protiviti®
Global Business Consulting

レッドチームと敵対的シミュレーション

標的型攻撃に対する対応力を可視化

プロティビティのレッドチームサービスは、通常のペネトレーションテストの範囲をはるかに超え、組織や業界を標的とする動機を持つ高度標的型攻撃（APT攻撃）をシミュレートする形で、標的型サイバー攻撃を立案・実行します。

プロティビティは、クライアントのネットワーク、システム、物理的な場所に対して一切の操作を行う前に、脅威インテリジェンスデータを活用し、広範な偵察と情報収集を行います。これにより、組織を保護するための構成とプロセスだけでなく、攻撃が発生している最中に組織がそれを特定する能力を評価するテスト計画を策定することができます。

レッドチーム演習では、複数の攻撃ベクトルとエクスプロイト手法を駆使し、以下のカテゴリにおける組織の成熟度を評価し、重要な問いに答えます。

People

- 従業員は、フィッシング、ビッシング、物理的なソーシャルエンジニアリングといった一般的な手口による攻撃に対して脆弱性がないか。
- 物理的な拠点において、オンサイトネットワークへの侵入を防止するための適切なセキュリティ制御が実装されているか。
- 従業員、ベンダー、または委託業者が意図せず組織に関する情報をインターネット上に公開していないか。

Process

- 企業のプロセスとポリシーは、外部からの不正アクセスを阻止するのに十分適切に設計されているか。
- 進行中の攻撃を検出し、その影響を軽減するための適切なインシデントレスポンスプロセスが存在するか。

Technology

- 組織のテクノロジー環境は攻撃に対して脆弱性がないか。
- システム、アプリケーション、ネットワークの構成は、不正アクセスを防止するように設計されているか。
- セキュリティ侵害を監視、検出し、対応するための適切なテクノロジーが導入されているか。

プロティビティの支援内容

- **セキュリティコントロールの最適化**
- **協調型パープルチームテスト**
- **脅威エミュレーション**
- **レッドチームおよび攻撃シミュレーション**

> データ侵害に関する報道が後を絶たない中、多くの組織が「我々は準備ができているのか?」と自問しています。レッドチームは、高度標的型攻撃をシミュレーションし、標的型攻撃を実行することで、組織が実際の攻撃に対してどのように対応するかを検証し、この問いに答えます。
>
> — **Krissy Safi**
> Managing Director, Attack & Penetration

レッドチームと敵対的シミュレーション

プロティビティのアプローチと手法

セキュリティコントロールの最適化：主要なセキュリティ技術（EDR、SIEM、AV、IPS/IDS 等）およびインシデントレスポンス担当者に対して、最新の攻撃者の戦術、技術、手順を用いて手動および自動でのテストを実施します。これにより、セキュリティコントロールの動作基準を評価・確立するとともに、組織が導入しているツールセットの効果を可視化します。

パープルチーム演習：組織のインシデントレスポンス「ブルーチーム」と連携し、様々な攻撃手法をシミュレーションしながら、そのような攻撃への対応方法に関する指導と教育を提供します。複数のシナリオを通じて協働し、標的型攻撃が軽減される可能性のある各段階を評価・特定し、防御コントロールの実装に関するガイダンスを支援します。

脅威エミュレーション：脅威プロファイリングまたはモデリング演習を実施し、組織にとって潜在的なリスク領域を特定します。プロファイリングとモデリングの結果に基づき、特定の脅威アクターやランサムウェアなどのリスクシナリオに対する組織の耐性を評価するため、標的型技術的脅威エミュレーションを実施します。

レッドチームおよび敵対的シミュレーション：組織を保護するための技術、プロセス、人材を評価するため、現実世界の脅威と攻撃を制限なし、または最小限の制限でシミュレーションします。

ビジネス要件

大手ヘルスケア組織のネットワークが重大なインシデントにより大きな影響を受けた後、取締役会と監査委員会は、将来同様の攻撃に対する組織の回復力をより深く理解したいと考えました。組織は成熟した脆弱性およびパッチ管理プログラムを有し、定期的なペネトレーションテストを実施していましたが、過去にレッドチーム演習を実施したことはありませんでした。

ソリューションの提供

プロティビティは、主要なクライアントのステークホルダーと協議し、演習の具体的な目標とターゲットを定義しました。プロティビティチームは、物理的なソーシャルエンジニアリング、フィッシング、アプリケーションベースの攻撃、ネットワークの悪用を含むさまざまな攻撃を実行し、ネットワークを侵害し、攻撃者が特権を昇格させ、機密性の高いシステムに横展開し、データを窃取する能力を実証しました。

ビジネス成果

クライアントは、レッドチーム演習の結果を活用し、特定されたギャップを埋めるための今後のセキュリティ戦略を策定し、ネットワークとエンドポイントにおける悪意のあるアクティビティをセキュリティチームに迅速に警告する技術とプロセスを導入することで、企業全体のセキュリティ体制を大幅に強化しました。

プロティビティLLC　*protiviti.jp*

東京：東京都千代田区大手町 2-6-4 TOKYO TORCH 常盤橋タワー24F　**大阪**：大阪府大阪市北区梅田 3-2-123 イノゲート大阪9F

protiviti®