サイバーリスクを客観的に把握するためのベストプラクティスとは？

～ サイバーセキュリティ評価支援サービスのご紹介

株式会社パロンゴ 代表取締役社長 近藤学

通知簿

通知簿

↓

ASM: Attack Surface Management
(アタックサーフェスマネージメント)

いつものアイスブレイク

部下がちゃんとやってる(はず)
業者がやってる(はず)
全ての設備は把握している(はず)
Excel シートに全部○ついてるからちゃんと
やってる(はず)

このサーバがあることはうちの人間しか知らない(はず)
Firewall があるから大丈夫(なはず)
アンチウイルス製品いれたから大丈夫(なはず)
外部とは通信しない環境だから大丈夫(なはず)
新環境使ってて古い環境使ってないので大丈夫(なはず)

この春に脆弱性診断受けたから今も大丈夫(なはず)
うちには取られるようなものないから大丈夫(なはず)
うちよりももっと大きな企業さんが攻撃される(はず)
パソコンが数台感染してもなんとかなる(はず)
取引先とはシステム接続してないのでリスクはない(はず)

感想・希望・期待

攻撃者は皆さんの都合や気持ちに合わせて
攻撃するわけじゃないですよ？

謙虚・客観

通知簿

サイバーセキュリティリスクに関する「通知簿」

企業のセキュリティリスク状況を OSINT(※) 等をベースに可視化

※合法かつ一般的に入手可能な情報を用い、事象を深く分析する手法

感染を示唆する情報はないか？
放置されている脆弱性はないか？
開いてるとまずいポートはないか？
などなど…

(余談)「勝手にうちを調べたのか!!」

企業のセキュリティリスク状況を OSINT(※) 等をベースに可視化

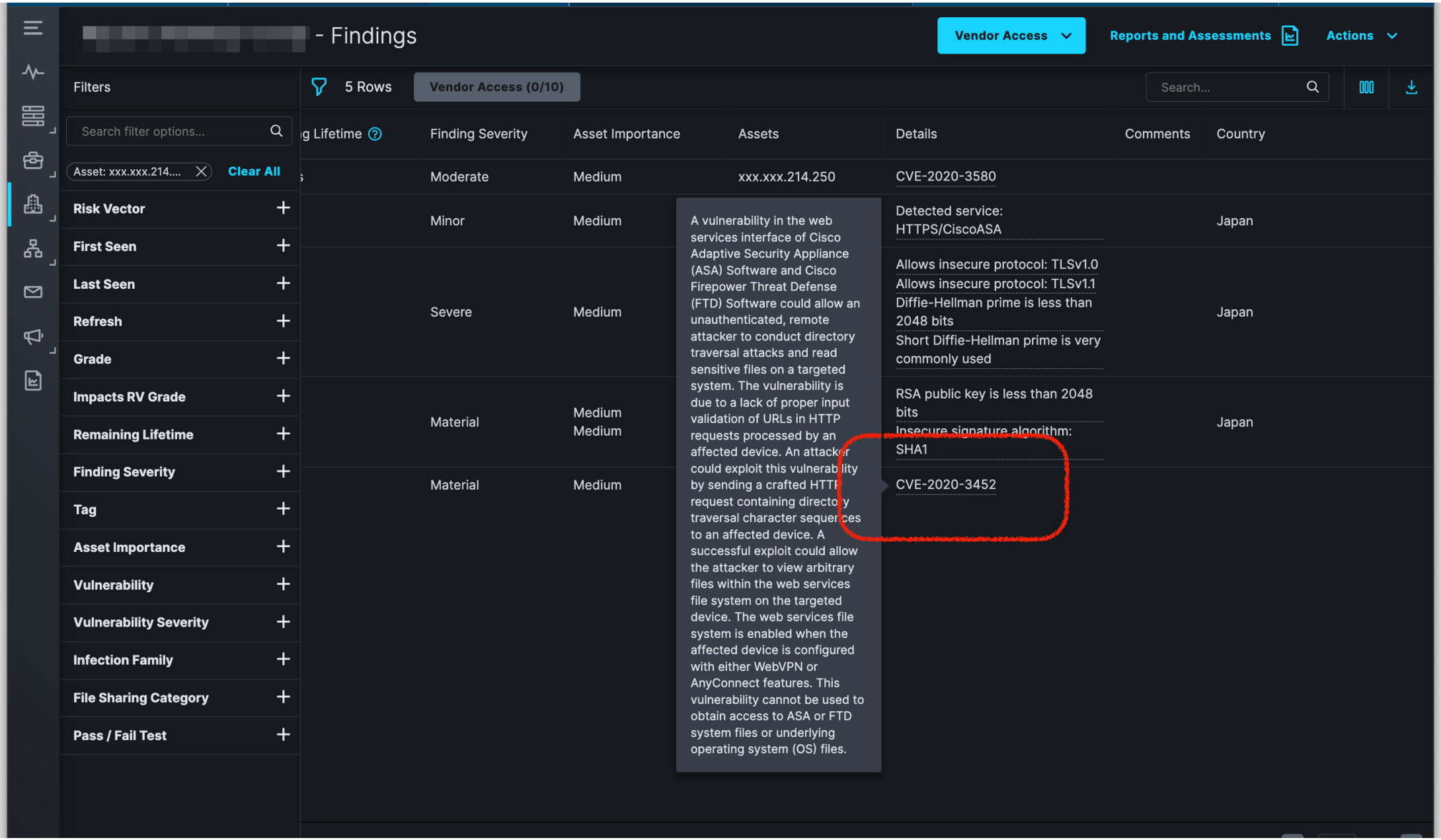
※合法かつ一般的に入手可能な情報を用い、事象を深く分析する手法

ちゃんとできているかを
客観的・継続的・網羅的に
確認しよう

他社の「通知簿」も!

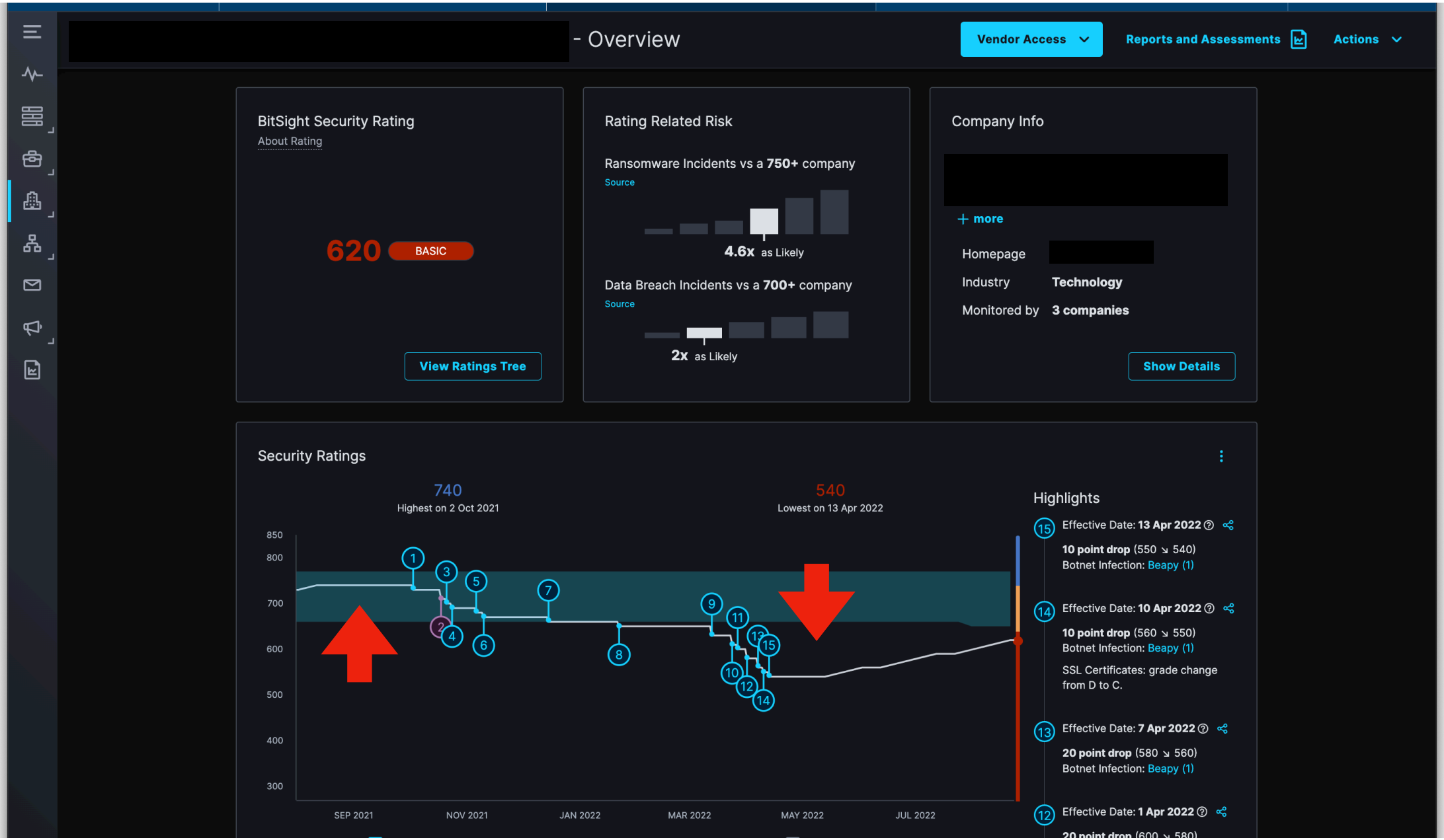
サプライチェーンリスクへの備え

実例:Firewall の脆弱性が放置されているケース


- Findings
Vendor Access
Reports and Assessments
Actions
Filters
5 Rows
Vendor Access (0/10)
Search...
Search filter options...
Asset: xxx.xxx.214....
Clear All
Risk Vector
First Seen
Last Seen
Refresh
Grade
Impacts RV Grade
Remaining Lifetime
Finding Severity
Tag
Asset Importance
Vulnerability
Vulnerability Severity
Infection Family
File Sharing Category
Pass / Fail Test
g Lifetime
Finding Severity
Asset Importance
Assets
Details
Comments
Country
Moderate
Medium
xxx.xxx.214.250
CVE-2020-3580
Minor
Medium
Detected service: HTTPS/CiscoASA
Japan
Severe
Medium
Allows insecure protocol: TLSv1.0
Allows insecure protocol: TLSv1.1
Diffie-Hellman prime is less than 2048 bits
Short Diffie-Hellman prime is very commonly used
Japan
Material
Medium
Medium
RSA public key is less than 2048 bits
Insecure signature algorithm: SHA1
Japan
Material
Medium
CVE-2020-3452
A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files.

いくら高価で高性能な
ソリューションを入れたって
こんな有様じゃ…

~~年一とかで見ておけばいいんじゃないの？~~


[redacted] - Overview
Vendor Access
Reports and Assessments
Actions
BitSight Security Rating
About Rating
620
BASIC
View Ratings Tree
Rating Related Risk
Ransomware Incidents vs a 750+ company
Source
4.6x as Likely
Data Breach Incidents vs a 700+ company
Source
2x as Likely
Company Info
[redacted]
+ more
Homepage [redacted]
Industry Technology
Monitored by 3 companies
Show Details
Security Ratings
740
Highest on 2 Oct 2021
540
Lowest on 13 Apr 2022
850
800
700
600
500
400
300
SEP 2021
NOV 2021
JAN 2022
MAR 2022
MAY 2022
JUL 2022
Highlights
15 Effective Date: 13 Apr 2022
10 point drop (550 ↘ 540)
Botnet Infection: Beapy (1)
14 Effective Date: 10 Apr 2022
10 point drop (560 ↘ 550)
Botnet Infection: Beapy (1)
SSL Certificates: grade change from D to C.
13 Effective Date: 7 Apr 2022
20 point drop (580 ↘ 560)
Botnet Infection: Beapy (1)
12 Effective Date: 1 Apr 2022

皆様の会社は大丈夫ですか？

お取引先は大丈夫ですか？

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

～ 企業のサイバーセキュリティリスクを可視化 ～

セキュリティ対応度合いを評価し、可視化

セキュリティ対策が適切に設定・運用できているかを外部から得られる情報にて監視・観察し、客観的にセキュリティ対策の抜け、漏れ、陳腐化を「通信簿」的に評価、ドリルダウンすることが可能。

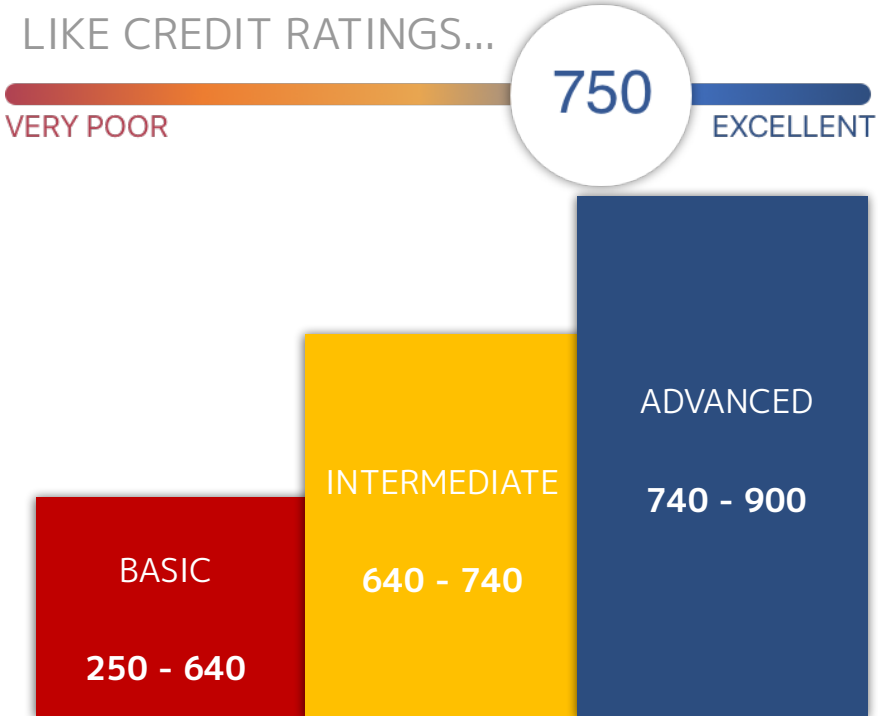
サプライチェーンリスクも可視化

自社のみならず、取引先や M&A 先にまでセキュリティ対応度合い評価の対象を広げることができるため、取引先等に対するサイバーセキュリティ的サプライチェーンリスクも明確化。

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までもパッケージ化。

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。

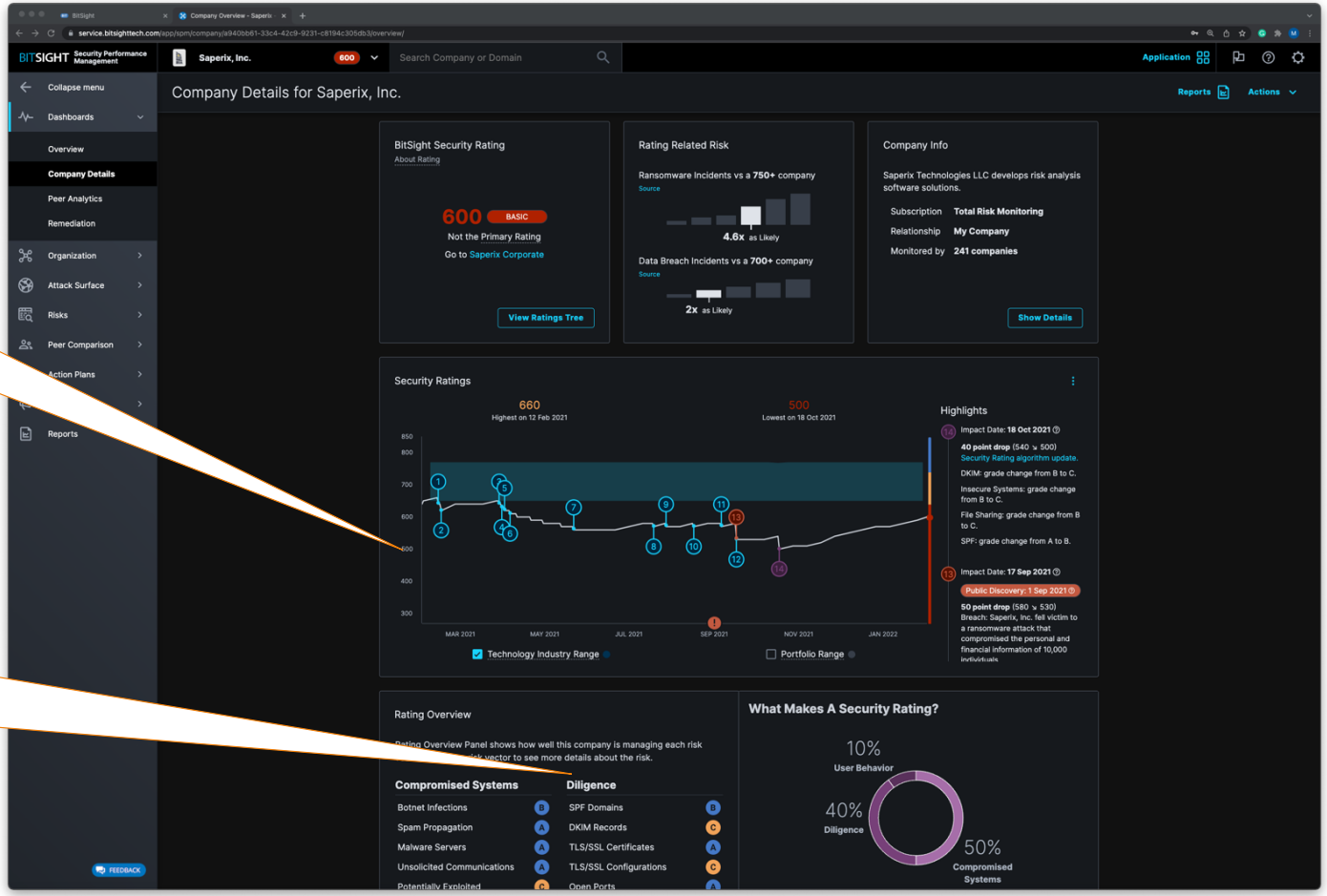


BitSight ダッシュボード

セキュリティ対応状況やリスクの詳細を一元管理し詳細まで可視化

スコアの変動を時系列で確認。
過去 1 年間の動きをチェックできる。

評価項目毎のグレードを表示。
どこができていてどこに問題があるのかが一目瞭然。

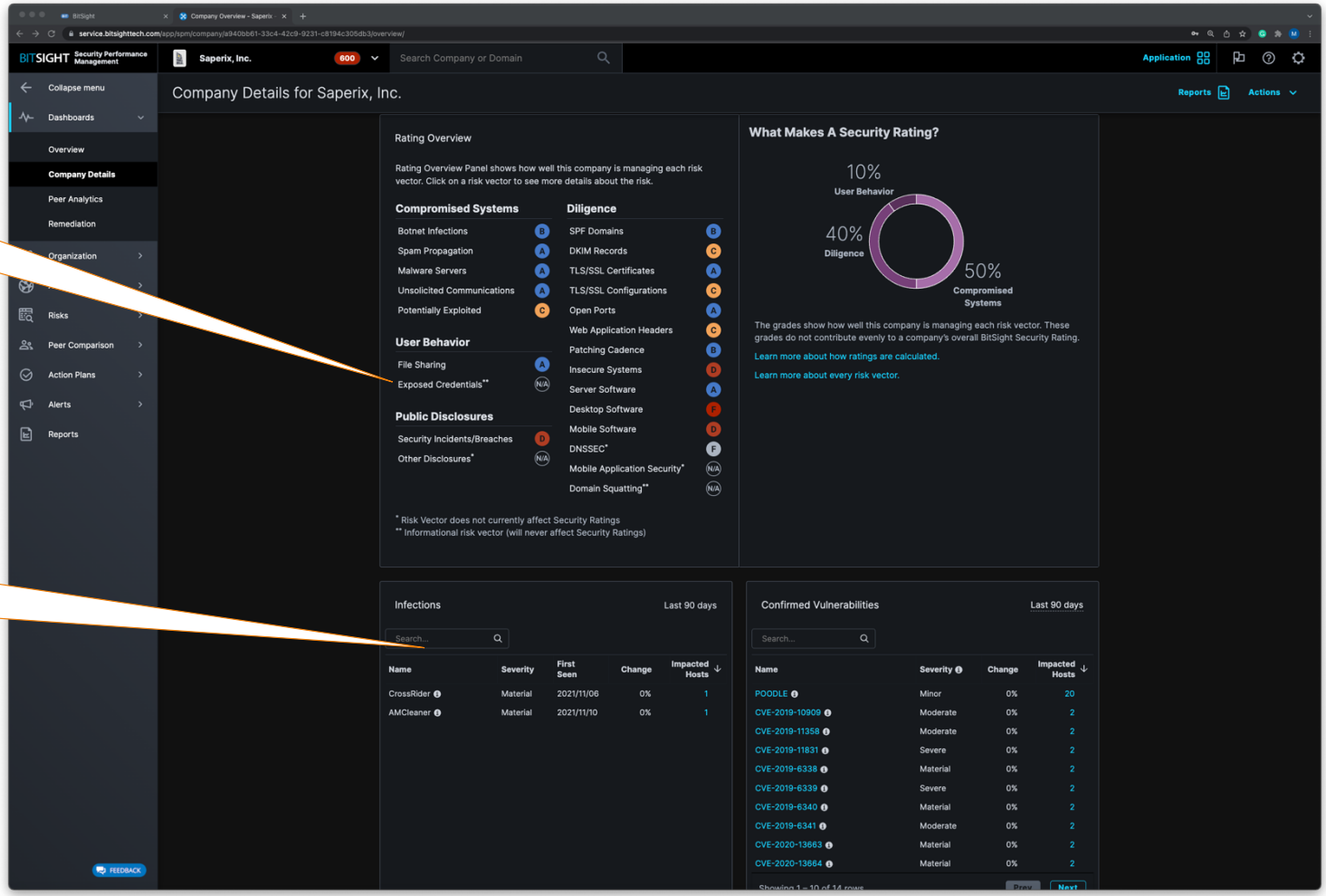


BitSight ダッシュボード

セキュリティ対応状況やリスクの詳細を一元管理し詳細まで可視化

評価項目毎に A (良) ～ F (悪) でグレード付け。

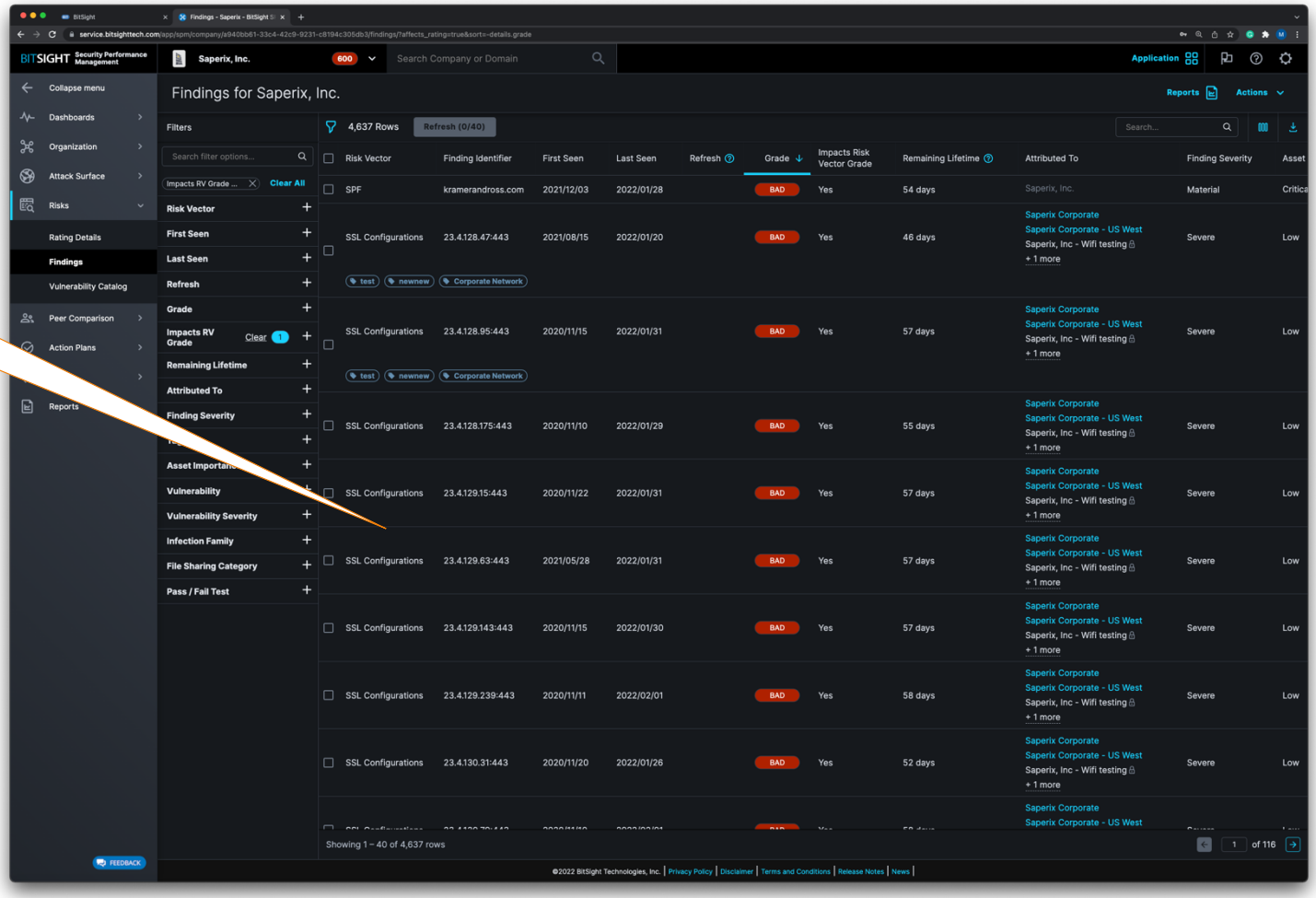
マルウェアへの感染状況や、放置されている脆弱性の一覧なども確認可能。



BitSight ダッシュボード

セキュリティ対応状況やリスクの詳細を一元管理し詳細まで可視化

良くない結果の詳細をドリルダウンして表示。
どこの何が悪いのかを深くチェックすることが可能。



ちゃんとできているかを
客観的・継続的・網羅的に
確認しよう

ASM: Attack Surface Management

「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました

2023年5月29日

▶ 安全・安心

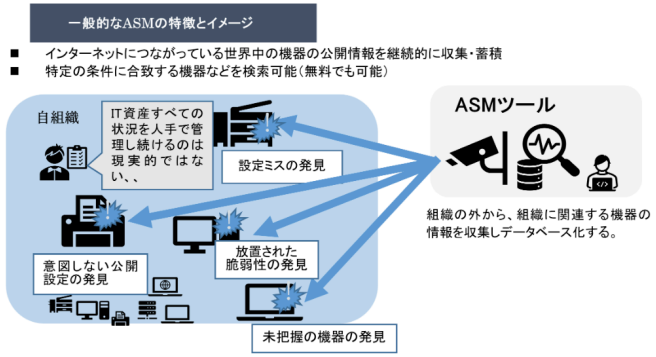
経済産業省は、サイバー攻撃から自社のIT資産を守るための手法として注目されている「ASM（Attack Surface Management）」について、自社のセキュリティ戦略に組み込んで適切に活用してもらえるよう、ASMの基本的な考え方や特徴、留意点などの基本情報とともに取組事例などを紹介した、「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を作成しました。

1．背景、趣旨

デジタルトランスフォーメーション（DX：Digital Transformation）が進展する中、クラウド利用の拡大に加え、民間事業者が所有するIT資産が増加、点在するとともに、コロナ禍によるテレワークの拡大等を通じて、社会全体でリモート化が進められました。これらにより、サイバー攻撃の起点が増加しています。

こうしたサイバー脅威に対して、自社が保有するIT資産を適切に管理しリスクを洗い出すことが求められますが、人手を介した管理の下では、システム管理部門の把握しきれないシステムが生じやすく、機器の実際の設定も見えづらいことなどから、自社の全てのIT資産を管理するのは必ずしも容易ではありません。一方で、IT資産について、外部（インターネット）から把握できる情報を用いた管理サービスを利用することで、既存の管理方法を補完することが可能となっていることから、このような管理サービスの提供が広がっています。

そこで、外部（インターネット）から把握できる情報を用いてIT資産の適切な管理を可能とするツールやサービスを活用して、外部（インターネット）に公開されているサーバやネットワーク機器、IoT機器の情報を収集・分析することにより、不正侵入経路となりうるポイントを把握するASM（Attack Surface Management）について、民間事業者における利用の実態を明らかにし、ASMに関連する各種ツールやサービスの特徴や活用方法について整理し、ガイダンスとして取りまとめました。



自分たちが実際はどう見えているのか
どういう状態にあるのかを
常に分析し、確認しておくことが
「想定外」を極力少なくする
第一歩ではないでしょうか？

お問い合わせ:
info@parongo.com