Darktrace Enterprise

脅威検知と分類

通常とは異なる動作が発生した時にそれを検知し分類する能力は、動きの速い新たなサイバー脅威の時代において極めて重要です。急激に進化する今日の脅威環境においては、攻撃による侵害が行われる前に早い段階で攻撃を検知する、根本的に新しいアプローチが求められています。

この課題に取り組むには、日々の業務の中の一見無害な活動が「異常」に変化したときにそれを理解し、味方と敵を識別しなければなりません。これには、多様かつ変化するデジタル環境全体に渡って自動的に判断を行い、セキュリティプロフェッショナルを本当に重要な業務に集中させることができるテクノロジーが必要です。

Enterprise Immune System

Darktrace EnterpriseはDarktraceの主力AIサイバー防御ソリューションです。リアルタイム脅威検知、ネットワーク可視化、高度な調査機能を、インストールが高速で簡単な統一されたシステムとして提供しています。

ケンブリッジ大学の数学者により開発された独自の機械学習およびAIアルゴリズムを使って、Darktrace Enterpriseは人目を盗むような内部関係者による脅威や、少しずつ時間をかけて行われる(low and slow)型の攻撃および自動化された脅威を含め、何が「悪意のある」活動なのかを事前に仮定することなく、あらゆる形態のサイバー脅威を検知しランク付けします。

このソリューションは企業のデジタル環境全体に渡り、生のネットワークトラフィックを受動的に解析し、何が正常で何が異常な挙動であるかについて絶え間なく確率論的判断を行います。これによりDarktraceはあらゆる機器およびユーザー、ネットワークおよびサブネットの「生活パターン」についての絶え間なく進化する理解を構築します。

Enterprise Immune Systemのコアテクノロジーに基づいてモデル化されるこれらの「生活パターン」は動的であり、ネットワークの変化に適応していきます。どのような活動が「悪意のある」ものであるか否か事前に仮定することなく、Darktrace Enterpriseは独立した学習によりビジネスの「生活パターン」からの顕著な逸脱を検知し、組織に対して脅威の危険性を即座に警告します。

確率論に基づくこのアプローチは、Darktrace Enterpriseがサイバー攻撃者または脅威の出処、攻撃手法、戦術および機能を問わないことを意味します。あらゆる重要な逸脱を認識して相関付けることにより、大量の擬陽性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。

重要な点として、Darktrace Enterpriseは自己改良性も備えており、時間の経過とともにより精度が高まります。

主要な利点

オンザジョブ学習

「正常」に対する理解を新しい証拠に照らして絶え間なく学習し適応させます。

ビジネス全体を理解

オンプレミスネットワーク、データセンター、仮想環境、クラウド、SaaS、産業用制御システムに対応します。

1時間でインストール

長期間のセットアップや人手によるチューニングは必要ありません。Darktrace Enterpriseはわずか1時間未満でインストールできます。

「Darktraceは他のセキュリティツールをすり抜けてしまう脅威を検知して対処します。」

- IDC

ネットワークの可視化

サイバーセキュリティアナリストたちは膨大なデータ量に圧倒されているだけでなく、ビジネスのデジタル化が進む中でネットワークの複雑性の高まりにも直面しています。このような環境下で高度な脅威検知および対策を行うには、相互に関係したデータを効率的かつ効果的に可視化する手段が不可欠です。

様々な攻撃タイプからネットワークを保護するには、新たな脅威を発生と同時に特定し調査を行うことができる、ネットワーク内の情報の関係と流れについての情報と、わかりやすく視覚的な説明を提供する強力なツールが必要です。

Darktrace Threat Visualizer

Darktrace Threat Visualizer

Threat Visualizer は Darktrace のグラフィカルな対話型 3D インターフェイスであり、ネットワークアクティビティをリアルタイムに可視化し異常の調査を可能にするツールです。Threat Visualizer はフォレンジックを担当するセキュリティエキスパートから、ビジネスエグゼクティブ、経験の少ない IT チームメンバーに至るまで、あらゆる知識レベルのユーザーが使えるよう設計されています。

Threat Visualizer が提供する対話型機能を使うことで、豊富な情報を様々な方法で調べて表示させることができます。このツールはサイバーセキュリティアナリストがサイバーインシデント調査に欠かせないシステムとして使用できるほか、可視化技術によりビジネスエグゼクティブに対してセキュリティ問題のハイレベルでの概要を提供するのにも使用でき、技術的スペシャリストと経営部門の溝を埋めるのに役立ちます。

> 「Darktraceは優れたユーザーインターフェイスを備えており、アナリストはネットワーク全体を視覚化することができます。」
>
> **- Gartner Peer Insights Review**

Dynamic Threat Dashboard

Dynamic Threat Dashboard は優先度の高い脅威や疑わしい活動に対する簡素化されたリアルタイムビューを提供し、対応プロセスの迅速化に貢献します。これにより、小規模なセキュリティチームでも最小限の操作できわめて迅速なトリアージを実施することが可能です。効率的なインターフェイスにより違反を素早くソート、表示、確認することができ、ここから Threat Visualizer に切り替えることで関連するネットワークアクティビティを包括的に表示させることができます。

> 「Dynamic Threat Dashboard は優先度を効果的に表示し、使い方は極めて簡単です。」
>
> **- Gartner Peer Insights Review**

Darktrace Mobile App

iOS および Android に対応した Darktrace Mobile App により、移動中でも Darktrace の警告に簡単にアクセスできます。最大限の柔軟性を提供し対応までのスピードを高めるよう設計されたこのアプリは、進行中の脅威に関するプッシュ通知、および Darktrace Antigena による自動対応アクションに対するワンクリックでの承認機能を提供しています。攻撃が発生次第、セキュリティチームは社内にいない時であっても数秒以内にリモートで確認および是正を行うことができます。

Darktrace Mobile App

> 「Darktrace Mobile App は素晴らしいアプリです。私がどこにいても、アクションを実行し、アラートを受け取り、ネットワークを監視できる柔軟性を与えてくれます。」
>
> **- ZPower**

Darktrace 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。Enterprise Immune System は、数学の専門家が開発した機械学習とAIのアルゴリズムを応用して、クラウド、仮想、IoT、産業用制御システム（ICS）を含むあらゆるデジタル環境で機能する自己学習型プラットフォームにより、事前定義を必要とせず、ゼロデイ攻撃や内部脅威、ランサムウェアなどのサイバー脅威をリアルタイムに検知・遮断します。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、世界に30以上の拠点を置いています。

お問い合わせ

シンガポール: +65 6804 5010
日本: +81 (03) 5456 5537
ヨーロッパ: +44 (0) 1223 394 100
japan@darktrace.com
darktrace.jp
@darktracejp