docomo Solutions

ペネトレーションテスト

攻撃者視点で侵入耐性を検証し、
弱点を明確化します。

自社環境の攻撃耐性は、試してこそ分かる。

現状把握のチェックポイント

- ☑ 対策は講じたが実攻撃に対する耐性を **定量的に示せない**
- ☑ リモートアクセス経路の安全性について **根拠をもって説明できない**
- ☑ 経営層からの「本当に安全か」に **客観的な裏付けで回答しづらい**
- ☑ 侵害を想定した対応設計が **整備できていない**

侵入可否を実証し、弱点を可視化。
貴社に合わせた柔軟な対策案まで提示します。

ペネトレーションテストで得られる3つのメリット

1 攻撃耐性を実証

侵入できるかの
達成可否を判定

2 弱点の可視化

被害影響と弱点の
明確化

3 貴社に合わせた改善提案

優先順位を付けた
具体策の提示

サービスの特長

- 専門資格保有者による高度なテストの実施
- 最新の攻撃手法を反映したテストシナリオの作成
- テスト実施後の具体的な対策案/緩和策のご提示
- テスト結果報告後、3か月以内の再テストを無料で対応

※サーバ侵入とマルウェア感染検証メニューの場合は、オプションにて提供

テストメニュー

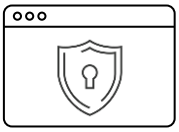
※実施範囲に応じて最適なお見積りをご案内いたします。

サーバ侵入

公開サーバ等への
侵入可否を検証

診断対象 公開サーバ

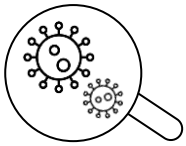
Webアプリ侵入



Webアプリに対して
侵入可否を検証

診断対象 公開Webサーバ
Webアプリ

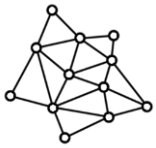
マルウェア感染検証



感染後のマルウェアの
検知・除去の検証

診断対象 メールフィルタ
EDR・NDR

オフィスハッキング



オフィス内ネットワークの
耐性を検証

診断対象 OA環境

提供の流れ

STEP 01	STEP 02	STEP 03	STEP 04	STEP 05
診断対象の決定	診断準備	診断作業	テスト結果報告書の作成	報告会 └検出内容 └対策説明

ペネトレーションテストに関するお申込み／お問い合わせ

docomo Solutions

ご興味がございましたら、当社営業担当までお問い合わせください