レポート

レポートの概要

Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションには、一連の定義済みレポートが含まれます。レポート機能は、Cisco Web セキュリティ アプライアンスのネイティブなレポート機能との一貫性をできる限り保ちます。

（注） Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションを使って生成されるレポートは、レポートのロード時間を促進するサマリー インデックスを使用することで、Splunk を通じて取得できるデータと比べ、より多くのデータを表示する場合があります。

ヒント Splunk の管理者は、概要レポートおよび Web トラッキング レポートに表示されるホストを制御できます。追加、削除、または名前を変更したいホストがある場合は、その詳細を Splunk 管理者に知らせてください。

データの書式

Cisco WSA Splunk アプリケーションを通じて取得できるデータの形式は、ネイティブなレポート作成機能で利用できるデータ形式とは異なる場合があります。

データ	フォーマット
大きな数（7 ケタを超える）	2E11 は、$2x10^{11}$ を意味する
時間	d+hh: mm: ss.ms 例 : 1+03: 22:36.00 1 日、3 時間、22 分、 36 秒、0 ミリ秒

時間範囲

ヒント　より迅速に結果を返すには、より小さな時間範囲を選択します。

データ可用性のタイミング

範囲	インデックス生成開始	データのレポート表示
時間（Hour）	1 時間経過後	インデックス生成開始後 60 ～ 90 分
日（Day）	午前 0 時すぎ	インデックス生成開始後 1 日
週（Week）	土曜日の午前 0 時すぎ （日曜日の早朝）	インデックス生成開始後 1 週間
90 日間	90 日目の午前 0 時すぎ	インデックス生成後 90 日
カスタム：1 時間未満	1 時間経過後	インデックス生成開始後 60 ～ 90 分
カスタム：1 日未満	午前 0 時すぎ	インデックス生成開始後 1 日
カスタム：1 週間未満	土曜日の午前 0 時すぎ （日曜日の早朝）	インデックス生成開始後 1 週間

ヒント　[ジョブ（jobs）] メニューを使用して、スケジュールされた検索が長時間実行していないことを確認します。[超過（Too long）] は、たとえば、週間検索が 1 週間以上続くなど、頻度が高いことを示します。

ヒント　[ジョブ（Jobs）] メニューを選択します。各レポートの検索に、検索の説明とインターバルのサマリーを表示するマーカーがあります。たとえば、「_dashboard_users_base-search(*,1d)」の検索は、ユーザの-1 日のサマリーを表します。

サマリー インデックス生成のタイミング

サマリー インデックスは、レポート生成のスピードを促進します。サマリーは 1 時間ごとに生成されます。毎晩、毎時のサマリーは日々のサマリーに集約されます。毎週、毎日のサマリーは週単位の要約に集約されます。

サマリー検索	頻度
[_dashboard_SOCKS_base-sum-search-top-1h]	毎時 10 分後
[_dashboard_SOCKS_base-sum-search-top-1d]	毎日 2:30 AM
[_dashboard_SOCKS_base-sum-search-top-1w]	毎週 1:45 AM
[_dashboard_anti-malware_base-sum-search-1h]	毎時 35 分後
[_dashboard_anti-malware_base-sum-search-1d]	毎日 1:30 AM
[_dashboard_anti-malware_base-sum-search-1w]	日曜日 2:15 AM
[_dashboard_application-visibility_base-sum-search-1h]	毎時 15 分後
[_dashboard_application-visibility_base-sum-search-1d]	毎日 12:30 AM
[_dashboard_application-visibility_base-sum-search-1w]	日曜日 2:45 AM
[_dashboard_overview_base-sum-search-bottom-1h]	毎時 50 分後
[_dashboard_overview_base-sum-search-bottom-1d]	毎日 6:00 AM
[_dashboard_overview_base-sum-search-bottom-1w]	毎週 3:15 AM
[_dashboard_overview_base-sum-search-top-1h]	毎時ちょうど
[_dashboard_overview_base-sum-search-top-1d]	毎日 5:00 AM
[_dashboard_overview_base-sum-search-top-1w]	毎週 3:45 AM
[_dashboard_overview_base-sum-search-uid-1h]	毎時 40 分後
[_dashboard_overview_base-sum-search-uid-1d]	毎日 4:00 AM
[_dashboard_overview_base-sum-search-uid-1w]	毎週 4:15 AM
[_dashboard_url-categories_base-sum-search-1h]	毎時 30 分後
[_dashboard_url-categories_base-sum-search-1d]	毎日 3:00 AM
[_dashboard_url-categories_base-sum-search-1w]	毎週 5:15 AM
[_dashboard_users_base-sum-search-1h]	毎時 20 分後
[_dashboard_users_base-sum-search-1d]	毎日 2:00 AM
[_dashboard_users_base-sum-search-1w]	毎週 5:45 AM
[_dashboard_web-reputation-filters_base-sum-search-1h]	毎時 45 分後
[_dashboard_web-reputation-filters_base-sum-search-1d]	毎日 1:00 AM
[_dashboard_web-reputation-filters_base-sum-search-1w]	毎週 4:45 AM
[_dashboard_web-sites_base-sum-search-1h]	毎時 55 分後
[_dashboard_web-sites_base-sum-search-1d]	毎日 0 時 AM
[_dashboard_web-sites_base-sum-search-1w]	日曜日 1:15 AM

エクスポート

.CSV ファイルにエクスポート

ステップ 1　レポートを生成します。

ステップ 2　[エクスポート（Export）] を選択します。

PDF ファイルにエクスポート

はじめる前に

- Splunk 管理者が PDF 出力を有効化していることを確認します。

ステップ 1　レポートを生成します。

ステップ 2　[PDF として保存（Save as PDF）] を選択します。

関連トピック

- 「（任意）スケジュール済 PDF レポートのセットアップ」（P.1-13）

汎用データと特定データ

事前定義された汎用レポートには、事前定義された特定レポートへのハイパーリンクがあります。

詳細を表示

ステップ 1　最適な定義済み汎用レポートを選択します。

たとえば、ユーザに関する特定の情報を表示する場合は、事前に定義されたユーザ レポートから開始します。

ステップ 2　詳細を知りたいサブジェクトのハイパーリンクをクリックします。

たとえば、ハイパーリンクがついたユーザ名、または個々のユーザの IP アドレスを指定します。

関連トピック

- 「エクスポート」（P.2-4）

検索

Web トラッキング レポートを使って、簡易検索およびアドバンス検索オプションを利用できます。

ワンポイントアドバイス　検索対象をできるだけ特定し、時間範囲を狭めてください。

ヒント　Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションでは、一連のファイルを使用して、Web トラッキング ページのメニューを表示します。[Web トラッキング（Web Tracking）] ページのメニューに問題が発生した場合は、これらのファイルがアプリケーションの参照フォルダにあることを確認します。

- malware_categories.csv
- transaction_types.csv
- url_categories.csv

ヒント　Splunk 管理者は、Splunk 内に表示される URL カテゴリのリストを編集できます。カテゴリがアクセス ログに表示されるが参照ファイルにはない場合、Cisco Web セキュリティ アプライアンス用 Splunk アプリケーションに [カスタムカテゴリ（Custom Category）] が表示されます。

部門

departments.csv は、役割ベースのセキュリティ機能の一部として使用されるファイルです。このファイルは、手動またはロール ディスカバリ スクリプトの設定（アプリケーションの bin フォルダで使用可能）によって編集できます。Linux と Windows、両方のスクリプトがあります。

- ファイルがアプリケーションの参照フォルダにあることを確認します。
- Linux バージョンを使用している場合は、CLI ldapsearch がインストールされ、Splunk ユーザのパスにあることを確認します。
- Windows バージョンを使用している場合は、どこでどのような理由でエラーが発生したかについての特定情報を明示するため、「option explicit」がコメントアウトされる可能性があります。
- LDAP パスの構文が正しいことを確認します。
- バインド サービスのアカウント名が正しいことを確認します。
- 正しいバインド パスワードが入力されていることを確認します。
- ポート 389 経由でリモート マシンにテスト接続
- 正しい属性がメンバ名に設定されていることを確認します。
- 正しい属性がグループ メンバーシップに使用されたことを確認します。
- 正しい属性がグループ名に設定されたことを確認します。

ヒント　Splunk 管理者は、Web トラッキング フォームのドロップダウン フィールドに使用できるオプションを制御できます。

定義済みレポート

汎用レポートのリスト

- 概要
- ユーザ
- Web サイト
- URL カテゴリ
- アプリケーションの可視性
- アンチマルウェア
- クライアント マルウェア リスク
- ウエブ評判フィルタ
- L4 トラフィック モニタ

特定レポートのリスト

- マルウェア カテゴリ
- マルウェアの脅威
- アプリケーション
- アプリケーション タイプ
- ドメイン
- URL カテゴリ
- ユーザ
- ロケーション別レポート
  - ロケーション別概要
  - ロケーション別 URL カテゴリ
  - ロケーション別アンチマルウェア対策
  - ロケーション別 Web レピュテーション フィルタ
  - ロケーション別アプリケーション可視性
  - ロケーション別ユーザ
  - ロケーション別 Web サイト

関連トピック

- 「検索」（P.2-5）

使用シナリオ

ユーザの調査

ここでは、システム管理者がどのように社内の特定ユーザを調査するかについて例を挙げます。このシナリオでは、ある従業員が勤務中に不適切な Web サイトにアクセスしている、という苦情を管理者が受け取っています。システム管理者は、この問題を調査するにあたり、従業員の Web 使用状況のトレンドおよびトランザクション履歴を見る必要があります。

- トータル トランザクション別の URL カテゴリ
- トータル トランザクション別のトレンド
- 一致する URL カテゴリー
- 一致するドメイン
- 一致するアプリケーション
- 検出されたマルウェア脅威
- 特定のユーザ ID またはクライアント IP と一致するポリシー

システム管理者は、これらのレポートを使用することにより、たとえば、ユーザの「johndoe」がブロックされた URL にアクセスしようとしていたかどうかを把握することができます。これは、[ドメイン（Domains）] セクションにある [ブロックされたトランザクション（Transactions Blocked）] 列に表示されます。

Web 使用トレンドの閲覧

ステップ 1　Cisco WSA Splunk アプリケーションのドロップダウンメニューから、[ユーザ（Users）] を選択します。

ステップ 2　ユーザ ID またはクライアント IP アドレスを指定します。

（注）　調べたいクライアント IP アドレスまたはユーザ ID が見つからない場合は、適当なユーザ ID またはクライアント IP を指定します。ユーザ ID またはクライアント IP アドレスのすべてまたは一部を検索します。

ステップ 3　（任意）[アクション（Actions）] > [印刷（Print）] を選択します。

トランザクション履歴の閲覧

ステップ 1　Cisco WSA Splunk アプリケーションのドロップダウン メニューから、[Web トラッキング（Web Tracking）] を選択します。

ステップ 2　ユーザ/クライアント IP アドレスを [検索（Search）] します。

ステップ 3　トランザクションごとに表示される情報を変更するには、トランザクション リスト上部の [選択フィールド（Pick fields）] をクリックします。

ステップ 4　（任意）CSV ファイルにデータをエクスポートするには、[エクスポート（Export）] をクリックします。

アクセスした URL

このシナリオでは、セールス マネジャーが、前週、社内において最もアクセス数の高かった Web サイトのうち、上位 5 つを知りたいと考えています。さらに、どのユーザがこれらの Web サイトにアクセスしているかについても知りたいとします。

最もアクセス数の高い Web サイトの閲覧

ステップ 1　Cisco WSA Splunk アプリケーションのドロップダウン メニューから、[Web サイト（Web Sites）] を選択します。

ステップ 2　[時間範囲（Time Range）] のドロップダウン リストから [週（Week）] を選択します。

ステップ 3　ドメインと一致する表で、上位 25 のドメインが表示されます。

ステップ 4　ドメインをクリックすると、そのドメインをブラウズしたユーザが頻度の高い順に表示されます。

アクセス数の高かった URL カテゴリ

このシナリオでは、人事部マネジャーが、過去 30 日間で社内において最もアクセス数の高かった URL カテゴリーの上位 3 つを知りたいと考えています。さらに、ネットワーク管理者が、同様の情報を使って帯域幅の使用状況をモニタし、最も帯域幅を使用している URL がどれかを知りたいと考えています。以下の例は、複数の人の関心事に対応するデータを 1 つのレポートで提供する方法を示します。

最も一般的な URL カテゴリの閲覧

はじめる前に

- 「（任意）スケジュール済 PDF レポートのセットアップ」（P.1-13）

ステップ 1　Cisco WSA Splunk アプリケーションのドロップダウン メニューから、[URL カテゴリ（URL Categories）] を選択します。

ステップ 2　トータル トランザクションのグラフでは、上位 10 の URL カテゴリを表示します。

ステップ 3　[アクション（Actions）] > [PDF 配信スケジュール（Schedule for PDF Delivery）] を選択します。

ステップ 4　人事部マネジャーに PDF を送信します。

ステップ 5　URL カテゴリの照合表で [許容バイト数（Bytes Allowed）] コラムを参照します。

ステップ 6　[アクション（Actions）] > [PDF 配信スケジュール（Schedule for PDF Delivery）] を選択します。

ステップ 7　ネットワーク管理者に PDF ファイルを送信します。

ステップ 8　より細かく制御するために、特定の URL カテゴリをクリックします。