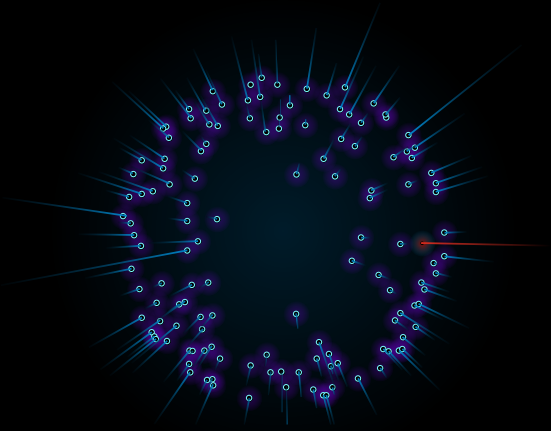
ベライゾンリスクレポート

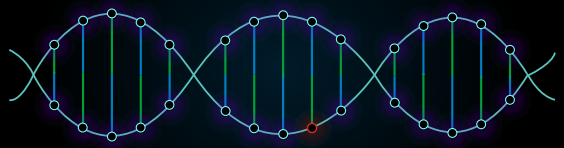
アクションにすぐに活かせるデータを用いて、セキュリティのROIを評価する。これにより、リスクやセキュリティギャップを明らかにし、ギャップの解消に必要なリソースの特定を行う。



レベル1：細部から全体を把握
アウトサイドイン・ビュー

アウトサイドイン・ビューでは、お客様組織の外部からの評価を行います。BitSightによるインターネット上のパブリックソースからデータを収集し、外部のリスク要因を評価して、お客様のセキュリティ対策をスコアリングします。また、ベライゾンのUnified Security Portalで自動生成された日次レポートを確認できます。

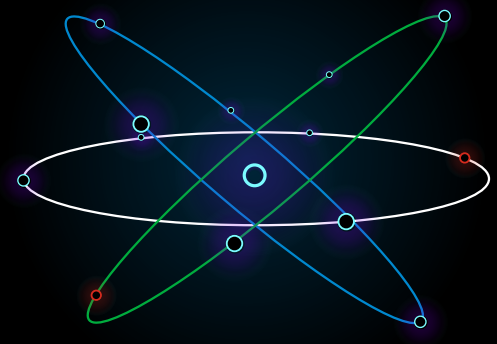
- ベースとなるインターネット上のパブリックデータソースは200以上
- 日次のレポートを自動で生成
- データソースには、BitSight、Recorded Future、ベライゾンのデータ漏洩/侵害調査報告書（DBIR）などを使用



レベル2：企業セキュリティの「精密検査」の実施
インサイドアウト・ビュー

レベル2では、エンドポイントやITインフラストラクチャの内部を自動的にスキャンしてマルウェアや不必要なプログラム、重複したツールの有無の確認といった内部評価を行います。これにより、より高精度にセキュリティを強化できます。

- レベル1のデータに加え、組織内部から収集したデータも評価に利用
- エンドポイントとインフラストラクチャを調査して、セキュリティ対策を評価し、リスクを明らかにする
- レベル1のデータソースすべてに加え、Tanium、Cylanceをソースに使用



レベル3：全方位的なリスク評価
カルチャー&プロセス・ビュー

お客様組織外部および内部のリスク要因の評価に加え、組織内のセキュリティカルチャーやプロセスも詳しく調査することで、より実態に即した状況の確認が可能になります。カルチャーおよびプロセスの評価では、自動化された複数のツールによる評価に加えて、人間の目による評価も行うことで、包括的な視点からリスクを分析し、お客様組織のセキュリティ対策を評価します。

- レベル1、レベル2で得られたデータに加えて、行動、文化、プロセス、ポリシーに基づく評価を付加
- 100時間のVerizonのプロフェッショナルサービスの提供により、セキュリティ対策の強化を支援
- 360度のあらゆる視点からセキュリティ対策を評価

verizon

詳細は、**VerizonEnterprise.com/products/security**をご覧ください。

各レベルにおける脅威ベクター

レベル1

アウトサイドイン・ビュー

BitSightによるデータソースに基づき、外部リスクベクターを評価します。リスクベクターのカテゴリーとして、侵害を受けたシステム、デリジェンスの問題、ユーザーの行動、データの漏洩があります。

- ボットネット感染
- スパムの拡散
- マルウェア
- 不審なネットワーク接続
- 脆弱性を攻撃されるおそれのあるシステム
- 開放されたポート
- TLS/SSLの証明書および構成
- Webアプリケーションヘッダー
- Sender Policy Framework（SPF）
- DomainKeys Identified Mail（DKIM）
- パッチ提供の頻度
- サーバー、デスクトップ、およびモバイルのソフトウェア
- セキュアでないシステム
- DNSSECレコード
- ドメイン悪用
- ファイル共有
- 公開にされた認証情報
- データの漏洩

レベル2

インサイドアウト・ビュー

レベル1の外部リスクベクターに加え、TaniumやCylanceによる情報をソースとした内部リスクベクターを評価します。これら追加のベクターのカテゴリーには、マルウェアや不審なプログラム、デュアルユーザーツール、インフラストラクチャの問題などがあります。

- 予期しないサービスの実行
- サポートが終了したソフトウェアの使用
- 脆弱性のあるファームウェアのバージョン
- 健全性の低いシステム
- エンドポイントで確認されたワイヤレスネットワーク
- デュアルホームデバイス
- 異常なコネクション
- 異常な操作/不適切なパスワード構成や監査ポリシー
- ユーザーによる不正な操作
- SSL証明書の問題
- ネットワークのセグメンテーション
- 承認されていないコネクションの確立
- アプリケーションのリスク
- 侵害行為の可能性がある異常な操作
- 一般的なマルウェア、ランサムウェア、トロイの木馬、偽のセキュリティソフト、バックドア攻撃、ウイルス、ダウンローダー、ルートキット、Infostealer、Remnant、ワーム、脆弱性攻撃、ドロッパー、ボットによって感染したエンドポイント
- 悪意をもつ可能性のある汎用プログラム、アドウェア、ゲーム、キー生成ツール、ツールバー、スクリプティングツール、リモートアクセスツール、PUP、ハッキングツール、ポータブルアプリケーションから接触を受けたエンドポイント
- デュアルユーザーツール、リモートアクセスツール、パスワードクラッカー、クラッキングソウトウェア、モニタリングツールから攻撃を受けたエンドポイント

レベル3

カルチャー&プロセス・ビュー

レベル1の外部リスクベクター、レベル2の内部リスクベクターに加え、Verizonによる個別監査の結果をソースとし、カルチャーおよびプロセス面のリスクベクターを追加します。これらのリスクベクターには次のようなものがあります。

- 外部の脆弱性
- IPレピュテーション
- NetFlow
- Webアプリケーション
- 内部の脆弱性
- メールフィルタ
- ファイアウォール
- エンドポイントシステム
- フィッシング
- 物理的な問題
- ポリシー、プロセス、手順
- ワイヤレス

verizon

詳細は、**VerizonEnterprise.com/products/security**をご覧ください。