Datasheet

システムの脆弱性評価
(System Vulnerability Assessment)

viettel security

システムで安全情報の脆弱性をチェックする事の必要性

情報技術が発展している時代では、人々の生活が情報技術の応用に依存する一方で、それは絶え間なく進行しています。特にデジタル化のプロセスで、現代の第4次産業革命の始まりに向けて進む中、個人や組織が自分たちのシステムを所有し維持することは、重要な業務を遂行するために不可欠なものです。例えばはビジネス運営、金融取引、ビジネス統計の計算、あるいはより大規模な工場の運営など。

したがって、システムで安全情報安全情報の脆弱性をチェックする事は組織・企業にとってとても重要になっています。これから、システムの安全を継続的で確保し、企業の定した運用を維持します。

システムで安全情報の脆弱性をチェックするサービス

システムで安全情報の脆弱性をチェックするサービスは次の事が含まれます：

- 脆弱性を特定するために、システムでコンポーネントの構成パラメーターを収集します。
- システムで存在している脆弱性をチェックします。
- システムで安全情報についてリストの見積もり、リスク評価レポート顧客にを提供します。
- サービスで検出された脆弱性が設定ミスと既知でのコンポーネントの使用という 2 つのグループの脆弱性に焦点を当てています。

システムで実行範囲に属するコンポーネントは次のものが含まれます：

- サーバのオペレーティングシステム。
- ウェブ・サーバ。
- データベースサーバ。
- メールサーバ。
- エンドユーザーのコンピューターのオペレーティングシステム。
- 管理機器、ネットワーク機器。

ポリシーの主な点

構成パラメーターを収集します。

システムのコンポーネントの構成パラメータのを収集します。次の情報が含まれます:

- パッチのインストール、バージョンの更新
- アカウントポリシーの設定
- 管理ポリシー
- アクセス・ポリシー
- 構成設定のポリシー

脆弱性をチェックします。

指定されたターゲットをスキャンするための専用ツールを使用し、システム内の存在する脆弱性を検出するためにスキャンを実行します。

評価報告

評価プロセスで検出された脆弱性の報告を送信します。顧客のインフラストラクチャに関する情報が外部に漏れないように保証されるために、この報告が安全な通信路を介して送信されます。

解決策のアドバイス

評価プロセスで検出された脆弱性に対して、ベトテル・サイバーセキュリティ・カンパニーの専門家は顧客がこの脆弱性を修正するために解決策とアドバイスを付けて送信します。

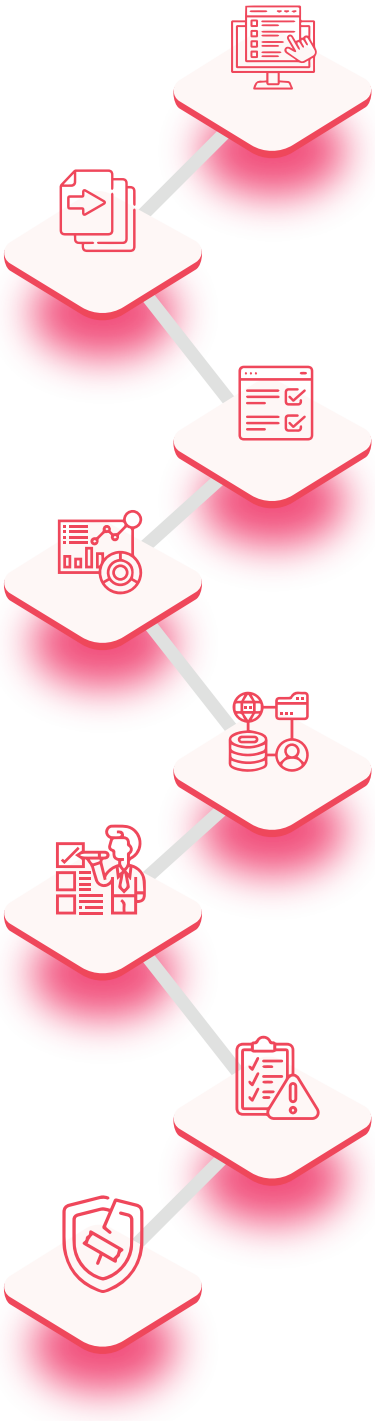
Datasheet

システムの脆弱性評価
(System Vulnerability Assessment)

viettel security

実行プロセス

評価プロセスが次のステップの通りに実行されます。



1. 調査

システムの初期調査を行い、展開計画を統一します。

2. 評価請求を送信

顧客は乙に評価請求を送信します。この請求が契約上の共同責任を負う側または代表者によって承認される必要があります。

3. 評価計画を送信

遅くとも 2 日以内に、乙は評価計画と追加請求の情報を再送します。

4. 評価環境を準備

評価プロセスを保証するために、顧客が評価環境を準備します。

5. システムの情報を提供

評価請求で脆弱性をチェックする事がある場合には、顧客は次の追加の情報を提供します:

- 検査するネットワークモデルを記述します。
- 必要な接続を実現するための方法。

6. 評価を実行

計画に通りに、乙は評価を実行します。

7. 評価結果と修正ガイドを送信

評価の後、乙は評価結果と指摘された弱点を修正するガイドを送信します。

8. 弱点と脆弱性を修正

評価結果が弱点と脆弱性を持つ場合には、顧客がガイドの通りに修正します。修正の後、顧客は再評価請求を送信し、ステップが最初の評価請求と同じです。下の場合には、プロセスが終わりになります。

- 評価結果と修正評価で不具合がありません。
- 2週間の後、顧客が修正された不具合に対する評価請求を送信しません。
- 修正された不具合を2回に評価した後、顧客がまだ修正を完了しません。