データ シート

Zscaler Threat Hunting

追跡、検出、防御

隠れた高度な攻撃を検出、防御し、侵害を防止します。

セキュリティ上の課題

絶えず進化する脅威とアラート疲れ：高度な標的型攻撃 (APT) をはじめ、攻撃は日々進化しており、MITRE ATT&CK フレームワークには 190 を超える手法と 385 を超えるサブ手法が存在します。世界中で多くの侵害が発生し、脅威の状況は絶えず変化しているため、組織は進化する手法に日夜対峙しています。多くの場合、大量のアラートの発生が防御側の疲弊を招き、侵害の痕跡の見落としにつながっています。

過剰な脅威インテリジェンス：無数のソースから得られる脅威インテリジェンスの量には際限がなく、多くの場合、防御側はそこから実用的なインサイトを抽出して高度な攻撃を検出することができません。

人材不足：防御側はかつてないほど多くのツールやテレメトリーを活用していますが、世界的なセキュリティ人材の不足が続くなか、業務過多に陥っています。

脅威の特定の遅れ：セキュリティ インシデントの特定には平均で 212 日かかり、その間に計り知れない損害が発生する可能性があります。一般的に、専任の脅威ハンティング チームでさえも、エンドポイント データのみに焦点を当てており、インターネットを介してすでに組織のインフラに侵入した脅威しか検出できません。

脅威の性質はそれぞれ異なり、すべての攻撃ベクトルが重要とは限りません。防御を担う部門が注力すべきことを明確化するとともに、人員に制約がある場合でもプロアクティブな防御を維持し、経験の浅いアナリストからパープル チームまでが足並みをそろえて最も効果的な防御を実践できるようにする必要があります。

Zscaler Threat Hunting のサービス

Zscaler Threat Hunting™ では、エキスパートによる 24 時間体制の脅威ハンティングによって、異常、高度な脅威、従来のセキュリティ対策を回避しようとする巧妙な脅威アクターを検出します。Zscaler Threat Hunting のチームは、世界最大のセキュリティ クラウドである Zscaler Zero Trust Exchange™ のデータを利用しながら、多様な専門知識とカスタムの機械学習モデルを活かし、脅威をプロアクティブに探し出し、分析、無力化します。1 日あたり 4,000 億件以上のトランザクションを監視するクラウド ネイティブ プラットフォーム、そして 200 以上の脅威グループに関するトップクラスのプライベート脅威インテリジェンスを備えた社内の調査チームである ThreatLabz の力も活用して、お客様の SOC がセキュリティ目標を達成できるよう支援します。

主なメリット

- **高度な脅威の追跡と検出**
  Zscaler Threat Hunting は、これまでにない精度、正確性、スピードで脅威に対抗します。Zscaler のミッションは、優れたプラットフォームを基盤として、人間の脅威ハンティング チームの多様な専門知識を活用し、高度な脅威を阻止することです。プロアクティブな脅威ハンティングにより、滞留時間と影響を低減します。
- **Zscaler のエキスパートによる SOC/IR 部門の支援**
  Zscaler 独自のツールと 24 時間体制の脅威ハンティング チームによるサービスを通じ、数十億件単位のトランザクションの生データからコンテキストの充実したアラートを生成し、SecOps にとって最も実用的なインサイトを抽出することで、アラート疲れを大幅に軽減します。
- **攻撃チェーンの早い段階での脅威の阻止**
  Zscaler Threat Hunting では、エンドポイント データではなくインターネットや SaaS のトラフィックを分析することで、攻撃を早期に検出、阻止し、エンドポイントの侵害や被害の発生を多くのケースで未然に防ぎます。
- **お客様に合わせたエンタープライズレベルのエクスペリエンス**
  上位プランの Zscaler Threat Hunting Advanced では、組織固有のビジネス課題に適応した脅威ハンティング ソリューションを提供しています。Zscaler Threat Hunting Advanced は、カスタマイズされた脅威ハンティング戦略を必要とする業界のリーダー向けに設計されており、パーソナライズされたオンボーディング、戦略的なブリーフィング、戦術に関するレポート、脅威ハンティングに関する継続的なサポートを提供します。信頼できるパートナーとしてお客様の成功を第一に考え、セキュリティのレベルアップをお手伝いします。

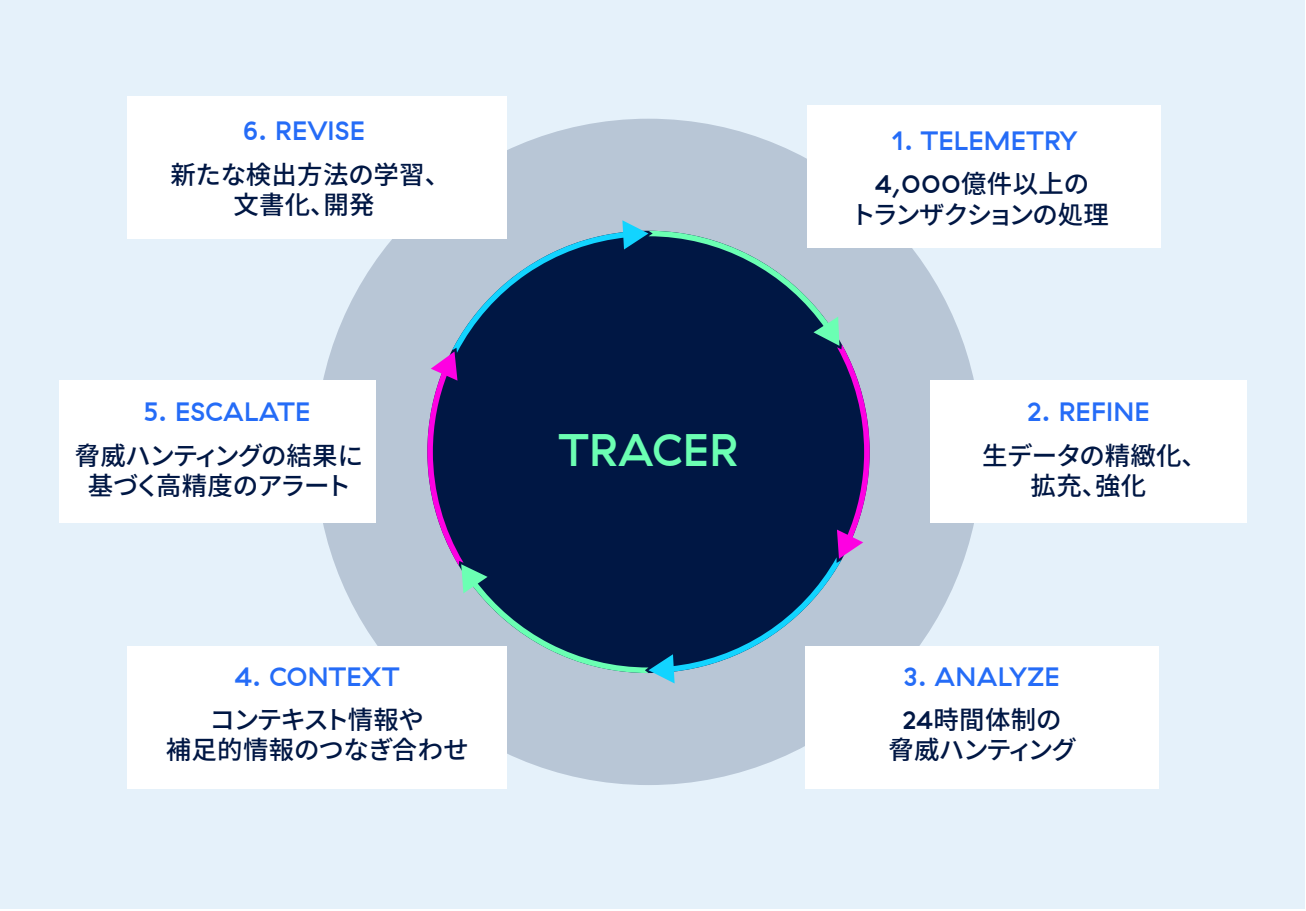
Zscaler Threat Hunting の手法

最適な対応を可能にするのは、優れたシグナルです。Zero Trust Exchange プラットフォームは、ユーザー、リソース、宛先の間でのすべての接続を仲介しているため、Zscaler は他社にない優れた可視性を得ることができます。Zscaler の脅威ハンターは、クラウドならではの規模のテレメトリーを活用して、Zscaler の世界中のインストール ベースから収集、関連付け、監視を行うことで、新たな脅威、脆弱性の悪用、攻撃戦術を特定、防御しています。

Zscaler Threat Hunting のフレームワークでは、ゼロトラストの原則、脅威インテリジェンスの焦点、仮説テスト、プレイブックを統合し、効果的な脅威ハンティングを実現しています。現場での長年の経験によって磨き上げられ、最新の脅威に合わせて調整されたこのフレームワークによって、組織は進化する脅威に正確かつ迅速に対処できるようになります。Zscaler のアプローチは柔軟性と拡張性を兼ね備えており、実際に運用して検証されたプロセスを通じ、サイバー脅威の効率的な特定と防御を実現しています。また、人間の専門性と最先端の AI を融合させた手法により、脅威を徹底的に検出します。適応性と効率性に重点を置くことで、日々変化する脅威に真っ向から立ち向かえるよう設計されています。

TRACER: Zscaler Threat Hunting の手法

TRACER は、Telemetry (テレメトリー)、Refine (精緻化)、Analyze (分析)、Context (コンテキスト)、Escalate (エスカレーション)、Revise (改善) の頭字語です。



- **Telemetry (テレメトリー):** Zscaler の脅威ハンターは、1 日あたり 4,000 億件以上のトランザクションを処理するZscaler Secure Web Gateway (SWG) から、リアルタイムの優れた可視性を得ています。
- **Refine (精緻化):** AI を活用しながら、数十億件のトランザクション データを脅威インテリジェンスで精緻化、拡充、強化します。カスタム ツールと脅威ハンティングのプレイブックを使用することで、正当なネットワーク トラフィックに紛れ込もうとする脅威アクターを検出できます。
- **Analyze (分析):** 強化されたさまざまなデータの詳細と全体像を確認しながら、構造型、非構造型、状況対応型の脅威ハンティングを 24 時間体制で実施します。
- **Context (コンテキスト):** コンテキスト情報や補足的情報をつなぎ合わせ、SOC/IR 部門に伝達します。
- **Escalate (エスカレーション):** すべての関連情報とインテリジェンスをつなぎ合わせたのち、脅威ハンターから SOC/IR 部門に実行可能なアラートのエスカレーションが行われます。
- **Revise (改善):** 脅威ハンターは、新たなプレイブックを学習、文書化、開発し、Zscaler 製品の強化と脅威ハンティングの効率性の向上に努めています。

Zscaler Threat Hunting Advanced

Zscaler Threat Hunting Advanced では、お客様のセキュリティ上の不安解消を最優先に、パーソナライズされた脅威ハンティングに加えエキスパートの助言を提供し、より高いレベルのセキュリティを実現します。

この高度なサービスでは、専任の脅威ハンターを割り当て、お客様の組織のためだけの防御戦略を策定します。担当の脅威ハンターは、戦略的なパートナーとして、プレイブックをカスタマイズし、お客様に代わってデジタルの脅威を積極的に特定します。

Zscaler Threat Hunting Advanced の特長

- **専任の脅威ハンター：**Zscaler Threat Hunting の専任の担当者が、優れたエクスペリエンスを提供します。
- **カスタムのガイダンスとコンテキスト情報：**カスタマイズされたガイダンスとコンテキスト情報によって、組織を狙った脅威を追跡する方法についてより深く理解できるようになります。
- **新たな脅威に関する実用的なレポート：**次に発生する新たな脅威をプロアクティブに追跡する方法を学ぶことで、先回りで対策を講じることができます。
- **細部にわたるカスタマイズ：**カスタマイズされた脅威ハンティングの運用アプローチにより、Zscaler Threat Hunting の効果を最適化します。
- **戦術に関する包括的なレポート：**脅威ハンティングの運用に関する詳細なインサイトを、SOC アナリスト、脅威ハンター、インシデント対応担当者向けの構成で提供します。
- **戦略的なハンティングのレビュー：**Zscaler Threat Hunting の活動をまとめた四半期ごとのエグゼクティブ向けプレゼンテーションと月次の技術レポートを提供します。セキュリティの優先順位の調整に役立てられるほか、脅威ハンティングにおける業界固有のインサイトを得られます。
- **ハンティング状況の検証：**専任の脅威ハンターによるハンティング状況の再確認を通じて、セキュリティ態勢を検証し、安心感を得られます。
- **環境に対する理解の強化：**組織の環境について深く理解した担当の脅威ハンターの知見を活用し、脅威を迅速に特定、無力化できます。
- **脅威ハンティングの新たなパターンや機能の先行提供：**担当の脅威ハンターと連携することで、脅威ハンティングの新たなパターンや機能をいち早く利用し、高度な脅威の検出に役立てられます。

Zscaler Threat Hunting Advanced は、戦略的かつカスタマイズされた、ワンランク上のコンサルティング型脅威ハンティングを提供します

	Zscaler Threat Hunting Essentials	Zscaler Threat Hunting Advanced	Zscaler Threat Hunting Advanced Dedicated
24 時間 365 日体制の脅威ハンティング	一般ハンティング チーム	一般ハンティング チーム ＋ Advanced のハンティング チーム	一般ハンティング チーム＋ Advanced のハンティング チーム＋専任の脅威ハンター
カスタマイズされた脅威ハンティング	–	✓	✓
脅威ハンティングに関する技術レポート	–	毎月	毎週
脅威ハンティングに関するエグゼクティブ向けプレゼンテーション	–	毎四半期	毎四半期 (対面)
前線からの充実したハンティング インサイト	–	✓	✓
新たな脅威への対応	継続的な脅威ハンティング	メールでのプロアクティブな情報提供	電話でのプロアクティブな情報提供
脅威ハンティングのプレイブック	Essentials	Advanced	カスタム
新しい行動分析と脅威ハンティングパターンの先行提供	–	✓	✓
先行リリース機能へのアクセス	–	✓	✓

お問い合わせ

Zscaler Threat Hunting の詳細は、Zscaler の担当者にお問い合わせいただくか、zth-sales@zscaler.com にメールでご連絡のうえご確認ください。無料の PoV も実施しております。

zscaler™ | Experience your world, secured.™

Zscaler について
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp