進化するAIと
それを支えるセキュリティ

トレンドマイクロ株式会社
バイスプレジデント
大場章弘

大場 章弘

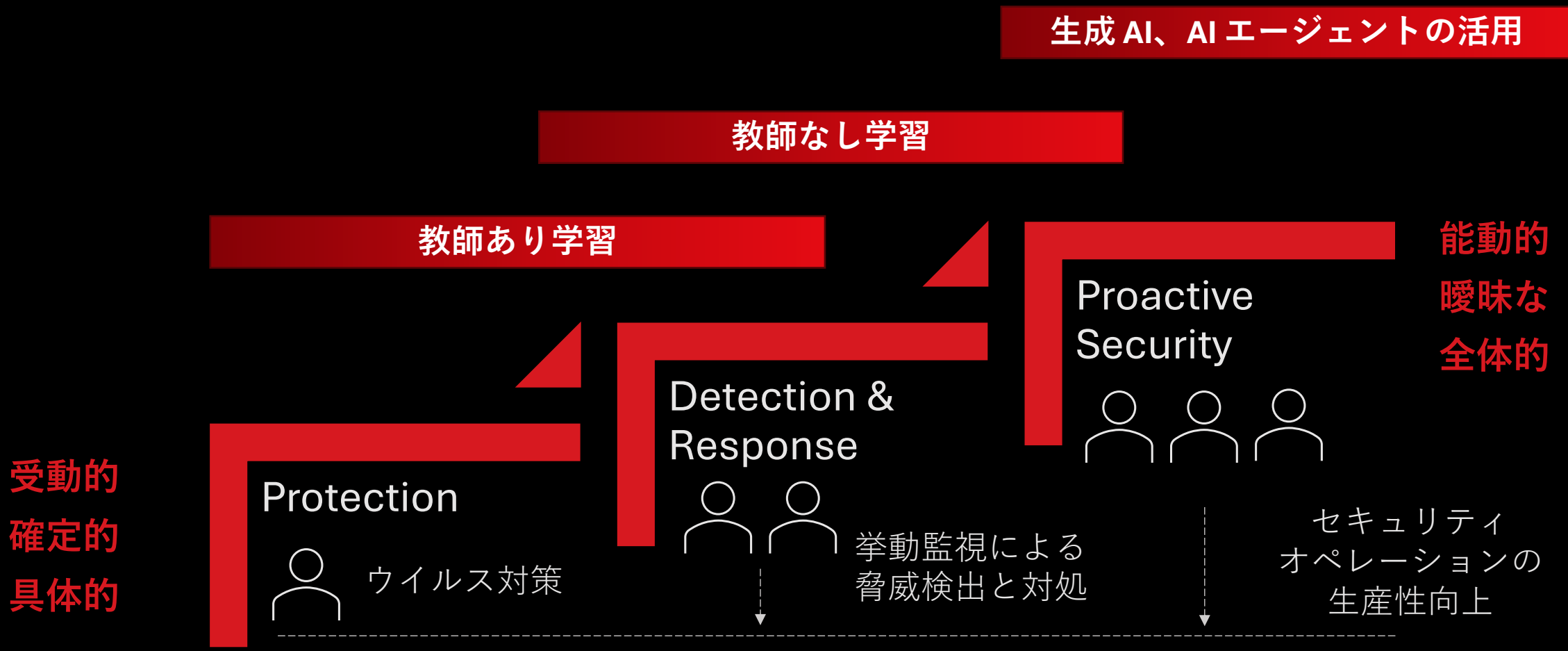
トレンドマイクロ株式会社
バイスプレジデント

クラウドセキュリティ、AIセキュリティの
新規事業開発を担当

＜職歴＞
日本IBM: 銀行勘定系SE
日本マイクロソフト: 先進技術責任者
トレンドマイクロ: 日本の営業責任者
AWS: 公共部門パートナー連携責任者

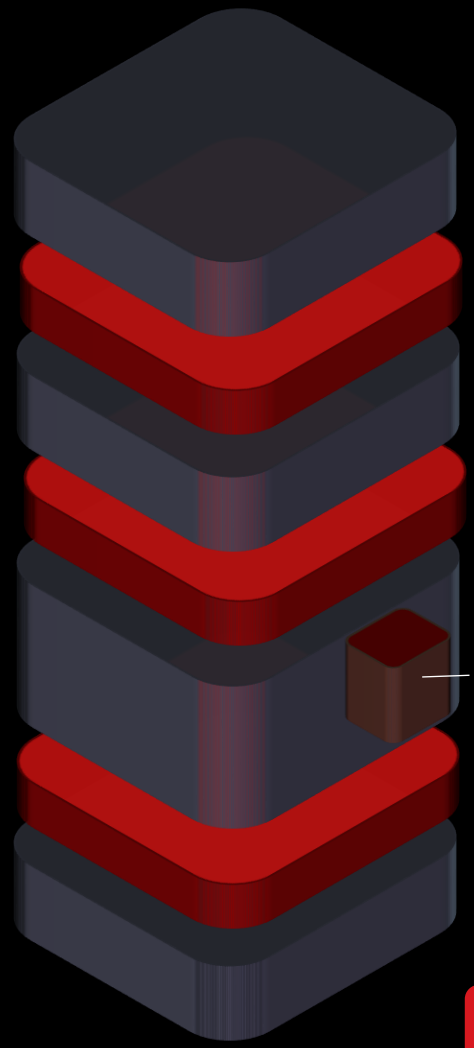
＜資格＞
AWS認定資格 全12資格取得
J.S.A. ワインエキスパート

サイバーセキュリティにおける AI の活用



ソフトウェア階層の変革

今までの
ソフトウェア階層



NVIDIA Tech Stack

NVIDIA NIM

NVIDIA Morpheus

NVIDIA
cuDF

AI環境の階層

TREND MICRO

NVIDIA Morpheus + Agentic AI

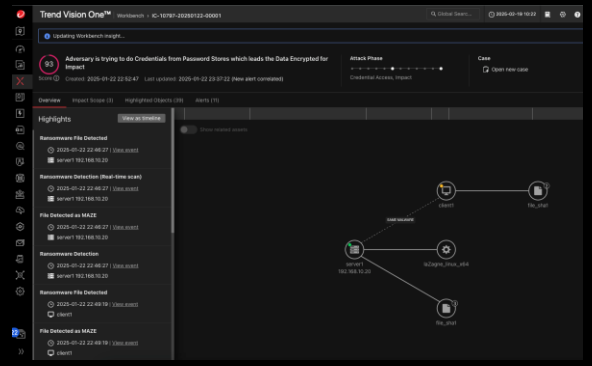
膨大なデータ

NVIDIA Morpheus

異常検知

セキュリティアラート

検出モデルで定義されていない脅威の検出



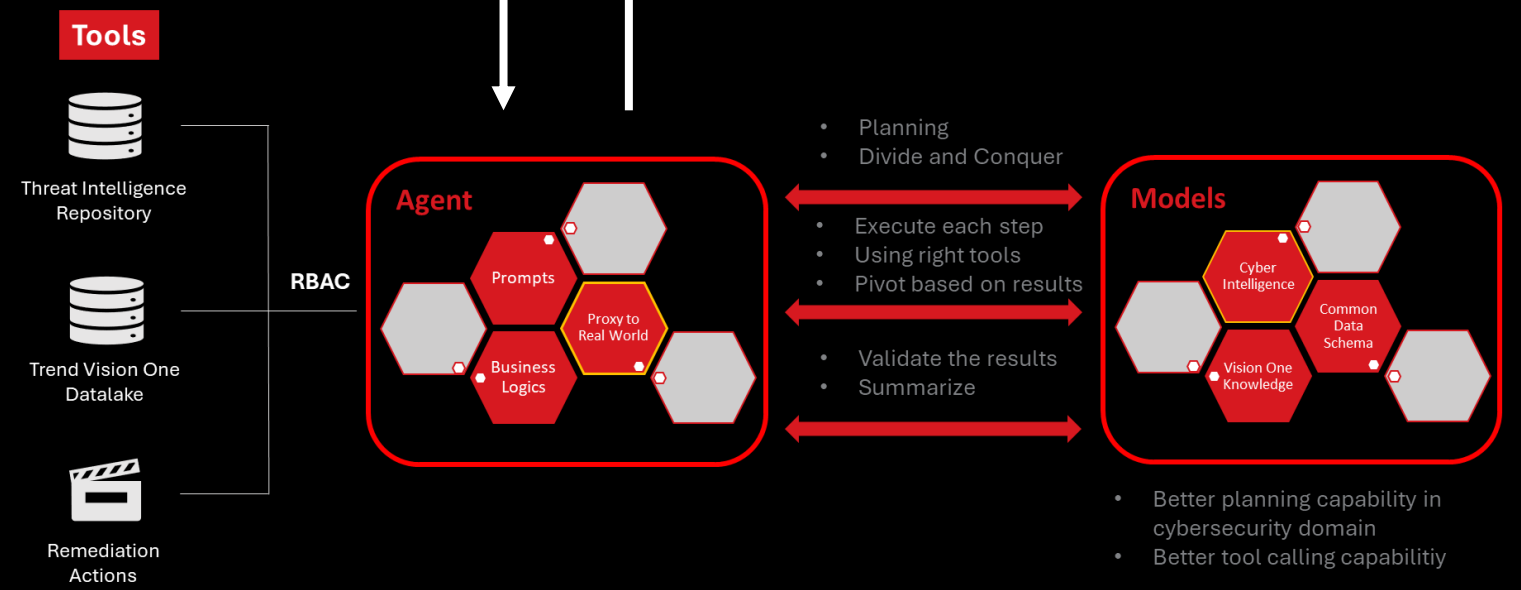
Trend Vision One

すべてのリソースにデジタル指紋

典型的な行動パターンを学習し、異常をリアルタイムに検出

ネットワーク上のデータを100%可視化

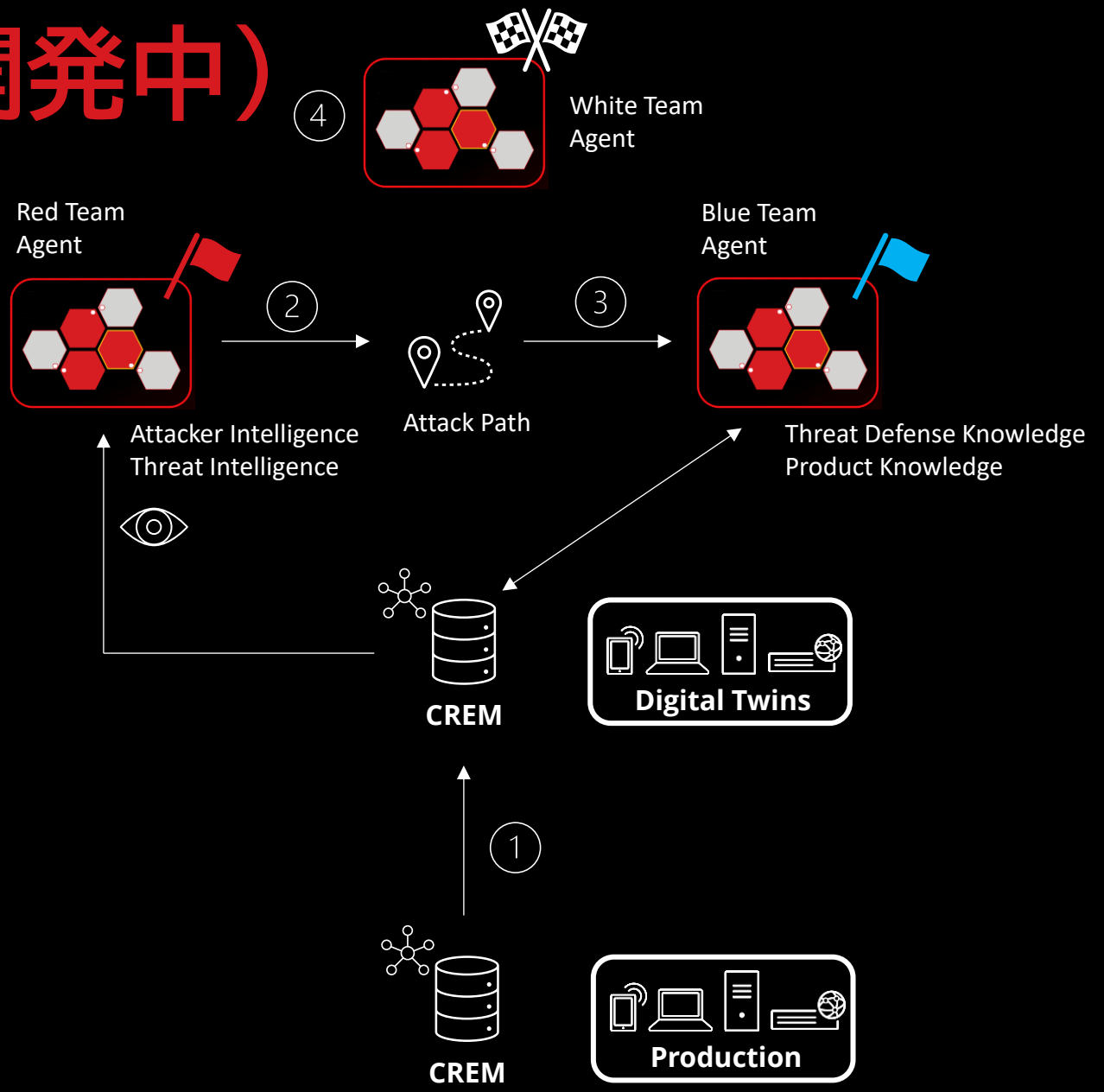
NVIDIA GPUの処理能力を最大限に活用



Public

Digital Twins（開発中）

1. CREM (攻撃対象リスク管理機能）がリアルタイムに本番環境から仮想検証環境用のデータベースを作成し同期
2. レッドチームのAgentが攻撃経路を提案
3. ブルーチームのAgentが各攻撃ステップに対する防御を提案
4. ホワイトチームのAgentが各攻撃ステップが成功したかどうかを判断
5. ２から４を繰り返し、実現可能な攻撃経路を見つけ出す



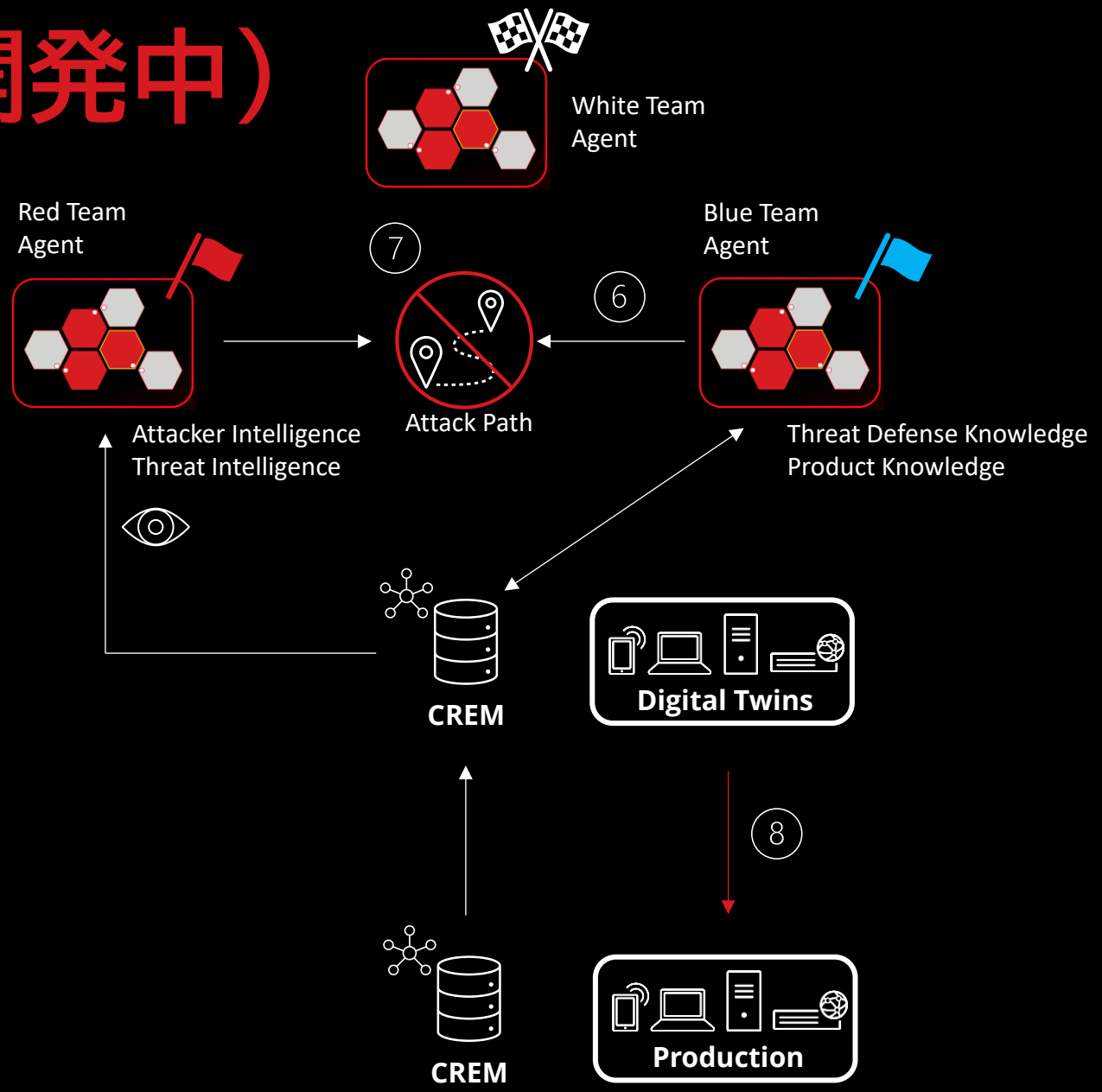
Digital Twins（開発中）

6. 実現可能な攻撃経路に対して、ブルーチームのAgentが対応する防御および修復アクションを提案し、仮想検証環境のデータベースを変更する

6. ホワイトチームのAgentが、攻撃経路がブロック可能かどうか評価する

7. ブルーチームのAgentが防御および修復アクションを本番環境に反映させる承認をリクエストする

8. 報告書を作成する

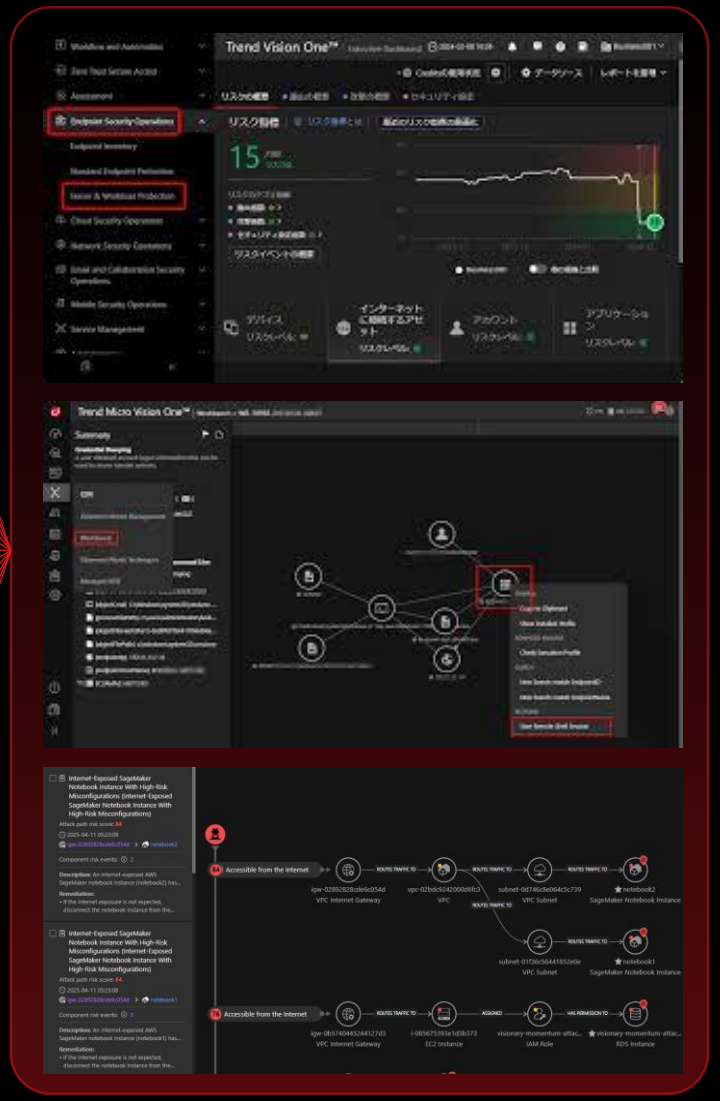


プロアクティブセキュリティ実現に向けて

保護、検知、挙動監視

ネイティブXDRセンサーおよび他社技術からの様々なデータを収集

- エンドポイント
- サーバ
- コンテナ
- **AI**
- IPS/IDS
- FW/UTM
- メール
- Web
- 他社センサー
- クラウド固有ログ
- **NVIDIA技術**



- 単一コンソールで一元管理
- 膨大なデータを相関分析し、高度な脅威検出、調査、対応、予防を支援、自動化
- 攻撃対象領域を可視化、サイバーリスクをスコアリングしすることで、対処・予防の優先順位を明確化
- 脆弱性検出と仮想パッチ
- 攻撃経路予測
- **NVIDIA技術やAIの活用**
- マルチクラウド、オンプレとのハイブリッドにも対応

Public

TREND MICRO™

THANK YOU

Questions?

Trend Research

TREND MICRO

Unlock safe AI innovation with Trend Micro's

SECURITY FOR AI BLUEPRINT

for your Datacenter and Cloud

Ready to transform your AI strategy?
Download the **BLUEPRINT**!

SCAN ME

Public