できるようにすることを意図しています。

本書に記載されているインシデント管理のフェーズは、SANS が推奨するインシデント対応フレームワークに準拠し、6 つの異なるフェーズから構成されます。このフレームワークは、インシデント管理ライフサイクルの各段階に対応しており、セキュリティプロフェショナルがインシデントに効果的に対応するための準備を進めることができるように設計されています。このフレームワークは、プレイブックとして使用されることは意図していません。サイバーインシデントは動的です。フレームワークは一般的なアプローチのための体制を示したものですが、実際のインシデントに対処するときには、セキュリティプロフェショナルやセキュリティに関する高度な知識を有する従業員が、専門的な判断を下さなければならないことが多くあります。

準備

インシデント対応サイクルで最初に取り組まなければならないのは準備段階です。準備段階で費やす活動や努力は、その後の段階における対策の効率性や効果に大きく影響します。準備段階は極めて重要であり、定期的に見直して更新する必要があります。準備段階の要素には、技術的な対策ではないプロセスや手順などの運用的な対策と、システムの強化、テレメトリの収集、トレーニングなどの技術的な対策の両方があります。十分な時間とリソースを準備に充てることで、組織は堅牢でレジリエンスなインシデント対応戦略のための強固な基盤を構築できます。

プロセスと手順

インシデント対応チームが効果的に機能するためには、プロセスと手順を詳細に文書化しておくことが不可欠です。インシデント対応プロセスに参加するように選ばれた従業員に対して、これらのガイドラインを配布して概要を説明することで、対応に関する情報を共有して、ステークホルダー間で目的を一致させることができます。プロセスと手順を明確に定義することで、常に一貫性のあるアプローチが可能となり、コミュニケーションを促進し、サイバーインシデントへの対応を合理的かつ協調的に進めることができます。

インシデント対応計画

効果的なインシデント対応計画を策定しておくと、すべての関係者に必要なガイダンスが提供され、サイバーセキュリティインシデントを管理するための明確な手順を理解できるようになります。インシデント発生時に包括的な対応を確実にできるようにするため、インシデント対応計画には以下の要素を組み込む必要があります。

- **ステークホルダーの定義：**主なステークホルダーを特定し、インシデント対応プロセスにおける役割を割り当てます。これらのステークホルダーには、インシデント対応の責任者、セキュリティインシデントを担当する IT チームメンバー、経営幹部の他に、IT サービスプロバイダー、法執行機関、インシデント対応ベンダーなどの外部関係者などが含まれる場合があります。
- **インシデントの分類と重大度レベル：**潜在的な影響、影響を受けるシステム、脅威のタイプなどの要因に基づいて、インシデントを分類する基準を確立します。重大度レベルを定義し、インシデント対応を進めるときの優先順度とガイドラインを示します。
- **エスカレーション方法：**初動対応の担当者の能力や権限を超えるインシデントが発生した場合の明確なエスカレーション方法を策定します。必要に応じて、より高い権限を有する管理職を関与させる、あるいは外部の専門家を関与させます。
- **コミュニケーション:**従業員、顧客、パートナーが使用するコミュニケーションテンプレートを事前に定義し、インシデント対応テンプレートを整備しておけば、危機が発生したときでも効果的にコミュニケーションを図ることができます。災害復旧計画や事業継続計画で策定している手法を取り入れて、メール、メッセージング、ビデオ会議などのフェイルオーバー (障害発生時のための) コミュニケーションチャネルを評価することを検討してください。
- **アセットインベントリ：**企業が導入しているアセットの最新のインベントリを維持しておき、すべてのハードウェアとソフトウェアを追跡して管理できるようにします。これらのアセット情報は、脅威の拡散、影響、対応を判断する上で極めて重要になります。
- **インシデント対応のタイムライン：**インシデント対応プロセスの各段階のタイムラインを作成し、重要なマイルストーンの期限を示して、迅速かつ組織的に対応できるようにします。
- **インシデント文書とレポート作成：**決定して実行した対策、達成できた成果など、インシデントのあらゆる側面を文書化するプロセスを標準化します。作成されるこれらの文書は、インシデント後の分析に役立ち、規制当局から問い合わせがあった場合にも提出が必要となる場合があります。
- **アフターアクションレビュー (AAR) と継続的改善:**インシデント発生後、対応が有効であったかどうかを評価し、改善すべき領域を特定するために、アフターアクションレビューを実施するプロセスを導入します。このレビューによって得られる知見は、必要に応じてインシデント対応計画を更新し、強化するために使用できます。

実際の対策から得られた知見をインシデント対応計画に組み込むことで、サイバーセキュリティインシデントを効果的かつ効率的に管理して対応する体制を整えることができます。

法的文書

この準備段階では、企業は情報開示に関する法的な責任、インシデント対応に関する規制、および、その他のサイバーセキュリティ関連の課題に対応する必要があります。以下のセクションには、一般的な法的要件を示しますが、それぞれの業界と国によって規制要件は異なりますので、自社の環境を考慮して、包括的な分析を行う必要があります。報告および法令遵守に対する自社の担当者を定めて、ロールを明確に定義して、インシデント対応計画のステークホルダーとして追加します。

- **法規制で求められる情報開示：**企業の業界や国によって、インシデントを開示するように法的に義務付けられていたり、奨励されていたりする場合があります。
  - 最重要インフラに関連する組織
  - 政府機関
  - 株式公開企業
- **データプライバシー：**個人情報保護委員会などの規制当局、データの権利が侵害される可能性のある顧客や個人に責任ある開示を義務付けるデータ保護法を遵守します。
- **データの保持と破棄：**インシデント対応時に収集したデータを、適用される法規制に従って保持、保管、および安全に破棄するためのポリシーおよび手順を確立します。
- **第三者との合意と契約：**ベンダー、サプライヤー、パートナーとの契約書や合意書を確認し、セキュリティ侵害やインシデントが発生した場合における、これらの第三者によるインシデント対応の義務や通知要件を理解しておきます。
- **知的財産 (IP) の保護：**企業秘密、特許、著作権、商標などの知的財産を、サイバーインシデント発生時および発生後に保護するための法的な側面を確認して解決します。
- **国境を跨ぐデータ転送と報告：**複数の国に拠点があり、国際的に活動している企業の場合には、いくつかの司法管轄区を跨いでデータを転送し、報告することになります。その場合には、関連する各国の法的な要件を理解しておきます。
- **従業員の権利と責任:**インシデントの報告義務や機密情報の保護義務など、サイバーセキュリティインシデントが発生したときの、従業員の法的権利と責任についてまとめておきます。
- **サイバー保険契約の文書：**サイバー保険の請求プロセスと要件を理解しておきます。
  - 保険約款を確認しておき、インシデントが補償の対象かどうかを判断します。
  - 社内の保険契約者と連携し、補償内容を十分に理解します。

インシデント対応プレイブック

インシデント対応プレイブックは、特定の脅威が特定された場合に実施する対策について、詳細で段階的なガイドラインを提供するものです。これらのプレイブックは、さまざまな攻撃シナリオの可能性と潜在的な影響を考慮し、リスクベースのアプローチに基づいて作成する必要があります。インシデント対応プレイブックを作成するときには、以下の要素を考慮してください。

- **自社に合ったプレイブックを作成する:**自社の環境、リソース、能力に合わせてプレイブックを作成してください。たとえば、組織の規模、業種、直面している特定のリスクなどを考慮してプレイブックを作成します。
- **特定の脅威とシナリオ：**組織の対策準備が成熟している場合、特定のタイプのマルウェアや標的型攻撃など、特定の脅威に対するプレイブックを策定することが推奨されます。しかし、リソースが限られている企業の場合、さまざまな脅威に対応できるように包括的なプレイブックを策定し、さまざまなシナリオで常に役立てることができるようにするべきです。
- **明確で簡潔な指示：**プレイブックでは、対応プロセスの各ステップについて、明確かつ簡潔に指示されている必要があります。これにより、担当者はインシデント発生時に必要な行動を迅速に理解し、実行できます。
- **役割と責任：**インシデント対応プロセスに関わる各チームメンバーの役割と責任を明確に定義します。これによって、自分に何が求められているかを関係者全員が理解して、効果的に協力できるようになります。
- **コミュニケーションとエスカレーション：**経営幹部への通知や外部ベンダーへの支援要請のタイミングなど、インシデント発生時のコミュニケーションとエスカレーションのガイドラインを追加します。
- **インシデント対応計画との統合：**プレイブックがインシデント対応計画全体と整合が取れており、計画に役立っていることを確認します。これにより、インシデント対応と矛盾がなく、首尾一貫している状態を維持できます。

- **定期的な更新と見直し：**脅威の進化や組織環境の変化があった場合でも、プレイブックが適切で効果的であり続けるように、定期的に見直し、更新する必要があります。

見直しと更新のプロセスをインシデント対応プレイブックに組み込むことで、さまざまなサイバーセキュリティインシデントに効果的に対応し、潜在的な影響を最小限に抑えるための準備を整えることができます。

バックアップ

バックアップは、事業継続性を確保し、インシデント、システム障害、サイバー攻撃によるデータ損失の影響を最小限に抑えるために不可欠です。堅牢なバックアップ戦略を実施するには、定期的にバックアップを作成し、作成したバックアップを復元して利用できるか検証し、データの可用性を最大化するためにさまざまなストレージオプションを選択することが必要です。バックアップ戦略を作成するときには、以下の要素を考慮してください。

- **バックアップの頻度：**データの重要性と許容できるリスクレベルに基づいて、バックアップを作成する適切な頻度を決定します。定期的にバックアップしておくと、データが損失した場合でも、その影響を最小限に抑えることができます。
- **バックアップの種類：**フルバックアップ、増分バックアップ、差分バックアップの手法を組み合わせて活用することで、ストレージ容量を最適化し、効率的なデータ復旧を実現できます。
- **ストレージオプション：**ローカルストレージ、クラウドベースのストレージ、オフラインバックアップなど、さまざまなストレージオプションを選択できます。利用するストレージオプションを検討することで、データの可用性を向上し、単一障害点によるデータ損失のリスクを軽減できます。
- **ビジネスクリティカルデータの優先度設定：**事業継続と主なビジネスプロセスをサポートするために不可欠な、ビジネスクリティカルデータとシステムをバックアップすることに重点を置きます。
- **バックアップの暗号化：**バックアップを暗号化することで、機密データを保護し、保管しているデータや送信しているデータへの不正アクセスを防止できます。
- **バックアップの検証：**バックアップしたデータを適切に利用できることを定期的に検証し、必要なときに正常に復元できるかどうかをテストします。復元プロセスをテストし、バックアップされたデータの完全性を検証するようにしてください。
- **データ保持ポリシー：**法規制やビジネス要件に従って、バックアップの保管と廃棄を管理するためのデータ保持ポリシーを導入します。
- **災害復旧計画：**バックアップ戦略を組織全体の災害復旧計画と統合することで、データが損失した場合でも、協調的かつ効果的な対応が可能になります。

これらの要素をバックアップ戦略に取り入れることで、組織は復旧に対して優れた準備ができるようになります。

システムとネットワークの強化

システムおよびネットワークの強化には、不要な機能、システムへのアクセス、ネットワーク接続を最小限に抑制し、攻撃対象領域を減らすことが含まれます。効果的な強化対策を実施することで、攻撃が成功する可能性を軽減できます。システムおよびネットワークを強化する戦略を策定するときには、以下の点を考慮してください。

パッチの適用

- **パッチ管理プログラム：**自動または半自動のパッチ適用ツールを活用し、ネットワークにあるアセットに対して迅速かつ一貫性のあるパッチ適用を可能にするプログラムを利用します。
- **文書化：**適用したパッチと、除外したケースを記録して管理します。
- **優先順位付け：**リスク分析に基づいてパッチの優先順位を決定し、最も大きな影響を与える可能性のある脆弱性への対策に重点を置きます。

設定

- **セキュリティコンプライアンス監査：**社内および社外の監査を継続的に実施し、セキュリティツールが適切に構成されていることを検証し、設定ミスや必要な機能がオフになっていないか確認します。
- **アプリケーションコントロール：**許可またはブロックするアプリケーションのリストを導入し、ホストでの実行を許可するアプリケーションの数やバージョンを制限することで、許可されていないソフトウェアや脆弱なソフトウェアが悪用されるリスクを低減できます。
- **ネットワークアクセスコントロール：**ネットワークツールを設定し、IP およびポートへアクセスできる対象を必要な内部および外部ホストのみにを制限することで、不正アクセスやデータ流出の可能性を最小限に抑えます。

- **最小特権の原則：**組織のユーザーのアクセス権限を、職務を実施するのに必要な最小限のレベルに制限することで、不正アクセスやデータ漏洩の可能性を低減します。

ネットワークセキュリティ

- **ネットワークセグメンテーション：**セキュリティ侵害による影響を制限し、攻撃者によるネットワークのラテラルムーブメントを困難にするために、ネットワークを小さな独立したセグメントに分割します。
- **ファイアウォールの設定：**不要な送受信トラフィックをすべてブロックするようにファイアウォールを設定し、定期的にルールを見直しおよび更新し、最適なセキュリティ対策を維持します。
- **侵入検知および防御システム (IDPS)：**IDPS を導入してネットワークトラフィックを監視し、悪意のある活動の兆候を見つけ、適切な措置を講じます。

監視とテレメトリ

監視とテレメトリは、組織のセキュリティ環境を向上するのに重要な知見を提供し、潜在的な脅威を早期に発見できるようにするため、効果的にインシデント対応戦略を進めるうえで極めて重要です。自社の環境を理解し、検出と防御レイヤーを適切に導入することで、インシデントに効率的に対応する能力を向上できます。

自社環境

自社環境を理解することは、効果的に監視し、テレメトリを収集するための基礎となります。自社環境を把握するために、以下が必要となります。

- アセットインベントリ：エンドポイント、サーバー、およびセキュリ ティプラットフォームによって保護されている範囲を正確に把握し、最新の記録を維持します。
- ネットワークトポロジー：トラフィックの送受信ポイント、セグメンテーション、コントロールポイントなどのネットワーク環境を明確に把握します。可能であれば、ネットワークトポロジー図を作成して最新の状態で維持してください。

検出と防御レイヤー

包括的なセキュリティ戦略を進めるときには、検出と防御のための多層防御を確立することが不可欠です。以下のテレメトリソースから情報を収集し、協定世界時 (UTC) を標準とするタイムスタンプですべてのソースで一貫性のあるデータを収集します。

- **周辺機器：**ファイアウォール、侵入防御システム（IPS）、侵入検知システム（IDS）、VPN、プロキシ。
- **エンドポイントの保護：**アンチウイルス、次世代アンチウイルス、EDR と XDR。
- **一元的なログ：**セキュリティ情報イベント管理 (SIEM) ツール、Syslog サーバー、クラウドベースのデータストレージ。
- **認証：**多要素認証サービス、およびアイデンティティとアクセス管理 (IAM) サービス。
- **脅威インテリジェンス：**データ相関と企業を監視する戦術的インテリジェンスにより、外部へのエクスポージャを警告します。

監視ツールと手法

インシデントを効率的に特定して対応するために、適切な監視ツールと手法を導入しなければなりません。以下のアプローチを取り入れることを検討してください。

- **継続的な監視：**リアルタイム監視と定期的な監視を組み合わせて導入し、自社環境を常時かつ包括的に把握します。
- **異常検出：**高度な分析と機械学習アルゴリズムを活用して、潜在的な脅威を示す異常なパターンや行動を特定します。
- **ログの相関：**複数のソースから取得したログデータを集約および相関して、攻撃の兆候となるパターンや傾向を特定します。
- **警告の優先順位付け：**重要度、潜在的な影響、脅威レベルなどの要因に基づいてアラートに優先順位を付けるプロセスを策定します。

自社環境の状況を正確に把握し、検出と防御のための多層防御を確立し、効果的な監視ツールと監視手法を導入することで、セキュリティインシデントを迅速かつ効率的に特定し、組織のインシデントへの対応力を大幅に向上できます。

コミュニケーション

効果的なコミュニケーション戦略を立てておくと、すべてのステークホルダー間で調整と協力を迅速に行うことができるようになるため、インシデント対応において極めて重要な役割を果たします。本セクションでは、法的要件を考慮しながら、インシデント対応における社内と社外とのコミュニケーションの重要な検討事項を概説します。

社内コミュニケーション

- **コミュニケーション計画：**エスカレーションパス、コミュニケーションチャネル、主要な連絡先について詳述した包括的なコミュニケーション計画を確立します。この計画は、インシデント発生時に確実に効果を発揮するように、定期的に見直して更新する必要があります。
- **インシデント対応チーム：**インシデント対応チーム (IRT) を結成し、対応の調整を担当するチームのリーダーを指名します。チームメンバーがそれぞれの役割と責任を理解し、インシデントが発生した場合でも常にオープンにコミュニケーションできる関係性を維持します。
- **安全なチャネル：**機密情報への不正アクセスを防ぐため、安全で信頼できる通信チャネルを活用します。メッセージを暗号化して送信するアプリ、安全なメール、または専用のコミュニケーションプラットフォームの導入を検討してください。
- **対応テンプレート：**さまざまなシナリオに対応する定義済みのインシデント対応テンプレートのライブラリを作成しておき、迅速で一貫性のあるコミュニケーションを可能にします。これらのテンプレートは、簡単にアクセスでき、カスタマイズ可能で、組織のコミュニケーションガイドラインを遵守している必要があります。
- **ステークホルダーへの最新情報の提供：**インシデント管理プロセスを通じて、状況報告、実施された対策、予想される結果など、ステークホルダーに最新情報を定期的に提供します。最新情報を提供することで、インシデント処理に対する信頼と信用を維持できます。

社外コミュニケーション

- **インシデント通知に関する戦略：**顧客、ベンダー、パートナー、および法執行機関に対して、セキュリティ侵害やこれらの組織に影響を及ぼす可能性のあるインシデントが発生した場合の通知戦略を策定します。この戦略では、通告の基準、適切な通知チャネル、指定された連絡担当者を定める必要があります。
- **法規制の遵守：**社外とのコミュニケーションが、データ保護法、責任ある情報開示に関するガイドライン、業界固有の規制など、法規制要件を遵守していることを確認します。法律顧問に相談し、コミュニケーションが関連するすべての義務を遵守していることを確認します。
- **広報担当者の指名：**広報担当者または広報チームを指名し、報道機関からの問い合わせに対応したり、会社からの正規の発表を行ったりするときに、一貫性のある正確なメッセージを伝えます。この担当者やチームは、危機発生時のコミュニケーションとメディア対応についてトレーニングを受けている必要があります。
- **社外コミュニケーションの準備：**さまざまなインシデントシナリオに対応したコミュニケーションテンプレートを準備し、外部関係者に迅速かつ明確にインシデントを通知できるようにします。顧客、パートナー、規制当局など、さまざまなステークホルダーのニーズに対応できるように、これらのテンプレートを調整します。
- **他部門との協力：**法務、広報、その他の関連部門と緊密に連携し、社外とのコミュニケーションが規制に準拠しており、会社の評判を保護し、影響を受ける関係者に正確な情報を常に提供できるようにします。

このようなコミュニケーション戦略を策定して実施すれば、サイバーセキュリティインシデントに対する協調的かつ効果的な対応が可能となり、最終的にインシデントに対する組織の対応に対する信頼と信用を維持できます。

従業員のセキュリティ意識向上とトレーニング

サイバーセキュリティの脅威とベストプラクティスについて従業員を教育することは、組織全体のセキュリティ体制を向上する上で極めて重要です。このセクションでは、セキュリティ意識向上への取り組み、トレーニングの内容と頻度、模擬的なインシデントと演習など、包括的なセキュリティ意識向上とトレーニングプログラムの主要な構成要素について説明します。

セキュリティ意識向上プログラム

- **プログラムの目的：**組織の資産と情報を保護するために従業員が習得すべき知識と行動習慣に焦点を当てながら、セキュリティ意識向上プログラムの明確な目標を設定します。
- **対象者に合わせたトレーニング：**各役職、部署の責任、機密情報へのアクセス状況を考慮しながら、さまざまな役割や部署に合ったトレーニング資料を作成します。

- **継続的なアップデート：**脅威は進化を続けています。最新の状況を反映し、最新のトレンドとベストプラクティスを取り入れて、セキュリティ意識向上プログラムを定期的に更新します。
- **指標と評価：**従業員の取り組み、トレーニングの修了率、セキュリティ行動の改善などに関する主要業績評価指標 (KPI) を使用して、セキュリティ意識向上プログラムの有効性を追跡および測定します。

トレーニングのコンテンツと頻度

- **コンテンツ開発：**パスワード管理、フィッシング攻撃の理解、ソーシャルエンジニアリング、安全なインターネット閲覧など、幅広いトピックを網羅し、受講していて楽しく、本当に役立つトレーニングコンテンツを作成します。
- **トレーニングの実施:**オンラインコース、対面式のワークショップ、インタラクティブウェビナーなど、さまざまなトレーニング形式を提供し、従業員が参加しやすい多様な学習方法やスケジュールに対応できるようにします。
- **頻度：**1 年を通じてトレーニングセッションを定期的に実施します。少なくとも四半期に 1 回の頻度で実施することを推奨します。さらに、特定のインシデントや新たな脅威に対応するためのトレーニングセッションを適宜実施してください。
- **継続的な学習：**サイバーセキュリティの知識を広げるのに役立つ記事、ビデオ、ポッドキャストなどのリソースを従業員が利用できるようにして、継続的に学習する文化を醸成します。

模擬インシデントと模擬演習

- **現実的なシナリオ：**従業員が日常業務で遭遇する可能性のある現実的なシナリオに基づいて、模擬インシデントや模擬演習を設計します。このような現実的なシナリオを用いることで、従業員がセキュリティ侵害による潜在的な影響について理解を深め、対応スキルを訓練できるようになります。
- **部門横断的なコラボレーション：**複数の部門に模擬演習に参加してもらい、専門分野が異なるチームが連携および協力してコミュニケーションを図るようにします。
- **評価とフィードバック：**模擬インシデントや模擬演習を実施するときには、従業員のパフォーマンスを徹底的に評価し、建設的なフィードバックを提供し、改善点を特定してください。
- **学びを得る:**模擬演習から学んだ教訓を組織全体で共有し、重要な概念やベストプラクティスを強化します。

強固なセキュリティ意識向上プログラムやトレーニングプログラムを実施することで、企業はサイバーセキュリティの脅威を特定し、脅威に対応するために必要な知識とスキルを従業員に習得させ、最終的に攻撃が成功するリスクを低減できます。

インシデント対応チーム

サイバーセキュリティインシデントが発生したときに迅速かつ協調的な対応するために、効果的なインシデント対応チームが不可欠になります。このセクションでは、インシデント対応における役割と責任、チーム構成、外部からの支援と専門知識の重要性について説明します。

役割と責任

- **インシデント対応マネージャー：**インシデント対応プロセスを監督し、チームによる活動を調整し、チームメンバー間および外部のステークホルダーと効果的にコミュニケーションできるようにします。
- **セキュリティアナリスト：**セキュリティインシデントを調査および分析し、インシデントの根本原因、影響の範囲や大きさを特定するための技術的な専門知識を提供します。
- **フォレンジックアナリスト：**証拠の収集、分析、保全などのデジタルフォレンジック業務を行い、調査や法的手続きを支援します。
- **IT 運用部門：**システムインフラを管理し、将来のインシデントを防止するために必要な変更を実施し、脅威の封じ込め、根絶、復旧を支援します。
- **法務とコンプライアンス部門：**インシデント対応に関連する法規制の要件についてガイダンスを提供し、情報を適切に開示および報告できるようにします。
- **広報とコミュニケーション：**社内外のコミュニケーションを管理し、従業員、顧客、パートナー、規制当局など、影響を受ける関係者への適切なメッセージを作成します。

インシデント対応チームの構成

- **部門横断的なチーム構成：**インシデント対応では多くの専門分野の知識が求められます。そのため、IT、セキュリティ、法務、人事、コミュニケーションなど、さまざまな部門の代表者を加えた多様なチームを編成して対応できるようにします。
- **スキルと専門知識：**チームメンバーがそれぞれの役割を遂行するために必要なスキルと専門知識を有していることを確認し、継続的なトレーニングと能力開発の機会を提供します。
- **24 時間対応とシフトのローテーション：**24 時間 365 日対応可能なチームを設立し、オンコールのローテーションや専用シフトを使用して、継続的に人員を配置します。

外部ベンダーからのサポートと専門知識

- **サードパーティーベンダー：**サイバーセキュリティのコンサルタントやマネージドセキュリティサービスプロバイダ (MSSP) などの外部の専門家を活用すれば、社内で不足している能力を補完できます。また、これらの外部のベンダーは、デジタルフォレンジックや脅威インテリジェンスなどの分野でも専門的な知識も提供します。
- **法律顧問：**サイバーセキュリティとデータプライバシーに関する法律に精通した外部の法律顧問と契約し、コンプライアンスと開示要件についての社内の方針を確定し、セキュリティインシデントに関連する法的手続を代行してもらいます。
- **法執行機関および規制当局：**セキュリティインシデントに関連する法執行機関や規制当局との関係を構築し、インシデントを調査するときに協力し合い情報を共有できるようにします。
- **セキュリティ業界との連携：**サイバーセキュリティ専門のフォーラムやこれらの情報共有グループに参加しておき、他の組織と脅威情報やベストプラクティスを交換し、新たな脅威やトレンドを常に把握するように努めてください。

インシデント対応チームをバランスよく編成し、外部ベンダーのサポートや専門知識を活用すれば、サイバーセキュリティインシデントを適切に管理し、潜在的な影響を最小限に抑えることができます。

特定

特定のフェーズは、ネットワークやシステムに攻撃者が存在することを検出するために極めて重要です。脅威が侵入してから特定するまでの時間を最短にするためには、ネットワークテレメトリを継続的に監視しなければなりません。チームが迅速に対応するほど、データ、システム、ネットワークの機密性、完全性、可用性への影響は小さくなります。MDR (Managed Detection and Response) ソリューションでは、専門家による優れた脅威の検出と応答機能を利用でき、脅威の特定を迅速かつ正確に行うことが可能になります。

脅威を特定するための主なコンポーネント

- **ネットワークとデバイスのテレメトリ：**「テレメトリ」のセクションで説明したように、さまざまなソースを包括的に監視し、そのテレメトリ (監視データ) を収集して分析することは、リアルタイムの脅威検出と対応に不可欠です。MDR ソリューションを実装すれば、このプロセスを強化できます。
- **外部からの通知：**法執行機関やその他の外部の情報ソースと協力して脅威インテリジェンスを収集および分析することで、侵入の可能性を迅速に特定できます。
- **脅威インテリジェンス：**ダークウェブやアンダーグラウンドの Web サイトを監視し、自社の情報が漏洩して販売されていないか確認することで、検出能力をさらに向上できます。
- **ユーザーからの報告：**不審なメールやリンクを報告するようユーザーに促し、重要な脅威の兆候がインシデント対応の担当者に伝わるようにすれば、潜在的な脅威に迅速に対応できます。

以下の基準に基づいてインシデントの重大度レベルを分類する厳格なプロセスを確立する必要があります。

- **精度：**ソース (IPS、FW、ウイルス対策、XDR など) の信頼性を示します。
- **重要性：**影響を受けたシステムの重要性を考慮します。
- **悪質性：**攻撃が疑われる行動を評価します。これにより、これまでに特定されていなかった侵害の発見につながる手がかりが得られる場合があります。
- **インシデントのタイプ：**サイバーキルチェーンや MITRE ATT&CK などのフレームワークを使用してインシデントを分類します。
- **タイムスタンプ：**UTC、NTP、および共通の標準を使用して一貫したタイムスタンプを確保し、データを正規化します。

インシデントのタイプ

NIST は、インシデントについて以下の 2 つのカテゴリを定義しています。

- **前兆 (Precursor)：**オープンポートやソフトウェアの脆弱性を特定することを目的としたスキャンなど、サイバー攻撃者による偵察の兆候を検出します。MDR ソリューションは、このような兆候の検出で特に有用です。リモートコードの脆弱性を攻撃する既知のエクスプロイトが組織のインフラに存在していないかを特定します。
- **痕跡 (Indicator)：**マルウェアのアラート、ファイルや Active Directory の変更、RDP 経由のログインのような通常とは異なるユーザーの行動など、さまざまなインシデントの痕跡タイプを特定し、インシデント対応を適切に開始します。MDR は、このようなインシデントの検出と対応において、強力に支援することができます。

包括的な監視戦略を導入し、外部ソースの通知や脅威インテリジェンスを活用し、不審な兆候を特定したときには報告するようにユーザーに奨励し、明確な基準でインシデントを分類できれば、全社的なセキュリティ対策を強化できます。さらに、MDR ソリューションを取り入れると、インシデントの検出と対応を効果的に行うためのさらなるサポートを利用できます。特定フェーズを強化できれば、セキュリティインシデントの影響を軽減できるだけでなく、プロアクティブなセキュリティ文化を醸成でき、最終的には事業継続を可能にし、貴重な資産を保護できます。

攻撃が疑われるファイル、ディレクトリ、プロセス、および常駐化

攻撃が疑われるファイル、ディレクトリ、プロセス、および常駐化のメカニズムを理解して特定することは、インシデントの早期発見に役立ちます。

- **ファイルとディレクトリ：**通常とは異なる、あるいは予期しないファイルやディレクトリがある場合、セキュリティインシデントが発生している可能性があります。以下のような例はインシデントの兆候である可能性があります。
  - 通常とは異なる拡張子や名前のファイルがある。
  - 予期せぬ場所にファイルが存在する。
  - アクセスすべきでない機密データがディレクトリに含まれている。
- **プロセス：**不審なプロセスは、システムで悪意ある活動が行われている兆候を示す場合があります。以下のような例はインシデントの兆候である可能性があります。

- CPU やメモリの使用量が多いプロセス。
- 予期しない場所から実行されているプロセス。
- 機密データやリソースへのアクセスを試みるプロセス。

- **常駐化：**攻撃者は、侵害したシステムに継続的にアクセスするために、常駐化のためのメカニズムを確立することも多くあります。常駐化の手法の例を以下に示します。
  - 悪意のあるスクリプトを定期的に実行するタスクや cron ジョブ。
  - 削除や再起動時に自身を再インストールするマルウェア。
  - 悪意のあるプロセスを起動するレジストリキーやスタートアップ項目。
- **認証情報へのアクセス：**認証情報へ不正にアクセスされると、システムや機密データがさらに侵害される恐れがあります。認証情報へのアクセスには、以下のような例があります。
  - ユーザーアカウントへのブルートフォース攻撃。
  - 従業員の認証情報を狙ったフィッシングキャンペーン。
  - 侵害されたシステムからのクレデンシャルダンピング。
- **攻撃の足掛かりとアクセス権限の追加：**攻撃者は、アクセス権限やコントロールを拡大するために、組織の環境でさらなる足がかりを構築するケースがあります。攻撃者は以下のような攻撃を行う場合があります。
  - 権限を昇格しユーザーアカウントを侵害する。
  - システムまたはアプリケーションに存在するパッチ未適用の脆弱性を攻撃する。
  - ネットワークでのラテラルムーブメントを行って別のリソースにアクセスする。

これらのタイプのインシデントとその事例を認識することで、潜在的な脅威を効果的に特定し、適切に対応できるようになります。セキュリティインシデントを迅速に検出してその影響を軽減するためには、このようなさまざまなインシデントタイプを認識できることが重要です。

フォレンジック分析

フォレンジック分析は、インシデント対応プロセスの重要な側面の 1 つであり、組織がインシデントの根本原因を特定し、その影響を理解し、追加の調査や法的な手続きで必要となる証拠を収集するのに役立ちます。フォレンジック分析の主要な要素を以下に示します。

フォレンジックツールと手法

インシデント対応を行っているときに、さまざまなフォレンジックツールや手法を利用して、システムやネットワークの分析を支援できます。これらのフォレンジックツールは、データの収集、分析、保存に役立ちます。フォレンジックツールや手法の例を以下に示します。

- 侵害されたシステムの状態を保存するために使用するディスクイメージ作成とクローン作成ツール。
- 揮発性データを調査し悪意のあるプロセスを特定するメモリ分析ツール。
- ネットワークアクティビティを調査し、セキュリティ侵害の潜在的な兆候を特定するネットワークトラフィック解析ツール。
- システムおよびアプリケーションのログをレビューし、不審な活動の兆候を確認するログ分析ツール。

証拠の収集と保全

フォレンジック分析では、データの完全性を確保し、法的手続きで使用する証拠を維持するために、証拠の適切な収集と保全が不可欠となります。証拠の収集と保全のベストプラクティスの一部を以下に示します。

- 使用したツールや手法など、証拠を収集するプロセスのすべてのステップを文書化します。
- インシデントに関連するイベントの詳細なタイムラインを作成します。
- 書き込み防止装置やその他のフォレンジックツールを使用して、データの収集中に証拠が改ざんされるのを防止します。
- 収集したデータは、不正開封防止機能付きのコンテナまたは暗号化された記憶媒体で保護します。
- 収集したデータは、必ず安全かつ管理された環境に保存します。

証拠保全

適切な証拠保全は、証拠の完全性を保ち、法的手続きで証拠として採用されるようにするために極めて重要です。証拠保全とは、調査全体を通じて、証拠の取り扱い、保管、移動を文書化して、追跡することです。適切な証拠保全のために、組織は以下を実行する必要があります。

- 証拠を扱うすべてのユーザーの氏名、役割、連絡先などの詳細を記録します。
- 証拠を転送または処理した日時および場所を記録します。
- コピー、分析、保管など、証拠に対して実行されたアクションの記録を保管します。
- 必要に応じて、不正開封防止シールや暗号化されたストレージを使用し、証拠が常に安全に保管・移動されるようにします。

フォレンジック分析をインシデント対応プロセスに組み込むことで、組織はセキュリティインシデントの性質と範囲に関する貴重な知見を得ることができます。また、重要な証拠を収集して、さらに詳細な調査を進めることや、法的な手続きに役立てることもできます。徹底的かつ効果的な分析を行うためには、適切なフォレンジックツールとその活用方法を理解して、取り入れることが不可欠です。

データ流出

データ流出とは、組織のシステムやネットワークから通常は攻撃者が管理する外部のシステムに機密情報やデータを不正に転送することを意味します。データ流出を検出し防止することは、セキュリティ侵害の影響を最小限に抑え、貴重なアセットを保護するために極めて重要です。データ流出に効果的に対処するために、組織は以下の対策を考慮する必要があります。

- **監視とアラート発行：**大容量のファイルを転送している、不審な IP アドレスと通信している、ログインに何度も失敗しているなど、異常なデータ転送やネットワークトラフィックパターンを検出できる包括的な監視システムを導入します。データが流出している可能性がある場合に、担当者に通知できるように、適切なアラート発行の仕組みが導入されていることを確認します。
- **データ流出防止 (DLP) ソリューション：**DLP ソリューションを導入して、機密データが組織のネットワーク外に転送されるのを特定して防止します。DLP ソリューションは、定義したポリシーとルールに基づいて、機密情報の不正な転送を検出し防止するのに役立ちます。
- **暗号化：**機密データを保管時と移動時の両方で暗号化し、流出した場合でも攻撃者がデータを利用できないようにします。
- **従業員のトレーニングと意識向上：**データ流出のリスクと、機密情報を安全でないチャネルや権限のない個人と共有しないなど、セキュリティポリシーを遵守することの重要性について従業員を教育します。

検証と優先順位付け

潜在的なセキュリティインシデントが特定されたら、そのインシデントを検証し、重大性と組織への潜在的な影響に基づいて対応の優先順位を決定することが重要です。検証と優先順位付けには、以下の操作を実行します。

- **インシデントの検証：**特定したインシデントが誤検出ではなく、本物のセキュリティ侵害であるかどうかを確認します。利用可能なデータを分析し、既知の脅威インテリジェンスと相関し、イベントのコンテキスト情報を確認することで、この検証を行います。
- **インシデントの優先順位付け：**インシデントが組織のアセット、業務、評判に及ぼす潜在的な影響を評価します。インシデントに関係するデータやシステムの種類、侵害の程度、インシデントの潜在的な影響などの要因を考慮します。
- **重要度レベル：**優先度の評価に基づいて、インシデントに重大度レベルを割り当てます。重大度レベルは、低、中、高、重大など、あらかじめ定義された尺度を使用して決定することができます。インシデント対応チームは、このレベルを参照して、対応に必要となるリソースと緊急性を決定できます。
- **対応計画：**重大度レベルとインシデントの性質に基づいて、策定したインシデント対応プレイブックから適切な対応計画を選択します。この計画には、インシデントの封じ込め、調査、修復に必要な手順、および必要な連絡や報告手順が分かりやすく記載されている必要があります。

セキュリティインシデントを効果的に特定し、その真偽を検証し、優先順位を付けることができれば、リソースを効率的に割り当て、最も重要なインシデントに対応を集中させて、組織全体への影響を最小限に抑えることができます。

封じ込め

封じ込めの主な目的は、侵害が確認された、あるいは侵害が疑われるシステムを隔離して、被害の影響を軽減することです。このステップは、マルウェアの拡散や継続的なデータ流出など、インシデントの拡大を防止し、システムを保全して、追加の証拠を収集できるようにします。適切な封じ込め戦略は、文書化し、詳細な分析に使用されるセキュリティ侵害の痕跡 (IOC) を収集するなど、詳細な調査を実行するために役立ちます。

短期的な封じ込め

短期的な封じ込めでは、インシデントの影響を抑えるための迅速なアクションを実行します。この作業は、侵害されたマシンを特定した時点で実施され、現在進行中の脅威を封じ込めるということを優先として実行されます。短期的な封じ込め対策の例を、以下に示します。

- **ホストベースの隔離：**Sophos Intercept X Advanced などのセキュリティプラットフォームの機能を使用して、侵害されたホストを隔離します。このときには調査を進めることができるようにホストへの接続は維持します。
- **SHA256 ハッシュのブロック：**Sophos Intercept X Advanced を使用して、SHA256 ハッシュによって悪意のあるファイルをブロックし、その実行を防止します。
- **ネットワークの隔離：**スイッチ、ルーター、ファイアウォールのデータ転送ポリシーを変更し、脅威が特定されたマシンを含むネットワークセグメントが他のマシンと通信し、脅威が拡散するのを阻止します。
- **手動による隔離：**セキュリティ侵害が確認された場合、ネットワークイーサネットケーブルを切断するか、マシンのネットワーク (Wi-Fi) を無効にします。
- **アカウントのリセット：**侵害されたことが判明している、または侵害が疑われるユーザーアカウントをリセットします。

長期的な封じ込め

長期的な封じ込めは、初期調査が終了した後、同じインシデントがネットワーク内の他のマシンやアセットへと広がるのを防止することに重点を置いています。長期的な封じ込め対策の例を、以下に示します。

- 調査によって特定された悪意のある URL やコマンド＆コントロール (C2) サーバーへのネットワーク接続をブロックします。
- 侵害されたドメインアカウントの一時停止し、ドメイン／ローカル管理者アカウントのパスワードのリセットや一時停止を行います。インシデントの全容が把握できない場合には、ドメイン全体のパスワードリセットを実施します。
- マシンの状態に基づいて、デバイスを自動的に隔離する仕組みを実装します。
- 保護されていないマシンや消去されたマシンにセキュリティエージェントをインストールし、可視化と保護を可能にします。

ベストプラクティス

効果的な封じ込めを確実にするために、以下のベストプラクティスを検討してください。

実施すべき対策

- 上記のいずれかの方法でマシンを隔離します。
- 実行した手順を記録し、誰がいつ何をしたのかを記録します。
- 特に訴訟が関係する場合には、インシデント対応計画と封じ込め戦略について検討します。フォレンジックイメージを取得し、サイバー保険に加入することを検討します。
- 脅威をレベルに応じて分類し、重大性の高いインシデントについては経営幹部に通知します。
- 調査に役立つ IOC を決定し、証拠を収集します。
- インシデントの重大性と潜在的な影響に応じて、経営幹部、法務、広報などのステークホルダーとコミュニケーションをとって連携します。

- 攻撃者は、活動が発見されたことに気付くと、損害をさらに与えようとする恐れがあるため、封じ込め中に攻撃者から報復や攻撃のエスカレーションの兆候がないか監視します。
- 誤検出や予期せぬ結果に備えて、封じ込め対策を必要に応じて元に戻せるようにします。
- インシデントを徹底的に分析して根本原因を特定し、その経験から学びセキュリティ対策とインシデント対応プロセスを改善します。

実施すべきではない対策

- セキュリティが侵害されたマシンをシャットダウンする、あるいは再起動すること。
- インシデント対応計画に従わず、インシデントマネージャーに相談せずに、急いで対策すること。
- IOC の収集や調査を完了することなく、すぐにバックアップから復元を行うこと。
- インシデントを公開したり、機密情報を権限のない個人と共有したりすること。これは、攻撃者への警告となり、封じ込めプロセスが妨害されるリスクがあります。
- 封じ込めは、自動化されたツールやプロセスだけに頼るのではなく、専門家の知識と判断に基づいて意思決定を行ってください。
- ダウンタイムや機能が利用できなくなることなど、封じ込めが業務に与える潜在的な影響を考慮しないこと。また、これらの要因については、アクションを実行しない場合のリスクと必ず比較してください。
- 将来のインシデントに備えてインシデント対応計画や手順を更新せず、封じ込めのプロセスから得た学びを無駄にすること。

あらゆるインシデントに対応できる万能型のアプローチは自社にとって最適ではない可能性があります。インシデントのタイプ、ネットワーク環境、アクセシビリティを考慮して、対策を講じる必要があります。封じ込めは進行中の脅威が拡散しないように食い止め、追加の対策を講ずるまでの時間を与えることができますが、通常はインシデント処理の最終的な段階ではありません。攻撃者は検出されたことに気づくと攻撃をエスカレートさせる恐れがあります。そのため、継続的なリスクの増大に警戒を怠らないでください。

根絶

根絶とは、脅威や攻撃者を自社から完全に排除するプロセスです。根絶には多くの場合、複数の段階が含まれます。サイバー攻撃者の活動、システムの変更、マルウェア、ネットワークやマシン上のすべての実行を特定および文書化し、根絶することを目的としています。甚大な影響を及ぼす多くのサイバー攻撃では、複数の足掛かりが作成され、手動でコマンドが実行されるため、脅威のスキャンでは検出できないような活動の痕跡も見つけなければなりません。脅威を根絶するには、潜在的なあらゆる影響を考慮することが重要です。

根絶には、マシンの再構築または再イメージ化と、脅威の除去という 2 つの主要な戦略があります。それぞれの戦略に長所と短所があり、最大限の効果を得るためには、これらの戦略を組み合わせて実施されることも多くあります。

マシンの再構築または再イメージ化

侵害されたアセットから脅威を根絶する最も効率的な方法は、ホストを再構築または再イメージ化することです。この方法では、侵害されていない状態へ確実にロールバックできます。組織が標準のソフトウェアイメージをホストに展開しており、復旧するときにマスターイメージにアクセスできるようにしておけば、このプロセスを簡単に実施できます。マスターイメージは、本番環境への配備前に作成しておき、イメージ自体が侵害されていないことを確認します。

ERP システム、メールサーバー、ファイルサーバーなどの基幹業務で使用している最重要サーバーの場合、データ損失の可能性とその場合に発生するコストが膨大であるため、古いマスターイメージから復元するのは一般的ではありません。マスターイメージの代わりに、クリーンなバックアップファイル (バックアップサーバー、テープ、クラウド、その他のメディアなど) から復元する場合があります。このプロセスでは、バックアップファイルを適切に利用できること、そして、感染していない状態に復元できることを確認する必要があります。再構築と再イメージ化の戦略の効果を最大限に高めるには、特に脆弱性のあるマシンを中心に、ネットワーク全体の IOC と戦術、手法、および手順 (TTP) を調査する必要があります。

脅威の除去

脅威を除去する戦略は、すべてのマルウェアとアーティファクトを特定し、攻撃者による最も重大なシステム変更を特定し、それらを除去するか、侵害される前の状態に戻すことを目的としています。生産システム、産業制御システム、またはデータの損失やダウンタイムによって大きな損害を被るような他の重要なビジネスシステムに使用されているマシンでは、このアプローチが必要になります。

脅威を除去する戦略は、多くの場合、最初に観測された IOC、関連する脅威インテリジェンス、TTP に関する経験に基づいて脅威ハンティングを行う熟達したインシデント対応者がツールを使用して展開します。脅威を除去する戦略によって攻撃を深く理解し、長期的な改善につなげ、将来的にサイバー攻撃のリスクを低減する教訓を得ることが可能になります。

たとえば、攻撃者が既存の脆弱性や設定ミスを悪用してホストを侵害した場合、また、既に侵害しているホストを最終的に攻撃する段階になった場合、この除去の戦略には、ホストが再感染したり、新たな攻撃の媒介となったりするのを防止するために、そのような弱点を解消する処理も含める必要があります。根本原因を分析することで、実際の影響を把握するまでに、攻撃者が行った手順を理解し、ホストの感染源を解消して、今後の攻撃を防止できます。

企業は、引き続き調査結果を文書化し、MITRE ATT&CK のようなフレームワークを使用して、攻撃の構造を明確に示しておくことが推奨されます。この構造化されたアプローチは、インシデントの根本原因を特定するのに役立ち、全社的なセキュリティ対策を改善できます。

復旧

復旧フェーズの目標は、影響を受けたマシンやシステムを段階的なアプローチで通常の運用に戻し、侵害前と同じように組織の機能を完全に回復させることです。復旧の戦略はインシデントによって異なります。数台のマシンを隔離して運用への影響を最小限に抑えるべきインシデントもあれば、ランサムウェアのような大規模な攻撃を受けて、多くのマシンが標的となっており、業務運営に重大な影響が及んでいたり、ビジネスダウンタイムが発生していたりする場合には、全く異なる復旧戦略が必要となる場合もあります。したがって、攻撃に合わせて復旧計画を進める必要があります。

- フィッシングメールによって影響を受けたホストが 1 台であり、そのペイロードがエンドポイントプロテクションエージェントによって検出されクリーンアップされている場合、セキュリティアナリストが調査し、問題をクリーンアップしている間、マシンが確実に隔離され全体的な運用への影響を最小限に抑えることが可能になる場合もあります。
- ネットワーク内でボットネットが早期に検出され、常駐化の仕組みが 2 台のユーザーマシンにインストールされている場合には、ユーザーマシンの隔離と再構築が直ちに行われる場合もあります。この場合、従業員のダウンタイムは発生しますが、会社の業務への全体的な影響は最小限に抑えられる可能性があります。
- ネットワークに数週間滞留しており、根本原因が特定されているネットワーク全体へのランサムウェア攻撃では、エンドポイントやサーバーだけでなく、メール、VPN、Active Directory アカウント、その他のサービスも隔離しなければなりません。この場合、インシデント対応の担当者は、攻撃の足掛かりを特定し、パッチを適用し、マシンを再イメージ化することによって、攻撃を完全に制御するまで、封じ込めの対策を維持する必要があります。代替となる「クリーンな」ネットワークを作成し、脅威の影響を受けているマシンがない状態でネットワークを再構築し、マシンを 1 台ずつ再統合する対策も考えられます。隔離されたマシンを再統合するかどうかを決定する場合、再侵入または再感染のリスクが十分に低いことが前提となります。インシデント対応の担当者は、このリスクを経営陣に伝え、業務とリスクに適したタイムラインとアプローチを判断してもらいます。

慎重なアプローチ

マシンを復旧するときには、最重要システムの細部にまで注意を払わなければなりません。脅威を完全に除去したという過信や、インシデントの作業による疲労もこの作業の妨げになる場合があります。常に警戒を怠ることなく、以下の点にも注意を払ってください。

- データの完全性とシステムの安定性をテストして、影響を受けたマシンをネットワークに再統合するときのシステム全体の状態を確認します。
- 特に、攻撃を繰り返し受ける恐れがある旧バージョンからマシンを復旧した後は、セキュリティの脆弱性にパッチを適用します。
- 各マシンに適切なセキュリティポリシーとコントロールが適用されていることを確認します。
  - セキュリティエージェントは、再統合されるすべてのマシンに展開する必要があります。
  - スキャンで除外する項目は最小限にします。除外する項目、マシン、ユーザーグループは慎重に設定してください。
- 攻撃で特定された IOC の存在と、サイバー攻撃者が残した可能性のある足掛かりをスキャンしてハンティングします。

さらに、インシデント対応の担当者とセキュリティアナリストは、さらなる脅威が活動していないかどうか環境を監視し続け、一般的なサイバー攻撃者の活動をプロアクティブに探索することで、脅威が出現したときに先手を打って特定し、対応しなければなりません。

脅威を除去するフェーズを完了してから、復旧フェーズを実施する必要はありませんが、除去戦略を実施していれば、システムをクリーンな状態に復旧したマシンを本番環境に再統合できますので、これらの作業は連携して実施する必要があります。

インシデント後の検証と教訓

サイバーセキュリティインシデントからの復旧に成功した後は、インシデント後の検証を実施し、教訓を明らかにすることが極めて重要です。このプロセスは、既存のインシデント対応がどれだけ効果的であったかを分析し、改善点を特定し、インシデント対応計画を向上していくために役立ちます。既存の計画を見直して改善することで、将来のインシデントに対しても優れた対応が可能となり、同様のセキュリティ侵害のリスクを最小限に抑えることが可能になります。

インシデント後の検証

インシデント対応の効果の分析

インシデント対応の効果を評価するには、インシデント対応チームが取った対策を検証して、その結果を測定します。以下の点について検証および評価します。

- インシデントの検出、封じ込め、修復に要した時間。
- チームメンバー間および外部関係者 (法執行機関やベンダーなど) とのコミュニケーションと調整作業。
- 封じ込め、根絶、復旧戦略の妥当性。
- 監視と検出ツールが提供する情報の正確性と有用性。

改善できる領域の特定

インシデント対応の効果を分析したら、組織がプロセスと手順を改善できる領域を特定します。改善が可能な一般的な領域を、以下に示します。

- スタッフのトレーニングと意識向上プログラム
- インシデントの検出と監視機能
- インシデント対応計画の更新
- 技術的な管理とセキュリティ対策
- インシデント対応チームの役割と責任
- 外部のステークホルダーとのコミュニケーションとコラボレーション

インシデント対応計画の変更および更新

改善できる領域を特定した後は、インシデント対応計画を実際に変更することが極めて重要です。必ず以下を行ってください。

- 必要に応じて、新たな手順、ガイドライン、技術的な対策を更新および追加して、インシデント対応計画を更新します。
- 従業員、経営幹部、社外のステークホルダーなどのすべての関係者に変更を伝達します。
- 更新された計画を社内に浸透させ、効果的に実行できるように、定期的にトレーニングと演習を実施します。
- 変更の経時的な効果を監視および評価し、必要に応じてさらに調整します。

インシデント発生後に徹底的に検証し、インシデントで得られた教訓を明らかにすることで、サイバーセキュリティ対策を強化し、将来のインシデントに備えることが可能になります。インシデント対応プロセスの策定は継続的な作業であり、定期的に計画を検証して更新することで、サイバー脅威が進化しても、組織はレジリエントであり続けることが可能になります。

学びを得る

インシデントから得られる教訓は、インシデントのタイプとインシデント処理プロセスによって異なります。また、この教訓から改善できる特定の分野がわかる場合もあります。学びを得る段階は重要ですが、「喉元過ぎれば熱さを忘れる」ように、緊急事態が過ぎ去り、通常の運用に戻り、経営幹部の支援も終了すると見過ごされることが多くあります。したがって、学びを得る段階は、復旧段階の直後に行い、インシデントの詳細を理解し、将来のリスクを軽減するための改善策について社内的な合意を得るために、経営幹部に関与させることが重要になります。

一般的なシナリオでは、インシデント報告書を作成し、要旨をまとめて、社内の技術部門以外のステークホルダーと共有して、理解を得るようにします。この報告書は、複数のステークホルダーがコメントを追加したり、編集したりできる共有ファイルにし、技術的な詳細や得られた学びが含まれ、関係者の合意が得られた最終的な報告書として完成させる必要があります。

改善すべき領域は広範に及ぶ場合があります。一般的な改善領域を以下に示しますが、これだけにとどまらないことを理解してください。

推奨されるセキュリティベストプラクティス

- 攻撃者に悪用されるリスクを最小限に抑えるため、企業環境にあるサポートされていないソフトウェア、アプリケーション、ハードウェアの使用を廃止します。
- 組織のニーズに沿ったソフトウェアとハードウェアへの堅牢なパッチ管理プロセスを確立し、定期的にパッチ更新を確実に実施します。
- 企業内のすべてのコンピュータにクラウドベースのエンドポイントプロテクションエージェントをインストールし、悪意のある脅威を検出して無効化します。
- VPN、RDP、その他の認証が必要なサービスには多要素認証 (MFA) を導入し、セキュリティを強化します。
- 中核となるセキュリティコントロールの仕組みを導入し、インターネットにアクセスするサービスを不正アクセスから保護して、インフラを守ります。
- パスワードの複雑さの要件を適用し、パスワードマネージャーを使用し、認証情報を定期的にローテーションすることにより、認証情報の管理を強化する。
- DMARC、DKIM、SPF などのメール認証プロトコルを導入し、フィッシングメールやなりすましメールから従業員を保護します。

ネットワークのセットアップ：

- ネットワークアクセスコントロール (NAC) を導入して、セキュリティレイヤーを追加し、不正なデバイスや悪意のある脅威から組織を防御します。
- VLAN を使用してネットワークをセグメント化し、重要なシステムや機密データを保護し、インターネットに接続するプラットフォームやサービスを DMZ 内に隔離します。

強化：

- IP アドレスなどの地理的条件でアクセスを制限するジオブロッキングをファイアウォールに導入し、不審なネットワークトラフィックを防止します。
- AppLocker などのアプリケーションコントロールソリューションを導入し、許可されていないアプリケーションやファイルが自社環境にインストールされ実行されるのを防止します。
- 不必要なサービス、サポートされていないソフトウェア、セキュリティリスクを引き起こす恐れのあるレガシープロトコルを見直して削除して、ドメインコントローラーを強化します。

プロアクティブな管理とセキュリティ上の予防措置：

- **インフラの監査：**インターネットにアクセスする組織のすべてのインフラのポート設定を定期的に監査し、必要なプロトコルサービスのみが許可されており、ネットワークフローポートが適切に設定されていることを確認します。
  - 例えば、eth0 はインターネットに接続し、eth1 は社内からしかアクセスできないようにします。
- **Web コントロールの監査：**プロキシサーバーや同様の Web トラフィックフロープラットフォームの Web トラフィック設定を定期的に検証します。最小特権の原則に従い、必要な場合はセキュリティコントロールを強化します。デフォルトの拒否またはブロックポリシーを導入します。以下のようなブロックポリシーを定めます。
  - 不必要なリスクをもたらすファイルタイプをブロックします。
  - 分類されていない URL やドメインのデフォルトの分類ポリシーを見直します。
  - 統計データをエクスポートして、異常なパターン、または攻撃が疑われるイベントや悪意のあるイベントが繰り返し発生していないか特定します。
  - セキュリティグループとポリシーが、RBAC (ロールベースのアクセス管理) の原則に沿って更新されていることを確認する。
- **アカウントの監査：**標準のガイドラインに従っておらず承認されていない、ローカル管理者アカウントや同等のアカウントが組織にないかを定期的に監査し、そのようなアカウントを削除する。
- **Windows イベントログ：**Windows イベントログを構成してデータを保存する。例えば、グループポリシーを通じて Windows イベントログのコアサイズを増加したり、サイズ制限に達したときに新しいイベントログを作成したりします。Windows イベントログは、貴重なフォレンジック情報を提供します。
- **インシデント対応計画：**自社のサイバーセキュリティインシデント対応計画を策定し、実施、テスト、維持する。計画は定期的に検証およびテストし、必要に応じて内容を更新して改善する。
- **ハードウェアとソフトウェアのアセット管理：**組織全体でハードウェアとソフトウェアの両方のアセットを管理する。アセット管理ソリューションに優先順位付け／重要度評価の機能を組み込み、価値の高いアセットを迅速に特定します。ハードウェアおよびソフトウェアアセットの最新のインベントリを維持し、潜在的なリスクを特定し、これらのリスクに対処する戦略的な計画を策定します。

- **ネットワークトポロジー：**最新で明確なネットワークトポロジー図を維持し、既存の構成やインフラのタイプを検証するときの参考資料とし、ネットワークの変更や実装に関する戦略的計画を策定するときに利用します。サイバーセキュリティ攻撃を受けた場合、ネットワークトポロジー図は、インシデント対応の担当者が組織のネットワーク構造を把握するのに役立ち、効果的なインシデント対応のアクションを正確かつ迅速に実行できるようになります。

データの完全性

バックアップ：

- さまざまなバックアップソリューションを導入し、バックアップデータを企業環境とは独立したネットワークの場所 / メディアタイプに完全に分離および保管し、適切なセキュリティコントロールの下でアクセスを管理し、バックアップデータを保護します。
  - 3-2-1 ルールを参照し、保管されているバックアップデータを適切に暗号化し、バックアップを二重化する対策を開始します。3-2-1 ルールとは、データのコピーを 3 部作成し、少なくとも 2 種類のメディアにデータを保存し、少なくとも 1 部のデータをオフサイトに保存する手法です。

暗号化：

- コンピュータ、モバイルデバイス、USB ドライブにフルディスク暗号化を導入し、デバイスが紛失や盗難に遭った場合に、不正アクセスからデータを保護します。
- 機密データを優先的に保護しながら、DARE (Data at Rest Encryption：保存データの暗号化) を導入することで、組織が保存しているデータを保護します。例えば、電子証明書を含む暗号化通信交換には最新の TLS (トランスポートレイヤーセキュリティ) のバージョンを使用し、非対応のブラウザータイプが使用される場合にサーバーが暗号スイートをダウングレードするのを防ぐなど、転送中のネットワークデータに適切な暗号化メカニズムが導入されていることを確認します。

セキュリティの投資

セキュリティインシデントから学んだ教訓を活かして、セキュリティ対策を改善するための資金や予算を確保してください。

- 従業員の意識向上とトレーニングに投資します。人間が最初の攻撃ベクトルとなることが多くあります。以下に対する投資を検討してください。
  - 一般的なフィッシングの手法についてエンドユーザーを教育およびテストするフィッシングの意識向上トレーニングまたはソリューション。このトレーニングは社内で定期的に実施します。また、攻撃シミュレーションを自動化して実施し、継続的な演習として組み込み、IT チームは攻撃を受けやすい従業員を把握し、詳細な指導を行うために必要なレポートを提供します。
  - IT セキュリティ、特にセキュリティ分析、脅威ハンティング、インシデント応答に関するスタッフのスキルをアップします。

マネージドセキュリティサービス

- セキュリティ分析、脅威ハンティング、インシデント応答、セキュリティツールを使用する脅威検出エンジニアリングなどを専門とするサイバーセキュリティの専門家を雇用します。サイバーセキュリティのオペレーションセンターを導入すれば、24 時間 365 日脅威を監視して対応できます。
- Sophos MDR (Managed Detection and Response) のようなマネージドのサイバーセキュリティサービスに投資してください。MDR サービスは、スペシャリストのチームが提供する外部委託されたセキュリティ運用であり、お客様のセキュリティチームを強化できます。

ツールへの投資

- Sophos XDR (Extended Detection and Response) は、エンドポイント、サーバー、ファイアウォール、メール、その他の XDR と連携する製品から重要な情報を保存し、クエリーできるようにするソリューションで、脅威の検出と対応のワークフローを合理化します。
- セキュリティ情報およびイベント管理 (SIEM) テクノロジーは、脅威データの一元化されたリポジトリにさまざまなデータソースのイベントや情報を収集して追加して、脅威検出、コンプライアンス、インシデント管理の機能を提供します。

- インシデントから学んだ教訓に基づいて追加の投資を検討し、保護／フィルタリング、検出、監視のギャップを解消して、自社のセキュリティ対策の強化を図ります。このようなツールには、ウイルス対策、侵入防御検知システム (IPS/IDS)、ファイアウォールなどがあります。

これらの一般的な領域の改善に取り組むことで、セキュリティ対策を大幅に強化し、将来のサイバーインシデントから自社を安全に守ることが可能になります。インシデントからの教訓の獲得は継続的な作業であり、定期的にセキュリティ対策を検証して更新することで、サイバー脅威が進化しても、組織はレジリエントであり続けることが可能になります。

インシデントレポート

サイバーセキュリティのインシデントが発生した後には、インシデントの詳細、発見した内容、および改善策をさまざまなステークホルダーに伝えることが不可欠です。インシデントを社内で共有し、規制当局や法執行機関に報告することは、透明性とコンプライアンスを維持し、調査を支援するために極めて重要です。

社内報告

継続的な改善と学びの文化を醸成するために、組織は社内報告のための明確なプロセスを確立する必要があります。このプロセスには以下を追加する必要があります。

- イベントのタイムライン、影響を受けたシステム、および攻撃の性質など、インシデントを文書化します。
- インシデントが組織の業務、財務、および評判に及ぼす評価します。
- インシデントを封じ込め、根絶し、影響を復元するために講じた措置の概要を記録します。
- セキュリティ対策を改善するための教訓と今後の推奨事項を特定します。
- 上級管理職、IT チーム、影響を受ける従業員や部署など、関連するステークホルダーにインシデントレポートを伝達します。

規制当局への報告

法域や業種によっては、サイバーセキュリティインシデントを規制当局に報告することが義務付けられている場合があります。罰金や罰則、組織の評判が低下することを避けるためには、これらの要件を遵守することが不可欠です。規制当局に報告する場合には、以下を行う必要があります。

- インシデントの性質、組織の業種、国に基づいて、インシデントを報告すべき適切な規制当局を理解します。
- 必要な情報や報告の期限など、報告に関連する要件を確認します。
- 規制当局が指定する書式と内容に従って詳細な報告書を作成します。
- 指定された期間内に報告書を提出し、調査および解決プロセスを通じて、規制当局とのオープンなコミュニケーションを維持します。

法執行機関への報告

犯罪行為や重大なサイバー攻撃の場合、法執行機関への報告することも検討しなければなりません。これによって捜査を支援でき、攻撃者の逮捕につながる可能性があります。法執行機関に報告する場合には、以下を行う必要があります。

- 警察、国のサイバー犯罪対策部門、専門機関 (FBI など) など、報告すべき適切な法執行機関を特定します。
- ログ、システムイメージ、ネットワークトラフィックのキャプチャなど、関連する証拠を収集し、適用される法要件に従って証拠を保全します。
- 攻撃の性質、影響を受けたシステムおよびデータ、イベントのタイムライン、攻撃者に関する既知の情報など、インシデントの詳細を記した報告書を作成します。
- 捜査中は法執行機関に協力し、必要に応じて追加情報を提供し、支援します。

インシデント報告に関するこれらのガイドラインに従うことで、透明性を維持し、規制要件を遵守し、サイバー犯罪を撲滅するための幅広い取り組みを支援できます。

まとめ

このインシデント対応計画ガイドは、サイバーセキュリティインシデントに効果的に対応して管理し、影響を復旧するための包括的な枠組みを提供するものです。プロアクティブな管理とセキュリティ対策を実施し、データの完全性を確保し、従業員のトレーニングとセキュリティツールに投資し、簡明な報告手順を確立することで、サイバー脅威に対するレジリエンスを大幅に強化できます。

効果的なインシデント対応計画を策定すれば、サイバー攻撃による損害を最小限に抑えるだけでなく、継続的な改善と学習の文化を醸成するのにも役立ちます。サイバー脅威の状況が進化し続ける中、企業は新たな脅威や脆弱性にも対応できるように、インシデント対応計画を定期的に検証して更新する必要があります。

本ガイドに記載されているガイダンスをできる限り取り入れることで、サイバーセキュリティインシデントを検出、封じ込め、影響を復旧するための体制を整え、貴重なデータとアセットを保護し、規制要件を遵守し、あらゆるモノがつながり合うこの世界で企業の評判を維持できます。

Sophos Incident Response の詳細については、
こちらをクリックしてください。

現在進行中のセキュリティ侵害がありますか？

以下の地域の番号へ連絡すると、いつでもインシデントアドバイザーと話すことができます。

オーストラリア：+61 272084454

オーストリア：+43 73265575520

カナダ：+1 7785897255

フランス：+33 186539880

ドイツ：+49 61171186766

イタリア：+39 0294752897

オランダ：+31 162708600

スウェーデン：+46 858400610

スイス：+41 445152286

英国：+44 1235635329

米国：+1 4087461064

Email：RapidResponse@Sophos.com

ソフォスのインシデントアドバイザーが可能な限り迅速に対応いたします。

2023-07-03 (IRG-MP)

SOPHOS