Datasheet

ベトテルのX－データサービス
(Red Teaming Service)

viettel security

初めに

デジタルと技術が進歩時代で、サイバーセキュリティの問題はほとんどのービスプロバイダー、組織などの懸念となっています。そのため、組織が情報セキュリティに対する投資を強化することは、ビジネスの効率性を確保し、データ損失、サービス中断、市場での信用失墜などのリスクを最小限に抑えるために必要な事です。

では、組織・企業が情報セキュリティの解決策を適切に備えているかどうか、ネットワークシステムが機能と任務に沿って適切に設計され、適切なセキュリティレベルに従っているかどうかを知るにはどうすればよいでしょうか？

現在在、セキュリティ上の脆弱性の検出結果、深刻度と潜在的な攻撃経路の短期期間の評価に基づいて情報システムのセキュリティレベルをレビューして評評価するために、組織・企業はPenetration Testing Service-Pentestとも呼ばれれるワークの安全情報評価・検査サービスや製品ツールを使用しています。

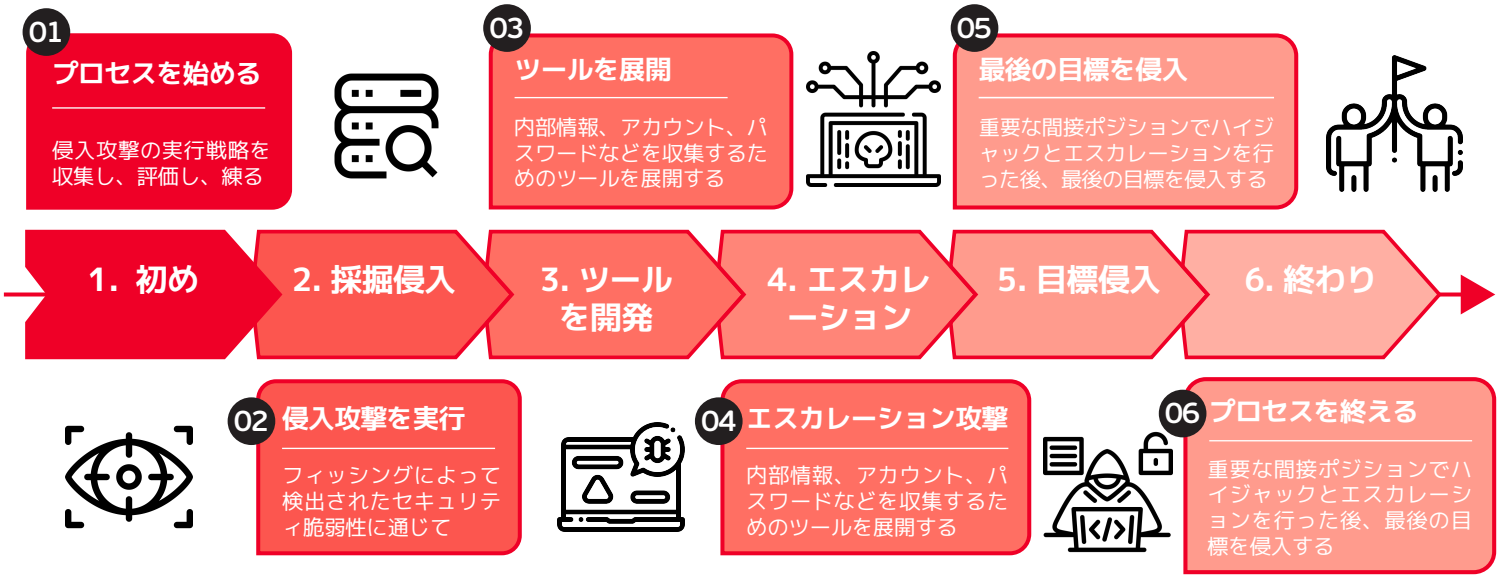
ただし、上のツールとペンテストを使用すると、次のリミットがあります。

・評価対象が通常に固定された範囲を囲んんでいますが、情報システムが常に相互互につながり、影響を及ぼし合う連鎖です。それで、限定された範囲で安全全情報を評価すると、アクティブ ディレクトリ(Active Directory)、データベースサーバー(Database Server)などのシステムの重要な箇所に深く侵入し、エススカレーション攻撃が可能ないくつかのケースを見逃す可能性があります。

・情報技術のレイヤーごとでリスク度合いだけ検出できますが、組織・企業の生産・営業プロセスに実際の影響を与える厳重なレベルを認識ことができません。いつかの場合には、中程度の多数のエラーが存在するシステムは厳重な脆弱性を持つシステムよりもデータの盗難の攻撃が高いことがあります。同時に、安全情報の問題と故障を修理し、検出する能力を評価できません。

ベトテルのX－データサービス（Red Teaming Service)

ベトテルのX－データサービス(Viettel X-Data)（意図的なデータマイニングテスト）は安全情報で存在している問題から企業が事業運営に影響を与える程度にたいしてより具体的な見方を持つのを助けるためです。
具体的な対象と表面上に限定された特定の対象だけを評価するに代わりに、顧客が向かいたい最も重要なXの位置に焦点を当てる。合意された時間枠内と制限されない範囲や実行方法で、X-データは、部から攻撃チェーン（kill-chain）を介して段階的に異なるシステムを経由することに通じて、安全情報システムの検出・修理能力を評価することを顧客に評価するのに役立ちます。また、攻撃を受け、支配権を奪われ、またはデータが盗まれた場合には、貴社にどのような影響があるかを認識する事ができます。



Datasheet

ベトテルのX－データサービス
(Red Teaming Service)

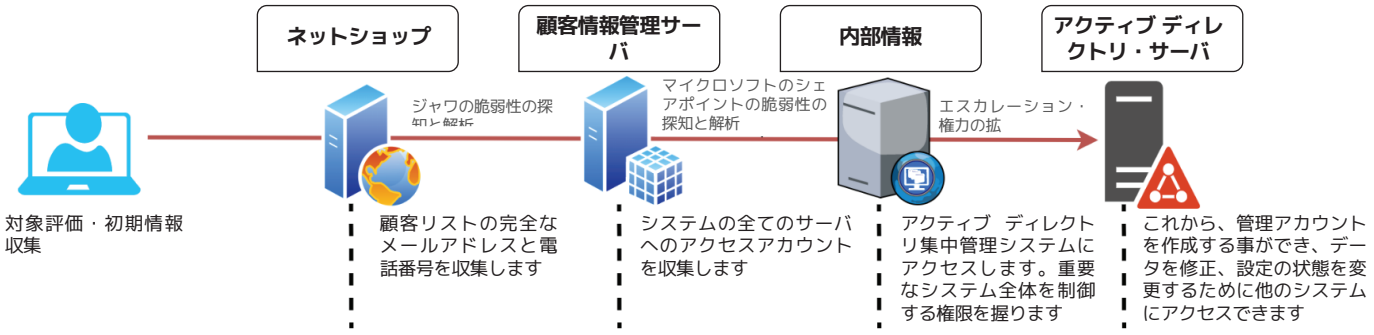
viettel security

サービル提供のステップ

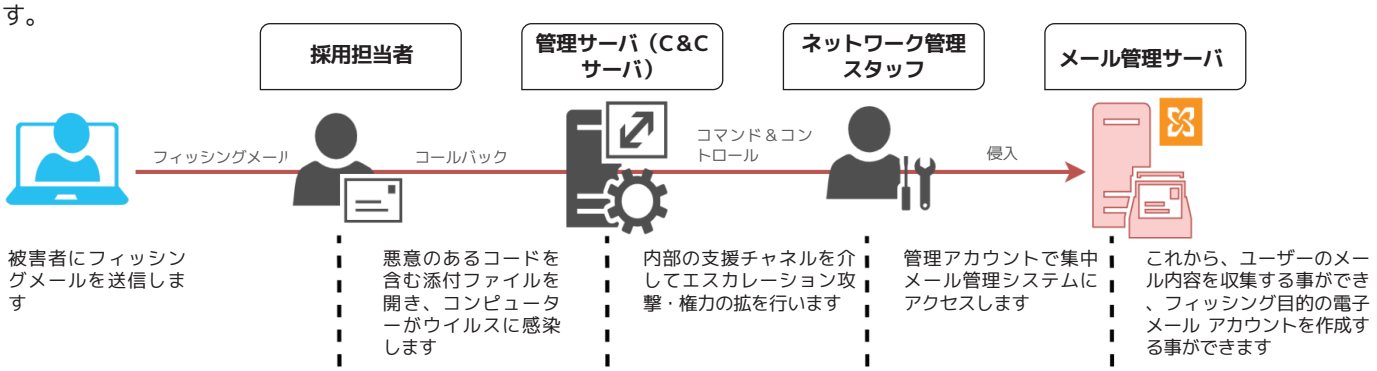
1. 顧客がシステムでの重要なポイントに対する請求を与えます。
   例えば：メールシステム、アクティブ ディレクトリ集中管理システム、銀行の国際送金システムなど。
2. 双方が実施時間を統合します。
3. 統合された時間の後、VCSが深層レポートを送信します。
4. 実際に実行プロセスを再演します。
5. 組織・企業に与える影響とリスクを分析します。
6. 完了します。

実際の場合

目標 01: アクティブ ディレクトリ集中管理システムのサーバ制御権を奪い、システムで最も高い権限のアカウントを作成します。



目標 02: 一般ユーザーに偽造メールを利用して、電子メール管理システムの制御権を奪取することによって、メールシステムの管理権を獲得します。



報告

任務完了後、顧客に提供される報告書には、以下の情報が含まれます。

1. 攻撃シナリオ、実際の行動。
2. 次の様々なポジションを通じたシステムへの侵入方法：
   - 侵入されて、制御権を奪取された各ポジションで安全情報が存在している問題。
   - このポジションが侵入された影響と収集情報が盗まれる可能性があるもの。
   - 各ポジションで安全情報の問題に対する対処法を推奨します。
3. 企業の生産・運用とシステムへの影響とリスクを分析します。（例：送金システムの中断、電気ネットワーク制御サーバーの停止など）。
4. 攻撃イベントを連鎖させ、全ての実行されたキルチェーンをデモします。
5. システムの安全情報の保証能力を向上し、回復するための総合的な解決策を提案します。