DARKTRACE

Data Sheet

# Darktrace アナリストサービス

Darktrace は、当社が提供するワールドクラスのサイバー AI テクノロジーおよびエキスパートアナリストから、お客様が最大限の価値を引き出して頂くことを使命としています。最適なサポートをご提供するため、Darktrace のサービスオプションはカスタマイズしてお客様のセキュリティおよび IT チームを補強、拡張できるようになっています。

サービスは脅威分析およびサイバーインテリジェンスのエキスパートである Darktrace のサイバーアナリストからご提供することも、Darktrace 認定パートナーからご提供することも可能です。あらゆる規模の企業や産業セクターで培われた経験に基づき、お客様に合わせたサービスを作成できることが最大の特徴です。

## 24 時間 365 日の Proactive Threat Notification（PTN）

### PTN サービスを 3 か月間無償で提供

英国ケンブリッジ、米国サンフランシスコ、そしてシンガポールに展開する Darktrace の Security Operations Center（SOC）は、お客様が運用する Darktrace 製品により発見された、お客様環境内の重要なインシデントに対して 24 時間切れ目のないカバレッジを提供します。Darktrace のワールドクラスのサイバーアナリストが提供するこのサービスは、脅威が進行中である可能性を示す特異なアクティビティ、または動作の逸脱についてお客様に通知します。これらのインシデントはオンデマンドで迅速にトリアージされ、イベントの発生に応じてアクションを取るために必要な情報をサイバーアナリストがお客様に提供します。

Proactive Threat Notifications（PTN）は、攻撃の発生を強く示す高確度のインシデントを世界中の Darktrace SOC に直接送信し、エキスパートで構成されるサイバーアナリストチームによるトリアージおよびレビューが行われます。

PTN サービスの一環として Darktrace が監視するアラートは、Enterprise Immune System では 'Enhanced Monitoring' タグを使って識別でき、Threat Visualizer と Model Editor 内でフィルタリングを行うことにより確認できます。また Enhanced Monitoring タグでは、どのモデルに対する違反が SOC にエスカレーションされトリアージされたかを具体的に確認できます。

Darktrace の研究開発チームは継続的に PTN サービスの評価と更新を続けることにより、最も優先度の高い違反を調査し、従来の既知の攻撃から新しい今までに出現したことのない脅威まであらゆる種類の攻撃に迅速に対処できるようにしています。

PTN により Darktrace SOC に送られたインシデントは、Darktrace のグローバルサイバーアナリストによるトリアージが行われます。より複雑な分析が必要なケースについては、Darktrace SOC は世界中のアナリストの中から上級 Level 3 アナリストにアクセスします。アラートに関する判断は、複数のアナリストが協議し、直接の差し迫った脅威に直面しているかどうかについて情報に基づいた判断を行います。

すべてのアラートがトリアージされるわけではなく、攻撃の兆候である可能性が高く Enhanced Monitoring タグでマークされたものが、PTN アナリストによりトリアージされます。

トリアージ段階で Darktrace が攻撃の有力な証拠を発見した場合には、お客様のセキュリティチームに即座に連絡が取られ、確認されたインテリジェンスが直ちにアクションを取るために送付されます。Darktrace はすべての PTN アラートを高優先度として扱うことを推奨します。完全にトリアージされたアラートは共有秘密鍵を使って暗号化され、お客様組織内の配信リストに E メールで送信されます。また、PTN から E メールアラートが発行される際、自動の電話および / または SMS メッセージを受信することも可能です。SOC の連絡方法とメッセージ送信方法は、カスタマーポータルのアカウント設定から指定することができます。

## 24 時間 365 日の Ask the Expert 機能

Threat Visualizer およびカスタマーポータルから使用できる Ask the Expert（ATE）機能を有効にすることにより、お客様のセキュリティチームから Darktrace のサイバーアナリストに質問を送り、脅威の調査を行いながらエキスパートによる支援を受けることができます。お客様の環境内の新たなまたは高度なサイバー脅威に対して、迅速なフィードバックを受けることができます。

Threat Visualizer から ATE にアクセスする際は、グラフィックやトラフィックのフローデータをドラッグ＆ドロップで問い合わせに含めることができます。このようなサポート方法により、お客様のセキュリティチームは幅広いトピックについて Darktrace のアナリストと共同で作業することができます。サイバーアナリストが ATE からの質問に対応した場合、回答は「Help -> View Questions」ドロップダウンメニューで表示できます。これらの回答はカスタマーポータルから確認することもできます。

ATE で作成できる質問の数に制限はありません。ただし、質問が分析ではなくソフトウェアの機能に関するものの場合、サイバーアナリストは質問を社内のトレーニングまたはテクニカルオペレーションチームに転送することがあります。ソフトウェア／ハードウェアサポートサービス、および機能要求については、通常通りカスタマーポータルから送信する必要があります。

ATE からのすべての質問は Darktrace サイバーアナリストチーム宛てのキューに入ります。したがって ATE は直接のチャット機能ではないものの、リアルタイムに攻撃に遭遇している場合には、Darktrace は SOC へのアクセス優先度を上げ、初期の調査段階から密接なサポートとフィードバックを提供し、Darktrace Cyber AI Platform から生成されたデータとインテリジェンスへのお客様のアクセスを確保します。

## サービスの提供とお客様データ

Darktrace のサービスは社内のグローバル SOC チームに所属するサイバーアナリストが提供します。Darktrace が提供する 24 時間 365 日のサービスへのアクセスは、サブスクリプション契約の内容によって決まります。PTN サービスを使用するには、お客様のマスターアプライアンスから標準 Call Home 機能を介した英国ケンブリッジ所在の Darktrace Management Center への接続が必要です。Darktrace は Darktrace Management Center からの詳細な監査ログを提供および監視し、契約したサービスの実施期間中に Darktrace の従業員が行うアクションを記録しています。Darktrace の従業員は、アクセストークンを付与される前に、なぜそのアカウントにアクセスするのかについて理由を提示する必要があり、これは監査対象となります。

Darktrace が提供するサービスは、分析およびレポート作成を Darktrace プラットフォーム外で行うこともあります。

Ask the Expert に入力するすべてのデータは、お客様によるものも Darktrace サイバーアナリストによるものも含め、Darktrace Management Center において Darktrace がホスティングする Darktrace カスタマーポータル内に保存されます。クローズされたチケットも、お客様によるレビューのためにカスタマーポータル内のアーカイブに保存されます。

PTN サービスで使用する 'Enhanced Monitoring' モデル違反データは、Darktrace Management Center が取得し、Darktrace SOC ダッシュボードに表示されます。このデータをアナリストがレビューした後、お客様の運用環境にログインしてさらなるトリアージを行います。即座に脅威アラートを出すべき違反の場合、アナリストが前述の方法で所見をお客様に送信します。アラートと関連したモデル違反データ、およびお客様に対して発行されたレポートは、お客様のレビューに備えて Darktrace SOC 内に保存されます。