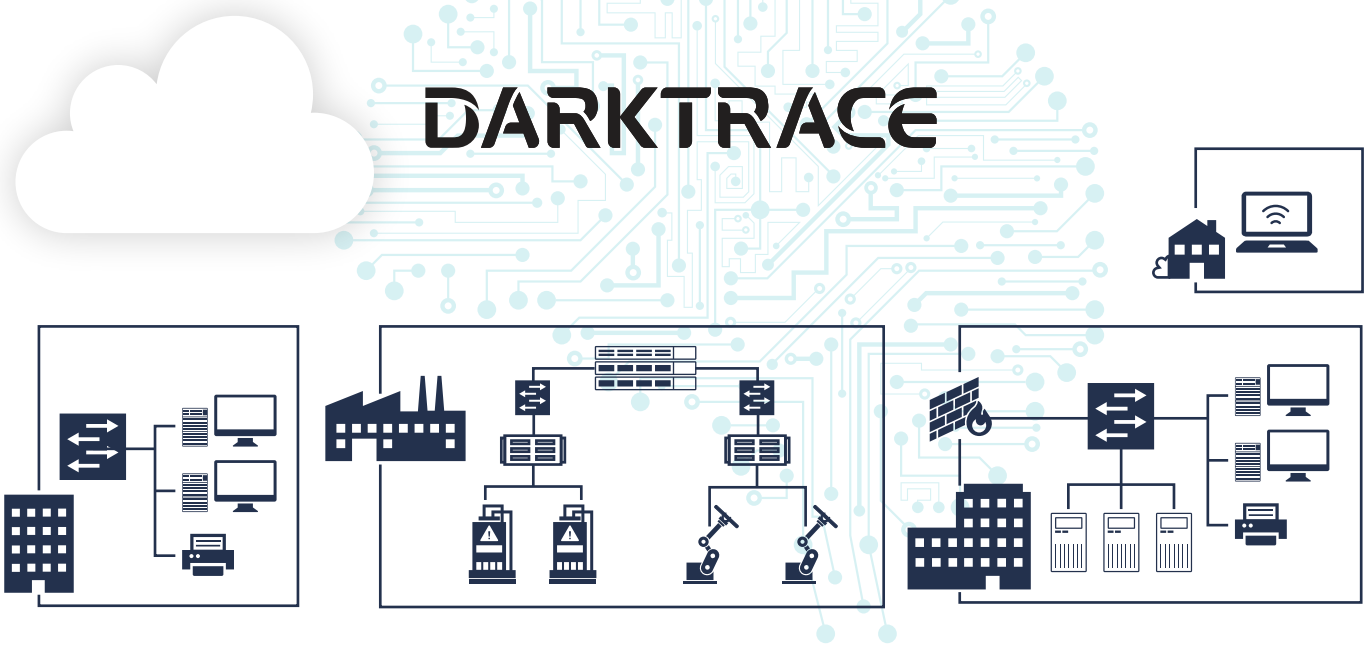
DARKTRACE

AIがネットワークを可視化
日本そして世界各国で数千社に導入される
NDRプロジェクト

Darktraceは、人間の免疫システムをセキュリティに応用し、
進化しつづける未知の脅威に対しルールやシグネチャに依存しない、
AIの自己学習によるアプローチでネットワーク上の脅威を検知します。
内部犯行をネットワーク内部ですばやく検知する
NDR（Network Detection and Response）という製品群に分類され、
他セキュリティ製品と連携し運用を補完することもできます。



あらゆる環境の監視

オフィス内の環境だけでなくクラウド、テレワーク、工場といった様々な環境の通信を AI が解析し、脅威を発見します。

日本語で脅威を確認

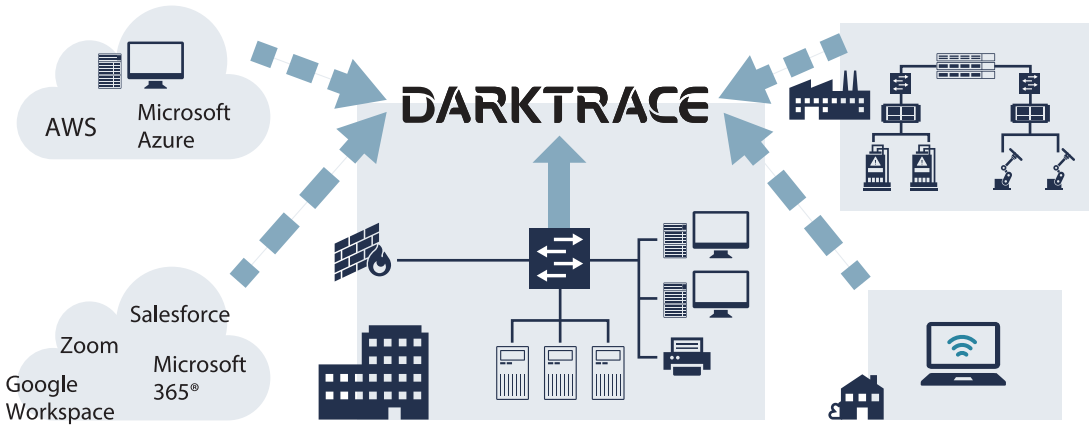
運用上のメイン画面“Cyber AI Analyst” 機能は、日本語で表示可能です。AI により発見された脅威が日本語でわかりやすく解説されます。

発見した脅威の軽減

ランサムウェアによるファイルサーバーへの侵害など、発見された脅威に関連する危険な通信を遮断することが可能です。

構築と監視範囲

Darktrace の基本的な構築方法は、主要なネットワークスイッチの通信パケットを、SPAN/TAP にてアプライアンスに流し込む（ケーブル接続）だけです。取り込んだ通信パケットから、AI が自動的にネットワークの構造を学習し監視を開始します。また、SaaS 等クラウドサービスのログ取込みや、子機アプライアンスならびにクライアントソフトウェアを利用することで、組織内の様々な環境の監視が可能となります。



日本語による脅威の解説とレポート

“Cyber AI Analyst” は、ダークトレース社サイバーアナリストが、顧客環境を調査分析する際 の数百万におよぶ思考パターンを AI に学習させることで開発された機能です。一見すると異質に見える事象の関連性を AI が自動的に調査、紐付け、画面上で可視化することで、セキュリティチームのインシデント対応時間の短縮に寄与します。

危険な通信の遮断

検知された脅威の対象通信を自動もしくは手動にて遮断することが可能です。ファイアウォールやクライアントの切り離しといった対処に比べ、正常な通信を止めることなく、脅威と判断された通信のみに絞った遮断が可能なため、ビジネスのスピードを緩めることなく脅威への対処が可能となります。

安心の運用サポートメニュー

▶ Security Operations Support

ダークトレース社サイバーアナリストとの Darktrace 管理画面上のチャットによるアドバイスサービスです。(24 時間 ×365 日対応)

▶ Managed Threat Detection

ダークトレース社によるプロアクティブな脅威通知サービスです。(24 時間 ×365 日対応)

▶ Darktrace アラート分析・監視サービス

日本のベンダーによる SOC サービスです。24 時間 365 日対応での検知解析に加え、月次のレポート提示など日本のお客様のニーズに合わせた運用サービスです。
任意のタイミングで利用可能なチケットタイプのメニューもラインアップ。

Darktrace 無償体験プログラム

Darktrace はお客様環境に製品を実際に設置し、無償で評価できる PoV（Proof of Value：価値証明）を実施します。
管理コンソールである Threat Visualizer の利用だけでなく、PoV 期間中、ダークトレース社サイバーアナリストから、検出内容についてのレポート（Threat Intelligence Report ）を提供、解説します。

Week 1	Week 2	Week 3	Week 4
初期学習	レポート①	レポート②	レポート③

J's Communication ジェイズ・コミュニケーション株式会社

Mail お問合せ先：darktrace_pr@jscom.co.jp

東京本社　東京都中央区新川1-16-3 住友不動産茅場町ビル
tel:03-6222-5858　fax:03-6222-5855
大阪本社　大阪府大阪市淀川区西中島5-5-15 新大阪セントラルタワー南館
tel:06-6309-7600　fax:06-6309-7677
中部営業所　愛知県名古屋市西区名駅1-1-17　名駅ダイヤメイテツビル
tel:050-5491-5769
九州営業所　福岡県福岡市博多区店屋町6-25　オクターブ店屋町ビル
tel:092-263-6700　fax:092-263-6710

202411