RSA NETWITNESS® SUITE

Malware Analysis構成ガイド

バージョン 11.0

連絡先情報

RSA Link(https://community.rsa.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/EMC-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、EMCが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事責任が課せられることがあります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、本使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

EMC Corporationは、この資料に記載される情報が、発行日時点で正確であるとみなしています。予告なく変更される場合があります。

2月 2018

目次

Malware Analysisの動作の概要

NetWitness Suite Malware Analysisは、自動化されたマルウェア解析ツールです。特定の種類のファイル オブジェクト(Windows PE(Portable Executable) 、PDF、MS Officeなど) を解析し、悪意のあるファイルである可能性を評価できるように設計されています。

Malware Analysisでは、4種類の解析手法を用いてセキュリティ侵害の兆候(本ソフトウェアでは、セキュリティ侵害インジケータと呼びます) を検出します。

- ネットワーク セッション解析(ネットワーク)
- 静的ファイル解析(静的)
- 動的ファイル解析(サンドボックス)
- セキュリティ コミュニティ解析(コミュニティ)

4種類の解析手法はそれぞれ、他の手法に固有の弱点を補完しています。たとえば、動的ファイル解析では、セキュリティ コミュニティ解析フェーズでは検出されないゼロ デイ攻撃の検出を補完できます。マルウェア解析を1つの手法だけで行わないようにすることで、偽陰性(false negative) 対策を強化することができます。

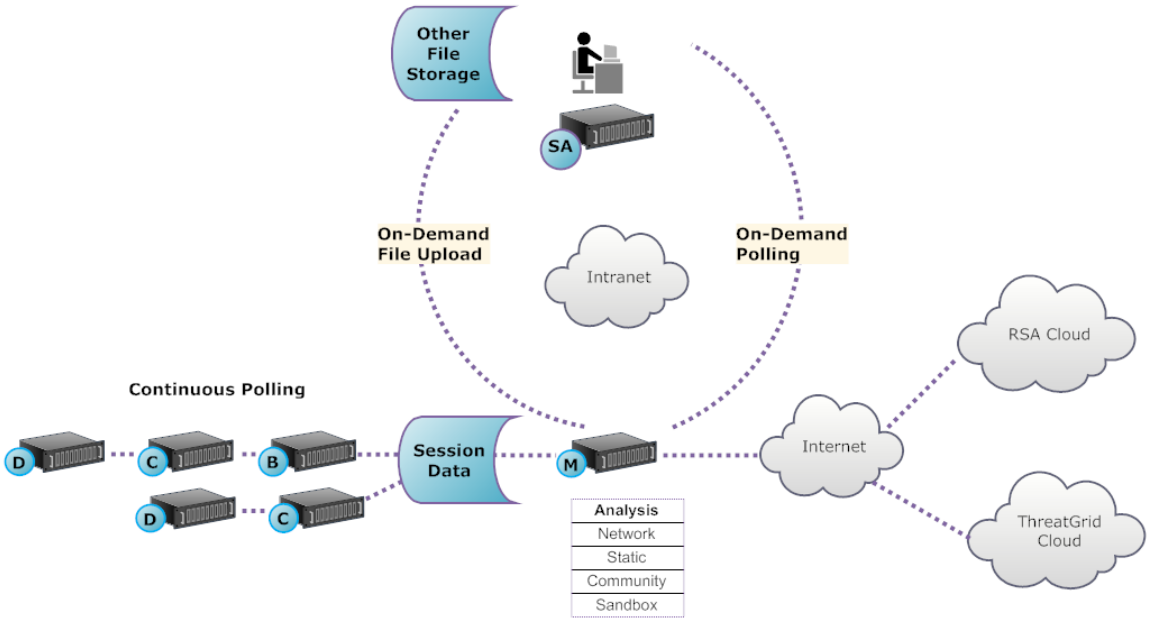
ビルトインのセキュリティ侵害インジケータに加えて、Malware Analysisでは、YARAで記述されたセキュリティ侵害インジケータもサポートされます。YARAは、マルウェアの調査担当者がマルウェアのサンプルの特定や分類を行えるようにするためのルール言語です。これにより、IOC(セキュリティ侵害インジケータ) の作成者は、YARAルールを作成してRSA Liveに公開し、RSA Malware Analysisの検出機能を拡張することができます。RSA Liveに公開されたYARAベースのIOCは、サブスクライブしているホストに自動的にダウンロードされ、アクティブ化されて、調査対象の各ファイルに対して実施する解析能力が補完されます。

Malware Analysisは、Incident Managementのアラートをサポートする機能も備えています。

機能説明

次の図は、コア サービス(Decoder、Concentrator、Broker) と、Malware Analysisサービス、NetWitnessサーバの機能的な関係を示しています。

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



Malware Analysisサービスは、次の手法を組み合わせてファイルオブジェクトを解析します。

- **ConcentratorやBrokerの継続的な自動ポーリング**(常時スキャン)。Parserによってマルウェアコンテンツを含んでいる可能性があると識別されたセッションを抽出します。
- **ConcentratorやBrokerのオンデマンドポーリング**。マルウェアアナリストによってマルウェアコンテンツを含んでいる可能性があると識別されたセッションを抽出します。
- **ファイルのオンデマンドアップロード**(ユーザ指定)。

ConcentratorやBrokerの自動ポーリングが有効になっている場合、Malware Analysisサービスは、使用しているCoreサービスによって収集および解析されたデータから直接、ネットワーク上の実行可能ファイル、PDFドキュメント、Microsoft Officeドキュメントを継続的に抽出し、優先順位を付けます。Malware Analysisサービスは、ConcentratorやBrokerに接続して、マルウェアの可能性ありとしてフラグが付けられている実行可能ファイルのみを抽出するため、処理は高速で効率的です。この処理は継続的に行われ、モニタリングは必要ありません。

ConcentratorやBrokerのオンデマンドポーリングを実行する場合、マルウェアアナリストはInvestigationを使用して、収集されたデータを詳しく調べ、解析するセッションを選択します。Malware Analysisサービスは、この情報を使用して自動的にConcentratorやBrokerをポーリングし、指定されたセッションを解析用にダウンロードします。

ファイルのオン デマンド アップロードでは、アナリストがCoreインフラストラクチャの外部で収集されたファイルをレビューするための手法を提供します。マルウェア アナリストは、フォルダの場所を選択し、1つ以上のファイルをアップロードしてMalware Analysisで解析することができます。これらのファイルは、ネットワーク セッションから自動的に抽出されたファイルと同じ手法で解析されます。

解析手法

ネットワーク解析の場合、Malware Analysisサービスは、一般的なマルウェア アナリストと同様に、標準的なファイルの性質から逸脱しているように見える特徴を検索します。数百個から数千個の特徴を調べ、結果を加重スコア システムと組み合わせることによって、疑わしいセッションがハイライト表示されます。ユーザは、セッション内の異常なアクティビティを示すパターンを、セキュリティ侵害インジケータとして識別し、さらに詳しい調査を実行することができます。

Malware Analysisサービスでは、ネットワーク上で検出した疑わしいファイルに対して静的解析を実行し、それらのオブジェクトに悪意のあるコードが含まれているかどうかを判断できます。コミュニティ解析では、ネットワーク上でマルウェアとして検出されたデータは、RSA Cloudにプッシュ送信され、RSA独自のマルウェア分析データや、SANS Internet Storm Center、SRI International、米国財務省、VeriSignといった組織からのFeedを使って確認されます。サンドボックス解析では、サービスは主要なSIEM(Security Information and Event Management) ホストやThreatGrid Cloudなどにもデータを送信して解析できます。

Malware Analysisでは、業界のリーダーやエキスパートとの提携によるユニークな解析手法が提供されており、そのテクノロジーによってMalware Analysisのスコア システムを充実させることができます。

Malware AnalysisサービスへのNetWitnessサーバアクセス

NetWitnessサーバでは、Investigationから、Malware Analysisサービスに接続し、タグ付けされたデータを送信して、より詳細な解析を実行することができます。解析は3つのサブスクリプション レベルに基づいて実行されます。

- 無料サブスクリプション: NetWitness Suiteを利用中のすべてのユーザが利用可能な、ThreatGrid解析用の無料の試用版キーによるサブスクリプションが提供されます。このレベルでは、Malware Analysisサービスでの処理数が、1日あたり100個のファイル サンプルに制限されています。ThreatGrid Cloudに送信されるサンドボックス解析用サンプルの数は1日あたり5件に制限されています。1つのネットワーク セッションに100個のファイルが含まれている場合、1つのネットワーク セッションを処理すると、処理数の制限値に達します。100個のファイルを手動でアップロードした場合でも、処理数の制限値に到達します。
- 標準サブスクリプション: Malware Analysisサービスへの送信回数は無制限です。ThreatGrid Cloudに送信されるサンドボックス解析用サンプルの数は1日あたり1000件まで可能です。

- エンタープライズ サブスクリプション: Malware Analysisサービスへの送信回数は無制限です。ThreatGrid Cloudに送信されるサンドボックス解析用サンプルの数は1日あたり5000件まで可能です。

スコアリング手法

デフォルトでは、IOC(セキュリティ侵害インジケーター) は、業界のベスト プラクティスを反映するように調整されています。解析中に、IOCのスコアによって、サンプルがマルウェアである可能性が示されます。NetWitness Suiteでは、IOCの設定をチューニングでき、マルウェア アナリストは割り当てられたスコアを変更したり、IOCの評価を無効にしたりすることができます。アナリストは、デフォルトの設定を使用するか、特定のニーズに合わせて設定をチューニングするかを柔軟に選択できます。

YARAベースのIOCは、ビルトインのIOCに混合されます。各ビルトイン カテゴリーのIOCとインタリーブされ、ネイティブのIOCと区別されません。[サービス] の[構成]ビューでIOCを表示するとき、管理者は、モジュール選択リストからYARAを選択することで、YARAルールを一覧表示できます。

NetWitness Suiteに格納されたセッションは、セキュリティ侵害インジケータをさらに解析するために、Investigationの表示および解析機能をすべて利用できます。Investigationで表示した場合、YARAのIOCは、`Yara rule.`というタグで、ビルトインのネイティブIOCと区別されます。

導入

Malware Analysisサービスは、個別のRSA Malware Analysisホストとして導入されます。専用Malware Analysisホストには、Coreインフラストラクチャ(他のBrokerやConcentrator) に接続するオンボードのBrokerが搭載されています。この接続の前に、Malware Analysisサービスがデータを取得する元になるConcentratorとBrokerに接続されているDecoderに、必要なParserとFeedを追加する必要があります。 これにより、疑わしいデータ ファイルが抽出用にマークされます。これらのファイルは、RSA Liveコンテンツ管理システムを通じて入手することができ、コンテンツには`malware analysis`というタグが付けられています。

スコア モジュール

RSA NetWitness Suite Malware Analysisでは、ネットワーク、静的解析、コミュニティ、サンドボックスの4つのカテゴリーで、セッションとそのセッション内のファイルを解析し、スコアを計算します。各カテゴリーは、多くのルールやチェックで構成されており、1～100のスコアを計算するために使用されます。スコアが高いほど、悪意のあるセッションである可能性が高くなり、より詳しい追加調査を行う必要があります。

Malware Analysisでは、警告やインシデントに至るまでの一連のイベントの履歴を簡単に調査することができます。ネットワークで特定のタイプのアクティビティが発生していることが分かっている場合は、関連性の高いレポートのみを選択し、データコレクションの内容を調べることができます。スコア カテゴリーやファイル タイプ(Windows PE、PDF、Microsoft Office) に基づいて、各スコア カテゴリーの動作を変更することもできます。

データ ナビゲーションの手法に慣れたら、次のような方法でより詳細にデータを調べることができます。

- 特定のタイプの情報を検索する。
- 特定のコンテンツを詳しく調査する。

ネットワーク、静的解析、コミュニティ、サンドボックスのカテゴリー スコアは、個別に保持およびレポートされます。個別のスコアに基づいてイベントを表示したときに、1つのカテゴリーでマルウェアが検出された場合には、詳細な解析が必要です。

ネットワーク

最初のカテゴリでは、各コア ネットワーク セッションを調査して、マルウェアと疑われるセッションがあるかどうかを判断します。たとえば、既知の安全なサイトから、適切なポートとプロトコルを使用して、通常の(悪意のない)ソフトウェアをダウンロードするアクティビティは、問題なしと見なされます。この条件セットのスコア計算で使用される要素の例として、次のようなセッションがあります。

- 脅威Feed情報に合致するような内容を含んでいる
- 既知の悪質なサイトに接続する
- 高リスクと見なされているドメインや国(.ccドメインなど) に接続する
- 標準以外のポートで既知のプロトコルを使用する
- 難読化されたJavaScriptを含んでいる

静的解析

2番目のカテゴリーでは、実行ファイルが悪意のある動作をする可能性を予測するために、セッション内の各ファイルについて難読化の兆候を解析します。たとえば、ネットワークライブラリにリンクされているソフトェアは、不審なネットワーク アクティビティを実行する可能性が高くなります。この条件セットのスコア計算で使用される要素の例として、次のようなものがあります。

- XORエンコードされていることが検出されたファイル
- EXE以外の形式で組み込まれていることが検出されたファイル(GIF形式で組み込まれていることが検出されたPEファイルなど)
- リスクの高いインポート ライブラリにリンクしているファイル
- PE形式から著しく逸脱しているファイル

コミュニティ

3番目のカテゴリーでは、セキュリティ コミュニティで蓄積されたインテリジェンスに基づいてセッションやファイルのスコアを計算します。たとえば、主要なアンチウイルス(AV) ベンダーによって、フィンガープリントやハッシュが有害か無害かがすでに分かっているファイルは、その情報に従ってスコアが計算されます。また、ファイルのスコア計算では、ファイルの配信元が有害と指定されているか無害とされているかといったセキュリティ コミュニティのインテリジェンスも考慮されます。

コミュニティ スコアは、ユーザ環境のAVソフトウェアがファイルを悪意のあるファイルとしてフラグを設定しているかどうかも示します。ただし、そのAV製品によってシステムが保護されていることを保証するわけではありません。

サンドボックス

4番目のカテゴリーでは、実際にソフトウェアをサンドボックス環境で実行することによって、ソフトウェアの動作を調べます。ソフトウェアを実行してその動作を観察することにより、既知の悪意のあるアクティビティを識別してスコアを計算できます。たとえば、再起動のたびに、自動起動してIRC接続するように自身を構成するソフトウェアは、既知の不正な動作をしないファイルよりもスコアが高くなります。

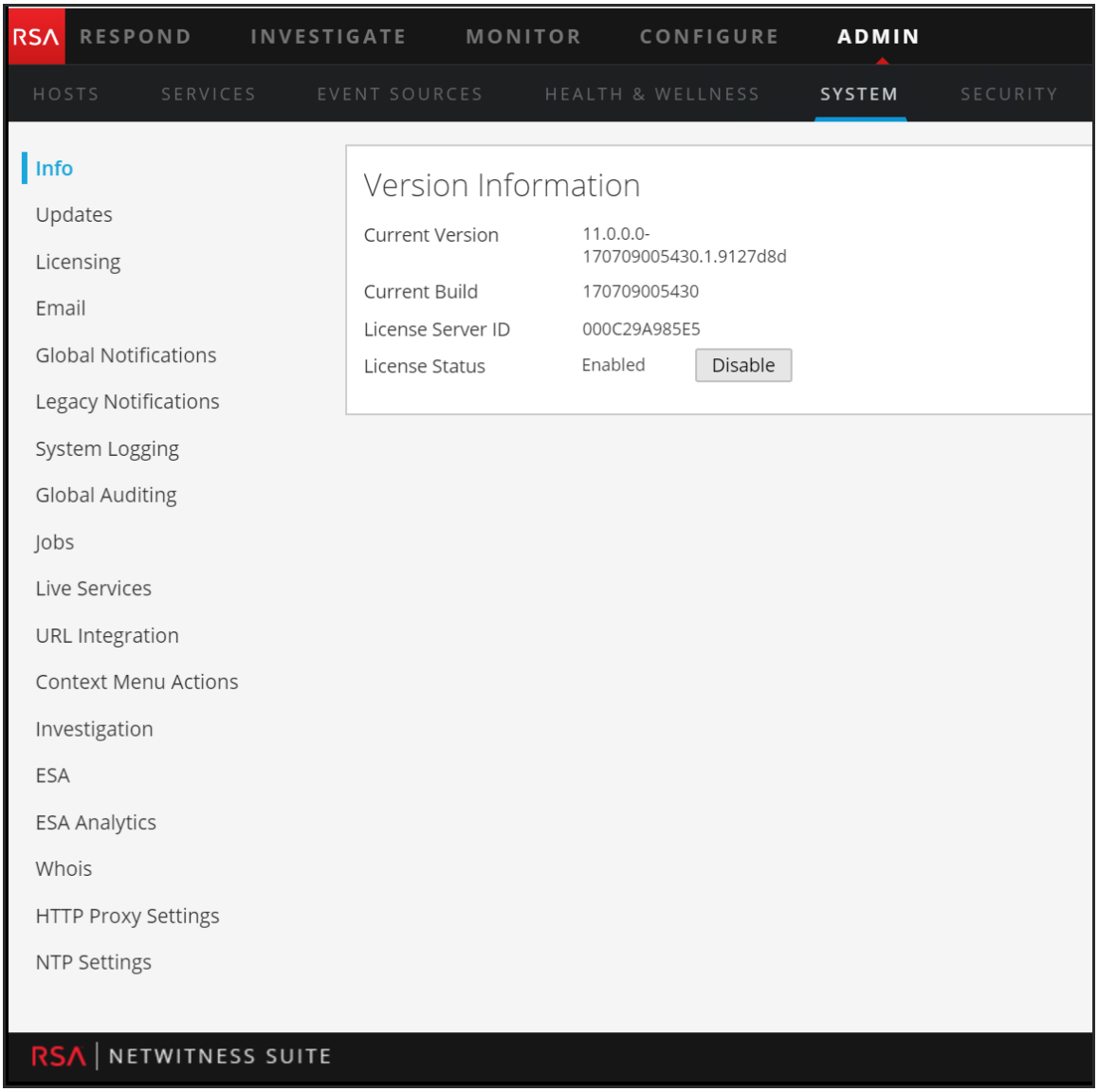
アナリストのロールと権限

このトピックでは、ユーザがNetWitness Suiteでマルウェア解析を実施するために必要なロールと権限について説明します。解析タスクを実行できないか、ビューを表示できない場合、ロールや権限が不足している可能性があります。

必要なロールと権限

RSA NetWitness Suiteでは、ビューや機能へのアクセスを許可する手段として、システムレベルの権限と個々のサービスレベルの権限の両方を使用します。

システムレベルでは、特定のビューや機能にアクセスを許可するシステムロールを[管理]>[システム]ビューでユーザに割り当てる必要があります。



NetWitness Suite 11.0のデフォルトのMalware_Analystsロールには、下に示すすべての権限が割り当てられています。必要に応じて、管理者は、次の権限を組み合わせてカスタムロールを作成できます。

- Investigationモジュールへのアクセス(必須)
- Investigation: イベントの参照
- Investigation: 値の参照
- Incidentモジュールへのアクセス
- インシデントの表示と管理
- マルウェアイベントの表示(イベントを表示する場合)
- ファイルのダウンロード(Malware Analysisサービスからファイルをダウンロードする場合)
- マルウェアスキャンの開始(1回限りのサービススキャンまたは1回限りのファイルアップロードを開始する場合)
- ダッシュレット権限(利便性の向上): ダッシュレット - Investigate 上位の値 ダッシュレット、ダッシュレット - Investigate サービスリスト ダッシュレット、ダッシュレット - Investigate ジョブ ダッシュレット、ダッシュレット - Investage ショートカット ダッシュレット。

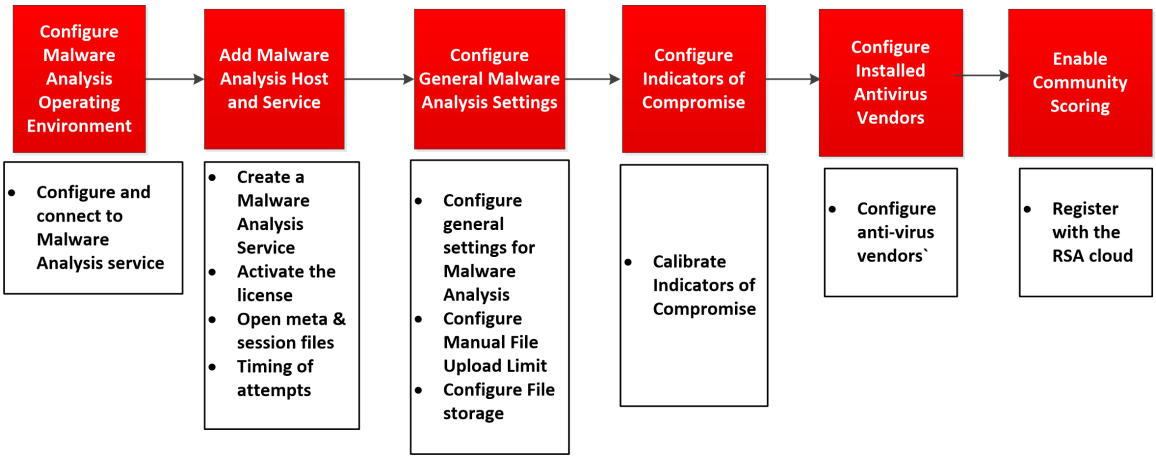
カスタムロールとしてたとえば、ファイルのダウンロード権限を持たないJunior Malware Analystというロールを作成することができます。

特定のサービスに対して、マルウェアアナリストを**Analysts**ロールのメンバーに追加するか、Analystグループに割り当てられる**sdk.meta**と**sdk.content**という2つのデフォルト権限を持つグループに追加する必要があります。この2つの権限を持つユーザは、サービスで解析を行う目的で、特定のアプリケーションの使用、クエリの実行、コンテンツの表示を実行できます。

Malware Analysis構成

Malware Analysisは、Decoder上のサービスまたは専用アプライアンスサービス上のサービスとして動作できます。このガイドでは、動作環境を設定し、次にMalware Analysisサービスを構成する手順について説明します。この構成が完了すると、アナリストがマルウェア解析を実施できるようになります。

Malware Analysisの構成に必要なステップと、既存の構成の変更に必要なステップについて説明します。以降のセクションに示されている順にステップを実行してください。



基本的な構成チェックリスト

次のチェックリストは、「*Hosts and Services Guide*」に従ってNetWitness Suiteに追加されたMalware Analysisを構成するために必要なタスクの順序を示しています。

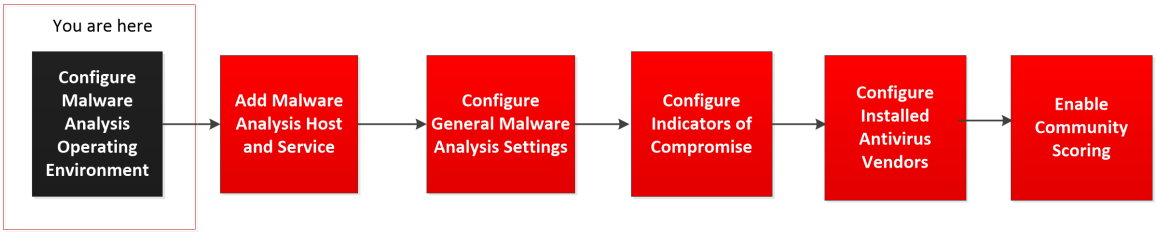
ステップ	タスクの概要
ステップ1.Malware Analysis動作環境の構成	Malware Analysis動作環境の構成 このトピックでは、Malware Analysisサービスに接続するためにの環境を構成する手順について説明します。

ステップ	タスクの概要
ステップ2.Malware Analysisのホストとサービスの追加	Malware Analysisのホストとサービスの追加 **注**:この手順を完了するには、「ライセンスガイド」に示されているNetWitness Suite License Serverの構成ステップを実行します。 NetWitness Suiteで、Malware Analysisサービスを作成し、ライセンスをアクティブ化します。デフォルトのRESTポートは60007です。無料バージョンのMalware Analysisを使用しているサイトでは、サービスのIPアドレスをlocalhostまたはループバックアドレスとして構成する必要があります。
ステップ3.一般的なMalware Analysis設定の構成	一般的なMalware Analysis設定の構成 • 常時スキャン構成を有効にします。 • 手動でのファイルアップロードの制限を構成します。 • ファイルストレージリポジトリとデータベースを構成します。 • 静的、ネットワーク、コミュニティ、サンドボックスの各スコアモジュールを調整します。
ステップ4.セキュリティ侵害インジケータの構成	セキュリティ侵害インジケータの構成 各スコアモジュール(静的、ネットワーク、コミュニティ、サンドボックス)とYARAベースのIOCに適用されるセキュリティ侵害インジケータを調整します。
ステップ5.インストール済みのアンチウイルスソフトベンダーの構成	インストール済みのアンチウイルスソフトベンダーの構成
ステップ6.コミュニティスコアリングの有効化	コミュニティ解析の有効化 RSAクラウドに登録して、コミュニティスコアリングを有効化するための接続をテストします。
ステップ7.Malware Analysisホストの監査の構成	(オプション) Malware Analysisホストの監査の構成 監査の閾値を構成し、Syslog、SNMP、ファイルの監査を有効にします。

ステップ	タスクの概要
ステップ8.ハッシュフィルタの構成	(オプション) ハッシュフィルタの構成 ハッシュフィルタを構成して、既知の無害なファイルハッシュや有害なファイルハッシュに基づいてMalware Analysisイベント解析を微調整します。
ステップ9.Malware Analysisのプロキシ設定の構成	(オプション) Malware Analysisのプロキシ設定の構成 (オプション) RSA Cloudと通信する際に、Webプロキシ経由で接続するようにMalware Analysisを構成します。
ステップ10.ThreatGrid APIキーの登録	(オプション) ThreatGrid APIキーの登録

Malware Analysis動作環境の構成

NetWitness Suite Malware Analysisサービスに接続するNetWitness Suiteオペレーティング環境を構成できます。



Malware Analysisは、Malware Analysis専用アプライアンス上のサービスとして動作します。専用アプライアンスを使用する場合は、次のいずれかのタスクを実行します。

- サイトで新しいNetWitness Suite Malware Analysis専用アプライアンスを追加する場合には、ネットワークに物理アプライアンスをインストールして動作環境を構成します。
- ご使用のサイトでSpectrum専用アプライアンスをNetWitness Suite Malware Analysis専用アプライアンスにアップグレードする場合は、SpectrumアプライアンスをMalware Analysisアプライアンスとして再初期化します。

Malware Analysisは、コアインフラストラクチャと協調して動作します。Malware Analysisで正しくデータを解析するには、次のステップを実行する必要があります。

1. Malware Analysisアプライアンスのオンボード Brokerを、既存のコアインフラストラクチャの別のBrokerまたはConcentratorに接続するように構成します。

注:コア インフラストラクチャが存在しない場合は、手動でアップロードされたファイルのみを解析することができます。

2. NetWitness Suite Liveを使用して、`malware analysis`タグを持つすべてのLiveリソースを検索し、Malware Analysisで解析するトラフィックをキャプチャする各Decoderサービスにこれらのリソースを導入します。NetWitness Suiteは、ParserとFeedのこの独自のセットを使用して、マルウェアの可能性があるイベントを検索します。
3. 通信ポートを構成します。Malware Analysisを実行するには、HTTPS用のTCP/443など、複数の通信ポートが開いている必要があります。これらについては、後述の「ネットワーク接続」セクションで説明します。
4. Malware Analysisが接続する先のNextGenソースを構成します。これはBrokerまたはConcentratorです。
   これで、Malware Analysisを使用してネットワークトラフィックの解析を開始する準備ができました。

ネットワーク接続

Malware Analysisアプライアンスがサービスやソフトウェア アップデートをRSAソースから受信したり、その他の重要な情報を外部と通信したりできるようにしておくために、ネットワーク接続を構成しておく必要があります。

ネットワーク環境のファイアウォールで、Malware Analysisによるインターネットへのアクセスを許可するように構成する必要があります。必要に応じて、プロキシ サーバを使用することもできます。

インバウンド接続

TCP/22:ログ ファイルを調べてトラブルシューティングを行うためのMalware Analysisサーバへの Secure Shellアクセス。アクセスは、Malware Analysisを管理する端末のIPアドレスに制限できます。

- TCP/443:Malware Analysisユーザ インタフェースにアクセスするためのWebベースのHTTPS接続。
- TCP/50008:JVisualVMなどのアプリケーションを使用して、パフォーマンスのトラブルシューティングを行うためのJMXポート。これはオプションです。アクセスは、Malware Analysisを管理する端末のIPアドレスに制限できます。

アウトバウンド接続

- TCP/443:SSLベースのWebサーバへのHTTPS接続。Malware Analysisで解析のためにサーバにファイルやドキュメントを送信する場合など、セキュア接続を必要とする機能で使用されます。Webプロキシ サーバの使用がサポートされています。

- (TCP/443 : Malware AnalysisからRSA CloudへのSSL接続。SOCKSプロキシ サーバの使用がサポートされています。既存のユーザは、cloud.netwitness.comへの接続用に443を開くようにインフラストラクチャの変更が必要になる場合があります) 。
- TCP/50103 : Brokerと通信するために使用されるREST APIポート(NetWitness Suite 10.3.x以前) 。
- TCP/50105 : Concentratorと通信するために使用されるREST APIポート(NetWitness Suite 10.3.x以前) 。
- TCP/50003 TCP/56003 : Brokerと通信するために使用されるポート(NetWitness Suite 10.4以降) 。
- TCP/50005 TCP/56005 : Concentratorと通信するために使用されるポート(NetWitness Suite 10.4以降) 。
- ICMP : ホスト名とIPアドレスが有効かどうかを確認するためのNetWitness SuiteからMalware Analysisサービスへの接続テスト用のJMS接続。

Malware Analysisのホストとサービスの追加

Malware AnalysisのホストとサービスをNetWitness Suiteに追加できます。ご使用のNetWitness Suite環境によって、ホストを追加する方法が決まります。ホストの追加に関する基本的な手順については、「ホストおよびサービス スタート ガイド」の「ホストの追加または更新」を参照してください。このセクションの手順は、Malware Analysisホストを手動で追加する必要がある場合にのみ実行してください。

注 : この手順を完了するには、「ライセンス ガイド」に示されているNetWitness Suite License Serverの構成ステップを実行します。

- Malware Analysisホストは、物理または仮想のMalware Analysisアプライアンスがある場合に追加してください。

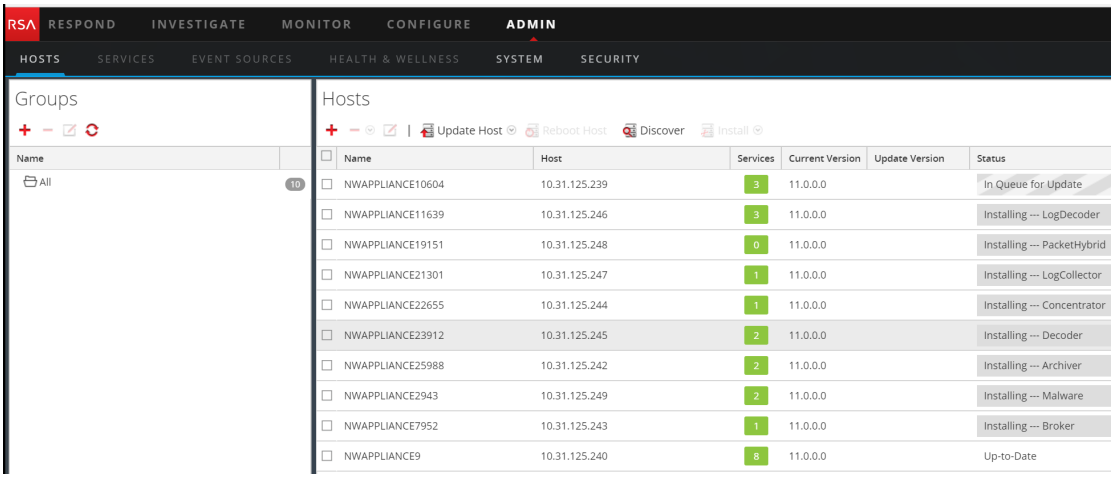
前提条件

ホストまたはサービスをNetWitness Suiteに追加するには、NetWitness Suiteインスタンスのインストールと構成が完了し、サービスが実行されている必要があります。

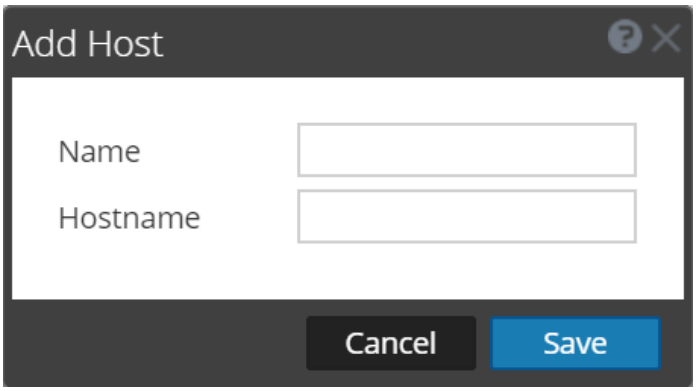
処理手順

NetWitness SuiteにMalware Analysisホストを手動で追加するには、次の手順に従います。

1. NetWitness Suiteにログインします。
2. メイン メニューで、**[管理]＞[ホスト]**を選択します。[管理]＞[ホスト]ビューが表示されます。

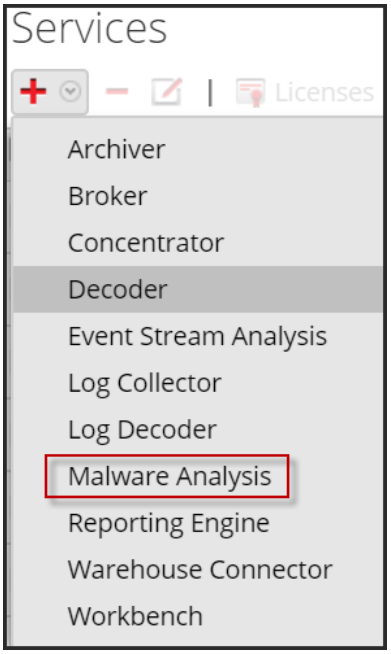


3. [ホスト]パネルのツールバーで  をクリックします。
[ホストの追加]ダイアログが表示されます。



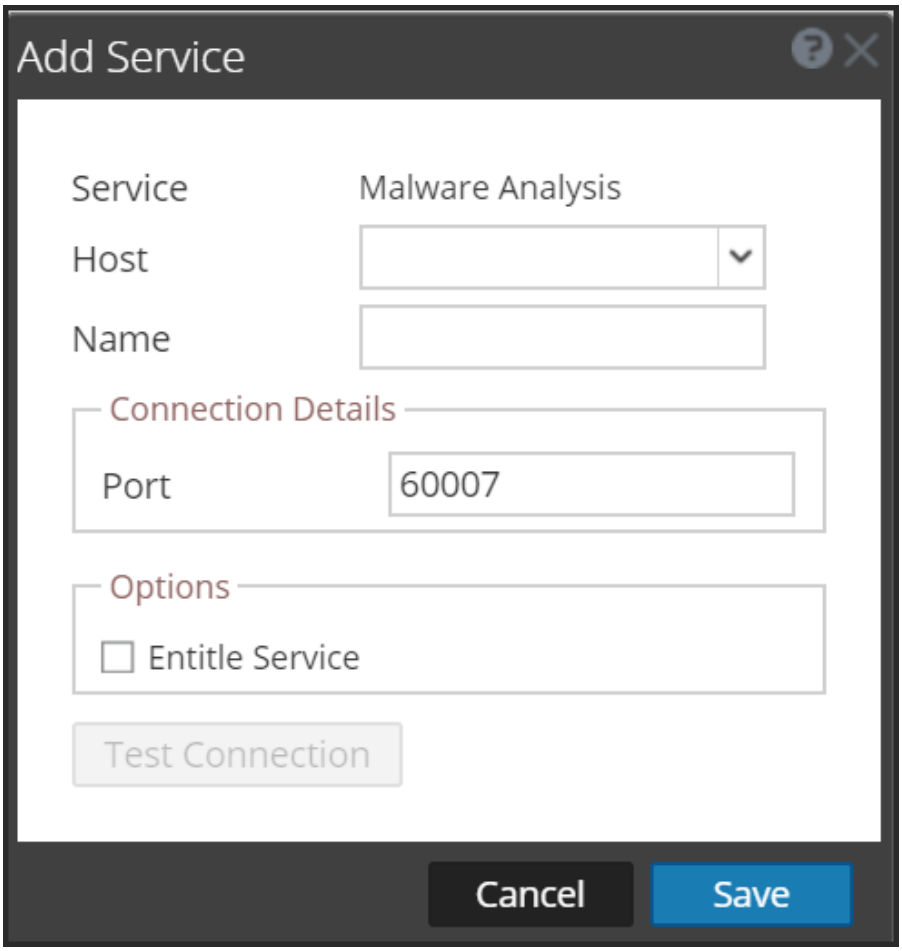
4. [**名前**]フィールドに、Malware Analysisホストの名前を入力します。[**ホスト名**]フィールドで、Malware Analysisのホスト名、仮想IPアドレス、IPアドレスのいずれかを入力します。[**保存**]をクリックします。
5. ツールバーで[**サービス**]を選択します。

6. [**サービス**]パネルのツールバーで  をクリックします。使用可能なサービスのドロップダウンリストが表示されたら、[**Malware Analysis**]を選択します。



[サービスの追加]ダイアログが、サービスタイプMalware Analysisとともに表示されます。

7. 次の情報を入力します。
[**名前**]フィールドに、Malware Analysisサービスの名前を入力します。
[**ホスト**]フィールドで、Malware Analysisのホスト名、仮想IPアドレス、IPアドレスのいずれかを入力します。
[**ポート**]フィールドに「**60007**」を入力します。
(オプション) [**オプション**]の[**サービスのエンタイトルメント**]を選択します。

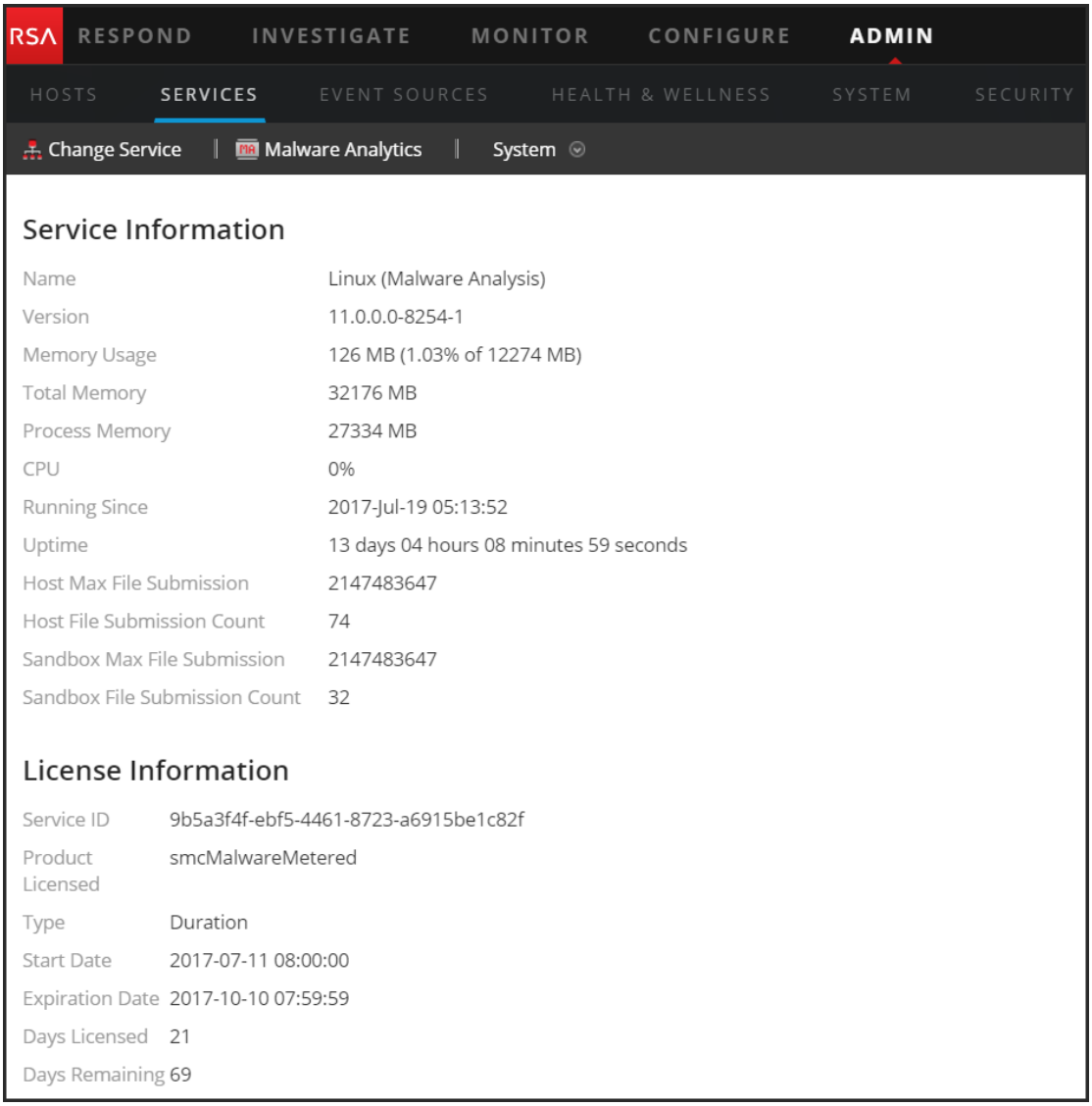


8. [**接続のテスト**]をクリックします。

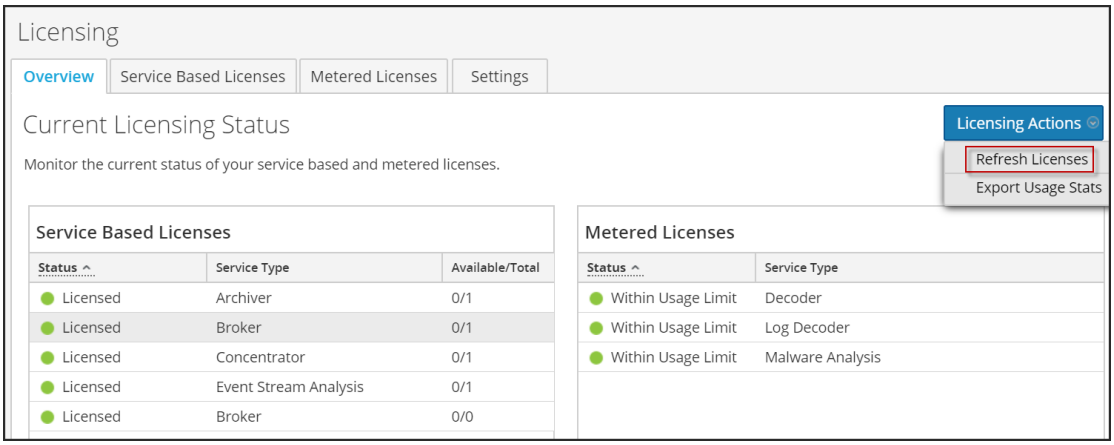
   サービスの追加中に、NetWitness SuiteによってICMPパケットがサービスに送信され、入力したホスト名またはIPアドレスへの接続が有効であるかどうかが検証されます。テストの結果が[サービスの追加]ダイアログに表示されます。テストが失敗した場合は、サービスの情報を編集し、再試行します。

9. テストに成功したら、[**保存**]をクリックします。[サービスの追加]ダイアログが閉じ、NetWitness SuiteでMalware Analysisサービスが使用可能になります。(オプション) Malware Analysisサービスのステータスを確認します。[管理]の[サービス]ビューからMalware Analysisサービスを選択し、[**表示**]>[**システム**]を選択します。次の図は、Malware

Analysisサービスの情報の例です。

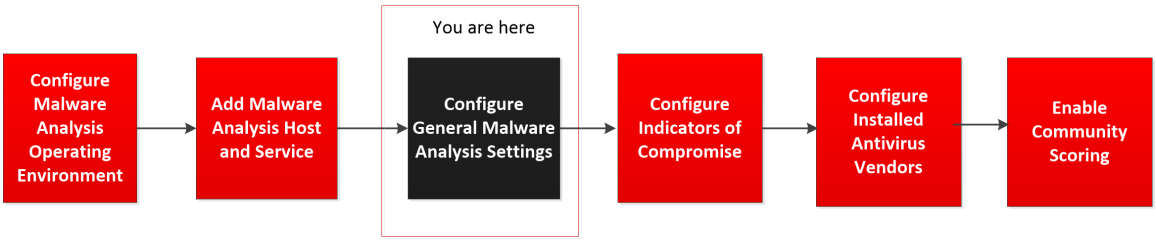


サービスがライセンスされていない場合は、[管理]＞[システム]＞[ライセンス]パネルに移動し、[**ライセンス アクション**]メニューで[**ライセンスの更新**]を選択します。



一般的なMalware Analysis設定の構成

セッションの解析、手動でのファイルアップロード、およびMalware Analysisが使用するさまざまなスコアモジュールを有効化し、調整するために必要ないくつかの基本的な設定を構成できます。



また、データリポジトリによるファイル共有も設定できます。Malware Analysisでは、セッションやファイルの解析に関する3つのモードがあります。3つの選択肢を組み合わせて使用することによって、Malware Analysisでの解析を実行できます。選択項目は次のとおりです。

- **コアサービスの常時ポーリング**: コアサービスの常時ポーリングを有効化および構成できます。有効化および構成すると、Malware Analysisは、コアサービスで要解析のタグが付けられたセッションを常時ポーリングします。デフォルトでは常時ポーリングは無効化されています。常時ポーリング中に使用するDOS(Denial of Service) 攻撃防止を有効化できます。[統合]タブ内のオプションを使用して常時ポーリングしているMalware Analysisサービスへの接続をテストできます。

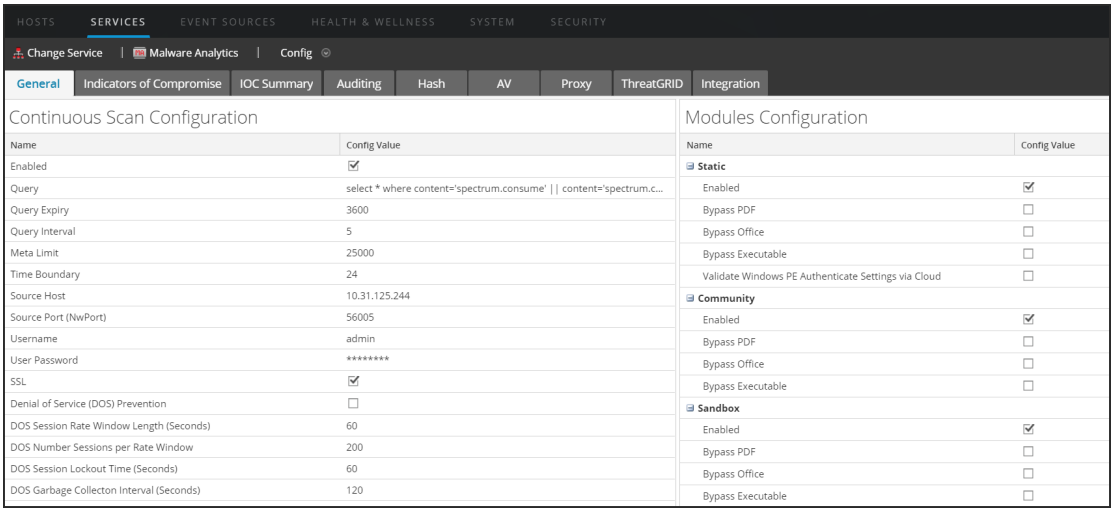
> **注**: 10.3.5以前のMalware Analysisでコアサービスを常時ポーリングのサービスとして追加する場合は、RESTポートを使用します。たとえば、ネイティブのNexGenポート(50005) ではなくRESTポート(50105) を使用して、10.3.5のMalware AnalysisにConcentratorを追加します。

- **コア サービスのオン デマンド解析**：NetWitness Suiteの調査モジュールから直接、セッションを解析できます。この方法では、Coreセッションを手動で制御し、セッションに含まれるファイルの処理方法(サンドボックスに送信するなど)をより細かく制御できます。解析するファイルのタイプごとに、特定のオプションを指定して、コミュニティやサンドボックスでの解析処理に送信できます。
- **手動でのファイルのアップロード**：ローカルやネットワークのディレクトリにあるファイルを手動でアップロードし、解析することができます。アップロードできるファイルの最大サイズを構成できます。

基本設定の表示

基本設定を表示するには、次の手順を実行します。

1. **メイン メニュー**で、[**管理**]＞[**サービス**]を選択します。
2. [**サービス**]グリッドで、Malware Analysisサービスを選択し、  ＞[**表示**]＞[**構成**]を選択します。
   [**全般**]タブが開いた状態で、サービスに対する[サービス]の[構成]が表示されます。



常時スキャンの構成

標準的なサブスクリプションのオプションでは、Malware Analysisのファイル処理数は制限されており、サンドボックス処理のためにThreatGrid Cloudに送信できるファイル数は1日あたり1,000個までです。サンドボックスの使用を最適化するため、Malware Analysis構成では、複数の使用方法からMalware Analysisで使うものを選択できます。常時ポーリングを有効または無効に設定できます。

常時ポーリングを構成する際の考慮点は、DOS防止(Denial of Service (DOS) Prevention)パラメータです。デフォルトではこの機能は無効になっています。この機能を有効にする前に、ご使用の環境の設定を慎重に検討する必要があります。

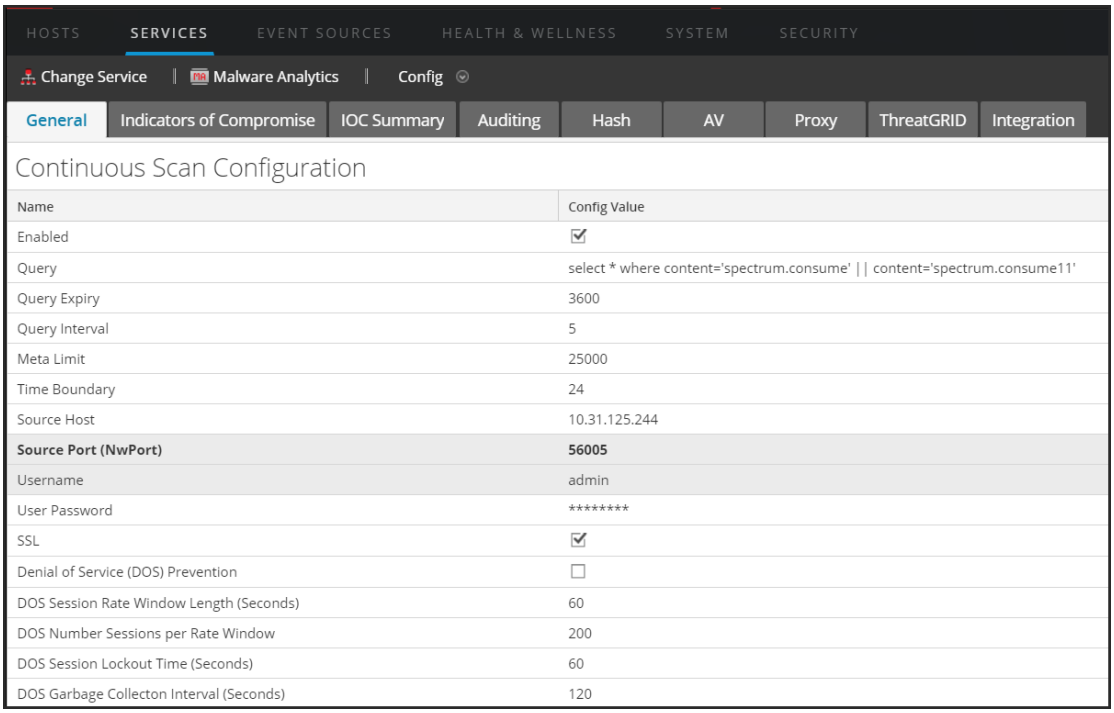
DOS防止が無効になっている場合、Malware Analysisは先入れ先出し方式でキューに入れられたセッションを解析します。DOS攻撃によって急激にキューがいっぱいになり、Malware Analysisがセッションの処理でビジー状態となっている間に、その後のセッションでマルウェア攻撃が発生していることがあります。後のセッション(実際の攻撃)がキューの先頭に到達せず、攻撃が開始されるまで解析されないことがあります。

DOS防止を有効にすると、Malware Analysisは、単一のIPアドレスからのセッションが多すぎる場合にそれをDOS攻撃として処理します。IPアドレスが[レート ウィンドウあたりのDOSセッション数]を超える場合、Malware Analysisは、[DOSセッションのロックアウト時間(秒)]に達するまで、そのアドレスからのセッションを無視します。その後、Malware AnalysisはそのIPアドレスからのセッションの解析を再開します。そのIPアドレスからの無視されたセッションはまったく解析されないため、セッションのロックアウト期間中にマルウェア攻撃がすり抜ける可能性があります。

[DOS Garbage Collection Interval (Seconds)]設定を使用して、Malware Analysisは、指定された秒数後にIPソースのメモリ内ストレージをクリアします。この間隔でアクティビティのほとんどないIPアドレスはメモリからクリアされます。IPアドレスが[DOS Garbage Collection Interval (Seconds)]以上の間隔でアクティブな状態になる場合、Malware AnalysisはそれをDOS攻撃として識別しないことがあります。

Malware Analysisで常時ポーリングを構成するには、[常時スキャン構成]セクションで次の手順を実行します。

1. [**管理**]で[**サービス**]をクリックします。
2. [**全般**]タブの[**常時スキャン構成**]で、常時ポーリングを構成できます。



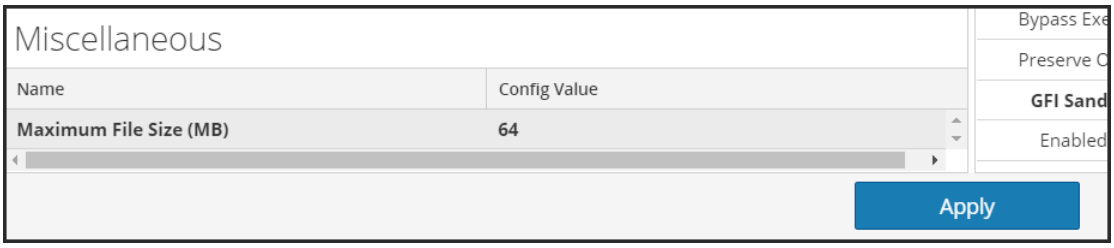
3. 常時ポーリングを有効にするには、[**有効**]をクリックします。

4. (オプション) クエリのデフォルト値を変更する場合は、[**Query Expiry**]、[**Query Interval**]、[**Meta Limit**]、[**Time Boundary**]に新しい値を入力します。
5. Malware AnalysisがMalware Analysisアプライアンスにクエリを実行して解析用のデータを取得できるよう構成するには[**ソース ホスト**]および[**ソース ポート(NwPort)**]を指定します。
6. (オプション) Malware Analysisアプライアンスのデフォルトのログオン認証情報を変更する場合は、[**Username**]と[**User Password**]を指定します。
7. Malware Analysisアプライアンスとコア サービスの間の通信にSSLを使用する場合は、[**SSL**]を有効化します。
8. (オプション) DOS(Denial of Service) 防止機能を構成するには、次の操作を行います。
   a. [**Denial of Service (DOS) Prevention**]パラメータを有効化します。
   b. DOS防止のためのセッション制限を設定します。
      - Malware Analysisが単一のIPアドレスのセッションをカウントするタイム ウィンドウの秒数([**DOS Session Rate Window Length**]) を指定します。このウィンドウはレート ウィンドウと呼ばれ、該当するIPソースから最初のセッションを受信したときにカウンターが設定されます。デフォルト値は60秒です。
      - [**DOS Number Sessions per Rate Window**]に、レート ウィンドウあたり許可されるセッションの数を指定します。デフォルト値は200セッションです。レート ウィンドウ内でセッション数が上限に達したとき、Malware AnalysisはそのIPアドレスからのセッションを無視します。そのIPからのセッションはまったく解析されません。Malware Analysisは、ロックアウト時間が終了するまでセッションを無視し続けます。
      - [**DOS Session Lockout Time (Seconds)**]にロックアウト時間(この間に該当IPアドレスからのセッションは無視され、解析もされません) を指定します。デフォルト値は60秒です。ロックアウト時間を経過すると、Malware AnalysisはそのIPアドレスからのセッションの解析を再開します。
      - [**DOS Garbage Collecton Interval (Seconds)**]に、NetWitness SuiteがIPソースのメモリ内オブジェクトを削除するまでの、IPアドレスの非アクティブ間隔を指定します。デフォルト値は120秒です。
9. [**適用**]をクリックして変更を適用します。
   変更は、Malware Analysisが新しいパケットを受け取るとすぐに有効となります。
10. 選択したコア サービスへのMalware Analysisサービスの接続をテストするには、[**統合**]タブの[**常時スキャンの接続テスト**]セクションの[**接続のテスト**]ボタンをクリックします。

手動でのファイルアップロードの構成

手動でのファイルアップロードの最大ファイルサイズを構成するには、次の操作を行います。

1. [その他]セクションで、Malware Analysisスキャン用に手動でアップロードできるファイルの最大サイズをMB単位で入力します。



2. [**適用**]をクリックします。
   変更はすぐに有効となります。

データリポジトリの構成

Malware Analysisでは、アプライアンスに格納できるファイル数に制限があります。データリポジトリの構成では、ファイルシステムの保存期間は60日間です。この設定によって、ファイルがMalware Analysisアプライアンスに保存される期間が決まります。古いファイルが削除された場合、リカバリすることはできません。Malware Analysisは毎日、ファイルシステムの保存期間を過ぎたファイルを削除し、ディスク領域を圧迫しないようにしています。

ファイルを定期的に削除するため設定は、ファイルシステムの保存期間だけです。使用されているディスク領域の容量に基づいて削除されるわけではありません。この設定を変更する必要がある場合、管理者は、指定された保存日数の間に予想されるディスク領域の使用量に基づいて、保存期間を構成する必要があります。

NetWitness Suiteユーザインタフェースで表示できるデータリポジトリのパラメータは次のとおりです。

- リポジトリの場所は**/var/lib/netwitness/malware-analytics-server/spectrum**です。この値は編集しないでください。
- ファイル共有プロトコル。[File Sharing Protocol]で指定するプロトコルによるアクセスを許可し、Malware Analysisサービスからファイルをコピーできるようにします。
- ファイル保存期間(日数)。

ファイル共有を構成するには、[リポジトリ構成]セクションで次の手順を実行します。

1. [ファイル共有プロトコル]をクリックし、[FTP]または[SAMBA]を選択します。
2. ファイルが削除される前にリポジトリに保持される日数を指定します。
3. [**適用**]をクリックします。

変更はすぐに有効となります。

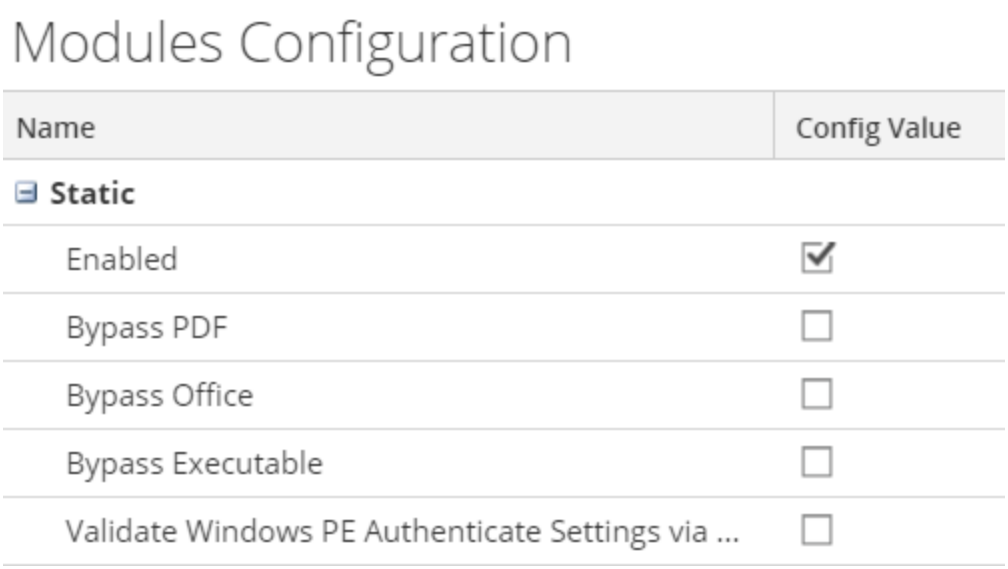
スコアモジュールの調整

[モジュール構成]セクションではMalware Analysisのコンポーネントを次のように構成できます。

- 3つのスコアモジュール(静的(Static)、コミュニティ(Community)、サンドボックス(Sandbbox))のいずれかまたはすべてを完全に無効にします。スコアモジュールを無効または有効にする場合には、各スコアモジュールが検出する対象を良く理解してから行うようにしてください。
- Malware Analysisは、Microsoft Office、Windows PE、PDFの各ファイルを含むセッションに、Malware Analysisサービスで調査するためのタグを付けます。Malware Analysisで、Windows PE、Microsoft Office、PDFドキュメントを完全に無視するように構成できます。必要に応じて、コアの設定を調整してこれらのファイルを無視するように設定します。これにより、Malware Analysisでの調査対象のタグが付けられなくなります。

スコアモジュール調整の適用例を次に示します。ルールグループを設定したり、システムパフォーマンスを解析したりする場合に、PDFドキュメントは解析せずに、Microsoft OfficeとWindows PEドキュメントは解析するなど、さまざまなシナリオをテストできます。このシナリオを3つのスコアモジュールのそれぞれでテストできます。テストの結果、システムパフォーマンスが向上した場合は、それらの情報や経験を活用できます。

静的解析のスコアの構成



静的(Static)解析のスコアを構成するには、[**モジュール構成**]セクションで次の手順を実行します。

1. デフォルトでは、静的解析モジュールは有効になっています。静的(Static)解析をすべて有効または無効にするには、[**Enabled**]チェックボックスで設定します。

2. セッションでPDF、Microsoft Office、Windows PEのファイルの解析を構成するには、[**PDFのバイパス**]、[**Offoceのバイパス**]、[**実行プログラムのバイパス**]のチェックボックスのいずれかを選択します。
3. デジタル署名されたWindows PEファイルのAuthenticode検証に対するユーザ環境設定を構成するには、[**クラウド経由のWindows PE認証設定の検証**]チェックボックスをオンにします。デジタル署名されたWindows PEファイルが検証のためにRSA Cloudに送信されないようにする場合は、このチェックボックスをオフにします。
   無効化した場合、(Authenticode検証をスキップして)すべての静的解析がローカルで実行されます。この設定に関係なく、PDFドキュメントとMS Officeドキュメントは Authenticode検証の対象ではないため、静的解析の実行中にネットワーク通信が行われることはありません。
4. [**適用**]をクリックします。変更はすぐに反映されるため、Malware Analysisが新しいパケットを受けとった時から有効になっています。

コミュニティ解析のスコアの構成

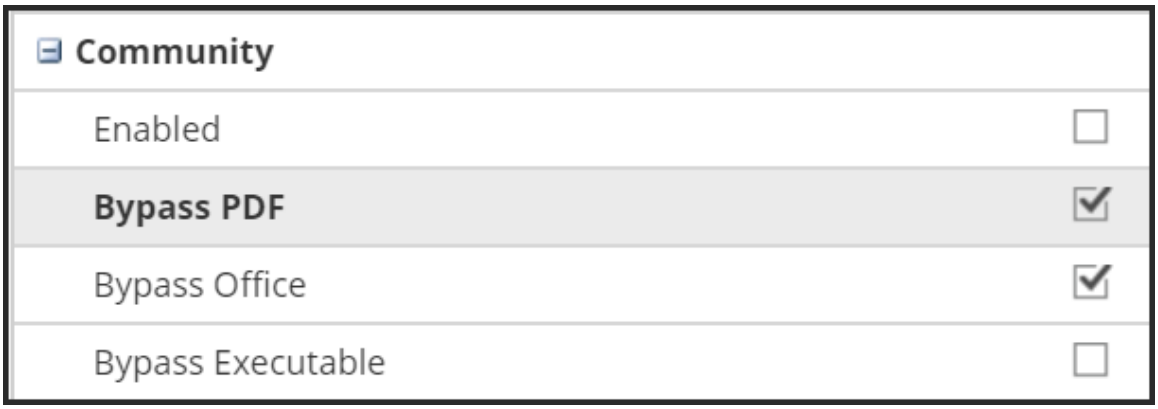
コミュニティ(Community)モジュールを有効にすると、セキュリティコミュニティでは、処理が可能なタイプのすべてのドキュメントを解析します。これは、ネットワーク セッションとファイルの属性を、RSA Cloudに送信することによって実現されます。RSA Cloudは、情報を処理するために、必要に応じて、セキュリティコミュニティ パートナーへの外部接続を行う場合があります。

ファイルのコンテンツが解析のためにコミュニティに送信されることはありません。その代わりに、ファイルのMD5/SHA-1ハッシュが送信され、アンチウイルスソフトを使用した検出とブラックリストへの登録に使用されます。同様に、この処理の一環として、セッション メタ情報も取得および解析されます。URLやドメイン名などのメタ要素が調べられ、既知の不正なURL/ドメインなどを識別するためにRSA Cloudに送信されます。

コミュニティ解析を有効にして、処理するドキュメント タイプを制限できます。ファイルのコンテンツ(ハッシュを除く)がネットワークの外部に送信されるリスクはありません。

注:処理が行われるRSA Cloudへのアクセスを取得するには、Malware Analysisサービスを RSAカスタマ サービスに登録する必要があります。これを行うには、[統合]タブ内のオプションを使用するか、またはRSA Customer Careに連絡する、という2つの方法があります。

コミュニティ(Community)解析のスコアを構成するには、[モジュール構成]セクションで次の手順を実行します。



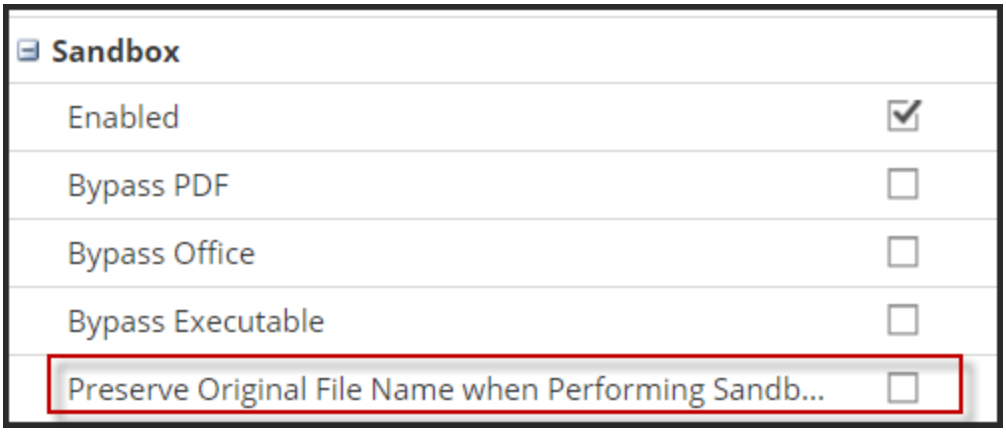
1. コミュニティ(Community)解析をすべて有効または無効にするには、[**Enabled**]チェックボックスで設定します。デフォルト値は、[**無効**]です。
2. セッションでPDF、Microsoft Office、Windows PEのファイルの解析を構成するには、[**PDFのバイパス**]、[**Offoceのバイパス**]、[**実行プログラムのバイパス**]の3種類のチェックボックスのいずれかを選択します。
3. [**適用**]をクリックして変更を保存するとすぐに反映され、Malware Analysisが新しいパケットを受信した時から変更が有効になっています。

サンドボックス解析のスコアの構成

デフォルトでは、サンドボックスモジュールは無効になっており、MS OfficeファイルとPDFファイルは処理されません。その目的は、外部のネットワークに機微情報を送信するかどうかをユーザが指定するようにするためです。ドキュメントタイプの処理が除外されていない場合、(ハッシュだけではなく)ファイル全体が宛先のサンドボックスサーバに送信されます。

加えて、サンドボックス解析を実行するときに元のファイル名を保存することを選択できます。

注:[**サンドボックス解析の実行時に元のファイル名を保持**]パラメータを指定しない場合、NetWitness Suiteはファイルをハッシュ化します。



サンドボックス モジュールを有効にする場合、サンドボックスの処理で、ローカルのGFI Sandbox、ローカルのThreatGrid Sandbox、またはCloudバージョンのThreatGrid Sandboxのいずれかを指定する必要があります。CloudバージョンのThreatGrid Sandboxは、ThreatGridによって直接提供されます。アクティベーション キーをThreatGridから取得し、[ThreatGRID]タブで構成します。

GFI Sandbox設定

ローカルにインストールされたGFI Sandboxを使用するには、GFIを有効にし、GFI Sandboxサーバのサーバ名とサーバ ポートを指定する必要があります。[最大ポーリング期間]と[ポーリング間隔]によって、送信したサンプルの処理が終了するのを待機する時間と、ステータスを確認する頻度(秒単位)を指定します。[Webプロキシ設定を無視]オプションを選択することにより、サンドボックスに接続するときにMalware AnalysisにWebプロキシ設定をバイパスするように設定することができます。Malware AnalysisでWebプロキシが構成されていない場合、この設定は無視されます。

GFI Sandbox (Local)	
Enabled	☐
Server Name	localhost
Server Port	80
Max Poll Period	1800
Ignore Web Proxy Settings	☐

ThreatGrid Sandbox設定

注: ThreatGridのスコアを有効にする場合には、このサイトから送信されたサンプルがThreatGridによって正当と認識されるようにするため、ThreatGridから提供されたサービス キーを構成する必要があります。NetWitness Suiteを使用してThreatGrid APIキーを登録してから、ローカルにインストールされたThreatGrid SandboxまたはThreatGrid Cloud Sandboxを有効化して構成できます。次の詳細タスクを参照してください。ThreatGrid APIキーの登録

[Webプロキシ設定を無視]を選択することにより、サンドボックスに接続するときにMalware AnalysisにWebプロキシ設定をバイパスするように設定することができます。Malware AnalysisでWebプロキシが構成されていない場合、この設定は無視されます。

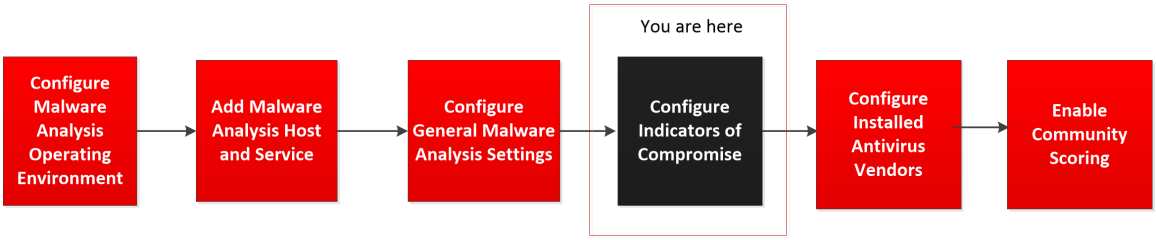
サンドボックスのスコアを構成するには、[モジュール構成]セクションで次の手順を実行します。

1. サンドボックス解析をすべて有効または無効にするには、[**有効**]チェックボックスで設定します。デフォルト値は、[**無効**]です。

2. セッションでPDF、Microsoft Office、Windows PEのファイルの解析を構成するには、[**PDFのバイパス**]、[**Offoceのバイパス**]、[**実行プログラムのバイパス**]の3種類のチェックボックスのいずれかを選択します。
3. 有効なサンドボックス ベンダーを構成します。3つのオプションが用意されています。
   a. ローカルにインストールされたGFI Sandboxのインスタンスを使用するには、GFI Sandboxサーバのサーバ名とサーバ ポート、[最大ポーリング期間]と[ポーリング間隔]を指定し、オプションで[Webプロキシ設定を無視]チェックボックスをオンにします。
   b. ローカルにインストールされたThreatGridのインスタンスを使用するには、ThreatGridスコアを有効にして、ThreatGridサービス キーを指定し、必要に応じて[Ignore Web Proxy Settings]チェックボックスをオンにします。
   c. ThreatGrid Cloudを使用するには、まずThreatGrid APIキーを登録する必要があります。その後でThreatGridスコアを有効化して、ThreatGridサービス キーを指定し、ThreatGridサーバのURL(https://panacea.threatgrid.com) を入力します。必要に応じて、[Webプロキシ設定を無視]チェックボックスをオンにします。
4. [**適用**]をクリックします。
   変更はすぐに有効となります。

セキュリティ侵害インジケータの構成

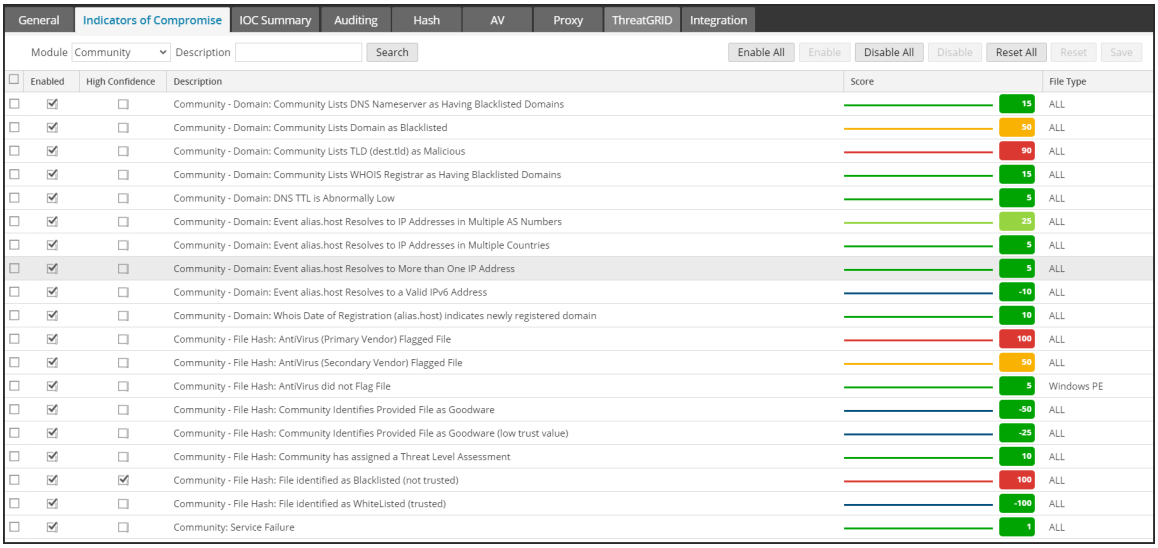
Malware Analysisスコア モジュールのIOC(セキュリティ侵害インジケータ) はすでに構成されています。なぜなら、Malware Analysisの各スコア モジュール(ネットワーク(Network) 、静的(Static) 、コミュニティ(Community) 、サンドボックス(Sandbox) 、YARAには、デフォルトのIOC(セキュリティ侵害インジケータ) が用意されており、マルウェアの可能性を調査する際に使用されるためです。



各IOCには、-100(無害) ～100(有害) の数値による加重スコアが割り当てられます。IOCがトリガーされると、数値スコアの加重が、解析されるセッションやファイルの合計スコアの計算で考慮されます。該当するすべてのIOCに対する個々のスコアの加重が集計され、各セッションやファイルの最終的なスコアが生成されます。集計されたスコアは、有効なスコアの範囲(-100～100) を超えないように調整されます。

注：IOCに割り当てられるスコアの加重は、常に明示的なスコア値として集計されるわけではありません(トリガーされる各IOCのスコアの加重を単純に加算したものではありません)。IOCのスコアは重要度の加重またはインジケータであり、全体的なスコアの計算で考慮されます。

Malware Analysis用のIOC(セキュリティ侵害インジケータ)の構成設定は、サービスの[構成]ビュー>[セキュリティ侵害インジケータ]タブにあります。以下は、タブの例です。



[**コミュニティ(Community)-ファイル ハッシュ: AntiVirus (Primary Vendor) Flagged File**た]というIOCを例とした場合、IOCのスコアの加重は100に設定できます。ただし、Malware Analysisでは、サンプルを悪意のあるファイルと見なしているプライマリAVベンダーの割合に基づいて、この値を調整します。サンプルを悪意のあるファイルと見なしているベンダーが100%に近くなるほど、スコアの集計時に使用される値が100ポイントに近づきます。割合が下がって0%に近づくと、スコアの集計で使用される100ポイントに対する比率が下がります。

IOCでは、Malware Analysisでネイティブ実装されているロジックを使用します。ロジックを調整することはできません。IOCの調整では、スコアに対するインパクトの増減、信頼性設定の指定、IOCのオンとオフの切り替えのみ行うことができます。標準的なシナリオでは、最終的なスコアを押し上げて偽陽性(false positive)の解析結果の原因となっているIOCについて、限定的にIOCスコアの加重値を下げるように調整します。IOCが一貫して継続的に偽陽性の結果の原因となっている場合は、そのIOC全体を無効にするという極端な調整を行うこともあります。さらに、すべてのIOCを無効にしてから、いくつかを選択して有効にしておくという対応もできます。たとえば、アンチウイルスソフトでの一致を検出した一部のIOCを除き、すべてのIOCを無効にすることができます。このような極端に限定された構成でMalware Analysisを使用して、Malware Analysisで既知のアンチウイルスソフトに一致する結果のみが生成されるようにして、結果を削減することもできます。

この機能は、いくつかの構成オプションがあります。

- IOCを無効にして、IOCが割り当て先のスコア モジュールの一部として評価されないようにします。

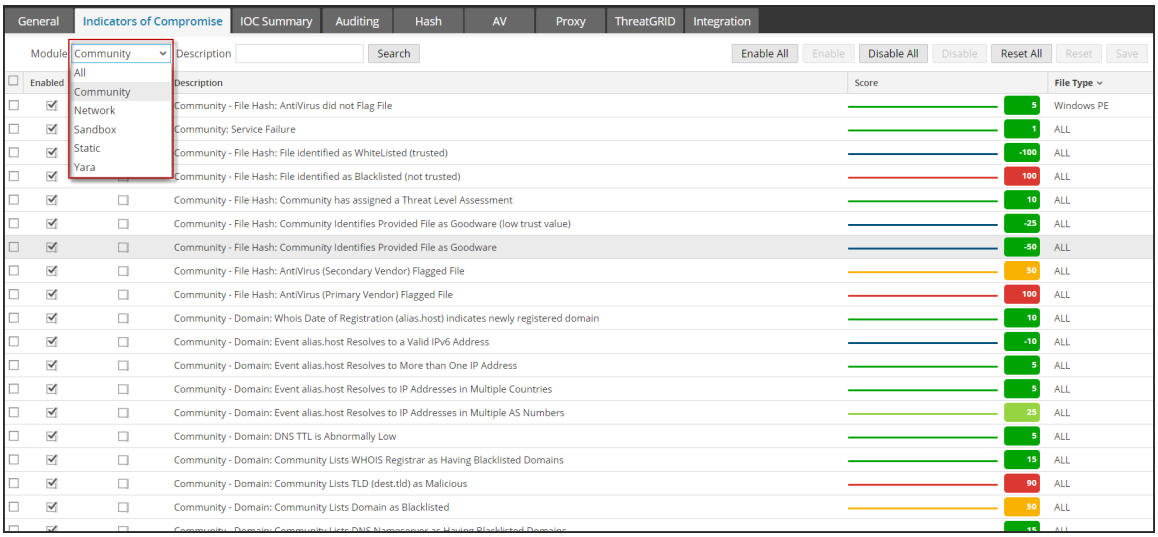
- IOCのスコアの加重を調整し、集計されるスコアに対するインパクトを調整します。
- マルウェアの強力な兆候であると判断されるIOCをマークし、Malware Analysisの結果で、これらのIOCをトリガーしたセッションにHC(高確率)フラグを表示します。
- 解析されるファイルタイプごとにスコアや信頼性の設定をカスタマイズします。各IOCには、適用先のファイルタイプがあらかじめ割り当てられています。値は、**ALL**、**PDF**、**MS Office**、**Windows PE**のいずれかです。ファイルベースの解析では、最も類似するファイルタイプが割り当てられたIOCが使用されます。たとえば、PDFを解析する場合は、同じIOCでもファイルタイプが[**ALL**]に設定されたIOCよりも、ファイルタイプが[**PDF**]に設定されたIOCの方が選択されます。ファイルタイプに一致するものが見つからない場合は、ファイルタイプが[**ALL**]に設定されたIOCが選択されます。
- ルールの説明を検索して、グリッドに結果を表示できます。

表示されたIOCのモジュールによるフィルタ

表示されたIOCをスコアモジュールでフィルタリングすることができます。4つのビルトインモジュールのいずれか、またはYARAを指定できます。YARAベースのIOCは、各カテゴリのネイティブIOCによってインターリーブされます。YARA IOCは他のビューでは識別されませんが、モジュール選択リストからYARAを選択してYARAルールのリストを参照できます。

4個のスコアモジュールまたはYARAに対してIOCを表示するには、次の手順を実行します。

1. **メインメニュー**で、[**管理**]>[**サービス**]を選択します。
2. Malware Analysisサービスを選択します。
3.  >[**表示**]>[**構成**]を選択します。
4. [**セキュリティ侵害インジケータ**]タブをクリックします。
5. [**モジュール**]選択リストで、All、NextGen、Static、Community、Sandbox、Yaraのいずれかを選択します。
   モジュールに対して構成されたルールおよび設定が表示されます。



表示したモジュールで変更済みモジュールのみを示すフィルタ

[**セキュリティ侵害インジケータ**]タブでは、ローカルで変更されたIOCを視覚的に識別できます。IOCが変更されたとき、たとえば、スコアの荷重が変更されたときに、名前は赤で表示され、IOC名に変更マークが付きます。変更マークは++で表示され、IOCを検索するときにフィルタすることができます。
ローカルで変更したIOCのみ表示するには、次の手順を実行します。

1. [**説明**]フィールドに「++」を入力します。
2. [**検索**]をクリックします。
   ビューがフィルタリングされ、変更したIOCのみが表示されます。

スコアモジュールでのIOCの有効化と無効化

IOCが無効である場合、そのIOCは属しているスコアモジュールの集計には影響しなくなります。IOCに複数のインスタンス(ファイルタイプだけが異なる)がある場合、特定のファイルタイプに固有のIOCを無効にすると、同じIOCでそのファイルタイプに依存しないIOCがスコアの計算に使用されます。
たとえば、ファイルタイプが[**ALL**]と[**Windows PE**]である同じIOCがある場合、このIOCの[**Windows PE**]のインスタンスを無効にすると、[**ALL**]のインスタンスのIOCがスコアの計算に使用されます。**Windows PE**についてはIOC全体を無効にし、他のファイルタイプについてはIOCを有効のままにするには、後で示すように、IOCの[**Windows PE**]インスタンスのスコアの加重値を0に設定します。これによって、Windows PEファイルについてIOCは有効のままですが(ただし、加重は0であるため、解析結果には表示されません)、他のファイルタイプには影響しません。残りのファイルタイプでは、引き続きIOCの[**すべて**]のインスタンスが使用されます。

IOCを有効または無効にして、スコアモジュールでの計算に使用されないようにするには、次の手順を実行します。

1. **メイン メニュー**で、**[管理]＞[サービス]**を選択します。
2. Malware Analysisサービスを選択し、その行の  ＞**[表示]＞[構成]**を選択します。
3. [**セキュリティ侵害インジケータ**]タブをクリックします。
4. [**モジュール**]選択リストで、All、Community、Network、Sandbox、Static、またはYaraのいずれかのスコア モジュールを選択します。
   モジュールに対して構成されたルールおよび設定が表示されます。
5. 次のいずれかを実行します。
   a. 有効にするルールの選択チェックボックスをオンにします。
   b. 1つ以上のルールを選択し、ツールバーの[**有効化**]または[**無効化**]をクリックします。
   c. ページに表示されているすべてのルールの有効と無効を切り替えるには、列タイトルの[**有効**]チェックボックスをクリックします。
   d. スコア モジュールのすべてのルールを有効または無効にするには、ツールバーの[**すべて有効化**]または[**すべて無効化**]をクリックします。
6. このページに対する変更を保存するには、ツールバーの[**保存**]をクリックします。

> **注**:設定が変更されたルールには、隅に赤い三角印が表示されます。保存する前に別のルールのページに移動すると、このページへの変更はすべて失われます。

IOCのスコア加重の調整

IOCのスコアの加重を調整すると、構成されているモジュールの集計スコアに対するIOCの全体的なインパクトが増減します。IOCの全体的なインパクトを増減するには、加重を変更します。

- -100～-1の範囲の値は、解析中のセッションやファイルがマルウェアである可能性が低いことを示します(-100は最も可能性が低い) 。
- 1～100の範囲の値は、解析中のセッションやファイルがマルウェアである可能性が高いことを示します(100は最も可能性が高い) 。
- 値を0にすると、IOCは有効なままですが、IOCは集計されたスコアに影響しなくなり、解析結果に表示されなくなります。値を0に設定することにより、同じIOCの他のファイル タイプのルールによるスコア計算は変更せずに、IOCのファイル タイプ固有のインスタンスを無効にすることができます。

スコアの加重を調整するには、次の手順を実行します。

1. **メイン メニュー**で、**[管理]＞[サービス]**を選択します。
2. Malware Analysisサービスを選択します。
3. **ツールバー**で、**[表示]＞[構成]**を選択します。
4. [**セキュリティ侵害インジケータ**]タブをクリックします。
5. [**モジュール**]選択リストで、All、Network、Static、Community、Sandbox、またはYaraのいずれかのスコア モジュールを選択します。
   モジュールに対して構成されたルールおよび設定が表示されます。

6. 次のいずれかを実行します。
   a. スコア スライダーを左または右にドラッグして、スコアの加重を小さくするか、または大きくします。
   b. 表示されているスコアの加重値をクリックし、新しい値を入力します。
7. このページに対する変更を保存するには、ツールバーの[**保存**]をクリックします。

注:設定が変更されたルールには、隅に赤い三角印が表示されます。保存する前に別のルールのページに移動すると、このページへの変更はすべて失われます。

IOCの高確率フラグの設定

[高確率]設定は、マルウェアが存在する可能性が非常に高いインジケータとして特定のIOCにフラグを設定する方法として使用されます。例として、[**Community - File Hash: AntiVirus (Primary Vendor) Flagged File**]というIOCについて、このIOCは偽陽性 (False Positive)である可能が低く、マルウェアの存在を正しく検出している可能性が高いことを示すフラグを設定することができます。IOCに高確率フラグを設定することにより、Malware Analysisの結果をフィルタし、1つ以上の高確率ルールが含まれているセッションのみを表示するように制限できます。このようにすることで、表示される結果はより小さなサブセットに限定され、その信頼性の精度が向上します。高確率のIOCに限定せずに結果を表示すると、グレーな結果を確認することもできます。これにより、偽陰性(false negative) が発生する可能性を低くした結果を得ることができます。このような利用から、信頼性のレベルに基づいて結果をフィルタするかしないかについては、NetWitness Suiteワークフローではいずれも有効な使用例と言えます。
高確率フラグを設定するには、次の手順を実行します。

1. [**セキュリティ侵害インジケータ**]タブで、[**モジュール**]選択リストからスコア モジュールを選択します。All、Network、Static、Community、Sandbox、Yaraから選択します。
   モジュールに対して構成されたルールおよび設定が表示されます。
2. フラグを設定/解除するルールの横にある[**高確率**]チェックボックスをクリックします。
3. このページに対する変更を保存するには、ツールバーの[**保存**]をクリックします。

注:設定が変更されたルールには、隅に赤い三角印が表示されます。保存する前に別のルールのページに移動すると、このページへの変更はすべて失われます。

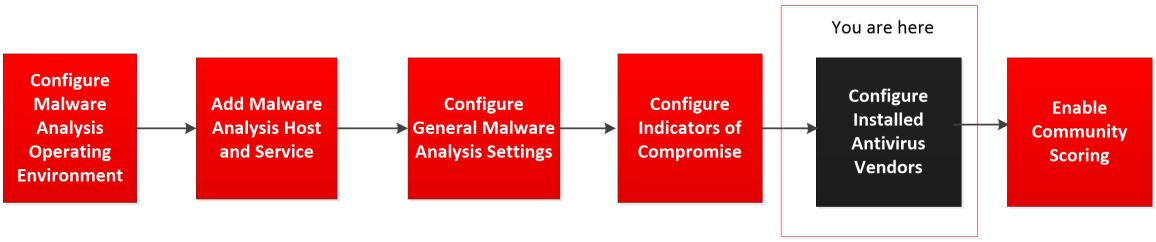
IOCのデフォルトの設定へのリセット

1. [**セキュリティ侵害インジケータ**]タブで、[モジュール]選択リストからスコア モジュールを選択します。All、Network、Static、Community、Sandbox、Yaraから選択します。
   モジュールに対して構成されたルールおよび設定が表示されます。
2. 現在のページのすべてのルールをデフォルトの設定にリセットする場合は、ツールバーの[**リセット**]をクリックします。
3. 選択したスコア モジュールのすべてのルールをデフォルトの設定にリセットする場合は、ツールバーの[**すべてリセット**]をクリックします。
4. このページに対する変更を保存するには、ツールバーの[**保存**]をクリックします。

インストール済みのアンチウイルスソフト ベンダーの構成

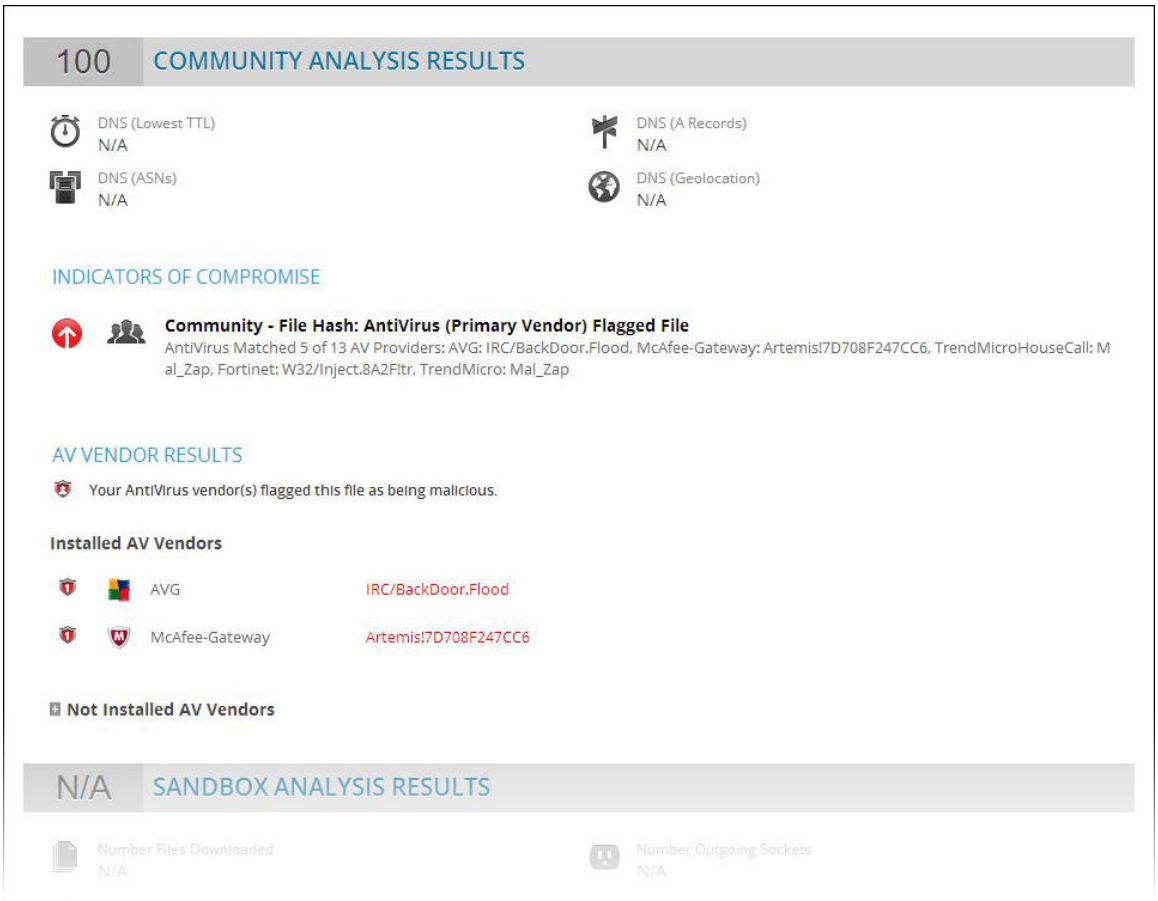
インストール済みのAV(アンチウイルス ベンダー) からのファイル解析結果とMalware Analysisナレッジベースからのコミュニティ解析結果を比較できます。コミュニティ解析によってファイルを解析する際に、Malware Analysisではアンチウイルスのナレッジベースを使用して、サンプルが既知の悪意があるファイルであるかどうかを判断します。ファイルが悪意のあるものであることが分かっている場合、NetWitness Suiteは、サンプルを識別したのがプライマリとセカンダリのアンチウイルス ベンダーのどちらであるかを示すフラグをそのファイルに付けます。NetWitness Suiteでは、ベンダーをプライマリとセカンダリに分類して、業界でのベンダーの評価レベルを示し、セキュリティ侵害インジケータでスコアの計算にこれらの評価を反映させます。たとえば、セカンダリ アンチウイルス ベンダーによってのみ検出された場合、プライマリ ベンダーによる検出よりもスコアは低くなります。

注 : ネットワークにインストールするアンチウイルス ベンダー ソフトウェアを選択する際は、NetWitness Suiteのプライマリ ベンダー リストからのソフトウェアを少なくとも1つ含めることを強く推奨します。



NetWitness Suiteでは、ネットワークにインストールされているアンチウイルス ベンダーを識別することができます。NetWitness Suiteは、アンチウイルスのコミュニティ解析の結果を、[アンチウイルス]タブで選択されているインストール済みベンダーからの結果と比較します。一致が検出された場合、解析中のファイルに、ローカルにインストールされたプライマリまたはセカンダリのアンチウイルスソフトウェアによってサンプルが検出されたことを示すフラグが設定されます。

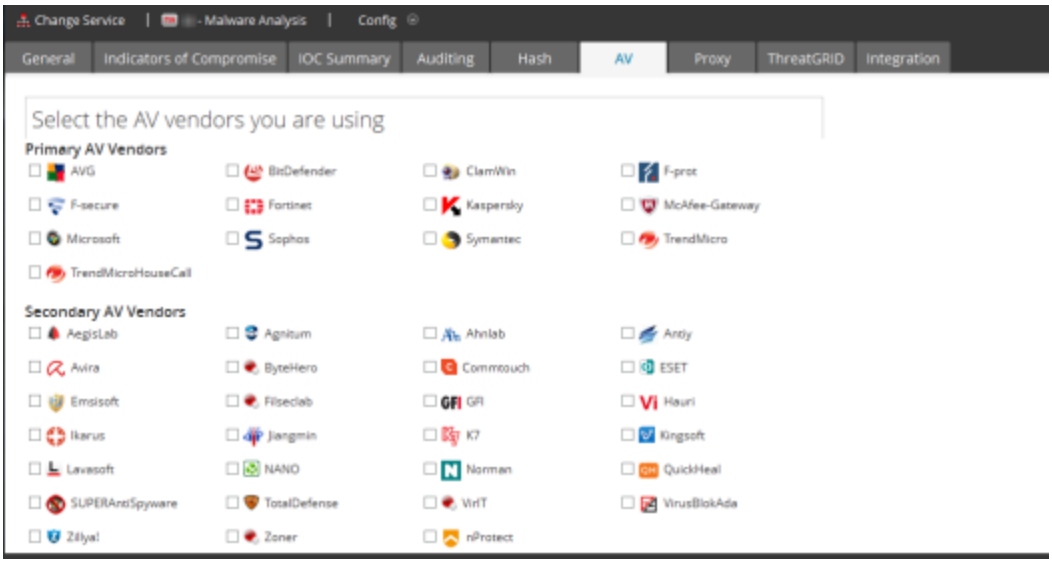
次の例は、100というスコアを取得したファイルのコミュニティ解析結果を示しています。[**セキュリティ侵害インジケータ**]に、コミュニティ解析内にリストされたアンチウイルスベンダーのフラグがこのファイルに設定されていることが示されます。NetWitness Suiteでは[**アンチウイルス ベンダーの結果**]に、使用環境にインストールされているアンチウイルス ベンダーがこのファイルを悪意のあるものとしてフラグを設定しているかどうかが示されます。インストール済みアンチウイルスベンダーがウイルスを検出した場合は、マルウェアの名前が表示されます。インストール済みアンチウイルスベンダーがウイルスを検出しなかった場合は、アンチウイルスベンダー名の横に「**--非検出--**」が表示されます。[**インストールされていないベンダー**]で[+]をクリックすると、セクションを展開して、システムにインストールされていない他のベンダーがウイルスを検出しているかどうかを確認できます。



インストールされたアンチウイルス ソフトウェアの識別

ユーザが使用中のアンチウイルスソフトウェアを識別するには、次の手順を実行します。

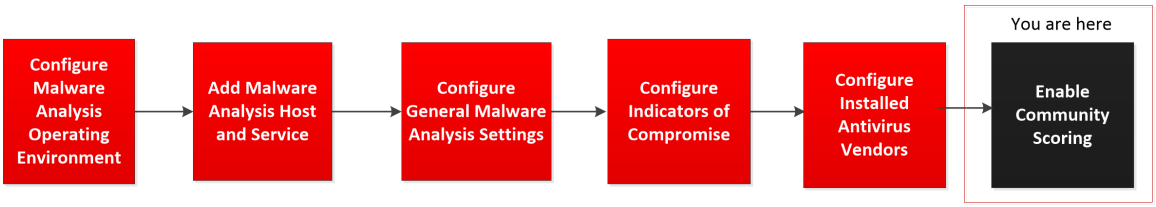
1. **メイン メニュー**で、[**管理**]＞[**サービス**]を選択します。
2. Malware Analysisサービスを選択し、その行の⚙＞[**表示**]＞[**構成**]を選択します。
3. [**サービス**]の[**構成**]**ビュー**で、[**アンチウイルス**]タブを選択します。



4. ユーザが使用中の各アンチウイルスベンダー(プライマリとその他)の横にあるチェックボックスをオンにします。
5. [**適用**]をクリックして、変更を保存します。
   コミュニティ解析の結果には、使用中のアンチウイルスソフトウェアがイベントにフラグを設定したかどうかが示されます。
6. (オプション)インストール済みのアンチウイルスソフトウェアのリストをリセットしてデフォルト値(なし)に戻す場合は、[**リセット**]をクリックします。
   すべての選択項目が削除されます。
7. 変更を保存するには、[**適用**]をクリックします。

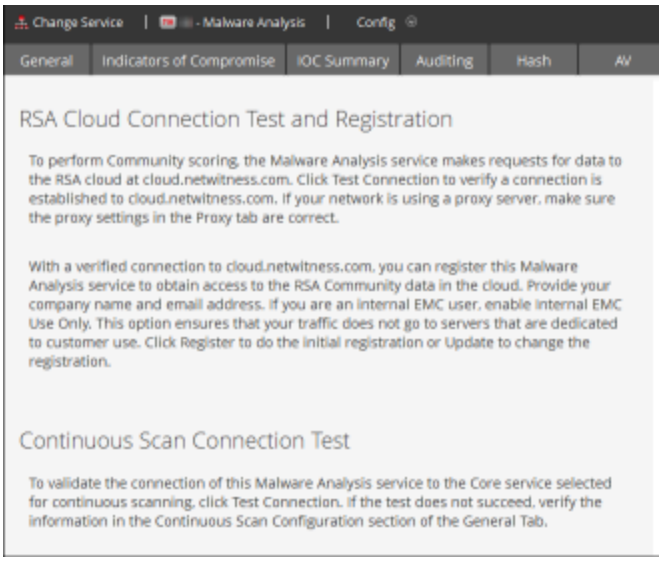
コミュニティ解析の有効化

管理者はコミュニティ解析を有効化できます。コミュニティ解析では、ネットワーク上でマルウェアとして検出されたデータは、RSA Cloudにプッシュ送信され、RSA独自のマルウェア分析データや、SANS Internet Storm Center、SRI International、米国財務省、VeriSignといった組織からのFeedを使って確認されます。コミュニティ解析を有効にするには、RSAクラウドに登録し、クラウドへの接続をテストしてから、常時スキャンが行われるように構成したサービスとRSAクラウドとの接続をテストします。



解析方法の詳細は、「Malware Analysisの動作の概要」を参照してください。

1. **メイン メニュー**で、[**管理**]＞[**サービス**]を選択します。
2. Malware Analysisサービスを選択し、その行の⚙＞[**表示**]＞[**構成**]を選択します。
3. [**サービス**]の[**構成**]**ビュー**で、[**統合**]タブを選択します。



4. [常時スキャンの接続テスト]まで下にスクロールし、[**RSAクラウド接続のテストと登録**]をクリックします。

   NetWitness Suiteにより`https://cloud.netwitness.com`のサイトとの通信がテストされます。会社でアウトバウンド トラフィックにプロキシを使用している場合は、プロキシの設定を確認してください。RSAコミュニティ サービスを登録するには、有効な接続が必要です。

5. 会社名と連絡先メールを入力します。**登録**をクリックします。

   すべての必須フィールドが入力されていれば、登録は完了します。登録に使用したボタンのラベルが[更新]に変わります。

6. Malware Analysisサービスが、常時スキャン用に選択したコア サービスと接続できていることを確認するには、[**常時スキャンの接続テスト**]をクリックします。

   NetWitness Suiteは、[全般]タブで指定されたソース ホスト、ソース ポート、ユーザ名、ユーザ パスワードに基づいてチェックを開始します。テストが正常に実行されると、アナリストはMalware Analysisでコミュニティ スコアリングを確認できます。

(オプション) Malware Analysisホストの監査の構成

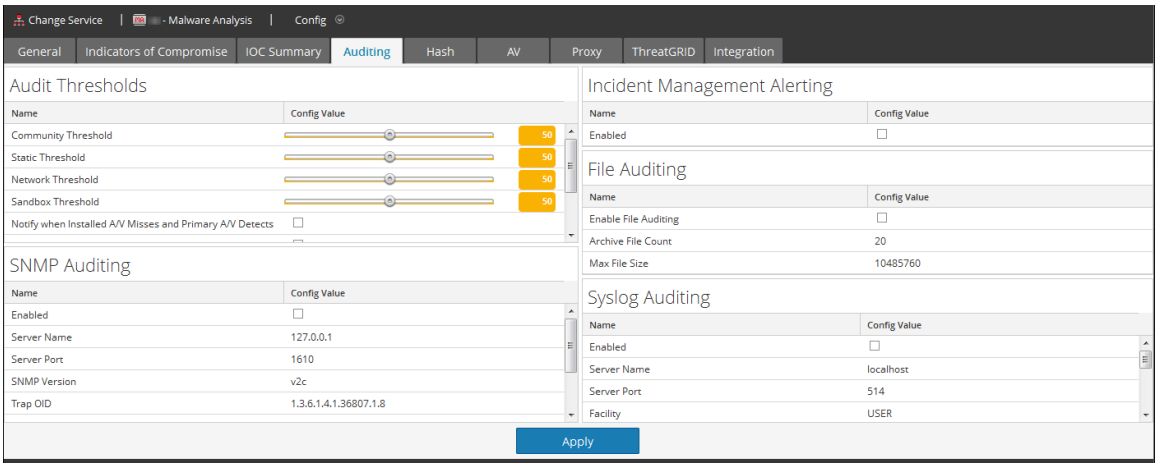
このセクションでは、Malware Analysis監査ログの機能と構成手順の概要を説明します。Malware Analysisでは、構成されたスコア モジュールの閾値に基づいて監査アラートを生成できます。解析中のセッションで、ファイルの解析スコアが構成された閾値に達するか、閾値を超えると、監査アラートが生成されます。この閾値の設定によって、セッション/ファイルがマルウェアである可能性が高いと判断されるスコアの場合に、自動的にアラートを生成できます。

アラートは、SNMP、Syslog、ファイル エントリーの形式として構成できます。さまざまな監査形式をサポートすることにより、外部システムで必要な監査イベントを取り込むことができます。

セッション解析の監査に加えて、次のようなイベントによって監査アラートがトリガーされます。

- ユーザ ログインの成功と失敗
- システム構成設定の変更
- サーバ再起動
- サーバのバージョン アップグレードやインストール

Malware Analysisの監査の構成設定は、[サービス]の[構成]ビュー>[監査]タブにあります。



監査の閾値の構成

閾値を設定する目的の1つは、解析するセッション/ファイルについてアラートを生成するのに必要な基準を指定することです。監査を有効にしている場合、スコアが計算された各ファイル/セッションを調べて、各スコア モジュールのスコアが構成された監査の閾値以上であるかどうかが確認されます。これに該当する場合、構成された監査アラート形式(SNMP、Syslog、ファイルなど)を使用してアラートが生成されます。たとえば、[SNMP]を構成し、[コミュニティの閾値(Community Threshold)]を90に設定することによって、コミュニティ(Community)スコア モジュールでスコアが90以上のすべてのセッション/ファイルについてSNMPトラップが生成されます。すべての閾値が90に設定されている場合は、ネットワーク、静的、コミュニティ、サンドボックスの各スコア モジュールでセッション/ファイルのスコアが90以上にならない限り、アラートは生成されません。

監査の閾値を構成するには、次の手順を実行します。

1. **メイン メニュー**で、**[管理]>[サービス]**を選択します。
2. Malware Analysisサービスを選択し、  **>[表示]>[構成]**を選択します。
3. **[サービス]の[構成]**ビューで、[**監査**]タブをクリックします。
4. [**監査の閾値**]セクションで、次の手順を実行します。

a. 各スコア モジュール、**コミュニティ**、**静的**、**ネットワーク**、**サンドボックス**の閾値を、次のいずれかの操作で設定します。
   - スライダで、ハンドルをクリックしていずれかの方向にドラッグします。
   - 値フィールドで、0～100の範囲の数値を入力します。

b. (10.3 SP2のオプション) 特定の条件に合致した場合にメッセージを記録し、有効なすべての監査方法で通知を行うトリガーを1つ以上選択します。

c. [**適用**]をクリックします。
   - 閾値の設定は、すべての有効な監査方法について直ちに有効になります (SNMP、ファイル、Syslog) 。
   - 記録されたメッセージは、有効化されているすべての監査方法で送信されます (SNMP、ファイル、Syslog) 。

Incident Managementアラートの構成

Incident Managementアラートを有効にした場合、Malware Analysisアラートを監査して、Incident Managementワークフローにフィードすることができます。

1. **メイン メニュー**で、[**管理**]＞[**サービス**]を選択します。
2. Malware Analysisサービスを選択し、＞[**表示**]＞[**構成**]を選択します。
3. **サービスの[構成]**ビューで、[**監査**]タブを選択します。
4. [**Incident Managementアラート**]セクションで、[有効]チェックボックスをオンにして、[適用]をクリックします。
   アラートはすぐに有効になります。

SNMP監査の構成

SNMP(Simple Network Management Protocol) は、IPネットワーク上のサービスを管理するためのプロトコルです。SNMP監査が有効になっている場合、Malware Analysisは監査イベントをSNMPトラップとして構成済みSNMPトラップ ホストに送信できます。スコアとイベントIDに加えて、アラートにはすべてのセッション メタと生成されたメタ データが含まれます。これは、サードパーティ システムにイベント データを送信する必要がある場合に便利です。

SNMP監査を構成するには、次の手順を実行します。

1. メイン メニューで、[**管理**]＞[**サービス**]を選択します。
2. Malware Analysisサービスを選択し、＞[**表示**]＞[**構成**]を選択します。
3. **サービスの[構成]**ビューで、[**監査**]タブを選択します。
4. [**SNMP監査**]セクションにある[Enabled]チェックボックスでSNMP監査をオンにします。

5. SNMPサーバ名とポートを構成します。
6. SNMPのバージョンとトラップを送信するためのトラップOIDを構成します。
7. Malware Analysisコミュニティと、トラップ送信時の再試行とタイムアウトのパラメータを構成します。
8. [**適用**]をクリックします。
   SNMP監査の設定はすぐに反映されます。

ファイル監査の設定の構成

ファイル監査が有効になっている場合、監査ログファイルは、Malware Analysisホームディレクトリに保持されます。このログファイルはデフォルトでは次の場所にあります。

```
/var/lib/netwitness/malware-analytics-
server/spectrum/logs/audit/audit.log.
```

個々のログが最大ファイルサイズに達すると、そのファイルはアーカイブされ新しいログが作成されます。これらの監査ログのサイズと数は、いずれも構成可能です。

注意：Malware Analysisアプライアンスのディスク領域を圧迫しないようにするため、最大ファイルサイズとアーカイブファイル数が大きくなり過ぎないようにします。

ファイル監査の設定を構成する方法

1. **メインメニュー**で、[**管理**]＞[**サービス**]を選択します。
2. Malware Analysisサービスを選択し、⚙＞[**表示**]＞[**構成**]を選択します。
3. **サービスの[構成]**ビューで、[**監査**]タブを選択します。
4. [**ファイル監査**]セクションにある[Enable File Auditing]チェックボックスでファイル監査をオンにします。
5. (オプション)[アーカイブファイル数]と[最大ファイルサイズ]を設定します。
6. [**適用**]をクリックします。
   ファイル監査の設定はすぐに反映されます。

Syslog監査設定の構成

Syslog通知サーバを有効にした場合、RFC 5424 Syslogプロトコルを使用して監査を行うことができます。SOX、PCI DSS、HIPAAなどの多くの規制では、組織が包括的なセキュリティ対策を実装することが要求されています。多くの場合、これらの対策には、さまざまなソースからのログの収集と解析が含まれます。Syslogは、さまざまなオープンソースや独自システムからのログを元にレポート作成や解析を行う場合に、ログを統合するための効果的な形式であることが証明されています。

スコアとイベントIDに加えて、Syslogにはすべてのセッション メタと生成されたメタ データが含まれます。これは、サード パーティ システムにイベント データを送信する必要がある場合に便利です。

Syslog監査設定を構成するには、次の手順を実行します。

1. **メイン メニュー**で、[**管理**]>[**サービス**]を選択します。
2. Malware Analysisサービスを選択し、  >[**表示**]>[**構成**]を選択します。
3. **サービスの[構成]**ビューで、[**監査**]タブを選択します。
4. [**Syslog監査**]セクションにある[Enabled]チェックボックスでSyslog監査をオンにします。
5. ターゲットSyslogプロセスが実行されているホストと、Syslogプロセスがリッスンしているポートを構成します。
6. 送信するSyslogメッセージのファシリティ、エンコーディング、形式、最大長、タイムスタンプの設定等を構成します。

   > **注**:(オプション) Syslogアラートに付加するID文字列を構成します。
   > CEF形式の追加の考慮事項については、「CEF形式のカスタム アラートの作成」を参照してください。

7. [**適用**]をクリックします。

   Syslog監査の設定はすぐに反映されます。

(オプション) ハッシュ フィルタの構成

このトピックでは、Malware Analysisで、ファイルを既知の無害なファイルまたは有害なファイルとしてマークすることができる、ハッシュ フィルタの概要を説明します。ハッシュ フィルタを使用すると、既知の無害または有害なファイルに関するハッシュのリストを管理できます。[ハッシュ]タブで、ファイル ハッシュに基づいて、Malware Analysisのイベント解析を微調整できます。ファイル ハッシュが無害としてマークされている場合、Malware Analysisは次回そのファイル ハッシュを検出したときにファイルを解析しません。ファイル ハッシュが有害としてマークされている場合、Malware Analysisは自動的にそのファイルのCommunityスコアのポイント数を大幅に上昇させます。Malware Analysisは、そのようなファイルの場合でも、新しい情報が利用可能になっている場合があるため、ファイルを解析します。

> **注**:イベントに単一のファイルが含まれており、ファイルのハッシュが無害としてマークされている場合、Malware Analysisによってイベント全体がフィルタ処理され、Malware Analysisの結果に表示されません。

ハッシュ リストにハッシュ フィルタを追加するには、次のいずれかの手動による方法を使用できます。

1. [イベントの詳細]ビューのコンテキスト メニュー: ファイルを右クリックし、コンテキスト メニューで選択したファイルのハッシュを無害(通常)または有害(悪意あり)としてマークすることができます。
2. [ハッシュ]タブのツールバー: [ハッシュ]タブの[追加]ボタンをクリックし、ファイル ハッシュとファイル サイズを入力し、必要に応じて、信頼できるハッシュとしてマークできます。

監視対象フォルダからハッシュ リストを一括してインポートすることにより、Malware Analysisへのハッシュ フィルタの追加を自動化する方法もあります。監視対象フォルダからインポートされたハッシュはハッシュ リストには表示されません。一括インポート機能と、Malware Analysisサーバ上で設定された監視対象ディレクトリ(/var/netwitness/malware-analytics-server/spectrum/hashWatch) を使用して、監視対象フォルダにハッシュ リストをコピーします。リストはシステムに自動的にインポートされます。一括インポートを使用してインポートされたハッシュは、前回までに監視対象フォルダを使ってインポートされたハッシュを上書きします。

ハッシュ リストの表示

ハッシュ リストを表示するには、次の手順を実行します。

1. **メイン メニュー**で、**[管理]**>**[サービス]**を選択します。
2. [サービス]ビューで、Malware Analysisサービスを選択し、  >**[表示]**>**[構成]**を選択します。
3. [**ハッシュ**]タブを選択します。

   ハッシュ リストが[ハッシュ]タブに表示されます。いずれかの方法を使用して追加されたファイル ハッシュのみが表示されます。

ハッシュ フィルタへのファイル ハッシュの追加

ハッシュ フィルタにファイル ハッシュを追加するには、次の手順を実行します。

1. [**ハッシュ**]タブのツールバーで、[**追加**]をクリックします。

   [ハッシュの追加]ダイアログが表示されます。
2. ハッシュが信頼済みである場合は、[**信頼済み**]を選択します。
3. MD5ハッシュと、バイト単位のファイル サイズを入力します。
4. [**保存**]をクリックします。

   ファイル ハッシュがハッシュに追加され、Malware Analysisでハッシュ フィルタを実行するために使用されます。

信頼済みまたは非信頼としてのハッシュのマーク

信頼済みまたは非信頼としてファイル ハッシュをマークするには、次の手順を実行します。

1. [**ハッシュ**]タブで、信頼済みと非信頼を切り替えるには、ハッシュの[**信頼済み**]チェックボックスをクリックします。
2. ツールバーで、[**編集内容の保存**]をクリックします。

ハッシュフィルタからのハッシュの削除

ハッシュフィルタからハッシュを削除するには、次の手順を実行します。

1. [**ハッシュ**]タブで、ハッシュフィルタから削除する1つ以上のハッシュを選択します。
2. ツールバーで、[**削除**]をクリックします。

   確認を求めるダイアログが表示されます。
3. ハッシュを削除するには、[**はい**]をクリックします。

   ファイルハッシュがグリッドから削除され、Malware Analysisのハッシュフィルタで使用されなくなります。

ファイルハッシュの検索

[ハッシュ]タブでは、グリッドに表示されているファイルハッシュを検索できます。検索するファイルハッシュを[MD5]フィールドに入力し、[**検索**]をクリックします。指定されたハッシュを含むファイルのリストがグリッドに表示されます。

監視対象フォルダを使用したハッシュリストのインポート

監視対象ディレクトリからハッシュリストをインポートするには、ハッシュリストが指定された形式で記載され、md5でソートされている必要があります。後で説明する形式のファイルをMalware Analysisアプライアンス上のフォルダ(/var/netwitness/malware-analytics-server/spectrum/hashWatch) にドロップすると、ファイルはローカルのハッシュデータベースに自動的にインポートされます。ファイルハッシュをにインポートする方法は、この方法だけです。その他の使用例として、システム管理者は監視対象ディレクトリを共有し、このディレクトリにリストをプッシュする特定のプロセスを使用してインポートを実行できます。こうすると、大量のハッシュのインポート処理が簡単になります。

このファイルは、csv形式のファイルで、各行間には空白がないようにする必要があります。ハッシュリスト内のデータには重複がないようにする必要があります。重複は処理の際に無視されます。重複するハッシュがあると、ログファイルに次のメッセージが表示され、ファイルに含まれる重複ハッシュの数が示されます。

2013-08-09 09:46:00,674 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processing - /var/lib/rsa>malware/hashWatch/test.csv
2013-08-09 09:47:56,619 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.services.file.hash.HashServiceImpl - Skipped 21 Duplicate Hashes Already on File
2013-08-09 09:48:06,638 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processed - /var/lib/rsa>malware/hashWatch/test.csv

デフォルトのファイル形式のハッシュリストの例を以下に示します。

```
[BeginFileExample]
392126E756571EBF112CB1C1cdEDF926,98865,True
0E53C14A3E48D94FF596A2824307B492,2226,True
176308F27DD52890F013A3FD80F92E51,42748,False
9B3702B0E788C6D62996392FE3C9786A,32768,False
937ADE76A75712B7FF339403B4FCB5A6,4821,False
B47139415F735A98069ACE824A114399,1723,False
E6CAF205E602CFA9A65663DB1A087874,704,False
680CA0BCE1FC7BC4136ADF4E210869C5,2075,False
[EndFileExample]
```

NetWitness Suiteの構成ファイル(**/var/netwitness/malware-analytics-server/spectrum/conf/hashFileWatchConfig.xml**) では、ハッシュリストのインポート プロセスで使用される形式およびオプションを指定します。構成ファイルのリストを以下に示します。

```
<config>
 <enabled>true</enabled>
 <distributedCacheEnabled>true</distributedCacheEnabled>

<watchDirectory>/
/var/lib/rsamalware/hashWatch</watchDirectory>

<processedDirectory>/
var/lib/rsamalware/hashWatch/processed</processedDirectory>
```

```
<erroredDirectory>/
var/lib/rsamalware/hashWatch/error</erroredDirectory>
 <md5Col>0</md5Col>
 <fileSizeCol>-1</fileSizeCol>
 <isTrustedCol>1</isTrustedCol>
 <isTrust>false</isTrust>
 <ignoreFirstLine>false</ignoreFirstLine>
 <frequencyInMinutes>1</frequencyInMinutes>
 <isGzipCompressed>false</isGzipCompressed>
 </config>
```

行	説明
<md5Col>0</md5Col>	各エントリーのmd5ハッシュの場所。デフォルト値は位置**0**、つまり最初の位置です。
<fileSizeCol>1</fileSizeCol>	各エントリーのハッシュサイズの場所。デフォルト値は位置**1**、つまり2番目の位置です。ハッシュサイズがcsvファイルに含まれていない場合は、この値を**-1**にする必要があります。
<isTrustedCol>2</isTrustedCol>	各エントリーの信頼済みパラメータ列の場所。デフォルト値は位置**2**です。信頼済みパラメータがcsvファイルに含まれていない場合は、この値を**-1**にする必要があります。
<isTrust>false</isTrust>	各エントリーの[**信頼済み**]パラメータに対するデフォルト値は**false**です。
<ignoreFirstLine>false</ignoreFirstLine>	ハッシュ内のヘッダの有無。デフォルト値は**false**です。ハッシュにヘッダがある場合は、この値を**true**に設定する必要があります。
<frequencyInMinutes>1</frequencyInMinutes>	NetWitness Suiteによる監視対象ディレクトリ内のチェックの間隔。デフォルト値は**1**分間です。
<isGzipCompressed>false</isGzipCompressed>	ハッシュはGzipを使用して圧縮されます。デフォルト値は**false**です。ハッシュがGzipで圧縮されている場合、この値はここで**true**に設定する必要があります。

ハッシュリストがインポートされた場合、ログのエントリーは次のようになります。

```
2013-04-11 03:22:00,597 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 2013-04-11 03:22:00,600 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processed -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

ファイルのロードに問題がある場合、ログのエントリーは次のようになります。

```
2013-04-11 03:17:00,597 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 ... Verbose log
 2013-04-11 03:17:00,632 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Error Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

監視対象フォルダを使用してハッシュリストをインポートするには、次の手順を実行します。

1. インポートするハッシュリストを**/var/netwitness/malware-analytics-sever/spectrum/hashWatch**ディレクトリにコピーします。
   Malware Analysisによってこのフォルダが自動的に監視され、ここに配置されたファイルが処理されます。
   Malware Analysisによって、ハッシュリスト内のすべてのハッシュがハッシュフィルタに追加されます。
   処理エラーが発生した場合、**/var/netwitness/malware-analytics-sever/spectrum/hashWatch/error**内のログに記録されます。
   処理されたファイルは、**/var/netwitness/malware-analytics-sever/spectrum/hashWatch/processed**でカタログ化されます。
   処理されたファイルはhashWatchディレクトリから削除されません。
2. ハッシュを一括してインポートした後、システム管理者はcronジョブを使用して以前の処理済みファイルをクリーンアップすることができます。

(オプション) Malware Analysisのプロキシ設定の構成

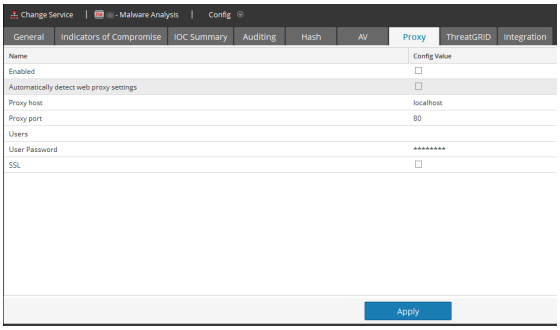
このトピックでは、RSAクラウド サービス、ローカルのThreatGridまたはGFIサービスと通信するためのWebプロキシの構成について説明します。[サービス]の[構成]ビュー> [プロキシ]タブの設定によって、Webプロキシによる通信を設定します。Malware Analysisでは、このWebプロキシを使用して、コミュニティ解析やサンドボックス解析のためにRSAクラウドと通信することができます。プロキシが構成されると、次の操作ができるようになります。

- Malware Analysisで、Webプロキシを経由してRSAクラウドと通信し、コミュニティ解析を実行する。
- Malware Analysisで、Webプロキシを経由して構成されているThreatGridまたはGFI Sandboxサービスと通信し、解析を実行する。Webプロキシを使用すると、パフォーマンスに影響を及ぼす可能性があります。[全般]タブの[ThreatGrid]および[GFI]セクションには、Webプロキシを無視して、直接サンドボックスと通信し、パフォーマンスを向上させるオプションがあります。

Webプロキシの構成

Malware AnalysisのWebプロキシを構成するには、次の手順を実行します。

1. **[管理]>[サービス]**ビューに移動します。
2. Malware Analysisサービスを選択し、⚙>**[表示]>[構成]**を選択します。
3. **[サービス]の[構成]ビュー**で、**[プロキシ]**タブを選択します。



4. プロキシを有効化するには、**[有効]**チェックボックスをオンにします。
5. (オプション) NetWitnessサーバのプロキシ設定を自動的に検出するには、チェックボックスをオンにします。

   プロキシ ホストとプロキシ ポートの各フィールドが自動入力されます。
6. 別のプロキシを使用する場合は、**[Proxy Host]**と**[Proxy Port]**に値を入力します。
7. プロキシ ホストにログオンするためのユーザ名とパスワードを入力します。

8. (オプション) プロキシ ホストとSSL経由で通信する場合は、[**SSL**]を選択します。
9. [**適用**]をクリックします。

   設定が保存され、すぐに反映されます。

注: Malware Analysisでは、NTML Webプロキシ認証をサポートしていません。

(オプション) ThreatGrid APIキーの登録

このトピックでは、ThreatGrid Cloud Sandboxで使用できる試用版ThreatGrid APIキーを取得する手順の概要を説明します。サンドボックス モジュール内のサービスとしてThreatGridを有効にする場合には、このサイトから送信されたサンプルが正当なものであるとThreatGridによって認識されるようにするため、ThreatGridから提供されたサービス キーを構成する必要があります。

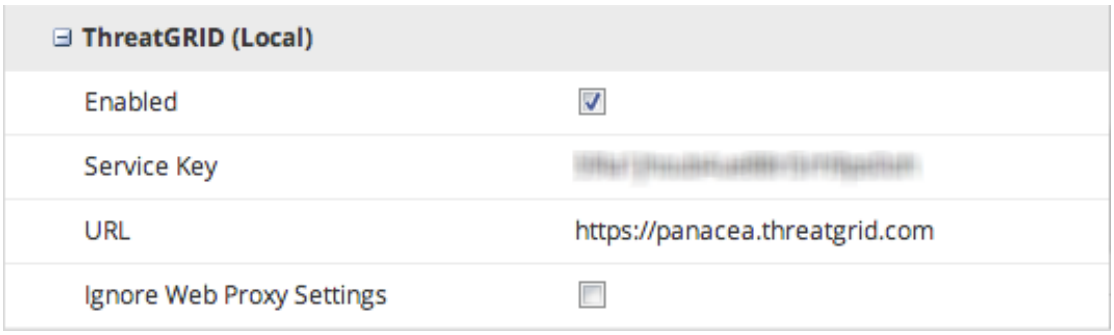
ThreatGridが提供するサービス キーを持っていない場合は、このタブを使用してキーを取得できます。キーは、試用版として提供されます。

ユーザ情報を入力して[**登録**]をクリックすると、このタブにキーが表示され、[**全般**]タブのThreatGridの構成に自動的に追加されます。数分後に、ThreatGridから、ログオンするためのページへのリンクを含むメールが送信されます。ThreatGridのページでライセンス条項に同意すると、解析用のファイルを送信できるようになり、Malware Analysisによってサンドボックス解析に送信されるファイルが、ThreatGridで認識されます。

試用版ThreatGrid APIキーを取得するには、次の手順を実行します。

1. NetWitness Suiteで、[**管理**]＞[**サービス**]に移動します。
2. Malware Analysisサービスを選択し、  ＞[**表示**]＞[**構成**]を選択します。
3. [**サービス**]の[**構成**]ビューで、[**ThreatGrid**]タブを選択します。
4. 登録するユーザの名前、役職、組織名、メール アドレスを入力します。
5. [ユーザID]フィールドと[パスワード]フィールドで、ThreatGridにログオンするためのユーザIDとパスワードを作成します。
6. **登録**をクリックします。

   登録情報がThreatGridに送信され、[登録]ボタンの下にAPIキーが表示されます。このキーは自動的に[**全般**]タブに入力されます。
7. [**全般**]タブをクリックして、ThreatGRIDの構成にAPIキーが含まれていることを確認します。



8. ThreatGridから、ログオンURLを含むメールを受信したら、ログオンして、ライセンス条項に同意します。

   ThreatGridの試用が開始され、Malware Analysisでは1日あたり5つまでのファイルをサンドボックス解析のためにThreatGrid Cloudに送信できます。

Malware Analysisを構成するための追加手順

このトピックでは、必要に応じて構成を行うMalware Analysisの追加の設定について説明します。Malware Analysisを構成した後、サービスを調整して詳細なカスタマイズを行う必要がある場合があります。例として、カスタムYARAコンテンツの導入があります。

- CEF形式のカスタム アラートの作成
- カスタムYARAコンテンツの有効化

CEF形式のカスタム アラートの作成

このトピックでは、CEF(Common Event Format) 形式でイベントを収集するサービスにアラートを送信するため、CEF形式のカスタム アラートを作成する手順について説明します。これは高度な構成タスクです。このタスクを実行するには、構成ファイル(`/var/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`) を手動で編集するための十分な知識が必要です。このファイルを編集する前に、オペレーティング システムでMalware Analysisサービスを停止する必要があります。Malware Analysisサービスを再開すると、CEFアラートがアクティブになります。

CEFテンプレート

イベントをCEFとして取り込むサービスにアラートを送信するために、NetWitness Suiteは、イベントの相関処理が行われる前に、CEFテンプレートとして機能する構成ファイルを介してイベントを処理します。構成ファイルを変更することにより、各アラートのSyslogフィールドの順序とマッピングを指定できます。

次の例のSyslogメッセージは、アラートの拡張セクションにあるCEFフィールドを示しています(アラートの最後の「|」以降) 。各フィールドを構成して、シーケンスを指定できます(以下の「例」セクションを参照) 。構成により、フィールドをアラートから完全に除外することもできます。

```
CEF:0|NetWitness|Spectrum|10.3.0.7995.1.0|Suspicious Event|Detected
suspicious network event ID 4 session ID n/a|2|static=100.0
nextgen=25.0 community=100.0 sandbox=25.0 file.name=myFile.exe
file.size=1234556 file.md5.hash=DEADBEEFBABECAFEDEADBEEFBABECAFE
event.source=spectrum://admin@0:0:0:0:0:0:0:1:64563
event.type=MANUAL_UPLOAD event.id=0 country.dst.code=--
country.dst=Unavailable ip.src=0:0:0:0:0:0:0:1
ip.dst=0:0:0:0:0:0:0:1 event.uuid=f7a6155a-31de-4fa6-ba16-
41fb9a8e5f26 ...
```

Syslog監査ファイルのエントリーの概要

次の例を使用して、ファイル構造を説明します。

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125
```

```
CEF: 0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected
suspicious
 network event ID 857 session ID 73|2|

static=100.0 network=29.0 community=8.0 sandbox=N/R

file.name=-CVE-00_DOC_2010-05-13_attachment.doc file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307

com.netwitness.event.internal.id=73
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2
referer=http://qa-fc12-149/files/MALWAREMALW...fficeDocs/DOC/
risk.info=http client server version mismatch
```

最初の行

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125
```

ログ情報	説明
Feb 6 10:02:28	エントリーのタイム スタンプ。
10.10.10.125	イベントのソースIPアドレス。
SpectrumServer125	イベントのソース ホスト名。

監査Common Event Format(CEF) ヘッダ

```
0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected suspicious
network event ID 857 session ID 73|2|
```

監査CEFヘッダには、縦棒で区切られた次のフィールドが含まれます。

ログ情報	説明
0	監査Syslogに使用されるArcSight Common Event Format(CEF) のバージョン。

ログ情報	説明
NetWitness	Syslogメッセージを作成したサービス。
Spectrum	Malware Analysisはイベントのロガーです。
1.2.1.130	Malware Analysisのバージョン。
event ID 857	このイベントの一意のネットワークイベントID。
session ID 73	このイベントが含まれるセッションのコアの一意のセッションID。
2	重大度。メッセージの重大度を示す1～6の整数。 • 1 = INFORMATION_LEVEL • 2 = WARNING_LEVEL • 3 = ERROR_LEVEL • 4 = SUCCESS_LEVEL • 5 = FAILURE_LEVEL • 6 = AUDIT_FAILURE_LEVEL

監査CEFの拡張フィールド

```
static=100.0 network=29.0 community=8.0 sandbox=N/R

file.name=-CVE-00_DOC_2010-05-13_attachment.doc  file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307
com.netwitness.event.internal.id=73

com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2 referer=http://qa-
fc12-149/files/MALWAREMALW...fficeDocs/DOC/ risk.info=http client server
version mismatch
```

解析スコア

監査のCEF拡張機能の最初のエントリーは、イベントの4つのMalware Analysisスコア(静的、ネットワーク、コミュニティ、サンドボックス) を示します。

ログ情報	サンプル値
static	100.0
network	29.0
community	8.0 スコアが0.0の場合、イベントのコミュニティスコアが0であるか、コミュニティサービスが有効になっていない可能性があります。
sandbox	N/R N/Rは実行されていないこと(not run) を示します。これは、GFI Sandboxが有効化されていなかったことを示します。

ファイル情報

次の3つのエントリはファイル情報(ファイル名、サイズ、ハッシュ) を示します。

ログ情報	サンプル値
file.name	-CVE-00_DOC_2010-05-13_attachment.doc
file.size	0
file.md5.hash	20a29259c0e5958afb2f50c4177bb307

NextGenが取得したイベントメタデータ

レコードでは、イベントのCoreメタデータが続きます。メッセージ内のメタデータはイベントによって異なります。メッセージ内のデータ量は、Syslog設定で構成されたバイト単位の最大長に切り詰められます。デフォルト値は1024です。

ログ情報	サンプル値
com.netwitness.event.internal.id	73
com.netwitness.event.internal.uuid	37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip	10.25.50.149

ログ情報	サンプル値
client	Wget/1.11.4 Red Hat modified
payload	108872
packets	136
country.dst	Private
time	Fri Jan 27 10:09:25 EST 2012
threat.source	netwitness
tcp.srcport	43580
action	get
com.netwitness.event.internal.source	http://QASpectrum2:50104/sdk
filetype	rtf
alias.host	qa-fc12-149
eth.src	00:25:90:18:76:E2
ip.proto	6
tcp.flags	27
ip.src	10.25.50.61
tcp.dstport	80
threat.category	spectrum
eth.dst	00:0C:29:F8:50:2D
lifetime	0
alert.id	nw32535
sessionid	73

ログ情報	サンプル値
medium	1
size	117864
content	spectrum.consume11
extension	doc
directory	/files/MALWAREMALWARE/OfficeDocs/DOC/
eth.type	2048
ip.dst	10.25.50.149
service	80
filename	-CVE-00_DOC_2010-05-13_attachment.doc
server	Apache/2.2.13 (Fedora)
streams	2
referer	http://qa-fc12-149/files/MALWAREMALWARE/OfficeDocs/DOC/
risk.info	http client server version mismatch

構成ファイルの編集

1. Malware Analysisサービスを停止します。
2. 「例」の説明に従って構成ファイルを編集します。
3. Malware Analysisサービスを開始します。
   Malware Analysisサービスにより、構成ファイルを使用したアラートの処理と、指定のサービスへのCEFアラートの送信が開始されます。

例

構成ファイルにより、各フィールドに関連づけられているラベルや生成されるアラートに表示されるフィールドを指定できます。データフィールドの表示の順序も指定できます。以下の例に示すとおり、構成ファイルは1つ以上のXML `MalwareCefExtension`ブロックで構成されます。構成ファイルにおけるこれらのブロックの順序は、CEFアラートにおけるデータフィールドの順序を示します。

次の例では、CEFアラートには、`ip.src`とそれに続く`ip.dst`という2つのデータフィールドが含まれます。`customKey`は、アラート内でのデータフィールドのラベルを設定するために使用されます。この機能を使用してカスタムラベルを設定し、アラートの形式をアラート送信先のシステムに対応する形式に合わせることができます。つまり、アラート形式を調整することにより、アラート送信先の既存のParserに余計な変更を加える必要がなくなります。さらに、`isDisplay`の設定によって、フィールドをアラート出力に含めるかどうかを指定できます。これを利用すれば、`MalwareCefExtension`ブロックを構成から物理的に削除しなくても、データフィールドを無効化することができます。

```
 <config>
 <malwareExtensionList>
<com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>ip.src</customKey>
   <malwareKey>ip.src</malwareKey>
   <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>ip.dst</customKey>
   <malwareKey>ip.dst</malwareKey>
   <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
 </malwareExtensionList>
</config>
```

このほか、構成ファイルの末尾には、アラートの形式をさらに調整するための設定が3つあります。具体的には、次のとおりです。

設定	説明
includesUnknownMeta	これをtrueまたはfalseに設定することで、生成されるアラートに不明なデータ要素を含めるかどうかを指定します。これにより、NextGenセッション メタを、CEFアラートに含めるか否かを選択できます。 新しいNextGen Parserを作成してセッション メタを追加することもできるため、デフォルトの構成には含まれないメタが存在する可能性もあります。includesUnknownMetaをtrueに設定すると、アラートに不明なメタを含め、NextGenメタ キー名を使用してラベリングできます。不明なメタにカスタム キーを適用するには、このファイルを編集して新しいMalwareCefExtensionをディクショナリに追加する必要があります。 アラートから不明なメタを削除するには、includesUnknownMetaをfalseに設定します。
displayNulls	これをtrueまたはfalseに設定することで、nullに設定されている値をアラートに含めるかどうかを指定します。displayNullsをfalseに設定した場合は、MalwareCefExtension isDisplayプロパティがオンになっていても、null値フィールドは省かれます。その結果、アラートの動的フォーマットにより、nullフィールドを除外することができます。
valueIfNull	この設定により、null値フィールドの値として使用するプレースホルダーの文字列(デフォルトはn/a)を指定できます。 displayNullsをtrueに設定した場合は、null値フィールドがアラートに含まれ、その値はvalueIfNullで指定した値に設定されます。

以下はデフォルトのCEF構成ファイルです。デフォルトの構成ファイルには、デフォルトのNextGenセッション メタがすべて含まれます。

```
<config>
  <malwareExtensionList>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>static</customKey>
```

```
<malwareKey>static</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>nextgen</customKey>
<malwareKey>nextgen</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>community</customKey>
<malwareKey>community</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>sandbox</customKey>
<malwareKey>sandbox</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.name</customKey>
<malwareKey>file.name</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.size</customKey>
<malwareKey>file.size</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.md5.hash</customKey>
<malwareKey>file.md5.hash</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<customKey>event.source</customKey>
<malwareKey>event.source</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.type</customKey>
<malwareKey>event.type</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.id</customKey>
<malwareKey>event.id</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.uuid</customKey>
<malwareKey>event.uuid</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.primary.detected</customKey>
<malwareKey>antivirus.primary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.secondary.detected</customKey>
<malwareKey>antivirus.secondary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.other.detected</customKey>
<malwareKey>antivirus.other.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst.code</customKey>
<malwareKey>country.dst.code</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>city.dst</customKey>
<malwareKey>city.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>org.dst</customKey>
<malwareKey>org.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>payload</customKey>
<malwareKey>payload</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>packets</customKey>
<malwareKey>packets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst</customKey>
<malwareKey>country.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>time</customKey>
<malwareKey>time</malwareKey>
<isDisplay>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.source</customKey>
<malwareKey>threat.source</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcpport</customKey>
<malwareKey>tcp.srcpport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filetype</customKey>
<malwareKey>filetype</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.dst</customKey>
<malwareKey>latdec.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src</customKey>
<malwareKey>eth.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>agency.dst</customKey>
<malwareKey>agency.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.proto</customKey>
<malwareKey>ip.proto</malwareKey>
```

```
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.flags</customKey>
<malwareKey>tcp.flags</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.src</customKey>
<malwareKey>ip.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.dstport</customKey>
<malwareKey>tcp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.category</customKey>
<malwareKey>threat.category</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst</customKey>
<malwareKey>eth.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>lifetime</customKey>
<malwareKey>lifetime</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.src</customKey>
```

```
<malwareKey>latdec.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>did</customKey>
<malwareKey>did</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alert.id</customKey>
<malwareKey>alert.id</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.src</customKey>
<malwareKey>country.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>sessionid</customKey>
<malwareKey>sessionid</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>longdec.src</customKey>
<malwareKey>longdec.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>medium</customKey>
<malwareKey>medium</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<customKey>size</customKey>
<malwareKey>size</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.computer.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.src</customKey>
<malwareKey>ad.username.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpackets</customKey>
<malwareKey>rpackets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>action</customKey>
<malwareKey>action</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.src</customKey>
<malwareKey>ad.domain.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src.vendor</customKey>
<malwareKey>eth.src.vendor</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpayload</customKey>
<malwareKey>rpayload</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.dst</customKey>
<malwareKey>ad.username.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>content</customKey>
<malwareKey>content</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>extension</customKey>
<malwareKey>extension</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst.vendor</customKey>
<malwareKey>eth.dst.vendor</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rid</customKey>
<malwareKey>rid</malwareKey>
<isDisplay>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>directory</customKey>
<malwareKey>directory</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.suspicious</customKey>
<malwareKey>risk.suspicious</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.type</customKey>
<malwareKey>eth.type</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.dst</customKey>
<malwareKey>ip.dst</malwareKey>
<isDisplay>false</isDisplay>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>service</customKey>
<malwareKey>service</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filename</customKey>
<malwareKey>filename</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>streams</customKey>
```

```
<malwareKey>streams</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.info</customKey>
<malwareKey>risk.info</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>dest.tld</customKey>
<malwareKey>dest.tld</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alias.host</customKey>
<malwareKey>alias.host</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcport</customKey>
<malwareKey>tcp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.srcport</customKey>
<malwareKey>udp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.dstport</customKey>
<malwareKey>udp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<customKey>domain.dst</customKey>
<malwareKey>domain.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.name</customKey>
<malwareKey>feed.name</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.description</customKey>
<malwareKey>feed.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.description</customKey>
<malwareKey>threat.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>referer</customKey>
<malwareKey>referer</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>client</customKey>
<malwareKey>client</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>server</customKey>
<malwareKey>server</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.warning</customKey>
<malwareKey>risk.warning</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>attachment</customKey>
<malwareKey>attachment</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.registrar</customKey>
<malwareKey>whois.registrar</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.registrant</customKey>
<malwareKey>whois.registrant</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.date.creation</customKey>
<malwareKey>whois.date.creation</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.server</customKey>
<malwareKey>whois.server</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
</malwareExtensionList>
<includesUnknownMeta>false</includesUnknownMeta>
<displayNulls>false</displayNulls>
<valueIfNull>n/a</valueIfNull>
```

```
</config>
```

カスタムYARAコンテンツの有効化

このトピックでは、Malware Analysisサービスがインストールされ ているNetWitness Suiteホストでカスタム YARAコンテンツを有効化する手順について説明します。ビルトインのセキュリティ侵害インジケータに加えて、Malware Analysisでは、YARAで記述されたセキュリティ侵害インジケータもサポートしています。YARAは、マルウェアの調査担当者がマルウェアのサンプルの特定や分類を行えるようにするためのルール言語です。RSAでは、YARAベースの組み込み型IOC(セキュリティ侵害インジケータ)をRSA Liveで公開しています。これらは、サブスクライブされたアプライアンスに自動的にダウンロードされてアクティブ化されます。

高度なスキルと知識を持つユーザは、YARAルールを編集してアプライアンスに配置することによって、RSA Malware Analysisに検出機能を追加したり、編集したYARAルールをRSA Liveでパブリッシュしたりすることができます。このセクションでは、アプライアンスを構成する管理者がカスタムYARAコンテンツの作成を有効化する手順について説明します。

前提条件

これは高度な構成タスクであり、このタスクを行うには、GCC(GNUコンパイラコレクション)、C++ Python開発ライブラリを構成してYARAをビルドするための十分な権限と知識が必要です。また、標準のYARAドキュメントを熟知している必要があります。次のコンポーネントが必要です。

- PCRE(Perl-Compatible Regular Expression)ライブラリ: pcre-8.33.tar.bz2
- YARA 1.7(リビジョン: 167)スタンドアロンYARAコマンドライン: yara-1.7.tar
- Python用YARA拡張機能: yara-python-1.7.tar.gz
- YARAルールのドキュメント: YARA User's Manual 1.6.pdf

コンポーネントはこちらからダウンロードできます。https://code.google.com/p/yara-project/downloads/list

注: 本書の執筆時点では、YARA 2.0が利用可能ですが、Malware Analysis 10.5ではサポートされていません。

CentOsベースのアプライアンスでYARAをビルドするために必要なライブラリとアプリケーションのインストール

CentOSを実行しているホストでYARAをビルドする前提条件として、`make`、GNUコンパイラコレクション、C++ `Python`開発ライブラリをアプライアンスにインストールする必要があります。YARAのビルドに必要なアプリケーションとライブラリをインストールするには、次の手順を実行します。

1. 次のコマンドを実行し、/etc/yum.repos.dフォルダに標準のYUM repoが存在し、その他のrepoファイルが存在しないことを確認します。
   ls -al /etc/yum.repos.d
   次のような結果が表示されます。
   ```
   -rw-r-r-. 1 root root 1926 Jun 26  2012 CentOS-Base.repo
    -rw-r-r-. 1 root root  637 Jun 26  2012 CentOS-Debuginfo.repo
    -rw-r-r-. 1 root root  626 Jun 26  2012 CentOS-Media.repo
    -rw-r-r-. 1 root root 2593 Jun 26  2012 CentOS-Vault.repo
   ```
2. アプライアンスにmakeをインストールするには、以下のコマンドを入力します。
   a. **yum search make**
      次のメッセージが返されます。`make.x86_64 : A GNU tool which simplifies the build process for user`
   b. **yum install make.x86_64**
3. GCCをインストールし、テストするには、次のコマンドを実行します。
   a. **yum search gcc**
      次のメッセージが表示されます。
      ```
      gcc-c+.x86_64 : C+ support for GCC
       gcc.x86_64 : Various compilers (C, C++, Objective-C, Java, ...)
      ```
   b. 以下のコマンドを実行します。
      yum install gcc.x86_64
      yum install gcc-c++.x86_64
   c. gccコマンドをテストするには、以下のコマンドを実行します。
      gcc -v
      cc -v
4. アプライアンスにC++ Python開発ライブラリをインストールするには、以下のコマンドを実行します。
   a. **yum search python dev**
      次のメッセージが返されます。
      ```
      python-devel.x86_64 : The libraries and header files needed for
      Python development
      ```
   b. **yum install python-devel.x86_64**

Yaraのセットアップ

Malware Analysisを実行しているNetWitness SuiteホストでYARAをビルドできるGCCおよびC++ Python開発ライブラリを作成するには、次の手順を実行します。

1. 次のいずれかの操作を実行します。
   a. インストール先のホストがMac OSを実行している場合は、Mac OS用のxCodeをインストールします。
   b. インストール先のホストがCentOSを実行している場合は、YUMコマンド ラインを使用して、make、GCC、C++ Python開発ライブラリをインストールします。
2. PCREライブラリをインストールするため、ターミナル ウィンドウを開き、以下のコマンドを実行します。

```
tar -xvf pcre-8.33.tar.bz2
 cd pcre-8.33
 ./configure
 make
 sudo make install
```

3. スタンドアロンYARAコマンド ラインをインストールするため、以下のコマンドを実行します:

```
tar -xvf yara-1.7.tar
 cd yara-1.7
 ./configure
 make
 sudo make install
```

4. スタンドアロンYARAコマンド ラインをテストします。
   a. 次のコマンドを実行します:
      yara
   b. コマンドが成功した場合は、ステップ7に進みます。コマンドが失敗し、「`yara: error while loading shared libraries: libpcre.so.1: cannot open shared object file: No such file or directory`」というエラーが返された場合は、次のコマンドを実行して`/etc/ld.so.conf`ファイルまたは`LD_LIBRARY_PATH`環境変数を確認します。
      ldconfig -v
5. Python用YARA拡張機能をインストールするには、以下のコマンドを実行します。

```
tar -xvf yara-python-1.7.tar.gz
 cd yara-python-1.7
 python setup.py build
 sudo python setup.py install
```

6. YARA拡張機能をテストする方法
   a. 次のコマンドを実行します:**python**

b. Pythonプロンプト(>>>) で、以下のコマンドを実行します。

```
import yara
 exit()
```

この構成が完了すると、アナリストは、「*調査およびマルウェア解析ガイド*」の「カスタムYARAコンテンツの実装」の説明に従って、Malware Analysisホストで使用できるカスタムYARA IOCを作成できます。

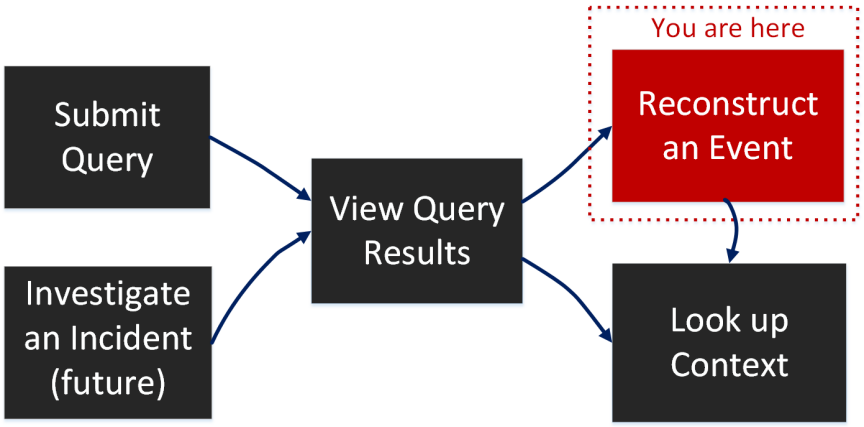
Malware Analysisの参考情報

- [サービス]の[構成]ビュー:[監査]タブ
- [サービス]の[構成]ビュー:[アンチウイルス]タブ
- [サービス]の[構成]ビュー:[全般]タブ
- [サービス]の[構成]ビュー:[ハッシュ]タブ
- [サービス]の[構成]ビュー:[セキュリティ侵害インジケータ]タブ
- [サービス]の[構成]ビュー:[統合]タブ
- [サービス]の[構成]ビュー:[IOCサマリ]タブ
- [サービス]の[構成]ビュー:[プロキシ]タブ
- [サービス]の[構成]ビュー:[ThreatGRID]タブ

[サービス]の[構成]ビュー: [監査]タブ

[イベント]ビューと新しい[イベント]ビューの[再構築]パネル(**[調査]>[イベント]パネル>イベントをクリック**) では、[ナビゲート]ビューまたは[イベント]パネルで見つけた関心のあるイベントの再構築を安全に表示することができます。

ワークフロー



どうしますか?

ユーザの役割	処理オプション...	ドキュメント
脅威ハンター	クエリの送信	調査の実施
脅威ハンター	クエリの結果の表示	[イベント分析]ビューでのイベントの分析
脅威ハンター	イベントの再構築*	イベントの再構築
脅威ハンター	イベントからのファイルのエクスポート	イベントの再構築
脅威ハンター	イベントの追加のコンテキストの検索	コンテキスト情報の検索

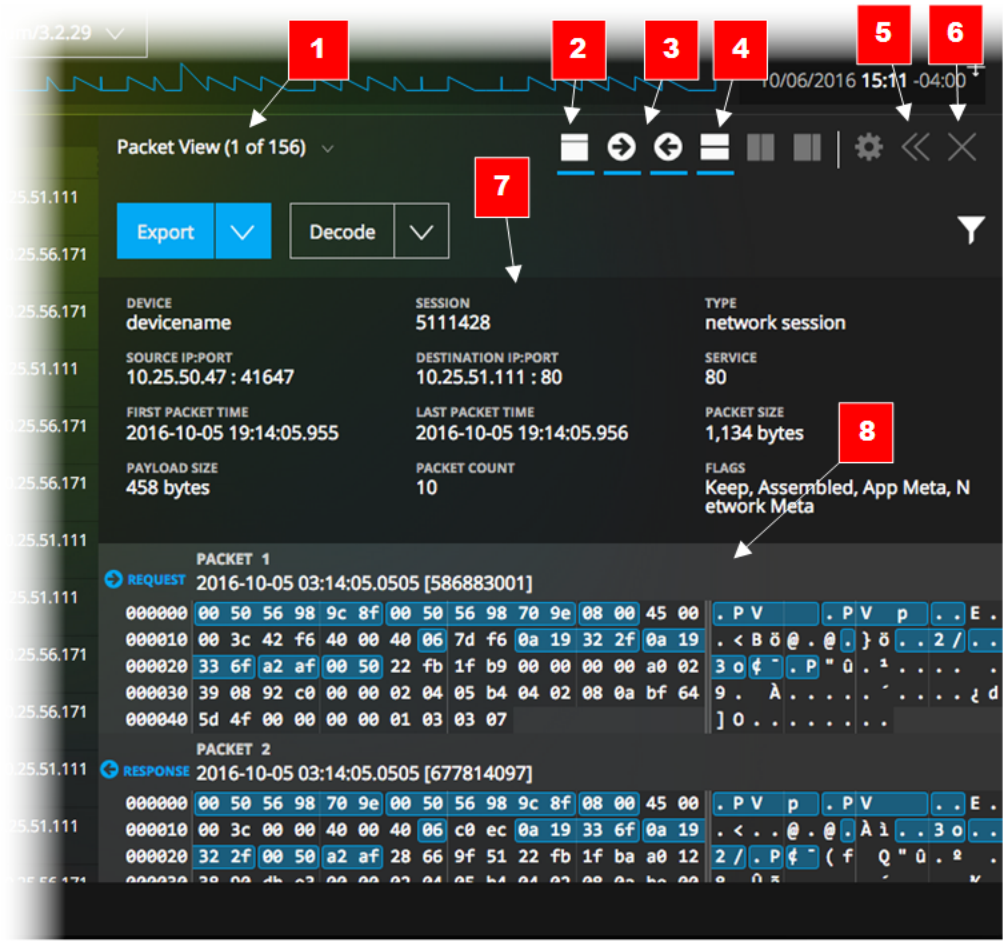
関連トピック

- NetWitness Investigateの仕組み
- 調査の実施
- [イベント分析]ビューでのイベントの分析
- [ナビゲート]ビュー
- [イベント分析]ビュー: [テキスト分析]パネル

簡単な説明

Investigateの[再構築]パネルは、パケット ビュー、ファイル ビュー、テキスト ビューで単一のイベントの再構築を表示します。[イベント]パネルでイベントをクリックすると、隣接する[再構築]パネルにイベントのパケット再構築が表示されます。[イベントの再構築]ツールバーのオプションを使用して、再構築タイプおよび方向(リクエストまたはレスポンス)を変更することや、ヘッダー パネルの表示と非表示を切り替えること、[イベントの再構築]パネルを拡張または縮小することや、閉じることができます。選択した再構築のタイプとペイロードの内容に応じて、追加のオプションが使用できます。たとえば、テキスト ビューでのみペイロードを表示し、ファイル ビューでファイルをダウンロードして、パケット ビューでPCAPファイルをダウンロードすることができます。

以下は、パケット再構築の例です。

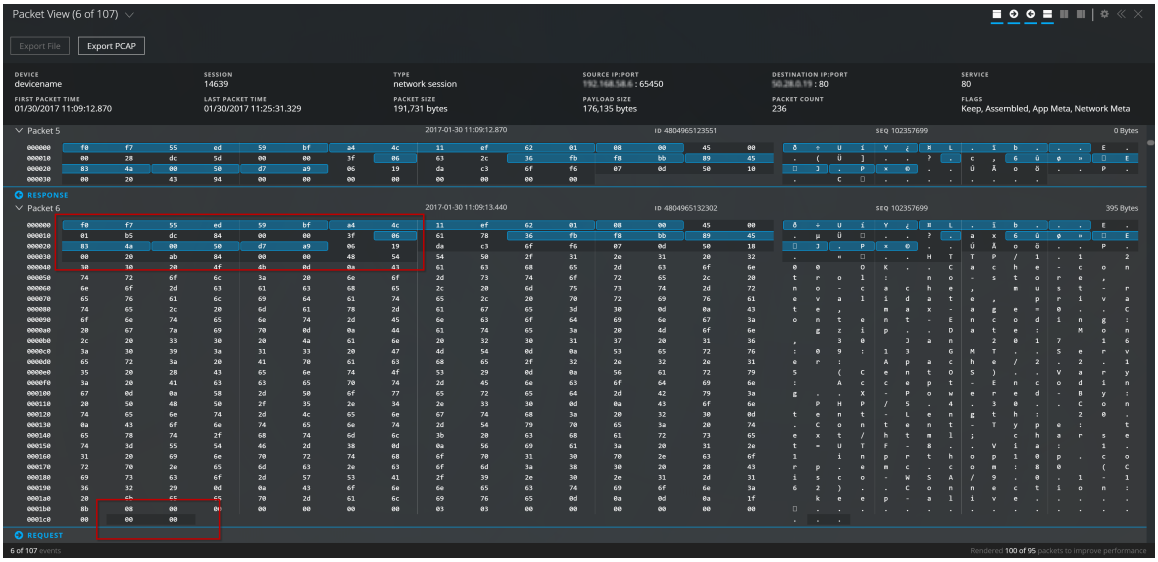


1	再構築タイプ(パケット ビュー、ファイル ビュー、テキスト ビュー) を選択するためのタブまたはドロップダウン メニューです。現在選択されているタイプがラベルに表示されます。
2	クリックすると、ヘッダー パネルの表示と非表示が切り替わります。
3	これらのアイコンをクリックすると、リクエスト、レスポンス、またはその両方が表示されます。
4	このアイコンをクリックすると、イベントに関連するメタ データの詳細なリストを提供する[イベント メタ]パネルの表示と非表示が切り替わります。
5	[ナビゲート]ビューで[再構築]パネルを水平方向に拡張または縮小するオプションです。
6	[再構築]パネルを閉じるオプションです。
7	ヘッダーには、再構築中のイベントのサマリ情報が表示されます。
8	イベントの各パケットが一覧表示されます。パケットごとに、パケット番号、方向(リクエストまたはレスポンス) 、パケットの内容を、左側にバイナリ形式、中央に16進形式、右側にテキスト形式で表示できます。

パケット再構築の詳細

パケット再構築では、Investigateによりパケット番号、パケットの方向(リクエストまたはレスポンス)、パケットの開始時刻、パケットの内容が表示されます。

すべてのパケットが、ヘッダーで開始され、パケットの一部にはフッターがあります。パケット ビューでは、パケットのペイロードと区別できるように、ヘッダーとフッターのバックグラウンドは暗い色で表示されます。ヘッダーおよびフッターの暗い色のバックグラウンドは、16進数とテキスト形式の両方で表示されます。



パケットの内容は、16進数とテキスト形式で提供されます。メタ データは青でハイライト表示されます。メタ データの上にマウスを置くと、メタ キーまたはメタ値の情報がスクリーン上にヒントとして表示されます。

パケット ビューのその他のオプションには、イベントのPCAPをダウンロードする機能や、ペイロードのみを表示する機能があります。ペイロードのみが表示されている場合は、[バイトの濃淡化]オプションを使用してデータのパターンを識別するために役立てることができます。

テキスト再構築の詳細

テキスト再構築では、ネットワーク イベントとログ イベントの表示方法が異なります。ネットワーク イベントでは、Investigateは、パケットの方向(リクエストまたはレスポンス)と、テキスト形式で各パケットの内容を提供します。

ログ イベント(中央のフィルタ=[ログ])では、リクエストまたはレスポンスはありません。rawログのみがテキスト再構築に表示されます。

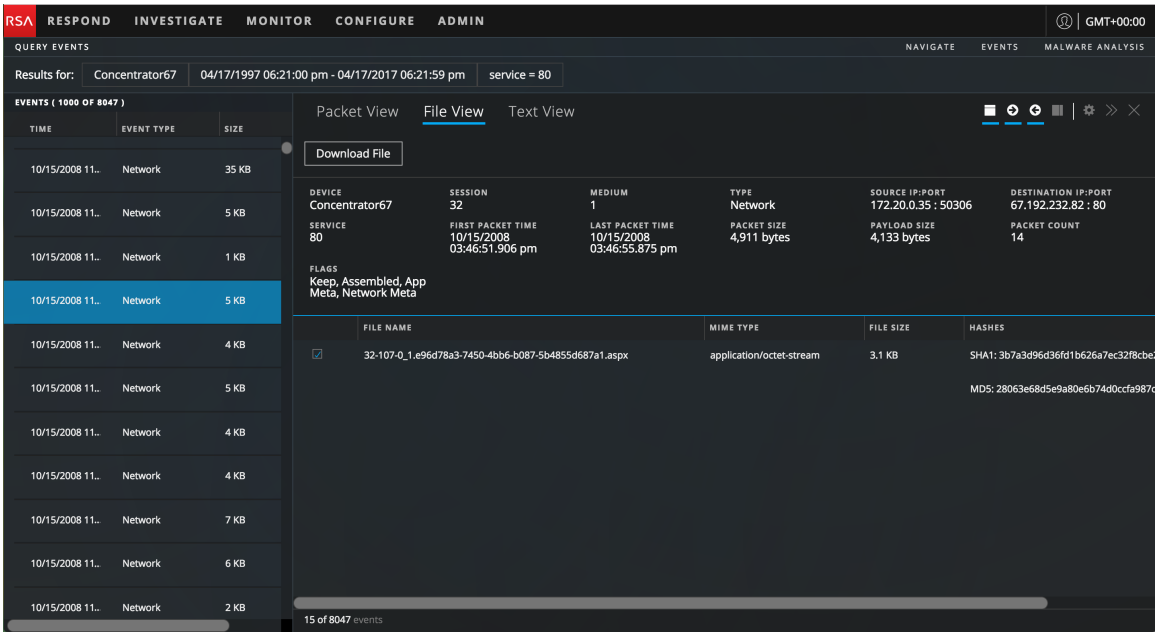
テキスト ビューでは、再構築オプションのサブセットが使用できます。実行できる操作：

- ヘッダーの表示と非表示を切り替えることができます。
- ネットワーク イベントの場合は、リクエストのみ、レスポンスのみ、またはその両方を表示できます。
- ネットワーク イベントの場合は、セッションをPCAPファイルとしてエクスポートできます。
- ログ イベントの場合は、rawログをエクスポートできます。
- ペイロードの圧縮と解凍ビューを切り替えることができます。セッションが解凍されると、テキストの圧縮された部分が読み取り可能になります。
- デコーディングとエンコーディングのためにテキストを選択できます。

注：この機能は、ファイル ビュー、HTTP以外のネットワーク セッション、ログ データでは使用できません。

ファイル再構築の詳細

ファイル再構築では、選択されたネットワーク イベントに関連するファイルのリストが調査により表示されます。



1個のファイル、1個または複数のファイル、すべてのファイルを選択してローカルファイルシステムにエクスポートできます。ファイルを選択したら、[ファイルのエクスポート]ボタンがアクティブになり、選択したファイルの数が反映されます。このボタンをクリックすると、選択したファイルがzipアーカイブとしてエクスポートされます。これにより、悪意のある可能性のあるファイルがデフォルトアプリケーションによって開かれることや、実行されることがなくなります。エクスポートされたアーカイブの名前には、次の規則を使用します。

```
<service-ID or host name>_SID<nnnnnnnn>_FC<n>.zip
```

各項目の意味は以下のとおりです。

- `<service-ID or host name>`は、セッションが保存されたサービスの名前(たとえばConcentratorまたはBroker)です
- `SID<nnnnnnnn>`は、セッションID番号です
- `FC<nnnnnnnn>`は、ファイル数またはアーカイブ内のファイルの数です。

ダウンロード時にアーカイブが自動的に解凍されるのを防ぐために、NetWitness Suiteはパスワード保護されたアーカイブをエクスポートします。アーカイブを開くには、パスワード「**netwitness**」を入力します。

注意:デフォルトのアプリケーションに関連づけられているファイルを解凍または開くときに警告が表示されます。たとえば、Excelスプレッドシートは、その安全を確認する前にExcelで自動的に開かれる可能性があります。

詳細説明

機能	説明
[再構築タイプ]メニュー	このメニューでは、再構築のタイプを選択できます。**選択できるタイプは、[パケット]**または[**ファイル**]です。最初に再構築を開くと、デフォルトでNetWitness Suiteにより最適な再構築が選択されます。
[ダウンロード]オプション	ログ、PCAP、ファイルをエクスポートして、より詳細な分析や、他のユーザとの共有を行うためのオプションです。

機能	説明
	パケット リストの上のヘッダーの表示を制御します。このアイコンをクリックすると、ヘッダーの表示と非表示を切り替えることができます。ヘッダーを非表示にすると、パケット リストのスペースが増えて、より多くのパケットを表示するために必要なスクロールの量が減ります。 ヘッダーには、パケットを収集したサービスの名前、セッション番号またはイベント番号、イベント(ネットワーク)のタイプ、ソースIP:PORT、宛先IP:PORT、サービス タイプ、イベントの最初のパケットの時刻、イベントの最後のパケットの時刻、イベント サイズ、バイト単位のペイロード サイズ、パケット数、イベントに適用されたフラグ(保持、アセンブル、アプリケーション メタ、ネットワーク メタ)などの再構築イベントに関する情報が表示されます。
	リクエストとレスポンスの表示をオンまたはオフにする2つのコントロールです(「イベントの再構築」を参照)。
	イベントのメタの詳細を別のパネルに表示します。
	(予定)[設定]メニューです。
 	[再構築]パネルのサイズ設定コントロールです(「イベントの再構築」を参照)。
	[再構築]パネルを閉じます。ビューには[イベント]パネルと[イベント]パネルのみが表示されるようになります。

[サービス]の[構成]ビュー: [アンチウイルス]タブ

このトピックでは、Malware Analysisサービスの[サービス]の[構成]ビューにある[アンチウイルス]タブの機能について説明します。[アンチウイルス]タブでは、ネットワークで使用するアンチウイルス ソフトウェアのベンダーを識別することができます。NetWitness Suiteは、Malware Analysisを使って解析したイベントの詳細結果ビューに、これらのベンダーからの結果を含めることができます。

これは、[AV]タブの例です。

機能

[アンチウイルス]タブには、主要なアンチウイルスソフトウェアのベンダーのリストがあります。ベンダーには2つのカテゴリーがあります。最も信頼できる「プライマリ」と、あまり知られていない「セカンダリ」です。それぞれのベンダー名には、チェックボックスとアイコンがあります。ベンダー名のチェックボックスをオンにすると、使用環境で選択したベンダーのアンチウイルスソフトウェアがインストールされていることを識別できるようになります。

この表は、[アンチウイルス]タブのオプションについて説明しています。

機能	説明
ベンダー チェックボックス	提供されたリストから1つ以上のウイルス対策ソフトのベンダーを選択して、システムにインストールされている製品を示します。
適用	[アンチウイルス]タブでの変更を保存します。
リセット	アンチウイルス ベンダーのリストを、ベンダーが選択されていないデフォルト状態にリセットします。

[サービス]の[構成]ビュー: [全般]タブ

このトピックでは、Malware Analysisの[サービス]の[構成]ビュー>[全般]タブの構成設定について説明します。この設定にはMalware Analysisサービスに固有のパラメータがあります。このタブでは以下の項目を構成できます。

- データを収集しているコア サービスのプロセス パラメータ。
- 収集されたデータのリポジトリ。
- データの解析に使用する静的、コミュニティ、サンドボックスのスコア カテゴリーの設定。

詳細な作業手順については、一般的なMalware Analysis設定の構成

これは、[全般]タブの例です。

このタブは次の4つのセクションに分かれています: [常時スキャン構成]、[リポジトリ構成]、[その他]、[モジュール構成]です。

常時スキャン構成セクション

この表は、[常時スキャン構成]セクションの機能について説明しています。

パラメータ	説明
Enabled	Coreサービスの常時ポーリングを無効化または有効化します。デフォルトでは、これは選択されていません(**無効**)。
Query	Decoderがネットワークトラフィックを解析するとき、マルウェアを含む可能性のあるセッションに、**spectrum.consume**という値を持つcontentメタ データ フィールドを作成します。デフォルトでは、Malware Analysisはこの特定のメタ値を持つイベントしか解析を実行しません。クエリを変更すると、Malware Analysisは異なるタイプのイベントを解析するよう構成できます。 クエリを変更して、条件をより広範にすると、Malware Analysisで多くのイベントを解析する必要が生じ、遅延が生じたり、パフォーマンスが低下したりする可能性があります。 デフォルトのクエリは、**select * where content='spectrum.consume'**です。

パラメータ	説明
Query Expiry	通常、Malware AnalysisがCoreサービスに対してメタのクエリを実行すると、数秒で結果が返されます。ネットワークなどが原因でクエリに応答がない場合、Malware Analysisはここで設定する期限が過ぎた後にクエリを放棄します。 デフォルト値は**3,600秒**です。
Query Interval	新しいセッション メタおよびファイルのクエリを実行する間隔です(分単位)。
Meta Limit	Malware AnalysisがCoreサービスに対してクエリを実行するたびに、ここで設定するメタ制限を上限に、一定量のメタを取り出します。この設定とクエリ間隔の設定とあわせて、Malware AnalysisのパフォーマンスをCoreインフラストラクチャで調整できます。 デフォルト値は**25000**です。
Time Boundary	Malware Analysisは、ここで設定する時間の境界値以降のセッションを解析します。この設定は、どれだけさかのぼって解析を始めるかを決めるため、新しいMalware Analysisアプライアンスをインストールするときに最も重要となります。境界値となる時間が大きすぎる場合、Malware Analysisが解析する過去のイベントの数が大量になり、リアルタイムのトラフィックが表示されるまでにかなりの遅延が生じる可能性があります。 デフォルト値は**24時間**です。
ソース ホスト	Malware Analysisアプライアンスのホスト名。 これは、Malware Analysisが解析用のデータを取得するためにクエリを実行するサービスのIPアドレスまたはホスト名です。ソース ホストとしてlocalhostは使用しません。 アプライアンスのモデルとNetWitness Suiteインフラストラクチャの構成に応じて、このソース ホストは異なります。
ソース ポート	Malware Analysisは、このポートをリッスンするRESTサービスを使ってNetWitness Suiteインフラストラクチャと通信します。このポート番号は、ソース ホストとして使用されているCoreサービスのタイプに固有のものです。これは、Coreサービスのアウトバウンド接続に対応します。

パラメータ	説明
Username	ユーザ名です。デフォルト値は**admin**です。 Malware Analysisは、データのクエリを実行するたびにソースホストに認証を行う必要があります。多くの場合、Malware Analysisが使うアカウントは、NetWitness Suiteを通してCoreサービスにアクセスするために使うアカウントと同じものを使用できます。しかし、Malware Analysis専用にCoreサービス上で新しいアカウントを作成することが推奨されています。
User Password	ユーザのパスワード。デフォルト値は**netwitness**です。
SSL	Coreとの通信時にSSLを使用します。Malware AnalysisがCoreサービスと通信するためにSSL接続を使用している場合、このオプションをオンにします。 デフォルトでは、チェックボックスはオフになっています。
Denial of Service (DOS) Prevention	DOS防止機能は、Windows PEのコンテンツを含む2つのエンドポイント間で大量のネットワーク接続を意図的に生成するマルウェアへの防衛手段です。大量の接続が人為的に生成されると、ネットワークを監視しているセキュリティサービスが処理し解析する必要のあるトラフィック量が急増し、結果的にサービスが機能不全に陥ります。そのようなセッションをこの機能を使って特定することにより、解析処理の対象外とすることができます。 デフォルトでは、チェックボックスはオフになっています。

パラメータ	説明
DOS Session Rate Window Length (Seconds)	Malware Analysisは、[**DOS Number Sessions per Rate Window**]パラメータと[**DOS Session Lockout Time (Seconds)**]パラメータに加え、このパラメータを使用することでDOS攻撃を特定し、単一のIPアドレスからのセッションを無視する時間を判断します。 DOS攻撃を特定するために、Malware Analysisは、特定のタイムフレーム内に単一のIPアドレスによって確立されたセッションの数を監視します。このタイムフレームは[**DOSセッション レート ウィンドウ長(秒)**]によって定義します。セッション数が、[**DOS Session Rate Window Length**]で定義された時間(秒数)内に[**DOS Number Sessions per Rate Window**]設定を超えた場合、Malware Analysisは、そのアクティビティをDOSの試みとして識別します。その場合、[**DOS Session Lockout Time (Seconds)**]で指定された期間、該当するIPアドレスからのトラフィックが無視されます。 デフォルト値は**60**秒です。
レート ウィンドウあたりのDOSセッション数	Malware Analysisは、[**DOS Session Rate Window Length (Seconds)**]パラメータと[**DOS Session Lockout Time (Seconds)**]パラメータに加え、このパラメータを使用することでDOS攻撃を特定し、該当するIPアドレスからのセッションを無視する時間を判断します。 DOS攻撃を特定するために、Malware Analysisは、特定のタイムフレーム内に単一のIPソースによって確立されたセッションの数を監視します。このタイムフレームは[**DOSセッション レート ウィンドウ長(秒)**]によって定義します。セッション数が、[**DOS Session Rate Window Length**]で定義された時間(秒数)内に[**DOS Number Sessions per Rate Window**]設定を超えた場合、Malware Analysisは、そのアクティビティをDOSの試みとして識別します。その場合、[**DOS Session Lockout Time (Seconds)**]で指定された期間、トラフィックが無視されます。 デフォルト値は**200**セッションです。

パラメータ	説明
DOS Session Lockout Time (Seconds)	Malware Analysisは、[**DOS Session Rate Window Length (Seconds)**]パラメータと[**DOS Number Sessions per Rate Window**]パラメータに加え、このパラメータを使用することでDOS攻撃を特定し、そのような攻撃を無視する時間を判断します。 DOS攻撃を特定するために、Malware Analysisは、特定のタイムフレーム内に単一のIPアドレスによって確立されたセッションの数を監視します。このタイムフレームは[**DOSセッション レート ウィンドウ長(秒)**]によって定義します。セッション数が、[**DOS Session Rate Window Length**]で定義された時間(秒数)内に[**DOS Number Sessions per Rate Window**]設定を超えた場合、Malware Analysisは、そのアクティビティをDOSの試みとして識別します。その場合、[**DOS Session Lockout Time (Seconds)**]で指定された期間、トラフィックが無視されます。 デフォルト値は**60秒**です。
DOS Garbage Collection Interval (Seconds)	DOS攻撃をトラッキングするために使用される内部メモリ構造に対し、ガベージコレクションを実行します。 メモリ使用量が異常に高い場合は、この設定を小さくすることで、使用されていないメモリを解放する頻度を上げることができます。CPU使用率が異常に高い場合は、この設定を大きくすることで、処理のオーバーヘッドを下げることができます(その分、メモリ使用量は大きくなります)。 デフォルト値は**120秒**です。

リポジトリ構成セクション

Malware Analysisは後で必要になった場合に備えてすべてのファイルを格納します。これらのファイルはユーザインタフェースからダウンロードするか、いずれかのファイル共有プロトコルからアクセスできます。

この表は、[リポジトリ構成]セクションの機能について説明しています。

パラメータ	説明
Directory Path	すべてのファイルは、Malware Analysisアプライアンスの次のディレクトリに格納されています。 **/var/lib/netwitnessnetwitness/spectrum**
File Sharing Protocol	ファイル共有プロトコルの値としてFTP、SAMBA、Noneが可能です。FTPアクセスとSAMBAファイル共有を有効にすると、ユーザはリモートからMalware Analysisに格納されたファイルにアクセスすることができます。これらのファイルにアクセスする場合、認証情報は必要ありません。FTPアクセスに必要なポートはTCP/21です。デフォルトのファイル共有プロトコル設定は**None**です。
Retention (in days)	Malware Analysisでは、リポジトリに格納されているファイルを、指定の日数、保持します。ファイルを削除するまでの保持日数を設定できます。デフォルト値は**60**日です。

その他の構成セクション(10.3 SP2以降)

この表は、その他の構成セクションの機能について説明しています。

パラメータ	説明
Maximum File Size	手動でスキャンできる最大ファイルのサイズを制限します。このパラメータは、「調査およびマルウェア解析ガイド」の「Malwareスキャン用ファイルのアップロード」に説明されている機能に適用されます。デフォルト値は**64 MB**です。 その制限をファイルサイズが超えた場合、ファイルのスキャンがによって禁止されます。

モジュール構成セクション

[モジュール構成]セクションでは、静的(Static)、コミュニティ(Community)、サンドボックス(Sandbox)のスコアカテゴリーを構成できます。

静的解析構成

静的(Static)モジュールは、デフォルトで有効になっている唯一のスコアカテゴリーです。この表は、静的解析を構成するためのパラメータについて説明しています。

機能	説明
Enabled	静的解析を完全に無効化または有効化します。デフォルトでは、これは選択されています(**有効**) 。
Bypass PDF	PDFドキュメントの解析を無効化します。デフォルトでは、これは選択されていません。すべてのPDFファイルは静的解析が行われます。
Bypass Office	Officeドキュメントの解析を無効化します。デフォルトでは、これは選択されていません。すべてのMS Officeファイルは静的解析が行われます。
Bypass Executable	Windows PEドキュメントの解析を無効化します。デフォルトでは、これは選択されていません。すべてのWindows PEファイルは静的解析が行われます。
Validate Windows PE Authenticate Settings via Cloud	Authenticode確認のために、Windows PEファイルがRSA-Netwitness Cloudに送信されるかどうかを指定します。デフォルトでは選択されています。 • 選択されている場合、デジタル署名されているWindows PEファイルは、確認のために(その全体が) ネットワーク経由でRSA-Netwitness Cloudに送信されます。Windows PEファイルがユーザネットワークの外部に出るのを防ぐには、このオプションを無効にする必要があります。 • 選択されていない場合、すべての静的解析はローカルで行われます(Authenticode確認はスキップされます) 。この設定に関係なく、PDFとM/S Officeドキュメントは Authenticode検証の対象にはならず、静的解析ではネットワークk経由で送信されません。

コミュニティ解析構成

デフォルトで、コミュニティ(Community)モジュールは無効になっており、PDFとMS Officeドキュメントが処理されないようにオプションが選択されています。その目的は、ユーザが選択しない限り機微性の高いファイルがネットワークから外部に送信されることを防ぐためです。この表は、コミュニティ解析を構成するためのパラメータについて説明しています。

機能	説明
Enabled	静的解析を完全に無効化または有効化します。デフォルトでは、これは選択されていません(**無効**) 。
Bypass PDF	PDFドキュメントの解析を無効化します。デフォルトでは、これは選択されています。PDFファイルは処理されません。
Bypass Office	Officeドキュメントの解析を無効化します。デフォルトでは、これは選択されています。Microsoft Officeドキュメントは処理されません。
Bypass Executable	Windows PEドキュメントの解析を無効化します。デフォルトでは、これは選択されています。Windows PEファイルは処理されません。

サンドボックス解析構成

デフォルトでは、サンドボックス(Sandbox)モジュールは無効になっており、MS OfficeファイルとPDFファイルは処理されません。その目的は、ユーザが選択しない限り機微情報がネットワークから外部に送信されることを防ぐためです。バイパスの設定をしていない対象のファイルでは、ファイル全体が宛先サンドボックス サーバに送信されます(ファイル コンテンツのハッシュだけではありません) 。

この表は、サンドボックス解析を構成するためのパラメータについて説明しています。

機能	説明
Enabled	サンドボックス解析を完全に無効化または有効化します。デフォルトでは、これは選択されていません(**無効**) 。
Bypass PDF	PDFドキュメントの解析を無効化します。デフォルトでは、これは選択されています。PDFファイルは処理されません。選択しない場合、すべてのPDFファイルはその全体が解析用にサンドボックスに送信されます。
Bypass Office	Officeドキュメントの解析を無効化します。デフォルトでは、これは選択されています。Microsoft Officeドキュメントは処理されません。選択しない場合、すべてのMS Officeファイルはその全体が解析用にサンドボックスに送信されます。

機能	説明
Bypass Executable	Windows PEドキュメントの解析を無効化します。デフォルトでは、これは選択されています。Windows PEファイルは処理されません。選択しない場合、すべてのWindows PEファイルはその全体が解析用にサンドボックスに送信されます。
Preserve Original File Name when Performing Sandbox Analysis	10.3 SP2以降で、ファイルをローカルサンドボックスに送信する際のファイル名のハッシュ機能を有効にします。デフォルトではオフになっています。 **注**：このパラメータを選択しない場合、NetWitness Suiteによってファイルがハッシュされます。

GFI Sandbox設定

[GFI Sandbox]セクションでは、GFIによるサンドボックス処理を有効にし、ローカルでインストールしたGFI Sandboxを構成できます。この表は、GFI Sandboxを構成するためのパラメータについて説明しています。

機能	説明
Enabled	有効な場合、サンドボックス処理はGFIのローカルコピーによって実行されます。デフォルト値は、[**無効**]です。GFIを有効にした場合、残りのパラメータを構成する必要があります。
Server Name	GFI Sandboxサーバ名です。デフォルト値なし。
Server Port	GFI Sandboxサーバのポート番号です。デフォルト値は**80**です。
Max Poll Period	送信されたサンプルの処理を待機する時間を指定します。デフォルト値は**600秒**です。

機能	説明
Ignore Web Proxy Settings	Webプロキシが構成されている環境で、サンドボックスに接続するときにWebプロキシをバイパスするようにMalware Analysisに指定します。Malware AnalysisでWebプロキシが構成されていない場合、この設定は無視されます。

ThreatGrid Sandbox設定

[ThreatGridSandbox]セクションでは、ThreatGridによるサンドボックス処理を有効化し、ローカルでインストールしたThreatGridまたはThreatGrid Cloudをサンドボックス解析に使うかどうかを選択できます。

- ThreatGridのローカルコピーがある場合、ローカルコピーを使うようサンドボックス処理を構成します。
- ThreatGridのローカルインスタンスを購入およびインストールしていない場合、ThreatGrid Cloudを構成します。

この表では、ThreatGridサンドボックスの構成パラメータについて説明します。

注:このサービスを有効にする前に、ThreatGrid提供のサービスキーを構成する必要があります。サービスキーは、このサイトから送信されたサンプルが正当であることをThreatGridが認識できるようにします。

機能	説明
Enabled	有効な場合、サンドボックス処理はThreatGridのローカルコピーまたはThreatGrid Cloudによって実行されます。デフォルト値は、[**無効**]です。
Service Key	サンドボックスモジュールを有効にする前に、ThreatGrid提供のサービスキーを構成する必要があります。サービスキーは、このサイトから送信されたサンプルが正当であることをThreatGridが認識できるようにします。
URL	使用するThreatGridサーバのURL(ローカルでインストールしたThreatGridを使用していない場合)。ThreatGrid Cloudのアクセス先:https://panacea.threatgrid.com

機能	説明
Ignore Web Proxy Settings	Webプロキシが構成されている環境で、サンドボックスに接続するときにWebプロキシをバイパスするようにMalware Analysisに指定します。Malware AnalysisでWebプロキシが構成されていない場合、この設定は無視されます。

[サービス]の[構成]ビュー: [ハッシュ]タブ

このトピックでは、Malware Analysisデバイスの[サービス]の[構成]ビュー> [ハッシュ]タブにある機能について説明します。

このタブでは、Malware Analysisのハッシュフィルタを管理できます。[ハッシュ]パネルのグリッドは、初期状態は空で表示され、Malware Analysisにフィルタが追加されると、それらのフィルタをリストします。このビューでは、ハッシュフィルタの追加、ハッシュフィルタの削除、ハッシュフィルタへのマーク(信頼または信頼されていないことを示す)、ハッシュフィルタの変更と保存、を行うことができます。

これは、[ハッシュ]タブの例です。

これは、[ハッシュの追加]ダイアログの例です。

機能

[**ハッシュ**]タブは、ツールバーとグリッドで構成されています。リストが1ページにおさまらない場合、複数ページに表示されます。

この表は、[ハッシュ]タブのツールバーについて説明しています。

機能	説明
MD5検索	ハッシュを検索するMD5ハッシュを入力します。検索機能では大文字と小文字が区別されます。
追加	[ハッシュの追加]ダイアログを表示します。ここでは、新しいハッシュをハッシュグリッドに追加し、ハッシュが信頼されているかどうかを指定し、ハッシュファイルサイズを提供できます。
編集内容の保存	グリッド内のハッシュに対する追加または編集を保存します。
削除	選択したハッシュをグリッドから削除します。

この表は、ハッシュグリッド列について説明しています。

機能	説明
選択チェックボックス	クリックしてハッシュを選択します。列ヘッダの選択チェックボックスをクリックするとすべてのハッシュを選択します。
信頼済み	ハッシュが信頼または信頼されていないことを示すマークを付けます。
MD5	MD5ハッシュを表示します。
ファイル サイズ	ハッシュ ファイル サイズをKB単位で特定します。

[サービス]の[構成]ビュー: [セキュリティ侵害インジケータ]タブ

このトピックでは、Malware Analysisサービスに適用される、[サービス]の[構成]ビュー> [セキュリティ侵害インジケータ]タブの機能について説明します。このタブでは、4つのスコア モジュールそれぞれについて、データのスコアリングに利用されるルールをどのように使用するかを構成できます。

これは、[セキュリティ侵害インジケータ]タブの例です。

機能

[セキュリティ侵害インジケータ]タブは、ツールバーとグリッドで構成されています。リストが1ページにおさまらない場合、複数ページに表示されます。

この表は、グリッドの機能について説明しています。

機能	説明
モジュール選択リスト	セキュリティ侵害インジケータを表示するスコア モジュールを、All、Network、Static、Community、Sandbox、Yara。
[検索]フィールド	テキストを入力して、グリッド内の[説明]フィールドのテキストを検索できます。
[検索]オプション	説明検索のテキストに一致するルールだけを表示するようグリッドをフィルタします。
[すべて有効化]オプション	グリッドで個別に[有効]列をチェックするのではなく、スコア モジュールのルールをすべて有効化します。
[有効化]オプション	クリックすると指定したルールを有効化できます。
[すべて無効化]オプション	グリッドで個別に[有効]列のチェックを外すのではなく、スコア モジュールのルールをすべて無効化します。

機能	説明
[無効化]オプション	クリックすると指定したルールを無効化できます。
[すべてリセット]オプション	クリックすると、ページのすべての行がデフォルト値にリセットされます。
[リセット]オプション	クリックすると、選択した行がデフォルト値にリセットされます。
[保存]オプション	このページに対して行った変更を保存します。保存せずにページを閉じると、変更は失われます。変更が保存されていない各行の説明には、隅に赤い三角印が表示されます。

この表は、ツールバーの機能について説明しています。

列	説明
選択チェックボックス	ページの個別の行またはすべての行を選択するためのチェックボックス。
有効チェックボックス	セキュリティ侵害インジケータが有効化されている場合、Malware Analysisはセッション データのスコアリングにそのルールを使用します。
高確率チェックボックス	オンの場合、Malware Analysisはルールに合致するセッションにマルウェアが存在する可能性が高いと見なし、ルールをトリガーするイベントが結果グリッドでマークされます。
説明	セキュリティ侵害インジケータの説明。
スコア	ルールをトリガーするイベントの合計スコアに加味するスコアを指定します。デフォルトのスコアが表示されています。スライド バーをドラッグしてスコアを増減するか、スコア ボックスに数値を入力します。

列	説明
ファイルタイプ	ルールが適用されるファイルタイプを表示します。値は、**ALL**、**PDF**、**MS Office**、**Windows PE**のいずれかです。

[サービス]の[構成]ビュー: [統合]タブ

このトピックでは、Malware Analysisの[管理]＞[サービス]＞[構成]ビューにある[統合]タブの機能について説明します。このタブでは、接続をテストし、Malware Analysisサービスを登録することによってコミュニティ スコアリングを有効にすることができます。管理者は、cloud.netwitness.comへの接続および常時スキャン用に構成されたコア サービスへの接続をテストできます。

次の図は、[統合]タブの例です。

機能

このタブには、[RSAクラウド接続のテストと登録]と[常時スキャンの接続テスト]の2つのセクションがあります。以下の表は、機能についての説明です。

機能	説明
[RSAクラウド接続のテストと登録]ボタン	このボタンをクリックすると、cloud.netwitness.comへのアクティブな接続がテストされます。NetWitness Suiteは、サイトとの通信をテストして、プロキシの設定を確認します。RSAコミュニティ サービスを登録するには、有効な接続が必要です。
会社名	これは会社の名前です。これは必須入力フィールドです。
連絡先メール	これは、連絡先メールです。これは必須入力フィールドです。

機能	説明
[EMC社内使用のみ]チェックボックス	これはオプションのフィールドです。EMCのお客様、セールス担当者、デモユーザは、このオプションをオンにして、リクエストが本番サーバの帯域幅を使用しないようにします。このチェックボックスをオンにすると、次の警告が表示されます。`Checking this box may cause a less robust performance because the production server isn't being used.`
[登録]ボタン	[登録]ボタンをクリックすると、すべての必須入力フィールドが入力されていれば、登録が完了します。登録が完了すると、[登録]ボタンが[更新]ボタンに変わります。
[更新]ボタン	登録の完了後に[更新]ボタンが表示されます。
[常時スキャンの接続テスト]ボタン	このボタンをクリックすると、Malware Analysisサービスが、常時スキャン用に選択されたコアサービスに接続できることを確認するテストが開始されます(ソースホスト、ソースポート、ユーザ名、ユーザパスワードは、[全般]タブの指定どおり)。

[サービス]の[構成]ビュー: [IOCサマリ]タブ

このトピックでは、サービスの[構成]ビュー> [IOCサマリ]タブの機能について説明します。このタブには、任意のIOCのサマリ情報を表示できます。各スコア モジュールのグリッドには、特定の期間にわたる、構成されたIOCと、そのIOCに関連づけられた統計情報が一覧表示されます。統計情報には、次の情報が含まれます。

- ネットワーク セッションのイベント数、またはIOCでフラグが付けられた静的イベント、コミュニティ イベント、サンドボックス イベントのファイル数。
- [セキュリティ侵害インジケータ]タブでIOCに構成されている現在のスコア。
- 各スコア モジュールから返されるスコア。

イベントを選択すると、IOCの[マルウェア イベント]ビューまたは[マルウェア ファイル]ビューを表示できます。また、選択したIOCを[セキュリティ侵害インジケータ]タブで開いて、現在のスコアを編集できます。

これは、ネットワーク スコア モジュールの[IOCサマリ]タブの例です。

機能

[IOCサマリ]タブには、スコア モジュールごとに4つのタブ(ネットワーク、静的、コミュニティ、サンドボックス) があります。それぞれのタブには同じフォームと情報が表示され、ツールバーとページ移動が可能なグリッドがあります。

次の表は、各タブの機能について説明しています。

機能	説明
時間範囲	IOCサマリの時間範囲を選択します。選択可能な値 : 直近5分、直近15分、直近30分、直近1時間、直近3時間、直近6時間、直近12時間、直近24時間、直近2日間、直近5日間、早朝、午前、午後、夕方、終日、昨日、今週、先週、カスタム。
[説明]列	IOCの説明が一覧表示されます。
[件数]列	IOCの発生回数が一覧表示されます。[ネットワーク]タブの場合、このカウントはIOCが検出されたイベントの数になります。それ以外のタブの場合、このカウントはIOCが検出されたファイルの数になります。

機能	説明
[現在のスコア]列	[セキュリティ侵害インジケータ]タブで構成されたIOCの現在のスコアが一覧表示されます。
[静的]、[ネットワーク]、[コミュニティ]、[サンドボックス]列	各スコア モジュールからIOCに与えられたスコアが一覧表示されます。
[アクション]ドロップダウン	[アクション]ドロップダウン メニューには、[イベント/ファイルの表示]と[編集]の2つのオプションがあります。[イベント/ファイルの表示]を選択すると、[Investigation]＞[イベント]ビューまたは[ファイル]ビューでIOCが開いて表示されます。このビューは、IOCをダブル クリックして開くこともできます。[編集]を選択すると、[セキュリティ侵害インジケータ]タブでIOCが開き、現在のスコアを編集できます。

[サービス]の[構成]ビュー:[プロキシ]タブ

このトピックでは、Malware Analysisサービスの[サービス]の[構成]ビューにある[プロキシ]タブで構成するパラメータについて説明します。このタブでは、Malware Analysisの、Webプロキシを経由したコミュニティ解析のためのRSA Cloudとの通信、およびサンドボックス解析のためのサンドボックス サービスとの通信を構成できます。ローカル サンドボックス サービスを使用している場合、サンドボックス用のWebプロキシ設定をオフにすることでWebプロキシによるパフォーマンスへの影響を抑えることができます。[**全般**]タブでサンドボックス モジュールを構成し、Webプロキシ設定をバイパスするよう選択できます。

これは、[プロキシ]タブの例です。

機能

この表は、[プロキシ]タブの機能について説明しています。

機能	説明
Enabled	Webプロキシを経由して外部と通信できるよう構成する場合はチェックボックスをオンにします。コミュニティ解析ではRSA Cloudとの通信、サンドボックス解析ではサンドボックス サービスとの通信をプロキシできます。
Automatically detect web proxy settings	[システム]の設定で構成したプロキシ設定を使用するには、チェックボックスをオンにします。
Proxy host	プロキシ ホストのホスト名を入力します。
Proxy port	プロキシ ホストでの通信で使用するポートを入力します。
Users	プロキシ ホストのログオン ユーザ名を入力します。
User Password	プロキシ ホストのログオン パスワードを入力します。
SSL	(オプション) SSLを使った通信を有効にする場合はチェックボックスをオンにします。
[適用]ボタン	選択した設定を送信するには、[**適用**]ボタンをクリックします。

[サービス]の[構成]ビュー: [ThreatGRID]タブ

このトピックでは、Malware Analysisの[**ThreatGRID**]タブで試用版のThreatGrid APIキーを取得するパラメータについて説明します。このタブでは、ThreatGridCloud Sandboxで使用するための試用版ThreatGrid APIキーを取得する方法を提供します。サンドボックス モジュール内のサービスとしてThreatGridを有効にする場合には、このサイトから送信されたサンプルが正当なものであるとThreatGridによって認識されるようにするため、ThreatGridから提供されたサービス キーを構成する必要があります。

ThreatGridが提供するサービス キーを持っていない場合は、このタブを使用してキーを取得できます。キーは、試用版として提供されます。

これは、[ThreatGRID]タブの例です。

機能

この表は、[**ThreatGRID**]タブの機能について説明しています。

機能	説明
名前	姓名を入力します。
役職	役職を入力します。
組織名	組織の名前を入力します。
メール	メール アドレスを入力します。
ユーザID	ThreatGridアクセス用のユーザIDを入力します。
パスワード	ThreatGridアクセス用のパスワードを入力します。
[登録]ボタン	[**登録**]をクリックすると、リクエストを送信できます。