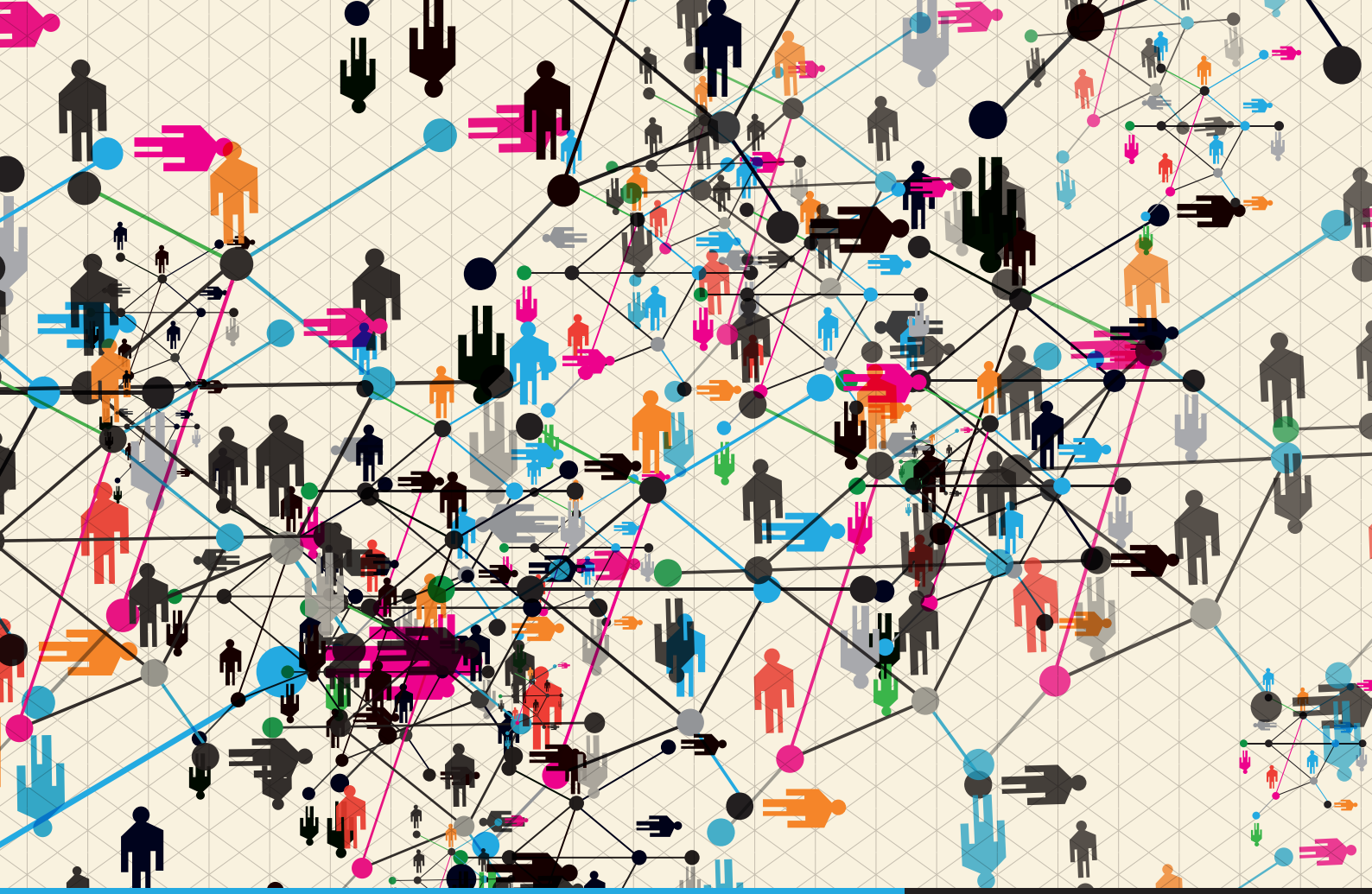
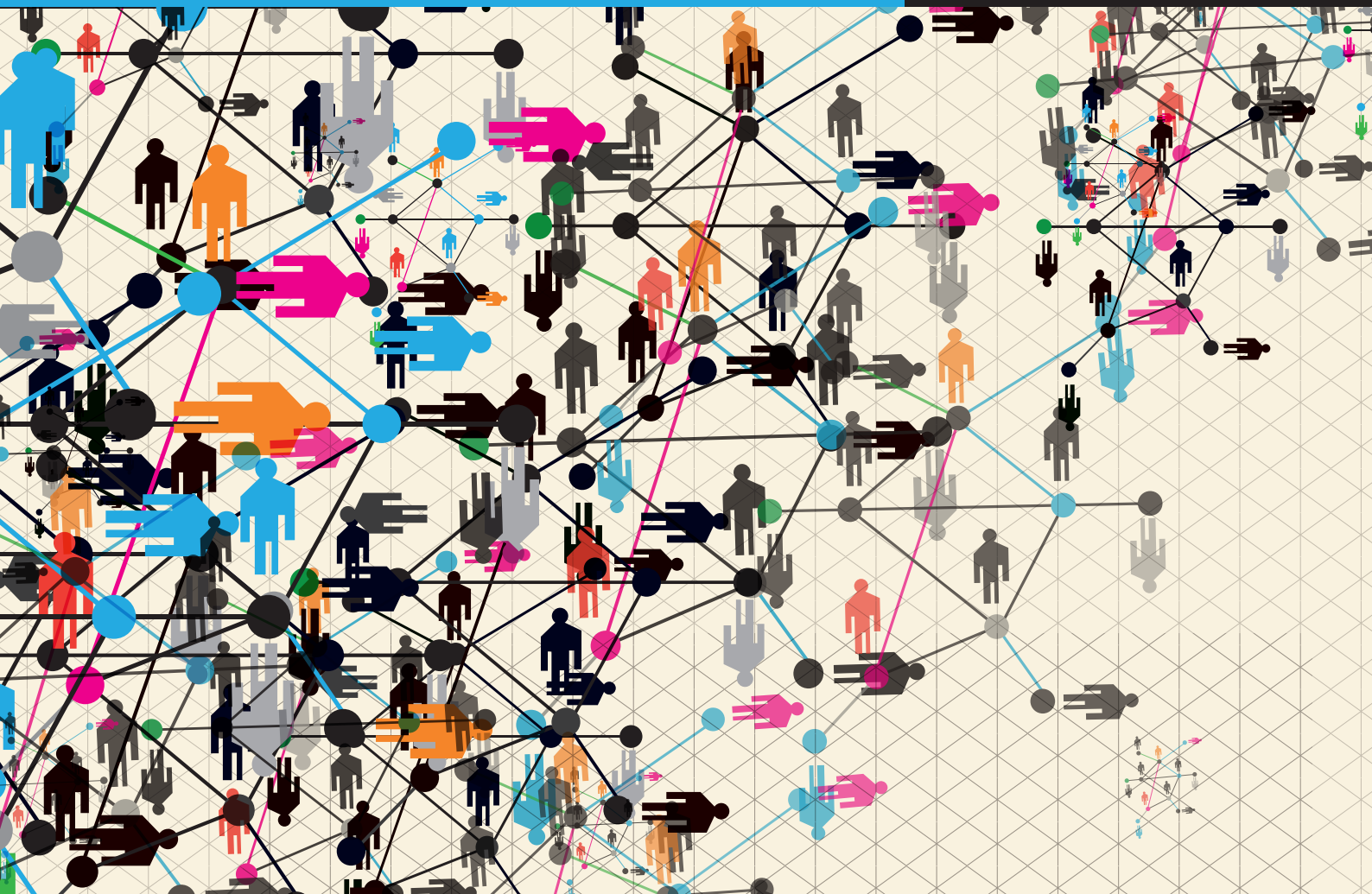


RedSealのサイバーセキュリティ分析プラットフォームでデジタルレジリエンスを最大限に

REDSEAL



デジタルレジリエンス（ネットワークの安全を維持する力）の必要性

デジタル資産は今や企業には欠かせないものとなりました。ビジネスはネットワークに大きく依存しています。そしてそのネットワークがより大きくかつ、複雑になるにつれ、セキュリティ事故や障害が発生する可能性も高くなります。ネットワークセキュリティ対策用のさまざまな製品に多額の費用を費やしても、まだまだセキュリティ事故や障害がなくならないのも事実です。そこで、昨今のビジネスリーダーの中では、デジタルレジリエンスに目を向け始めている人が増えています。私たち RedSeal がそのソリューションを提供します。

デジタルレジリエンスというのは、障害中でも運用を継続しながら、顧客の損害そして自社への風評被害と金銭的損害を最小限に抑えることができる能力です。RedSeal のサイバーセキュリティ分析プラットフォームは、最も大規模で複雑なネットワークを想定して構築されています。ネットワークの安全を維持する力を測定し、その力を最大限に発揮させビジネスを円滑に進めることを可能にします。

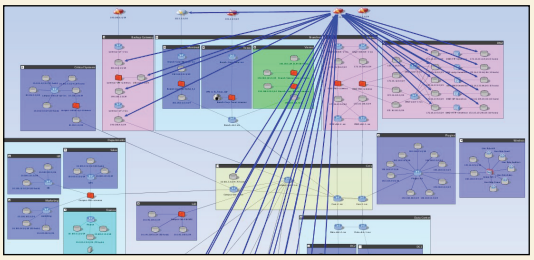
RedSeal のアプローチ

RedSeal の高度な分析プラットフォームは、正確なネットワークのモデルを作るために、最初にすべてのセキュリティとネットワークデバイスの設定を検証します。その後、セキュリティリスクを特定するためのテストを行い、脆弱性の深刻度およびアクセスの可能性に基づいて、最も重要な問題を優先的に対処できるようにします。RedSeal では、これらの作業を自動的かつ継続的に行うことができます。

現状ネットワークの把握

既存のネットワークの可視化

現状のネットワークを正確に捉えてマッピングする RedSeal のモデル — このモデルにはクラウドベースのネットワーク、仮想ネットワーク、物理的およびワイヤレスインフラストラクチャーも含まれます。RedSeal のモデルでは、それぞれのビジネスの形に合わせネットワーク内のデバイスをグルーピングすることができます。



エンドツーエンドアクセスの可視化

RedSeal はネットワーク内のすべてのポイント間において、意図的なアクセス、意図しないアクセス、不正アクセスの可能性も想定します。

詳細なアクセス経路を可視化

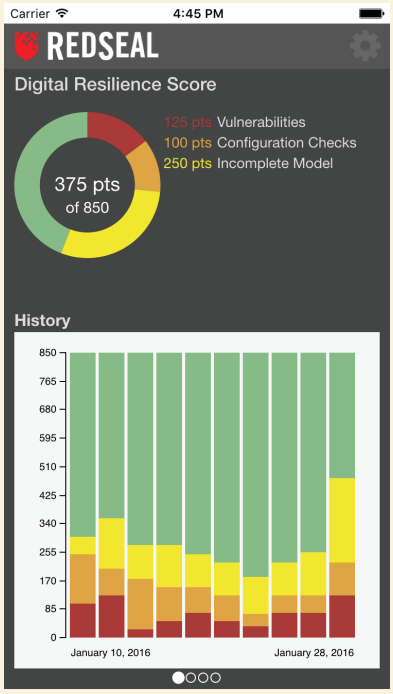
アクセス経路に存在するすべてのデバイスを認識し、すべてのデバイスのアクセスに影響を与えるルールを把握します。

ネットワーク内の認識されていないエリアを可視化

RedSeal の分析能力は、ネットワーク上で今まで存在が認識されていなかったエリアにまでおよびます。それにより、すべてのネットワーク構成情報を把握し、そしてあらゆる資産へのアクセス方法を理解することができます。

デバイスが効果的に設定されているかをチェック

RedSeal は、ネットワークのモデル作成に際し、ネットワークセキュリティリスクにさらされる可能性のあるデバイス設定を検証します。検証にはネットワークデバイスメーカーが推奨する設定や、その環境に合ったカスタムメイドチェック項目も作る事ができます。ときには、基本的な検証を怠ることが深刻なセキュリティ事故や障害を発生させる原因になることもあるからです。



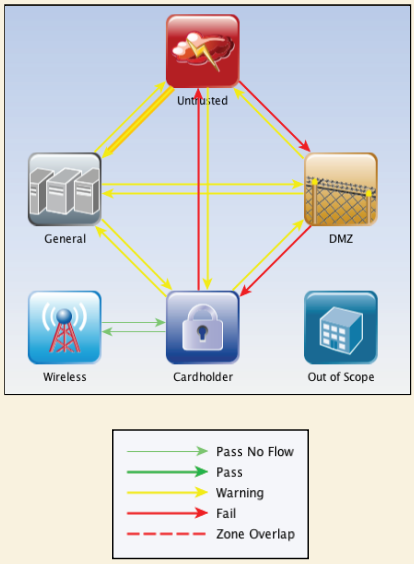
デジタルレジリエンスを判定しネットワークを常に監視

RedSeal は、ネットワークのセキュリティリスク管理の状況を反映する、ポイント制の RedSeal デジタルレジリエンススコア™ を導入しています。RedSeal のコントロールパネルまたは携帯アプリからも見ることができるこのスコアは、深刻なリスクに対する脆弱性のまん延度、デバイス設定の不備そして可視化されたネットワークに存在するギャップなどの分析をまとめた安全維持能力を示すものです。それぞれの項目の分析結果とスコアは、継続的に記録され「デジタルレジリエンスは改善されているだろうか？」という問いに的確に答えることができます。

コンプライアンスおよび企業特有のポリシーの順守を確認

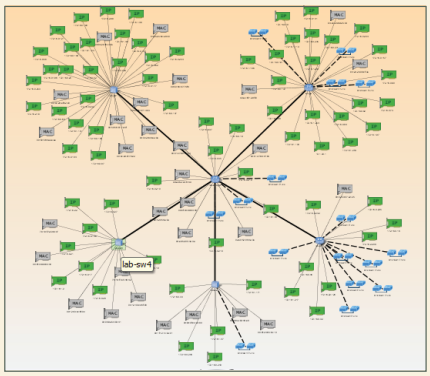
攻撃の頻度や巧妙性が増すにつれ、ネットワークの安全を守るためにコンプライアンスや企業特有のポリシーが導入されています。ポリシーは、企業活動やネットワークの統制をとれた運用を行う上で非常に重要であると言ってよいでしょう。RedSeal はこれらのポリシーへの順守を効率的かつ簡潔に確認することを可能にします。ネットワークに修正や更新作業を行った場合でも、安全性に対するポリシーを明確にすることができ、常にポリシーへの順守を確認することができます。また意図のない、または不正アクセスなどをすぐに見極め、対策を打つこともできます。そして何より、RedSeal はコンプライアンスのプロセスを自動的に行うことにより、コストを最小限に抑えることができるのです。

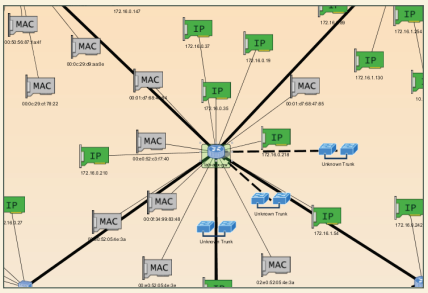
RedSeal にはPCI、NERC CIP、NIST 800-53、DISA STIG および HIPAA等のコンプライアンスに対応可能な機能が搭載されています。



最も危険な脆弱性の改善への優先付け

RedSeal は脆弱性スキャナーから出力されたデータをより効率的に活用することができます。RedSeal は、優先順位をつけるためによく使われる、CVSSスコアや資産価値を検証するだけではなく、信頼度の低いネットワークからアクセスがある可能性、そしてそこから踏み台攻撃等でどの資産やどのデータが二次影響を受けるかも明確に表します。これにより、アクセスとホスト両面での脆弱性を見ることができ、ネットワーク内に存在する本当のリスクに貴重な人材と資金を投入することができるのです。





インシデントレスポンスの向上

RedSeal は、ネットワークへの侵入が判明した時、それに効率的に対処するための支援ができます。ホストに不正アクセスが発生した場合、どの資産またはホストがどの段階で攻撃されるか判断します。Layer 2 の可視化により、影響を受けているホストを迅速に特定し抑圧、もしくは隔離することもできます。RedSeal は、影響を受けた資産を単にネットワークから外すオフライン処理を示唆するのではなく、資産を守るために必要なデバイス設定を調査することができます。これまで、何時間も何日もかかっていた確定作業が、マウスを数クリックするだけで可能になるのです。

あなたのビジネスにも RedSeal の活用を

RedSeal のセキュリティ分析プラットフォームは、仮想および物理的な機器両方で活用いただけます。

REDSEAL

株式会社 RedSeal
〒104-0061 東京都中央区銀座1-16-7
銀座大栄ビル5F

電話：03-4360-8740
E-mail: info_jp@redseal.co
www.redseal.jp

お問い合わせ