本当の評価はできていますか？ ～それ、攻撃者は知っています～

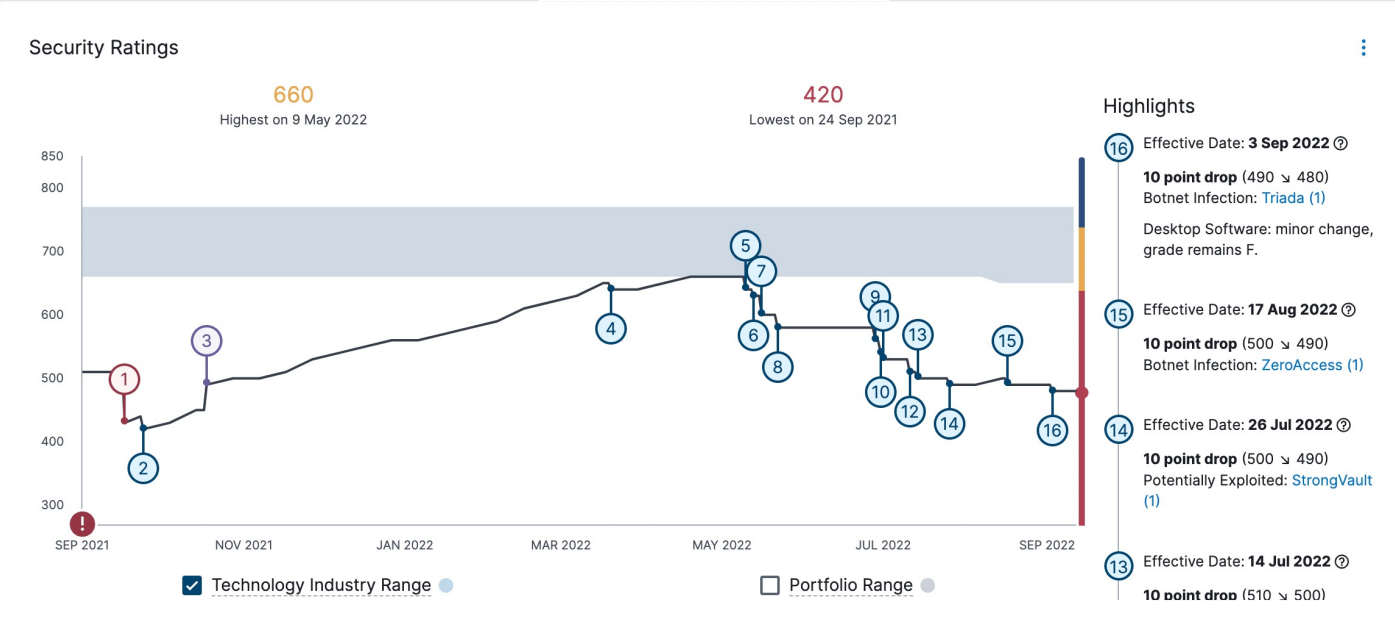
サイバーセキュリティリスク評価支援サービス
Powered by BitSight

攻撃者は知っています！貴社のセキュリティリスクを

◆ 求められるこれからのサイバーセキュリティリスク評価

- ✓ 攻撃者と同じように、外部から客観的に自組織のセキュリティ対応度合いを把握
- ✓ 脆弱性対応漏れや甘い設定を速やかに把握し対応につなげる
- ✓ シャドー IT などセキュリティチームの認識外の環境を把握
- ✓ 取引先やサプライチェーンも同じようにセキュリティ対策状況を把握

BITSIGHT®
The Standard in SECURITY RATINGS



◆ BitSight の 4 つのポイント

種々の観点による「外から見た」可視化

各種リスクベクターによる OSINT ベースの可視化を行う。調査はデイリーベースで行われるため、いち早く、継続的に評価・監視できる。

サプライチェーンも可視化

取引先などの対応状況も「外から見た」状態を可視化。サプライチェーンリスク対策に活用。新規取引先や M&A 予定企業などへのチェックにも活用可能。

各種レポートでの分析

業界分析、Peer to Peer 分析等、経営的視点で自組織を分析し、今後のセキュリティ戦略立案の指標として活用可能。

継続的かつ網羅的な可視化

継続的な監視により状態変化を常に把握できる。対象となる組織に関連すると思われるネットワークやドメインを網羅的にチェックする。システム増減考慮不要。

◆ パロンゴアドバイザリーサービス

エキスパートによる対応方針アドバイス

- 業界経験 25 年以上のエキスパートによる、評価結果のレビューから改善方針に対するアドバイス
- 重要度、優先度の選定を効率的かつ確実に行うことで、より効果的なセキュリティ施策実現をサポート

株式会社パロンゴ：https://www.parongo.com　email：info@parongo.com

◆ サイバーセキュリティリスク評価/管理の重要性と求められる対策
～ 客観的データに基づいた評価による、経営リスクへの対策強化へ ～

“サイバー攻撃 = 経営リスク” と捉える必要がある

- 把握していないシステム環境からのサイバー攻撃
- サプライチェーンへのサイバー攻撃

工場停止や決算の遅延など、事業継続停止につながる事案も既に発生

経済産業省からも、2020 年 12 月に“最近のサイバー攻撃の状況を踏まえ、経営者の皆様へサイバーセキュリティの取組の強化に関する注意喚起”がなされています。

※ 経済産業省による経営者向け注意喚起
https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

経営リスク対策強化に求められる対策

01 データに基づく把握
外からどのように見えているのか、データに基づく客観的なサイバー防衛力の把握

02 サイバー防衛力強化
脆弱性対応の抜け漏れ排除や通信ポート設定の甘さチェックなど、気付きにくいポイントを強化

03 長期的な監視・経過観察
事業継続性を維持するためにも脆弱性に対する適切な対応と運用ができているか常に把握

04 サプライチェーンリスク対策
自社だけでなく、取引先やグループ会社、M&A 予定企業等含めてリスクを把握

◆ サイバーセキュリティリスクを把握するためのポイント

客観的か?

データに基づき、客観的に評価し、セキュリティ観点の通信簿として可視化

- リスクを最小限に抑えつつ、優先的に実施すべきセキュリティ対策の棚卸しが可能
- セキュリティ対策立案や予算策定に活用が可能

継続的か?

適切な設定や運用を継続的かつ長期的に可視化

- 日々発生するするサイバー攻撃や新たな脆弱性への適応状況把握が可能
- セキュリティ部門や IT システム部門の KPI として活用することも可能

網羅的か?

自組織のシステム環境や取引先を網羅的に可視化

- シャドー IT、海外支社、グループ会社等のシステム環境までセキュリティ達成度の可視化が可能
- サプライチェーンリスクも可視化可能

BitSight なら可能です！

BitSight を導入することにより、経営リスクまで鑑みたセキュリティリスク評価/管理が可能です

客観的
2,000億件以上のデータをデイリーで収集し分析・調査。世界最大規模のシンクホールも運用しデータを活用。

継続的
継続したモニタリングにより、日々変化し得るリスクもキャッチアップ。

網羅的
OSINT 等から、自組織全般のシステム環境だけでなくサプライチェーンまでの可視化を提供。

セキュリティ効果測定として、 ISO/IEC 27001、CIS Controls、NIST CSFへのマッピングが可能

株式会社パロンゴ：https://www.parongo.com　email：info@parongo.com