DARKTRACE

Darktrace 製品概要

Darktrace社が提供するEnterprise Immune Systemは、洗練された機械学習と数学に基づいて組織内のネットワーク挙動をモデル化します。そのモデルをベースとして、組織内のユーザの活動を監視し、異常な挙動を検知します。

不審なネットワーク偵察や走査、見慣れないインターネットドメインからの予期せぬダウンロード、イントラネットやファイルシステムのクローン化、新しい端末や場所からのアクセス、通常とは異なるアプリケーションやプロトコルを介した機密データへのログイン、または情報のアップロードのパターンの変化などが検出可能です。
これらの挙動が「平常パターン」から著しく逸脱している場合には、新たな調査に値するかもしれません。

Enterprise Immune Systemは、組織内のコアスイッチから、生のネットワークトラフィックを受動的にフィード取得するアプライアンスとして提供されます。アプライアンスを接続すると、社内の個別ユーザおよびネットワーク挙動のモデル作成を即座に開始します。この自己学習型数学モデルは導入初日から機能し、ネットワーク上の異常挙動検知を始めます。学習は継続的に行われ、組織の変化に応じて常に更新されます。

ネットワーク上のユーザおよび端末の「平常パターン」を作成することで、Enterprise Immune Systemはほんのわずかな挙動変化、例えばユーザによる使い方、端末のデータアクセスパターン、または通信傾向の変化などを検知可能です。これにより、ユーザの認証情報不正取得、端末のマルウェア感染、悪意を持った、または不注意なユーザの行為など、脅威となる可能性のあるイベントを発見することにつながります。

Threat Visualizer

Threat Visualizerは、Enterprise Immune Systemを補完する視覚的な対話型3Dインタフェースです。セキュリティ担当者やリスク管理者が可視化されたネットワーク挙動から直感的に異常を発見し、調査することができます。
Threat Visualizerは、異常が発生すると、発生中のイベントばかりでなく、履歴を遡り、疑わしい一連のイベントの発生の様子を再生することができます。
また、アラートに0～100までのスコアが付けられていますので、アラートのスコアを確認して、対応の優先順位を決めることも可能です。
対話型ツールであるThreat Visualizerを使って、セキュリティ分析担当者はレイヤを深く掘り下げて調査したり、複雑なクエリーを実行することができます。
また、関連する生のネットワークパケットをダウンロードして任意のツール（Wireshark等）で詳細な分析を行うことが可能です。

相補的な技術

Enterprise Immune Systemは、既存のセキュリティインフラを補完するよう設計されています。適切に設定されたネットワーク境界防御およびホスト防御対策に、シグネチャを必要としない監視および検知機能を追加することにより、日々巧妙化するサイバー攻撃や高度な標的型攻撃にも対応することが可能になります。
また、Enterprise Immune Systemからの出力は、既存の市販セキュリティダッシュボードあるいはSIEMに対して、任意の仕組み（syslog、SNMP, コネクタ、ファイル、データベース、API）を使って転送することができます。

コンプライアンスに合わせたポリシーのカスタマイズ

Enterprise Immune System は、ポリシーおよびコンプライアンスの監視および徹底のための統合モジュールも活用しています。このモジュールではお客様固有の検出条件 (例：組織指定以外のオンラインストレージ・サービスへのアクセス禁止、機密情報を帯同して特定のエリアへの移動禁止、社内DNSサービスのみ、等) に合わせた追加のコンプライアンス・ポリシーの定義をサポートします。

データの秘匿性

Enterprise Immune Systemは、すべての処理および出力をお客様のデータセンター内で行います。事前に特定の合意がない限り、データをクラウドに送信したり、Darktrace側からデータにアクセスしたりすることはありません。もちろん、お客様のデータおよびインテリジェンスの出力結果がお客様が知らないユーザコミュニティで共有されることもありません。

手間が掛からない導入およびサポート

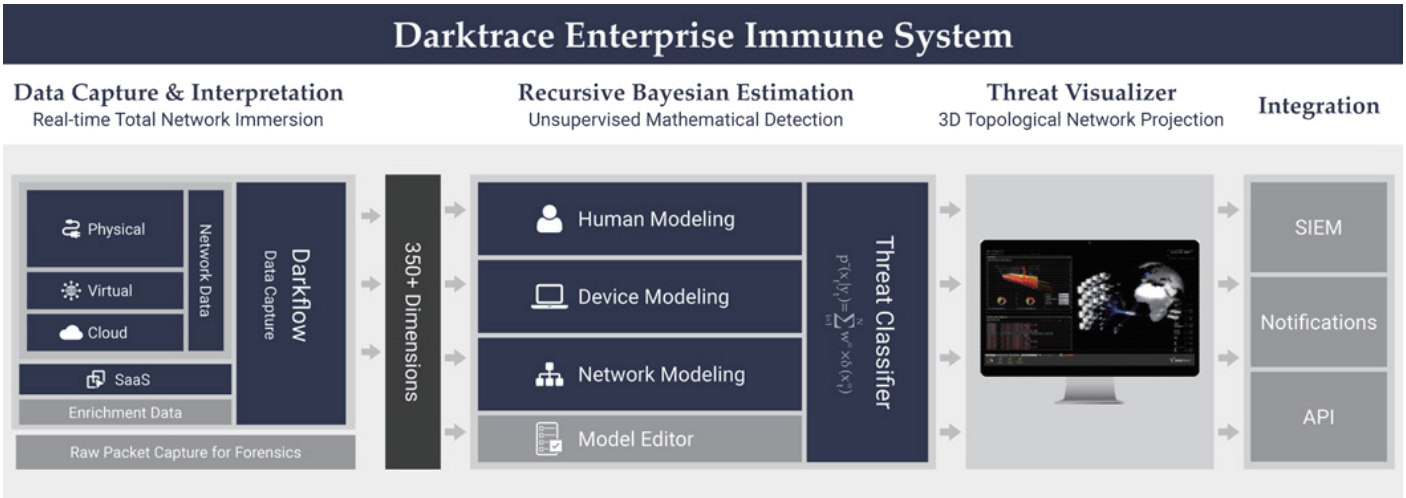
- アプライアンス1台はラックスペース2Uサイズ
- 既存のネットワーク機器に存在するポートまたはTAPにより生のネットワークトラフィックを取得
- 半日未満でインストール、設定、テスト可能
- すべてのユーザインタフェースにはWebブラウザからアクセス
- サポートはほとんど必要なし

拡張が簡単

1台のアプライアンスに複数のネットワークトラフィックを入力することが可能で、ピークトラフィック量に応じて数万台規模までの機器をカバーすることができます。
複数台のアプライアンスをクラスタ化し、地理的に分散したネットワークをカバーすることも可能です。

Darktrace 製品技術

Darktrace社のEnterprise Immune Systemは、ネットワークの健康を守るために生物学的免疫システムの原則を適用することで、革新的な自己学習型のサイバー防衛ソリューションを提供します。Darktraceの機械学習技術は、ケンブリッジ大学の数学者によって開発され、未知の脅威をルールなしで検出し、ネットワークを自動的に防御することができます。
今日の攻撃は、激しく、人間の反応が付いていけないほどのスピードで実行されることもあります。しかしながら、これらの自己学習の進歩により、機械が新たな脅威を発見し、適切なリアルタイム対応を実行し、最も深刻なサイバー脅威に対抗することが可能になりました。
Darktrace製品の中心となるのは、革新的な再帰的ベイズ推定（Recursive Bayesian Estimation）を含む様々な数学的アプローチを駆使した4つの数学エンジンです。「教師無し機械学習」で、各ユーザ、端末および組織全体の「平常パターン」モデルを生成します。その後、3つのエンジンで「平常パターン」と異なる挙動が検出されると、警告の候補が「包括的」エンジンであるThreat Classifier (脅威分類) に送信されます。Threat Classifier は、出力履歴と付合せ、誤検出をフィルタにより排除し、かすかな兆候であっても調査に値する異常を報告します。Threat Classifier が行う複数のベイズ理論アプローチを独自の組み合わせで関連付けと調整により、大規模組織での異常検出を非常に高精度に行うことができます。



再帰的ベイズ推定

再帰的ベイズ推定に基づいたアルゴリズムを利用することで、Darktraceは、ネットワークの振る舞いの様々な測定値に対する複数の分析を組み合わせ、各機器の状態を示す包括的な単一画像を生成します。そして、新しい情報がシステムで利用できるようになるにつれ、計算効率の良い方法でそれらを常に適応することができます。
従来のシグネチャベースの方法が通用しない変化する攻撃の振る舞いを特定し、新しいデータに照らして脅威レベルを継続的に再計算します。
Darktraceが提供する革新的なサイバーセキュリティ対策は、変化する機器の振る舞いとコンピュータ・ネットワーク構造を追跡するために数学的モデルを新しいネットワーク・データにリアルタイムで適用できる洗練されたソフトウェア・プラットフォームによって実現される正常な振る舞いを決定することです。
その結果が、サイバー脅威や不正アクセスを示す可能性のあるコンピュータ・ネットワークの行動履歴内の微妙な変化を識別できるシステムなのです。

脅威ランキング

Darktraceのアプローチは、データに存在する必然的な曖昧さを説明し、異なるデータに含まれる微妙なレベルの証拠を区別します。Darktraceの数学的アルゴリズムは、単純なバイナリ出力を「悪意のある」または「良性」として生成する代わりに、異なる程度の潜在的な不正アクセスを示す出力を生成します。
この出力により、システムのユーザは、様々なアラートを厳格な方法でランク付けし、最も緊急にアクションが必要なものに優先順位を付け、同時にルールベースのアプローチに関連する多数の誤検出の問題を取り除くことができます。
中核となる機能として、Darktraceは、機器のネットワークの振る舞いの多数の異なる測定値の分析に基づいて、何が「正常な」動作を構成するかを数学的に特徴付けます。

- サーバへのアクセス
- データボリューム
- イベントのタイミング
- 資格情報の使用
- DNS (Domain Name System) 要求

次に、異常な振る舞いを検出するために、ネットワークの振る舞いをあらゆる角度でリアルタイム監視します。

危険なマルウェアにリンクされたリモートアクセス攻撃

Darktraceは、RAT（リモートアクセスツール）を使用して、企業のネットワークに対する攻撃を特定しました。これは、攻撃者がインターネット上で制御する感染コンピュータで構成された有名なボットネットに関する活動の結果であると思われます。メディアは、このボットネットが東ヨーロッパのサイバー犯罪グループによって管理されていると報告しました。攻撃者はボットネットを利用して、クレジットカード情報の収集、機密データの漏洩、電子メール攻撃の実行など、様々な悪質な活動を行っています。
このウイルスの特定の亜種は、サンドボックス防御によって検知されることを避けるだけでなく、ホストベースのセキュリティツールやウイルス対策を回避するために、その運用プロセスの一部を隠すように作られていました。これは、従来のセキュリティツールで検知されないように複雑なアルゴリズムを使用する、非常に巧妙かつ動的なマルウェアです。
Darktraceは、時間の経過とともにこれらのコンピュータの挙動を比較することによって、存在の痕跡を見つけることができました。

異常なデータ転送

Darktraceは、しばしば不正使用されたAdobe Flashソフトウェアを使用して、ある組織のPCが1つのIPアドレスに異常なインターネット接続を行っていることを確認しました。
怪しいことに、DNSを介してこのIPが解決されたという証拠はなく、接続にはHTTP GET要求のコマンド名が含まれていました。
これは、組織のファイアウォールやその他の境界防御システムをすり抜けるチャネルを使用して、攻撃者が開始した秘密の通信方法だろうと推測されました。さらなる調査の結果、これはマルウェア感染であることが判明しました。

ドメイン名の生成アルゴリズム

Darktraceは、企業の数台の端末が同じような異常な振る舞いをしていることを検知しました。該当端末は、ドメイン名生成アルゴリズムを使って、ランダムに生成されたドメイン名を使用して短時間に1,000以上の接続を試みました。これは、攻撃者が多くのドメイン名でサーバを移動させるために一般的に使用される方法で、セキュリティ担当者が正確に特定することが難しく、攻撃者が検知を回避できるようにします。

匿名通信システム「Tor」の使用

Darktraceは、ある組織のマシンが「Tor」ネットワークを介してインターネットに接続していることを特定しました。「Tor」ネットワークは、接続を匿名化し暗号化します。Darktraceは、これが組織の方針への明らかな違反になるとして報告しました。

悪意のある Web ドライブバイ・ダウンロード

ある企業のユーザは、ブルース音楽についての正当なWebサイトを閲覧しながら悪意のある「ドライブバイ・ダウンロード」攻撃を受けました。そのユーザは気がついていなかったのですが、使用しているPCは、最近カリフォルニア州で登録された別のサイトにリダイレクトされました。
詳細な分析によると、疑わしく見えるドメイン名で、ドメイン名の一部に偽装された別のドメイン名が含まれていました。その後、該当PCはさらにいくつかのサイトにリダイレクトされました。
Darktraceは、これはユーザの行動ではないと判断し、マルウェアが既にそのPCにインストールされていることを示唆しました。

ランサムウェアへの感染

Darktraceは、ある組織のPCに疑わしい行動を示す複数のサインを検知しました。あるユーザが、朝の早い時間帯に、人気のあるニュースサイトを閲覧していたところ、疑わしい検索バーがユーザのブラウザに表示されました。これは恐らく、ユーザがページ上の悪意のある広告コンテンツをクリックしたためと考えられます。該当PCは、恐らくクリックによる収入を得るために、ユーザの検索結果を裏で操作するようになりました。
悪意のあるリンク先をクリックすると、ユーザはその後疑わしいWebサイトにリダイレクトされ、そこでも沢山のダウンロードが行なわれました。詳細に分析したところ、このWebサイトは、そうした活動が見られた前日に登録されていました。登録された電話番号はロシアでしたが、アドレスは米国を拠点としたものでした。この活動は、よく知られたランサムウェアへの感染のサインを示していました。それは、ユーザのファイルを暗号化し解読不能にするマルウェアの一種で、それらを解除する料金をユーザーに強要するものです。これは、会社のデータ保全および継続的な事業運営に対する明白なリスクです。Darktraceは、写真、会議の詳細、製品テスト報告を含む多数の内部ファイルを介して、マルウェアが既に展開されていたことに気づきました。

管理者資格情報の不正使用

Darktraceは、特権ユーザ認証で、異常な時間に会社のネットワークへ、繰り返しログインされていることに気づきました。この活動は、朝の早い時間帯に始まり、正午ごろ終わりました。このユーザが通常就業日のみログインしているとすれば、これは異常行動であり、会社のセキュリティへの深刻な脅威となります。なぜなら、システム管理者は、会社のネットワークやデータへの最高のアクセス権を有しており、攻撃者はこうした認証情報を悪用していたかもしれないからです。

NVC NETWORK VALUE COMPONENTS

株式会社ネットワークバリューコンポネンツ

〒144-0035 東京都大田区南蒲田2-16-2
電話: 03-5714-2050　　http://www.nvc.co.jp/