AI機械学習で未知の脅威検知と遮断が可能なサイバー防御ソリューション

Enterprise Immune System(免疫システム)

DARKTRACE

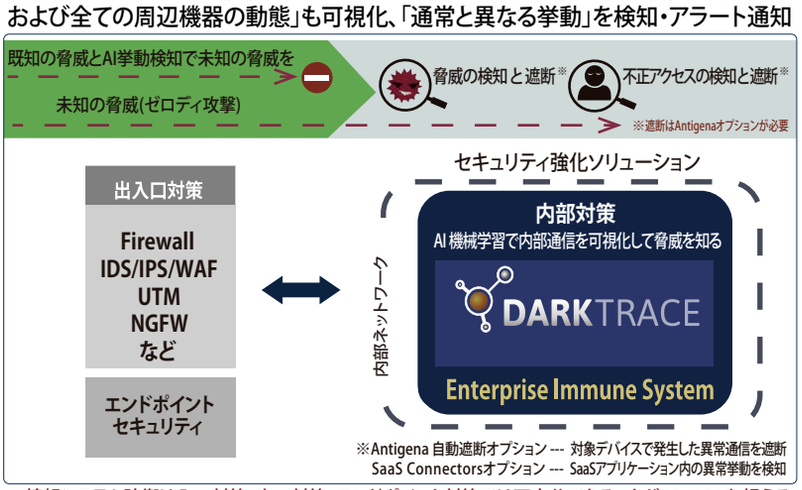
Enterprise Immune Systemは、既に導入されたセキュリティ・システムを補完・強化する新サイバー防衛ソリューション

世界有数のAI 機械学習が内部ネットワークを可視化し、侵入した脅威・内部不正などをリアルタイムに検知・防御します。
またオプション機能のAntigenaで異常通信を遮断したり、SaaS ConnectorsでSaaSアプリケーションの動態をも可視化できます。

サイバー攻撃は、現在リリースされている全ての出入口対策製品(Firewall, IPSなど)では防御できないことがこれまでの情報流出事件で明白になっています。それでも高価な出入口対策製品を導入しているので安心と誤解している方が多数います。どんなに高価な出入口対策製品であっても、既に侵入してしまったマルウェアおよび内部不正利用の検知はできません。社内ネットワーク内で何が起きているのかを知るには、内部ネットワークの可視化が必須です。

➤ 内部ネットワークの通信伝送を可視化して監視することの重要性を痛感する、というユーザが増加しています。

「既に侵入してしまった悪意のプログラムの動態」をはじめ「内部不正利用・操作ミス等および全ての周辺機器の動態」も可視化、「通常と異なる挙動」を検知・アラート通知



※ 情報システム防衛は入口対策・出口対策・エンドポイント対策では不十分であることが48，000を超える新たな脅威をDarktraceが検出したことで証明されています。

Enterprise Immune Systemの概要

- 洗練された機械学習と数学に基づく新しい高度な脅威検知
- シグネチャを必要としないアプローチで、ネットワーク境界をすり抜けたこれまでに出現したことのない新たな攻撃や標的型攻撃の検知が可能
- 内部の不正アクセスやIoT機器を含むあらゆるネットワーク機器の異常挙動も検知
- リアルタイムに機能し脅威の出現と同時に警告を出力
- 3D可視化画面で脅威を直感的に分析と調査が可能
- パケットのヘッダーを収集。通信本文(ペイロード)は収集しないので秘匿性を保持
- アプライアンスでの機能提供

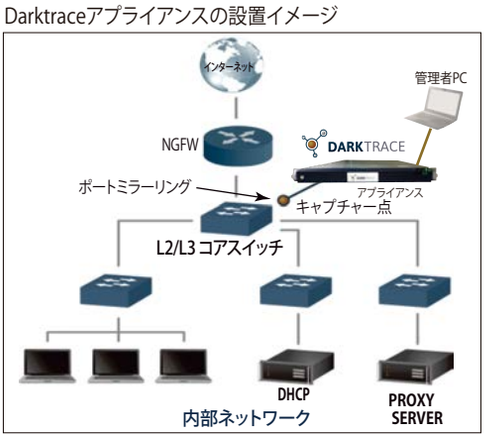
挙動の検知基準

・ネットワーク上のあらゆるデバイスの「生活パターン」をモデル化し動作のほんのわずかな変化をリアルタイムに検知します。

検知の事例

- 通常と異なる動作　- 通常と異なる接続先　- 新しい外部への接続
- 通常と異なる内部ダウンロード　- これまでに無いドメインとの通信
- 外部ストレージの使用　- 希な外部へのFTP　- ランサムウェアの感染など

Darktraceアプライアンスの設置イメージ



Darktrace Cyber Intelligence の仕様

モデル名	キャプチャースループット	最大監視IP数	キャプチャーポート
DCIP-S	300Mbps	1000	1Gbe x 3
DCIP-M	2Gbps	8000	1Gbe x 3 , SFP+ x 2
DCIP-X2	5Gbps	36000	1Gbe x 1 , 1Gbe/10Gbe x 2 , SFP+ x 2

内部ネットワークに光を灯す

Threat Visualizer

Threat Visualizerは、Enterprise Immune Systemの対話型3Dインターフェイスで、プラットフォームの基盤である高度な数学を理解する必要なく、分析担当者が直感的にネットワークの動作を可視化し異常を調査することができます。ネットワーク全体にわたるデータフローや関係性をリアルタイムまたは履歴の任意の時点でインテリジェンスに基づいた考察をユーザへ提供します。異常が発生すると、異常発生までおよび発生中のイベントを表示し、疑わしい一連のイベント発生の様子を再生することができます。

Threat Visualizer分析画面例

Darktrace Enterprise Immune System (オプション機能)

Darktrace Antigena(抗体)

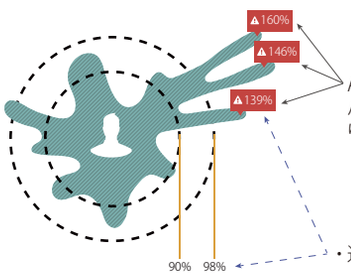
Darktrace AntigenaはEnterprise Immune Systemのアプリケーションで、過去に特定されたことのない内部脅威を含む進行中のサイバー脅威を検知した通信に対して自動的に反応してエンタープライズ免疫システムを完成させます。この技術は、デジタル抗体のように機能し、対象デバイスで発生した脅威通信に対してのみアプライアンスからRSTパケットを送信して自動遮断します。他のデバイスやネットワーク通信へは影響を与えません。RSTパケットは、管理ポートより送出されます。

異常な挙動

Darktraceは、希なソースから希なファイルをダウンロードする挙動を異常な活動として識別し通知します。その他、様々な観点から全てのデバイスの挙動を監視しています。
通常と異なる乖離を比率%で数値化する独自の脅威レベルで管理しています。

自動的に対応

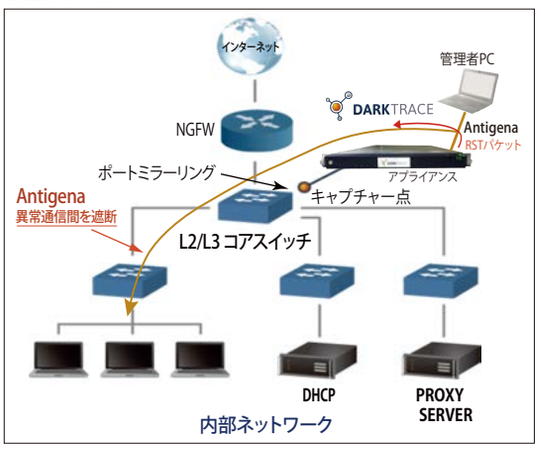
異常な活動に巻き込まれたデバイスの通信に対して自動、または状態確認後に手動で遮断の設定が可能です。遮断中に、セキュリティ・チームはその脅威に対する防御処理が行えます。



Antigenaが監視対象に指定したデバイスで通常の生活パターンと大きく外れた通信を検知すると、その脅威となり得る通信をリアルタイムで検知して自動遮断が可能です。

・通常「生活パターン」との乖離を%で脅威度を表示

設置イメージ



Darktrace SaaS Connectors

ユーザの SaaS プラットフォームへのアクセス状況を可視化

クラウドアプリケーションの利用が進む中、SaaS アプリケーション内の貴重な企業データやユーザによるクラウドとのデータのやり取りには重要な守るべき情報が含まれていますが、これに対して IT セキュリティチームはアクセス状況を把握できていません。
Darktrace SaaS Connectors を使用することで、SaaS アプリケーション内の異常な挙動をユーザのログイン場所に関わらず検知することができます。セキュリティ担当者へ新しい脅威に関する詳細情報を提供することで、SaaS 利用がどの様な状態か可視化ができます。

※ Darktrace SaaS connectors は、Salesforce.com, Box.com G Suite, Dropbox, Microsoft Office 365 を含む主要な SaaS プロバイダに対応しています。

・ユーザログイン

Darktrace の自己学習テクノロジーは SaaS アプリケーションならびにネットワーク内の各ユーザの変化する「生活パターン」を理解します。その結果、SaaS アプリケーションに対するユーザの認証情報が盗まれた場合、Darktrace はこれを異常な動作として検知し、調査対象としてフラグを立てることができます。同様に Darktrace はログインの失敗 (パスワードの推測を意味する場合が多い) も通常と異なるパターンとして認識します。

・ファイルの変更

SaaS アプリケーションのユーザがフィッシング攻撃の犠牲者となる場合があります。これらの攻撃はますます洗練されており、見分けがつきにくくなっているため、十分なトレーニングを受けた従業員も騙される可能性があります。　攻撃の結果として発生するあらゆる異常な動作、例えばファイルに対する変更やアイテムの削除なども SaaS Connectors によって検知することができます。

・データ転送およびダウンロード

退職を前にしたユーザが異常に大規模なデータのダウンロードを始めた、あるいは攻撃者またはユーザが異常な量のデータの転送を始めた、または特定のユーザが通常とは異なるタイプのデータ転送を始めた場合にも、Darktrace はこれらの動作を異常として認識して特定します。

利点

- SaaS アプリケーションに対するエンドツーエンドの可視性
- インフラストラクチャ全体に渡って異常な動作を詳細に認識できます。
- 遠隔地勤務、フレックス勤務のサポート

その他オプション機能：vSensor , OSS

vSensorとOSSは、仮想環境やクラウド環境でのユーザ間の通信なども100%可視化します。

PSI
株式会社ピーエスアイ
〒160-0022 東京都新宿区新宿5-5-3　建成新宿ビル4F
TEL: 03-3357-9980 FAX: 03-5360-4488
大阪営業所
〒532-0011 大阪府大阪市淀川区西中島3-21-13 新大阪日新ビル4F
TEL: 06-4805-9601 FAX: 06-4805-9610
http://www.psi.co.jp

問い合わせ先:

2017/09