elastic | The Search AI Company

モダンセキュリティオペレーションにAIが必要な理由と、なぜ今なのか？

Elasticsearch株式会社
叶 彩 | Aya Kano

2024年9月10日

Who Am I?

- 10年以上システムエンジニアとして組み込みシステムの開発を担当
- 5年間セキュリティエンジニアとしてSIEM検知ルールの設計やチューニング、マルウェア解析、デジタルフォレンジックを担当
- 3年以上にわたりクラウドソリューションアーキテクトとして主にセキュリティソリューションの技術支援を担当

elastic

SOCが抱える現在の課題

急速に変化する環境

マルチクラウドやハイブリッド環境は、監視、管理、対処が困難である

洗練された攻撃者

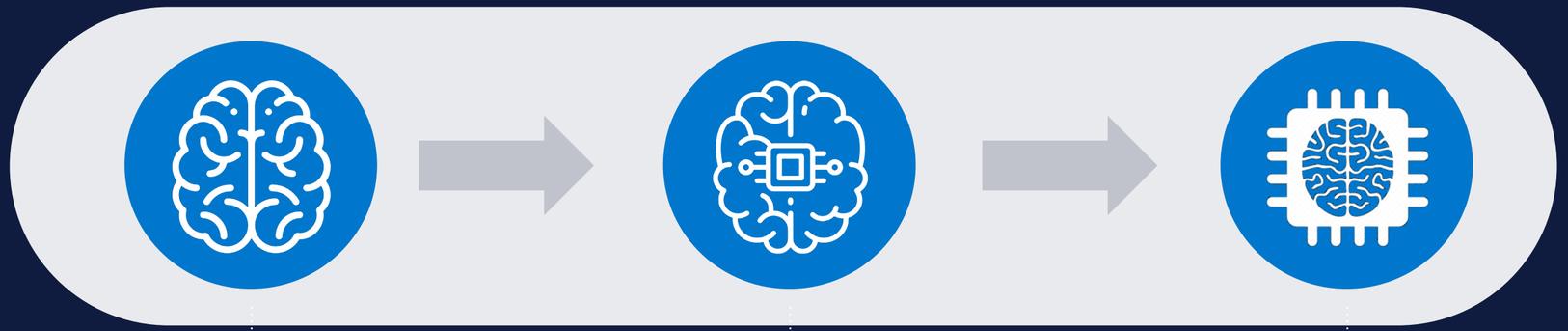
洗練された敵が増加し、グローバルなサイバー犯罪のエコシステムがその勢力を拡大している

過負荷のSOCチーム

セキュリティ専門家の雇用と確保が依然として困難である

elastic

自動化がよりスマートに



アシスト
インテリジェンス

反復的で標準化
された作業の自動化

明確に定義された
反復可能なタスク

拡張インテリジェンス

人間と機械の
コラボレーション

需要と供給と共有

自律的インテリジェンス

適応型インテリジェンスの
自立した意思決定

自動運転

elastic

従来の分析と高度な分析

	従来の分析	高度な分析
スコープ	個別領域	複数の領域にまたがる
方法	イベントレベルでの条件分析	エンティティレベルでのMLによる行動分析
汎用性	静的ルールロジックは定期的なメンテナンスが必要	モデルはトレーニングによって自動的に適応
既知の脅威の検出	既知の攻撃活動の検出に優れている	リスクを確率的に評価
未知の脅威の検出	未知の脅威に対するルールはない	事前に定義されたルールなしで異常を検出
アラートのノイズ	厳格なルールのためノイズが多い	残存ルールのノイズを低減

elastic

データを新たな次元で見るエンティティ分析

ホスト

エンド
ポイント

サーバ

クラウド
資産

ユーザ

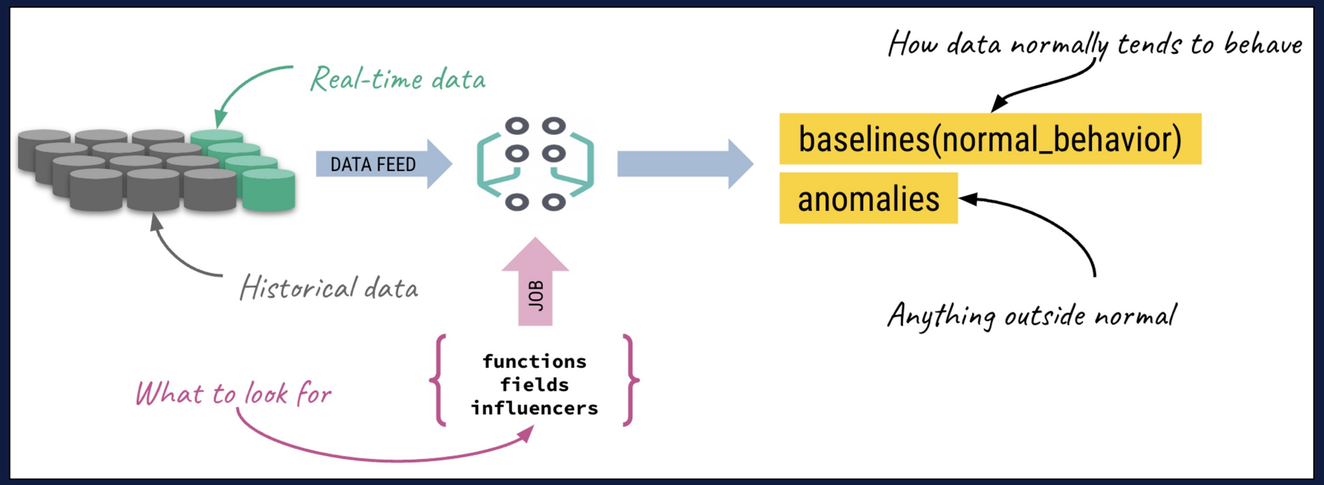
ユーザー
アカウント

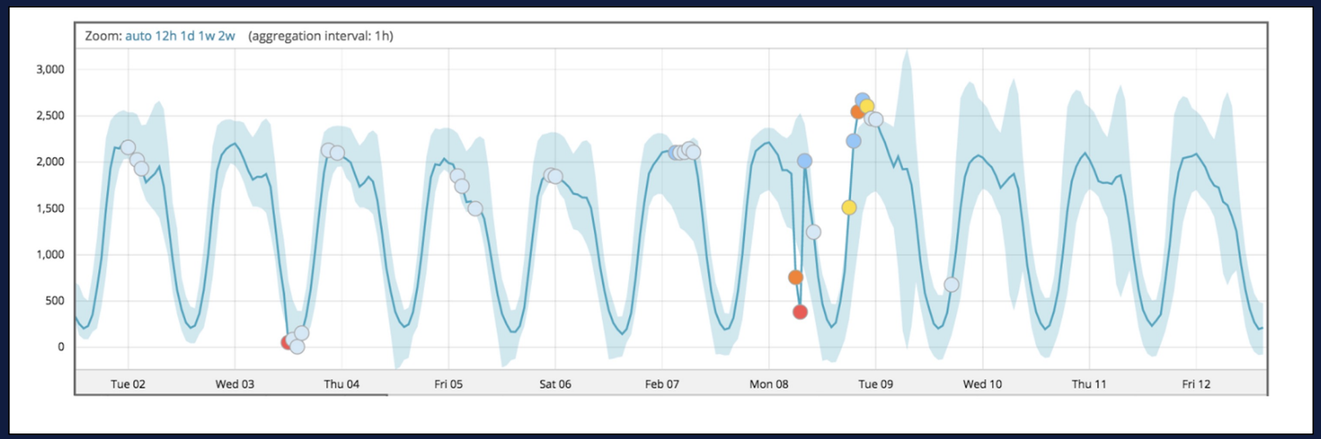
サービス
アカウント

elastic

高度なエンティティ分析により隠れた脅威を検出

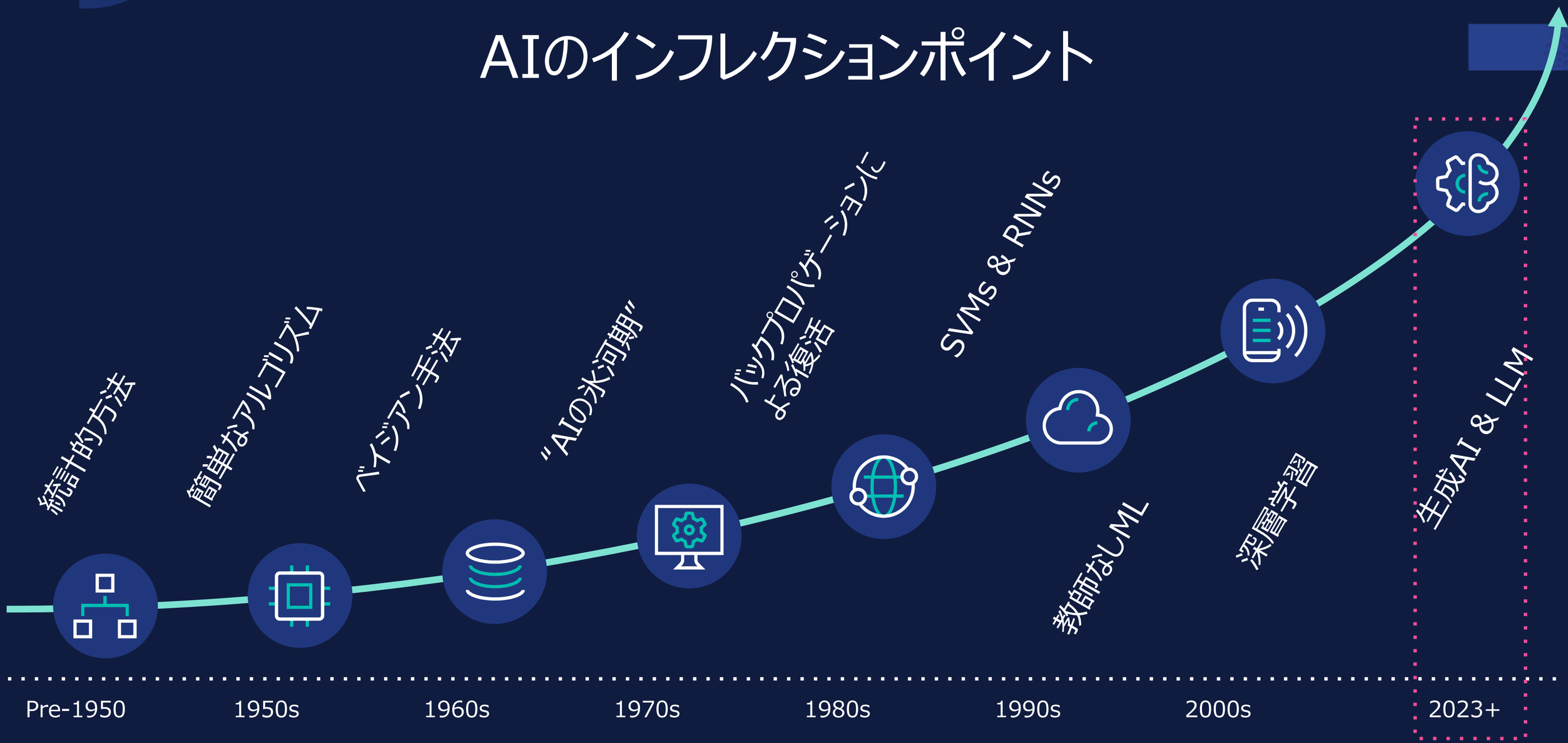
- アラートをエンティティ分析で補完することで、未知の脅威を発見する
- イベントとアラートを分析することで、異常なエンティティの動作を特定する
- SIEMの中で最も成熟したMLですぐに価値を得る





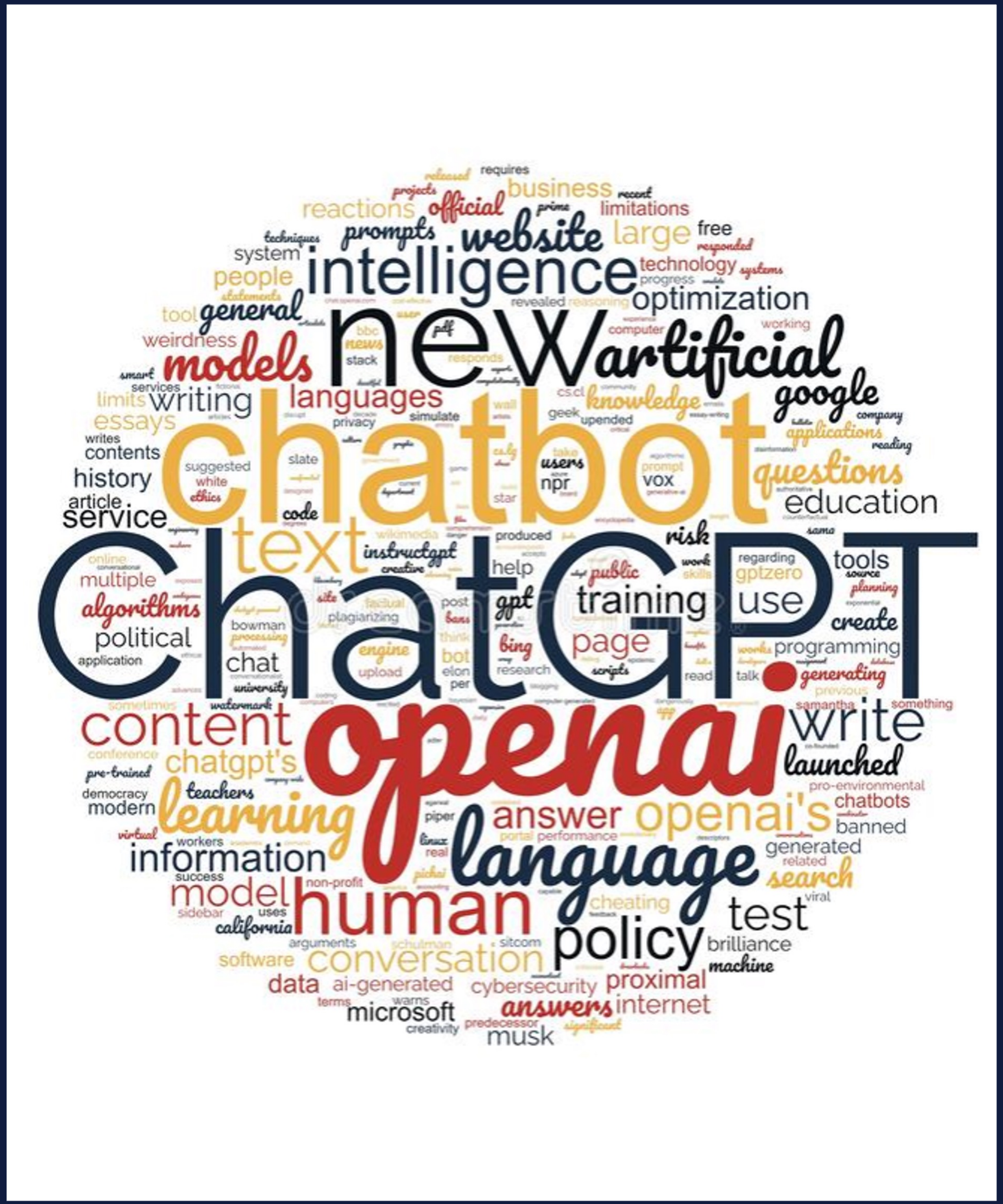
elastic

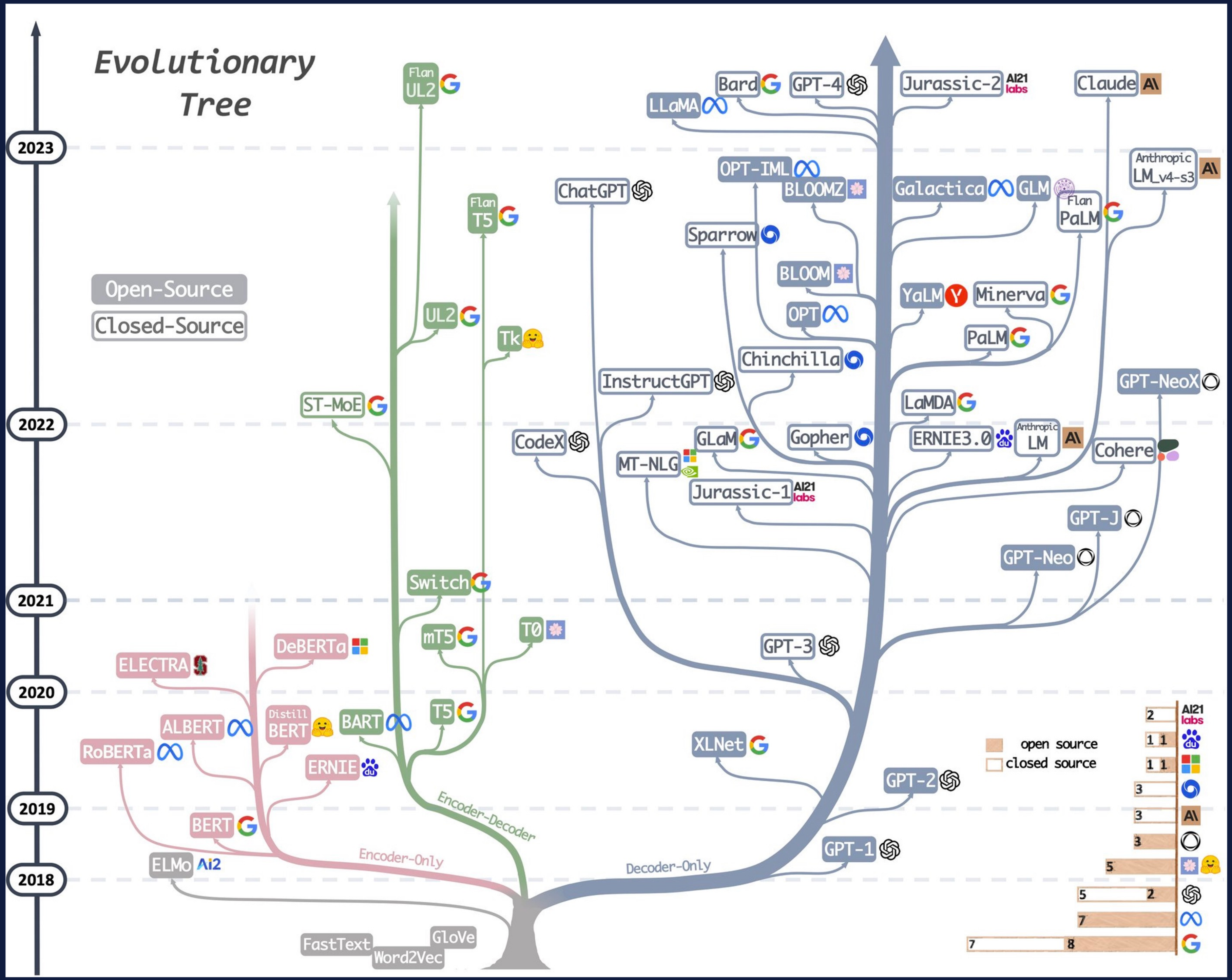
AIのインフレクションポイント



elastic

LLMと生成AIの急激な台頭





生成AIが検索に革命を起こす

人間的で反復的なコンテンツ作成に優れている

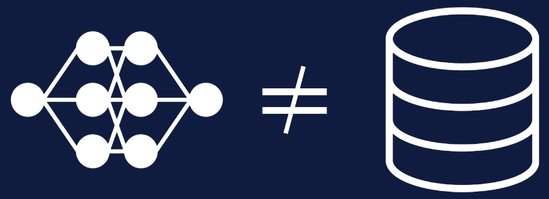
人間のような会話を作成したり、コンテンツを書いたり、コード例を提供したりするために使用される、大規模なデータセットの自然言語処理である。

公開トレーニングデータ、一般的なコンテキストによる制限

訓練されたデータと同程度の性能と最新性しかない。
特にドメイン特有の質問をされると、幻覚（自信ありげに聞こえるが誤った出力）を見ることがある。

elastic

LLMの課題



大規模言語モデルは
データベースではない

公開データで
トレーニング

生成AI 単体では、トレーニングに使用されたデータと同等の品質しか得られない。大規模な基礎モデルは、多くの場合何年も前のものであり、プライベートデータの知識がない大規模な公開情報セットに基づいてトレーニングされている。

時代遅れ

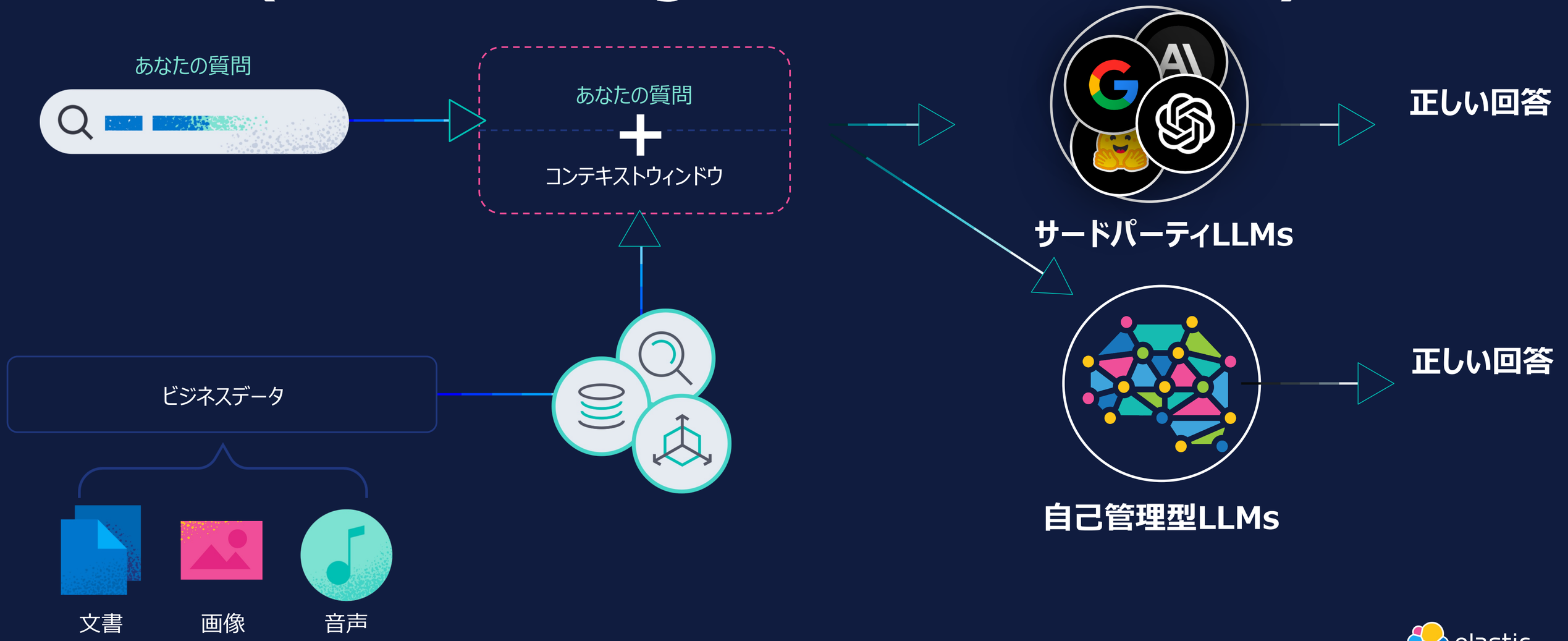
LLM の知識はトレーニング データが収集された時点から凍結され、ライブ更新することはできない。トレーニングや微調整には専門知識が必要であり、コストがかかる場合がある。

幻覚
(Hallucinations)

トレーニング データを超える質問に直面すると、生成AI は幻覚を起こし、ユーザーに誤った自信に満ちた答えを提供し、ユーザーを意図せず　誤解させる。これはミッションクリティカルな環境では受け入れられない。

elastic

検索拡張生成
(Retrieval Augmented Generation)



elastic

生成AIによるSIEMの進化

SIEM 1.0 - 2000s

SIEMの誕生

- ログの一元化
- コンプライアンスとIRにフォーカス
- オペレーション機能
- セキュリティチーム向けの可視化

SIEM 2.0 - 2010s

検出、分析、オーケストレーション

- 他者が見逃した脅威を発見
- MLがルールベースの検出を強化
- 分析主導の調査
- UEBAがコアユースケースに追加
- レスポンスと修復ワークフロー

SIEM 3.0 - 2023+

生成AI革命

- AI活用の組み込みワークフロー
- 関連性と自動化にフォーカス
- アラートではなく、攻撃を優先
- スキルギャップの課題への対応

レガシー　現行　未来

elastic

AIを活用したセキュリティアナリティクスにより、
SecOpsチームはあらゆるデータソースからリアルタイムで
検知、調査、対応することができます。

elastic

AIを活用したセキュリティ分析ビジョン

セキュリティ分析の要点

ファーストおよびサードパーティの組織的対応

継続的なリスク認識

脅威の相関性の調査

高度な脅威検知

オープンスキーマ、全体的な可視性、分散検索可能なデータレーク

すべてのワークフローにAIを組み込む

- **回答に関する推奨事項**
- **AI主導のランブック**

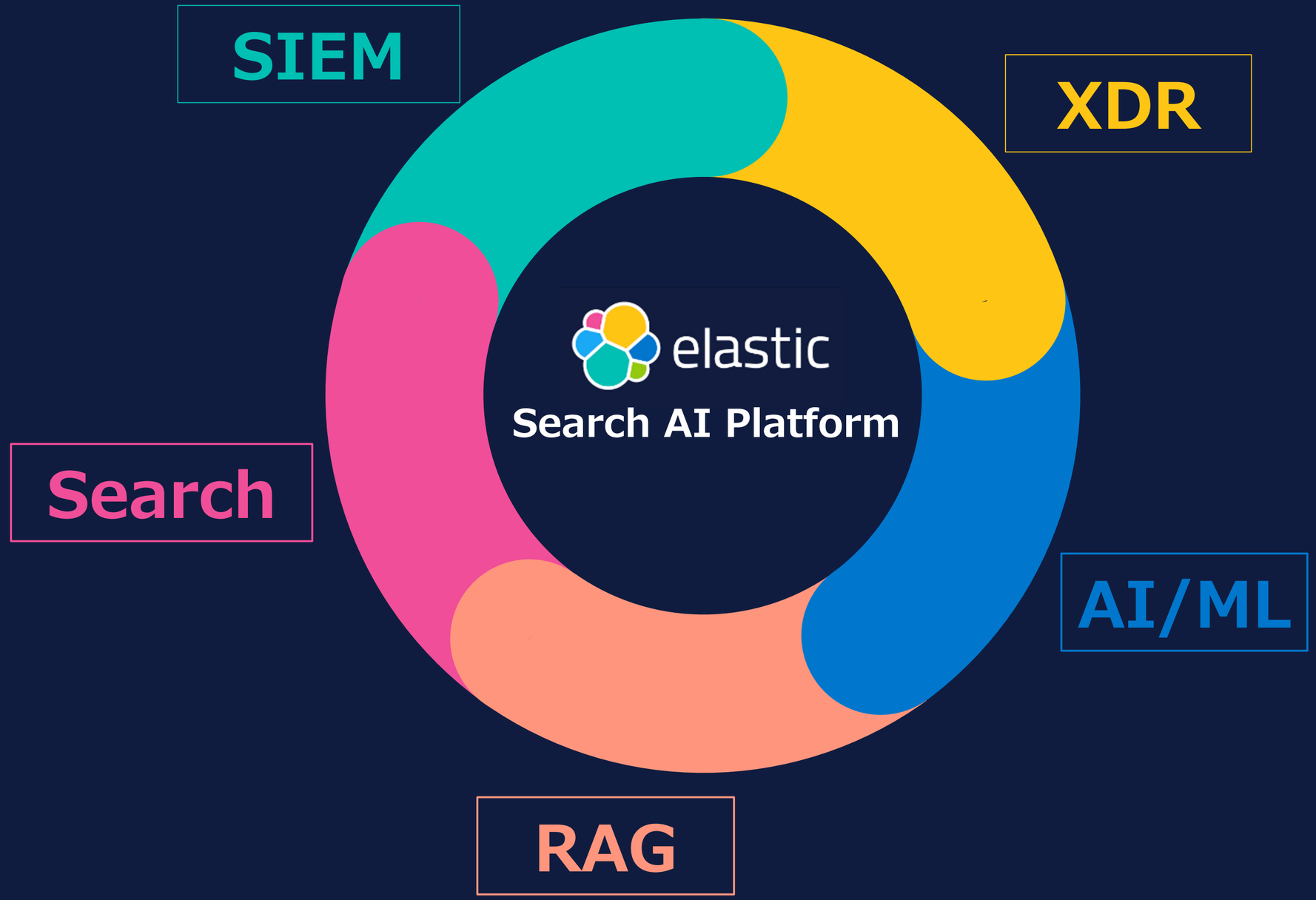
- **AIを活用したリスク評価**

- **AIによる攻撃発見**
- **調査およびトリアージガイド**

- **AIによるルール／クエリ変換**
- **脅威の説明とナレッジベース**

- **インジェストとパイプラインの推奨事項**
- **AIを活用した統合**

elastic



elastic

リアルタイムで適切な結果を提供する セキュリティソリューション

参考情報

Elastic Cloud 2週間無料トライアル
https://cloud.elastic.co/registration?elektra=en-cloud-page

Elastic Security導入事例
https://www.elastic.co/jp/customers/success-stories?usecase=security-analytics&industry=All

Elastic ビデオ&ウェビナー
https://www.elastic.co/jp/videos

elastic

Thank you!