Zscaler™ のセキュリティ解析機能およびロギング機能をセキュリティ運用ワークフローに統合するためのベスト プラクティス

zscaler™

目次

目次

概要

セキュリティの脅威が進化し続けるなか、セキュリティ運用は私たちのデジタル ライフを守るために必要な機能となっています。セキュリティ部門は、高精度のインテリジェンス、コンテキストに基づくデータ、自動化防止ワークフローなど、急速に進化する脅威を特定して対応するための運用を継続的に改善する必要があります。アナリストの負担を軽減し、脅威を特定、調査、軽減するというセキュリティ オペレーション センター(SOC)のミッションを遂行するには、自動化を活用しなければなりません。

このガイドでは、セキュリティ運用によって新たな脅威を検出し、効果的かつ迅速に対応できるようにするための重要なプロセスとベスト プラクティスを確立するための支援を提供します。各ステップにおいて、Zscalerのセキュリティ分析機能とロギング機能を統合し、脅威の防止、ロギング、検出、調査、軽減のプロセスなど、SOCを強化するためにポリシーを最適化する方法を紹介します。

3部構成シリーズの第1回は、Zscalerダッシュボードを使用した分析とインシデント調査におけるZscalerログの活用、およびNanolog Streaming Service (NSS)を介してセキュリティ情報およびイベント管理(SIEM)システムにエクスポートされたセキュリティ ログの分析を中心に説明します。後続のドキュメントでは、Zscalerのテクノロジー パートナーシップと、SIEM、SOAR、CASB、TIPなどのSOCツールとのAPI統合による自動対応、修復、脅威ハンティングについて詳しく説明します。

SOCの目標と主なプロセス

セキュリティ運用は、より広義には脅威を特定、調査、軽減する機能として定義できます。セキュリティ運用の主な機能は以下の4つです。

- リアルタイムのイベント監視、分類、トリアージ
- 脅威の評価、優先順位付け、分析
- インシデントの対応、修復、回復
- 脆弱性の評価、監査、コンプライアンス管理

このセクションでは、これらのプロセスごとにZscalerの主な機能の概要を説明します。その後、インシデント対応のライフサイクルを通じてZscalerを使用するための設定、ポリシー、アプローチに関する詳細なアドバイスについて、さらに詳しく説明します。

リアルタイムのイベント監視、分類、トリアージ

最初のトリアージは、ログ データを収集し、関連付け、分析して「ノイズ内の信号」を見つけるための重要なステップです。侵害の主な指標(IoC)は、ユーザー アクティビティー、セキュリティ イベント、ファイアウォールの許可/ブロックなどの中にあります。さらに、これらのイベントの特定の連続や組み合わせが特定のパターンで発生している場合、注意が必要なイベントが発生していることがわかります。

環境内で脅威や異常なアクティビティーが検出されると、Zscaler Internet Access™ (ZIA™)のセキュリティ エンジンはログを生成し、リアルタイムでNanologクラスターに送信します。これらのログは、Zscalerダッシュボード、分析、ログ内で表示/分析できるほか、Nanolog Streaming Service (NSS)を介してSIEMにエクスポートすることもできます。

Zscaler Nanologは、豊富な脅威のコンテキストと、イベントの分類と脅威ハンティングに役立つその他の情報を含む圧縮形式の詳細な記録です。

脅威の評価、優先順位付け、分析

優先順位付けはあらゆる取り組みを成功させるための鍵であり、サイバーセキュリティではさらに重要です。イベントに優先順位を付けることで、セキュリティ運用部門はビジネス運営や事業継続性の維持に最も影響を与える可能性のあるイベントに集中できます。この段階では、攻撃者が環境に侵入したことを示すあらゆるアクティビティーを確認して対応することが、セキュリティ運用部門の責任となります。

Zscalerは、Zscaler ThreatLabZ調査チームからの脅威インテリジェンスと、Microsoft Active Protections Program (MAPP)を含むパートナーからの多数の脅威インテリジェンス フィードを利用することで、特定の攻撃ツールや手法、使用中のインフラストラクチャーのアクティビティーを示す特定の指標を検出し、新たな脆弱性からの積極的な保護を実現できます。

ログにはイベントを生成したエンジン、脅威の名称、脅威の種類、リスク スコア、マッチング ルール、実行したアクションなどの情報を特定するフィールドがあり、イベントの迅速な分析、特定、分類、優先順位付けに役立てることができます。

インシデントの対応、修復、回復

インシデントの検出と対応が早ければ早いほど、被害を食い止め、今後同様の攻撃が発生するのを防ぐことができる可能性が高くなります。この段階では、影響を受けるユーザーとネットワークを特定してセグメント化し、回復のための改善策を講じることが、セキュリティ運用部門の責任です。より多くのデータ ポイントと証拠があれば、その決定を下し、迅速に行動するのに役立ちます。場合によっては、セキュリティ運用部門がインシデント対応のみを担当し、修復や回復は他の部門が担当することもあります。

Zscalerはイベントの迅速な検出を支援することで修復と回復を簡素化するため、被害の拡大を防ぐために適切な対応を取ることができます。Zscaler Client Connectorによる資産検出機能やデバイス ポスチャー評価機能などのツールにより、資産に関する最新の詳細情報を得られます。ユーザー / ロケーションのプロファイルを使用することで、ポリシーを迅速に展開し、影響を受けるユーザーを特定して分離できます。

さらに、ZscalerのAPI機能と統合により、SIEM、SOAR、EDRなど、セキュリティ運用ワークフローで通常使用されるパートナー セキュリティ ソリューションを介した脅威の関連付け自動対応が可能になります。

脆弱性の評価、監査、コンプライアンス管理

セキュリティにおける最良の成果は、攻撃者がシステムに侵入するのを完全に防ぐことです。攻撃者に悪用されて環境に侵入される前に、脆弱性や設定ミスを見つけて修正することが最善です。脆弱性スキャンの実行、設定の監査、コンプライアンス レポートの生成は、このような脆弱性と設定ミスの発見に努めるSOC部門にとって最も一般的な監査アクティビティーに含まれます。これらの評価では、手続き上の脆弱性ではなく、技術的な脆弱性しか特定できないことに注意してください。

Zscalerでは、監査人、経営管理者、セキュリティ担当者などの対象者に合わせた情報を提供するレポートを、オンデマンドや事前のスケジュールに沿ってダッシュボードから生成し、コンプライアンス、ユーザー レベルのリスク エクスポージャー、ポリシーの設定ミス、推奨されるセキュリティ ポリシーの設定を確認できます。

攻撃者の行動とMITRE ATT&CKフレームワーク

MITRE ATT&CKは、攻撃者が企業ネットワークを侵害し、その中で活動するために取りうるアクションを記述するための攻撃者モデルおよびフレームワークです。このフレームワークでは、攻撃の戦術、手法、手順(TTP)を定義し、攻撃に関連する一連の手順に基づいてそれらを分類します。ログ/アクティビティーとMITRE ATT&CKの戦術を関連付けることで、攻撃の段階を特定し、攻撃者の進行を阻止するのに役立ちます。MITRE ATT&CKの詳細と、ZscalerがATT&CKをZIAに統合する方法については、こちらのホワイト ペーパーを参照してください。

Zscalerクラウド：多層防御型の脅威対策機能

ZIAは、クラウド提供型のセキュア インターネット ゲートウェイとセキュアWebゲートウェイです。ZIAは、高度にスケーラブルで真に分散されたマルチテナントの専用TCPフォワード プロキシー アーキテクチャーを基に構築され、SSL復号を含む完全なコンテンツ インスペクションに対応するよう設計されています。ZIAの詳細はZIAのデータシートを参照してください。

Zscalerクラウド プラットフォームは、キル チェーンの破壊に非常に効果的な設計を有しています。インバウンドの脅威に対しては複層的アプローチを採用し、高度な行動分析を提供するとともに、レピュテーションベースのブロックにより脅威を阻止します。

アウトバウンドの保護では、Zscalerはボットネットのコールバックや悪意のあるアウトバウンド アクティビティーを完全に防御し、データの流出やネットワーク内に潜伏しようとするマルウェアを阻止します。

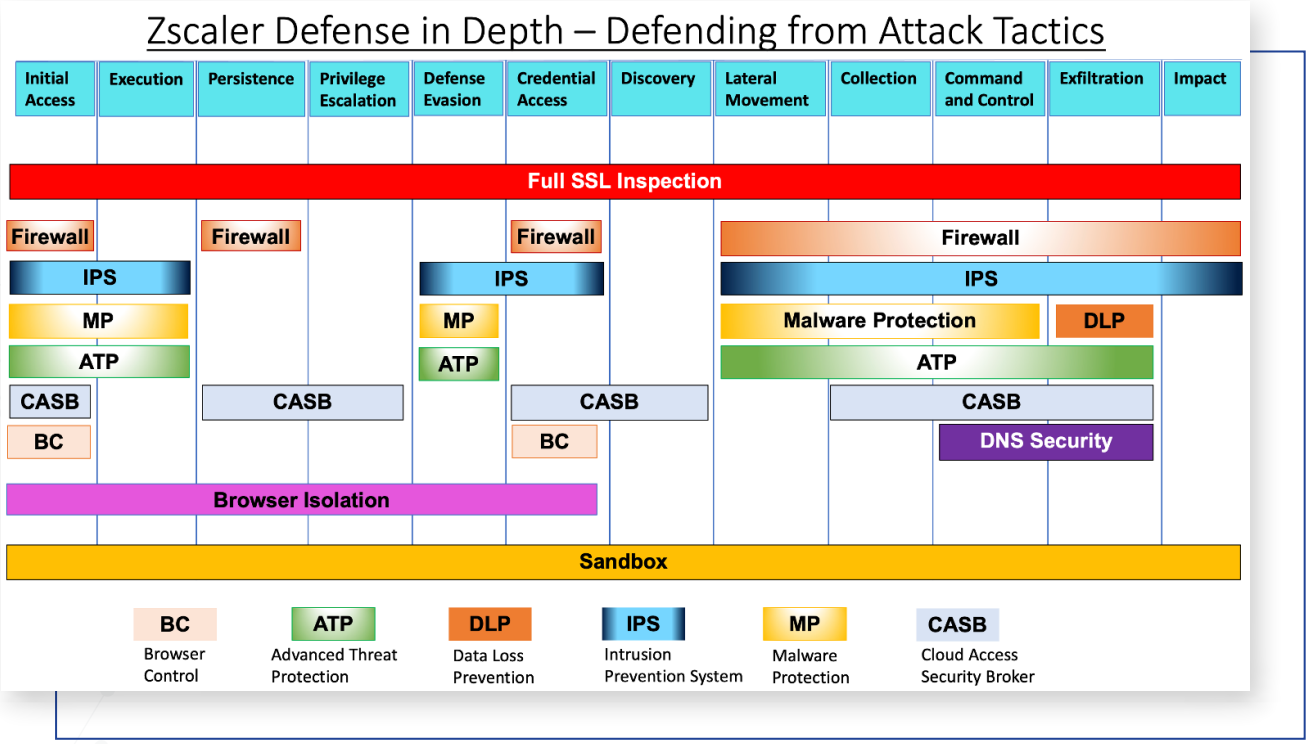


図1. ZIAセキュリティ エンジンとMITRE ATT&CKフレームワークの戦術との関係

Zscalerのセキュリティ サービスには、高度な脅威対策(ATP)、ブラウザー コントロール、ブラウザー分離、クラウド アクセス セキュリティ ブローカー(CASB)、情報漏洩防止(DLP)、DNSセキュリティ、ファイル タイプ制御、次世代ファイアウォール コントロール、侵入防止システム(IPS)コントロール、マルウェア対策、サンドボックス、SSLインスペクション、URLフィルタリング、クラウド アプリ コントロールが含まれています。

Zscaler Internet Access (ZIA)のロギング アーキテクチャー

NanologおよびNanolog Streaming Service (NSS)

すべてのユーザー トラフィックについて、Zscaler Nanologサービスは接続の終了時に詳細なログ行を作成します。一般的なプロキシー ログとは異なり、Nanologには豊富な脅威のコンテキストや脅威ハンティングに役立つその他の情報が含まれています。

Zscaler Nanologは、世界中のすべてのユーザー、ロケーション、デバイスからのログを、お客様が決める中央リポジトリーに統合します。管理者は、ユーザー、デバイス、アプリケーション、ロケーションごとにトランザクション データをリアルタイムで表示し、取り出すことができます。ログは、お客様が指定した北米または欧州のZscaler Nanologサーバーに180日間保存されます。

Zscaler Nanologは、ダッシュボード、解析、レポートなどの分析機能を強化し、ユーザーと脅威のアクティビティーをリアルタイムで可視化します。

また、Zscalerは、NSSを利用してこのログをオンプレミスまたはクラウドのSIEMにほぼリアルタイムで転送する機能にも対応しており、リアルタイムのアラート、ファイアウォールや他のデバイスのログとの関連付け、ローカルのログの長期的なアーカイブが可能です。

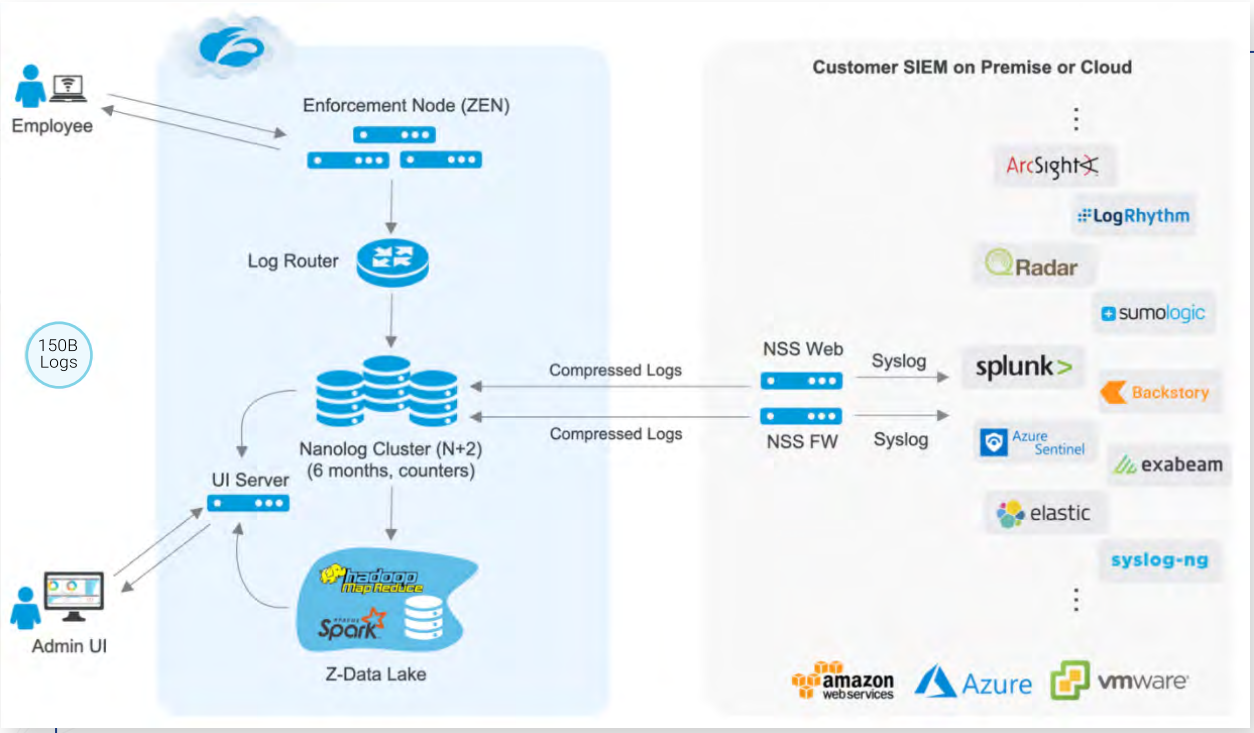


図2. Zscaler NanologおよびNanolog Streaming Service (NSS)のアーキテクチャー

ZIAの解析

セキュリティの運用や調査には、可視性が重要です。コンテキストに富んだ脅威のログは、分析、修復、脅威ハンティングに有用な情報を提供します。ZIAでは、ログ解析のための以下のようなツールを用意しています。

- **ダッシュボード** - 組織のインターネット トラフィックや脅威をほぼリアルタイムで可視化
- **解析とログ** - Nanologクラスターからのトラフィックをグラフにより解析
- **レポート** - 組織のサブスクリプションに基づき、さまざまな標準レポートを通じてデータを分析し、最大500個のカスタム レポートの作成も可能

ロールベースの管理では、ZIA Admin Portalでさまざまな管理者が実行できる操作とアクセス レベルをきめ細かく制御できます。これには、ダッシュボードの**[表示のみ]**または**[フル アクセス]**、ポリシー設定、トラフィック転送などの設定や、管理者が競合するポリシーや設定を作成しないようにするための階層が含まれます。詳細については、次のページを参照してください：
https://help.zscaler.com/zia/about-administrators

ダッシュボード

複数のダッシュボードで異なるビューを確認できるため、インターネットの使用状況を追跡し、異常な傾向やセキュリティの脅威が発生した場合に迅速に対応できます。Zscalerのサービスは、セキュリティ運用に関連する以下の定義済みダッシュボードを提供します。

- **Webの概要**ダッシュボードでは、高度な脅威を含む組織のWebトラフィックを俯瞰的に把握できます。
- **セキュリティ** ダッシュボードは、ウイルス、スパイウェア、高度な脅威など、ブロックされたさまざまな脅威に関するデータを提供します。また、サンドボックスのペイシェントゼロ イベント ウィジェットには、組織で発生したペイシェントゼロ イベントが一覧表示されます。
- **Webブラウジング** ダッシュボードでは、ブロックされた上位のURLカテゴリーや上位のユーザーなど、ユーザーのブラウジング アクティビティーを可視化できます。
- **DNS概要**は、組織のDNSトラフィックに関するデータを提供します。
- **ファイアウォール** ダッシュボードは、ファイアウォール トラフィックに関するデータを提供します。
- **IPS概要**ダッシュボードでは、組織のIPSトラフィックをリアルタイムで可視化できます。

デフォルトのダッシュボードの詳細については、次のページを参照してください：
https://help.zscaler.com/zia/about-dashboards

解析とログ

[解析]ページと[ログ] ページでは、チャートによるトラフィックの分析や、対応するNanologデータへのアクセスの際に、トラフィック情報の表示と定義が可能です。解析は以下の項目で利用可能で、特定のトランザクションにインタラクティブに掘り下げることができます。

- **Web解析とログ** - 要求されたURL、それぞれのページ リスク インデックス スコア、送受信されたバイト数など、Webトランザクションとセキュリティ イベントに関連するログ データへのアクセスを提供します。
- **モバイル解析とログ** - モバイル トラフィックについて、要求されたURL、それぞれのページ リスク インデックス スコア、送受信されたバイト数など、Webトランザクションとセキュリティ イベントに関連するログ データへのアクセスを提供します。

- **ファイアウォール解析とログ** - 適用されたファイアウォール ポリシー、ネットワーク トランザクション、クライアントとサーバーの詳細、ネットワーク サービスとアプリケーションに関連するログ データへのアクセスを提供します。
- **DNS解析とログ** - DNS要求と応答の詳細などのデータへのアクセスを提供します。データ タイプとフィルターを使用して、表示するDNSトラフィック情報を定義できます。
- **脅威解析**ページ - 組織固有の脅威を発生元からターゲットへの経路として視覚的に表示できます。脅威の統計情報の表示は2Dマップまたは3D地球儀を選択できます。
- **トンネル解析とログ** - GREトンネルとIPSecトンネルに関するデータ(健全性、ステータス、認証、暗号化アルゴリズムなど)へのアクセスを提供します。
- **SaaSセキュリティ解析とログ** - 設定されたSaaSアプリケーション/テナントに固有のWebトランザクションとセキュリティ イベントに関連するログ データへのアクセスを提供します。

解析を使用してトラフィックを分析する方法の詳細については、次のページを参照してください：
https://help.zscaler.com/zia/analyzing-traffic-using-insights

Zscaler Nanologサービスは、世界中でリアルタイムにログを統合するため、あらゆるロケーションのユーザーが実行したすべてのトランザクションを確認できます。[解析]ページでは、[ログ]タブをクリックするか、グラフ内の特定の項目をクリックして[ログを表示]を選択することで、ログを表示できます。ログはZscaler Nanologサーバーに180日間保存されます。フィルターを適用してリストを絞り込むことも、特定のユーザーやURLに関連するトランザクションを検索することもできます。ログはCSVファイルとしてエクスポートできます。

レポート

[レポート]ページでは、特定の経営管理者/部署/ユース ケースを対象とした事前定義済みのレポートを表示および作成できます。以下の事前定義済みレポートが用意されています。

- **エグゼクティブ解析レポート** - 組織の主要な役職を対象に、組織のトラフィック量とセキュリティ ポスチャーに関する概要を毎月提供します。
- **CIPAコンプライアンス レポート** - 法的責任クラスによってブロックされた上位のURLカテゴリーと、わいせつまたは有害なコンテンツへのアクセスをブロックされた上位のユーザーとドメインに関する情報を提供するインタラクティブなレポートです。
- **企業リスク スコア レポート** - 組織、ロケーション、ユーザーレベルのリスク エクスポージャーを監視および評価できます。
- **企業サマリー レポート** - 組織のCIOやCSOなどの対象ユーザー向けにカスタマイズされた情報を提供する、インタラクティブなレポートです。
- **セキュリティ ポリシー監査レポート** - セキュリティ ポリシーの設定を確認し、ベスト プラクティス ガイドラインに従って設定を改善できます。
- **四半期ビジネス レビュー レポート** - 四半期ごとに、Zscalerがどのようにネットワークの保護に役立っているかについて幅広い解析結果を提供します。このレポートは、新たなトラフィックの傾向や、Zscalerがブロックしている脅威の種類を観察するのに役立ちます。
- **SaaSアセット サマリー レポート** - SaaSセキュリティ APIベースの検出および修復活動の概要を確認できます。どのデータが影響を受けているかを調査し、リスクのあるユーザーを特定する際の出発点となります。
- **SaaSアセット レポート** - ファイルや電子メール メッセージの現在の状態を表示します。また、特定のファイルや電子メール メッセージの活動を一度に確認することも可能です。

- **異常検知レポート**(リリース 6.1 の新機能) - 異常なユーザー行動と組織レベルの異常を高い信頼度で検出し、データ流出の可能性があるイベントや悪意のある内部関係者を特定するのに役立ちます。

また、インタラクティブ レポートではリアルタイムのインタラクティブ分析が可能で、企業サマリー レポート(CSO)などの標準的なレポートも豊富に用意されています。さらに、ユーザーが要求した特定のURLや、各URLのリスク スコアなどの詳細を確認できます。レポートのスケジューリングでは、指定した受信者に標準レポートやカスタム レポートを定期的に配信することが可能です。

Zscaler Nanolog Streaming Service (NSS)

Zscaler NSSは、以下の2種類の高度に圧縮されたログのストリームを提供し、SIEMにストリーミング配信できます。

- Web用のNSS: Webおよびモバイルのトラフィック ログをストリーミングします。
- ファイアウォール用のNSS: Zscalerの次世代ファイアウォールのログをストリーミングします。

Webとモバイルのトラフィック ログとファイアウォール ログは、Zscalerサービス クラウドのNanologに保存されます。ログは暗号化され、帯域幅のフットプリントを削減するために高度に圧縮された形式でストリーミングされます。組織は、ログのスクランブルを解除し、設定されたフィルターを適用して不要なログを除外し、フィルターされたログを設定された出力形式に変換してログをSIEMで解析できるようにし、Raw TCP接続を介してSIEMにログをストリームするNSS仮想マシン(VM)を導入する必要があります。

少なくとも、Webログとモバイル ログ用に1つのNSSを導入し、ファイアウォール ログ用にもう1つのNSSを導入することをお勧めします。各NSSは、Zscalerクラウド内のNanologへの安全なトンネルを開きます。

Webログ用のNSS

Webログ ストリーム用のNSSは、圧縮形式の詳細な記録であり、豊富な脅威のコンテキストや、修復や脅威ハンティングに役立つその他の情報を含んでいます。100を超えるフィールドが含まれています。NSSフィードを設定して、Webプロキシー、トンネル、SaaSセキュリティ、アラートのログを選択的にフィルタリングし、個別のフィードとしてSIEMに送信できます。

イベントのストリームは以下のログ タイプについて生成されます。

- プロキシー ログ：IPS (Web)ログなど、Zscalerプロキシーによって処理されるすべてのアクセス ログ
- トンネル ログ：アップ/ダウン トンネル イベントと使用統計情報の概要
- SaaSセキュリティ ログ：SaaSアプリケーションで発生したクラウド アクセス セキュリティ ブローカー(CASB)イベント
- アラート ログ：接続損失などのイベントに対するシステム アラート

ファイアウォール ログ用のNSS

ファイアウォール ログ用のNSSストリームには、圧縮形式のファイアウォール ログとDNSログが含まれます。NSSフィードを設定して、ファイアウォール、DNS、アラートのログを選択的にフィルタリングし、個別のフィードとしてSIEMに送信できます。

イベントのストリームは以下のログ タイプについて生成されます。

- Cloud Firewallログ：IPS (非Web)ログなど、Zscaler Cloud Firewallによって処理されるすべてのアクセス ログ
- DNSログ：Zscaler経由で送信されるDNSトラフィックのログ
- アラート：接続損失などのイベントに対するシステム アラート

Web用のIPSと非Web用のIPS

高度な脅威対策に含まれるWeb用のIPSは、クロスサイト スクリプティング、ボットネット、コマンド＆コントロール トラフィック、埋め込み型の/悪意のあるWebページなど、Webトラフィック(HTTP、HTTPS、FTP)から発生する脅威を検出するシグネチャーベースのエンジンです。

Cloud Firewallに含まれる非Web用IPSは、すべてのポートとプロトコル経由のネットワーク レベルの侵入を検出するシグネチャーベースのエンジンです。これには、HTTP、HTTPS、FTP、DNS、TCP、UDP、IPベースのポートおよびプロトコルに対する保護が含まれます。IPSコントロールでは、特定のユーザー、グループ、部署などに対してきめ細かなルールを作成することもできます。**[IPSコントロール]**はロケーションごとに有効にすることも可能です。

Webトラフィックで検出された脅威は**Webログ**に表示され、非Webトラフィックは**ファイアウォール ログ**に表示されます。Webトラフィックと非Webトラフィックの両方で検出された脅威は、**[ファイアウォール解析] > [ログ]**に表示されます。Web専用トラフィックから検出された脅威は、**セキュリティ ダッシュボード**にも表示されます。Web以外のトラフィックから検出された脅威は、**IPSダッシュボード**にも表示されます。

注：Web IPSポリシーが最初に適用され、次に非Web IPSが適用されます。

NSSの導入

NSSインスタンスは、オンプレミス、ESX仮想マシン、EC2インスタンス、AWS、Microsoft Azureにも導入できます。これらのプラットフォームに対するNSSの導入ガイドは以下のとおりです。

https://help.zscaler.com/zia/nss-deployment-guide-amazon-web-services
https://help.zscaler.com/zia/nss-deployment-guide-microsoft-azure
https://help.zscaler.com/zia/nss-deployment-guide-vmware-vsphere

Syslogフォーマット

Zscalerは多くのsyslogフォーマットをサポートしています。これには、業界標準のフォーマットと、カスタム ログ文字列を作成する機能が含まれます。SIEMで使用される主な規格として、Common Event Format (CEF)とLog Event Extended Format (LEEF)の2つがあります。詳細については、次のページを参照してください：https://help.zscaler.com/zia/syslog-overview

NSSフィード

NSSフィードは、NSSがSIEMに送信するログのデータを指定します。各フィードには、異なるフィールドのリスト、異なる形式、および異なるフィルターを含めることができます。ログに1つ以上のフィードを追加し、アラートに1つのフィードを追加できます。NSSごとに最大8つのNSSフィードを追加できます。

NSSフィードの設定については、以下のヘルプ記事を参照してください。

https://help.zscaler.com/zia/adding-nss-feeds-alerts
https://help.zscaler.com/zia/adding-nss-feeds-dns-logs
https://help.zscaler.com/zia/adding-nss-feeds-firewall-logs
https://help.zscaler.com/zia/adding-nss-feeds-saas-security-logs
https://help.zscaler.com/zia/adding-nss-feeds-tunnel-logs
https://help.zscaler.com/zia/adding-nss-feeds-web-logs

NSSフィード出力形式

フィード出力形式は、出力に表示されるフィールドを定義します。NSSフィード/ログのタイプごとに、新しいフィードを追加してログ タイプを選択すると、デフォルトのフィード出力形式が設定されます。デフォルトのリストは編集できます。**[フィード出力タイプ]**で**[カスタム]**を選択した場合は、区切り文字も変更します。

設定可能なすべてのフィールドと形式については、以下のページを参照してください。

https://help.zscaler.com/zia/nss-feed-output-format-dns-logs
https://help.zscaler.com/zia/nss-feed-output-format-firewall-logs
https://help.zscaler.com/zia/nss-feed-output-format-tunnel-logs
https://help.zscaler.com/zia/nss-feed-output-format-saas-security-logs
https://help.zscaler.com/zia/nss-feed-output-format-web-logs

次のヘルプ記事に記載されている、NSSフィードとフィード形式に関する一般的なガイドラインに従うことをお勧めします：**https://help.zscaler.com/zia/general-guidelines-nss-feeds-and-feed-formats**

Webログの詳細な分析

Webログでは、Webトランザクションとセキュリティ イベントに関連するログ データを確認できます。Webログは、100のフィールドにわたる脅威コンテキストを提供します。大きく分けると、Webログは次の5種類のセキュリティ ログに分類して分析することができます。

- **コンテンツ フィルタリング**(URLフィルタリングとファイル タイプ制御)
- **マルウェア対策**(レピュテーション、アンチウイルス、Yara)
- **高度な脅威対策**(レピュテーション、IPS (Web))
- **サンドボックス** – 既知の悪意のある(クラウド効果)
- **サンドボックス** – 不明(ゼロデイ攻撃の可能性あり)

Webログにはカテゴリーごとに多くのフィールドが含まれていますが、一般に、以下のキー フィールドを使用して、上記の5種類のセキュリティ ログを検索/識別し、調査に利用できます。

Webログ フィールド	Web解析フィールド	説明と例
Ruletype	ポリシー タイプ	ポリシー タイプ(ブロック ルールにのみ適用され、許可には適用されません)。例：ファイル タイプ制御、情報漏洩防止、サンドボックス
Rulelabel	ルール名	適用されたルールの名前(ブロック ルールにのみ適用され、許可には適用されません)。例：URL_Filtering_1
malwareclass	脅威のクラス	トランザクションで検出されたマルウェアのクラス。例：Win32.Ransom.WannaCry
malwarecat	脅威のカテゴリー	トランザクションで検出されたマルウェアのカテゴリー。例：アドウェア、トロイの木馬、サンドボックス マルウェア
urlclass	URLクラス	宛先URLのクラス。例：一般的なネット サーフィン、プライバシー リスク
urlcat	URLカテゴリー	宛先URLのカテゴリー。例：エンターテイメント、アダルト テーマ、ゲーム
filetype	ファイル タイプ	トランザクションに関連するファイルのタイプ。例：RARファイル、ZIP、Windows実行可能ファイル
fileclass	ファイル クラス	トランザクションに関連するファイルのタイプ。例：アクティブWebコンテンツ、アーカイブ ファイル、オーディオ
threatname	脅威の名前	トランザクションで検出された脅威の名前。例：win32.banker.trickbot
reason	ポリシー アクション	トランザクションがブロックされた場合に、サービスが実行したアクションと適用されたポリシー。例：ウイルス/スパイウェア/マルウェアのブロック(このカテゴリーの閲覧は許可されていません)

また、[reason] フィールドを使用して、レピュテーション ブロックとコンテンツベースのブロックを区別することもできます([IPS block outbound request: botnet command-and-control traffic]と[reputation block outbound request malicious URL]など)。

また、以下のフィールドも調査に役立つ場合があります。

Webログ フィールド	解析フィールド	説明と例
ssldecrypted	SSL検査済み	トランザクションがSSLインスペクションを受けたかどうか。例：はい/いいえ
referrer	参照元URL	HTTPの参照元URL。例：www.google.com
location	ロケーション	ゲートウェイのロケーションまたはソースのサブロケーション。例：本社
bamd5	MD5	トランザクションで検出されたマルウェアファイルのMD5ハッシュ、または解析用にSandboxエンジンに送信されたファイルのMD5
riskscore	URLクラス	宛先URLのページ リスク インデックスのスコア。このサービスは、いくつかの要因を比較検討することによって各ページのリスクを計算します。リスクが最も低いものから高いものまで、0～100の範囲で設定されます。例：10

さらに、**[プロトコル]**をキー フィールドとして使用し、HTTP、HTTPS、SSLを使用するステルス脅威を特定/検索できます。

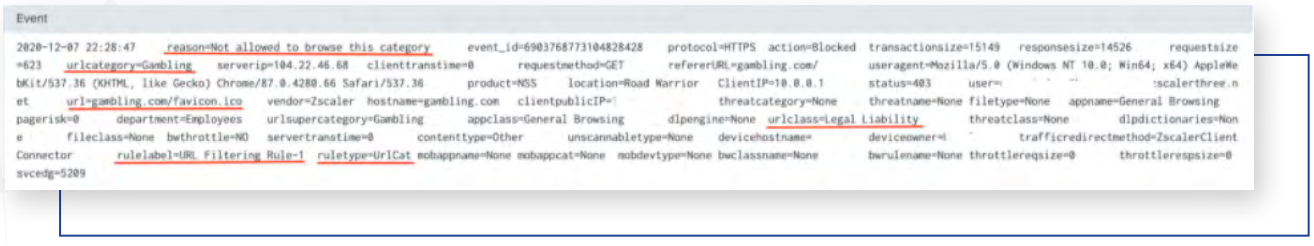
コンテンツ フィルタリング(URLフィルタリングとファイル タイプ制御)ログ

コンテンツ フィルタリング ログを分析することで、URLのカテゴリーが許可されていない、EXEファイルなどのファイル タイプのダウンロードが許可されていないなど、ポリシー違反によるトラフィック ブロックを特定できます。

Webログを詳細に分析して、URLカテゴリー フィルタリング ポリシー違反によるトラフィック ブロックを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

ruletype=“UrlCat”
rulelabel=“<rulename>”
urlcat=<predefined>, <custom> or <TLD>

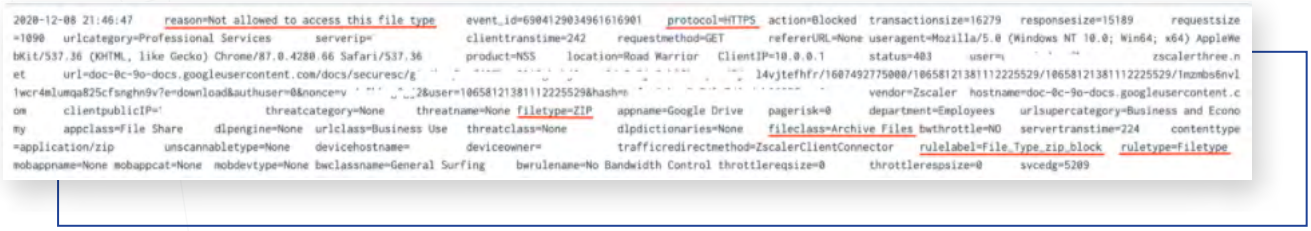
URLフィルタリング ログのサンプル



Webログを詳細に分析して、ファイル タイプ制御ポリシー違反によるトラフィック ブロックを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

ruletype=“Filetype”
rulelabel=“<rulename>”
fileclass=“Executable, Archive, Office,…”
filetype=“exe, exe64, py,…”

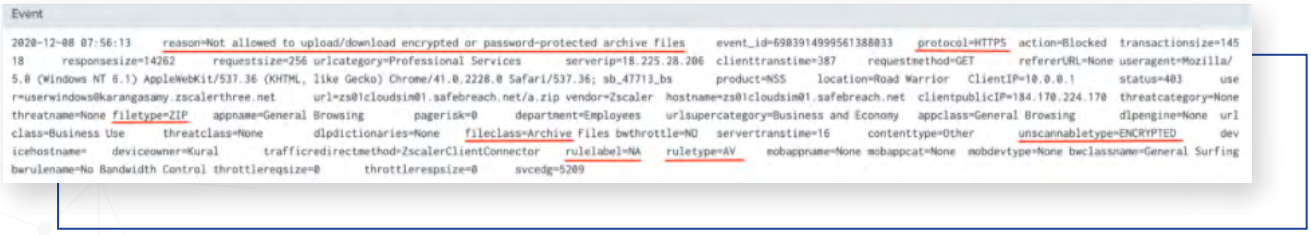
ファイル タイプ制御ログのサンプル



さらに、何らかの理由でファイルの内容を解析またはスキャンできない場合(アーカイブの破損、パスワードで保護されている、ファイル タイプを特定できないなど)、特別なフィールド[unscannabletype]にスキャン失敗の理由が表示されます。このフィールドを使用して、スキャンされなかったファイルを検索/特定できます。

unscannabletype=“Unscannable”, “Undetectable”, “Encrypted/Password Protected”

スキャン不可能なファイル ログのサンプル



マルウェア対策(レピュテーション、アンチウイルス、Yara)ログ

マルウェア対策のログを分析することで、セキュリティ部門は、ポリシー違反者、悪意のあるファイルのダウンロード、侵害されたユーザー/エンドポイント/デバイスなどの潜在的な脅威を特定し、脅威が広まる前に是正措置を講じることができます。このタイプのログには、HTTP(S)経由で転送されたファイルに対するマルウェア検出の評決、つまりファイル レピュテーション、アンチウイルス、Yaraファイル スキャンが含まれます。

Webログを詳細に分析して、マルウェアによるトラフィック ブロックを特定するには、次のキー フィールドと検索パラメーターが役立ちます：**ruletype**=“AV”

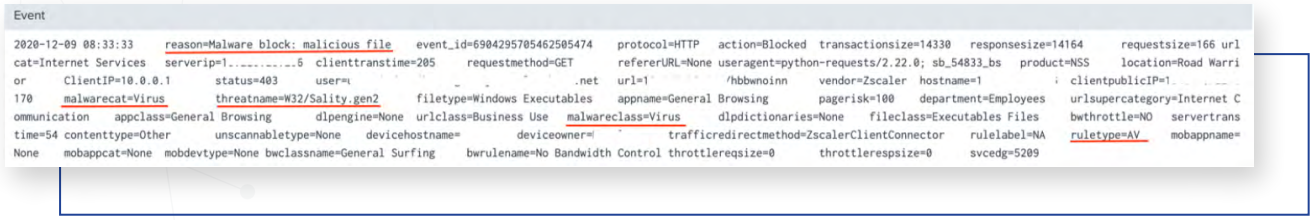
さらに、**[malwarecat]**または**[malwareclass]**フィールドを使用して、特定のマルウェア カテゴリーまたはマルウェア クラスでブロックされた脅威を検索/特定できます。

malwarecat= “Adware,” “Archive Bomb,” “Backdoor,” “Dialer,” “Downloader,” “Exploit,” “Macro Virus,” “MalwareTool,” “Other Malware,” “Other Spyware,” “Other Virus,” “Password Stealer,” “Ransomware,” “Trojan,” “Unrecognized Virus,” “Unwanted Application,” “Worm,” “None”

malwareclass=<custom>
e.g. **malwareclass**= “Virus”, “Spyware”

[reason]フィールドを使用して、マルウェアのブロックを検索/特定することもできます。

マルウェア対策のログのサンプル



高度な脅威対策(レピュテーション、IPS (Web))ログ

高度な脅威対策のログを分析することで、セキュリティ部門は、悪意のある宛先/コンテンツ/トラフィックのパターン、フィッシング、コマンド＆コントロール トラフィック、侵害されたユーザー /エンドポイント/デバイス、脆弱で望ましくない可能性のあるアプリケーションなどの潜在的な脅威を特定し、脅威が広まる前に是正措置を講じることができます。このタイプのログには、クラウドIPSおよびレピュテーションベースのエンジンによる高度な脅威の検出が含まれます。レピュテーションベースの検出では、不審な宛先IP、ドメイン、URLを検索し、ページ内の悪意あるコンテンツを特定することでページのリスクをリアルタイムで計算するページ リスク インデックスを活用します。IPSエンジンはシグネチャーベースの検出を使用し、高い忠実度を誇ります。IPSボットネット コールバックは、通信パターンに基づいて記述されているため、高い信頼性があります。ブラウザー エクスプロイト、SSHトンネリング、Cookieの盗難などの一部の脅威は、 IPSによってのみ検出できます。

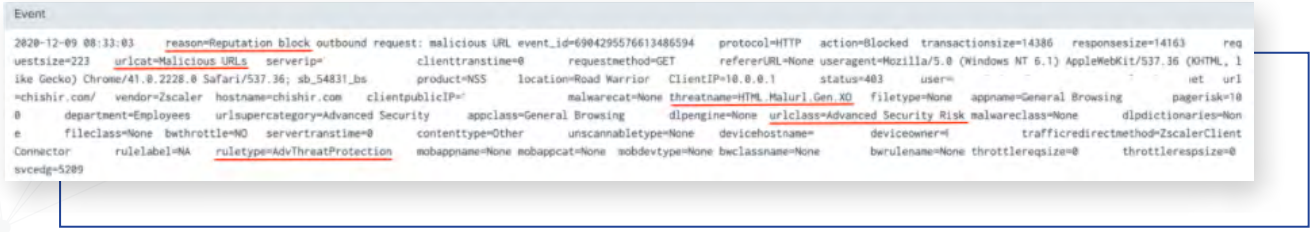
[reason]フィールドを使用して、高度な脅威ブロックを検索/特定し、レピュテーションに関するブロックとIPSに関するブロックを区別できます。

Webログを詳細に分析して、高度な脅威によるトラフィック ブロックを特定するには、次のキー フィールドと検索パラメーターが役立ちます：**ruletype**="AdvThreatProtection"

さらに、**[urlcat]**または**[urlclass]**フィールドを使用して、高度なセキュリティ リスクとして分類された特定のURLカテゴリーまたはURLでブロックされた脅威を検索/特定できます：**urlclass**="Advanced Security Risk"

urlcat= “Adv Security,” “Phishing,” “Botnets,” “Malicious URLs,” “Peer-to-peer,” “Unauthorized Communication,” “Cross-site Scripting,” “Browser Exploit,” “Suspicious Destinations,” “Suspected Spyware or Adware,” “WebSpam,” “PageRisk,” “Adware/Spyware Sites,” “Cryptomining”

高度な脅威対策のログのサンプル

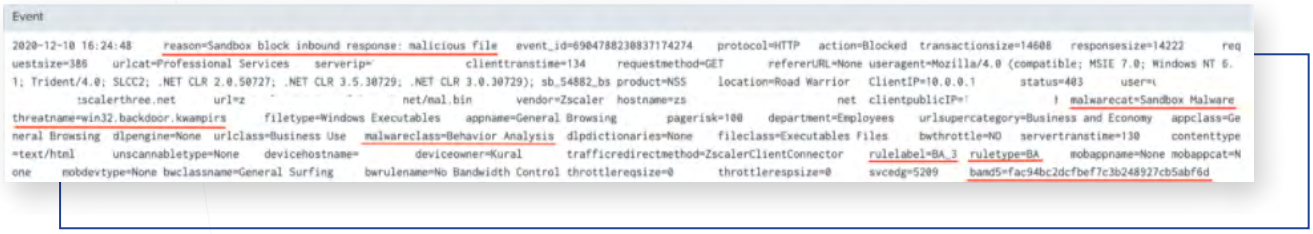


サンドボックス – 既知の悪意ある(クラウド効果)ログ

サンドボックス環境は、不明なファイルのサンプルを実行して、悪意のある動作があるかどうかを判断するために使用されます。分析のためにサンドボックスにファイルが送信されると、エンド ユーザーは隔離されるかファイルのダウンロードを許可されますが、これはお客様固有のサンドボックス ポリシーによって決定されます。このタイプのログには、サンドボックスに送信された不明なファイルのうち、サンドボックスが悪意があると判断したファイルに対する評決が含まれます。

Webログを詳細に分析して、サンドボックスが判断した悪意のある動作によるトラフィック ブロックを特定するには、次のキー フィールドと検索パラメーターが役立ちます：**ruletype**= “BA”
malwarecat= “Sandbox Malware”, “Sandbox Adware”, “Sandbox Anonymizer”

既知のサンドボックスの悪意のあるログのサンプル



Advanced Cloud SandboxとAPIライセンスをお持ちの場合、SIEMのログから取得したMD5パラメーターに基づいてサンドボックス詳細レポートを取得できます。MD5がログに含まれていない場合は、キー フィールド[**bamd5**]をフィードに追加することで、Webログから取得できます。Cloud Sandbox APIを使用して、MD5ハッシュの完全な詳細レポートを取得できます。このレポートを取得するための構文は、次のAPIリファレンスのリンクを参照してください：**https://help.zscaler.com/zia/api**

サンドボックス – 送信(不明)ログ

サンドボックス環境は、不明なファイルのサンプルを実行して、悪意のある動作があるかどうかを判断するために使用されます。分析のためにサンドボックスにファイルが送信されると、エンド ユーザーは隔離されるかファイルのダウンロードを許可されますが、これはお客様固有のサンドボックス ポリシーによって決定されます。このタイプのログには、サンドボックスに送信され、サンドボックスの実行フェーズを通過する不明なファイルが含まれます。

Webログを詳細に分析して、サンドボックス分析に提出されたファイルを検索/特定するには、以下のキーフィールドと検索パラメーターが役立ちます。

ruletype= “BA”
malwarecat= “Sent for Analysis”

エンジンおよびポリシーの理由へのアクション/イベントのマッピング

Webログに含まれる[reason]フィールドは、脅威イベントを検出したイベント タイプとエンジンの詳細な記述です。可能な値は100を超えており、個々のセキュリティ /ポリシー エンジンに適切にマッピングされています。たとえば、[Malware block: malicious file]はマルウェア対策エンジンによって検出され、[IPS block inbound response: anonymization site]は高度な脅威対策エンジンのクラウドIPSによって検出されます。詳細については、次のページを参照してください：**https://help.zscaler.com/zia/policy-reasons**

ファイアウォール ログの詳細な分析

ファイアウォール ログは、NGFW、DNS、IPS (非Web)のトランザクションとセキュリティ イベントに関連するログ データへのアクセスを提供します。IPSイベントは、ファイアウォール イベントと一緒に送信されます。DNSイベントは別のフィードで送信されます。ファイアウォール ログは、50のフィールドにわたる脅威コンテキストを提供します。大きく分けると、ファイアウォール ログは次の3種類のセキュリティ ログに分類して分析することができます。

- **ファイアウォール**(セッション、デバイス、ネットワーク サービスとアプリケーション、宛先)
- **IPS** (非Web)
- **DNS**

ファイアウォール ログにはカテゴリーごとに多くのフィールドが含まれています。一般に、以下のキーフィールドを使用することで上記のさまざまなカテゴリーのセキュリティ ログを検索/識別し、調査に利用できます。

ファイアウォール ログ フィールド	ファイアウォール解析 ログ フィールド	説明と例
Rulelabel	ルール名	トランザクションに適用されたルールの名前。 例：推奨されるファイアウォール ルール
nwsvc	ネットワーク サービス	使用されたネットワーク サービス。 例：HTTP、DNS
nwapp	ネットワーク アプリケーション	アクセスされたネットワーク アプリケーション。 例：Skype
cdip / cdport	クライアントの宛先IP/クライアントの宛先ポート	クライアントの宛先IP/ポート。 例：198.51.100.54、53
tsip	クライアント トンネルIP	クライアント(送信元)のトンネルIPアドレス。 例：192.0.2.15
destcountry	国	宛先IPアドレスの国。例：米国
ipsrulelabel	IPSルール名	ファイアウォール セッションに適用されたIPSポリシーの名前。例：デフォルトのクラウドIPSルール
threatcat	脅威のカテゴリー	IPSエンジンによるファイアウォール セッションでの脅威のカテゴリー。例：ボットネット コールバック
threatname	脅威の名前	IPSエンジンがファイアウォール セッションで検出した脅威の名前。例：Win32.Trojan.DNSpionage
ipcat	サーバー IP カテゴリー	サーバーのIPアドレスに対応するURLカテゴリー。 例：インターネット サービス

DNSログ フィールド	DNS解析ログ フィールド	説明と例
reqtype	DNSリクエスト タイプ	要求されたDNSレコード。例：Aレコード
req	リクエストされた ドメイン	DNSリクエストの完全修飾ドメイン名(FQDN)。例：mail.safemarch.com
res	DNSレスポンス	DNSレスポンス。例：198.51.100.54
sport	サーバー ポート	リクエストのサーバー ポート。例：53
domcat	IPドメイン カテゴリー	DNSリクエストに含まれるFQDNのURLカテゴリー。例：プロフェッショナル サービス

Zscaler API

Zscalerは、お客様が活用できるように、読み取りと書き込みの機能を含む多くのオープンAPIをサポートしています。クラウド サービスAPIを使用すると、以下のZscaler Internet Access (ZIA)機能へのプログラムによるアクセスを得られます。

- ZIA Admin PortalおよびAPIで行われたポリシー変更の監査ログ レポートの作成とダウンロード
- 管理者ロールの取得と管理者の管理
- 特定のロケーションのVPN資格情報の取得と更新
- サンドボックス詳細レポートの取得
- 個々のユーザー、グループ、部署の管理
- SD-WANパートナー統合のためのIPSec VPNトンネルの管理
- ロケーションとサブロケーションの管理
- ルート証明書、証明書署名要求(CSR)、中間証明書チェーンの管理
- URLカテゴリーの管理と更新
- URLのホワイト リストとブラック リストの管理

Zscaler APIの仕様の一覧は、次のページを参照してください：**https://help.zscaler.com/zia/api**

サンドボックス

Zscaler Cloud Sandboxサービスは、統合ファイル動作分析であるサンドボックス分析を通じて、未知の脅威やゼロデイ脅威、高度な永続的脅威(APT)に対する追加のセキュリティ層を提供します。分析のためにサンドボックスにファイルが送信されると、エンド ユーザーは隔離されるかファイルのダウンロードを許可されますが、これはお客様固有のサンドボックスポリシーによって決定されます。詳細については、次のページを参照してください。**https://help.zscaler.com/zia/configuring-sandbox-policy**

サンドボックスの実行結果は、悪意のある評決が出た場合、ユーザーが侵害されていること、またはお客様の組織やビジネスにリスクをもたらす行動に関与していることを示す可能性があるため、お客様にとって大きな関心事になる可能性があります。そのため、Zscalerはサンドボックスの完全なレポートを製品の機能にしており、これにはサンドボックスの実行後の詳細なレポートをAPIで取得する機能が含まれています。

Advanced Cloud Sandboxを使用している場合は、SIEMのログから取得したMD5パラメーターに基づいてサンドボックス詳細レポートを開くことができます。詳細は次のページを参照してください：
https://help.zscaler.com/zia/viewing-sandbox-reports-data

監査ログ

管理者がZscalerコンソールにアクセスし、コンソール内で変更を加えると、監査ログが生成されます。これらのイベントは、たいていの場合はZscalerの外部にアーカイブする必要がありますが、Zscalerはこれらのイベントを Zscaler API経由で利用できるようにしています。

Zscalerアラート

ア**ラート** サブスクリプション サービスは、セキュリティやアクセス制御のイベント、システムやコンプライアンス違反のアラート、ペイシェントゼロ イベントなど、特定のイベント発生時に特定の個人に電子メールを送信する機能を提供します。アラートの詳細とアラートの定義方法については、次のヘルプ テキストの記事を参照してください：https://help.zscaler.com/zia/about-alerts

セキュリティ運用のベスト プラクティス

セキュリティ ポリシーのベスト プラクティス

マルウェア対策ポリシー：

- マルウェア対策ポリシーを設定し、ウイルス、トロイの木馬、ワーム、マルウェア、ランサムウェア、不要なアプリケーション、アドウェア/スパイウェアなどから組織を保護します。
- インバウンドとアウトバウンドの両方のトラフィック検査を有効にします。
- セキュリティの例外 – パスワードで保護されたファイルやスキャンできないファイルのうち、組織内で日常的に使用されていないものはブロックすることをお勧めします。
- 推奨されるマルウェア対策ポリシーに従います。

高度な脅威対策(ATP)ポリシー：

- ATPポリシーを設定して、詐欺、ボットネット アクティビティー、不正な通信、クロスサイト スクリプティング(XSS)、コマンド＆コントロール トラフィック、ToRやBitTorrentなどの危険なアプリケーション、フィッシング サイト、疑わしい宛先(国)、その他の悪意のあるオブジェクトやスクリプトから組織を保護します。
- ページ リスク設定 – これは不審なコンテンツの保護(ページ リスク指数)の値であり、すべてのWebページに対してリアルタイムで動的に計算されます。その後、このスコアは設定した値と照らし合わせて評価されます。推奨設定は35です。組織のリスク回避の度合いに基づいて、異なる値に設定できます。値が大きいほどリスクが高くなります。

- セキュリティ例外 – [これらのURLからコンテンツをスキャンしない]の設定を使用し、組織の公開サイトや、ウイルス対策、スパイウェア対策、マルウェア対策のポリシーが原因で失敗している可能性がある他の信頼済みサイトなど、スキャンしないサイトのURLを追加できます。このサービスにより、ユーザーはトラフィックを検査することなく、これらのURLからコンテンツをダウンロードできます。詳細については、次のページを参照してください：**https://help.zscaler.com/zia/adding-urls-allowlist**
- **推奨される高度な脅威対策ポリシー**に従います。

ブラウザー コントロール ポリシー：

- ブラウザーの脆弱性保護 – ブラウザー コントロール ポリシーを設定し、ユーザーが古いブラウザーや脆弱なブラウザー、プラグイン、アプリケーションを使用している場合、インターネットに出ないように警告します。
- ブラウザーのブロック – 古い脆弱なブラウザーが使用されるリスクを軽減するために、古いバージョンのブラウザーの使用をブロックすることをお勧めします。

ファイル タイプ制御ポリシー：

- ファイル タイプ制御ポリシーを設定し、未分類のWebサイトからの実行可能ファイルのダウンロードのブロック、任意のURLカテゴリーからのダウンロードに対する警告、任意のURLカテゴリーへの実行可能ファイルのアップロードのブロック、検出不可能なファイル タイプのブロックを行います。
- **推奨されるファイル タイプ制御ポリシー**に従います。

情報漏洩防止(DLP):

- DLPポリシーを設定し、Webメール、クラウド ストレージ、ソーシャル メディア、その他のさまざまなアプリケーションから漏洩する可能性のあるデータ損失から組織を保護します。

ファイアウォール制御ポリシー：

- ファイアウォールのフィルタリング ポリシーを設定し、特定の送信元からの、また特定の宛先へのどのタイプのトラフィックが許可されるかを定義します。デフォルトでは、Zscalerファイアウォールは、ネットワークからインターネットへのすべての非HTTP/HTTPSトラフィックを許可します。
- DNS、HTTP、HTTPSなど、必要な特定のサービスのみを許可し、それ以外はすべてブロックします。
- SSH、TFTPなど、環境内で使用されていないプロトコルをブロックします。
- POP3、IRC、Telnet、FTPなど、安全でないプロトコルをブロックします。
- 推奨されるファイアウォール管理ポリシーに従います。

侵入防止システム(IPS)制御：

- IPS (非Web)は、シグネチャーベースの検出を使用し、信頼性の高いエンジンによってすべてのポートとプロトコルのトラフィックを制御し、侵入から保護します。
- IPSのデフォルトのロギングは集約に設定されており、ユーザー、ルール、ネットワーク サービスに基づいて個々のセッションをグループ化し、定期的に記録します。
- ルールのすべてのセッションを個別にログに記録する完全なロギングが必要な場合は、デフォルトのIPSポリシーを編集し、**[ロギング]**で**集約**を選択して有効にします。
- IPSポリシーを設定したら、ファイアウォールを有効にする際にロケーションごとに**[IPSコントロールを有効化]**できます。
- **推奨されるIPS管理ポリシー**に従います。

URLフィルタリングとクラウド アプリの制御ポリシー：

- URLフィルタリングを設定し、サイトのカテゴリーに基づいてWebコンテンツへのアクセスを管理することで、法的責任を制限できます。
- クラウド アプリのコントロールを設定し、インスタント メッセージング(Google Hangouts、チャット、ファイル転送など)、ソーシャル ネットワーキング(Facebookの表示と投稿など)、ストリーミング メディア(YouTubeの視聴/再生、アップロードなど)、Webメール(Yahoo!メールの表示、送信、添付ファイルの送信など)など、認可されたクラウド アプリケーションと関連するアクティビティーのみにアクセスできるようきめ細かく制御します。
- デフォルトでは、クラウド アプリの制御はURLフィルタリング ポリシーよりも優先されます。この動作を変更し、クラウド アプリの制御ポリシーを既に適用している場合でもURLフィルタリング ポリシーを適用するには、**[管理] > [高度な設定]**で**[URLフィルターまでのカスケードを許可]**を有効にします。
- [新しく登録されたドメイン]の検索設定を有効にして、URLフィルタリング ポリシーで使用します。
- URLフィルタリング ポリシーを設定し、未分類のURL、新規に登録されたドメイン、未分類/不明のカテゴリーにアクセスしたときにユーザーに警告します。
- **推奨されるURLとクラウド アプリ管理ポリシー**に従います。

SSLインスペクション：

- 暗号化されたトラフィック内にマルウェアが潜むことが多くなっているため、考えられるすべてのトラフィックに対してSSL復号とインスペクションを有効にすることをお勧めします。
- 以下を含む[SSLを検査しない]リストを定義します。
  i. 顧客または地方自治体のコンプライアンス要件に準拠
  ii. クライアント証明書による認証が必要なサイト
  iii. 証明書ピンニングを行うサイト
  iv. IDP URL (Okta、Azure ADなど)
- 次の手順に従い、ロケーション設定からSSLインスペクションを有効にします：**ZIA Admin Portal > [管理] > [ロケーション管理]**> ([ロケーションのポリシー]) **> [SSLインスペクションを有効化]**。
- 次の手順に従い、SSLインスペクションの設定で、モバイル ユーザーのクライアントのSSLインスペクションを有効にします：**ZIA Admin Portal > [ポリシー] > [SSLインスペクション] > [Zscaler Client Connectorのポリシー]** セクション。
- SSLインスペクションが無効の場合、[SSLインスペクションが無効の場合、これらのサイトへのHTTPをブロック]の設定を使用して、リスクの高いURLカテゴリーへのHTTPSをブロックします。
- [復号できないトラフィックをブロック]の設定を有効にすることをお勧めします。
- SSLインスペクションの詳細については、**こちらの記事**を参照してください。

サンドボックス ポリシー：

- サンドボックス ポリシーを設定することで、不明なファイルを検査し、未知の脅威やゼロデイ脅威をブロックします。
- リスク許容度とパフォーマンス要件に応じて、[検疫]または[許可してスキャン]のポリシー アクションを使用できます。
- ヌード、ポルノ、アノニマイザー、未分類、不明のカテゴリーなど、リスクの高いカテゴリーからダウンロードされた実行可能ファイルとOfficeドキュメントに対して、検疫アクションを設定することをお勧めします。

- 他のすべてのファイル タイプに対しては、[許可してスキャン]を設定し、その後**[ペイシェントゼロ アラート]**を設定することをお勧めします。
- **Sandboxポリシー**に従います。

ZIA Admin Portal > [管理] > [高度な設定]ページから、**RFC違反のHTTP トラフィックをブロック**します。

既定以外のポートを使用している場合、**ZIA Admin Portal > [管理] > [高度な設定]**ページから、HTTP/HTTPS/FTP/DNS/RTSP/PPTPの**自動プロキシー転送を有効化します。**

セキュリティ ログ分析のベスト プラクティス

ZIAダッシュボード、解析、ログ：

1. **ダッシュボード**には、ほぼリアルタイムのデータが表示されます。脅威のイベントを監視する場所として、まずセキュリティ **ダッシュボード**を使用し、グラフをロールオーバーして詳細情報を取得し、イベントが発生した場合は、そのイベントをクリックして、イベントから直接ログまたは解析情報にピボットできます。

2. **[ロールベースの管理]**を使用して管理者ロールを定義し、許可されたユーザーのみが**[表示のみ]**や**[フルアクセス]**などの適切なレベルでダッシュボードにアクセスできるようにします。

3. **ダッシュボードのカスタマイズ**：ウィジェットの追加、編集、削除により、ダッシュボードをカスタマイズして関心のあるイベントを表示できます。**[脅威のカテゴリー]** カスタム ダッシュボードを追加すると、組織のすべてのさまざまな脅威カテゴリーのイベントをすばやく表示できます。フィッシング イベントなどの特定の脅威カテゴリーについては、[高度な脅威のスーパー カテゴリー] データ タイプの [フィッシング] フィルターを使用して、以下の表に示すようにカスタマイズされたウィジェットを作成できます。

デフォルトのダッシュボードを編集し、追加したいフィルターを含めることもできます。たとえば、ロケーション固有のイベントを表示する場合は[ロケーション]を追加し、HTTP、HTTPS、SSLを使用するステルス型脅威を探す場合は[プロトコル]をフィルターとして使用します。

4. **ダッシュボードの更新**：ダッシュボードは15分ごとに自動的に更新されるように設定することをお勧めします。これにより、セッションがタイムアウトするのを防ぐとともに、ウィンドウ内の情報を最新の状態に保つことができます。**[管理] > [プロフィール]**に移動して、自動更新を有効にします。

5. ウィジェットをダッシュボードに追加するには、**[ウィジェットを追加]**アイコンをクリックします。Web、モバイル、ファイアウォール、DNSイベント用のウィジェットを追加できます。ダッシュボードには、最大12個のウィジェットを含めることができます。

6. [解析]ページと[ログ] ページでは、70以上のフィールドにわたる脅威の豊富なコンテキストを含むNanologデータにアクセスできます。ベスト プラクティスとして、ダッシュボードのイベントから始めて、ログにピボットし、フィルターを使用して検索を絞り込むか、[解析]タブの[解析]セクションから直接アクセスし、ログをクリックします。

7. 解析ログで使用できるフィルターは多数ありますが、一般に、以下の主要なフィルターを1つ以上設定し、ユーザーやロケーションなどの他のフィルターを加えて、検索をさらに絞り込むことがベスト プラクティスです。

Web解析ログのフィルター：

Web解析ログのフィルター	用途
高度な脅威のスーパー カテゴリー	このフィルターを使用することで、データをアドウェア/スパイウェア サイト、ブラウザー エクスプロイト、クロスサイト スクリプティング、クリプトマイニング＆ブロックチェーン、フィッシングなど、特定の高度な脅威カテゴリーに絞り込めます。
ポリシー タイプとルール名	このフィルターを使用することで、指定されたポリシー タイプと設定されたルール名に一致するトランザクションを表示します。
サンドボックス	このフィルターを使用することで、サンドボックスの結果(サンドボックス アドウェア、サンドボックス アノニマイザー、サンドボックス無害、サンドボックス マルウェア、分析のために送信)に基づいてファイルのダウンロードを表示します。
脅威のカテゴリー	このフィルターを使用することで、データをエクスプロイト、プロキシー、ランサムウェア、トロイの木馬、ワームなど特定の脅威カテゴリーに絞り込めます。
脅威のスーパー カテゴリー	このフィルターを使用することで、データをマルウェアやウイルスなど特定の脅威のスーパー カテゴリーに絞り込めます。
脅威のクラス	このフィルターを使用することで、高度な脅威、ウイルス/スパイウェアなどの特定の脅威クラスに関連付けられているトランザクションを検索できます。
脅威の名前	このフィルターを使用することで、特に関心のある特定の脅威に関連付けられているトランザクションを探せます。
スキャンできないタイプ	このフィルターを使用することで、暗号化されたファイル、検出できないファイル、スキャンできないファイルなどの理由によるファイル スキャンの失敗を探せます。
URLカテゴリー	このフィルターを使用することで、データを特定のURLカテゴリーに絞り込めます。特定のカテゴリーを含めるか除外するかを選択できます。
プロトコル	このフィルターを使用することで、HTTP、HTTPS、SSLを使用するステルス脅威を検索できます。

その他のデータ タイプとフィルターについては、次のページを参照してください：
https://help.zscaler.com/zia/web-data-types-and-filters

モバイル解析ログのフィルター：

モバイル解析ログのフィルター	用途
モバイル アプリケーションのカテゴリー	このフィルターを使用することで、データをマルウェア アプリ、SNS、ストリーミング メディア、脆弱なアプリなど特定のモバイル アプリケーション カテゴリーに絞り込めます。
モバイル デバイス タイプ	このフィルターを使用することで、データをApple iPad、Google Android、Samsung Galaxy S、Windows Mobileなど特定タイプのモバイル デバイスに関連付けられたトラフィックに絞り込めます。
プロトコル	このフィルターを使用することで、データをHTTP、HTTPS、SSLなどモバイル トラフィックのプロトコルへのトラフィックに絞り込めます。

その他のデータ タイプとフィルターについては、次のページを参照してください：
https://help.zscaler.com/zia/mobile-data-types-and-filters

ファイアウォール解析ログのフィルター：

ファイアウォール解析ログのフィルター	用途
クライアントIP/ポート	このフィルターを使用することで、表示を特定のクライアントの送信元/宛先IPアドレスまたはポートに絞り込めます。
クライアント トンネルIP	このフィルターを使用することで、表示を特定のクライアントのトンネルIPアドレスに絞り込めます。
サーバー IP/ポート	このフィルターを使用することで、表示を特定のサーバーの送信元/宛先IPアドレスまたはポートに絞り込めます。

その他のデータ タイプとフィルターについては、次のページを参照してください：
https://help.zscaler.com/zia/firewall-data-types-and-filters

DNS解析ログのフィルター：

DNS解析ログのフィルター	用途
DNSリクエスト タイプ	このフィルターを使用することで、データを特定のタイプのDNSリクエストに関連付けられたトラフィックに絞り込めます。
DNSレスポンス	このフィルターを使用することで、データをDNSエラー コードを含む、特定のDNSレスポンスに関連付けられたトラフィックに絞り込めます。
IPドメイン カテゴリー	このフィルターを使用することで、データを要求されたドメインのURLカテゴリーに関連付けられたトラフィックに絞り込めます。
リクエストされたドメイン	このフィルターを使用することで、データをDNS解決が要求されたドメインに関連付けられたトラフィックに絞り込めます。
サーバー IP/ポート	このフィルターを使用することで、データを特定のサーバー IPアドレスまたはサーバー ポートに関連付けられたトラフィックに絞り込めます。

その他のデータ タイプとフィルターについては、次のページを参照してください：
https://help.zscaler.com/zia/dns-data-types-and-filters

トンネル解析ログのフィルター：

トンネル解析ログのフィルター	用途
トンネル ソース/宛先IP	このフィルターを使用することで、特定の送信元/宛先IPアドレスに関連付けられたメトリックを表示できます。
トンネル タイプ	このフィルターを使用することで、GREやIPSecなどさまざまなタイプのトンネルに基づいてメトリックを表示できます。

その他のデータ タイプとフィルターについては、次のページを参照してください：
https://help.zscaler.com/zia/tunnel-data-types-and-filters

SaaSセキュリティ分析ログのフィルター：

SaaS セキュリティ分析ログのフィルター	用途
アプリケーション カテゴリー	このフィルターを使用することで、データをCRM、メール、ファイル、リポジトリーなど特定のSaaSアプリケーション カテゴリーに絞り込めます。
アプリケーション	このフィルターを使用することで、データをBox、Dropbox、Google Drive、OneDrive、ShareFile、SharePointなど特定のSaaSアプリケーションに絞り込めます。
DLP辞書	このフィルターを使用することで、クレジット カード、社会保障番号、Salesforce.comデータなどのイベントをトリガーした辞書を表示できます。
DLPエンジン	このフィルターを使用することで、クレジット カード番号、HIPAA、PCI、社会保障番号などの特定のDLPエンジンに関連付けられているスキャンを表示できます。
インシデント タイプ	このフィルターを使用することで、DLPやマルウェア検出などの特定のインシデント タイプに関連付けられているスキャンを表示できます。
テナント	このフィルターを使用することで、特定のテナントに関連付けられているスキャンを表示できます。
脅威のカテゴリー	このフィルターを使用することで、特定の脅威カテゴリーに関連付けられているスキャンを表示できます。これらの脅威は、マルウェア対策によって検出されます。
脅威のスーパー カテゴリー	このフィルターを使用することで、高度な脅威、マルウェア検出、サンドボックス、スパイウェア、ウイルスなど、特定の脅威のスーパー カテゴリーに関連付けられているスキャンを表示できます。

その他のデータ タイプとフィルターについては、次のページを参照してください：
https://help.zscaler.com/zia/saas-security-insights

NSSのベスト プラクティス

1. AWSまたはAzure上にNSSを導入し、ZscalerクラウドからSIEMへのシームレスなクラウド統合を実現します。
2. NSS Webログのデフォルトのフィード出力形式には、30を超えるフィールドが含まれています。**NSSのフィードの出力形式：Webログ**の手順に従い、さらにフィールドを追加できます。
3. 一般に、syslogメッセージのサイズ制限に対応するために、NSSフィードに含めるフィールドは50以下にすることをお勧めします。ただし、SIEMでより大きなメッセージ サイズを取り込むことができる場合は、50以上に設定できます。

セキュリティ ログ レポートのベスト プラクティス

1. ロールベースの管理を使用して、承認された管理者のみがレポートの作成を許可されるようにします。
2. **[セキュリティ ポリシー監査レポート]**を実行し、すべての推奨設定に従っていることを確認します。
3. **[対話型レポート] > [標準レポート] > [セキュリティの脅威]**セクションから[高度な脅威を検知したユーザー] レポートを定期的に実行して危険なユーザーを特定し、Web解析またはSIEMを使用してそれらの特定のユーザーについてさらに調査します。
4. **[対話型レポート] > [標準レポート] > [セキュリティの脅威]**セクションから[上位の脅威名]レポートを定期的に実行して、フィッシング キャンペーンの開始やコマンド＆コントロール/ボットネット アクティビティーなど、Webおよび非Webの脅威の傾向を特定し、ログにピボットしてWeb解析またはSIEMを使用してさらに調査します。
5. **[対話型レポート] > [標準レポート] > [セキュア ブラウズ]** セクションの[プロトコルごとのトラフィック分布]レポートを定期的に実行して、暗号化されたプロトコルと暗号化されていないプロトコルの脅威の傾向を特定します。たとえば、[SSL]でブロックされる脅威が増えた場合は、SSL復号ポリシーを見直して、より多くのトラフィックをSSLインスペクションの対象に含めます。
6. **[対話型レポート] > [標準レポート] > [ファイアウォール アクティビティー]** セクションから[ファイアウォール アプリケーション/サービス概要]レポートを定期的に実行して、疑わしい異常なアプリケーションやトラフィック量を見つけ、Web解析またはSIEMを使用してさらに調査します。
7. 以下の目的で、**[企業リスク スコア]**レポートを毎日実行します。
   - 組織の全体的なセキュリティ リスク エクスポージャー スコア、リスク スコアの傾向、同じ業界の他の企業および全体的なクラウド顧客と比較したリスク スコアを理解するため。
   - ボットネット アクティビティー、悪意のあるコンテンツ、フィッシングなど、リスク スコアに影響したイベントを特定するため。
   - リスク スコアに最も影響した上位1%のリスク ユーザーを含む、リスクの非常に高いユーザーとその行動、リスク スコアへの影響後を特定するため。
     - » このレポートを定期的に実行して、最もリスクの高いユーザー/ロケーションを見つけ、Web解析ログまたはSIEMにピボットして、そのユーザーについてさらに調査を行うことが有効です。
8. 以下の目的で、**[異常検知レポート]**を毎日実行します。
   - 組織の異常なユーザー アクティビティーの概要と脅威のアクティビティーを理解するため。
   - 潜在的なデータ流出イベント、悪意のあるインサイダー アクティビティー、不審なアクティビティーを検出するため。

- 関連付けられたファイルのアップロード/ダウンロードの傾向、認可されたアプリケーションと認可されていないアプリケーションの使用、ログイン試行の不可能な移動シナリオ、データ漏洩の試みなど、異常なユーザー行動を特定するため。
- クラウド アプリケーションを使用する際のアップロードやダウンロードのトラフィック パターンの異常など、組織レベルの異常なアクティビティーを特定するため。
- アプリケーションへのアクセスや使用パターンが類似しているグループ内のユーザーと比較して、これらの異常な動作に影響した上位ユーザーを特定するため。
  - » このレポートを定期的に実行して、最もリスクの高いユーザー/ロケーションを見つけ、Web解析ログまたはSIEMにピボットして、そのユーザーについてさらに調査を行うことが有効です。

9. カスタム レポートを使用して、確認したいイベントを表示します。多くのお客様にとって関連性が高い週次レポートには、次のようなものがあります。

- ファイル アップロード レポート：過去1週間にファイルをアップロードしたユーザー、アップロード先のサイト、ファイル名/種類が一覧表示されます。
- 実行可能ファイルのダウンロード レポート：過去1週間に実行可能ファイルまたはスクリプト ファイルをダウンロードしたユーザー、ダウンロードしたサイト、ファイル名/種類が一覧表示されます。
- 例:**[対話型レポート] > [カスタム レポート] > [新規レポート]> [Web]**を選択し、**[ファイル共有アクティビティー]** フィルターを追加した後、**[アップロード] / [表示] / [すべて]**のフィルターを追加し、ユーザーなどその他のフィルターを追加し、**ウィジェット**を追加します。

10. **[サンドボックスの悪意のあるファイル]** レポートを毎週実行し、分析のためにサンドボックスに送信され、悪意があることが判明した不明なファイルをハイライト表示します。

セキュリティ運用におけるインシデントへの対応のベスト プラクティス

1. **ボットネット アクティビティーの検出：**

- セキュリティ ダッシュボードの**[高度な脅威]**ウィジェットで**[ボットネット コールバック]** カテゴリーを探し、[ログを表示]をクリックします。
- Webログ フィールドの**[reason]**またはWeb解析フィールドの**[ポリシー アクション]**で、[IPS block inbound response: botnet command-and-control traffic]または[IPS block outbound request: botnet command-and-control traffic]を検索して信頼度の高いコンテンツ ブロックを探します。
- 信頼度の低いブロック(レピュテーションベース)については、Webログ フィールドの**[reason]**またはWeb解析フィールドの**[ポリシー アクション]**で[Reputation block outbound request: botnet site]を検索します。**ポリシーの理由の文字列に関する記事**も併せて参照してください。
- [ボットネット コールバック] アラートを設定し、ボットネット コールバックのアクティビティーが検出されたときに電子メールを受信するようにします。

  注：宛先IP、ドメイン、URLに基づくレピュテーション ブロックは、特定のサイトのレピュテーションの変更が遅れることがあるため、誤検出の可能性が高くなります。

2. **フィッシング アクティビティーの検出：**

- セキュリティ ダッシュボードの**[高度な脅威]**ウィジェットで**[フィッシング]**カテゴリーを探し、[ログを表示]をクリックします。
- **[高度な脅威のユーザー/ロケーションのトップ]** ウィジェットを使用して、最もフィッシングなどの高度な脅威の標的にされているユーザーを確認します。

- また、[データ タイプ]として[ユーザー]を選択し、[高度な脅威(スーパー カテゴリー)]フィルターで[フィッシング]を選択することで、フィッシングの標的となっている上位のユーザーを表示するカスタム ダッシュボード ウィジェットを作成することもできます。
- Webログから、高度な脅威対策のログで[フィッシング]または[Webスパム]のURLカテゴリーを検索します。
- Webログ フィールドの[reason]またはWeb解析フィールドの[ポリシー アクション]で[IPS block inbound response: phishing content]を検索して、信頼度の高いコンテンツ ブロックを探します。
- Webログ フィールドの**[reason]**またはWeb解析フィールドの**[ポリシー アクション]**で、[Reputation block outbound request: phishing site]を使用してレピュテーションベースのブロックを探します。
- また、フィッシングの**アラート**を設定することで、フィッシング アクティビティーが検出され、5分以内に100回発生するなど一定のしきい値に達した場合に、電子メールを受信するようにできます。

3. **不審なアウトバウンド接続の検出：**

- [ファイアウォールの概要]ダッシュボードで、[ネットワーク サービス]のカスタム ダッシュボード ウィジェットを作成し、SSHなどの不審なサービスが使用されていないか確認します。
- ファイアウォールのログ/解析で、SSHなどの通常とは異なるネットワーク アプリケーションやネットワーク サービスが使用されていないか検索します。
- ファイアウォールのログの[nwapp]または[nwsvc]フィールドで、通常とは異なるアプリケーション/サービスを検索します。
- Webログの高度な脅威対策のログで、[不審な宛先]のURLカテゴリーを検索します。

4. **データ流出アクティビティーの検出：**

- 代替プロトコルを介した流出 – FTP、SMTP、DNS、SMBなどの代替プロトコルで交換されるデータ量が異常に多いかどうかを確認します。
- HTTP/Sを介した流出 – 交換されるデータ量が異常に多いかどうかを確認します。
- クライアントがサーバーよりもはるかに多くのデータを送信している、クライアントが長い接続を維持し、一定サイズのデータ パケットを一貫して、または一定の間隔で送信しているなど、通常とは異なるデータ フローがないか探します。
- 暗号化されたアーカイブを介した不審なデータ転送がないか探します。
- ファイアウォールのログ/解析で、大量のデータ転送/異常なボリュームについて、FTP、DNS、SMTP、SMBなどの通常とは異なるネットワーク アプリケーションやネットワーク サービスが使用されていないか検索します。
- Webログから、高度な脅威対策のログでFTP、DNS、SMTP、SMBなどのプロトコルと不審な宛先URLのカテゴリーを検索します。
- DLPポリシーを設定し、クレジット カード番号などの機密データの交換をブロックします。

5. **潜在的に望ましくないアプリケーションの使用の検出 – Tor、プロキシー、アノニマイザー、P2Pアプリ**

- セキュリティ ダッシュボードの**[高度な脅威]**ウィジェットで、[P2P]または[不正な通信]カテゴリーを探して、[ログを表示]をクリックします。
- **[高度な脅威のユーザー/ロケーションのトップ]** ウィジェットを使用して、Torや不正な通信などのP2Pアノニマイザー アプリケーションを使用する上位の脅威ユーザーを確認します。
- [データ タイプ]として[ユーザー]を選択し、[高度な脅威のスーパー カテゴリー] フィルターで[P2P]または[不正な通信]を選択することで、P2Pアプリケーションまたは不正な通信を使用する上位ユーザーを表示するカスタム ダッシュボード ウィジェットを作成することもできます。

- Webログから、高度な脅威対策のログで[P2P]または[不正な通信]のURLカテゴリーを検索します。
- Torトラフィックが環境で使用するアプリとして認可されていない場合、高度な脅威対策ポリシーでそのトラフィックをブロックするように設定します。

6. **悪意のあるトンネリング アクティビティーの検出 – IRCトンネリング、SSHトンネリング、DNSトンネリング**

   - Webログ フィールドの**[reason]**またはWeb解析フィールドの**[ポリシー アクション]**で、[IPS block inbound response. IRC use/tunneling]、[IPS block outbound request. IRC use/tunneling]または[IPS block: SSH use/tunneling]を検索して、信頼度の高いコンテンツ ブロックを探します。
   - **DNS概要**ダッシュボードで[DNSトンネル] カテゴリーを探し、[ログを表示]をクリックします。
   - DNSトンネル検出の詳細については、次のページを参照してください：
     https://help.zscaler.com/zia/about-dns-tunnel-detection

7. **悪意のあるドメイン フロンティング アクティビティーの検出：**

   - すべてのトラフィックでTLSインスペクションが有効になっていることを確認します。
   - NSSフィード形式にWebログの[df_hostname]フィールドを追加します。
   - このフィールドの値を検索して実際の[host]フィールドの値と比較し、不一致がないか確認します。
   - [host] (HTTPホスト ヘッダー)と[df_hostname] (SNI)の間で大文字と小文字を区別しない比較を実行するアラートをSIEMで作成し、df_hostnameに基づいて結果を集計してアラートの数を減らします。

     注：ドメイン フロンティングは正当な目的にも使用できます。まず、推奨されるアラートの結果を調査し、誤検出を減らすために検索を最適化する必要があります。

8. **マルウェア アクティビティーの検出：**

   - セキュリティ ダッシュボードの**[ウィルス/スパイウェア]**カテゴリーから開始し、[ログを表示]をクリックします。
   - **[ウィルス/スパイウェアを検知したユーザー/ロケーションのトップ]**ウィジェットを使用して、どのユーザーが最もマルウェアの標的にされているかを確認します。
   - Webログ フィールドの**[reason]**またはWeb解析フィールドの**[ポリシー アクション]**で[Malware block: malicious file]を検索します。
   - Webログ フィールドの**[reason]**またはWeb解析フィールドの**[ポリシー アクション]**で、[Reputation block outbound request malicious URL]を使用して、レピュテーションベースのコンテンツ ブロックを探します。
   - ブロックが報告された時間帯のユーザー アクティビティーとログを調べて、成功した可能性のある不審なアクティビティーが他にあったかどうかを確認します。

9. **使用中の安全でないプロトコルの検出：**

   - ファイアウォールの概要ダッシュボードから開始して、HTTP、FTPなど、使用率上位の安全でないアプリケーションが使用されていないか確認します。
   - ファイアウォール解析の[ネットワーク サービス]フィルターまたはファイアウォール ログの[nwapp]または[nwsvc]フィールドで、FTP、HTTP、IMAP、IRC、TELNET、POP3などの安全でない/暗号化されていないプロトコルが使用されていないか検索します。
   - **[対話型レポート] > [標準レポート] > [セキュア ブラウズ]**セクションから、[プロトコルごとのトラフィック分布]レポートを定期的に実行し、暗号化されたプロトコルと暗号化されていないプロトコルの脅威の傾向を把握します。

10. **Zscaler脅威ライブラリーを使用して脅威名をドリル ダウン**

11. **サンドボックス アクティビティー – 不明なファイル：**

    - Webログの[malwarecat]フィールドで[Sent for Analysis]を探します。Basic Sandboxのお客様に対しても、サンドボックス分析のためにファイルのサブセットが送信されます。
    - 評決を表示するには、Zscalerの[Web解析]ログ ビューにピボットしてMD5ハッシュを検索するか、**サンドボックス レポート ダッシュボード**を活用する必要があります。
    - **サンドボックス レポートAPI**を使用して、MD5ハッシュによってサンドボックス分析ファイルの詳細を取得することもできます。

12. **サンドボックス アクティビティー – 悪意のあるファイルを検出：**

    - **[サンドボックスの悪意のあるファイル]**レポートを毎週実行します。このレポートを実行するには、次のように操作します。
      ZIA Admin Portal > [解析] > [サンドボックス アクティビティー レポート]ドロップダウンから**[サンドボックスの悪意のあるファイル]**を選択します。
    - SOAR/IRワークフローを使用し、EDRを介してMD5をスキャンし、このマルウェアの存在と誰が以前にダウンロードしたかを確認します。
    - **ペイシェントゼロ アラート** – 高精度のペイシェントゼロのメール アラートに対応する自動IRワークフローを設定します(**ヘルプ記事**を参照)。

13. **サンドボックス アクティビティー – 既知の悪意のあるファイル**

    - Webログの[malwarecat]フィールドで、[Sandbox Malware]または[Sandbox Adware]または[Sandbox Anonymizer]を探します。Zscalerのお客様から分析用に以前送られたファイルが悪意のあるものと判断された場合、このWebログのフィールドにサンドボックスの評決が表示されます。
    - 分析用に送られ、既知のレピュテーションがないファイル、または当社のアンチウイルス エンジンのいずれによってもブロックされていないファイルは、リスクが高いものと見なされる可能性があります。
    - **サンドボックス詳細レポートAPI**からIOCを抽出することもできます。

14. 脅威解析の地球儀からSIEMにピボットします。お客様によっては、Zscaler脅威解析の地球儀をSOCの大画面に表示している場合があります。これは24時間ごとに更新されるので、環境内のアクティブな脅威のおおまかな状況を把握するのに便利です。詳細については、次のページを参照してください：
    https://help.zscaler.com/zia/about-threat-insights

15. 遡及的な脅威の検出 – セキュリティ ブロック(レピュテーション、アンチウイルス エンジン、高度な脅威)を検出した際、MD5ハッシュ/ドメイン/URL/IP指標の最初の検出を数日(または数か月)振り返って、ペイシェントゼロ イベントと脅威がネットワークに残っている可能性のある期間を特定すると有効です。

16. セキュリティ ブロック(レピュテーション、アンチウイルス エンジン、高度な脅威)を検出するたびに、ブロックが報告された時間帯のユーザー トラフィック アクティビティーとログを調べて、成功した他の悪意のあるアクティビティーがあったかどうかを確認すると有効です。

Zscalerアラートのサブスクリプションのベスト プラクティス

1. ベスト プラクティスとして、次のような高リスクのセキュリティ アクティビティーに対してメールを受信するようにアラートを設定します。
   - ボットネット コールバックとしきい値
   - マルウェア/スパイウェア/ウイルスの受信
   - フィッシングとしきい値
   - サンドボックス アドウェア、アノニマイザー、マルウェアとしきい値
   - 不審な宛先
   - ペイシェントゼロ アラート
2. 最大128件のアラートを作成できます。
3. アラートを定義したら、[アラートの発行]を使用してアラートの登録を行い、アラートのカテゴリーと重大度に基づいてさまざまな受信者にメールを送信できます。

まとめ

Zscalerの独自のアーキテクチャーは、包括的なカバレッジと拡張性でお客様を保護し、多層防御型アプローチを可能にします。

SOC部門がセキュリティ上の脅威を特定、分離し、これに対応するためには、ユーザー トラフィックとセキュリティ アクティビティーの可視化が重要です。Zscaler Nanologサービスは、世界中のすべてのユーザー、ロケーション、デバイスの脅威ログをお客様が決める中央リポジトリーに統合し、管理者がユーザー、デバイス、アプリケーション、ロケーションごとにトランザクション データをリアルタイムで表示し取り出すことのできる機能です。Zscaler Nanologは、豊富な脅威のコンテキストと、イベントの分類と脅威ハンティングに役立つその他の情報を含む圧縮形式の詳細な記録です。

これらのログは、ダッシュボード、解析、レポートなどの解析機能を強化し、ユーザーと脅威のアクティビティーをリアルタイムで可視化します。また、Zscalerは、NSS (Nanolog Streaming Service)を利用してこのログをオンプレミスまたはクラウドのSIEMにほぼリアルタイムで転送する機能にも対応しており、リアルタイムのアラート、ファイアウォールや他のデバイスのログとの関連付け、ローカルのログの長期的なアーカイブが可能です。

さらに、この記事で紹介しているベスト プラクティスは、提供される機能を最大限に活用し、より迅速に脅威を特定して対応するために役立ちます。

付録A – 脅威検出のユース ケースと例

フィッシング攻撃

フィッシングは通常、偽装されカスタマイズされたメッセージを使って、あたかも本物のビジネス目的のようにユーザーを誘い、機密情報を提供するように仕向けます。このようなメッセージには、悪意のあるリンクや添付ファイルが含まれています。フィッシングは、スピアフィッシングと呼ばれる標的型攻撃で行われることがあります。スピアフィッシングでは、特定の個人、企業、業界が攻撃者の標的になります。

MITRE ATT&CKに関連する戦術、テクニック、サブテクニック

初期アクセス >	
フィッシング(3) >	添付ファイル型スピアフィッシング >
	リンク型スピアフィッシング >
	サービス経由のスピアフィッシング >

Zscaler検出エンジン

フィッシング攻撃の検出に役立つZscalerセキュリティ ログは以下のとおりです。

- 高度な脅威対策：フィッシングWebサイト/ドメイン/IP検出のレピュテーションに基づく
- サンドボックス：不明な添付ファイル

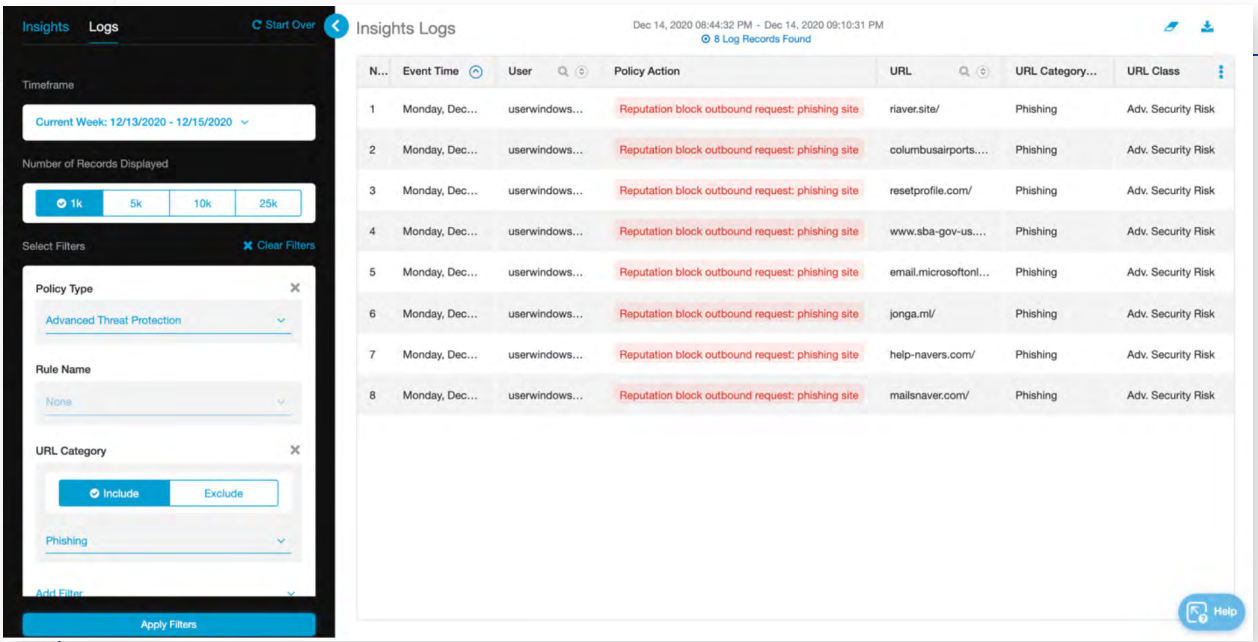
調査

Web解析の使用

解析ログをフィルタリングしてフィッシングの試みを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

Policy Type="Advanced Threat Protection", **URL Category**="WebSpam"
Policy Type="Advanced Threat Protection", **URL Category**="Phishing", **URL Class**="Advanced Security Risk"

フィッシングの試みに関するWeb解析の検索例

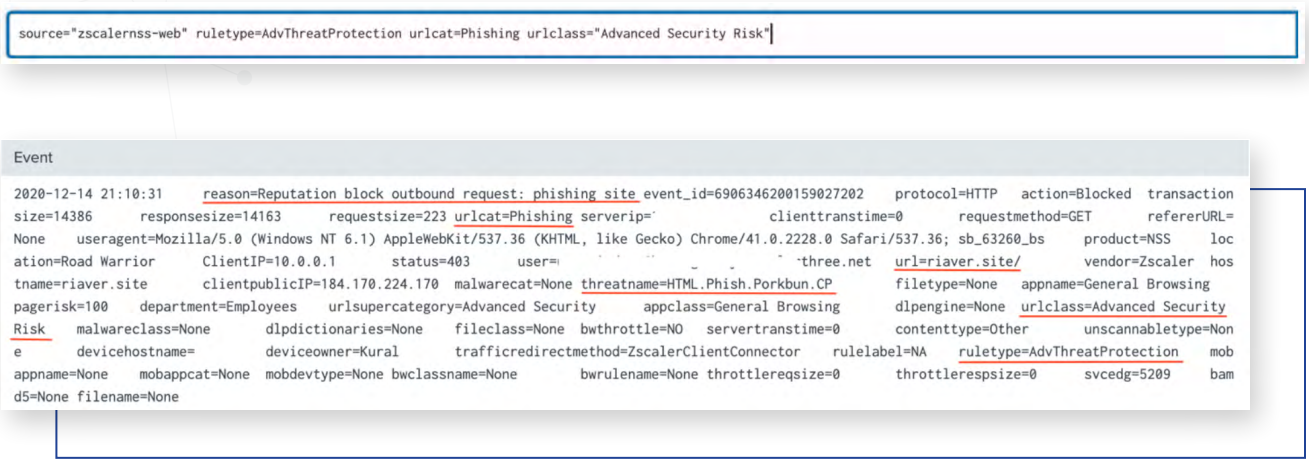


NSS Webログの使用

NSS Webログを詳細に分析してフィッシングの試みを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

ruleType="AdvThreatProtection", **urlCat**="WebSpam"
ruleType="AdvThreatProtection", **urlCat**="Phishing", **urlclass**="Advanced Security Risk"

フィッシングの試みに関するNSS Webログの検索例



推奨される防止/軽減策

インシデント前：

- アンチスパムのフィルタリング
- フィッシング対策の定期的なチェック
- フィッシング セキュリティの定期的な啓発(ネット上での成功事例と活動事例の監査に基づく)
- インシデント対応部門のトレーニングとケースへの対応準備(ケース、プロセス、参加すべきユーザーの把握)
- 不審なURLカテゴリーやページ リスクの高いURLへのWebトラフィックの制限
- アンチウイルス/アンチマルウェア

インシデント後：

- アラート レベルのアップグレード
- 影響を受けた/調整されたユーザーへの通知
- アンチウイルスの実行

予防保守：

この手順には、既存システムの定期的な保守と更新、ファイアウォール ポリシーの更新、脆弱な部分へのパッチ適用、アプリケーションのホワイトリスト登録、ブラックリスト登録、保護など、攻撃の成功をより困難にするために行うすべてのアクションが含まれます。

マルウェアの検出

ボットネットとコマンド＆コントロール トラフィック

説明

コマンド＆コントロールは、攻撃者が被害者のネットワーク内の制御下にあるシステムと遠隔通信するために使用する戦術であり、さまざまなレベルのステルスで制御を確立するために多くの手法を使用する場合があります。攻撃者は通常、検出を回避するために、通常予想されるトラフィックを模倣しようとします。

MITRE ATT&CKに関連する戦術、テクニック、サブテクニック

コマンド＆コントロール >	
アプリケーション層プロトコル(4) >	Webプロトコル >
	ファイル転送プロトコル >
	メール プロトコル >
	DNS >
リムーバブル メディア経由の通信 >	
データ エンコーディング(2) >	標準エンコーディング >
	非標準エンコーディング >
データ難読化(3) >	ジャンク データ >
	ステガノグラフィー >
	プロトコル偽装 >
動的解決(3) >	ドメイン生成アルゴリズム >
	高速フラックスDNS >
	DNS計算 >
暗号化チャネル(2) >	対称暗号化 >
	非対称暗号化 >
フォールバック チャネル >	
侵入ツールの送り込み >	
マルチステージ チャネル >	
非アプリケーション層プロトコル >	
非標準ポート >	
プロトコル トンネリング >	

プロキシー (4) >	内部プロキシー >
	外部プロキシー >
	マルチホップ プロキシー >
	ドメイン フロンティング >
リモート アクセス ソフトウェア >	
トラフィック シグナリング (1) >	ポート ノッキング >
Webサービス (3) >	デッド ドロップ リゾルバー >
	双方向通信 >
	片方向通信 >

Zscaler検出エンジン

コマンド＆コントロール トラフィックの検出に役立つZscalerセキュリティ ログは以下のとおりです。

- 高度な脅威対策：ボットネット/コマンド＆コントロール トラフィック/レピュテーション ブロック
- サンドボックス：不明な添付ファイル

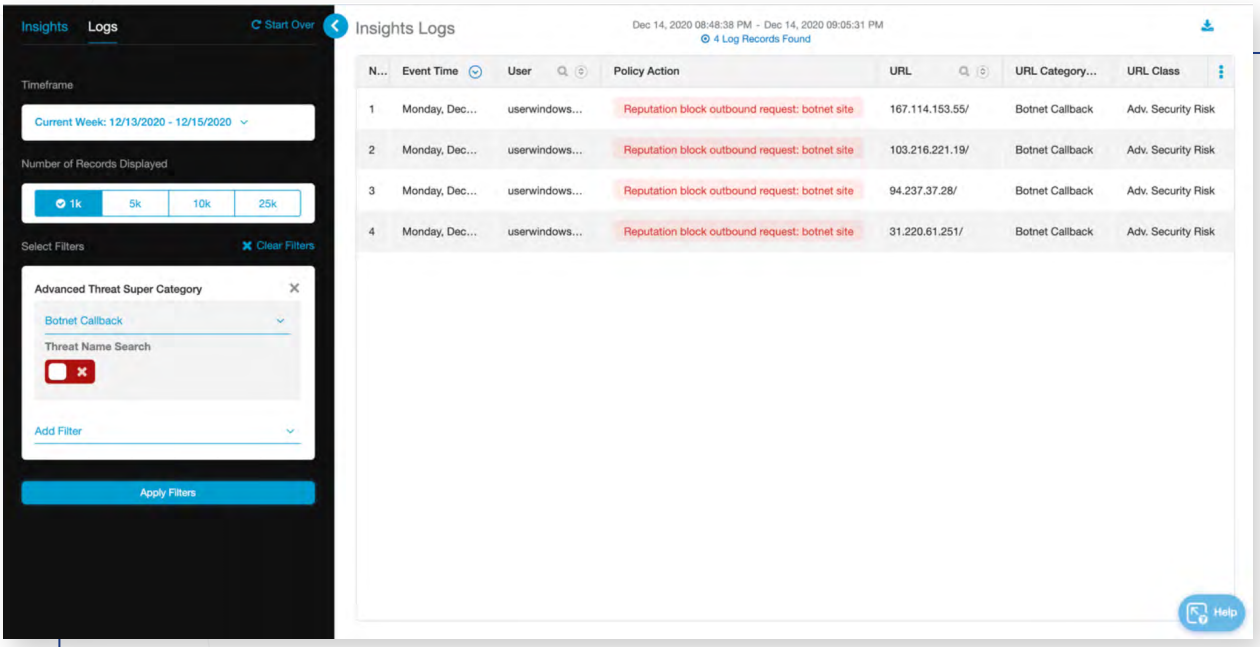
調査

Web解析の使用

解析ログをフィルタリングしてボットネット/コマンド＆コントロール トラフィックを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

Advanced Super Threat Category= “Botnet Callback”
Policy Type="Advanced Threat Protection", **URL Category**="Botnet Callback"

ボットネット/コマンド＆コントロール トラフィックに関するWeb解析の検索例



NSS Webログの使用

NSS Webログを詳細に分析してボットネット/コマンド＆コントロール トラフィックを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

ruleType="AdvThreatProtection", **urlCat**="Botnets"
ruleType="AdvThreatProtection", **urlCat**="Botnets", **urlclass**="Advanced Security Risk"
reason= “IPS block outbound request: botnet command and control traffic”
reason= “Reputation block outbound request: botnet site”

ボットネット/コマンド＆コントロール トラフィックに関するNSS Webログの検索例

```
source="zscalernss-web" ruletype=AdvThreatProtection urlcat=Botnets urlclass="Advanced Security Risk"
```

Event

```
2020-12-14 21:05:31 reason=Reputation block outbound request: botnet site event_id=6906344911668838402 protocol=HTTP action=Blocked transaction
size=14392 responsesize=14167 requestsize=225 urlcat=Botnets serverip= clienttranstime=0 requestmethod=GET refererURL=
None useragent=Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36; sb_63199_bs product=NSS loc
ation=Road Warrior ClientIP=10.0.0.1 status=403 user= net url=31.220.61.251/ vendor=Zscaler hos
tname=31.220.61.251 clientpublicIP=184.170.224.170 malwarecat=None threatname=Win32.Backdoor.Drovorub.LZ filetype=None appname=General Browsing
pagerisk=100 department=Employees urlsupercategory=Advanced Security appclass=General Browsing dlpengine=None urlclass=Advanced Security
Risk malwareclass=None dlpdictionaries=None fileclass=None bwthrottle=NO servertranstime=0 contenttype=Other unscannabletype=Non
e devicehostname= deviceowner= trafficredirectmethod=ZscalerClientConnector rulelabel=NA ruletype=AdvThreatProtection mob
appname=None mobappcat=None mobdevtype=None bwclassname=None bwrulename=None throttlereqsize=0 throttlerespsize=0 svcedg=5209 bam
d5=None filename=None
```

推奨される防止/軽減策

インシデント前：

- アンチウイルス ソフトウェアを最新の状態に保つ
- オペレーティング システムとパッチを最新の状態に保つ
- 不審なリンクをクリックしたり、不明な送信元からの添付ファイルをダウンロードしたりしないようにユーザーを教育する
- ネットワークをスキャンし、異常や不審なアクティビティーにフラグを付ける

インシデント後：

- 調査によって、感染経路を見つけ、他の資産が侵害されているかどうかを確認する
- アンチウイルス スキャンを行う
- マシンを再構築する

マルウェア トロイの木馬/RAT/パスワード スティーラー/ワーム

説明

トロイの木馬とは、正当なように見えるものの、コンピューターの制御を奪うことができる、悪意のあるコードまたはソフトウェアの一種です。

Zscaler検出エンジン

マルウェア トロイの木馬/RAT/パスワード スティーラー/ワームを検出するには、以下の各種Zscaler検出エンジンが役立ちます。

- マルウェア対策(レピュテーション、アンチウイルス、Yara)
- 高度な脅威対策(レピュテーション、IPS)

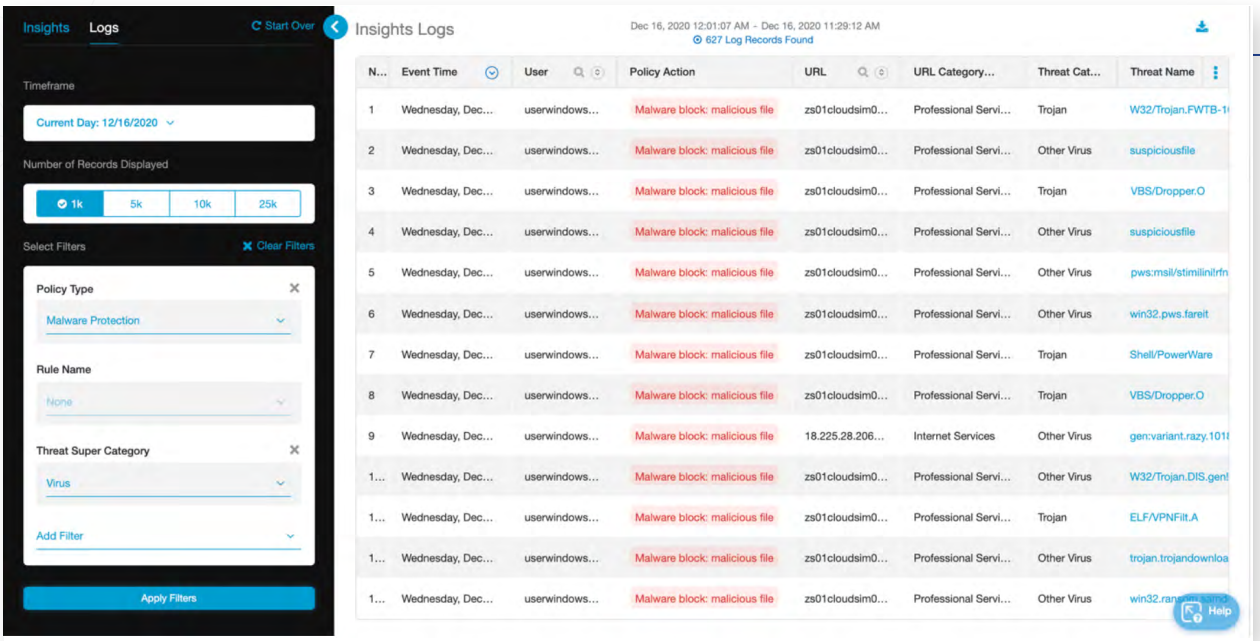
調査

Web解析の使用

解析ログをフィルタリングしてマルウェア/トロイの木馬/RAT/パスワード スティーラー/ワームの試みを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

Policy Type="Advanced Threat Protection", “Malware Protection”
Threat Super Category="Virus"
Threat Category=” Macro Virus," “Malware Tool,” “Password Stealer,” “Trojan,” “Worm,” “Unrecognized Virus,” “Other Virus,” “Other Malware,” “Boot Virus”

マルウェア トロイの木馬に関するWeb解析の検索例



NSS Webログの使用

NSS Webログを詳細に分析してマルウェア/トロイの木馬/RAT/パスワード スティーラー/ワームの試みを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

ruleType="AV" **malwareclass**="Virus"
malwarecat="Trojan." "Macro Virus," "Malware Tool," "Password Stealer," "Worms," "Unrecognized Virus"
reason="Malware block:malicious file"
urlclass="Advanced Security Risk"
urlcat="Malicious URLs", "Suspected Spyware or Adware"
urlclass="Advanced Security Risk"

マルウェア トロイの木馬に関するNSS Webログの検索例

```
source="zscalernss-web" ruletype=AV malwareclass=Virus malwarecat=Trojan OR malwarecat=Virus OR malwarecat=Worms
```

Event

```
2020-12-16 11:29:12  reason=Malware block: malicious file  event_id=6906938566343458818  protocol=HTTP  action=Blocked  transactionsize=14593  res
ponsesize=14207 requestsize=386 urlcat=Professional Services  serverip=  clienttranstime=134  requestmethod=GET  refererURL=None use
ragent=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729); sb_75006_bs  pro
duct=NSS  location=Road Warrior  ClientIP=10.0.0.1  status=403  user=u  .net  url=
ch.net/mal.bin  vendor=Zscaler  hostname=zs  t  clientpublicIP=  malwarecat=Trojan  threatname=W97M/Agent  fil
etype=Microsoft Installer  appname=General Browsing  pagerisk=100  department=Employees  urlsupercategory=Business and Economy  appclass=Ge
neral Browsing  dlpengine=None  urlclass=Business Use  malwareclass=Virus  dlpdictionaries=None  fileclass=Executables Files  bwthrottle=NO  ser
vertranstime=80 contenttype=text/html  unscannabletype=None  devicehostname=  deviceowner=  trafficredirectmethod=ZscalerClientConnecto
r  rulelabel=NA  ruletype=AV  mobappname=None mobappcat=None  mobdevtype=None bwclassname=General Surfing  bwrulename=No Bandwidth Control thr
ottlereqsize=0  throttlerespsize=0  svcedg=5209  bamd5=c6c4ce020e76de3dab7684fed5083c8f  filename=mal.bin
```

推奨される防止/軽減策

インシデント前：

- アンチウイルスを最新の状態に保つ
- オペレーティング システムとパッチを最新の状態に保つ
- 完全に信頼できない提供元のソフトウェアをダウンロードまたはインストールしない

インシデント後：

- 調査によって、感染経路を見つけ、他の資産が侵害されているかどうかを確認する
- アンチウイルス スキャンを行う
- マシンを再構築する

高度な標的型攻撃

マルウェア ランサムウェア

説明

攻撃者は、ターゲットとなるシステムやネットワーク内の多数のシステム上のデータを暗号化して、システムやネットワーク　リソースの可用性を妨害することができます。これは、復号または復号キーと引き換えに被害者から金銭的な補償を引き出すため(ランサムウェア)、またはデータを永久にアクセス不能にするために行われる場合があります。

Zscaler検出エンジン

マルウェア ランサムウェアを検出するには、以下のZscaler検出エンジンが役立ちます。

- **マルウェア対策**(レピュテーション、アンチウイルス、Yara)

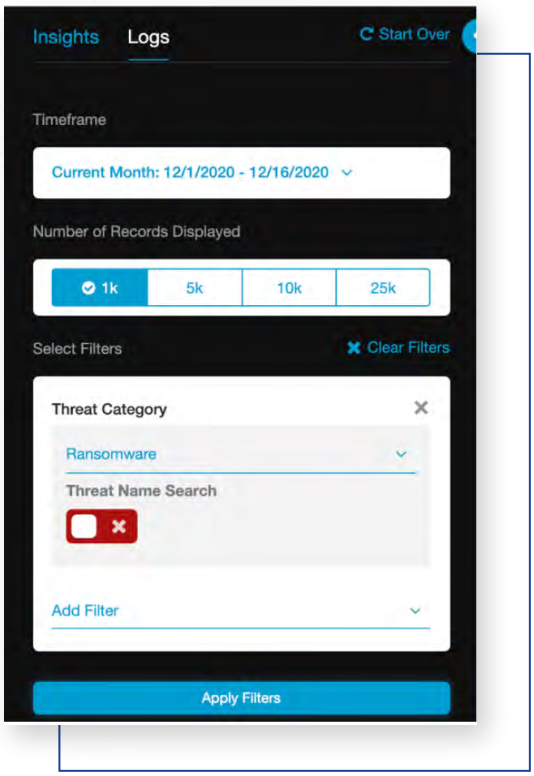
調査

Web解析の使用

解析ログをフィルタリングしてランサムウェアの試みを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

Threat Category=” Ransomware”

ランサムウェアに関するWeb解析の検索例



NSS Webログの使用

NSS Webログを詳細に分析してクリプトマイニングの試みを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

ruleType="AV", **malwareclass**="Virus", **malwarecat**="Ransomware", **reason**="Malware block:malicious file"

クリプトマイニングに関するNSS Webログの検索クエリ例

```
"ruletype=advthreatprotection" "urlclass=Advanced Security Risk" urlcat=cryptomining
```

推奨される防止/軽減策

インシデント前：

- アンチウイルスを最新の状態に保つ
- オペレーティング システムとパッチを最新の状態に保つ
- 完全に信頼できない提供元のソフトウェアをダウンロードまたはインストールしない

インシデント後：

- 調査によって、感染経路を見つけ、他の資産が侵害されているかどうかを確認する
- アンチウイルス スキャンを行う
- バックアップ データやシステムをオフラインにして、直ちに安全を確保する
- 法執行機関に連絡する

インサイダー脅威

クリプトマイニングなど、企業のリソースを利用した悪意のあるアクティビティーを追跡します。

クリプトマイニング マルウェア

説明

クリプトマイニング マルウェアとは、ユーザーの明示的な許可なくコンピューターのリソースを乗っ取り、暗号通貨のマイニングに使用するために開発されたマルウェア プログラムのことです。

Zscaler検出エンジン

クリプトマイニングを検出するには、以下のZscaler検出エンジンが役立ちます。

- 高度な脅威対策(IPS)
- サンドボックス

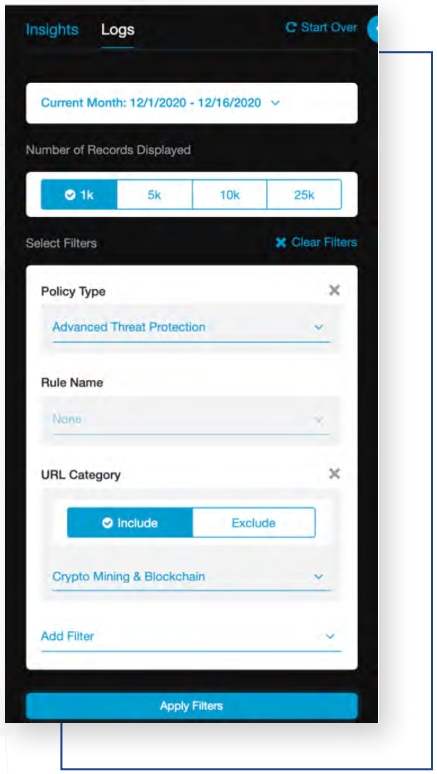
調査

Web解析の使用

解析ログをフィルタリングしてクリプトマイニングの試みを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

Policy Type="Advanced Threat Protection"
URL Category= “Crypto Mining & Blockchain”

クリプトマイニングに関するWeb解析の検索例



NSS Webログの使用

NSS Webログを詳細に分析してクリプトマイニングの試みを特定するには、以下のキー フィールドと検索パラメーターが役立ちます。

セキュリティ ログを詳細に分析するには、以下のパラメーターが役立ちます。

ruleType="AdvThreatProtection", **urlCat**="Cryptomining", **urlclass**="Advanced Security Risk", **reason**="IPS block”

クリプトマイニングに関するNSS Webログの検索クエリ例

```
"ruletype=advthreatprotection" "urlclass=Advanced Security Risk" urlcat=cryptomining
```

推奨される防止/軽減策

インシデント前：

- 不審なアクティビティーがないかネットワークを監視する
- クリプトマイニングの脅威をセキュリティ教育のトレーニングに取り入れる
- Webブラウザーにクリプトマイニング防止の拡張機能をインストールする

インシデント後：

- 調査によって、感染経路を見つけ、他の資産が侵害されているかどうかを確認する
- アンチウイルス スキャンを行う
- マシンを再構築する

Advanced Cloud Sandboxによる脅威検出

未知のマルウェアの検出

説明

ほとんどのセキュリティ ソリューションは、何らかの形式のシグネチャーに依存して悪意のあるトラフィックを検出しています。サンドボックスでは、動的分析を使用し、ファイルの動作を隔離された環境で監視することで、ゼロデイ脅威からユーザーを保護します。Zscaler Cloud Sandboxは、高度な動作分析テクノロジーを使用して未知のマルウェアの脅威を発見し、ブロックします。Zscaler Cloud Sandboxは、ネットワークへの侵入前に脅威をブロックするインライン保護を提供するように設計されています。事前に定義したポリシーに基づき、悪意のあるファイルは瞬時にブロックされ、隔離またはフラグ付けされます。

Zscaler検出エンジン

未知のマルウェアや潜在的なゼロデイ脅威のマルウェアを検出するには、以下のZscaler検出エンジンが役立ちます。

- サンドボックス

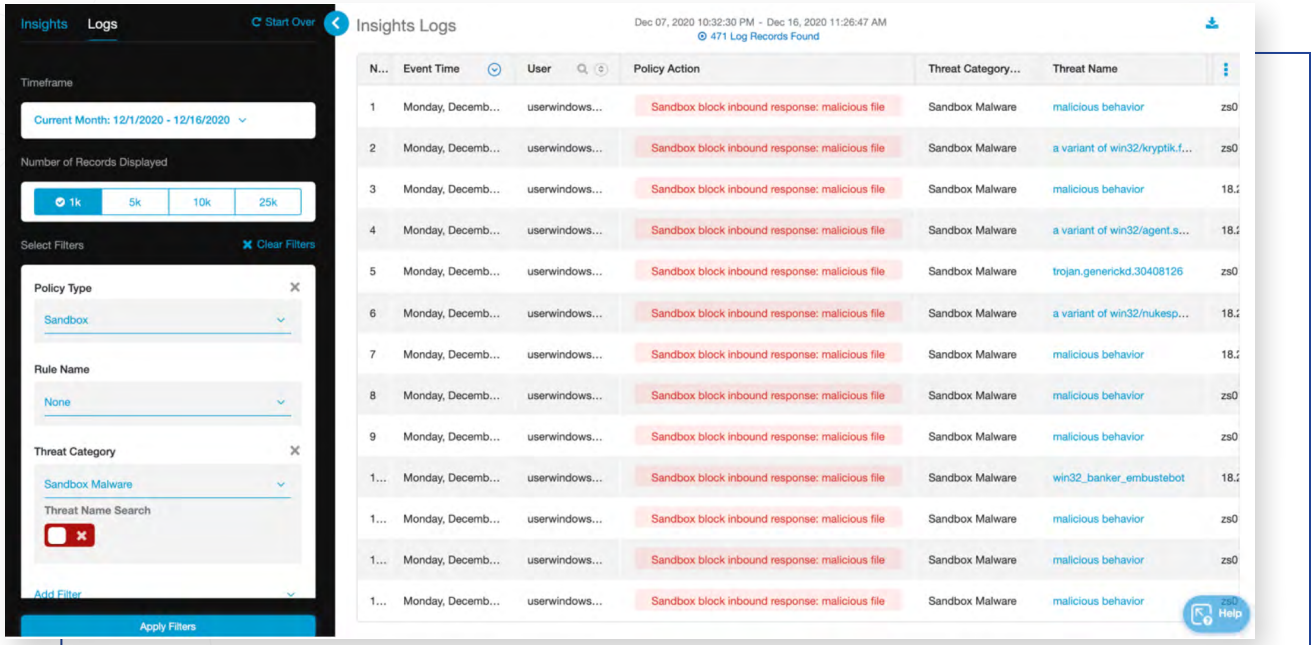
調査

Web解析の使用

解析ログをフィルタリングして、サンドボックスに送信された不明なファイルを特定するには、以下のキーフィールドと検索パラメーターが役立ちます。

Policy Type="Sandbox"
Threat Category= “Sent for Analysis,” “Sandbox Adware,” “Sandbox Anonymizer,” “Sandbox Malware”

サンドボックス マルウェアに関するWeb解析の検索例



NSS Webログの使用

NSS Webログを詳細に分析して、サンドボックスに送信された不明なファイルを特定するには、以下のキーフィールドと検索パラメーターが役立ちます。

ruleType="BA"
malwarecat="Sent for Analysis," “Sandbox Malware,” “Sandbox Adware,” Sandbox Anonymizer”
reason="Allowed - No Active Content,’ “Quarantined,” “Sandbox block inbound response: malicious file,” “Allowed and No Scan”

Advanced Cloud SandboxとAPIライセンスをお持ちの場合、SIEMのログから取得したMD5パラメーターに基づいてサンドボックス詳細レポートを開くことができます。MD5がログに含まれていない場合は、キーフィールド[bamd5]をNSSフィードに追加することで、Webログから取得できます。Cloud Sandbox APIを使用して、MD5ハッシュの完全な詳細レポートを取得できます。このレポートを取得するための構文は、次のAPIリファレンスのリンクを参照してください。

https://help.zscaler.com/zia/api

サンドボックスに送信された不明なファイルを探すためのNSS Webログの検索例

```
source="zscalernss-web" ruletype=BA "malwarecat=Sandbox Malware" OR "malwarecat=Sandbox Adware" OR "malwarecat=Sent for Analysis" OR "malwarecat=Sandbox Anonymizer"
```

Event

```
2020-12-16 11:26:47     reason=Sandbox block inbound response: malicious file   event_id=6906937943573200897    protocol=HTTP   action=Blocked  transaction
size=14410      responsesize=14228      requestsize=182 urlcat=Professional Services    serverip=               clienttranstime=83      requestmethod=GET
refererURL=None useragent=python-requests/2.22.0; sb_74966_bs   product=NSS     location=Road Warrior   ClientIP=10.0.0.1       status=403      user=userwi
ndo                     three.net       url=z                                   skqlqx      vendor=Zscaler  hostname=z                              :  clientpubli
cIP='                   malwarecat=Sandbox Malware      threatname=win32_trojan_badcall filetype=Windows Executables    appname=General Browsing        pag
erisk=100       department=Employees    urlsupercategory=Business and Economy   appclass=General Browsing       dlpengine=None  urlclass=Business Use   mal
wareclass=Behavior Analysis     dlpdictionaries=None    fileclass=Executables Files     bwthrottle=NO   servertranstime=81      contenttype=Other       uns
cannabletype=None       devicehostname=         deviceowner=            trafficredirectmethod=ZscalerClientConnector    rulelabel=BA_3  ruletype=BA     mob
appname=None    mobappcat=None  mobdevtype=None bwclassname=General Surfing     bwrulename=No Bandwidth Control throttlereqsize=0       throttlerespsize=0
svcedg=5209     bamd5=c6f78ad187c365d117cacbee140f6230  filename=None
```

推奨される防止/軽減策

インシデント前：

- パッチ管理を実装する
- ホスト侵入防止システム(HIPS)を使用する
- 重要なアプリケーションのみを使用する

インシデント後：

- 調査する
- 包含する – ホストレベルとネットワークレベル
- 揮発性データを保存する

付録B – Zscalerとサードパーティーのセキュリティ インテリジェンスおよび自動化ツールとの統合

Zscalerのテクノロジー パートナー プログラムは、主要なテクノロジー ソリューションとの統合を合理化することにより、セキュリティとクラウド アジリティーの向上というお客様の目標達成を支援します。Zscalerは、以下のセキュリティ運用テクノロジー パートナーと統合し、情報の拡充と自動化により、効率的かつ効果的なリスクとコンプライアンスの管理を可能にします。

セキュリティ情報およびイベント管理(SIEM)と解析

NSSを使用することで、Zscalerのお客様はWebログ データをSIEMシステムに送信して、複数のソースからのログの関連付けを容易にすることができ、ネットワーク全体のトラフィック パターンを分析できるようになります。さらに、SIEMのWebログ データを活用して、長期的な履歴分析(6か月以上)を実施できます。さらには、ローカル ログ アーカイブを法規制のコンプライアンスに利用することもできます。

Zscalerは多くのSIEMパートナーと連携し、シームレスな統合を実現しています。
https://www.zscaler.jp/partners/technology/siem-analytics

- **AT&T AlienVault - https://www.zscaler.jp/press/alienvault-and-zscaler-announce-partnership-provide-customers-increased-security-visibility-and-control**
- **BT - https://www.zscaler.jp/resources/solution-briefs/partner-bt-assure.pdf**
- Exabeam
- Expel
- **Gigamon - https://www.zscaler.jp/resources/solution-briefs/partner-gigamon-threat-insight.pdf**
- JASK
- LogRhythm
- **IBM Security - https://www.zscaler.jp/resources/solution-briefs/partner-qradar.pdf**
- **SecBI - https://www.zscaler.jp/resources/solution-briefs/partner-secbi.pdf**
- **Splunk - https://www.zscaler.jp/resources/solution-briefs/partner-splunk.pdf**
- **Sumo Logic - https://www.zscaler.jp/resources/solution-briefs/partner-sumo-logic.pdf**
- **WitFoo - https://www.zscaler.jp/resources/solution-briefs/partner-witfoo.pdf**

Security Orchestration, Automation and Response (SOAR)

Zscalerは主要なSOARプラットフォームとの統合をサポートしており、SOC部門によるZscalerを使用したイベント検索、レピュテーション チェック、さまざまな侵害の阻止の適用と自動化を支援します。SOARとZscalerのワークフローが合理化されることで、セキュリティ部門は更新されたポリシーをリアルタイムで適用し、ネットワーク内外のユーザーの保護を強化できます。

Zscalerは多くのSOARパートナーと連携し、シームレスな統合を実現しています。
https://www.zscaler.jp/partners/technology/soar

- **D3Security - https://www.zscaler.jp/resources/solution-briefs/partner-d3security.pdf**
- **Demisto - https://www.zscaler.jp/resources/solution-briefs/partner-demisto.pdf**

- Exabeam
- LogicHub - https://www.zscaler.jp/resources/solution-briefs/partner-logichub.pdf
- SecBI - https://www.zscaler.jp/resources/solution-briefs/partner-secbi.pdf
- Siemplify - https://www.zscaler.jp/resources/solution-briefs/partner-siemplify.pdf
- Splunk Phantom - https://www.zscaler.jp/resources/solution-briefs/partner-splunk.pdf
- Swimlane - https://www.zscaler.jp/resources/solution-briefs/partner-swimlane.pdf

脅威インテリジェンス プラットフォーム(TIP)

Zscaler ThreatLabZの調査チームは、Zscalerクラウドで発生する1日あたり1500億件以上のトランザクションと1億件以上のブロックされた攻撃とともに、多数の主要な脅威インテリジェンス フィードを分析し、Zscalerのすべてのお客様の利益のために検出と製品の機能を更新し続けています。

さらに、Zscalerは主要なTIPと統合しているため、SOC部門はZscalerの導入環境内で重要な脅威への対応を用意に行うことができます。Zscalerはユーザー定義のIOCをTIPから自動で取得することで、リアルタイムのポリシー適用を可能にし、すべての支社とネットワーク内外のすべてのユーザーに対して、新たな脅威や標的型攻撃からの完全な保護を実現します。

Zscalerは以下のTIPパートナーと連携し、シームレスな統合を実現しています。
https://www.zscaler.jp/partners/technology/threat-intelligence-platform

- Anomali - https://www.zscaler.jp/resources/solution-briefs/partner-anomali.pdf
- Intsights - https://www.zscaler.jp/resources/solution-briefs/partner-intsights.pdf
- Recorded Future - https://www.zscaler.jp/resources/solution-briefs/partner-recorded-future-integration-deployment-guide.pdf
- SecLytics - https://www.zscaler.jp/resources/solution-briefs/partner-seclytics.pdf

CASB

Zscalerクラウド セキュリティ プラットフォームは、ネットワーク内外のすべてのユーザーを保護するための完全なインラインCASB機能を備え、粒度の細かいコントロールとともに、すべての入出力トラフィックをリアルタイムで可視化できます。Zscalerは、SaaSアプリケーションに対する独自の帯域外の可視性および制御機能を提供するだけでなく、一部のCASBベンダーと提携して、お客様がリスク評価を実行し、クラウド サービスとシャドー ITにアプリケーション制御を適用できるよう支援しています。

Zscalerは以下のCASBパートナーと連携し、シームレスな統合を実現しています。
https://www.zscaler.jp/partners/technology/cloud-access-security-broker

- Bitglass - https://www.zscaler.jp/resources/solution-briefs/partner-bitglass-casb.pdf
- Microsoft - https://www.zscaler.jp/resources/solution-briefs/partner-microsoft-cloud-app-security.pdf
- McAfee - https://www.zscaler.jp/resources/solution-briefs/partner-mcafee-mvision-deployment-guide.pdf
- Proofpoint - https://www.zscaler.jp/resources/solution-briefs/proofpoint-deployment-guide.pdf

ファイアウォール

企業はマルチベンダーのファイアウォール管理ツールを利用して、環境内のすべてのファイアウォールが一貫して企業ポリシーを実施し、リスクを管理できるようにしています。APIを利用して主要なファイアウォール管理パートナーをZscalerと統合することで、ルールのレビューや変更の追跡が可能になり、コンプライアンス監査やアクセス分析に利用できるようになります。

Zscalerは以下のファイアウォール パートナーと連携し、シームレスな統合を実現しています。
https://www.zscaler.jp/partners/technology/firewall-policy-management

- **Firemon - https://www.zscaler.jp/resources/solution-briefs/partner-firemon.pdf**
- **Skybox Security - https://www.zscaler.jp/resources/solution-briefs/partner-skybox-security.pdf**

エンドポイント(EDR)

Zscalerは、主要なエンドポイント保護プラットフォーム(EPP)やエンドポイント検出および応答(EDR)ソリューションとの統合により、エンドポイントからクラウドへのセキュリティを実現します。これらの統合により、Zscalerはエンドポイントのセキュリティ ポスチャーを検証し、API統合を介して感染したデバイスを隔離して脅威の水平移動を防ぐことで、企業資産への接続を制御できます。Zscalerは、EPP/EDRクラウドから脅威のインテリジェンスを共有、受信し、エンドポイント レポートを企業のお客様に提供します。

Zscalerは以下のエンドポイント保護パートナーと連携し、シームレスな統合を実現しています。
https://www.zscaler.jp/partners/technology/endpoint-security

- VMware Carbon Black
- CrowdStrike
- SentinelOne

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SASE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。

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.jp