Secureworks®

Secureworks®
Red Teamサービス

組織としてサイバー攻撃への耐性（サイバーレジリエンス）を向上するために、従来のセキュリティ診断やペネトレーションテストだけではアプローチが不十分です。サイバー攻撃の多くは、社内ネットワークやクラウドサービスからの不正アクセスを発端としています。サイバーレジリエンスを強化するには、第三者の視点から現状のセキュリティ対策が必要不可欠で、さらに実際のサイバー攻撃同等の攻撃を体験し、それから得られた情報を経営層に提示することで、適切な経営判断するための指針にもなります。

Red Team を一言で言うと…

- 「超」実践的なサイバー攻撃シュミレーション
- インシデントマネジメント活動の一環
- 目的：組織の危機対応能力の訓練・評価

Red Team に関するよくある誤解

- 脆弱性診断
- （従来の）ペネトレーションテスト
- バグハンティング（Bug Hunting）

セキュアワークスの Red Team サービスは、「友好的敵対立場」として、外部公開システムや Web アプリケーション、業務端末などの IT 部門に対する攻撃だけではなく、ソーシャルエンジニアリングや物理侵入を含む総合的な攻撃アプローチを実施します。
これにより、「人・プロセス・技術」の３つの構成要素から総合的に組織のサイバーレジリエンスを評価し、経営層、IT 部門・セキュリティ部門、社員全体のセキュリティ意識を向上させ、効果的なセキュリティ対策を促進します。

情報セキュリティの構成要素と Red Team
組織のインシデント対応能力をあらゆる側面から評価・訓練

People（人）

- インシデントに対応するための能力は十分？
- 緊急時に連携できる専門チームや外部機関は？

Process（プロセス）

- インシデントの報告フローは組織の実状に合っているか？
- 端末隔離後の復旧プロセスに問題はないか？

Technology（技術）

- 適切な防御システムが実装されているか？
- 攻撃を検知するシステムは有効に機能するか？

Red Team サービスの特徴

1 攻撃目標の設定

ビジネスクリティカルな要件をゴールに設定し、
ゴール達成に向けたサイバー攻撃を実施

- サイバー攻撃グループはお客様に対して何をしますか？その理由は？
- お客様にとって守るべき情報資産は何ですか？
- お客様にとって「ビジネスクリティカル」なのはどんな状況ですか？

ゴールの設定例

- 社員の端末のマルウェア感染
- Active Directoryの管理者権限窃取
- クラウドサービス(AWS/Azure)の管理者権限の窃取
- プラントデータの窃取
- データセンター/サーバー室への物理侵入

2 事前通告なし

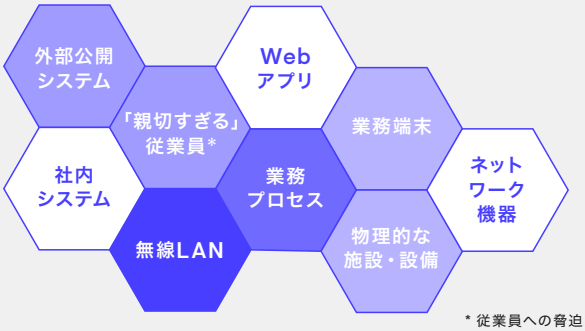
日常のオペレーションの中で起こる
サイバー攻撃の兆候に気づけるか？

- 攻撃者は予告なく、目立たないように活動
- Red Teamも、ごく少数の関係者にのみ事前通知

- システム的に異常を検知できるか？
- その異常はインシデントとして認識されるか？
- インシデントに適切に対応できるか？

3 組織全体が対象

ソーシャルエンジニアリングや物理侵入を含む
総合的な攻撃アプローチ



* 従業員への脅迫・暴行またはそのおそれを抱かせる調査は実施しません

Red Team サービス実施の流れ

主なポイント

- キックオフ時に、攻撃目標（ゴール）、演習アプローチに関する合意を締結
- 演習内容や実施時期などについては、お客様内のごく限られたプロジェクトメンバーのみで共有
- 演習実施に際し、プロジェクト（お客様）ごとに攻撃環境（フィッシング用ドメイン、C2 サーバなど）を個別に構築、プロジェクト終了後に破棄
- 攻撃演習が開始すると、端末感染や物理侵入などの境界突破後、お客様内部ネットワークへの侵入や横断的侵害を繰り返し、目的遂行を目指す
- 成果物は、攻撃実施フェーズごとに詳細を記載した報告書、および報告会（経営層、CSIRT、システム管理者など）
- プロジェクト終了後には、侵入した端末やサーバへのクリーニング（ファイル削除など）を行う

Red Team サービスラインナップ

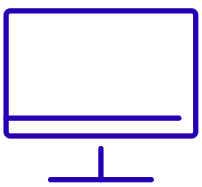
Red Teamサービスをサイバーキルチェーンの各フェーズに分割して提供可能

各種Red Teamサービスの比較

特定の範囲を評価したい場合、ご要望に応じて推奨テスト案を提示します

	Red Team PBT	Red Team	Red Team ABT
実施目的	**境界突破**に関する セキュリティリスクを評価したい	**リアルなサイバー攻撃演習**により セキュリティの総合力を評価したい	**侵入された後**の セキュリティリスクを評価したい
評価対象	主に「人・プロセス」	人・プロセス・技術	主に「プロセス・技術」
攻撃範囲	境界突破まで	全て	境界突破後
訓練対象	検知・防御・対応	検知・防御・対応	主に「検知・防御」
事前通知	最小限 CXO、IT管理者、広報責任者、など	最小限 CXO、IT管理者、広報責任者、など	原則、通知して実施 主に攻撃起点に関わる従業員の方、など
制限事項	原則なし	原則なし	一部で設定可能
ゴール設定	内部ネットワークへのアクセス	自由に設定可能	自由に設定可能
攻撃期間	1か月	2か月	1か月

Secureworks®



サービスに関するより詳細な内容に関しては、下記までご連絡ください

セキュアワークス株式会社
SCWX_PreSales@secureworks.com
Tel.03-4400-9373
www.secureworks.jp

Secureworks®

■ 記載内容は、2024 年 2 月 6 日時点のものであり、予告なく変更する場合があります。最新の仕様については、弊社ホームページにてご確認ください