AI攻撃に対抗する次世代セキュリティ運用とは
～AI SOC導入の勘所と現実解～

株式会社マクニカ
ネットワークスカンパニー
セキュリティソリューション営業統括部
セールススペシャリスト
柴田 帆香

MACNICA

©Macnica,Inc.

本日お持ち帰りいただきたいこと

なぜ今、セキュリティ運用にAIが必要なのか？

AI SOCとは？

自社に合ったAI SOCの始め方を判断するための視点とは？

©Macnica,Inc.

この数字は何を表していると思いますか？

29分

©Macnica,Inc.

侵入後、攻撃者は平均29分で別端末へ横展開

侵入後、攻撃者が別端末へ横展開するまでのBreakout time（2025）

29分

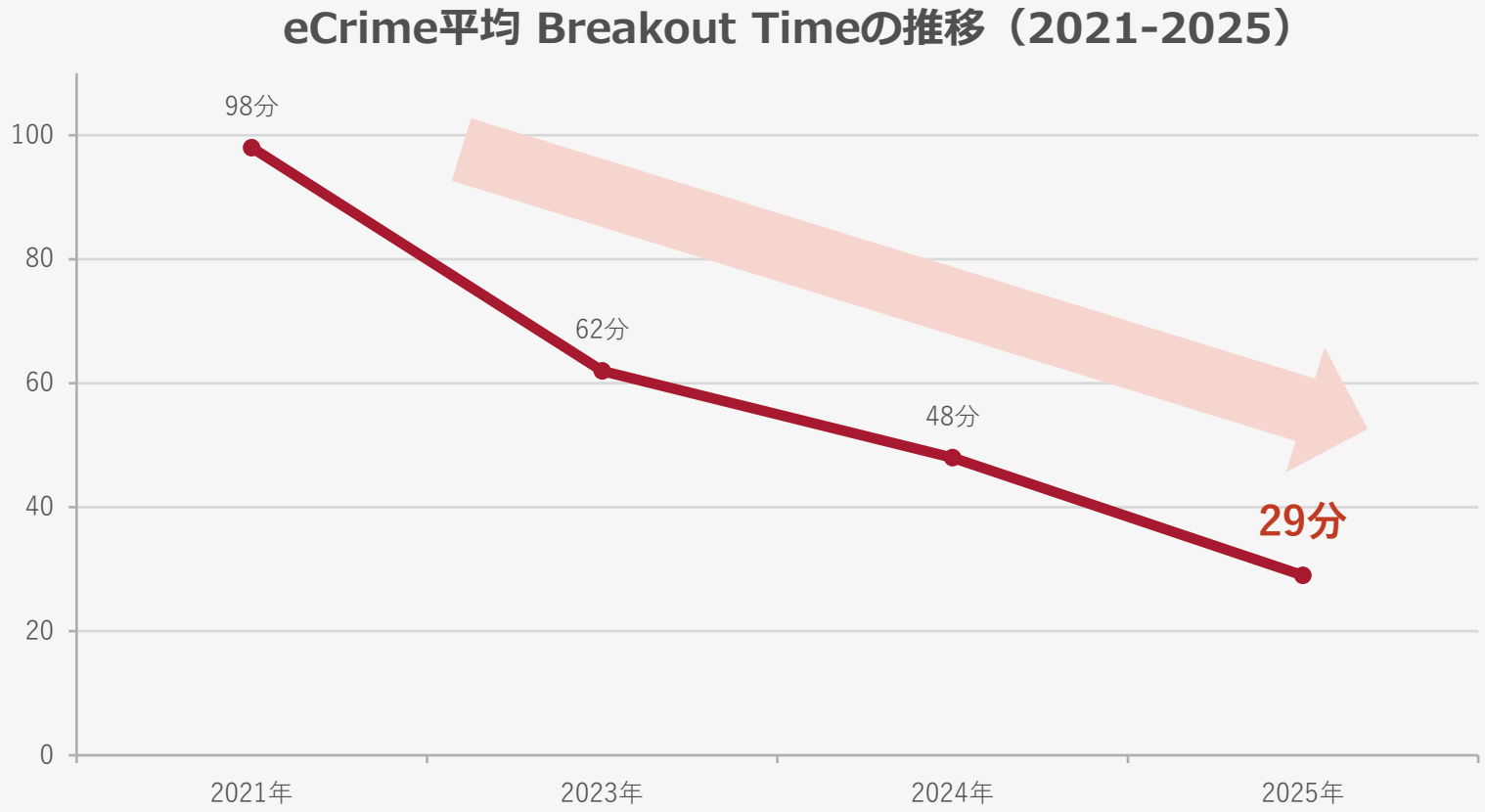
Breakout Timeとは：

攻撃者が最初の端末への侵入に成功してから、組織内の別の端末へ横展開するまでにかかる平均時間。

出典：[4]（詳細は巻末「参考文献」）

©Macnica,Inc.

攻撃者の横展開までの時間は、2021年から約70%短縮



AI活用による攻撃プロセスの高速化により、侵入後の横展開までの時間は急速に短縮

注：本スライドは、公開情報に記載された数値という端的な事実を参照し、グラフ自体はマクニカにて作成。
※各数値は各年に観測されたeCrimeの平均Breakout Time。レポート発行年はそれぞれ翌年。

出典：[1]～[4]（詳細は巻末「参考文献」）

©Macnica,Inc.

AI時代の攻撃側の変化

＜攻撃側の変化の実例＞

速度

攻撃プロセスにおけるAI活用の広範化により攻撃がより速く変化

攻撃者が初期侵害から組織内へ横展開する平均時間は、2024年の48分から2025年には29分へ短縮したとCrowdStrikeが報告。前年比で攻撃速度が約65%加速（出典②）。

量

AIによる自動化、低コスト化、容易化により、攻撃がより大規模に変化

AI活用により、往来のサイバー攻撃よりもスケール化が図りやすく収益化も約5倍容易になっているとハーバード大学による研究で発表。サイバー攻撃への参入障壁の低下が攻撃増加につながっている。（出典③）

巧妙さ

攻撃がより本物らしく、標的化され、高精度に変化

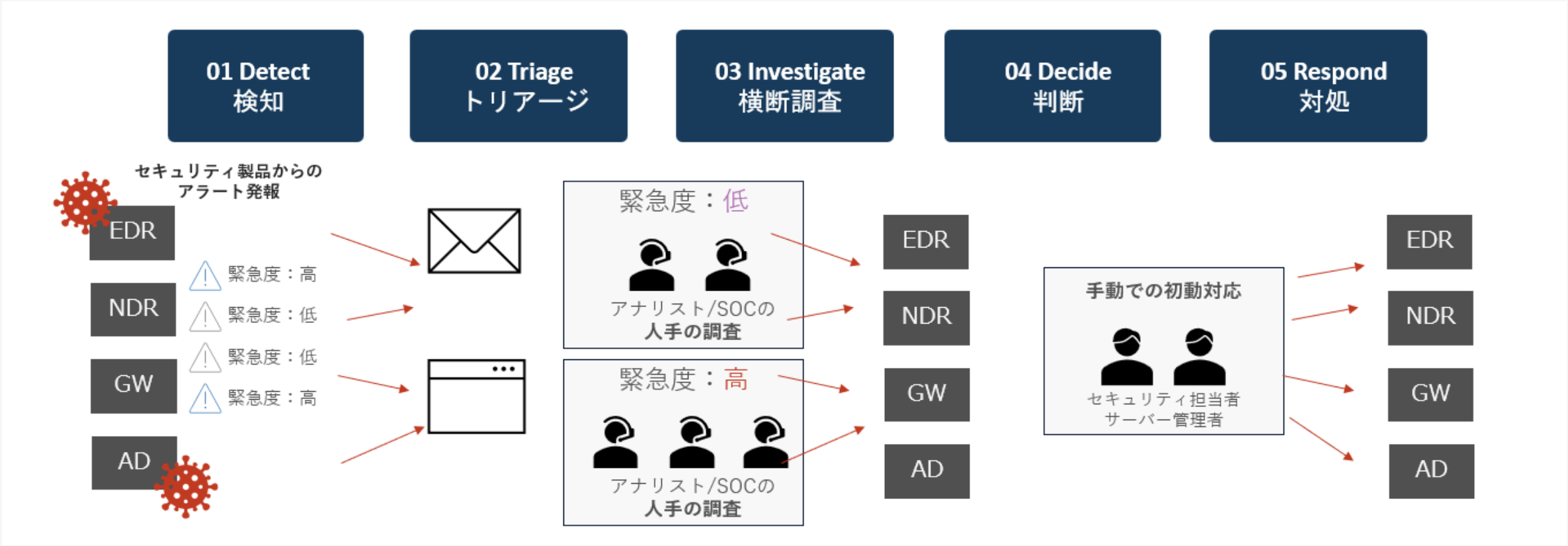
AI自動化フィッシングのクリック率が54%と、通常試行の4.5倍に。

より優れた誘導メッセージが可能となり、標的化が高度になっているとMicrosoftが報告。（出典④）

AI時代において、攻撃の「量、速度、巧妙さ」が進行。防御側にもそれに対応するAIが必要になる。

©Macnica,Inc.

AI時代におけるセキュリティ運用の限界



大量アラート・工数の増加

属人化・人材不足

攻撃速度に対する対応遅延

人手に依存した防御側の運用は限界に直面しており、AIによる変革が必要

©Macnica,Inc.

フロンティア AI は「脅威」にも「盾」にも

「攻撃側と同じ AI を、守る側こそ使っていく」ことが鍵。

脅威 —— 攻撃の“武器”として

- フィッシング・マルウェアを自動作成
- 脆弱性の発見や攻撃を高速・大規模化
- 人を狙う攻撃は、すでに現実に多発

いまは攻撃側がやや優位

盾 —— 守りの“最強の味方”に

- 膨大なログを瞬時に分析し脅威を検知
- 調査～対応を自動化し、対処を高速化
- 脆弱性の発見・修正まで AI が支援

AIの活用が発展中

AI時代における防御側の課題に対するソリューションとして、AI SOCが注目されている。

©Macnica,Inc.

AI SOCとは

AI SOCは「すべてをAIに任せる」ことではない

セキュリティ運用にAIを組み込み、人とAIの役割分担によって運用の速度・処理能力・品質を高めるアプローチ



自律型AI
(Agentic AI)

判断依頼・報告

フィードバック・承認



人間

“AIによる自律的調査と対応の自動化”

データ監視、トリアージ、一次対応などの対応領域に応じた範囲で自動化

- 大量データの整理・分析
- 定型的な調査の高速化
- 判断材料・推奨アクションの提示
- あらかじめ定めた範囲での自律的処理・対応

“組織としての最終意思決定と管理”

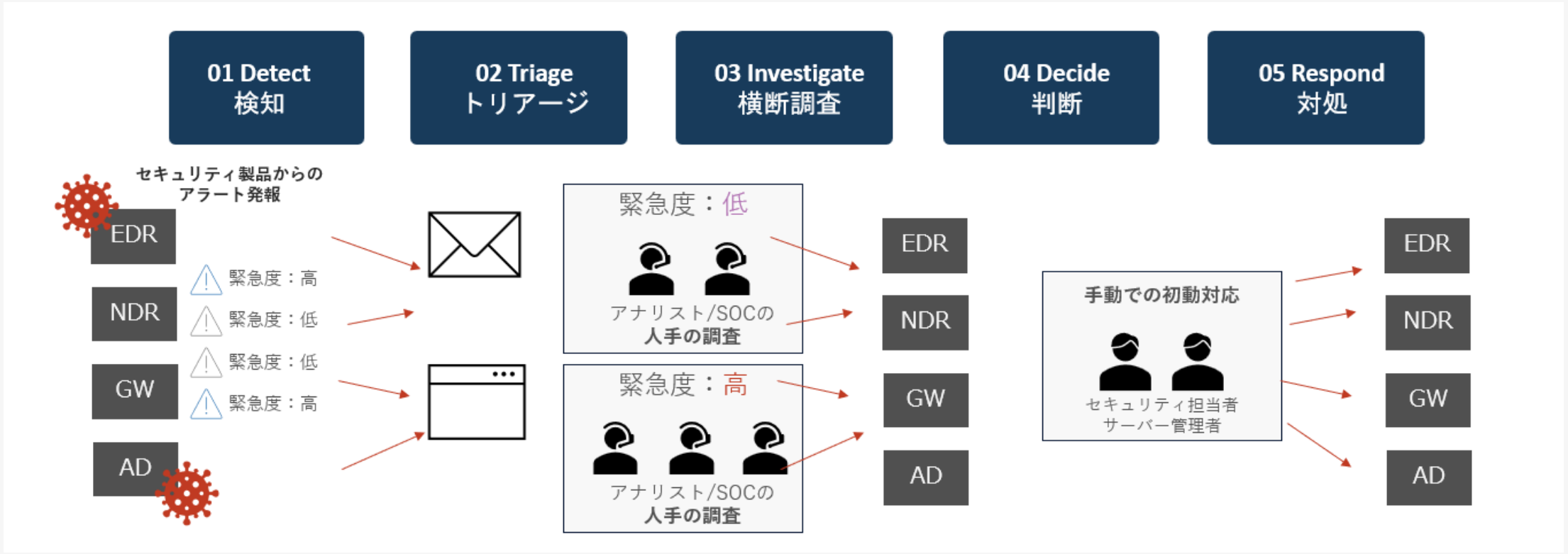
ビジネス影響度に照らした最終意思決定

- ビジネス影響をふまえた判断
- 組織固有の例外判断
- AIに任せる範囲・ルールの設計
- 運用プロセスの改善

Human in the loop：AIが初動を自律実行し、人間が最終判断と改善の役割を担う「協調型」運用

©Macnica,Inc.

AI SOCによって「何が変わるのか」　＜Before＞



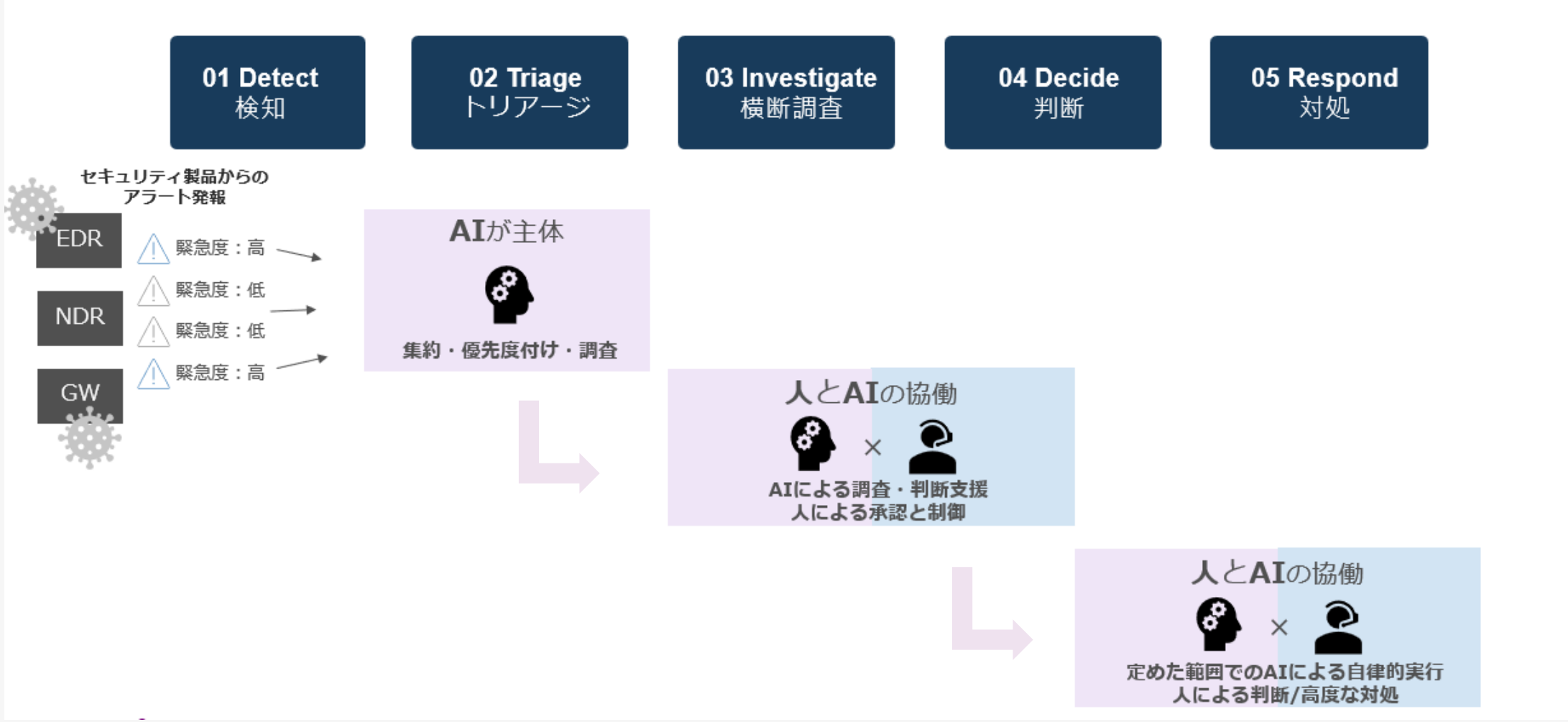
大量アラート・工数の増加

属人化・人材不足

攻撃速度に対する対応遅延

©Macnica,Inc.

AI SOCで変わるセキュリティ運用　＜After＞



人が対応すべき案件に集中でき、対応品質の均一化と初動の迅速化につながる

©Macnica,Inc.

AI SOCをどう選ぶか

©Macnica,Inc.

AI SOC導入検討時に考えたい2つのポイント

重要なのは、「AI SOCを導入すること」ではなく、自社に合うアプローチを見つけること

1.

主導権を、人とAIのどちらにどのくらい持たせたいか
— 人が最終判断を担うか／AIに調査・判断まで委ねるか

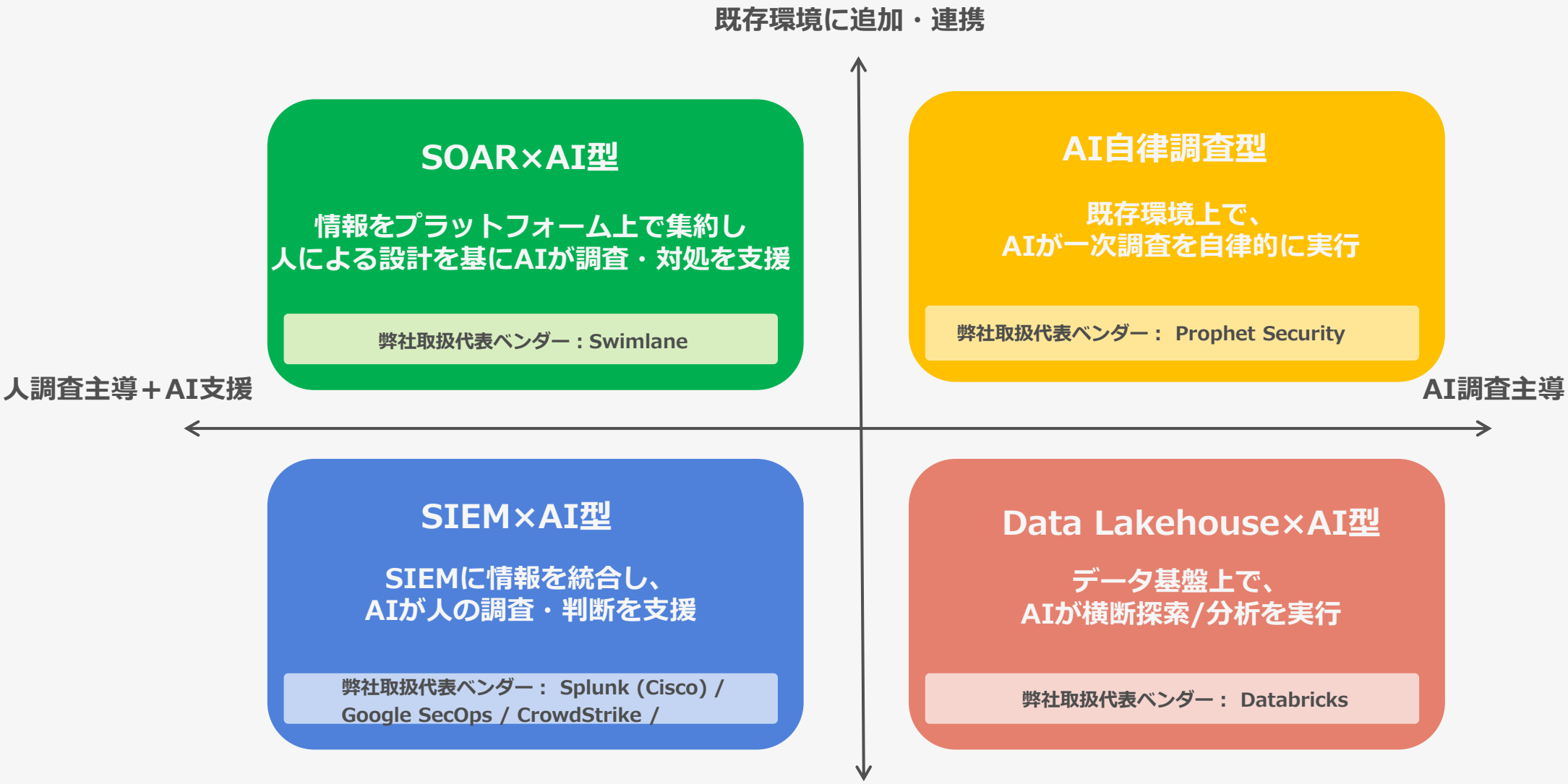
2.

既存環境の、何をどこまで変えたいか
— 今の基盤を活かしたいか／基盤ごと作り替えたいか

どちらの軸も「正解」はありません。
各社のポリシー、既存投資、規制・要件、運用体制によって、最適なソリューションは変わります。

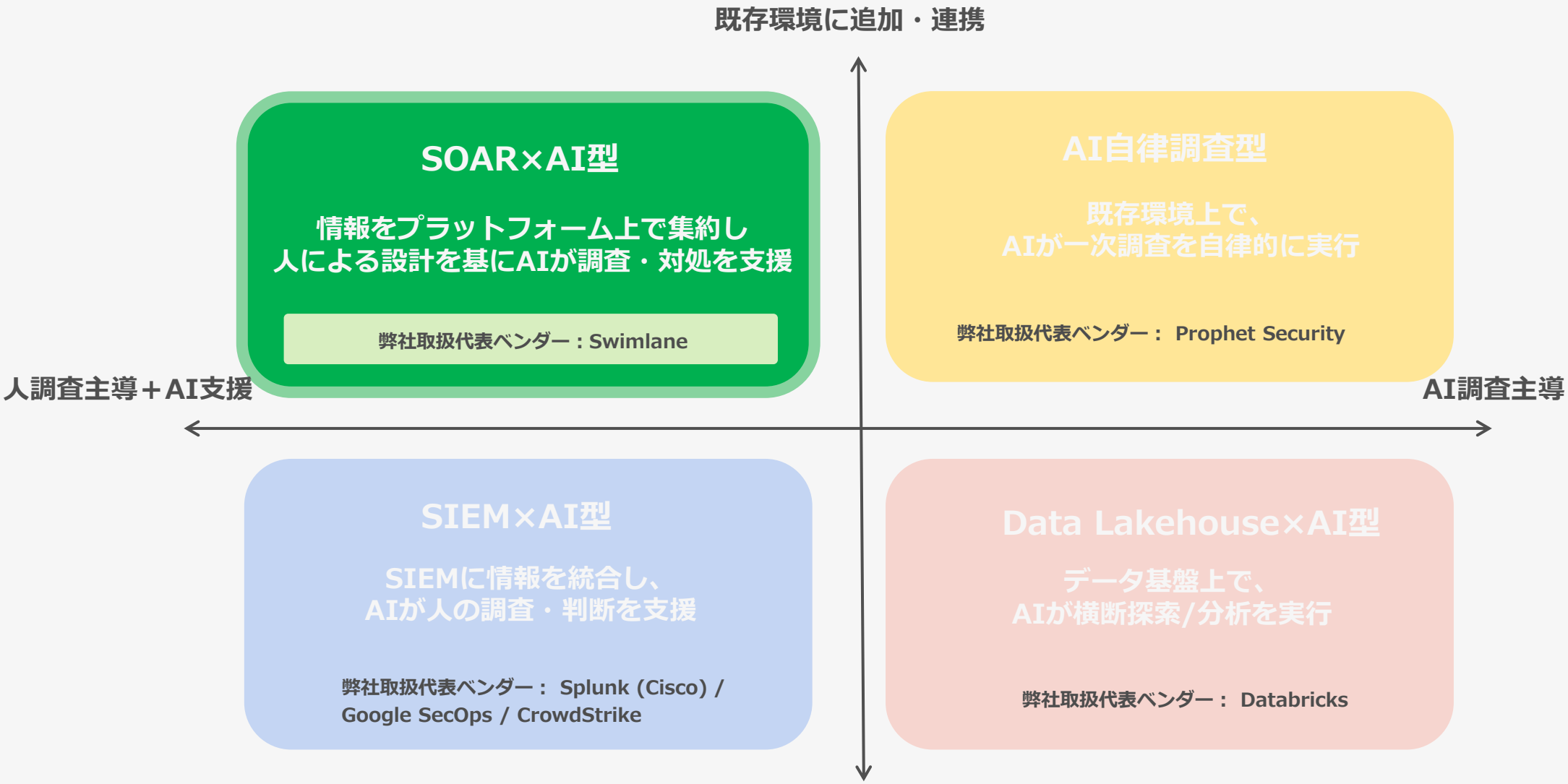
©Macnica,Inc.

マクニカが考えるAI SOC選定マップ



©Macnica,Inc.

マクニカが考えるAI SOC選定マップ



©Macnica,Inc.

代表例　Swimlaneのご紹介

SOAR×AI型

既存環境を活かし、AI×Automationで「調査→対処→運用改善」までを効率・高度化

■Swimlaneはこんなお客様におすすめ！

AIを活用したいが、AI任せにはしたくない

セキュリティ製品はそろっているが、
既存ツール間の”人手つなぎ“を減らしたい

■Swimlaneがその実現を支えるポイント

①AIと人の役割を柔軟に設計
- Playbookをベースに、AI支援/自動化/人の判断・承認を柔軟に設計可能

②今あるセキュリティ環境を活用
- 網羅的なコネクタの提供により、御社既存導入製品と柔軟に連携し、運用全体のハブに

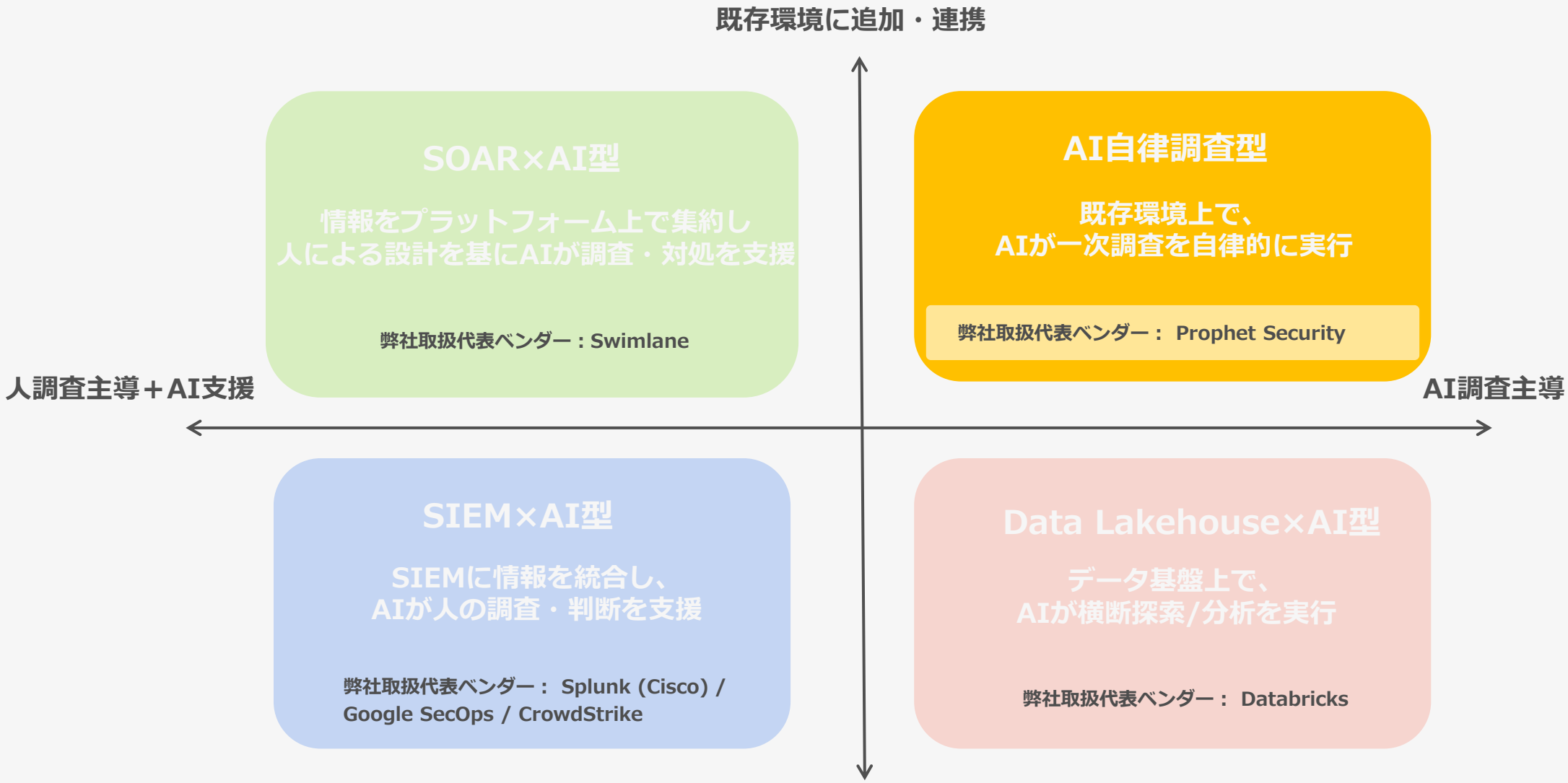


■製品の特徴

1. 独立系ベンダーならではの多数製品との柔軟な連携
2. 自動ケース作成・更新機能によるケース管理の効率化・ダッシュボードでの運用組織全体のボトルネックの可視化
3. AI支援機能、直感的なUIでローコードPlaybook開発が可能
4. Hero AI×Playbookの両輪による自動化範囲の継続的拡張

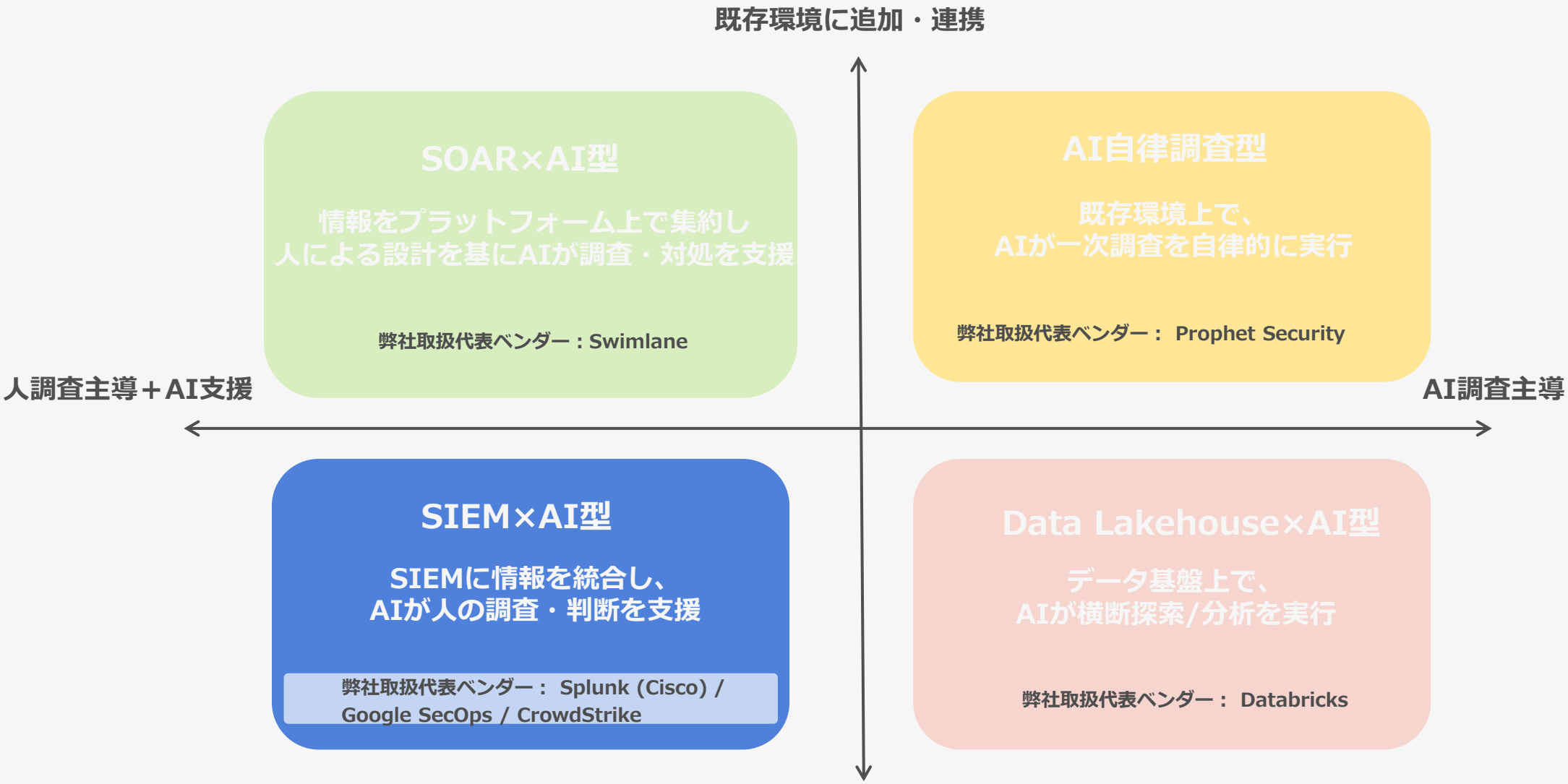
©Macnica,Inc.

マクニカが考えるAI SOC選定マップ



©Macnica,Inc.

マクニカが考えるAI SOC選定マップ



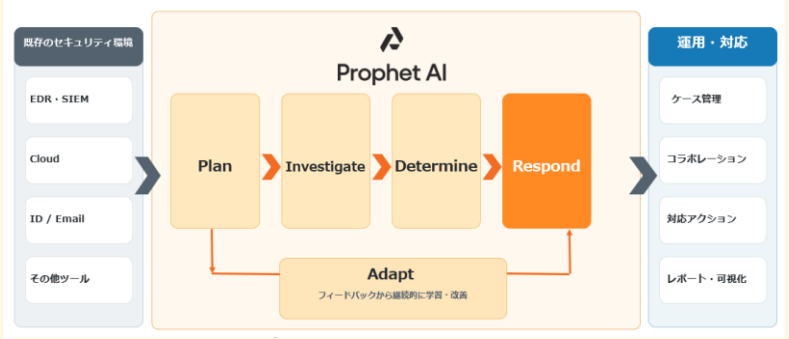
©Macnica,Inc.

代表例　Prophet・GoogleSecOpsのご紹介

AI自律調査型

Prophet：

既存環境を活かし、AIが「調査・判断・対応」を自律的に実行



■Prophetはこんなお客様におすすめ！

人が行っているアラート調査・トリアージを、AIに大きく任せたい

現在導入済みの製品・データソースを活かしたい

■Prophetがその実現を支えるポイント

①AI主体で調査～対処を実行

- アラートと根拠の紐づけ調査、FBを受けた組織ポリシーに合わせた適応までも自律化

②今あるセキュリティ環境を活かした導入

- 既存環境上にアドオンするため、導入～利用開始までがスムーズ

©Macnica,Inc.

代表例　Prophet・GoogleSecOpsのご紹介

SIEM×AI型

GoogleSecOps：

データを統合し、SIEM×AIで「検知→調査→対処」を効率化



■GoogleSecOpsはこんなお客様におすすめ！

人による判断を軸に、AIに調査・分析を支援させたい

SIEMを含むデータ・検知基盤を見直し、
SOC環境全体を統合・高度化したい

■Google SecOpsがその実現を支えるポイント

①AIでアナリストの調査・判断を支援

- Geminiが自然言語でデータ検索～対応推奨、Playbook作成等を支援

②データ・検知基盤から運用までを一体化

- セキュリティデータ収集・調査/分析・SOARによる対応までを統合し、全体を高度化

©Macnica,Inc.

まとめ　一本日お持ち帰りいただきたいこと

なぜ今、セキュリティ運用にAIが必要なのか？

- 攻撃がAIにより高速化、大規模化する中、

防御側もAIを活用してセキュリティ運用を変革していく必要がある。

AI SOCとは？

- セキュリティ運用にAIを組み込み、人とAIの役割分担によって

運用の速度・処理能力・品質を高めるアプローチ。

自社に合ったAI SOCの始め方を判断するための視点とは？

- 重要なのは「AI SOCを導入すること」ではなく、

「AIに任せる範囲」や「既存環境との関係」の観点から自社に合うアプローチを見つけること。

©Macnica,Inc.

御社に合うAI SOCの始め方を、一緒に整理しませんか？

- 既存のセキュリティ環境をどこまで活かせるか
- AIに任せる範囲と、人が判断すべき範囲
- どのアプローチが御社課題に合うか

各製品に興味をお持ちの場合は、
マクニカブースにぜひお越しください。

©Macnica,Inc.

参考文献

1. CrowdStrike, “2022 Global Threat Report - Adversary and Tradecraft Highlights”, CrowdStrike, February 2022,https://www.crowdstrike.com/wp-content/uploads/2022/02/crowdstrike-2022-global-threat-report-infographic.pdf, 参照日：2026年10月20
2. CrowdStrike, “2024 CrowdStrike Global Threat Report: From Breakout to Breach in Under Three Minutes; Cloud Infrastructure Under Attack”, CrowdStrike, February 21, 2024,https://www.crowdstrike.com/en-us/press-releases/2024-crowdstrike-global-threat-report-release/, 参照日：2026年10月20日
3. Adam Meyers, “CrowdStrike 2025 Global Threat Report: Beware the Enterprising Adversary”, CrowdStrike, February 27, 2025,https://www.crowdstrike.com/en-us/blog/crowdstrike-2025-global-threat-report-findings/, 参照日：2026年10月20日
4. CrowdStrike, “2026 CrowdStrike Global Threat Report: AI Accelerates Adversaries and Reshapes the Attack Surface”, CrowdStrike, February 24, 2026,https://www.crowdstrike.com/en-us/press-releases/2026-crowdstrike-global-threat-report/, 参照日：2026年10月20日
5. Stephanie Carruthers、”AI vs. human deceit”、IBM、2025年11月19日、AI vs. human deceit: Unravelling the new age of phishing tactics | IBM、2026年10月5日
6. CrowdStrike、CrowdStrike 2025 Global Threat Report、CrowdStrike、2025年2月、クラウドストライク2025年版グローバル脅威レポート：エグゼクティブサマリー、2026年10月5日
7. Heiding, Lermen, Kao, Schneier, Vishwanat 、Evaluating Large Language Models’ Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects、Harvard Kennedy School、2024年11月、(PDF) Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects、2026年10月5日
8. Microsoft、Microsoft Digital Defense Report 2025、Microsoft、2025年10月、2026 Microsoft Digital Defense Report – Decoding emergence、2026年10月5日

©Macnica,Inc.

ご聴講いただきありがとうございました。

ぜひアンケートにご協力ください。



©Macnica,Inc.