\Orchestrating a brighter world NEC

機械学習と AI を駆使して未知の脅威を可視化

Enterprise Immune System 導入サービス

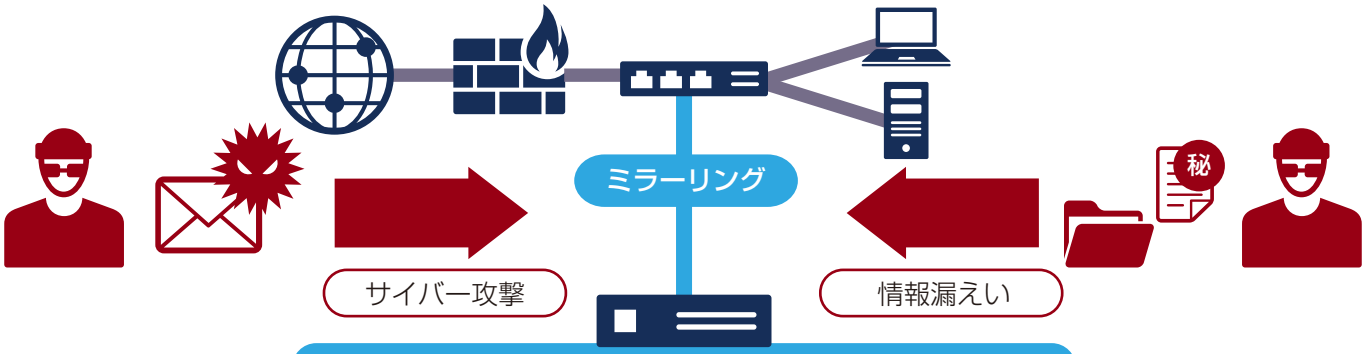
Darktrace 社の「Enterprise Immune System」は、AI を応用した機械学習のアプローチにより、従来の手法では発見出来なかった未知のセキュリティ脅威をリアルタイムに可視化します。

概要

高度化・巧妙化する外部からの攻撃と内部脅威に備える、AI を活用した可視化・検知ソリューションです。

サイバー攻撃の脅威
- AI を利用した高度な攻撃
- 1日10万件の新種マルウェア

内部犯行リスク
- 企業情報の漏えい
- なりすまし



DARKTRACE
Enterprise Immune System

- ✔ 異常な行動を自動検知
- ✔ ネットワークをリアルタイムに可視化
- ✔ 1時間でインストール可能

特長

ネットワークの生活パターンを学習

AI によりトラフィックパターンを自己学習

内部ネットワークを 100%可視化

IT ネットワーク全体を 3D ビジュアル化

内部脅威と外部からの攻撃双方を検知

従来の検知手法では発見できなかった脅威を検知

あらゆるネットワーク / デバイスを対象

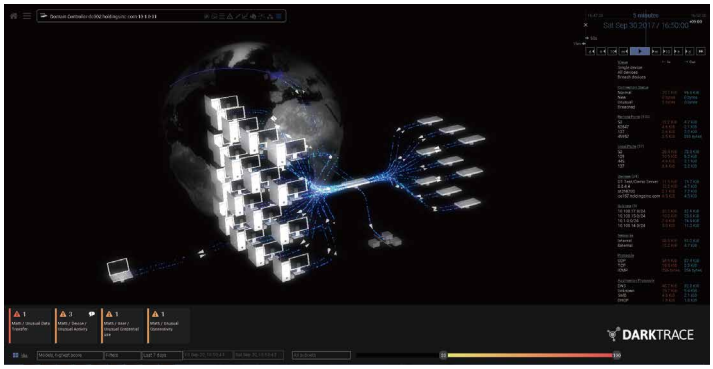
クラウドや産業用制御システム (ICS) にも対応

NECネッツエスアイ

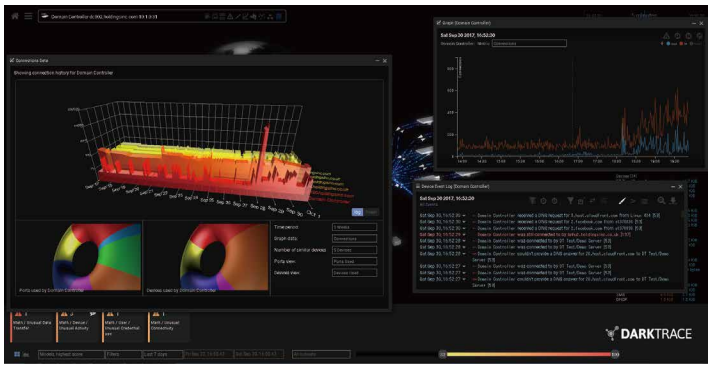
可視化機能 (Threat Visualizer)

Threat Visualizer は Enterprise Immune System の分析結果を 3D インタフェースで提供することで、ネットワークの動作を可視化しインシデント調査にご利用頂けます。

内部ネットワークの可視化



トラフィック分析



事例

1 クラウドからのデータ窃取

小売業
クラウドサービス
顧客データベースのダウンロード

・従業員が顧客のクレジットカード情報をダウンロード
・通常アクセスを行わないデバイスからの接続
・そのデバイスからファイル転送サービスへの接続

生活パターンからの逸脱を検知

2 生体認証スキャナへの侵入

製造業
指紋スキャナ
生体認証アクセスキーの改ざん

・スキャナのソフトウェア脆弱性を利用
・スキャナから送受信される情報を制御
・通常のアンチマルウェアソリューションで検出できない攻撃

全てのデバイスを可視化

3 内部関係者のデータ収集

ヘルスケア
内部関係者
ユーザー名とパスワードの収集

・２台のデバイスが異常性の高い挙動を開始
・ゲートウェイ機器のような振る舞い
・偽のログインページへのリダイレクト

内部脅威の可視化・検知

4 会議用カメラのハッキング

小売業
ビデオ会議用のカメラ
ネットワークから大量のデータ送信

・カメラ画像データを社外へ送信
・攻撃者は企業情報の入手等を意図してカメラに侵入
・アクティビティは一概に不正とはいえず見落とされる

あらゆるデバイスを対象

お問い合わせは、下記のNECネッツエスアイへ

テクニカルサービス事業本部
テクニカルサービス販売推進本部
電話　03-6699-7191　FAX　03-6699-7369

e-mail：tssol@ml.nesic.com
http://www.nesic.co.jp/

NECネッツエスアイ株式会社　〒112-8560　東京都文京区後楽2-6-1　飯田橋ファーストタワー　電話　03-6699-7000