ペネトレーションテスト診断
サービス紹介

今までに存在しなかった
「攻撃する側の視点」で診断結果を提供！

INTELLIGENT WAVE INC.

今までのセキュリティ診断で課題は網羅できているか？

顧客や社内の大切なデータを扱っている企業にとって、「セキュリティの脆弱性」や、「現在のセキュリティ課題と今後の対策」はできるだけ把握したいはずです。

セキュリティ課題を洗い出すために定期的にセキュリティ診断サービスを利用する企業が増えています。この流れについては、私たちも大いに賛成しています。

セキュリティ診断結果は今後の対策に大きく関わるものとなるでしょう。そのため、セキュリティ診断ベンダの選定を「価格」や「診断までの日程」だけで選ばれていることに私たちは違和感を感じております。
このままの診断サービスで、お客様のセキュリティ課題の解決に導いているのか。

従来型のセキュリティ診断は「ツール診断」と「手動診断」のどちらかを選択し、診断結果を算出します。

●ツール診断
多くのテストを短期間かつ診断速度が速い利点に対して、細かな点まで配慮ができず網羅性が担保出来ない特徴があります。

●手動診断
細かく柔軟な対応が実現可能でありますが、診断時間がかかりコストが大きくなってしまい、企業側の予算と合わないことが多い状況です。

私たちは両診断のメリット・デメリットを踏まえ、セキュリティ診断を**「ツールと手動の両面」**で提供することをスタートしました。

実現が可能とした理由は、多くのセキュリティ診断を企業様に提供した実績をもとに、ツール診断での対策可能な範囲と手動診断が必要な範囲を明確化し、診断前に網羅化・定型化を行ったことです。これにより、従来型のセキュリティ診断よりも高品質かつ低価格に抑えた形でお客様へ提案することが実現しました。

また、より付加価値を高めるために**「ホワイトハッカー」**による手動診断を採用し、**「攻撃者目線」**での診断結果をご提供が可能です。多くの企業様へ対策価値の高いセキュリティ診断をご案内いたします。

Contents

脆弱性診断とペネトレーションテストの違い(1) ・・・・・・・・・・・・・・・・・・・・P.2
脆弱性診断とペネトレーションテストの違い(2) ・・・・・・・・・・・・・・・・・・・・P.3
ペネトレーションテストの流れ ・・・・・・・・・・・・・・・・・・・・・・・・・・・P.4
ペネトレーションテストのスコープについて ・・・・・・・・・・・・・・・・・・・・P.5
①標的型メール攻撃（マルウェア感染/フィッシング）による侵入 ・・・・・・・・・・P.6
①標的型メール攻撃：ご検討事項 ・・・・・・・・・・・・・・・・・・・・・・・・・P.8
②外部公開リソース（Webサイト/クラウドなど）からの侵入 ・・・・・・・・・・・P.10
②外部公開リソースからの侵入：ご検討事項 ・・・・・・・・・・・・・・・・・・・P.13
③物理環境からの侵入（オンサイト対応）・・・・・・・・・・・・・・・・・・・・・P.15
③物理環境からの侵入：ご検討事項 ・・・・・・・・・・・・・・・・・・・・・・・P.17
④複合的なサイバー攻撃による侵入 ・・・・・・・・・・・・・・・・・・・・・・・P.18
オプション ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P.20
お問い合わせ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P.22