ソリューションカタログ

SOPHOS

ソフォスアドバイザリーサービス

進化するサイバー脅威に対する
プロアクティブなリスク軽減とレジリエンスの強化

カスタマイズされた専門家によるセキュリティ評価

デジタルトランスフォーメーションの需要の高まり、AI の台頭、そして絶えず進化するサイバー脅威を受けて、先見の明のある組織は、サイバーセキュリティが単なる技術的課題ではなく、戦略上の優先課題であることを理解しています。高度なスキルを持つ攻撃者、規制当局の監視、およびステークホルダーの期待に対応するには、デジタル資産を保護するための能動的かつ包括的なアプローチが必要です。ソフォスアドバイザリーサービスは、独立性の高い専門知識、豊富な経験、カスタマイズされた戦略を提供し、システム全体の脆弱性の特定、防御の強化、ビジネスレジリエンスの向上を実現します。

高度な認定を受けたソフォスのセキュリティ専門家が、実際に攻撃で用いられる戦術、手法、手順 (TTP) に基づいてネットワーク、システム、従業員をテストし、以下の目標達成を支援します。

- 攻撃者に悪用される前に脆弱性を特定する。
- 高度な脅威に対する防御を強化する。
- 規制遵守の要件を満たす。
- インシデント対応の準備状況を評価する。
- 顧客、パートナー、ステークホルダーとの信頼を築く。

防御とセキュリティポスチャのプロアクティブな強化

ペネトレーションテスト (侵入テスト)

ペネトレーションテストでは、現実のサイバー攻撃をシミュレートして、システム、ネットワーク、アプリケーションの脆弱性を特定します。経験豊富なテスター (ホワイトハッカー) が、攻撃で脆弱性が悪用されると何が起きるかを実証します。

ペネトレーションテストには、主に 2 種類あります。外部ペネトレーションテストは、Web サイト、VPN、公開サービスなど、インターネットからアクセス可能なシステムに焦点を当て、外部から攻撃者が境界を突破しようとする状況をシミュレートします。内部ペネトレーションテストは、ネットワーク内部のシステム、アプリケーション、データに焦点を当て、内部関係者による脅威や境界を突破して侵入した攻撃者をシミュレートします。

このサービスの特長：

- 定期スキャンでは検出できない隠れた脆弱性を特定します。
- 防御を強化するための具体的な推奨事項を提示します。
- プロアクティブなリスク管理への取り組みを証明します。
- 境界および内部のセキュリティリスクを包括的にカバーします。

提供される重要な情報：

- 自社のインフラストラクチャで最も重大な脆弱性はどこにあるか。
- 外部の攻撃者は自社の防御をどの程度簡単に突破できるか。
- 攻撃者にアクセスされた場合、ネットワーク内にどのようなリスクが存在するか。
- 攻撃が成功した場合、どのような影響が考えられるか。
- 特定された弱点を修正するために、どのような対策を講じることができるか。

ワイヤレスネットワークのペネトレーションテスト

ワイヤレスネットワークのペネトレーションテストは、組織の Wi-Fi ネットワークおよびインフラストラクチャのセキュリティを評価し、適切な要件への準拠を検証します。テスターは、暗号化、認証、およびアクセスコントロールに存在する脆弱性の悪用を試みます。

ワイヤレスペネトレーションテストのスコープは次の 2 つです。「パッシブアセスメント」では、能動的に接続を試みることなく、ワイヤレストラフィックを監視して、許可されていないデバイス、不正なアクセスポイント、および設定ミスを特定します。「アクティブアセスメント」では、暗号の解読、認証の回避、不正アクセスを介してワイヤレスネットワークの脆弱性を悪用しようとする攻撃者をシミュレートします。

このサービスの特長：

- ワイヤレスネットワーク経由で送信される機密データを保護します。
- 不正なアクセスポイントや設定ミスを特定します。
- ベストプラクティスに準拠しているワイヤレスセキュリティポリシーを適用します。
- Wi-Fi の脆弱性によるデータ漏洩のリスクを軽減します。
- 受動的なリスクと能動的に悪用されるリスクの両方を評価します。

提供される重要な情報：

- 許可されていないユーザーがワイヤレスネットワークにアクセスできるか。
- 強力な暗号化と安全な認証方法を使用しているか。
- ネットワークに不正なデバイスが接続されているか。
- 攻撃者は自社のワイヤレス保護を回避できるか。
- ワイヤレスセキュリティを強化するためにどのような対策を講じることができるか。

Web アプリケーションのセキュリティ評価

Web アプリケーションは、重要なビジネスデータや顧客データを扱うことが多いため、攻撃者の標的になります。Web アプリケーションのセキュリティ評価は、SQL インジェクション、クロスサイトスクリプティング (XSS)、認証の脆弱性など、一般的な脆弱性に焦点を当てて、Web アプリケーションが保護されていることを確認します。

このサービスの特長：

- Web アプリケーションで処理される顧客データと企業データを保護します。
- リスクを高めるコーディングや設定のミスを特定します。
- OWASP Top 10 や PCI DSS などの基準への準拠を支援します。
- Web サイト改ざん、データ漏洩、評判低下のリスクを軽減します。
- 外部からの視点で、アプリケーションのセキュリティを詳細に分析します。

提供される重要な情報：

- 自社の Web アプリケーションは一般的な攻撃手法に対して脆弱か。
- コーディングの欠陥や設定ミスにより、機密データが流出していないか。
- ユーザー認証とセッション管理をどのように保護するべきか。
- Web アプリケーションの脆弱性を修正するために、どのような対策を講じることができるか。

セキュリティ評価サービスの概要

評価の種類	重点領域	提供される重要な情報	導入例
ペネトレーションテスト（侵入テスト）	インフラストラクチャ、システム、ネットワーク	脆弱性はどこにあるのか。攻撃者はどのような方法で防御を突破するのか。	外部：公開されている Web サイトとサービスのテスト。内部：内部のアクセスコントロールと権限昇格のテスト
ワイヤレスネットワークのペネトレーションテスト	Wi-Fi セキュリティ、暗号化、アクセスコントロール	Wi-Fi は安全か。許可されていないデバイスや不正なデバイスは存在するか。	オフィス Wi-Fi のセキュリティのテスト。不正なアクセスポイントの特定。許可されていない接続の試行
Web アプリケーションのセキュリティ評価	Web アプリケーション、コーディングの欠陥、認証	自社のアプリケーションは安全か。機密データが漏洩する可能性はあるか。脆弱性をどうすれば修正できるか。	顧客ポータル、EC サイト、社内の Web アプリのテスト。SQL インジェクション、XSS、または認証の欠陥の特定

その他のサイバーセキュリティテストサービス

個々の評価や手法だけでは、組織のセキュリティの全体像を把握することはできません。それぞれの敵対的テストには、独自の目的と許容可能なリスクレベルが設定されています。ソフォスは、セキュリティポスチャと対策の評価、および脆弱性の特定のために、どのような評価と手法の組み合わせを使用すべきかを決定するお手伝いをいたします。

詳細情報:
sophos.com/ja-jp/advisory-services

ソフォス株式会社営業部
Email: partnersales@sophos.co.jp

2025-05-30 BREN (MP)