DARKTRACE

Darktrace / NETWORK

自己学習型AIによる業界で最も高度なNDRソリューション

ネットワーク複雑性の拡大

現代のネットワークはオンプレミスをはるかに超えて、仮想環境、クラウドおよびハイブリッドネットワークへと拡大しています。2029年までにインシデントの50%以上がクラウドネットワークアクティビティ由来となる[1]ということは、デジタルエステート内の南北、東西のトラフィックを含めさまざまなエリアを通る複雑な攻撃に対して、同じ土俵で対抗できるソリューションが必要となるということを意味します。

従業員の63%がハイブリッドベースでリモート勤務[2]する状況において、リモート勤務者のデバイスに対するネットワーク可視性を維持することはますます重要になりつつありますが、これは他のNDRやEDRツールではカバーされていません。

古いツールは新しい脅威に対して盲目

ほとんどのNDRベンダー、そしてIDS/IPS等のネットワークセキュリティツールは過去のデータと教師あり機械学習を使って既知の攻撃を検知する手法に頼っており、組織はゼロデイのような新手の攻撃、既知の攻撃のバリアント、サプライチェーン攻撃や内部関係者による脅威等に対して脆弱なままとなります。

こうした従来のアプローチでは、少なくとも1つの組織が、「患者第一号」、つまり新手の攻撃の最初の被害者となってからでないと、他のところでは検知できないことを意味します。また、他のNDRベンダーは全体でトレーニングされたモデルを適用しており、各組織の環境に固有のモデルではないため、ビジネスのコンテキストを欠いた大量の偽陽性やアラートが発生します。

1 Gartner Market Guide for Network Detection and Response, 2024.

2 McKinsey Global Institute, 2023

SOCチームにかかるプレッシャー

SOCアナリストの70%以上が極度の疲労を経験していると報告しており[3]、結果に妥協することなくセキュリティチームにかかるプレッシャーを下げるためには、組織はネットワーク脅威と戦う新しいアプローチを活用する必要があります。

組織の57%が、自社のSOCの集約および相関能力を強化する必要があると報告しており[4]、SOCチームは調査AI等の代替ソリューションを導入することでアナリストの負担を軽減し、アラート疲れを和らげ、ネットワークセキュリティ業務をよりプロアクティブな状態に変革することを検討する必要があります。

ビジネス上の利点

- **既知および新手の脅威からビジネスを保護**
  過去の攻撃データ、脅威インテリジェンスあるいはクラウド接続に頼ることなくリアルタイムに保護します。
- **完全なネットワーク可視性**
  オンプレミス、仮想環境、クラウド、ハイブリッドネットワーク全体を、リモートデバイスを含めて可視化します。
- **AIでセキュリティチームを補強**
  セキュリティインシデントの調査とトリアージをマシンスピードで自動化し、時間とリソースを大幅に節約します。
- **ビジネスの中断を回避**
  ビジネスのコンテキストを理解し、精密なアクションを実行してリアルタイムに脅威を封じ込める自律遮断ソリューションにより、ビジネスに影響を与えません。
- **組織全体の情報を統合**
  ネットワーク、クラウド、アイデンティティ、OTデバイス、Eメール、エンドポイント、サードパーティアラートよび脅威インテリジェンスからのデータを統一されたソリューションでコンテキスト化します。

3 Tines - Voice of the SOC Analyst, 2022

4 Gartner Peer Community One-Minute Insights - Modern Security Operations Center (SOC) Strategies, 2023

Darktrace
/ NETWORK

自己学習型AIによる業界最先端のNDR

検知

組織にとって何が正常な状態であるかを理解する自己学習型AIにより、ネットワーク全体で既知および新手の脅威を検知します。オンプレミス、クラウド、ハイブリッドおよび仮想環境に対し、リモート勤務者のエンドポイントも含めて完全な可視性と脅威検知能力を得ることができます。

調査

Cyber AI Analystを活用してネットワーク内のすべての重要なアラートを継続的に調査しコンテキストを理解することができます。Cyber AI Analystは人間のアナリストが行うように自律的に仮説を立て、結論を導き出すことができ、SecOpsを変革し他のNDRプロバイダーの能力をはるかに超えた運用が可能です。

遮断

ダークトレースの自己学習型AIは既知の脅威と新手の脅威のどちらに対してもリアルタイムかつ自律的に遮断し、組織についての文脈的理解および動作の理解に基づいて精密なアクションを実行し、業務に影響を与えることなく脅威を封じ込めることができます。

Darktrace / NETWORK の主な機能

ネットワーク全体に渡って既知と未知の脅威を検知

完全なネットワークカバレッジを実現し精密な脅威検知によってブラインドスポットを明らかにします。

概要：

- ネットワークに対する完全な可視性
- 異常なアクティビティをリアルタイムに発見
- 既知および新手の脅威を検知
- ローカルに展開される自己学習型AI
- 暗号化および復号化トラフィックを分析

完全なネットワーク可視性

Darktrace / NETWORKはオンプレミス、仮想、クラウドおよびハイブリッド環境およびリモートデバイスからのネットワークトラフィックを受動的に取り込み、データポイントを抽出してあらゆる接続の暗号化および復号化パケットを分析し、通常とは異なるアクティビティをリアルタイムに見つけ出します。

データをクラウド上で処理する、あるいはグローバルにトレーニングされるモデルの一部として処理する他のNDRベンダーとは異なり、業界をリードするDarktraceの自己学習型AIはローカルに展開され、クラウド接続の必要なく個々の組織のデータのみでトレーニングされます。これによりプライバシーに妥協することなく組織専用のセキュリティが実現されます。

既知と未知の脅威を検知

Darktrace / NETWORKは他のNDRベンダーとは根本的に異なるアプローチにより、既知のマルウェアシグネチャや外部インテリジェンス、過去の攻撃データに頼ることなく脅威を検知します。 ダークトレースの自己学習型AIは組織のネットワークにとって何が正常な状態であるかを理解し、異常なアクティビティや既知および新手の脅威を検知します。

ネットワーク内のあらゆる接続が継続に分析、マッピング、モデル化され、組織のデバイス、アイデンティティ、接続および潜在的な攻撃経路の全体像を作り出します。 ダークトレースの自己学習型AIはビジネスの中断を引き起こす可能性のあるあらゆるネットワーク動作を識別し、IDS/IPSのようなパケットサンプリングツールと比較して前例のないビジネス全体の文脈を提供することにより、ゼロデイからサプライチェーン攻撃、内部関係者による脅威に至るまで、外部と内部両方の脅威を照らし出します。

正確な脅威検知

ダークトレースの自己学習型AIは自身を自律的に最適化してノイズを排除し、純粋な、優先付けされたネットワークセキュリティインシデントを素早く提示します。これにより偽陽性を大幅に削減し、人手により絶え間なくアラートを調整する面倒を解消できます。

希望する場合には、ユーザーが運用を完全にコントロールし、直感的なモデルエディターを使ってAIの出力結果がどのように処理されるかを管理することも可能です。 熟練したユーザーはあらゆる設定を直接変更または無効にすることができ、開発のコストをかけずにカスタムの検知を容易に作成することができます。

Darktraceは本物のAIです。本当に自己をトレーニングし、私は一切モデルに手を加える必要がありません。このシステムは驚くほど正確です。

■ ジョセフ・ブッティンガー
コーポレートIT & セキュリティマネージャー // EV Group

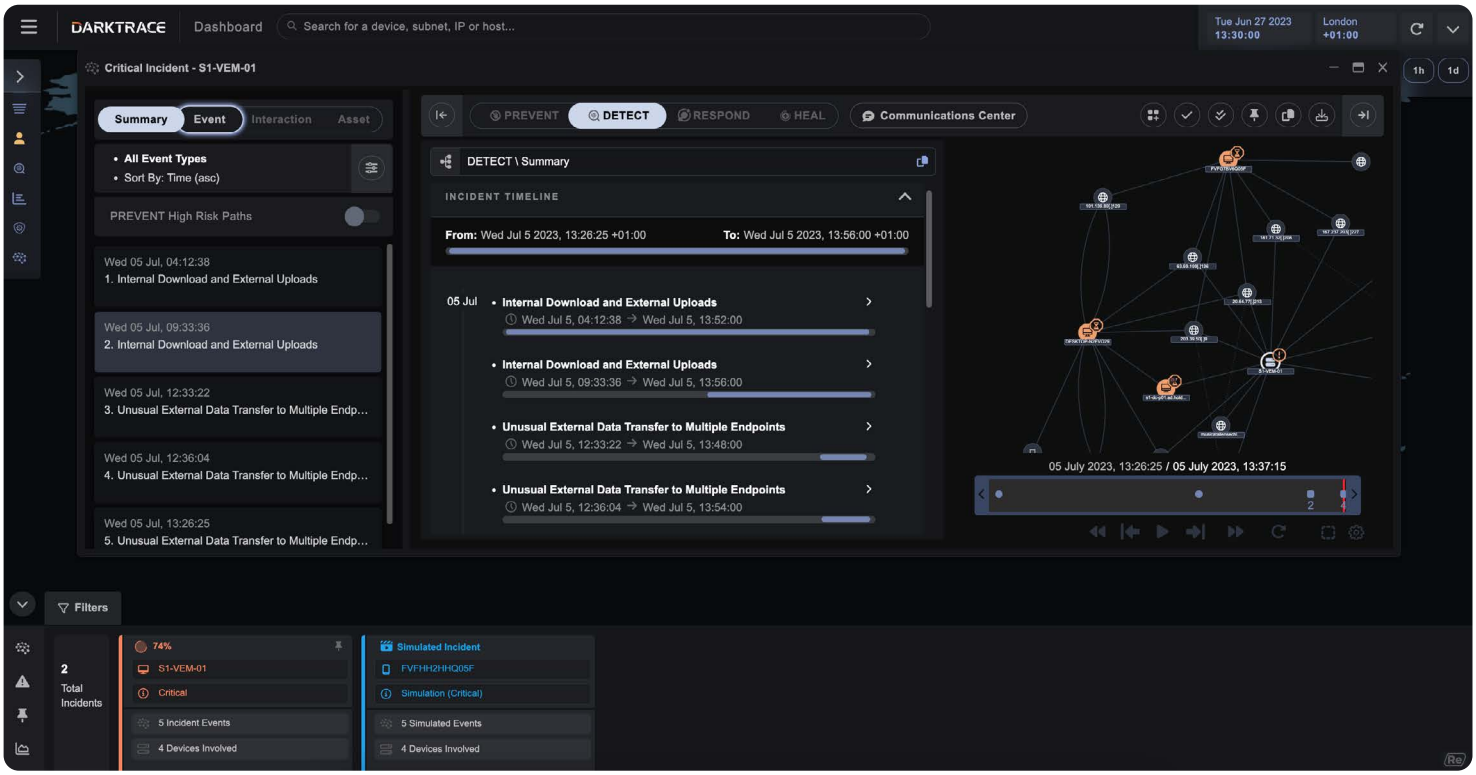


図 01: Darktrace / NETWORKは組織のネットワーク全体にとって何が正常な動作であるかを学習し、異常なアクティビティを検知して、ビジネスの中断を引き起こしかねないあらゆる問題についてそれらの優先度を判断します。

検知モデルの例

Darktrace / NETWORKはMITRE ATT&CKの14のカテゴリーすべてに対するカバレッジを提供し、過去のデータや静的なルール、あるいはシグネチャベースの手法に頼ることなく攻撃ライフサイクルのあらゆる段階で脅威を検知します。以下はネットワーク内の異常な動作や脅威を検知するのにDarktrace / NETWORKが使用することのできる検知モデルの一部の例です：

内部偵察

- Device / Suspicious SMB Scanning Activity
- Device / Network Scan
- Device / RDP Scan
- Device / ICMP Address Scan
- Device / Suspicious Network Scan Activity other NDR providers.

ラテラルムーブメント

- Device / Multiple Lateral Movement Model Breaches
- Anomalous Connection / Unusual Admin RDP Session
- Device / SMB Lateral Movement
- Compliance / SMB Drive Write

C2通信

- Anomalous Server Activity / Outgoing from Server
- Anomalous Connection / Multiple Connections to New External TCP Port
- Anomalous Connection / Rare External SSL Self-Signed
- Device / Suspicious Domain

漏えい

- Unusual Activity / Enhanced Unusual External Data Transfer
- Anomalous Connection / Data Sent to Rare Domain
- Unusual Activity / Unusual External Data Transfer
- Compliance / FTP / Unusual Outbound FTP

業界初のAI Analyst で環境内のアラートを調査

Darktrace / NETWORKはCyber AI Analystの力を活用して組織のデータにコグニティブオートメーションを適用し、トリアージの時間を劇的に短縮します。

概要：

SOCチームの能力を補強

単にインシデントのサマリーを作成するためのプロンプトベースのLLMや、ベーシックなAI調査機能を提供する他のベンダーとは異なり、Cyber AI Analystは経験豊富な人間のアナリストのように実際に機能することができる市場で唯一のテクノロジーです。セキュリティインシデントの調査をマシンスピードで自動化し、トリアージにかかる時間を劇的に短縮してSOCチームを支援します。

Cyber AI Analystは組織にとって何が正常な動作であるかについての理解に基づき、ネットワーク内のあらゆるアラートを継続的に分析しコンテキストにあてはめます。人間のアナリストが行うように自律的に仮説を立てて結論を導き出すことが可能で、SOCチームは時間とリソースを大幅に節約することができます。

詳細な調査により高度な脅威を解明

Cyber AI Analystはネットワーク内のあらゆるアラートをインテリジェントに調査し、良性と見えるようなイベントを結び付けて高度な脅威を解明し、さまざまなアクティビティを相関づけて1つのインシデントを明らかにします。無害と見えるようなネットワークの異常をつなぎ合わせることにより、Cyber AI Analystは悪意あるアクションのかすかな兆候も自律的に識別し、高度なネットワーク脅威を見つけ出してキルチェーン全体をリアルタイムかつ大規模に追跡します。

ネットワーク調査に対するこの包括的アプローチにより、Darktrace / NETWORKはゼロデイ攻撃や内部関係者による脅威その他多くの問題をすばやく見つけ出し、組織が「患者第一号」になることを防止するとともに、「既知の悪性」動作にのみ注目した従来型のNDRソリューションよりも格段に優れた結果を提供します。

ビジネス全体のコンテキストを理解

組織の環境内のあらゆる部分から発生した重要なアラートのコンテキストを理解することができあす。Darktrace Cyber AI Analystは、組織のネットワーク、エンドポイント、クラウド、アイデンティティ、OTデバイス、Eメールおよびリモートデバイス全体に渡って接続とイベントを追跡し、デジタルエステート全体を移動する最新の脅威の検知と調査に役立ちます。

Darktrace / NETWORK および Darktrace / CLOUD に既存のEDRを追加することで、元のEDRに限定されネイティブな機能に欠けるXDRベンダーと比較して、きわめて効果的なXDRソリューションの基礎を構築することができます。セキュリティチームはActiveAI Security Platformを利用してプロアクティブな能力と修復機能を追加することができ、接続された1つのソリューション内でEメール、アイデンティティ、およびOTをカバーすることができます。

自己学習型AIはエンドポイント上の動作を、Microsoft 365および当社のクラウド環境全体の動作と併せて調査してくれます。

■ テリー・ライト
ITインフラ責任者、Scope Markets社

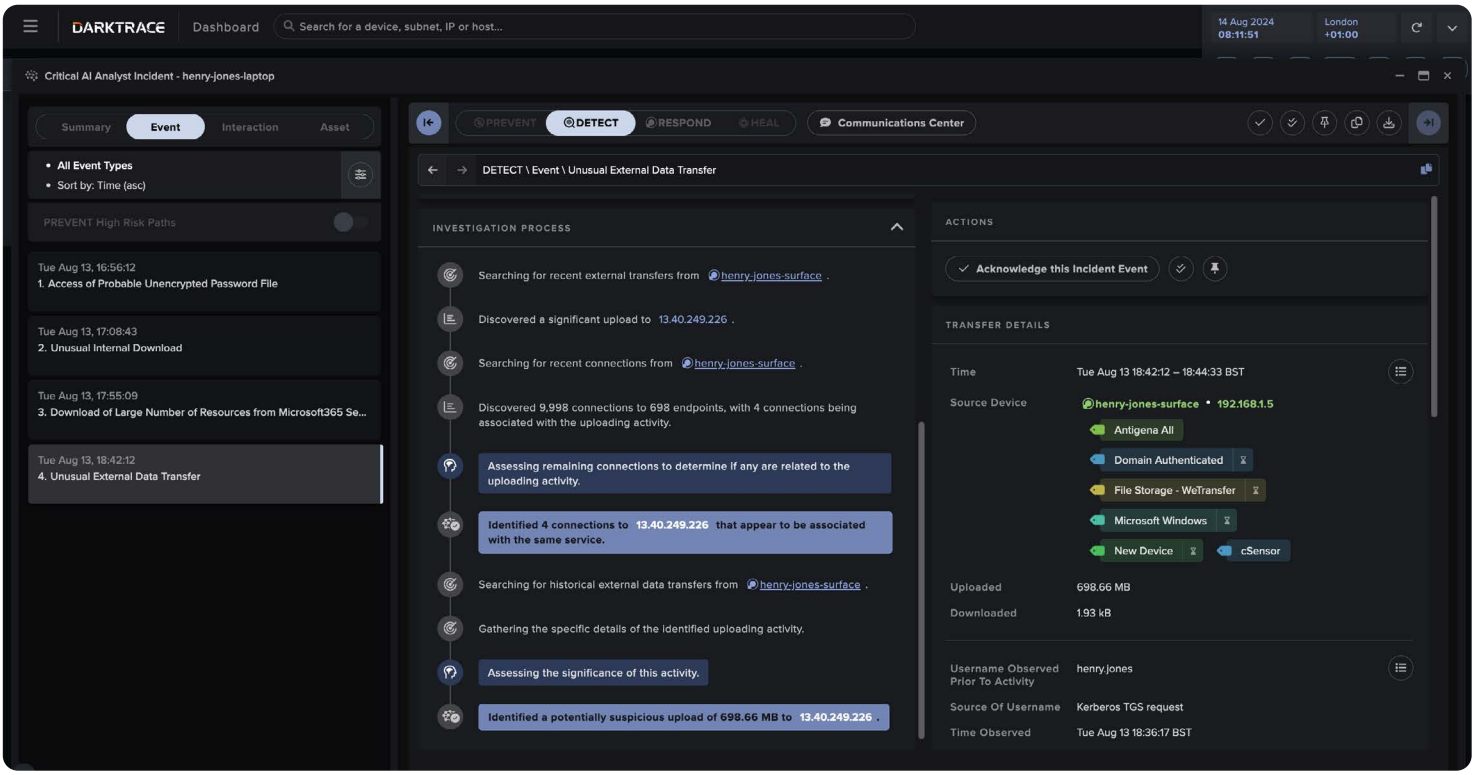


図 02: Cyber AI Analystは組織にとって何が正常な動作であるかについての理解に基づき、ネットワーク内のあらゆる重要なアラートを継続的に分析しコンテキストにあてはめます。インシデントの詳細なタイムラインと完全なサマリーが提供され、チームは意味付けまでの時間を短縮することができます。

エンタープライズでの実効性が実証された業界初の自律遮断ソリューションでネットワーク脅威を無害化

ビジネスオペレーションを中断することなくリアルタイムかつ自律的に封じ込めおよび対処

概要：

自律遮断

生活パターンと動作のコンテキスト

的を絞ったアクションにより中断を回避

ネイティブおよびサードパーティの対処アクション

完全にカスタマイズ可能

自律的脅威遮断

Darktrace / NETWORK は過去の攻撃データに頼ることなく、環境の全体的コンテキストと、デバイスまたはユーザーにとって何が正常であるかについての詳細な理解に基づいて、脅威をすばやく封じ込め無力化します。Darktrace / NETWORK は単独のデバイス、またはそのピアグループにとって何が正常であるかに基づいて、生活パターンを自律的に強制することのできる唯一のNDRソリューションです。

Darktrace / NETWORK は精密な対処アクションをリアルタイムかつ自律的に実行することにより、ビジネスオペレーションを中断することなく、ネイティブに、またはサードパーティツールとのインテグレーションを通じて脅威を封じ込めます。 また、Darktrace / ENDPOINT と組み合わせることにより、リモートユーザーデバイスに対して、エンドポイントの場所に関わらず、またコーポレートネットワーク外にある場合にもアクションを実行することができます。

完全なコントロールを維持

Darktrace / NETWORK はネットワーク上の脅威に対して最も効果的なアクションを自律的に実行し、メンテナンスはほとんど必要なく、初期セットアップの作業も最小限です。

ほとんどの顧客はデフォルトの遮断アクションを使用していますが、希望する場合には対処ロジックをカスタマイズする、または独自のロジックを作成することもできます。デバイスタイプ、IP範囲、業務時間、およびその他のさまざまなパラメータに基づいて、精密な調整を行うことが可能です。

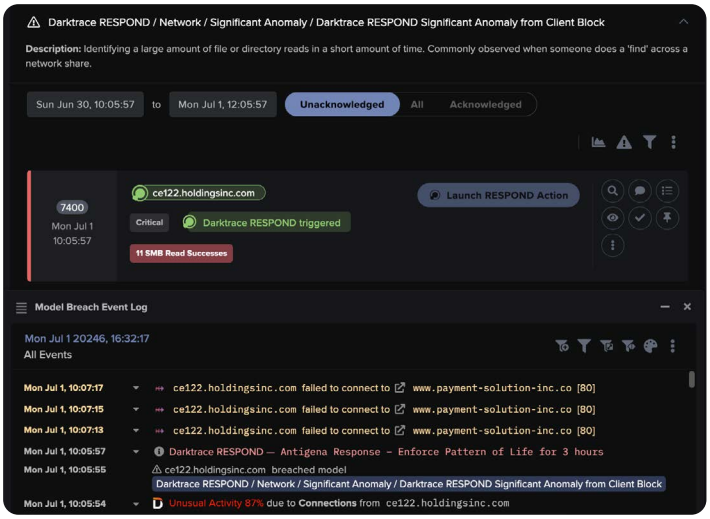


図 03: 各イベントとインシデントのつながり、またAIがどのように自律的に対処してビジネスを保護したかを完全に可視化

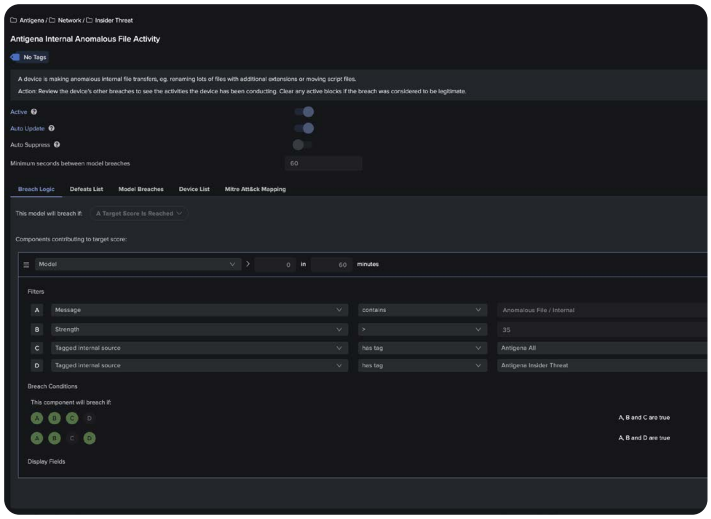


図 04: 必要な場合にはDarktrace Model Editorを使って対処ロジックを細かく調整することが可能

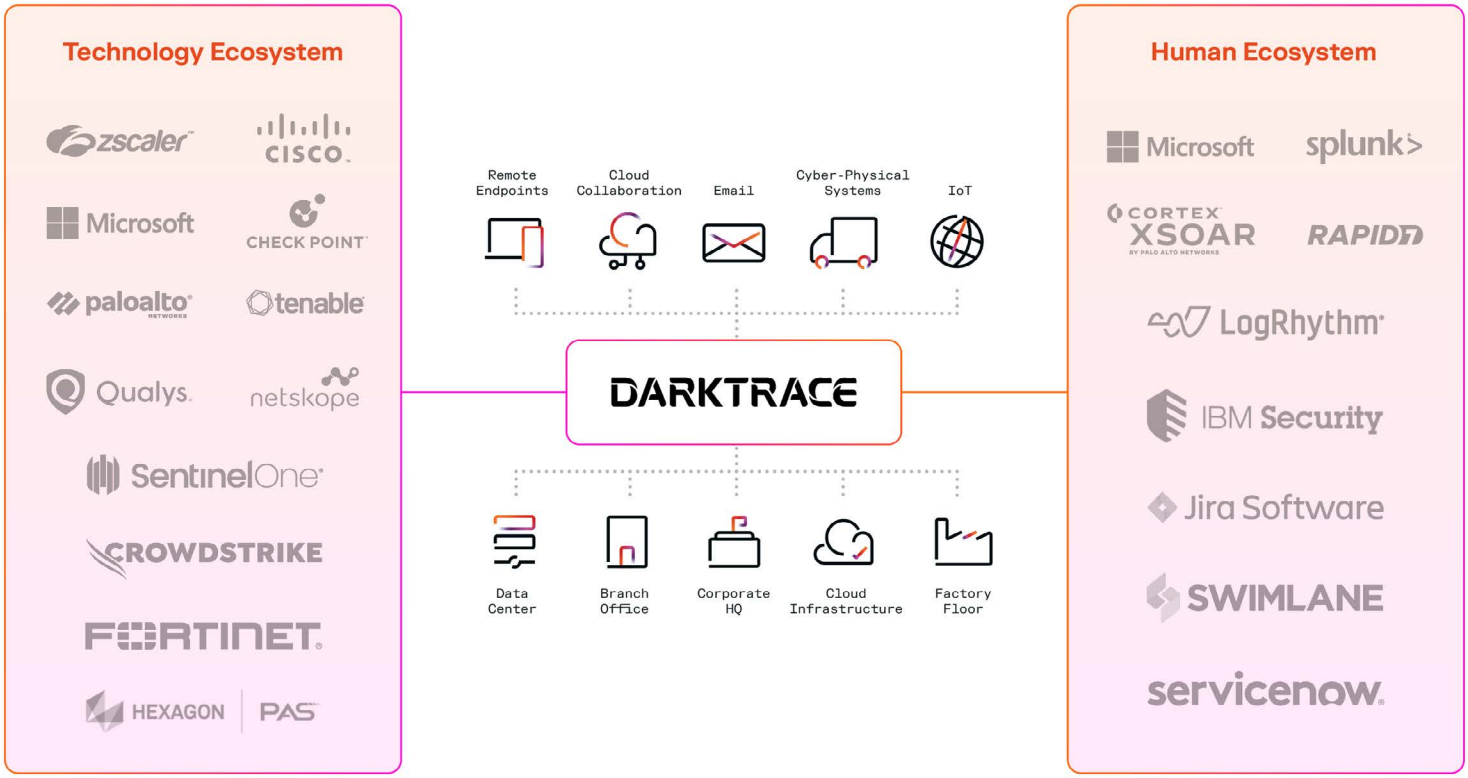


図 05: Darktraceと組み合わせることにより脅威検知、調査、遮断アクションを促進し業務ワークフローを効率化することができる多数のネイティブインテグレーション

当社のチームがいないときにも、自律遮断機能がこれらの検知結果すべてを監視し対処してくれていると思うと安心できます。

■ リチャード·ロビンソン
ネットワーク管理者、LSUA社

AIを既存のツールに適用

豊富なネイティブインテグレーションとオープンなAPIアーキテクチャにより、複雑でコストのかかる開発は必要ありません。Darktrace / NETWORK は的を絞ったネイティブな対処アクションを実行して数秒で脅威を無力化すると同時に、サードパーティ製ファイアウォール、ZTNA、SIEM、SOAR、およびITSMソリューションとのインテグレーションにより、対処機能を組織の既存のテクノロジースタックに適用することもできます。アラートは必要な任意の場所に送信して既存のワークフローを補完することができます。

また Darktrace / NETWORK は、Microsoft Defender、CrowdStrike、SentinelOne等のあらゆる主要なEDRプロバイダーとのインテグレーションも行われており、エンドポイントからのアラートを環境全体のテレメトリーのコンテキストに当てはめ、インシデントをより効果的に検知、調査および対応することができます。

ネットワーク可視性を分クラウドやリモートデバイスにも拡大

Darktrace / CLOUD

Darktrace / CLOUD により検知および遮断能力をハイブリッドクラウド環境に適用し、エンタープライズ全体のカバレッジを実現することができます。 プラットフォームネイティブな自律遮断アクションにより既知および未知のクラウドベースの脅威を数秒で無力化します。

Darktrace / ENDPOINT

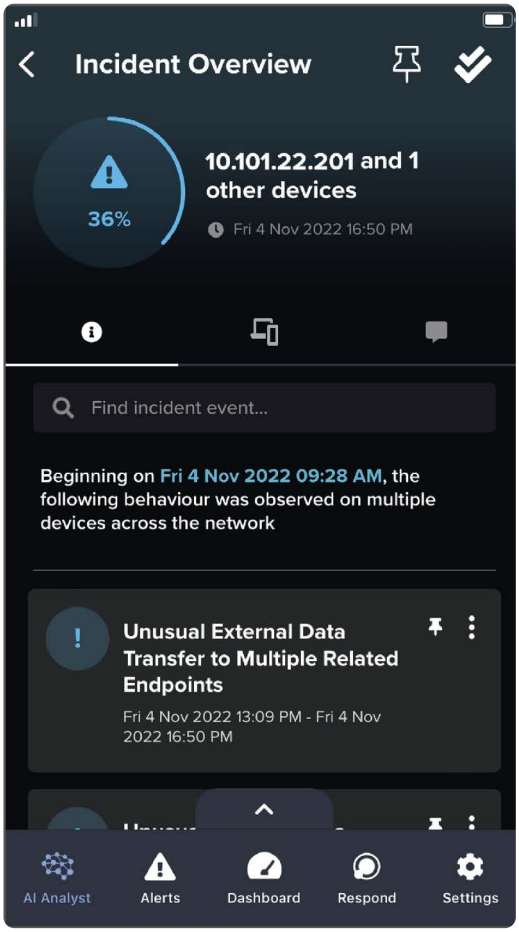
Darktrace / ENDPOINT によりリモートデバイスのネットワーク可視性を維持し、自律遮断能力をエンドポイントに適用することができます。的を絞った対処アクションにより異常な接続をシステムレベルで抑制することが可能です。

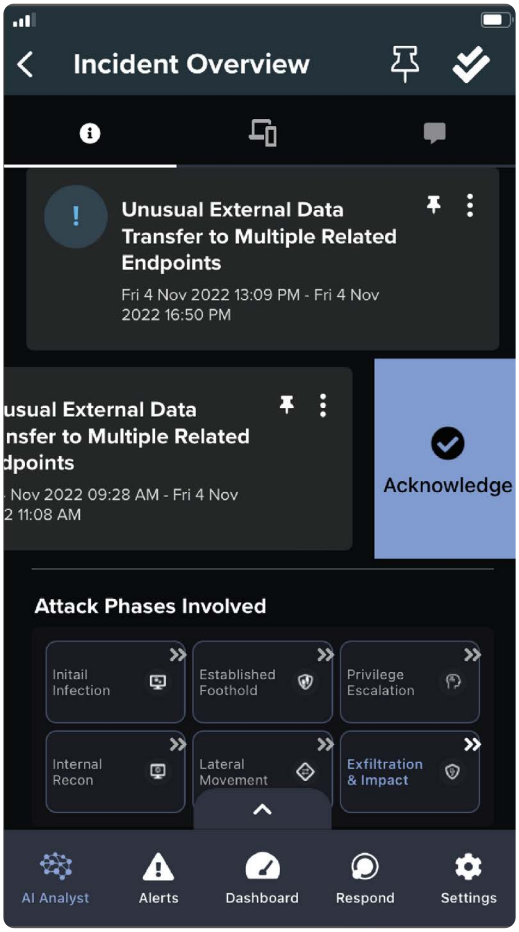
Darktrace Mobile App を使った人間の関与

Darktrace Mobile Appでは、効率的なユーザーインターフェイスを使って、どこにいてもネットワークの調査と対処が可能です。

検知された異常なアクティビティを調査する、人間の確認を待っている自律遮断アクションを承認する、同僚とアラートを共有する、またクリティカルな優先度のCyber AI Analystインシデントが作成されたときには通知を受けることができます。

Darktrace Mobile App は Android と iOS で利用することができます。





展開
Darktrace / NETWORK

Darktrace
/ NETWORK

オンプレミスからハイブリッドクラウド、そして仮想環境に至るまで、Darktrace / NETWORK はあらゆるタイプのネットワークに展開でき、最も複雑な、あるいは高度にカスタマイズされたエンタープライズ構成にも対応できます。　遮断アクションはDarktraceによりネイティブに実行することも、サードパーティファイアウォール、EDR、ZTNA、SIEM、SOARおよびITSMソリューションとのインテグレーションを通じて実行することも可能です。

展開オプション

分析

Darktraceはさまざまな方法で展開して組織の物理および仮想ネットワークへの完全な可視性を提供することができます。いずれの展開方法もDarktraceの「マスター」インスタンスのプロビジョンから開始されます。これは仮想インスタンスとして展開することも、物理ハードウェアアプライアンスを使用することもできます。環境内のネットワークデータはDarktraceマスターインスタンスにより処理および分析され、出力は Darktrace Threat Visualizerに表示されます。

Darktraceはクラウドベースのマスターインスタンスをクラウド環境（AWSおよびAzure）内でホスティングすることにより完全に仮想化された展開も可能で、これにより仮想および物理両方のネットワークロケーションに対応できます。必要に応じて、Darktrace / NETWORKはハードウェアアプライアンスをネットワークに対してパラレルに設置し、生のネットワークトラフィックを受動的に取り込むように展開することもできます。これは通常、Darktraceアプライアンスをコアスイッチに対してSPANセッションを使って接続することにより実現されます。複数のマスターが必要な場合、'Unified View' を使用することで、すべてのマスターインスタンスに対して単一の一元化されたユーザーインターフェイスを提供することができます。必要に応じてHigh Availability（HA）オプションも使用できます。

接続

Darktraceマスターインスタンスはそれ自身で生のトラフィックを処理しネットワーク全体のローカル「プローブ」（仮想または物理）からネットワークデータを収集することができます。このトポロジーでは、Darktraceプローブが取り込んだデータに対してDeep Packet Inspection（DPI）を実行し、元のトラフィックと比較してごくわずかな帯域幅でマスターアプライアンスに対して絶え間なくデータを送り続けます。パケットキャプチャデータ等の生データはプローブに保持され、マスターインスタンスのThreat Visualizer Webインターフェイスからオンデマンドで呼び出されます。

vSensorは軽量な仮想プローブであり、パブリッククラウドVPCトラフィックミラーリングにおいて仮想スイッチからパケットを受信するスタンドアロン仮想マシンとして運用することも、VM上に展開されたホストベースのosSensorエージェントからパケットを収集することも可能です。 DarktraceはKubernetes等のコンテナ化された環境と統合することもできます。

必要に応じて、ハードウェアプローブを物理的なロケーションに展開することも可能です。ネットワーク内のトラフィックの量やデバイス数に応じて、さまざまなハードウェアアプライアンスが用意されています。お客様それぞれの環境に対して、特に大規模および/または分散型ネットワーク構成の場合には、Darktrace担当者が最も適した展開方法をご提案することができます。

Darktrace / NETWORK はDarktrace / ENDPOINTの一部として展開されるホストベースのClient Sensor、統合されたサードパーティサービス（SaaSやクラウドアプリケーション等）、および連携しているDarktrace / EMAIL、Darktrace / IDENTITY、Darktrace / CLOUD等のDarktrace製品からのデータも収集します。

OT

Darktrace / NETWORK の検知および遮断機能を、お使いのOT（Operational Technology）デバイスにも適用することができます。Darktrace / OTはITとOTをネイティブにカバーし、OT、IoT、ITアセットの可視性を一元的に提供します。

Darktrace / OTは外部の接続を必要とせずエアギャップで隔離された環境にも展開することができ、Purdueモデルのすべてのレベルに渡りOTおよびITデバイスに対する優れた可視性を達成しています。

Darktrace ActiveAI Security Platformでサイバーレジリエンスを実現

Darktrace / NETWORK はDarktrace ActiveAI Security Platformの一部であり、ネットワークセキュリティをデジタルエステートの他のエリアと組み合わせて、クラウド、エンドポイント、Eメール、アイデンティティ、およびOTデバイス全体に渡るセキュリティの可視性とコントロールを強化することができます。

Darktrace / NETWORKはDarktrace / Attack Surface Managementとの連携により、外部に露出したアセットに対する継続的な、カスタマイズされた検知を提供します。 Darktrace / Proactive Exposure Managementと組み合わせることにより、組織は内部と外部のセキュリティリスクに先手を打って識別、分析、緩和するためのアクションを実行することができます。

Darktrace / Incident Readiness & RecoveryはDarktrace / NETWORKならびにActiveAI Security Platformの他のすべてのエリアから情報を受け取り、あらゆるサイバーインシデントを予測、検知、封じ込め、修復し、そこから学習するのに役立ちます。それぞれの組織専用のプレイブックと効果的な修復は組織のネットワークと脅威ランドスケープについての深い理解に基づいており、現代の攻撃者からオペレーションの継続性を守ることができます。

Darktrace ActiveAI Security Platformはサイバー攻撃のプロアクティブな予防、インシデントからのすばやい修復、セキュリティ体制の継続的強化のすべてを1つのプラットフォームから実現することにより、組織のサイバー防御に革命をもたらします。

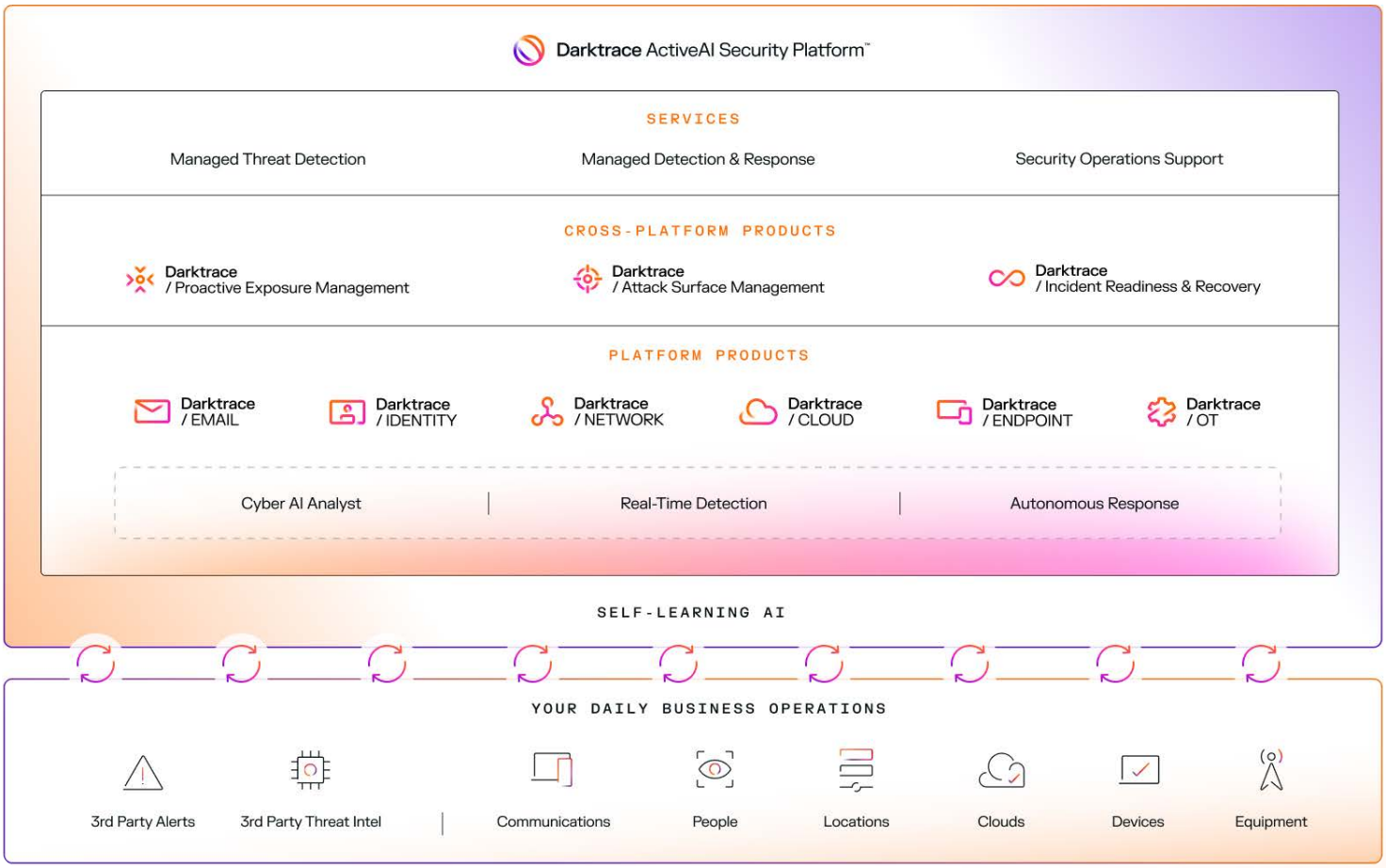


図 06: The Darktrace ActiveAI Security Platform.

運用上の利点

- **運用効率の向上**

  自律的に自身を調整する自己学習型AIにより、人手による面倒なチューニングを行うことなく重大なアラートを通知させることができます。

- **セキュリティチームに対する圧力を軽減**

  人間のアナリストと同じように分析を行うCyber AI Analystを活用することにより、セキュリティインシデントの調査を自動化してトリアージにかかる時間を92%短縮[5] することができます。

- **AIを既存のワークフローに適用**

  ファイアウォール、EDR、ZTNA、SIEM、SOARおよびITSMソリューションを含む多数のサードパーティインテグレーションを通じてワークフローを統合します。

- **完全なコントロールを維持**

  デバイスタイプ、IP範囲、業務時間、およびその他の無数のパラメータに基づく高度なカスタマイズオプションと対処アクションにより完全なコントロールを維持できます。

- **NDRを超えたセキュリティ**

  Darktrace ActiveAI Security Platformでプロアクティブにサイバー攻撃を予防し、セキュリティ体制を強化することができます。

- **サイバー防御を最大化**

  Darktrace MDR（Managed Detection & Response）によりSOCチームから24時間、週7日のサポートを受け、セキュリティの成果に集中することができます。

早期に通知を受け、個別の隔離措置についてそのコンテキストも含めて知ることができるため、対処にかかる時間がDarktrace導入以前よりも格段に改善されました。

■ ネットワーク運用マネージャー // Hauraki 地区評議会

Darktraceは他のツールが見逃しているものを検知していることに気づきました。

■ CIO // Grupo Mexicano de Seguros社

Darktraceは導入が簡単で、当社の監視と対処のニーズにも効果的であり、必要なすべての情報を提供してくれます。

■ 上級情報セキュリティアナリスト// AAA Washington

Customer's Choice for Network Detection and Response に選出

Gartner Peer InsightsのCustomers' Choice は、個々のエンドユーザーのレビューによる主観的意見、格付け、および文書化された方法論へのデータの適用に基づくものであり、Gartner社あるいはその関連会社の見解を示すものでも、それらによる保証を示すものでもありません。

■ **ダークトレースについて**

ダークトレースは、日々変化する脅威ランドスケープに組織が自律対処できるように支援するAIサイバーセキュリティのグローバルリーダーです。2013年に設立されたDarktraceは、各顧客固有の生活パターンをリアルタイムに学習する独自のAIを使用して、未知の脅威から組織を保護するために不可欠なサイバーセキュリティプラットフォームを提供しています。Darktrace ActiveAI Security Platform™は、セキュリティ体制の完全可視化、リアルタイムの脅威検知、自律遮断機能により、サイバーレジリエンスに対して先手を打つアプローチを提供し、クラウド、Eメール、アイデンティティ、OT、エンドポイント、オンプレミスネットワークを含むあらゆるデジタル環境でビジネスを保護します。英国ケンブリッジとオランダ・ハーグの研究開発チームによる画期的なイノベーションにより、これまでに200件以上の特許を出願しました。ダークトレースの従業員数は世界各国で2,400名を超え、10,000社近くの顧客を既知、未知および新手のサイバー脅威から保護しています。

北米: +1 (415) 229 9100　ヨーロッパ: +44 (0) 1223 394 100　日本: 03-5456-5537　ラテンアメリカ: +55 11 4949 7696

darktrace.com/ja | japan@darktrace.com