サイバーセキュリティ チェックリスト

一歩先を行く備えを固めるための 57 のヒント

組織のセキュリティ確保の旅に終着駅はありません

防御の取り組みのどこに重点を置くかは、皆さんの判断に委ねられています。侵害を防ぐことはできないかも知れませんが、発生する前に十分な防御体制を敷くことは可能です。今すぐ対策すれば、攻撃者の格好の標的にならずに済みます。また、万一サイバー攻撃を受けたとしても、ネットワークを介して攻撃が拡散する能力を制限すれば損害を最低限に抑えることができます。脅威の排除、業務の再開、損害の復旧のために組織が行うべきことを、あらかじめ検討しておく必要があります。

以下の推奨事項は、インシデント レスポンスの最新の事案に基づいたもので、弊社の Unit 42 インシデント レスポンス レポート (2022 年版) を元にまとめました。注力する領域を絞り込んでセキュリティ プログラムの回復力を強化できるように、いくつかのセクションに分けて解説しています。

組織のセキュリティを強化する包括的な推奨事項

ID およびアクセス管理 (IAM)

- ウェブ アプリケーションにはシングル サインオン (SSO) プラットフォームを使用します。多要素認証 (MFA) を、使用できる場所には必ず導入します。
- Active Directory を定期的に点検し、新たに作成されたアカウントやメールボックス、身に覚えのないグループ ポリシー オブジェクトなどがないかを確認します。
- 不正アクセスやディレクトリ リスト出力を予防するようにサーバを設定します。強力なアクセス管理を適用します。
- 従業員を解雇する場合、そのアクセス (アクティブなセッション、トークン、アカウント、MFA デバイス、ローテーション認証情報など) をただちに無効化したうえで、適切に無効化されたことを検証します。調査が必要になった場合に備えて、離職者のシステムやデータは確実に保管しておく必要があります。
- 特権アカウントは、業務上妥当な必要性が認められる場合、またはユーザーが業務を遂行するために必要とする場合に限って使用します。その際、ローカル管理者アカウントのパスワードを再利用してはなりません。
- 管理者用インターフェイスやデバッグ ツールへのアクセス権は、これらを必要とする職務の担当者を除いて無効化します。

最も標的とされた 7 つの業界は、金融、専門サービス、法律サービス、製造、医療、ハイテク、および流通業 (卸売と小売) でした。

リスク、脆弱性、パッチ管理

- 組織にとって不可欠かつ最も貴重な資産を特定します。その際、重要資産の棚卸しを行う必要があります。最も価値の高い標的が組織内のどこにあるのか、それらの保護を強化する必要があるのかなどを見極めるためです。
- オープン ソース コードを実装する場合、公開された脆弱性の有無を吟味し、入念な審査とパッチ適用を経たコードのみを使用します。
- ウェブ アプリケーション / コードの定期レビューと、すべての公開インフラストラクチャに対する年 1 回の侵入テストを実施して脆弱性の有無を確認し、軽減のための推奨手順を実行します。
- ベストプラクティスに基づいて開発環境のセキュリティを設定します。
- 設定チェックを含む定期スキャンを実行し、設定ミスを検出するシステム監査を定期的に実施します。
- 設定変更に対して審査と承認を必要とする変更管理手順を実装します。
- オペレーティング システムとオンプレミス アプリケーションのパッチ管理は不可欠です。APT 攻撃者は、脆弱性が見つかると即座に悪用に向けた行動を開始します。新たに公開された脆弱性は、デュー デリジェンスが許す範囲で、できる限り迅速に対策します。

データとソフトウェアのセキュリティ

- 機密データの保管場所を把握し、そのデータを保護するために厳密なアクセス管理を実装します。アクセスを定期的に監視、監査します。機密データへのアクセスは、組織内およびサードパーティ内でそれらを必要とするユーザーに限ります。
- ノート PC とリムーバブル デバイスについてはディスク全体を暗号化します。紛失または盗まれたデバイスを無効化する、非常時対応計画を策定します。
- モバイル デバイスの位置特定およびデータのリモート消去 (または、そのいずれか一方) の機能を備えた、モバイル デバイス管理アプリケーションを実装し、使用します。
- データの分類とタグ付け、機密情報または企業が特定したその他の関連情報が組織から漏洩した場合のアラート発報を担当する DLP プログラムを確立します。

脅威の検出とレスポンス

- 認証情報の侵害検出サービスや攻撃対象領域の管理ソリューションの導入を検討します。脆弱なシステムや侵害の可能性の追跡管理が容易になります。
- EDR または XDR ソリューションを活用するとともに、ネットワーク全体の完全な可視性を確保するために、この技術の利用方法をセキュリティ運用チームが十分に理解していることを確認します。
- インシデントに対するレスポンスと修復の計画を策定します。最大限の努力を払ってもインシデントは発生する可能性があるため、迅速な対策を確実に講じることができるように、テスト済みの包括的な計画を作成します。サイバー保険に加入している場合 (推奨します)、契約に関わる重要な手続きや連絡先が計画に含まれていることを確認します。

その他のヒント

- ログ保存リポジトリを維持し、異常な行動パターンがないか定期的にすべてのログとログイン試行を点検します。ログが、法律または規制の要件を満たせるように、適切な期間保存されていることを確認します。Unit 42 のコンサルタントは 1 年以上を推奨していますが、不可能な場合は少なくとも 90 日間は保存してください。

- SIEM (セキュリティ情報とイベント管理) などのログ集約システムを活用し、ログの保存性、整合性、可用性を高めます。
- 請負業者を含むすべてのユーザーに対してセキュリティ意識向上定期トレーニングを年 1 回実施します。トレーニングのカリキュラムに独自の目標や目的を設定できる、信頼できるトレーニング プラットフォームの利用を検討してください。
- フラット ネットワークの利用を避けます。ネットワークとアクティブ ディレクトリを分離し、機密データをセグメント化し、セキュアな仮想ローカル エリア ネットワーク (VLAN) を活用します。
- 多層防御のアプローチに従い、ウェブ アプリケーション スタックの階層ごとに保護対策を実装します。これには、ウェブ アプリケーションのファイアウォール、オペレーティング システムの強化、アプリケーション入力管理、ファイル整合性監視のほか、データベースへのアクセスや業界標準の暗号化に最低権限のユーザー アカウントを使用することなどが含まれます。
- 従業員がルールに従って業務を遂行できる環境を提供します。単に特定の経路をブロックしただけでは、管理者が見逃しがちな巧妙な回避策を講じられます。
- 組織名の一般的なスペルミスや変形例を含むドメインの購入を検討します。攻撃者が、組織になりすますことを困難にします。

侵入の 77% が 3 種類の初期アクセス経路から発生していると推定されています。それらの経路は、フィッシング、既知のソフトウェア脆弱性、ブルートフォース認証情報攻撃 (主にリモート デスクトップ プロトコル (RDP) が対象) です。

フィッシング攻撃防御のための推奨事項

- ☐ 「セキュリティ意識の高い企業文化」を醸成します。企業のリーダーがサイバーセキュリティの重要性を認識し、より充実したサイバー トレーニング プログラムを支持、促進し、セキュリティを強調したメッセージを発信していくことが不可欠です。
- ☐ 組織と従業員の役割に合わせてカリキュラムをカスタマイズでき、攻撃者の手法の持つ急速に進化するという特徴に配慮した、信頼できるトレーニング ベンダーまたはプラットフォームを利用します。
- ☐ ユーザーが、フィッシングが疑われるメールの受信を報告しやすく、そうした報告が迅速に確認され対策が講じられるような環境を整備します。
- ☐ 外部の送信者からのメールの添付ファイルに対して、ユーザーに視覚的に注意を促します。会社のドメインと紛らわしい、偽装されたドメインを識別するのに役立つ場合があります。
- ☐ フィッシングおよびスピア フィッシングはもちろん、さらに広範な脅威にも対応した総合的なトレーニングを開発します。その他のソーシャル エンジニアリングの懸念にも配慮してください。物理的なセキュリティ、デバイス紛失に対する業界のベストプラクティス、内部関係者による脅威の兆候などです。
- ☐ 社内での役割と、その役割固有の狙われ方に応じたグループごとに、ウェブベースのモジュールをカスタマイズします。これによって従業員は自分に対して使われる可能性がある戦術をより的確に見極め、回避できます。
- ☐ 全社トレーニングを毎年実施します。さらに、年度半ばに全従業員に対して、高度な手法などの特定領域を重点化した「復習」の機会を与えます。
- ☐ 目標、目標達成のためのルール、表彰、褒賞、フィードバックの仕組み、リーダーボードなどを設定して、セキュリティ トレーニングをゲーム形式にすると従業員の参画意識を高められます。部門間で競争させてもいいでしょう。
- ☐ フィッシング テストのトップ スコアを注視していれば、組織のニーズに応じてフィッシングの内容や難度を調整できます。
- ☐ 機密情報は、電子メールではなく、ロールベースのアクセス管理機能を備えたファイル共有で保存することを奨励します。

- ☐ 添付ファイルとメッセージの内容をスキャンするだけでなく、送信者の評判も評価する電子メール セキュリティ ソリューションを活用します。
- ☐ SPF (Sender Policy Framework) などの、対偽装手法や電子メール認証手法を使用します。
- ☐ 通常業務に必要のない地域であれば、その地域に基づくアカウントのログインを阻止することを検討します。
- ☐ 高度なフィッシング キャンペーンを検出、阻止する、高度なフィッシング防御 / 機械学習ソリューションまたは他のサードパーティ ソリューションを導入します。フィッシングに対するレスポンス作業を自動化して、必要な人手による操作を減らすことを検討します。

組織のシステムを最新の状態に保つパッチ適用に関する推奨事項

- ☐ 分散化された組織の全体を対象に、すべての IT 資産 (ストレージ、スイッチ、ノート PC など) を棚卸しします。自動化されたディスカバリ ツールを使用し、管理すべき対象を明確に把握します。
- ☐ パッチ適用の必要性に優先順位を設定します。各脆弱性のリスク レベル (高、中、低) と、ビジネス上の優先度を、組織のリスクに対する許容度に応じて判断します。
- ☐ パッチを定期的に適用するスケジュールを策定します。パッチ適用の頻度を最低でも月 1 回として、高優先度のパッチが必要になった場合は随時適用できる体制を検討します。
- ☐ パッチを開発 QA 環境でテストし、実働環境に導入した途端「システム故障」という事態にならないことを確認します。
- ☐ パッチを適用したら、その安定性を監視します。これには、ネットワークの安定性の監視も含まれます。
- ☐ サポートが終了したオペレーティング システムで動作するシステムは廃棄します。

報告されたクラウド セキュリティ インシデントの 65% が、設定の不備に起因しています。

クラウド環境を保護するための推奨事項

- ☐ どのようなデータがアクセス可能であるのか、または公共インターネットに公開されているのかを定期的に評価します。
- ☐ 脆弱なシステムや管理されていないクラウド資産の追跡を支援する、攻撃対象領域管理ソリューションの導入を検討します。
- ☐ プラットフォームごとにクラウド セキュリティの専門知識を活用します。クラウドでのセキュリティ管理には、各プラットフォームの微妙な差異に応じた専門知識が必要です。プラットフォームが複雑なほど、不注意によるデータ漏洩を招くミスの可能性が高まります。
- ☐ クラウドの管理アクセス権を持つユーザーが、各クラウド環境でのトレーニングを十分に積んでいることを確認します。
- ☐ 社内に専門知識を有する者がいない場合、またはクラウド資産が特別に複雑で常時変化する状態にある場合には、マネージド セキュリティ サービスという選択肢を検討します。
- ☐ クラウド環境へのアクセスを管理します。CSP コンソール、API、クラウドの CLI など、クラウド管理機能へのアクセスは必要なユーザーに限定します。そうしたロールベースのアクセス制御 (RBAC) は、設定ミスやその他のセキュリティ上のミスのリスクを最小限に抑えるために不可欠です。

- ☐ 管理者とユーザーで認証情報を分け、日常のユーザーには実働環境へのアクセス権のみを与えます。
- ☐ 可能な場合は許可リストを実装して、さらにアクセス権を狭め、既知および信頼できるエンドポイントに限定します。
- ☐ クラウド データを定期的に監査し、どのような機密データが、どこに保存されているかを把握します。
- ☐ 機密データは (最低限) 暗号化し、セグメント化して RBAC に基づくアクセス制御を適用し、キーの定期的なローテーションを実施します。キーをクラウド プロバイダまたは自社組織内のどちらで維持するのが最適であるかを検討します。ただし、キーへのアクセスを制限し、リスクへの露出を抑えるキーのセキュリティ ポリシーが設定されていることを確認してください。

Cortex によるセキュリティ運用の強化

知っての通り、セキュリティは、人材、プロセス、テクノロジの絶妙なバランスの下で運用されます。そこで、SOC 向けに設計されたセキュリティ ソリューションの総合スイートを紹介します。

Cortex ポートフォリオは、セキュリティ運用全般にわたって検出率と運用効率を向上する、エンドツーエンドのセキュリティ ソリューションを提供します。これらのテクノロジはパロアルトネットワークス自身の SOC と、世界中の数千に及ぶ SecOps で稼働しています。

Cortex XDR は、最先端のエンドポイント防御と、ネットワーク、クラウド、エンドポイント、実質的にあらゆるデータ ソースに対する全社規模の脅威検出とレスポンス機能を提供して、組織を攻撃から保護します。特許取得済みの動作と機械学習ベースの分析で、回避能力を備えた脅威を特定し、侵害の発生前の対応に必要なインテリジェンスを提供します。攻撃が発生してから結論が出ても遅いのです。侵害が発生する前に攻撃を阻止してください。

Cortex XSOAR は、インシデントを管理し、ワークフローを自動化して運用効率を最大化する、単一プラットフォームによる SOC を実現します。チェックリスト内のプロセスのうち手動で繰り返されるものは、いずれも自動化の候補です。ユーザー アクセス管理、フィッシング レスポンス、脆弱性管理、クラウド セキュリティなどの主要プロセス用に 900 以上の構築済み自動化パッケージが用意された XSOAR は、SOC の仮想的なパートナーとなり、インシデント レスポンスを加速したり、アナリストの日常業務の負担を軽減したりします。

Cortex Xpanse は、クラウドが常に変化し続けていること、セキュリティ ギャップを露呈していることを前提としています。攻撃者がネットワークに侵入するには、ギャップが 1 つあれば十分です。Xpanse は攻撃対象領域を継続的に監視し、インターネットに公開されているクラウド資産や設定ミスの最新リストを提示します。攻撃者よりも先にシャドー IT を発見してください。

エンドツーエンドのネイティブな統合と相互運用性を備えた SOC チームは、Cortex Ecosystem 全体での継続的なシナジー効果により、脅威のループを終息できます。これら 3 つの製品はすべて連携して機能し、脅威の状況を監視するだけでなく、最も堅牢な検出、レスポンス、調査機能を実現します。

- Cortex XDR と Cortex Xpanse は、インターネットの攻撃対象領域、エンドポイント、クラウド、およびネットワークにわたり、リモート ワーカーも含め、究極の可視性と検出を実現します。
- Cortex XDR は Cortex XSOAR を活用して、マルウェア調査とレスポンスを自動化できます。
- Cortex Xpanse と Cortex XSOAR は連携して、Xpanse の資産情報を使用して自動的にインシデントをエンリッチ化し、新たに検出された資産の修復を自動化します。
- Cortex XSOAR は、パロアルトネットワークスのすべての製品と数百に及ぶその他のセキュリティ ツールからアラートと脅威情報を取り込み、インシデントの調査を促進するとともに、インシデント レスポンスの自動化を後押しします。

Unit 42 MDR による 24 時間 365 日のサイバー攻撃検出とレスポンス

Unit 42 のセキュリティ専門家は、組織保護の長年の経験をお客様の環境の監視や、疑わしい活動の検出に生かしています。アナリストは Cortex XDR を駆使してエンドポイント、ネットワーク、クラウドからのセキュリティ テレメトリ データを集約してソースを特定します。そして正確な脅威インテリジェンスと AI を活用した分析により、最も高度な脅威の防御、検出、レスポンスを実現します。

Unit 42 MDR チームは、独自のプロセス、インフラストラクチャ、エンリッチメントを組み合わせて、検出、レスポンス、脅威ハンティングを加速することで、組織に影響を与える可能性がある悪意ある活動を迅速に阻止します。

Unit 42 保護契約を結べば数分もせずにレスポンスが開始されます

侵害に気付いた瞬間に、時計は動き出します。即座に侵害を封じ込めて根本原因を突き止めないと、敵は再び攻撃してきます。

Unit 42 保護契約を結べば、弊社の専門家を短縮ダイヤルでいつでも呼び出せる、自社チームの延長のように活用できるため、攻撃の影響を最小限にとどめ、より早く通常業務に戻ることができます。

今後の SOCXSIAM で未来を先取り

Cortex 製品は可視化、保護、自動化に関する SOC の主な要件に対処できますが、大半の組織は今も SecOps のコア コンポーネントとして SIEM に頼っています。しかし SIEM 製品は、無数のアラートと手動のプロセスでアナリストに負担をかけているため、効果的で一元化された脅威の検出とレスポンスという約束を実現できていません。セキュリティ チームは、複数のセキュリティ機能を 1 つの土台となるソリューションにまとめて自動化し、全社的なセキュリティ データを可視化する集中管理プラットフォームを必要としています。

拡張セキュリティ インテリジェンス & 自動化管理 (XSIAM) は必要性に対処するために設計されており、AI を活用する自動化機能を利用してセキュリティ成果を根本的に改善し、手動の SecOps モデルを変革します。インテリジェントなデータ基盤を構築し、統合された SOC 機能を自動化することで、XSIAM はレスポンスを高速化し、脅威に先手を打ち、アナリストの作業を大幅に合理化します。

Cortex 製品ポートフォリオが実現する、業界最高峰の脅威検出機能、防御機能、攻撃対象領域管理機能、セキュリティ自動化機能の詳細は、ホワイト ペーパーをご覧ください。

Cortex を用いた仮想 SOC プラットフォームの構築

明日の SOC 計画を今日立てるには

サイバー脅威環境の現況、攻撃者が好む戦術などの詳細は、「Unit 42 インシデント レスポンス レポート (2022 年版)」をご覧ください。

〒 100-0011
東京都千代田区内幸町 2 丁目 1 番 6 号
日比谷パークフロント 15 階
電話番号 : 03-6205-8061
www.paloaltonetworks.jp

unit42_cybersecurity-checklist-57-tips_112222