

# ULTRA RED AI駆動型CTEM

AIを活用した外部サイバー防御プラットフォーム  
攻撃者のインテリジェンスから自律的な修復まで

# サイバーセキュリティは新たな時代を迎えつつある

- AIがサイバー攻撃を劇的に加速
- 攻撃キャンペーンはより高速に, より低コストに, 推移して自動化へ
- AIの台頭により, 攻撃者はかつてない規模で組織の脅威エクスポージャー（外部への脅威の露出）を発見し, 悪用することが可能に
- 各組織が急速にAIを採用した結果, 新たなデジタルアセット, アイデンティティ, そしてアタックサーフェス（攻撃対象領域）が次々と生成
- 政府や規制当局の指針は, 継続的なサイバーレジリエンス（回復力）へとシフトしている（例：日本における能動的サイバー防御（ACD））

## サイバー防衛のルールは根本から覆り次世代へ

# これらがサイバー防御にもたらす意味

## ➤ 近代的な現代のサイバー防衛に求められる要件：

- ✓ 手動プロセスに代わる「継続的な自動化」
- ✓ 悪用される前に特定する「プロアクティブな認知」
- ✓ アラート過多を解消する「インテリジェンス駆動の優先順位付け」
- ✓ サイロ化したバラバラのツールからを廃した「統合ワークフロー」へ
- ✓ 定期的な診断ではなく「継続的な検証（Validation）」
- ✓ 可能な限りの「自動復旧（Remediation）」

スピードアップ, 自動化, 統合が今や不可欠な時代に

# ULTRARED AI駆動型CTEM | 弊社独自の価値提案



## AIを活用したインテリジェンス

高度なAIモデルが、脅威、脆弱性および  
攻撃者のデータを統合し、  
比類のない精度を実現します。



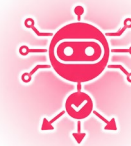
## アウトサイド・イン型防御

攻撃者が「視認」「到達」「悪用」  
できる範囲を制御することで、  
脅威が侵入する前に防御します。



## リアルタイム適応

絶えず学習し、変化し続ける脅威の  
状況や攻撃者の行動に適応します。



## 自律的な対応

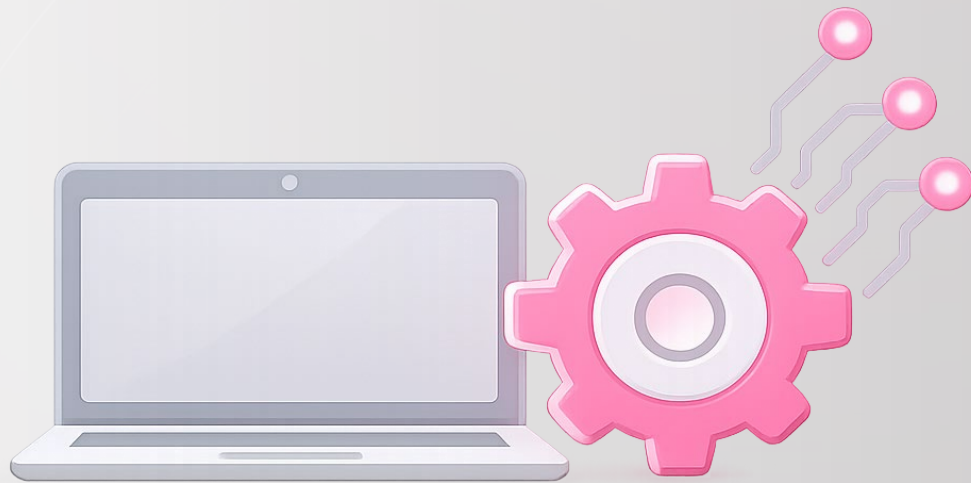
展開や業務への支障を伴わずに、  
即座かつ的確な対応を行います。



## ビジネスのレジリエンス

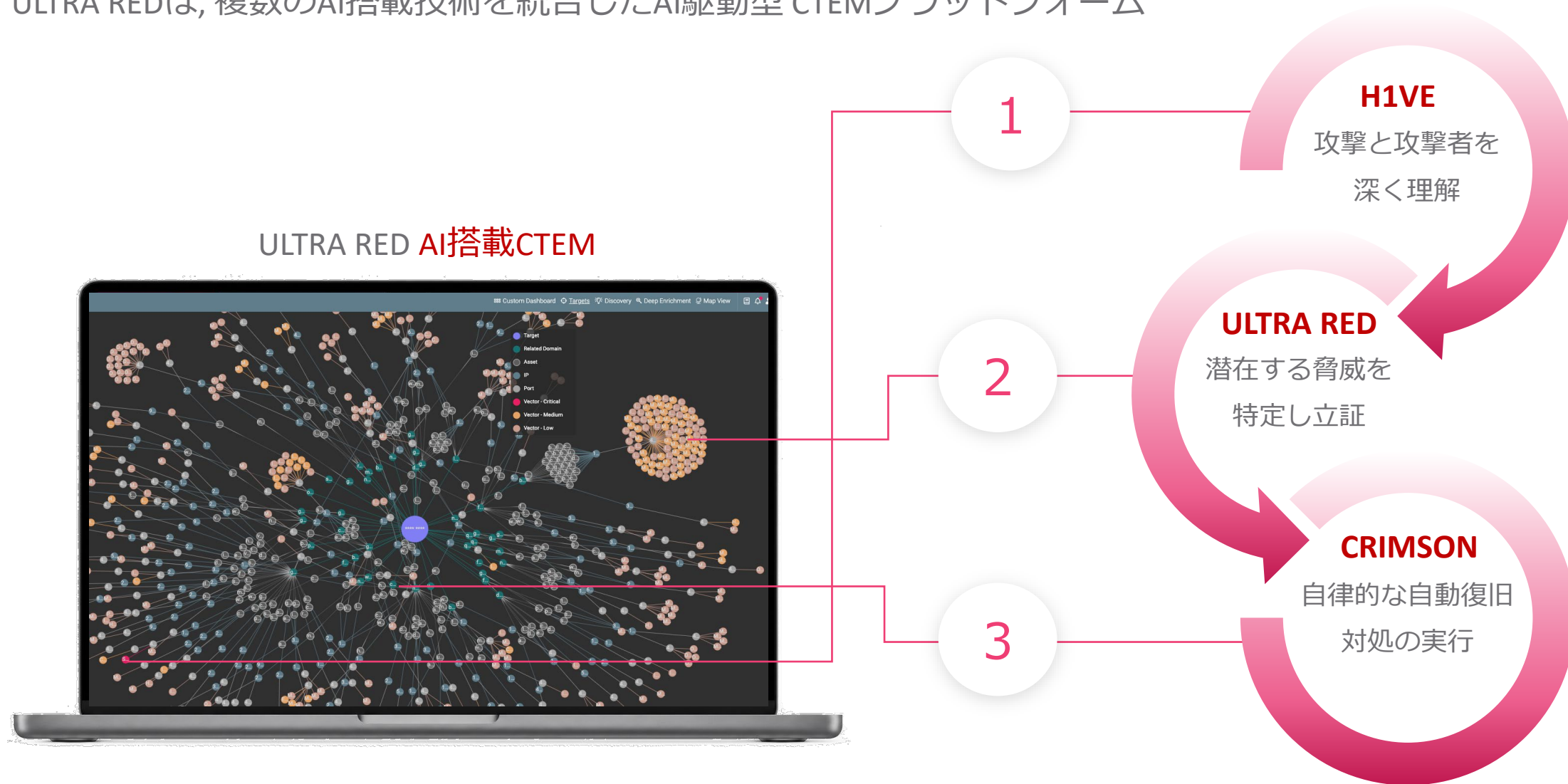
リスクを低減し、脆弱性を解消し、ビジ  
ネスの継続的な運営を確保します。

# ULTRA TECHNOLOGY



# 単一の連続的なセキュリティパイプライン

ULTRA REDは、複数のAI搭載技術を統合したAI駆動型 CTEMプラットフォーム



# ULTRA RED AI駆動型CTEM | 統合型AI防御プラットフォーム

## 継続的な学習ループ

現実世界のリアルな脅威アクター活動に基づいて, AIが検知, 検証, および自動復旧の精度を絶え間なく向上させ続ける

ディセプション（おとり）駆動型  
インテリジェンスを通じて, リアル  
な攻撃者の行動を捕獲

外部アタックサーフェス全体にわたり,  
悪用可能な攻撃ベクトル（侵入経路）  
を実証検証

検証された脅威エクスポージャー  
（外部への脅威の露出）を自動的  
に緩和, または自動復旧・対処



H1VE



ULTRA RED



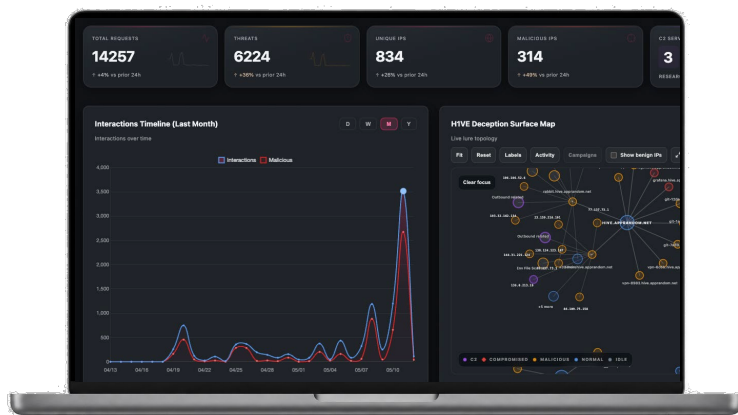
CRIMSON

# ULTRA RED AI駆動型CTEM | 統合型AI防御プラットフォーム

1

H1VE

実際の攻撃者に関する  
インテリジェンス



H1VEは、ディセプション（おとり）技術を駆使した積極的なサイバー防御プラットフォームで、以下の情報を収集：

- ✓ 攻撃者のペイロード（攻撃コード）
- ✓ ゼロデイおよび未公開（Pre-CVE）脆弱性の可視化と取得
- ✓ 悪用・侵入手法の可視化と取得
- ✓ コマンド&コントロール (C2) サーバーなどの攻撃者のインフラ
- ✓ マルウェアの挙動とマルウェア本体の取得
- ✓ 攻撃キャンペーンの攻撃パターン
- ✓ 想定や仮定ではなく、実際の攻撃者とのリアルな相互作用（インタラクション）

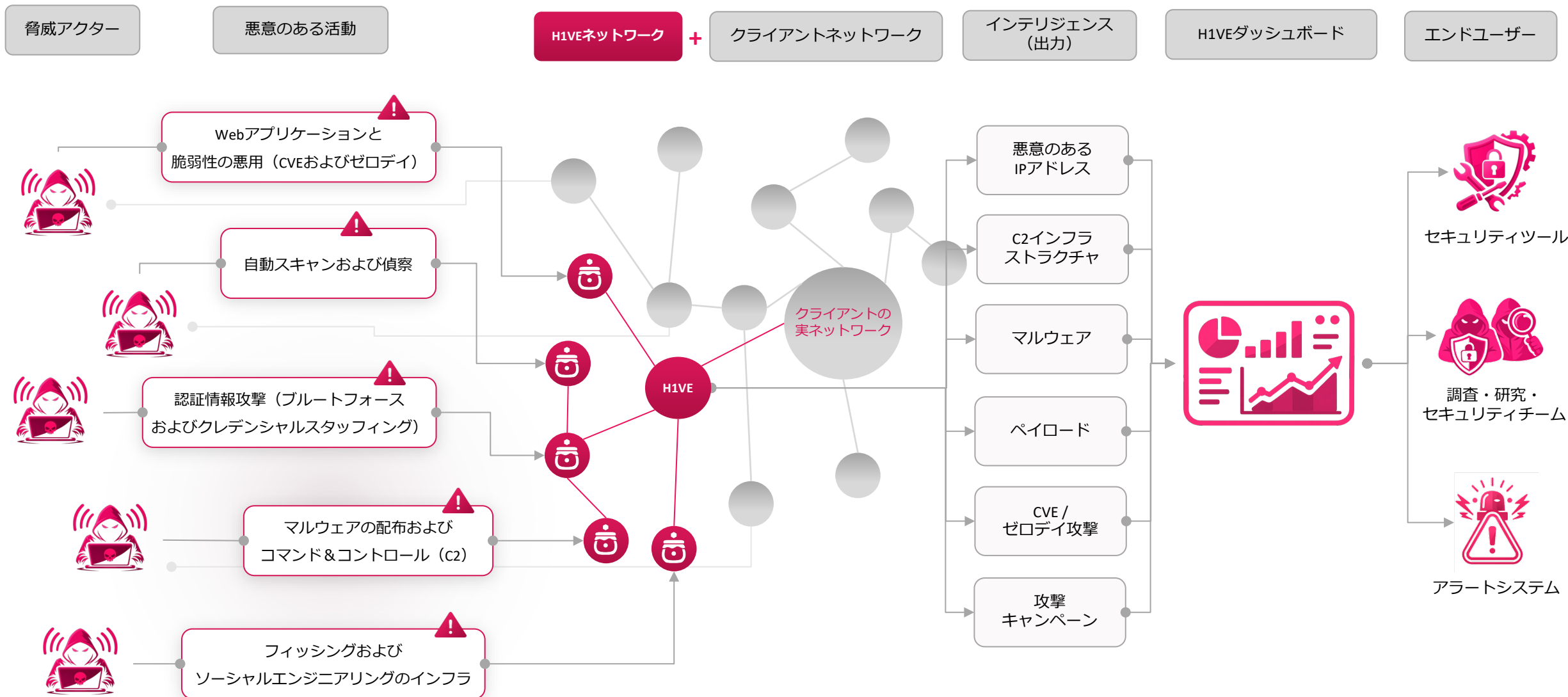
2

ULTRA RED

3

クリムゾン

# H1VE | 仕組み



# ULTRA RED AI駆動型CTEM | 統合型AI防御プラットフォーム

終わりのない大量のアラートを出し続ける従来のスキャナーとは異なり、ULTRA REDは「実際に検証され、悪用可能な侵入経路（露出）」だけにフォーカス

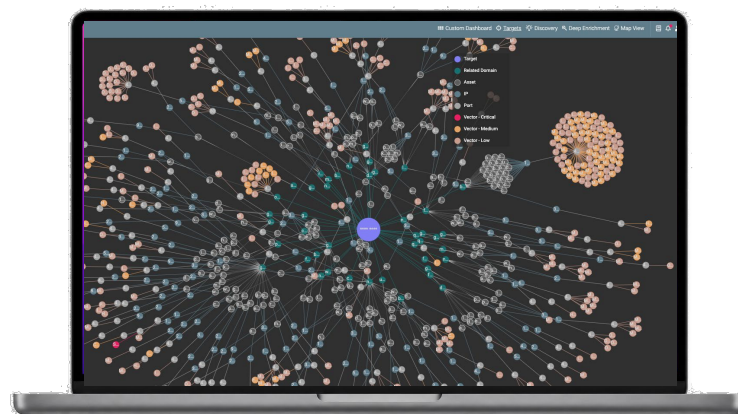
主要コンセプト：

- ✓ 外部攻撃サーフェス管理 (EASM)
- ✓ 継続的なスキャン
- ✓ エクスプロイト悪用検証（実証テスト）
- ✓ 誤検知ほぼゼロ
- ✓ 攻撃ベクトル分析
- ✓ AIを活用した優先順位付け

1 H1VE

2 ULTRA RED

**Validation-First  
CTEM**



存在する事実を立証する  
CTEMプラットフォーム

**100%**  
脅威エクスポート  
(外部への脅威の露出) の立証

**0%**  
誤検知・過検知

**1/2~1/3**  
MTTRの短縮

**100%**  
エージェントレス  
SaaS提供

3 CRIMSON

# ULTRA RED | 仕組み

**Validation-First CTEM**（検証優先のCTEM）は、すべての資産と攻撃ベクトル（侵入経路や攻撃チャンス）を自動的に発見、収集、および実証（検証）することで誤検知を完全に排除し、最も正確で網羅された「脆弱なアタックサーフェス」を提示



# 「ULTRA RED」 詳細解説 | 当社のAI哲学

AIはサイバーセキュリティを「強化（拡張）」するためのものであり、人間のエンジニアリングを「置き換える」ものではない。

当社のアプローチの融合：

- ✓ 確定的な継続資産発見
- ✓ 完全なアタックサーフェスの網羅
- ✓ AI駆動の調査
- ✓ AIが支援する実証検証
- ✓ 継続的な監視

「カバレッジ最優先」 - AIは最も価値を生む場所へ適用して活用していく

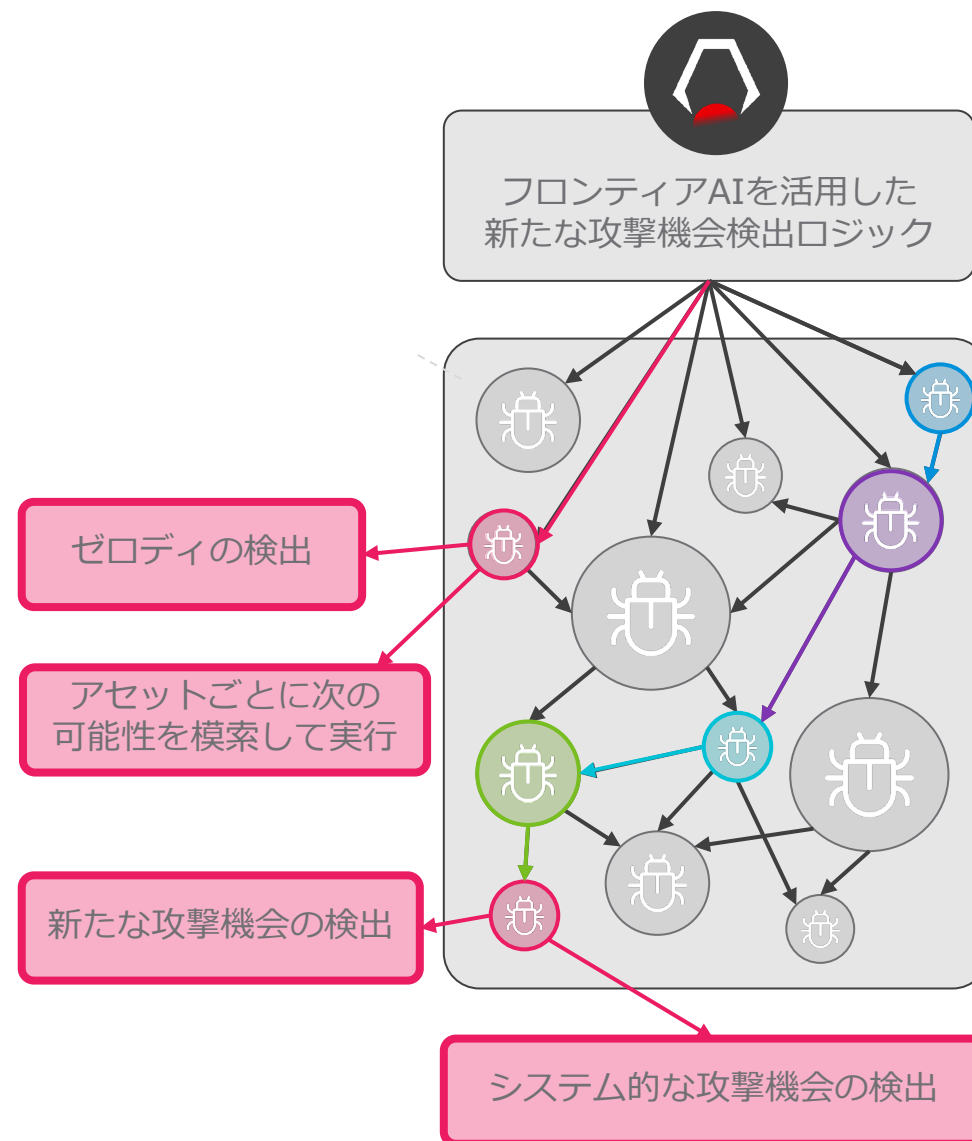
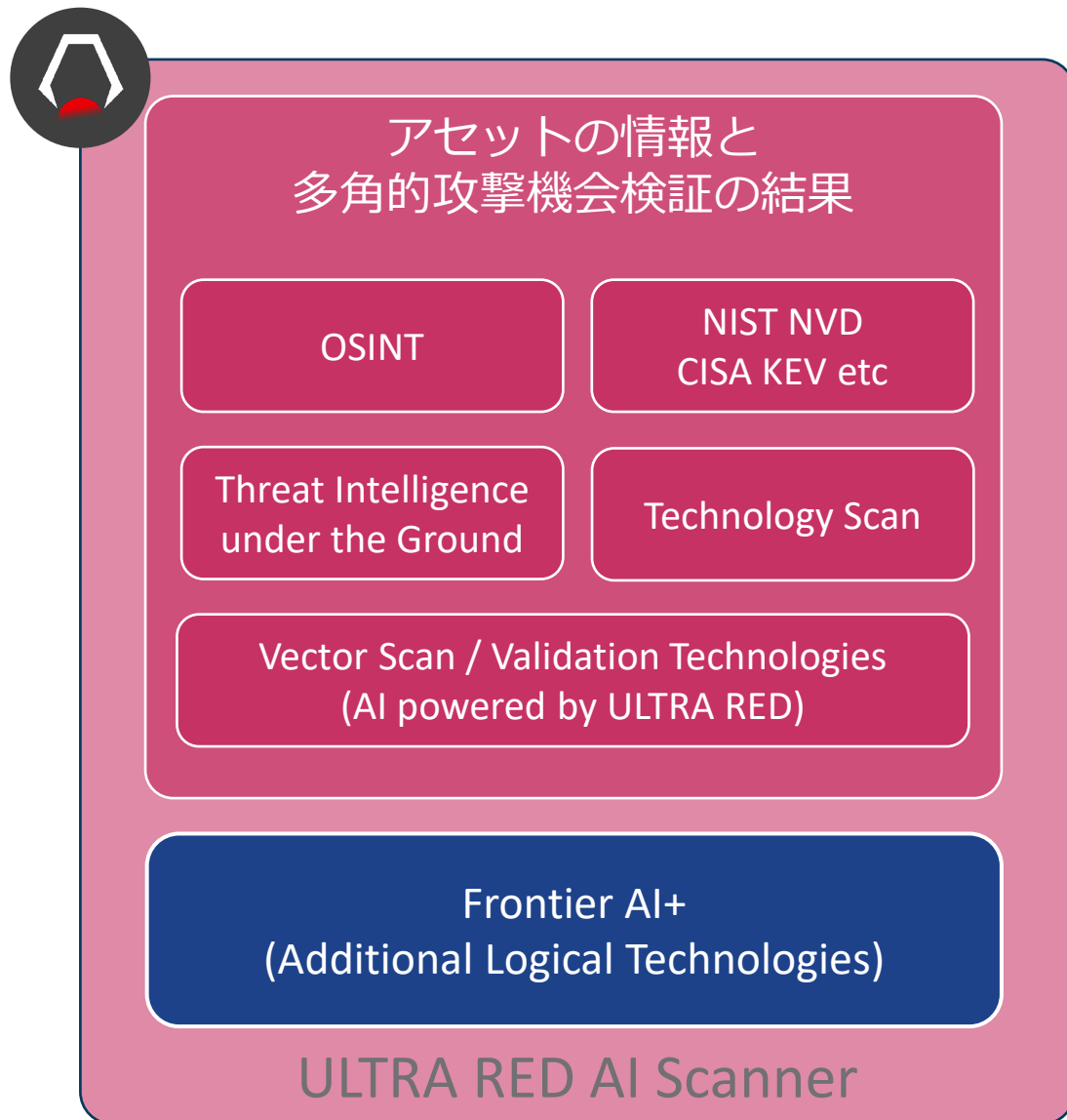
# 「ULTRA RED」 詳細解説 | ULTRA RED上でのAI動作プロセス



AIは無差別に作動されるのではなく、必要な時にインテリジェントにアクティベート（起動）

# AI Scanner - 新たな検出口ジック

TLP:AMBER+STRICT



# ULTRA RED AI駆動型CTEM | 統合型AI防御プラットフォーム

CRIMSONは、検証された脅威エクスポージャー（外部への脅威の露出）を、自動的に修復・復旧アクションへと実用的なインテリジェンスとして変換

- ✓ ULTRA REDが攻撃ベクトルを特定
- ✓ AIがその文脈（コンテキスト）を分析
- ✓ CRIMSONが修復案を自動生成
- ✓ 各システムが自動的に応答・防御を実行

アクションの例

- ✓ WAF（Webアプリケーションファイアウォール）ルールの生成
- ✓ ファイアウォール設定のアップデート
- ✓ OSSのソースコードの修正案
- ✓ GitHubのプルリクエスト（PR）の自動生成
- ✓ SOCにおけるインシデントの自動起票

1

H1VE

2

ULTRA RED

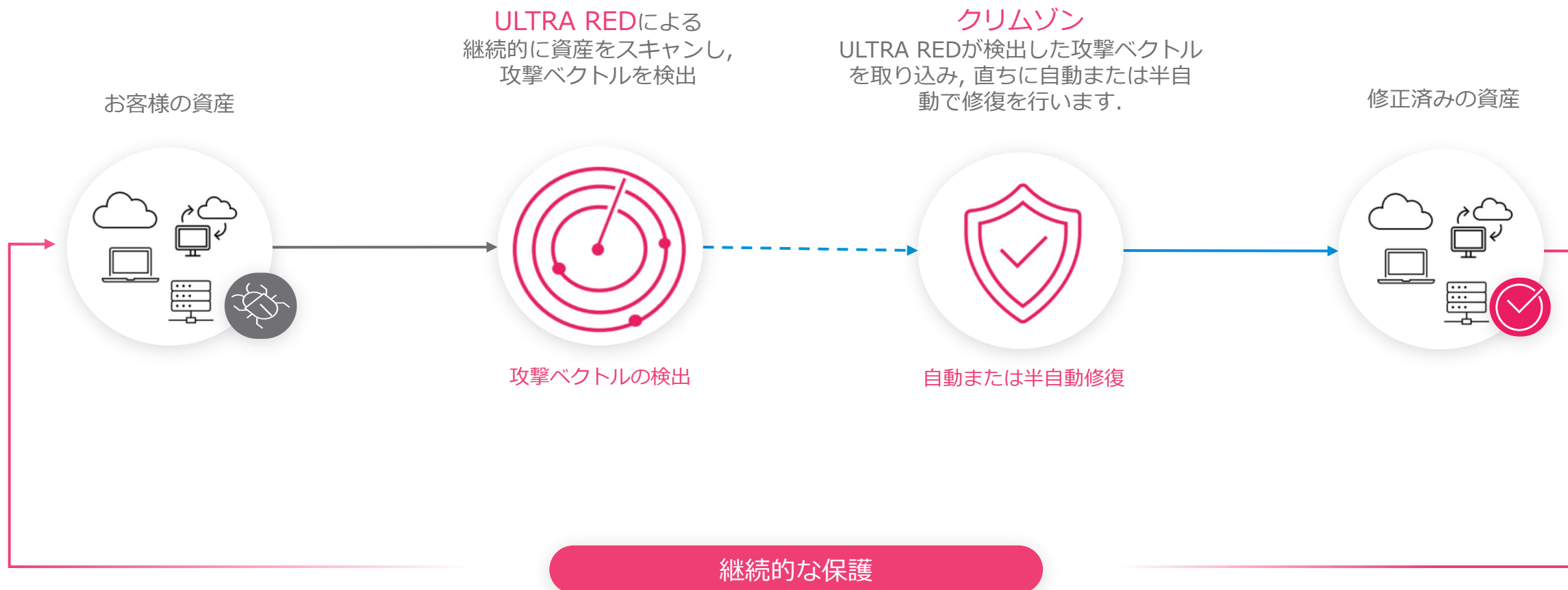
3

CRIMSON

エージェントレスの  
AI駆動型ダイナミック自動復旧



# ULTRA RED + CRIMSON | 仕組み



Thank you...

