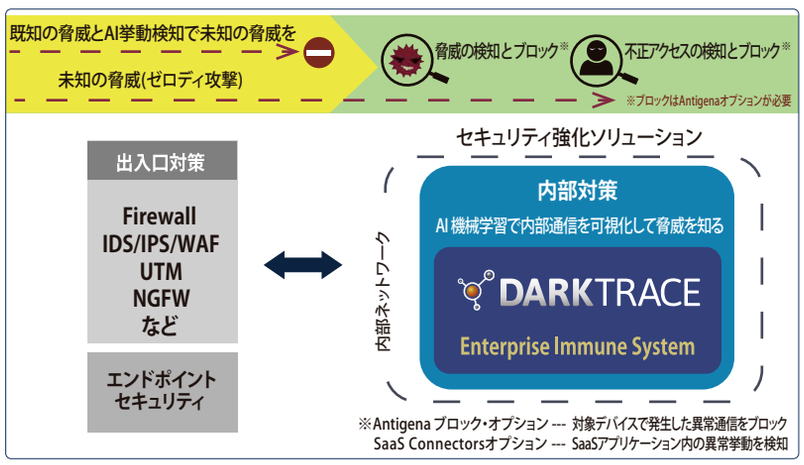
Darktrace Enterprise Immune System

機械学習AIがネットワーク通信を可視化してリアルタイムに監視

可視化ソリューションはサイバー攻撃のインシデントを未然に防ぎます。

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

「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



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

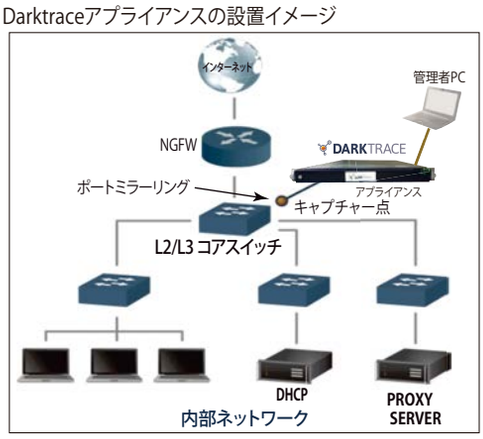
挙動の検知基準

・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



Cyber Intelligence アプライアンス

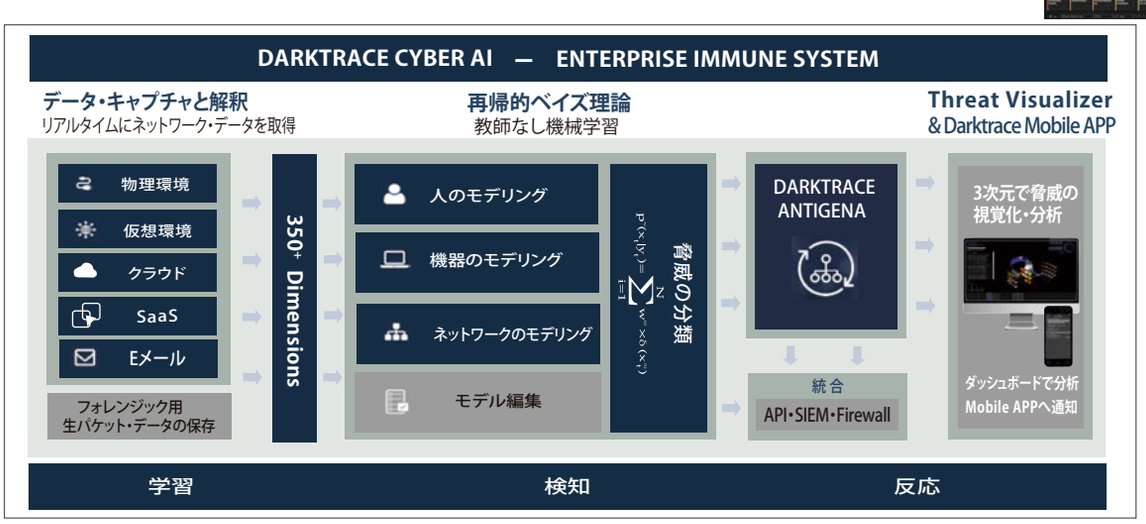
仕様

モデル名	キャプチャースループット	最大監視IP数
DCIP-S	300Mbps	1,000
DCIP-M	2Gbps	8,000
DCIP-X2	5Gbps	36,000
DCIP-Z	5Gbps	50,000

Threat Visualizer画面例

Threat Visualizer

Threat Visualizerは、Immune Systemの対話型3Dインターフェイスです。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。異常発生までの流れや発生中のイベントを表示し、疑わしい一連のイベントの様子を再生することができます。



※データ・キャプチャは、パケットのヘッダーのみで通信本文(ペイロード)は収集されず、秘匿性が保持されます。

Darktrace Cloud

Darktrace SaaS Connectors

Darktraceのサイバー AI テクノロジーはクラウド内でのリアルタイムなサイバー防御に新たな独自のアプローチをもたらします。教師なし機械学習と AI を基盤として構築された Darktrace Cloudは、クラウドワークロードおよび SaaS アプリケーション内および相互のリッチデータの流れを解析し、あらゆるユーザやデバイスおよびコンテナの通常の「生活パターン」を学習します。挙動のわずかな逸脱をリアルタイムに相関づけることにより、Darktrace Cloudは、悪意をもった内部関係者や外部からの攻撃、デジタル環境を重大な侵害の危険に晒す設定ミスに至るまで、クラウド内の幅広いサイバー脅威を特定し、阻止することできます。

Darktrace のテクノロジーの強みは自己学習アプローチにあり、事前に「良性」や「悪性」の動作を定義しておく必要がありません。Darktrace Cloud はユーザ、コンテナ、デバイスの通 常の動作をそれらの過去の挙動、所属するグループおよびより広い組織との関係でモデル化し、新しい証拠に照らして絶えず計算し直し、わずかな兆候を相関づけることにより脅威の蓋然性に対する変化する指標を確立します。

Darktrace のアプローチは、特権的アクセスを持つ内部関係者や管理者認証情報を持った外部の脅威者がアラームなくクラウドインフラ全体をスイープする可能性がある、クラウドベースのサイバー脅威の新時代において極めて重要です。クラウドプロバイダが信頼できる接続に対してクラウドを保護することは期待できず(またするべきでもありません)、その一方で異常検知機能を備えたサードパーティ製ツールも、力ずくで固定的な方法でしかそれを実現できません。固定された学習期間と事前定義された「良性」および「悪性」の考え方に依存するこれらのツールは、あからさまな脅威しか検知できません。それとは対照的に、Darktraceの教師なし機械学習とAI は人間が既に知っているまたは想像できる範囲を超え、進行中の脅威を示す可能性のあるわずかな逸脱を検知することができます。

事前定義済みのルールやポリシーに依存するのではなく、Darktrace Cloudは今日の複雑なデジタル環境に内在する不確実性に対応します。あらゆる重要な逸脱を認識および相関づけすることにより、大量の誤検知を発生させることなく純粋な脅威の検知につなげることができます。

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。

ダークトレースについて

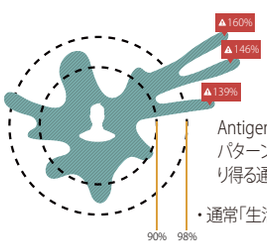
ダークトレースは、サイバーセキュリティ分野で世界をリードするAI企業です。世界各国において数千社の顧客を擁する Enterprise Immune Systemは、クラウド、SaaS、企業ネットワーク、IoT、産業用システムで機能する自己学習型プラットフォームにより、内部脅威やランサムウェアなどあらゆる種類のサイバー脅威や脆弱性をリアルタイムに検知・遮断します。従業員は800名を超え、本社は米国サンフランシスコと英国ケンブリッジにあり、東京オフィス、大阪オフィスを含めて世界に40の拠点を置いています。

Darktrace Cloud のIaaS と SaaS への適用

Darktrace Cloudは多様なデジタル環境と容易に統合することが可能で、これにはAWSやAzureのようなIaas環境、そして Saleseforce、Box、Dropbox、Office365のようなSaaSアプリケーションが含まれます。

box / salesforce / Microsoft Azure / aws / Office 365 / G Suite / Dropbox

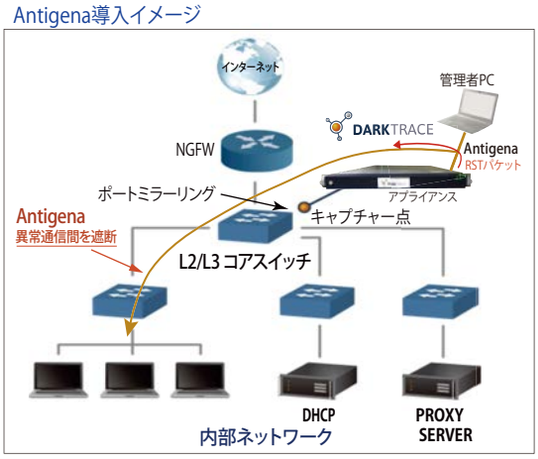
Darktrace Antigenaオプション



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

Antigena導入イメージ



PSI
株式会社ピーエスアイ　http://www.psi.co.jp
〒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
福岡営業所
〒810-0001 福岡県福岡市中央区天神1-15-5 天神明治通りビル 301
TEL: 092-600-4570

問い合わせ先:

2019/09