サイバーセキュリティの新たなアプローチ

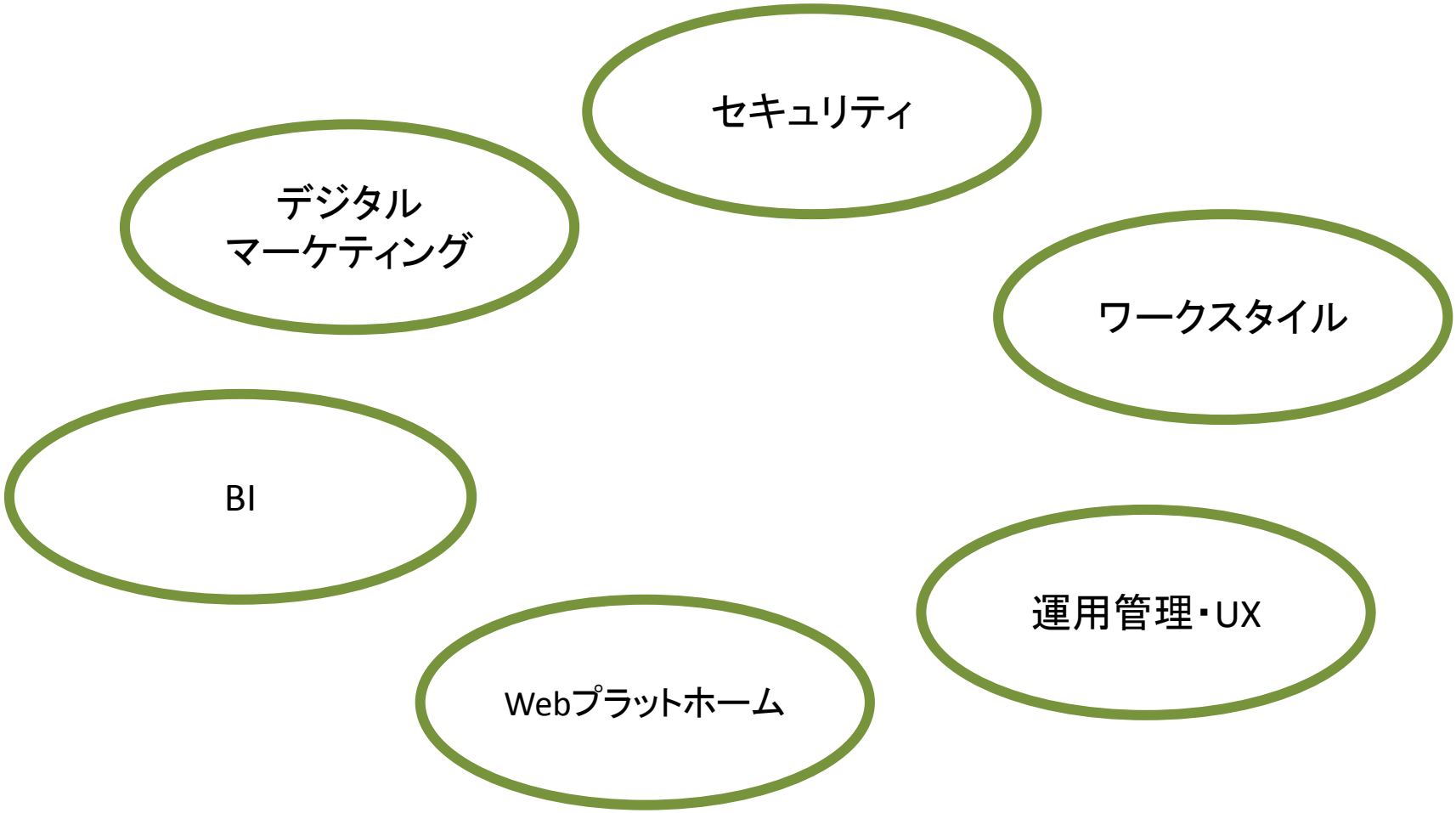
未知なる脅威、潜在的な危機を未然に防ぐには？

株式会社サムライズ
マーケティンググループ
ビジネスデベロップメントユニット
藤井義隆

SAMURAIZ

サムライズのご紹介

2006年創業



SAMURAIZ

サイバーセキュリティの新たなアプローチ

従来のセキュリティのアプローチ

何が危険なのか？

従来のセキュリティのアプローチ

危険と判断されたものを排除する！

従来のセキュリティのアプローチ

危険と判断できないものは察知できない！

従来のセキュリティのアプローチ

察知するために更新され続ける必要がある

従来のセキュリティのアプローチ

検知するためのルールやシグニチャを
常に完全な状態にすることは難しい

新たなアプローチとは？

危険と判断された **もの/事象** を検知しようとするのではなく、

それら が起こす **怪しい兆候を検知** する。

怪しい兆候とは・・・？

URL
IPアドレス

時間帯

通常と合致しない異常な挙動

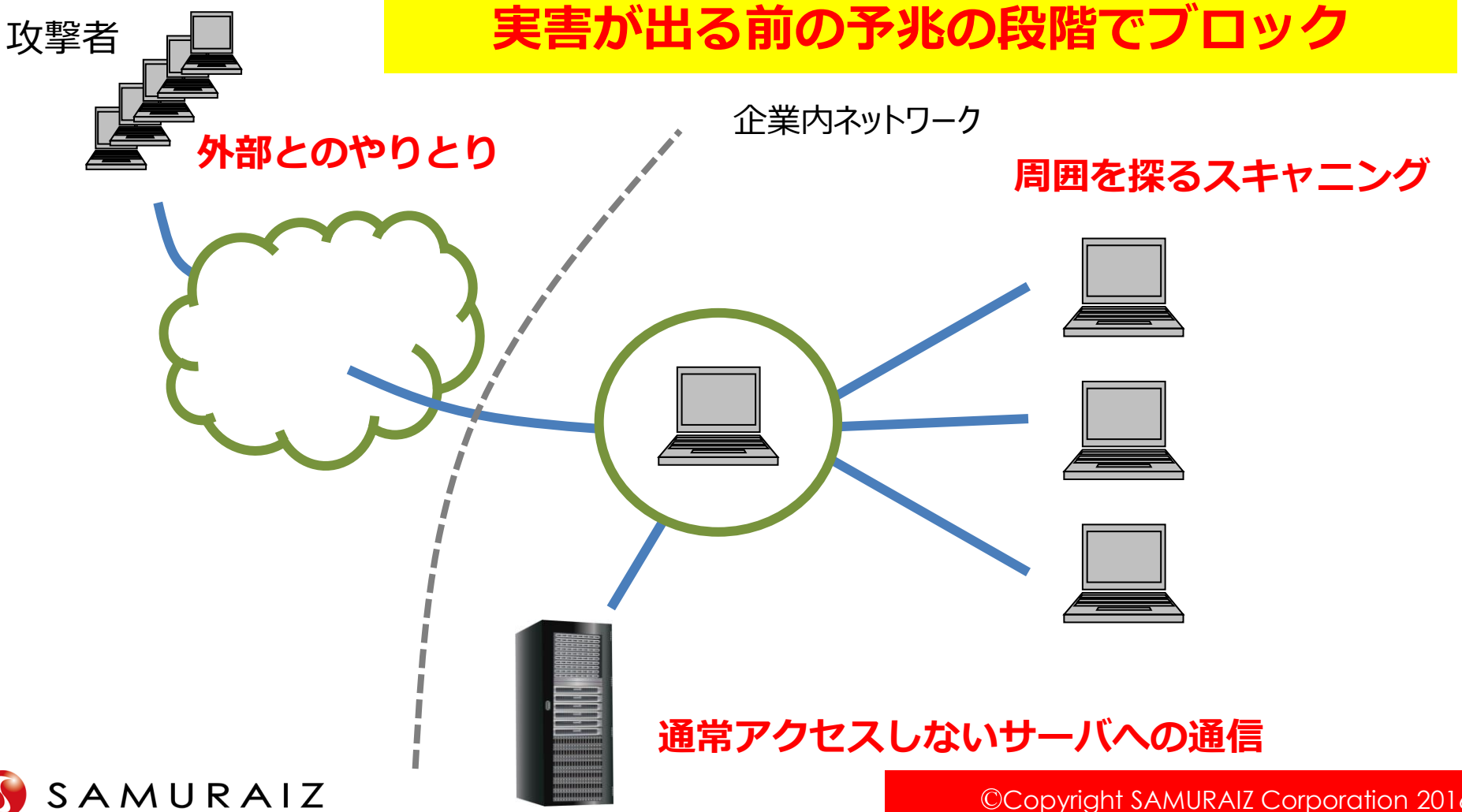
ポート
スキャン

サーバー
アクセス

検出パターン例

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

未知の脅威や潜在的な危機をブロックするのではなく、

遭遇してしまうことを前提として、
遭遇した結果起こる事象を検知するというアプローチ

SIEMでは実現しえなかった
ネットワーク全体のリアルタイムな可視化

セキュリティモニタリングソリューション

Darktrace Enterprise Immune System
Darktrace Industrial Immune System　のご紹介

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

なぜ Immune（免疫）なのか？

人体が多様な外的や環境変化（感染、発病等）に対抗する仕組みを
ITセキュリティに応用している

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**

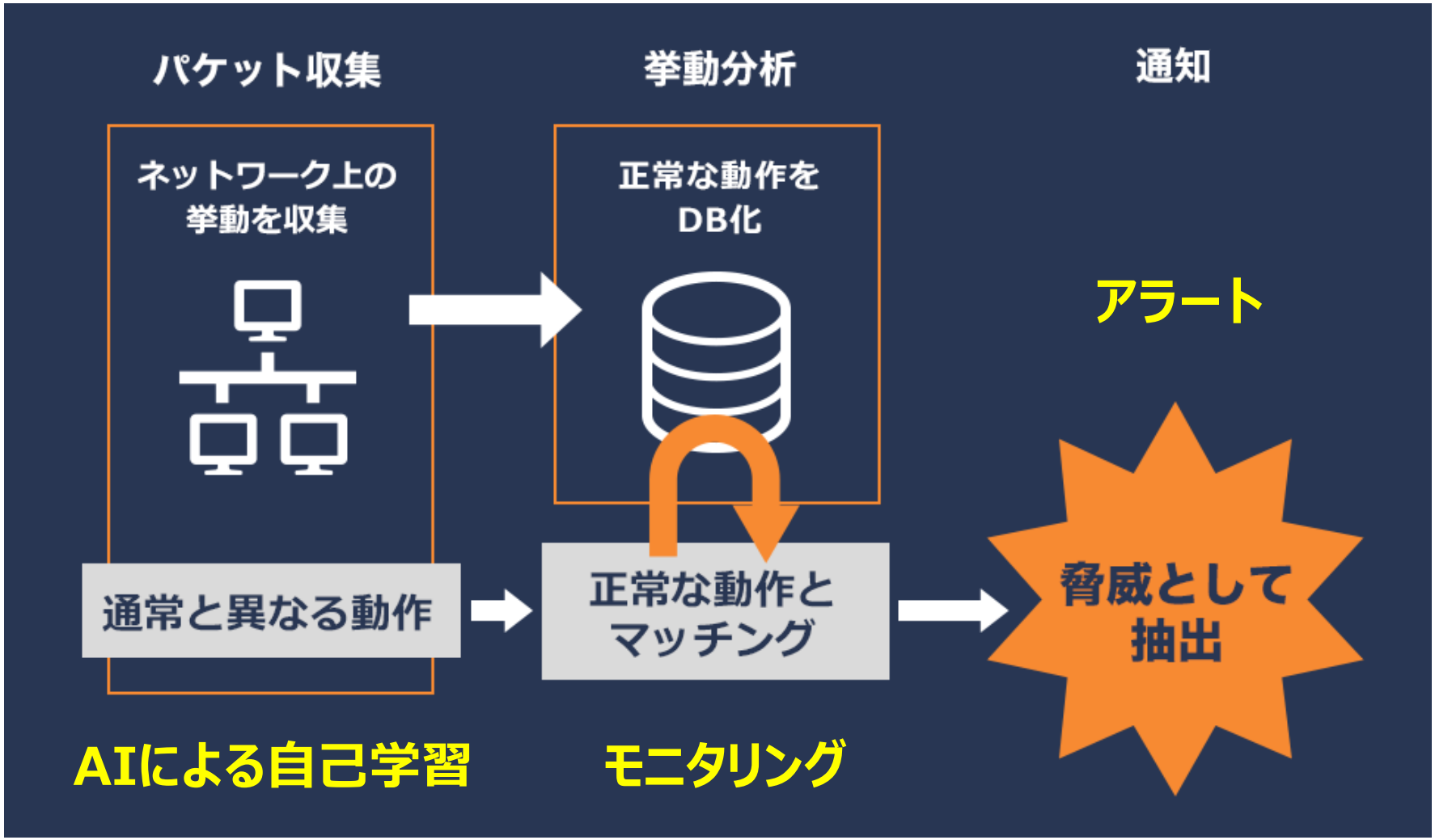
SAMURAIZ

最新ニュースリリース（9月13日付け）

- 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

具体的には・・・。

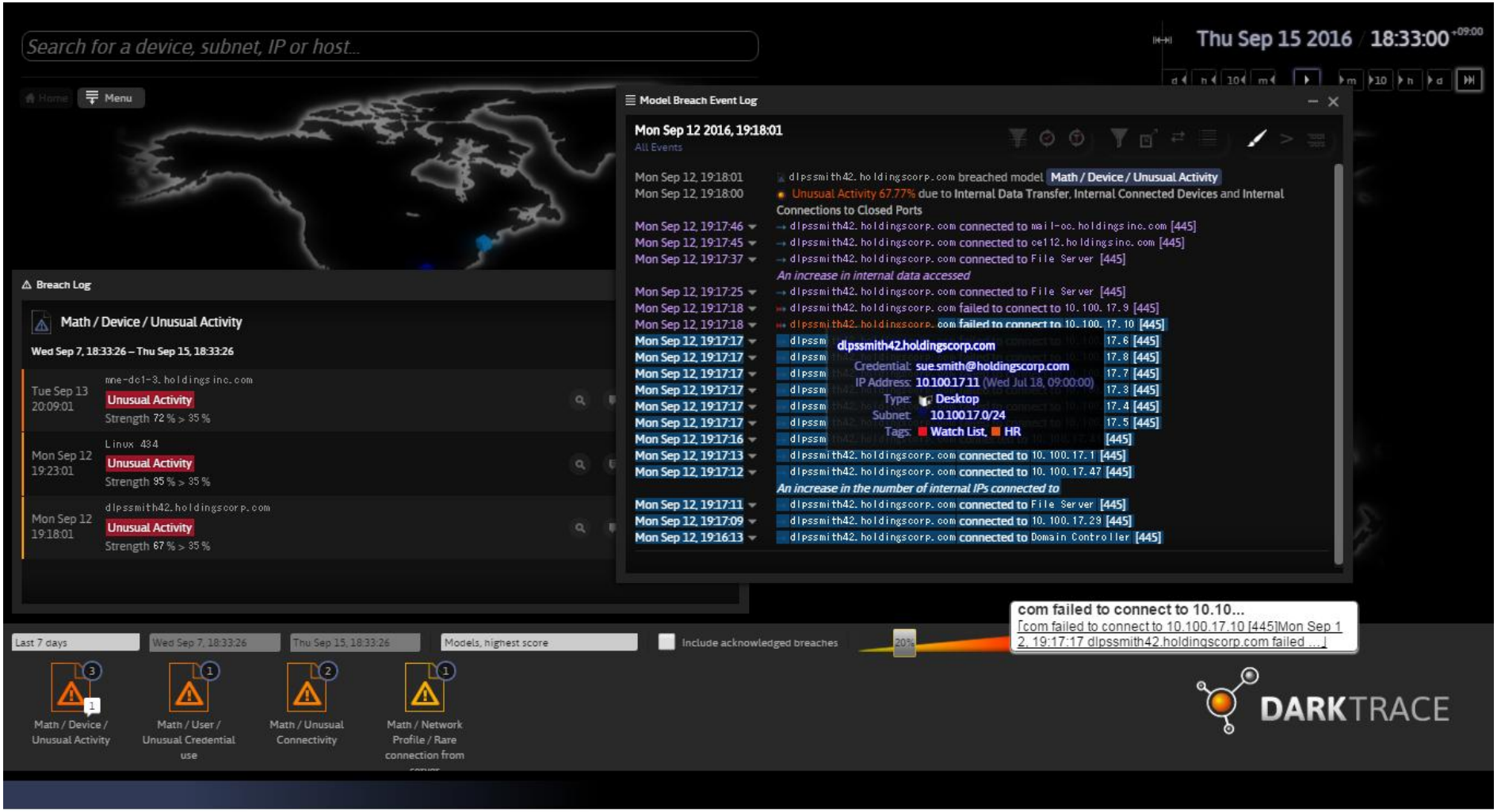
DARKTRACE



SAMURAIZ

デモ

DARKTRACE



SAMURAIZ

Enterprise Immune System の位置付け

Enterprise Immune System の効果

- 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
- 内部による脅威対策
- 内部統制の効果
- SIEMでは実現しえなかったネットワーク全体のリアルタイムな可視化

Enterprise Immune System の特徴

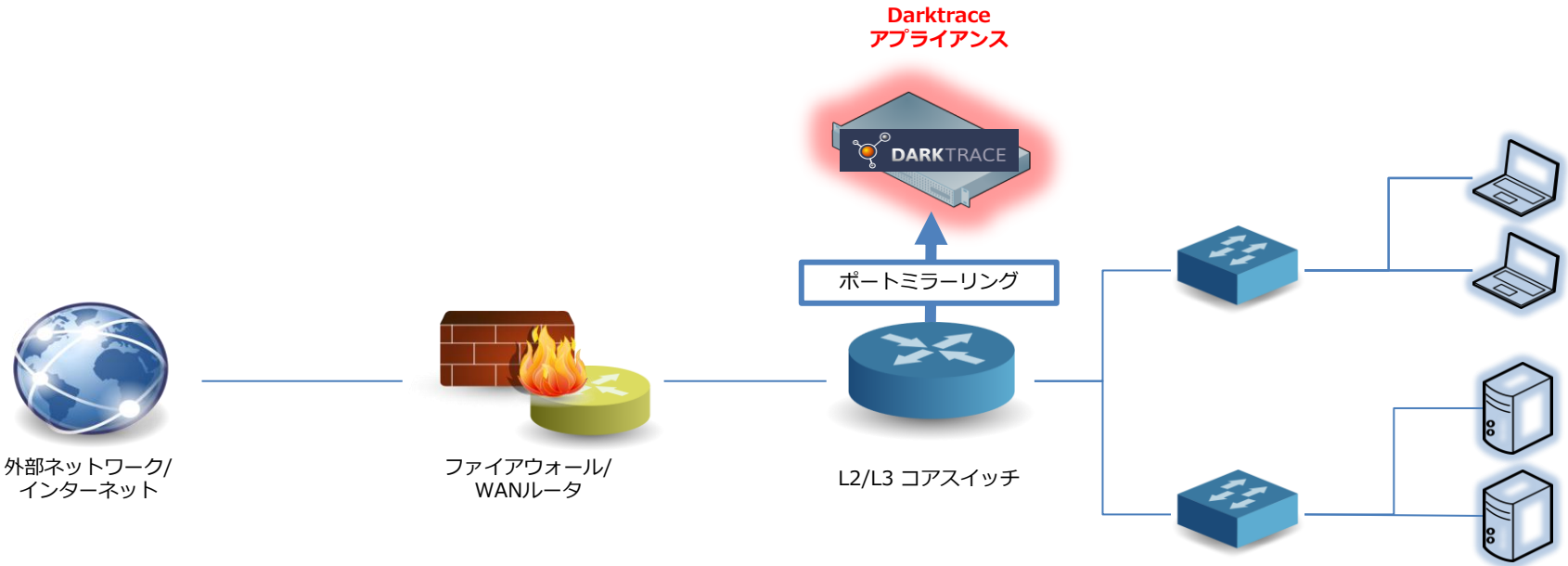
DARKTRACE

- 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
- 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
- システムの可用性に影響を与えない

SAMURAIZ

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



価格

監視対象：1,000ノード
月額：240,000円～

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

Mail：darktrace_info@samuraiz.co.jp
http://www.samuraiz.co.jp/darktrace

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

フォローアップセミナーのご案内

2016年10月18日（火）15:30より

サムライズセミナールーム（エメラルドマウンテン）
http://www.samuraiz.co.jp/event/31_161018.html

DARKTRACE

ご清聴ありがとうございました。

※アンケート回収にご協力下さい。

SAMURAIZ