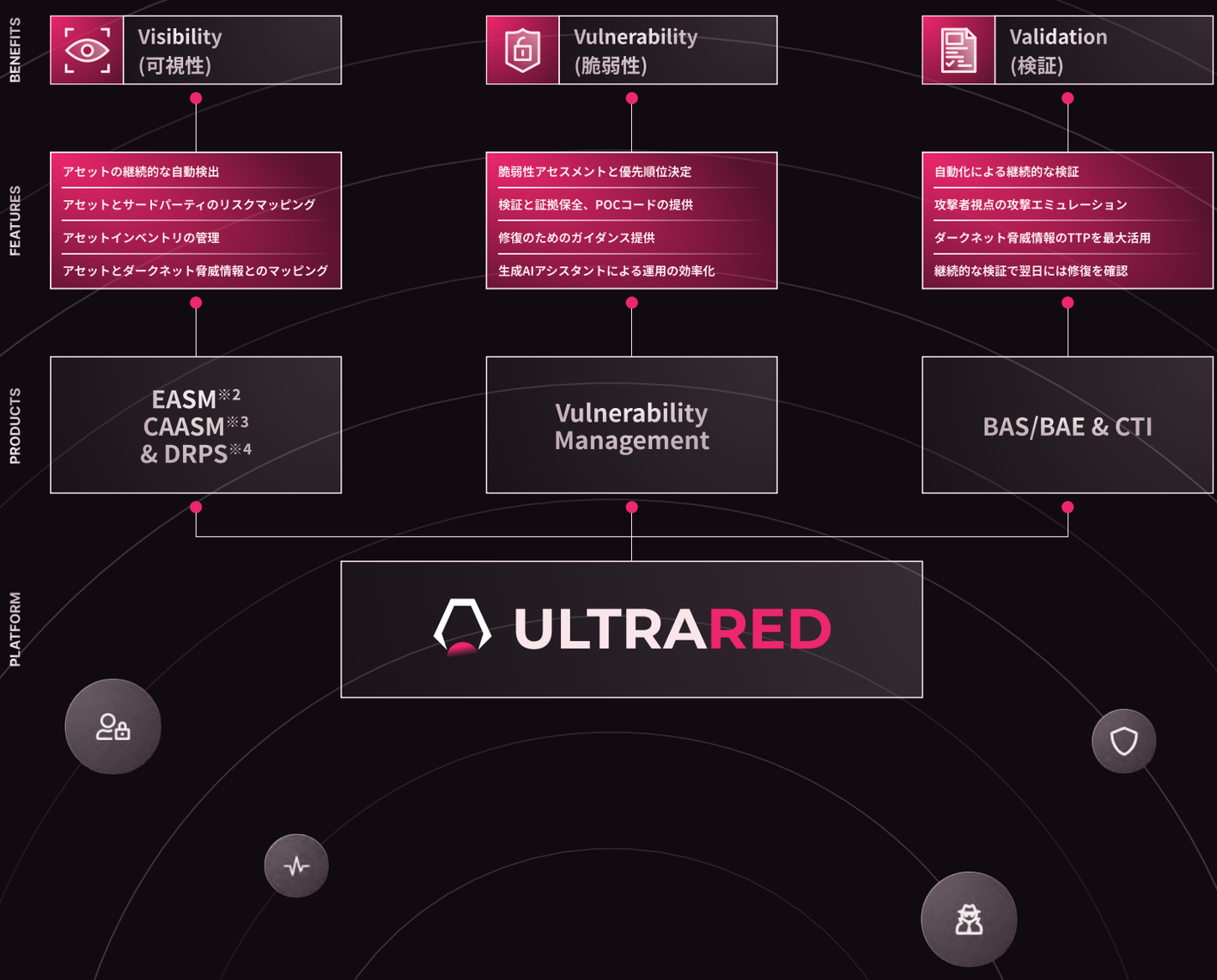
ULTRARED

攻撃者視点でアタックサーフェスを見抜く

ULTRA REDのCTEM※1プラットフォームは、デジタル資産を毎日自動的に検出および検証することで、潜在的な攻撃機会を立証します。その検証結果には、アクションに結び付く脆弱性や弱点等の詳細な解析結果が含まれ、それを活用することで、攻撃者よりも先回りしてアセットを保護できます。



※1 CTEM: Continuous Threat Exposure Management　※2 EASM: External Attack Surface Management
※3 CAASM: Cyber Asset Attack Surface Management　※4 DRPS: Digital Risk Protection Services

お問い合わせ

www.ultrared.ai

ULTRARED

継続的脅威エクスポージャ管理

ULTRA REDのCTEMプラットフォームはお客様のビジネスに最も影響のある脆弱性や脅威から優先的にアセットを保護するように設計されています。

アセットディスカバリの自動化

- 未知のドメインやアセットを正しく検出
- マニュアルでの管理から解放
- 常に最新レコードを維持

脆弱性の検出、検証、優先順位付け

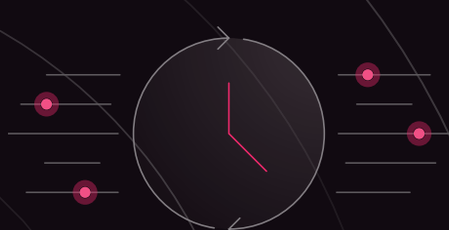
- 常に最新に自動更新される検出ロジック
- 各攻撃ベクターにPoCコードを提供
- アセットが提供するサービスへの影響に配慮した設計
- ビジネスインパクトを考慮した優先度付け

攻撃ベクターの情報と修復のためのガイダンス

- セキュリティ管理者とアセット管理者のコラボレーションを強化
- 修復までのパフォーマンス向上
- MTTR※5の短縮

一貫性のある継続した管理プロセス

- 重大度・緊急度の高い脅威を継続的に削減
- 潜在するユニークなCVE数を最小化
- 各オペレーションチームの生産性向上



※5 MTTR: Mean-Time-To-Remediate

詳細の動画解説はこちら

www.ultrared.ai