DARKTRACE

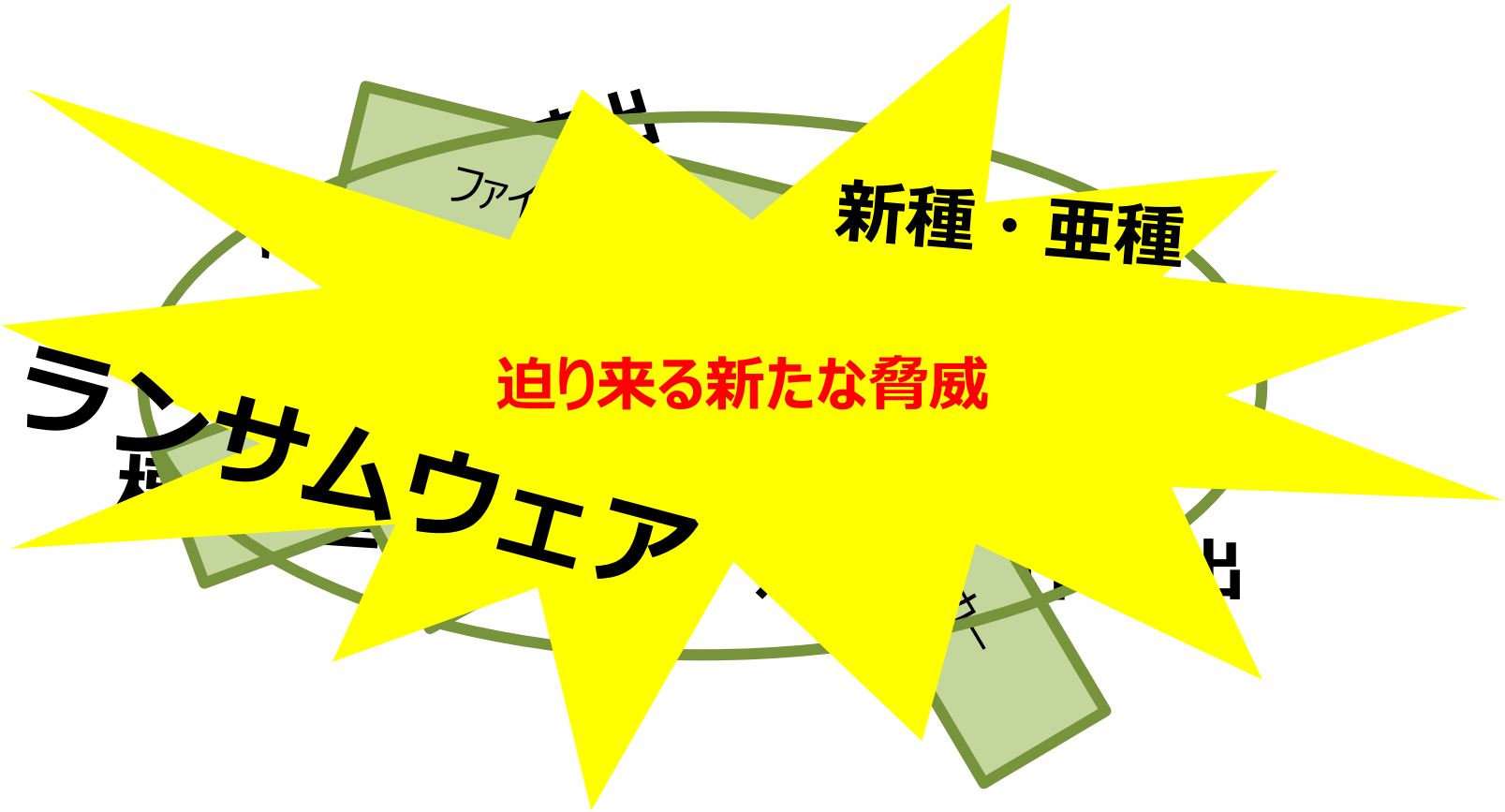
サイバーセキュリティにおける新たなアプローチ

Darktrace Enterprise Immune System　のご紹介

株式会社サムライズ
マーケティンググループ

SAMURAIZ

サイバーセキュリティの実情



どうしたら良いのか？

「Darktrace Enterprise Immune System が終止符を打ちます。」

どうしたら終止符が打てるのか？

DARKTRACE

ルールや事前の定義に基づく以上、未知の攻撃はなくならない！

ルールや定義に基づかず、攻撃や脅威を検出する！

SAMURAIZ

どうやって検出するのか？

DARKTRACE

ネットワーク上のデバイスの通常の動きと比較

通常と異なる怪しい挙動

SAMURAIZ

怪しい兆候とは・・・？

DARKTRACE

URL
IPアドレス

時間帯

怪しい挙動

ポート
スキャン

サーバー
アクセス

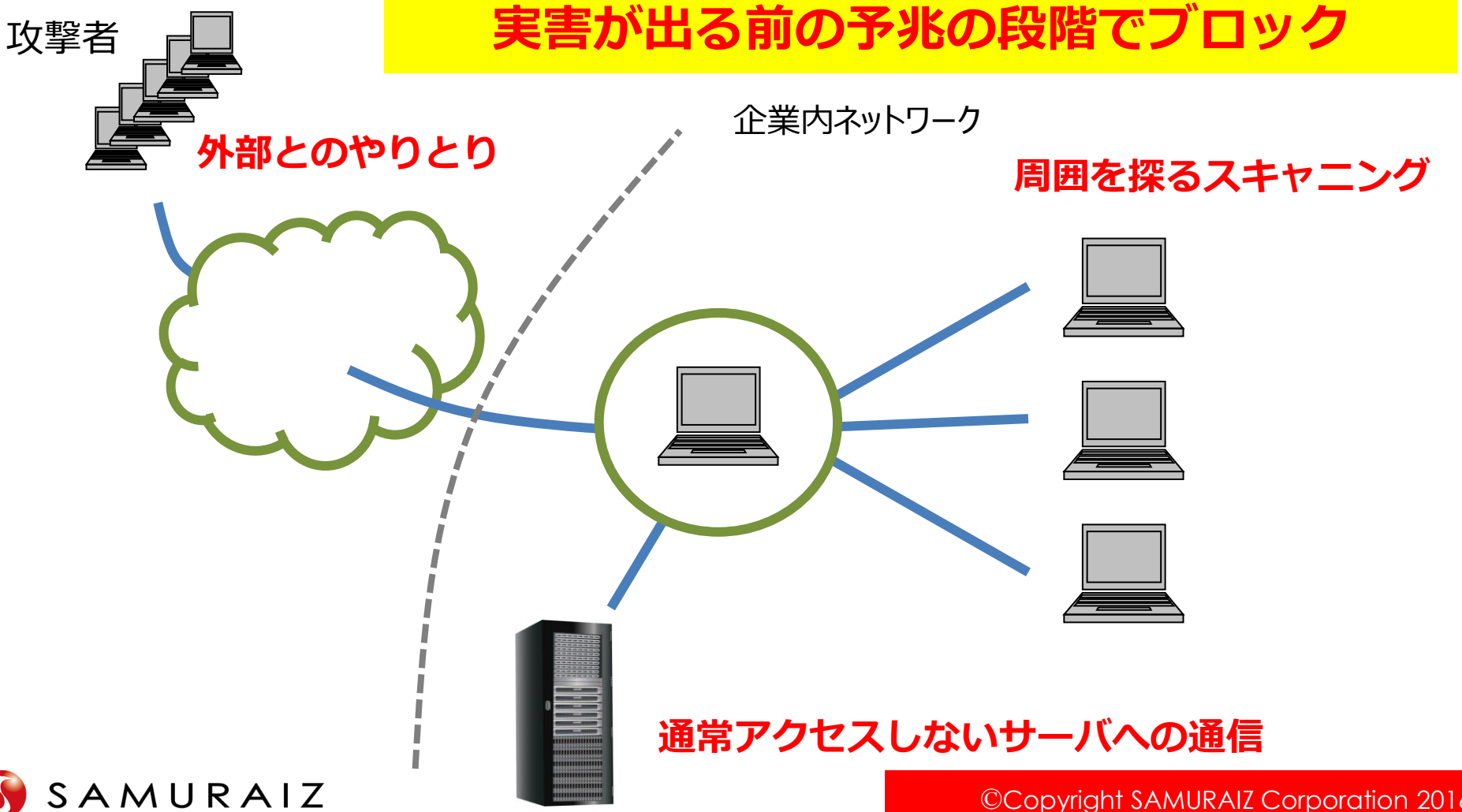
SAMURAIZ

検出パターン例

DARKTRACE

例えば、「マルウェア」

データ流出などの
実害が出る前の予兆の段階でブロック



SAMURAIZ

まとめ

DARKTRACE

未知の脅威や潜在的な危機を想定し事前に定義して防御するのではなく、

防御しきれないことを前提として、
それらが起こす怪しい挙動を検知する

SIEMの構築で最も困難な
ネットワーク全体のリアルタイムな可視化を迅速に実現

SAMURAIZ

Enterprise Immune System とは？

新たなアプローチを実現するために英国ダークトレース社が提供する、

セキュリティモニタリング用のアプライアンス製品

■ダークトレース社

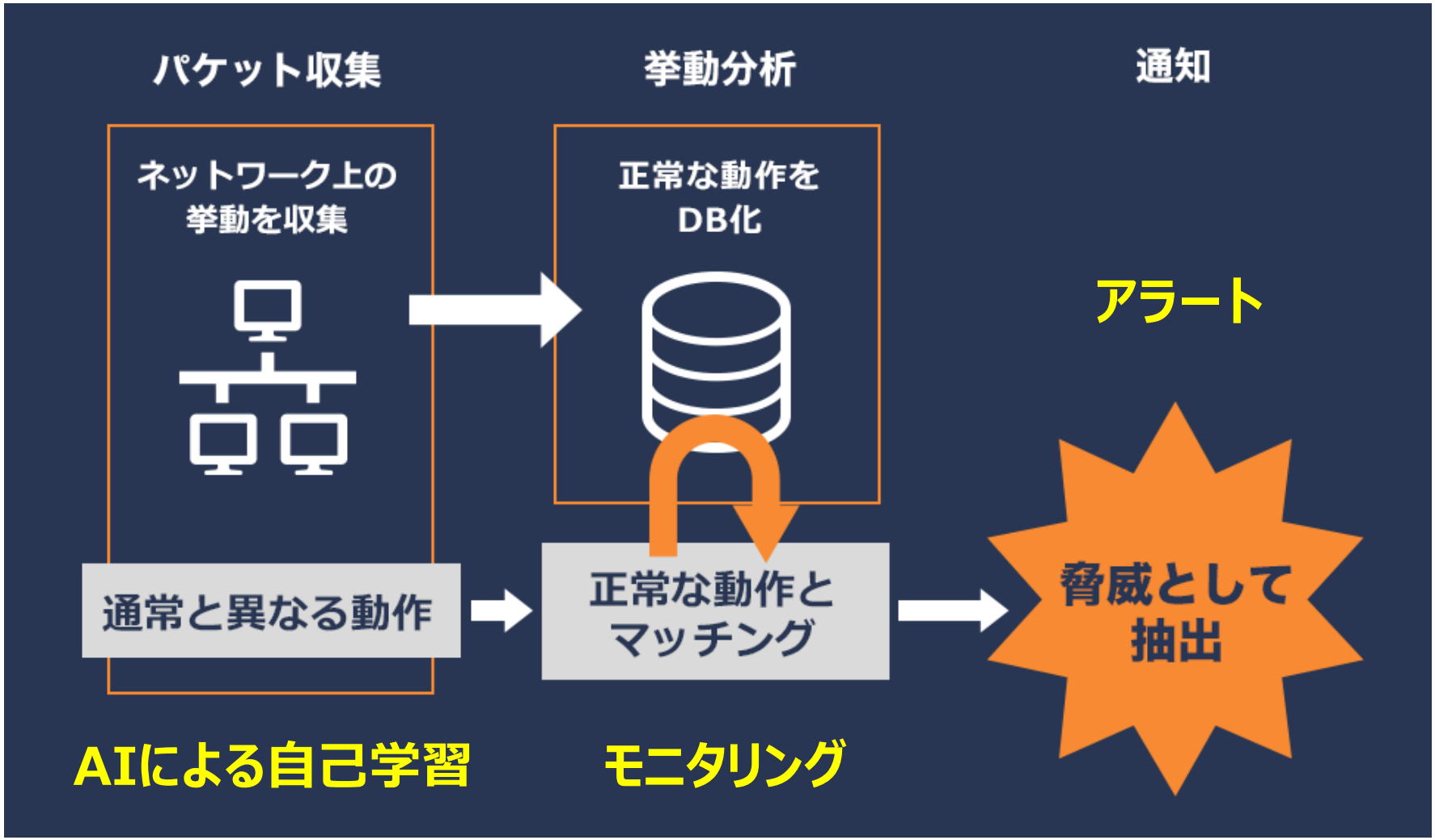
数学者と政府情報機関のスペシャリストにより、2013 年英国ケンブリッジにて設立

英国ケンブリッジ、米国サンフランシスコを本拠点とし、21カ所にオフィスを展開

全世界で1,200社以上の導入実績、16,000以上の脅威を検出

具体的には・・・。

DARKTRACE



SAMURAIZ

Enterprise Immune System の特徴

DARKTRACE

- 事前の定義を必要とせず、自己学習してモニタリングを開始
- メンテナンスフリー
- 既存のセキュリティを否定するものではなく強化するもの

SAMURAIZ

Enterprise Immune System の位置付け

DARKTRACE

External threat intelligence

防御		対処
ファイアーウォール	セキュリティ対策が健全に機能	セキュリティインシデント管理
侵入検知	していることをモニタリング	
アンチウイルス		

エンドポイント機器の保護

セキュリティログの統合管理

SAMURAIZ

デモ

DARKTRACE

SAMURAIZ

Enterprise と Industrial に違いは？

DARKTRACE

Enterprise Immune System → **通常の企業ネットワーク向け**

Industrial Immune System → **制御系ネットワーク向け**

SAMURAIZ

Enterprise Immune System の効果

DARKTRACE

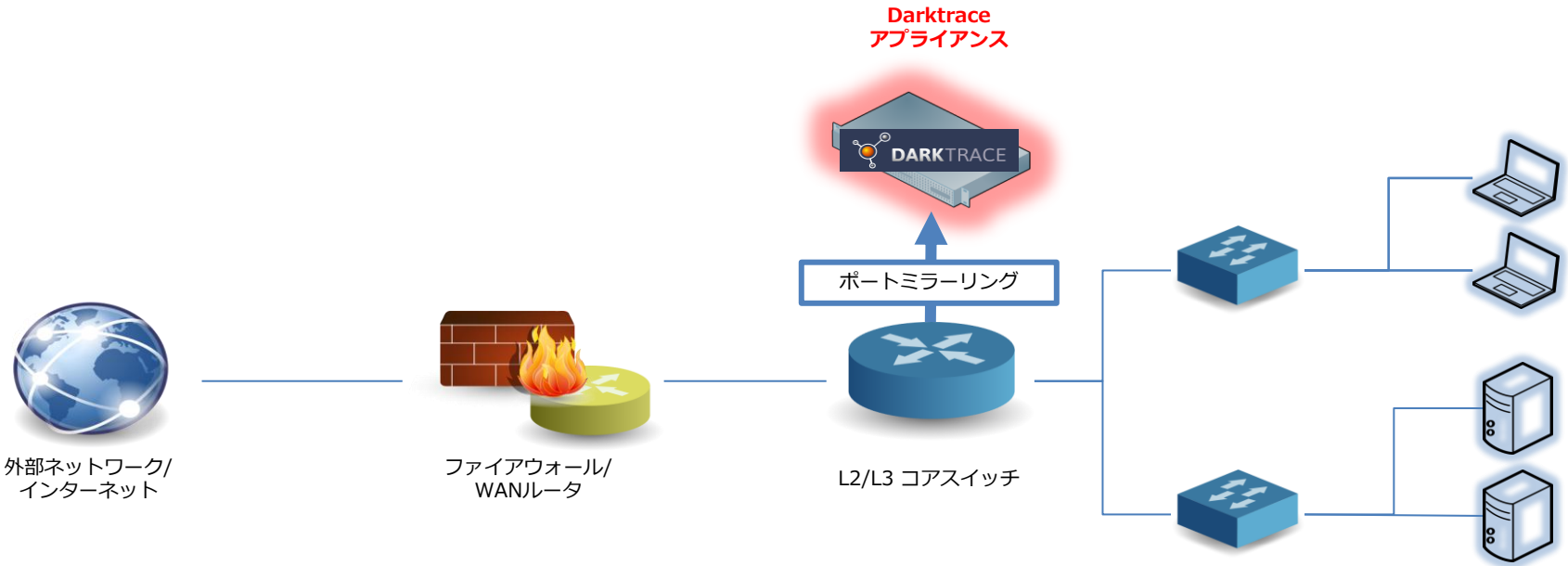
- マルウェア/ランサムウェアをはじめとした未知の脅威対策
- 内部からの脅威対策
- 内部統制の効果
- SIEM、SOCの構築において困難なネットワーク全体のリアルタイムな可視化を迅速に実現
- セキュリティ対策が健全に機能していることをモニタリング

9月13日付 ニュースリリース

- Enterprise Immune Systemの脅威検知対象をSaaSアプリケーションに拡大
  - SaaSアプリケーションに接続する各デバイスのログイン情報、データ通信およびダウンロード、アップデート情報を常に可視化することで、クラウド上の疑わしい振る舞いや異常な挙動のリアルタイム検知が可能になりました。
  - Salesforce.com、Box、Google Apps、Microsoft Office 365 については、ユーザーのやりとりを100%可視化することが可能

アプライアンス概要

- ポートミラーによるパケット収集
- 監視対象ノード数に応じたサーバー構成
  – S（1,000）、M（10,000）、X2（35,000）
- 階層化構成による複数トポロジーの一括管理



参考価格

タイプS（1,000）
月額24万円

タイプM（10,000）
月額110万円

タイプX2（35,000）
月額288万円

（各1年契約の場合）

3週間のPoV（Proof of Value）

- 3週間の無償トライアル
- 毎週検出結果をご報告 ＆ 脅威度の確認
- 導入価値のご判断

お問合せ先：

株式会社サムライズ
マーケティンググループ

〒141-0032 東京都品川区大崎1-6-4 新大崎勧業ビル10F
TEL: 03-5436-2044

http://www.samuraiz.co.jp/
http://www.facebook.com/SamuraizCorp