DATASHEET

DIANNA - Deep Instinct's Artificial Neural Network Assistant

(Deep Instinct の人工ニューラルネットワークアシスタント)

プロアクティブな **未知の** 脅威解析

比類のない **マルウェア** に関する洞察

合理化された **SOC** ワークフロー

強化された **説明可能性** とコンテキスト

マルウェア解析のための仮想 AI コンパニオン

脅威情勢が複雑になり、その拡大スピードが加速するにつれて、SOC チームは、効率的な調査能力の範囲を超えて増えつづけるセキュリティアラートの管理に苦慮しています。これがプロアクティブな脅威ハンティングを妨げ、燃え尽き症候群を悪化させています。何より重要なのは、「アラートストーム」の増加によって重要なアラートが見逃されるということです。

生成 AI による脅威解析の再定義

DIANNA は、生成 AI を活用して予防ファーストのサイバーセキュリティ機能を強化します。マルウェアアナリストとインシデント対応の専門家からなる仮想 AI チームとして機能する究極の生成 AI サイバーコンパニオンであり、Deep Instinct のディープラーニングによる予防ファーストの機能とシームレスに統合されています。

悪意のあるファイルの振る舞いを理解

DIANNA は、バイナリ、スクリプト、ショートカットファイルなどのサイバー脅威をはじめ、さまざまな形式のファイルに静的解析を行い、その振る舞いや意図を掘り下げます。これまで知られていなかったファイルの解析と振る舞いの調査に優れており、脅威の理解と実行前の修正を促進します。

説明可能性：未知の脅威解析のための生成 AI

現在のサイバーセキュリティソリューションは、ログやレピュテーションエンジンのような既存のソースからのデータを要約するために生成 AI を使用しています。しかしこれでは、限られたコンテキストを用いたレトロスペクティブ (振り返り) 解析しかできません。Deep Instinct は、生成 AI を活用して、LLM 内に効果的に組み込まれた無数のサイバーセキュリティ専門家の集合的な知識を DIANNA に与え、未知のファイルに対する詳細なマルウェア解析を行い、比類のない精度で悪意のある意図を特定します。

DIANNA のメリット

脅威配信ファイルを解析

バイナリ、スクリプト、ドキュメント、ショートカットファイルなど脅威を配信するファイルタイプを解析します。

コードを自然言語に変換

バイナリコードやスクリプトを自然言語に変換し、コードの意図、悪意のある側面、システムに影響を与える可能性について説明します。

未知の脅威を説明

DIANNA の静的解析は、未知のスクリプト、ドキュメント、生のバイナリに対する前例のない洞察を提供し、これがゼロデイ攻撃の理解に役立ちます。

可視性を強化

Deep Instinct の予防モデルの意思決定に関する洞察を提供し、SOC チームがセキュリティ体制を微調整することを可能にします。

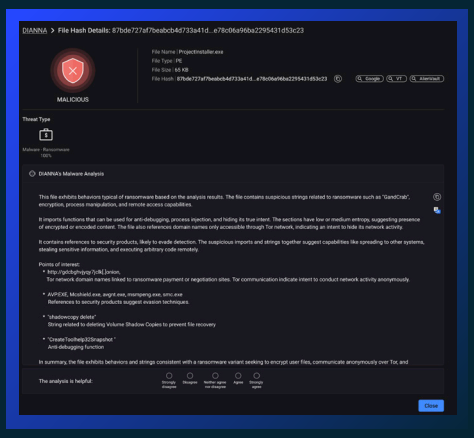
ワークフローを合理化

ティア 1 と ティア 2 のアナリストにティア 3 の専門知識を提供することで、調査を合理化し、複数のツールにわたる作業を減らして、SOC の面倒なタスクを自動化します。

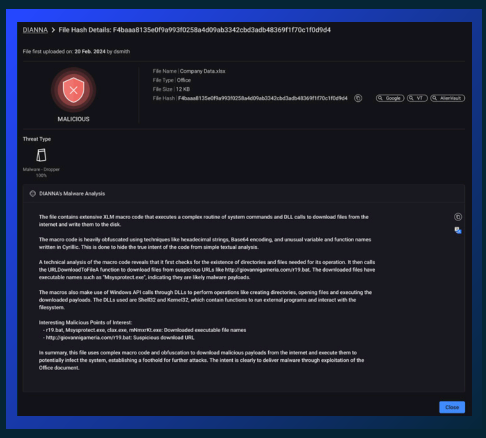
DIANNA のユースケース

DIANNA は、スクリプトからバイナリまでの未知のファイルの解析に優れており、Deep Instinct の予防ファーストのアプローチを活用しています。

スタンドアロンのマルウェア解析 - 悪意のあるファイルに対するあらゆる調査を行います。

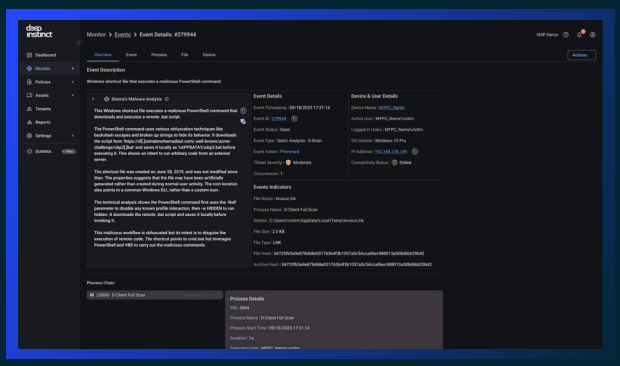


Windows 実行ファイル

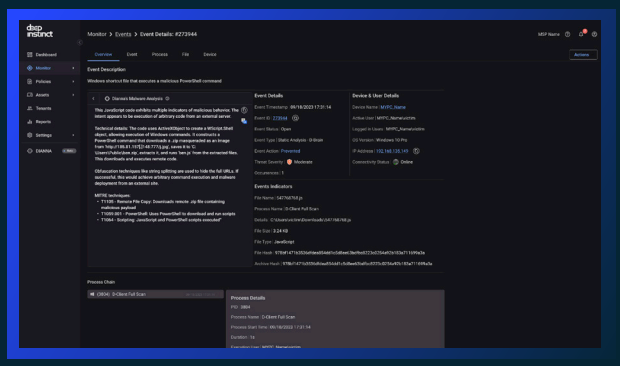


Office ファイル

インシデントのトリアージ - DIANNA が提供するファイル解析に関する充実したデータを用いて、迅速にインシデントをトリアージします。



Windows ショートカットファイル



スクリプトファイル - JavaScript

主な機能

- ファイルをアドホックにスキャンします。
- さまざまなファイルタイプの詳細なマルウェア解析レポートを数秒で提供します。
- ファイル解析プロセスを合理化します。
- Office ファイル、Windows 実行ファイル、スクリプトファイル (JavaScript および PowerShell)、Windows ショートカットファイル (.lnk) など一般的なファイルタイプをサポートします。
- 悪意のあるファイルを効率的に調査するためのコンテキスト解析、トリアージ、実用的な洞察を提供します。
- 悪意のあるファイルの振る舞いに関する明確な洞察を提供することで、SOC チームが手動でマルウェア解析を行うことなく、情報に基づいた意思決定を下せるようになります。
- サンドボックスや VirusTotal にファイルをアップロードする必要はありません。

www.deepinstinct.com/ja | info-japan@deepinstinct.com

Deep Instinct は世界初・世界唯一の特定用途向けディープラーニングサイバーセキュリティフレームワークを用いた予防ファーストアプローチで、ランサムウェアおよびその他のマルウェアを阻止しています。Deep Instinct は未知 / 既知 / ゼロデイ脅威を 20 ミリ秒未満で予測・予防します。これは最も高速なランサムウェアの暗号化速度の 750 倍高速です。Deep Instinct は 99% 超のゼロデイ脅威検知精度を誇り、誤検知率 0.1% 未満を約束します。Deep Instinct Prevention Platform はすべてのセキュリティスタックに追加される基本機能であり、脅威に対する完全な多層防御をハイブリッド環境全体にわたって提供します。