ULTRA REDご紹介

KELA株式会社

ULTRA RED とは

ULTRARED

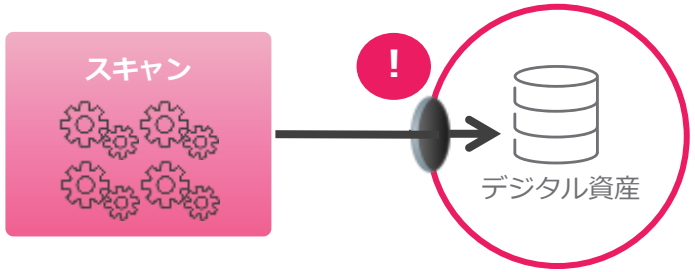
な　　チームが攻撃機会の検出を自動化

（攻撃担当チーム）

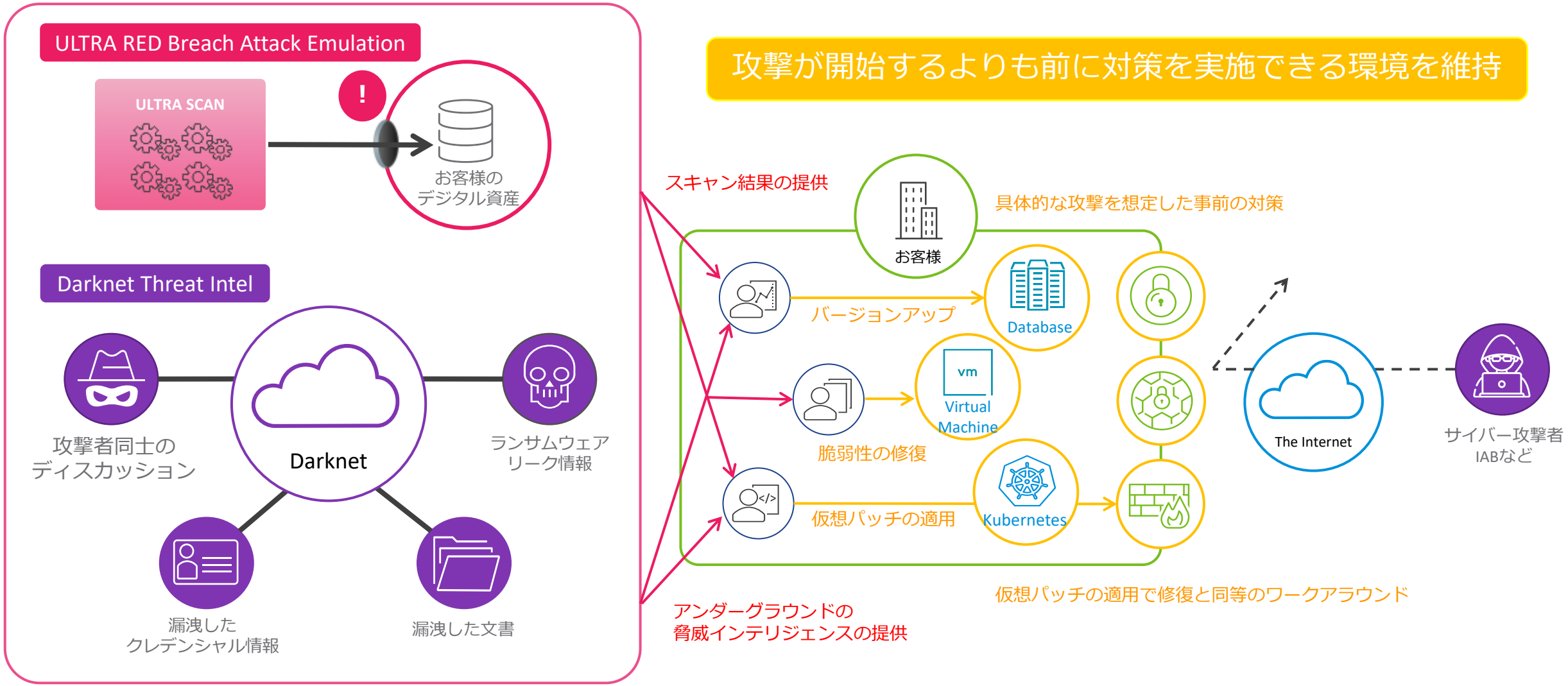
ダークウェブの情報を
積極的に活用

サイバー戦争の諜報機関で
培った技術と経験

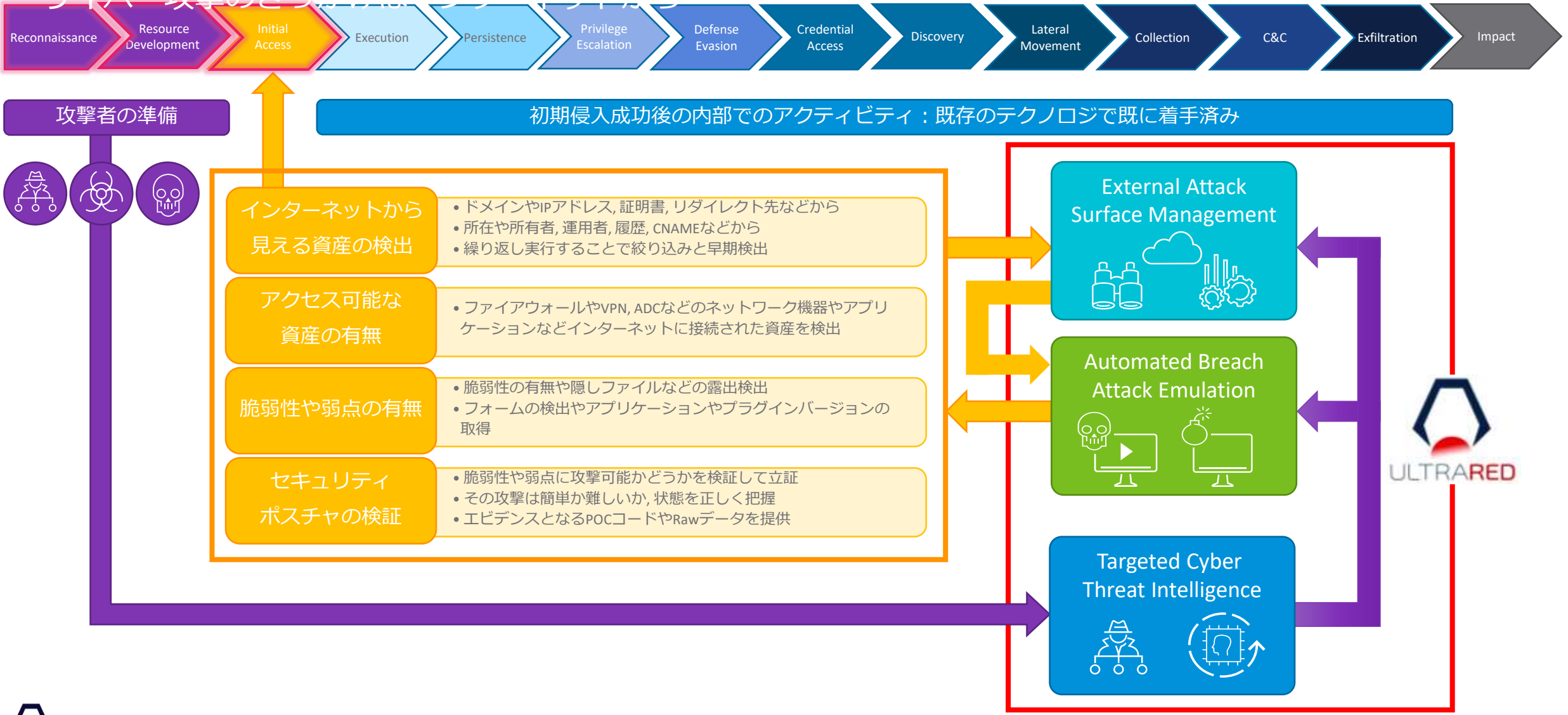
これらの情報と技術を組み合わせて
自組織の攻撃機会を検出



ULTRA REDのアクティブディフェンス



ULTRA REDのディフェンスポイント



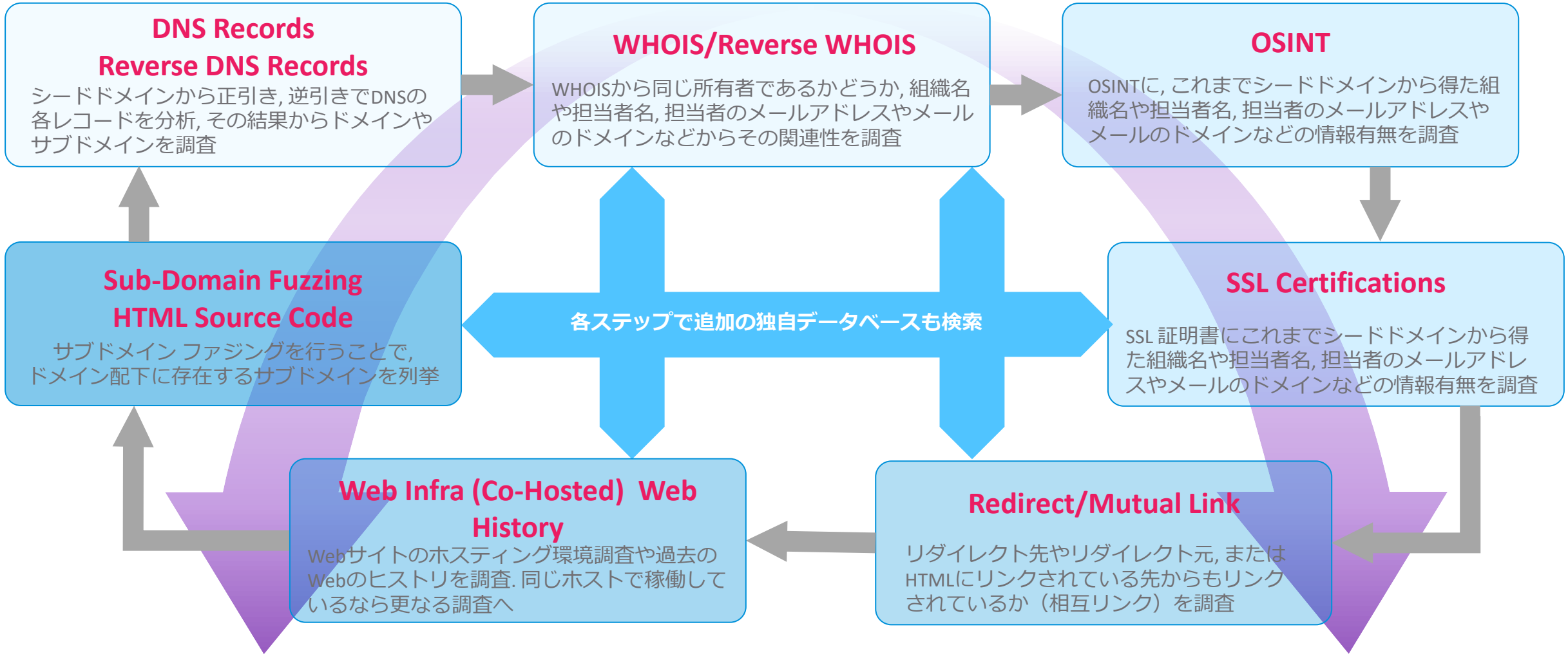
ULTRA RED CTEMプラットフォーム概要

セキュリティ ポスチャから優先度付け	✓ **ダークウェブ**の脅威情報やCVEの**EPSS**, OWASPの**Likelihood**との自動マッピング ✓ 攻撃機会の悪用**難易度**や**複雑性**, 必要な**特権レベル**, **ユーザー関与**必要性などから優先付け
検出した攻撃機会を多角的に調査・立証	✓ エミュレーションによって**多角的に立証**, その状態からトリアージのための優先順位付け ✓ ダイナミック・パラメータ, ダイナミック・ペイロードによる**動的な繰り返し検証**
毎日実行する攻撃機会の検出	✓ 空きポート確認, 最新バージョンの有無検出, デジタル証明書の不備検出など ✓ 設定ミスによる情報の露出, 露出している**情報の重要度チェック**, 脆弱性有無の**可能性**, シグネチャによる脆弱性の存在有無の検証, 疑わしい攻撃機会を多角的調査の候補に列挙
再帰的ドメイン・アセットディスカバリ	✓ シードドメインから, 関連ドメインや関連アセットを**繰り返しディスカバリ** ✓ 関連会社や買収などによる統廃合による**未把握のドメインやデジタル資産などを広く検出** ✓ モニターしておくことで, 検出時には**自動的にアセットスキャンの実行**可能

エージェントレス　アセットへの影響なし　ALL in ONE

SaaSで提供するULTRA REDのプラットフォーム

再起的ドメイン・アセットパッシブディスカバリ



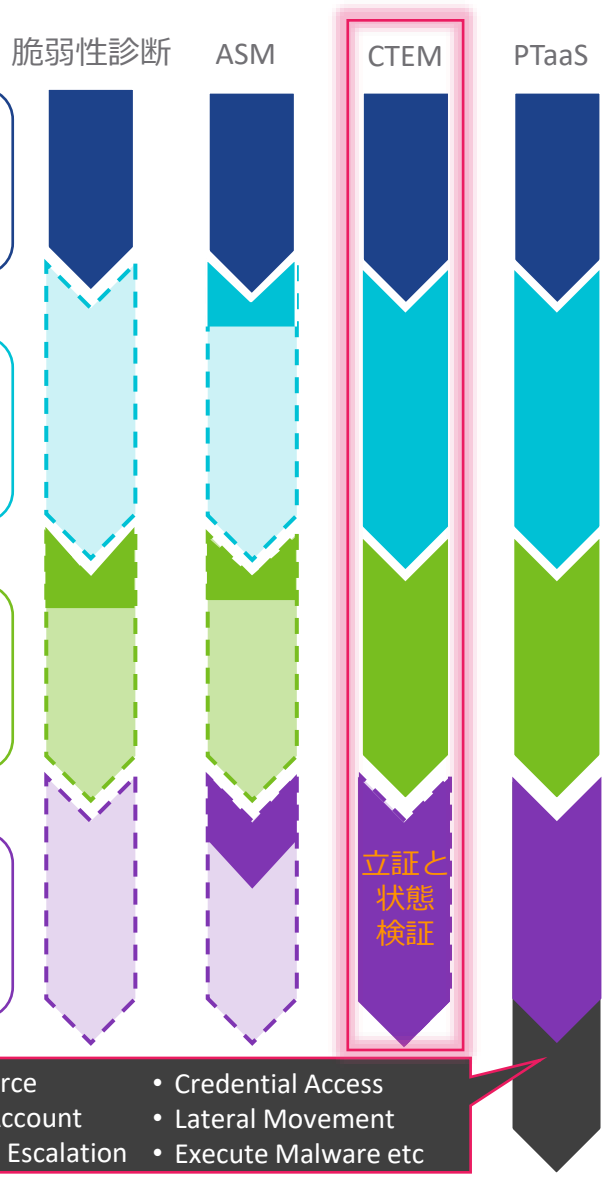
脆弱性悪用の可能性に関するエスカレーション

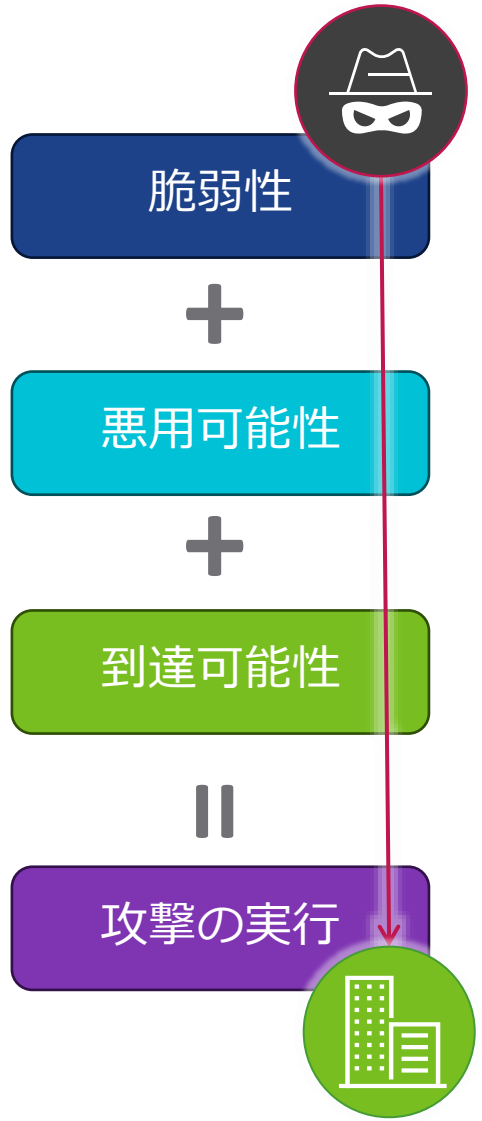
可能性
- 共通脆弱性識別子「CVE」の存在
- 共通脆弱性評価システム「CVSS」のスコア

蓋然性
- その可能性が悪用できるのかどうかの確実性の度合いを計測
- 「シナリオの現実性」「難易度」「想定被害内容」
- 「PoCコードの有無」「詳細情報公表の有無／予定」など

実態確認
- 脆弱性に対するスキャンや攻撃の試行
- 国内外, 業界での悪用事例の有無
- ダークネット上の情報や攻撃トレンドの有無

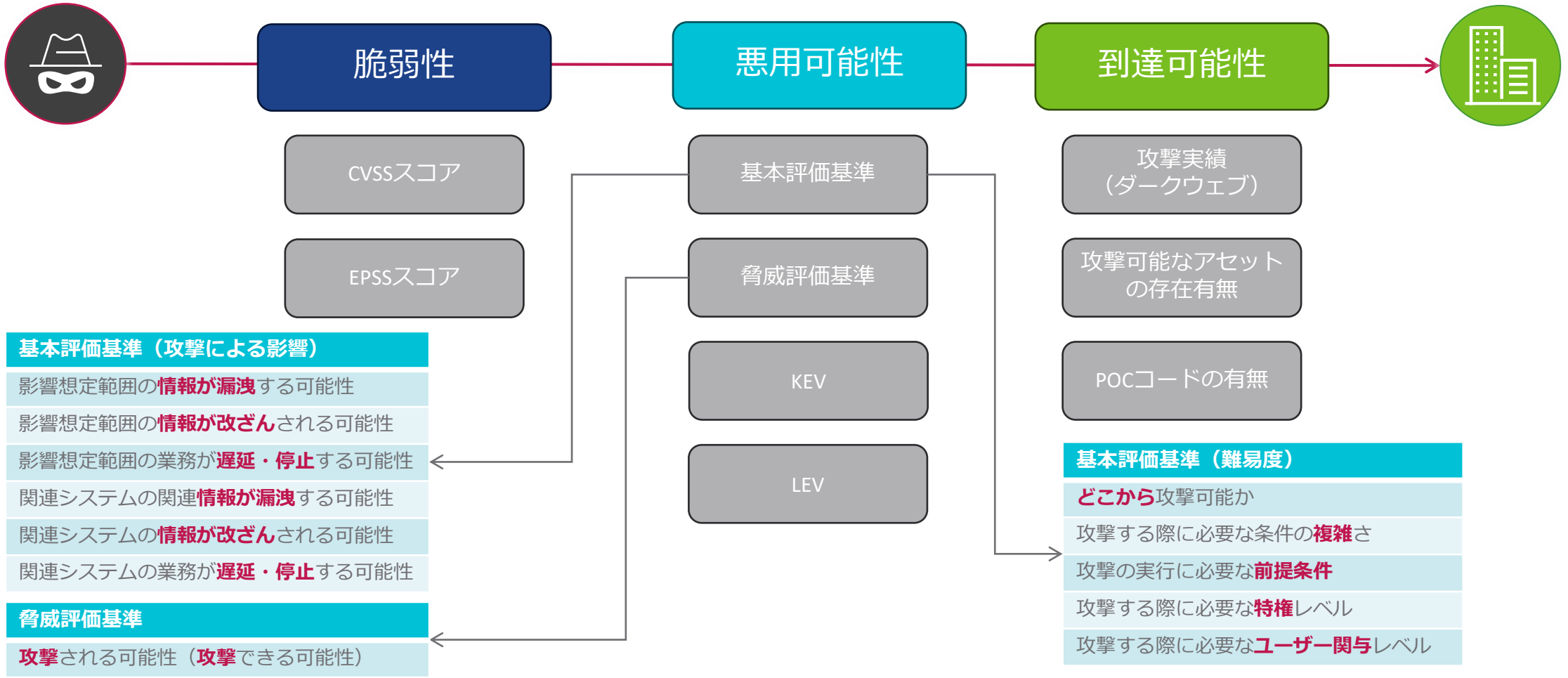
攻撃実行
- 攻撃の実行
- MITRE ATT&CKのInitial Accessから, Exfiltrationまで実行





ASM : Attack Surface Management
CTEM: Continuous Threat Exposure Management
PTaaS : Penetration Test as a Service

攻撃者は何を考えるか



存在する脆弱性をリストするだけでは優先度づけするには不十分

攻撃機会の検出, ダイナミックな多角的調査による立証

攻撃ベクターは？

悪用するためにログイン必要？

ユーザーのクリック必要？

悪用するのは複雑な手順必要？

やられたらシステム落とせる？

悪用するために特権レベル必要？

やられたらデータはどこまで露出？

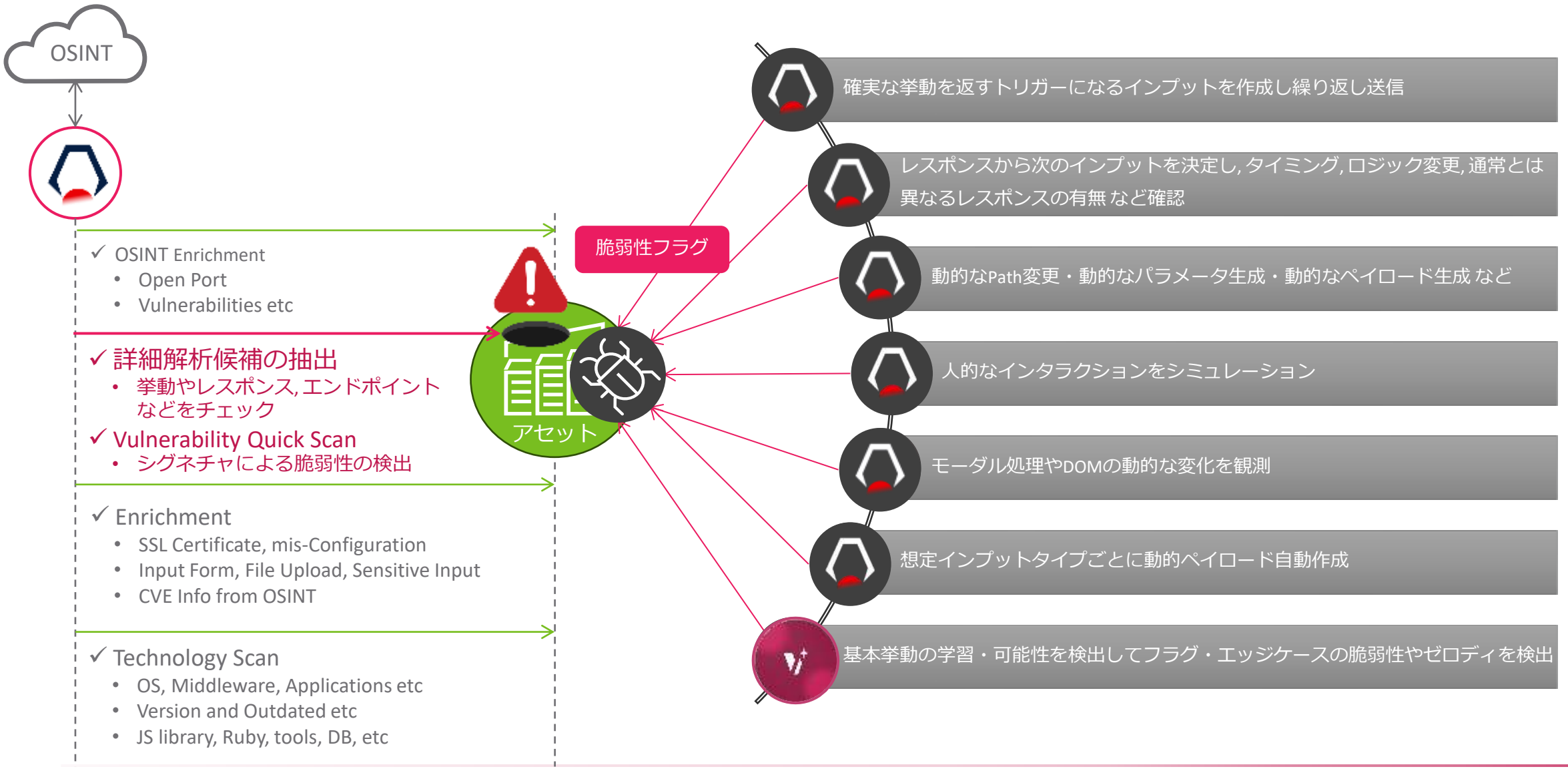
やられたら改ざんまで可能？

ブラインドベースは大丈夫？

複数の攻撃機会の組み合わせは？

該当アセットはCIAのどれが重要？

攻撃機会の検出, ダイナミックな多角的調査による立証



スキャンレベルのイメージ

	一般的な自動化された 攻撃対象領域の検証と可視化	一般的な手動での 攻撃対象領域の検証と可視化	攻撃者や攻撃技術の可視化 手動解析・研究	高精度な攻撃対象領域の 自動検証と可視化

3-Level Deep ：フルスキャン（例: 専門知識を持ったULTRA REDのRed Teamによる攻撃機会の詳細解析のレベル）

Level 2 Deepまでの全てのスキャンを網羅することに加え, Nmapのトップ1,000ポートを対象に, 高度なペイロードの変異およびパス・パラメータのファジングを用いたより深いクロールを行い, さらに多くの脆弱性（例：BAC, キャッシュポイズニング, CSRF, リクエストスマグリング, (Blind Based) SQLi, SSRF, SSTI, XSS）を検出します.
スキャン対象ポート - 上記のすべてに加え, 常時Nmapのトップ1,000ポート*1を対象*2にしている.

2-Level Deep ：高度なスキャン（例: ペネトレーションテストレベルのイメージ）

Level 1 Deepのすべてに加え, 独自に開発された検出メカニズムに基づく脆弱性を検出します. これには, カスタマイズされたペイロード, パス, パラメータ（例：隠された graphql/wsdl/swagger/asp.net API エンドポイントの検索）が利用されます.
スキャン対象ポート – Level 1 Deepのすべてに加え, OSINT 経由で開いていると報告されたポートがない場合は, Nmap のトップ 1,000 ポート*1を対象にします.

1-Level Deep ：基本スキャン（例: Technology Scan, 簡易なシグネチャベースの脆弱性検出など）

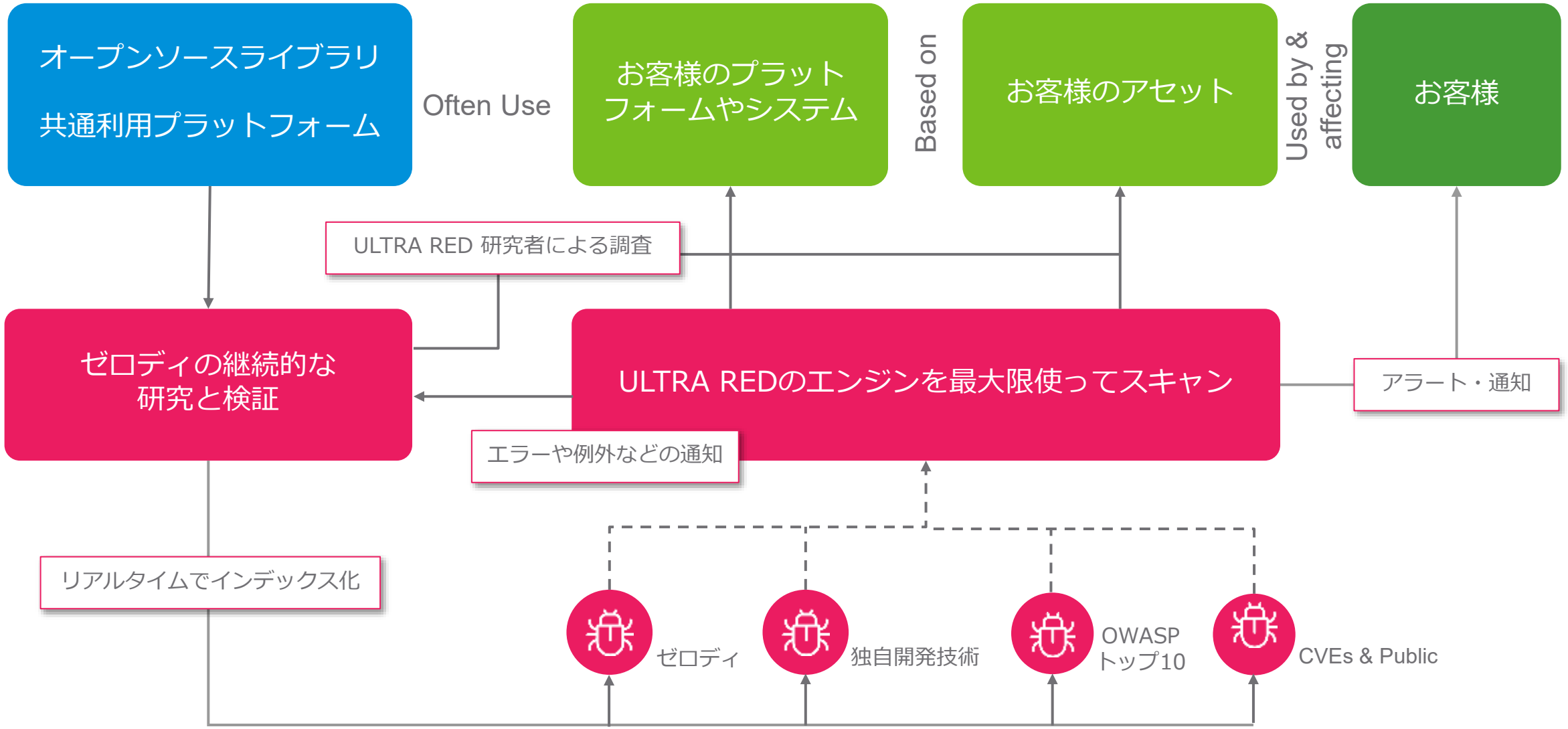
サポートされている CVE, SMTP の設定ミスによる脆弱性, サブドメイン乗っ取りの脆弱性, および一般的な情報漏洩の脆弱性（例：公開された phpinfo）を含みます.
スキャン対象ポート – 80, 443, OSINT により開いていると報告されたポート, および各 CVE に記載されているポートが対象.

0-Level Deep （例: DNS, WHOIS, nmap, SHODANなどからの情報を取得）

完全パッシブスキャン. OSINT/オープンソースの情報から空きポートの検出,
アプリケーションやプラグイン, それらのバージョン情報収集など
脆弱性情報はEnrichmentに”Unvalidated CVE”として記載

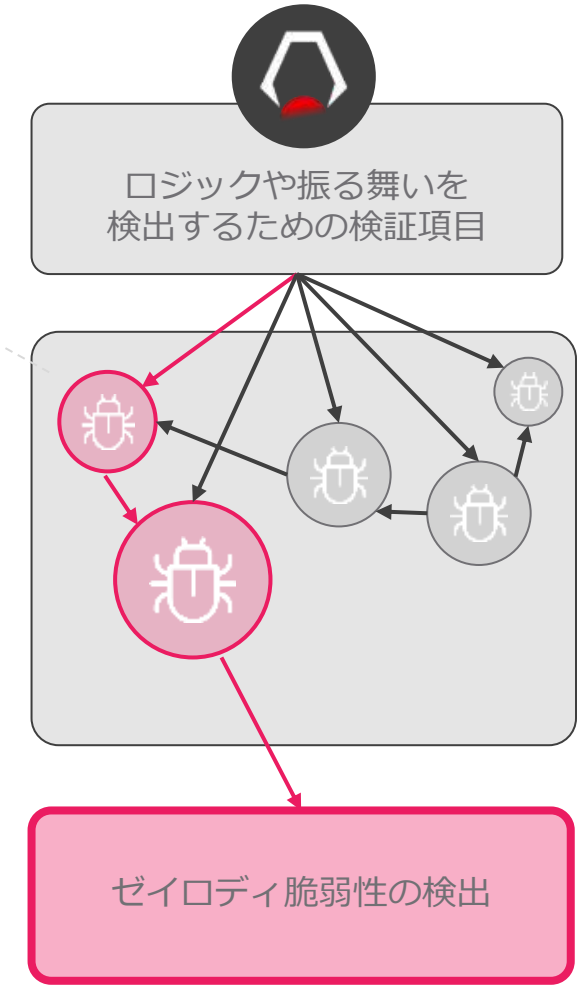
*1 Nmap top 1000 ports:
https://nullsec.us/top-1-000-tcp-and-udp-ports-nmap-default/
*2 今後, 独自に前提した1,400ポートに移行予定

スキャナーの継続強化サイクル



ゼロディ脆弱性の検出が可能

- 影響のあるプラットフォームの特徴
  - ✓ 確実になんらかの振る舞いを行う
  - ✓ その特徴ある振る舞いは, 意図していないか, 型にはまらない方法でエクスプロイトが可能
- 検出方法
  - ✓ シグネチャを利用した一つのサービスベースに対するスキャン方法では立証できない
  - ✓ 複数の技術と実行タイミングの組み合わせ
  - ✓ 反復検証と結果の比較
  - ✓ レスポンスによって動的に次の検証を自動的に選択
  - ✓ 繰り返し実施することでゼロディを検出



AI Scanner - 新たな検出ロジック

アセットの情報と
多角的攻撃機会検証の結果

OSINT

NIST NVD
CISA KEV etc

Threat Intelligence
under the Ground

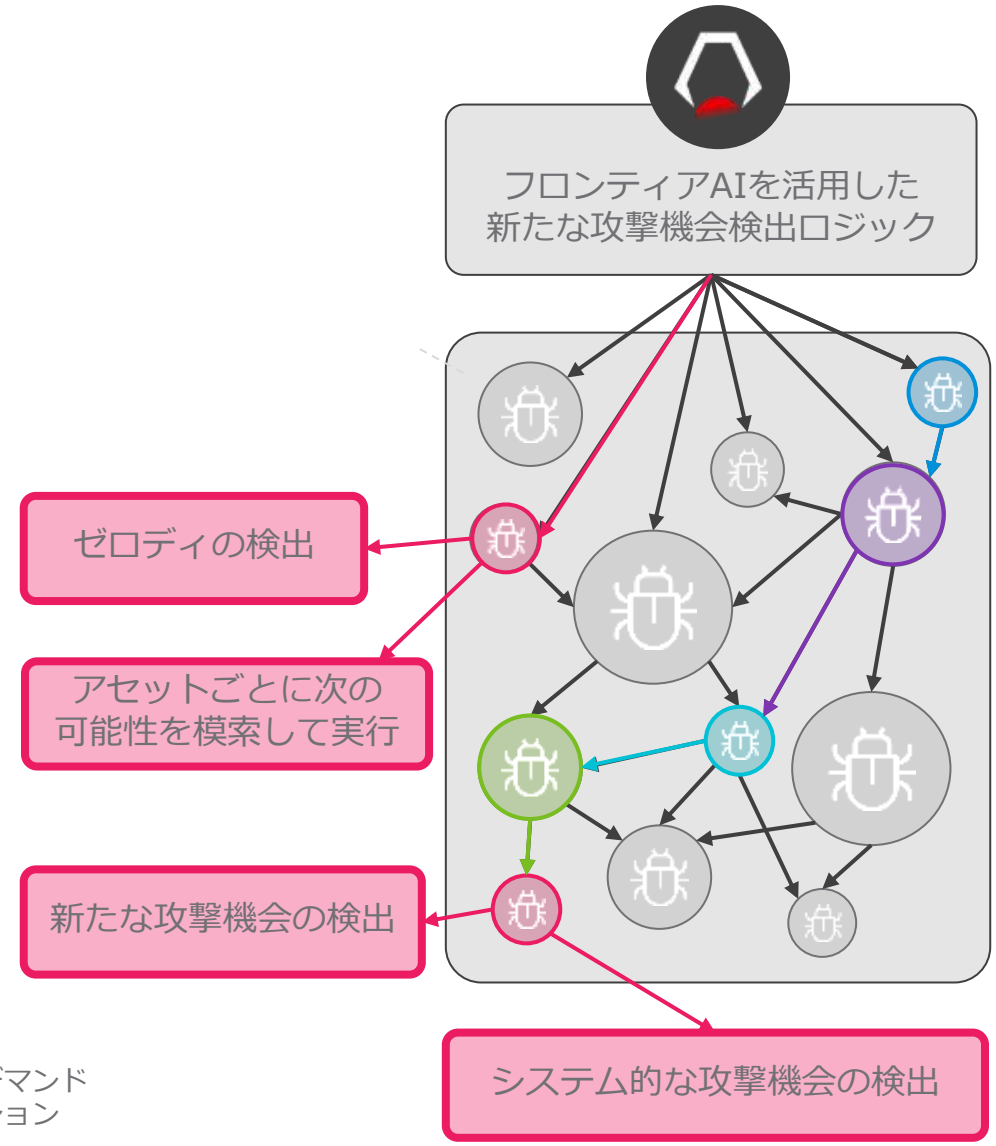
Technology Scan

Vector Scan / Validation Technologies
(AI powered by ULTRA RED)

Frontier AI+
(Additional Logical Technologies)

ULTRA RED AI Scanner

※オンデマンド
※オプション



AI Scannerの利点

ゼロディの検出

新たなベクターの検出

新たなエクスプロイト・パスの検出

システム的な攻撃機会の検出

軽微な情報から新たな攻撃機会の検出

ロジカルなエクスプロイト・パスの検出

コードベースの解析や仮想環境のサンドボックス解析ではなく,

今, 現場に実在する攻撃機会を深く, 幅を持たせて, 可能性から検証して立証していく

※オンデマンド
※オプション

証明した結果で優先度づけ

アセット

5

インパクトアセスメント

バリデーションの証明

AIチャットによる支援

MTTR向上に向けた修復管理

毎日スキャンを実施

ULTRA SCAN

ULTRA RED
Scan Engine

Vul’ Scan & Validation

NIST SP800-30: 適切なリスク対応のタイプ			
リスクの回避	リスクの軽減	リスクの移転	リスクの許容

アセット → 攻撃ベクターが修復されず再度確認できる → Verified

アセット → リスクの回避 → 攻撃ベクターが修復されて再度確認できない → Archived

アセット → リスクの回避 / リスクの軽減 → 仮想パッチによって, 攻撃ベクターが再度確認できない → Archived

アセット → リスクの許容 → 攻撃ベクターが再度確認できるが, 許容すると判断 → Accepted

MTTR: Mean Time to Repair（平均修復時間）

NIST SP800-30:リスクアセスメントの実施の手引き
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000balw.pdf

トリアージ（優先順位付け）をよりシンプルに

セキュリティだけでなく
その状態まで評価する

脆弱性や設定ミスなどを検出するだけでなく
どういう状態か, 多角的に立証する

アクティブ・ディフェンス
積極的防御で攻撃者の先手を打つ

サイバー攻撃が発生・拡大しないように
より早く継続的に立証し優先付けする

- ✓ 自組織は攻撃者からどう見えているか
- ✓ 攻撃者が最初に見つける攻撃機会はどこか
- ✓ 攻撃者はどの攻撃機会から悪用するか（優先づけ）

ULTRA REDの特徴

セキュリティ ポスチャから優先度付け

- ✓ **ダークウェブ**の脅威情報やCVEの**EPSS**, OWASPの**Likelihood**との自動マッピング
- ✓ 攻撃機会の悪用**難易度**や**複雑性**, 必要な**特権レベル**, **ユーザー関与**必要性などから優先付け

検出した攻撃機会を多角的に調査・立証

- ✓ エミュレーションによって**多角的に立証**, その状態からトリアージのための優先順位付け
- ✓ ダイナミック・パラメータ, ダイナミック・ペイロードによる**動的な繰り返し検証**

- ✓ 空きポート確認, 最新バージョンの有無検出, デジタル証明書の不備検出など

- ✓ シードドメインから, 関連ドメインや関連アセットを**繰り返しディスカバリ**

✓ 自組織は攻撃者からどう見えているか

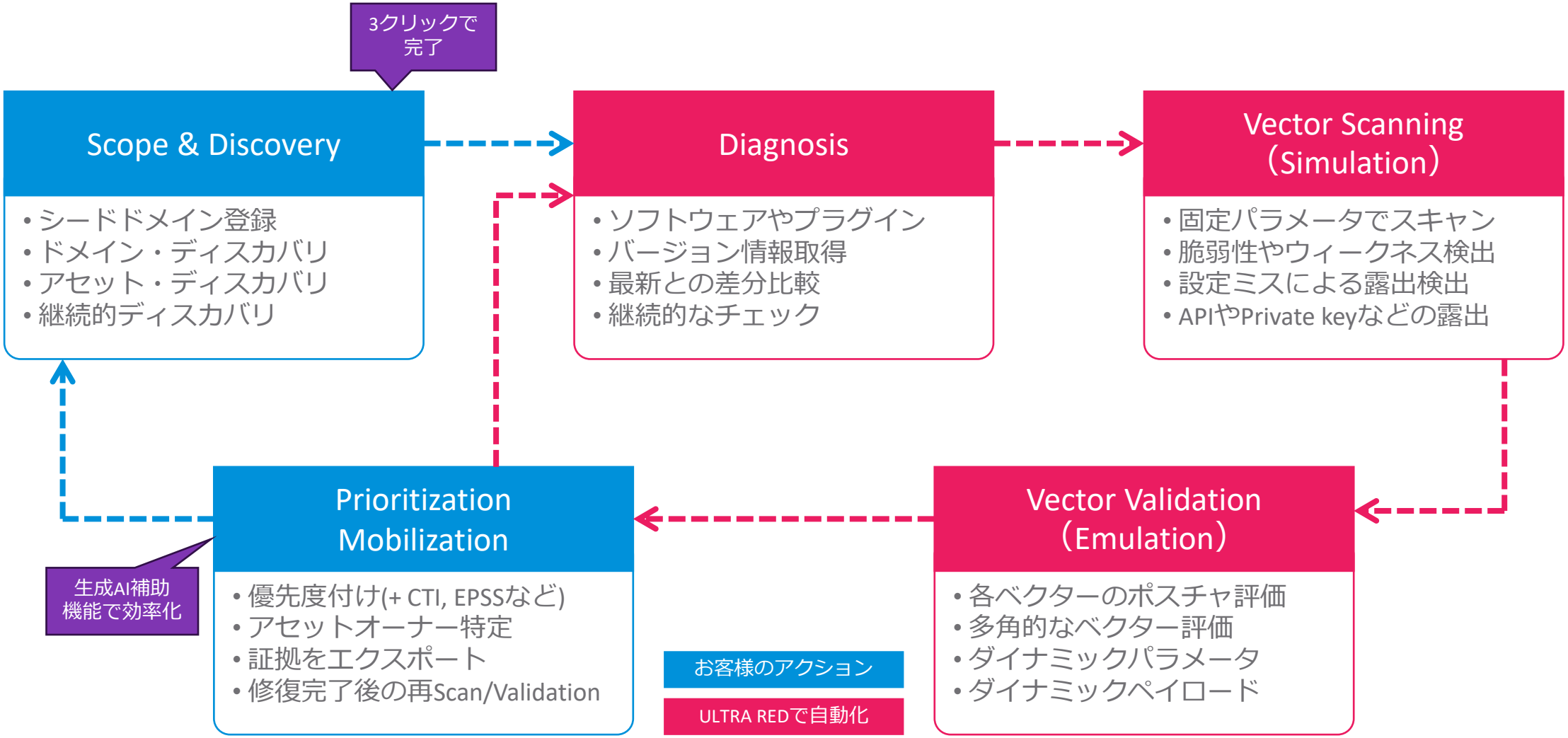
✓ 攻撃者が最初に見つける攻撃機会はどこか

✓ 攻撃者はどの攻撃機会から悪用するか（優先づけ）

エージェントレス | アセットへの影響なし | ALL in ONE

SaaSで提供するULTRA REDのプラットフォーム

ULTRA RED運用イメージ



ULTRA REDの特徴

➢ アセットの検出能力の高さと管理の自動化

✓独自の再帰的ドメイン・アセット検索による高い検出能力と自動検出

✓詳細なテクノロジースタックレポート，バージョニング，タイムスタンプ，ログ，自動タグメカニズムにより管理効率を上げて自動化

➢ ビジネスインパクトに基づく優先順位付け

✓CVSSのスコアだけでなく，攻撃可能かどうか，その容易性，ビジネスへの影響度も含めてスコア計算

✓脆弱性やウィークネスそのものの調査に必要な豊富な情報を一元的に提供

✓ダークネットの情報とのコンテキストを優先度の計算に利用

➢ 繰り返しの検出作業を自動化

✓毎日（Default）継続的にスキャンすることで新たな脆弱性やウィークネスをリアルタイムに検出

✓モニターの範囲は，関連会社や子会社，サプライチェーンも含めることを推奨

➢ 攻撃者の立場でアセットをスキャンし脆弱性や弱点を検出

✓サイバー戦争の実戦で培われた技術と経験をスキャン技術に適用

✓ダークネット脅威インテリジェンスから取得する最新の攻撃者のTTPを活用した攻撃手法で確実に検出

➢ 脆弱性やウィークネスや修復の確認用POCコードを提供

✓検出した時のPOCコードを提供することで再度検証可能で，修復後の確認としても利用可能

➢ アセットやパッチ管理に適したユーザーインターフェース

✓アセット管理に加え，パッチマネージメントとしての活用も可能なユーザーインターフェースを提供

➢ CTEMに必要な機能をオールインワンで提供

✓CTEMに必要な，「ASM」「Validate（検証）」を自動化，「Remediate（修復）」に必要なPOCコードまで提供

✓完全エージェントレスでSaaSとして提供

ULTRARED

CTEM: Continuous Threat Exposure Management
ASM: Attack Surface Management

ULTRA REDの特徴

アセットや脆弱性の
検出能力の高さと継続性

完全エージェントレスで
攻撃者の立場での検証と
エビデンスの提供

ビジネスインパクト
を考慮した優先度づけ

➢ アセットの検出能力の高さと管理の自動化

✓独自の再帰的ドメイン・アセット検索による高い検出能力と自動検出

✓スタックレポート，バージョニング，タイムス
管理効率を上げて自動化

➢ 攻撃者の立場でアセットをスキャンし脆弱性や弱点を検出

✓サイバー戦争の実戦で培われた技術と経験をスキャン技術に適用

✓ダークネット脅威インテリジェン
撃者のTTPを
活用した攻撃手法で確

脆弱性やウィー
供

検出した時のPO
確認としても

く優先順位付け

可能かどうか，

調査に必要な

キストを優先度の計

セットやパッ

アセット管理に加え
ユーザーインターフェー

業を自動化

✓毎日（Default）継続的にスキャンすることで新たな脆弱性やウィ
ネスをリアルタイムに検出

✓モニターの範囲は，関連会社や子会社，サプライチェーンも含めることを
推奨

➢ CTEMに必要な機能をオールインワンで提供

✓CTEMに必要な，「ASM」「Validate（検証）」を自動化，
「Remediate（修復）」に必要なPOCコードまで提供

✓完全エージェントレスでSaaSとして提供

CTEM: Continuous Threat Exposure Management
ASM: Attack Surface Management

ULTRARED

Thank you…