Cyber Risk Monitoring*

ファクトシート

個々の組織に生じるリスクと組織のセキュリティの状態を、日々更新される情報を活用し、包括的な視点から評価します。実用性の高いデータが利用できるため、セキュリティギャップの問題が解消し、セキュリティのROIが最大限に高まります。

レベル1：アウトサイドインの視点による評価 - 全体の確認を通じて細部を把握する

アウトサイドインの視点による評価では、外部の視点から組織を評価します。BitSightを活用し、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の状態をスコアリングします。また、ベライゾンのUnified Security Portalから、完全自動で日次レポートが配信されます。

- 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、ベライゾンデータ漏洩/侵害調査報告書（DBIR）などを使用

リスクベクター

評価対象のリスクベクターには、BitSightを使用して収集したデータのほか、Recorded Future（RF）やベライゾンデータ漏洩/侵害調査報告書（DBIR）を情報ソースとしたデータがあります。これらベクターのカテゴリーには、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、データの漏洩などがあります。

- 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
- センダーポリシーフレームワーク（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
- ファイル共有
- 公にされた認証情報
- データの漏洩
- ダークWebの脅威インテリジェンス

* 旧称、ベライゾンリスクレポート

レベル2：インサイドアウトの視点による評価 - 企業セキュリティの「MRI検査」を実施する

レベル2のCyber Risk Monitoringでは、エンドポイントやインフラストラクチャ内を自動的にスキャンしてマルウェアや不要なプログラム、重複したツールの有無を確認する内部評価を行います。これにより、さらに踏み込んでセキュリティの状態をスコアリングすることができます。

- レベル1のデータに加え、組織の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の状態を評価し、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

リスクベクター

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、マルウェアや不要なプログラム、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
- サポートがすでに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/不適切な構成のパスワードや監査ポリシー
- ユーザーの操作ミス
- 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
- 次の攻撃を受けたエンドポイント：一般的なマルウェア、ランサムウェア、トロイの木馬、偽のアンチウイルスソフト、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
- 次の攻撃を受けたエンドポイント：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
- 次の攻撃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

verizon

レベル3：包括的な視点による評価 - カルチャーおよびプロセスの視点による評価を行う

外部と内部のリスク要因の評価に加え、組織内部のセキュリティカルチャーやセキュリティ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。カルチャーとプロセスの評価では、複数の自動ツールを使用するほか、人間の目による確認も行い、包括的な視点から分析を実施して、セキュリティとリスクの状態を評価します。

- アクティビティ、カルチャー、プロセス、ポリシーを考慮して、レベル1とレベル2のデータにキャップストーンを付加
- プロフェッショナルサービスを通じ、セキュリティの強化に向けたサポートを100時間まで提供
- 360度のあらゆる視点からセキュリティの状態を評価

リスクベクター

レベル1の外部リスクベクターとレベル2の内部リスクベクターに加え、ベライゾンの個別監査による情報をソースとしたカルチャーとプロセスのリスクベクターを評価します。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
- メールフィルター
- 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
- 物理レベルのチェック
- ポリシー、プロセス、手順
- ワイヤレス

Vendor Risk Dashboard

今日のデジタルエンタープライズでは、アウトソーシングテクノロジーやクラウドベーステクノロジーの普及に伴い、サードパーティと接触する機会が増えています。そのような機会の増加はいずれの場合も組織に一定水準のリスクをもたらします。結局のところ、組織のセキュリティは、その最も弱い部分のレベルに左右されます。取引先ベンダーのいずれかで侵害が発生した場合、重要な資産データや顧客情報が漏洩するおそれがあり、そうなると、自社のブランドイメージや評判が損なわれ、事業にリスクが生じかねません。

Vendor Risk Dashboardでは、取引先となるベンダーやパートナーのセキュリティの状況を監視することができます。実用性の高いカスタムのインテリジェンスやリスクレーティングの機能を通じ、契約先のサードパーティのセキュリティリスクの状態を包括的に把握することが可能です。

また、タイムリーな通知が行われるため、潜在的な問題をプロアクティブに把握でき、リソースを適切に割り当てられ、サプライチェーンと協力して危険性の高い脅威に対処可能です。提供されるレポートは、合併や買収に関係するセキュリティリスクを評価したり、リスクエクスポージャーやセキュリティ対応戦略の有効性を適切に把握したりするうえでも役立ちます。

このダッシュボードは、脅威のレベルやセキュリティのレーティングを取引先ベンダーの業種に合わせてカスタマイズしてから使用できます。カスタムのベンダーグループを作成したり、特定の脅威ベクターを優先的に確認したりできるほか、複数のグラフを使用し、すべてのベンダーおよびベンダーグループのスコアをまとめて表示することも可能です。

ポートフォリオ管理

ポートフォリオ管理は、アドオンのサービスです。このサービスでは、系列会社のような法律上関連性のある事業主体のセキュリティの状況をエグゼクティブサマリーのかたちで確認できます。また、ドリルダウンの機能を使えば、詳細な情報を表示することも可能です。また、ログアウトをしなくても表示対象の事業主体を簡単に切り替えることができるので、ポートフォリオをすばやくスキャンできます。Portfolio Dashboardでは、ポートフォリオセキュリティの全体の状況や脅威レベルのスコアリングを反映したさまざまなチャートを確認できます。一方、Manage Portfolioビューを使用すれば、系列会社のセキュリティの状態を階層的に一覧表示することが可能です。

詳細情報

Cyber Risk Monitoringを活用すれば、セキュリティ戦略の策定と評価のプロセスを強化できます。詳細は、
https://enterprise.verizon.com/ja-jp/products/security/cyber-risk-monitoring/