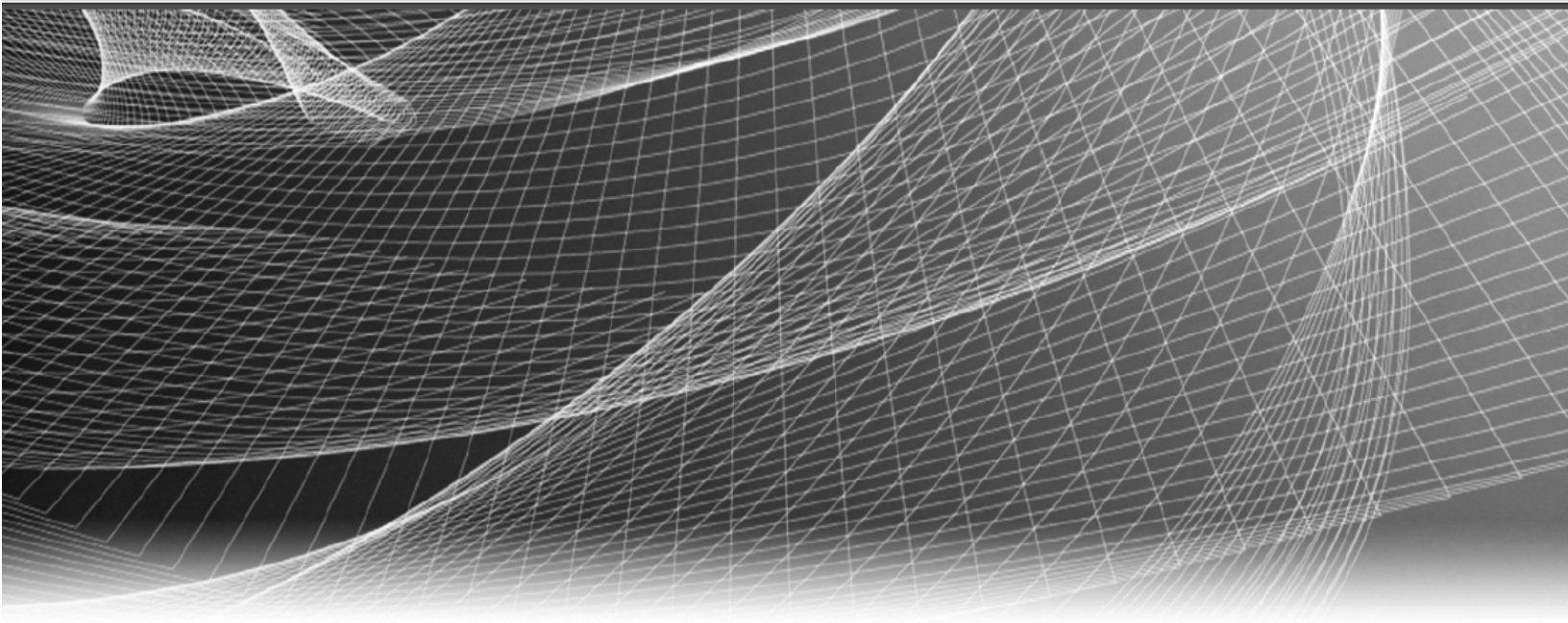


RSA Security Analytics

Security Analyticsスタート ガイド

バージョン 10.6

RSA

EMC²

商標

使用許諾契約

サード パーティ ライセンス

暗号技術に関する注意

配布

目次

Security Analyticsの概要

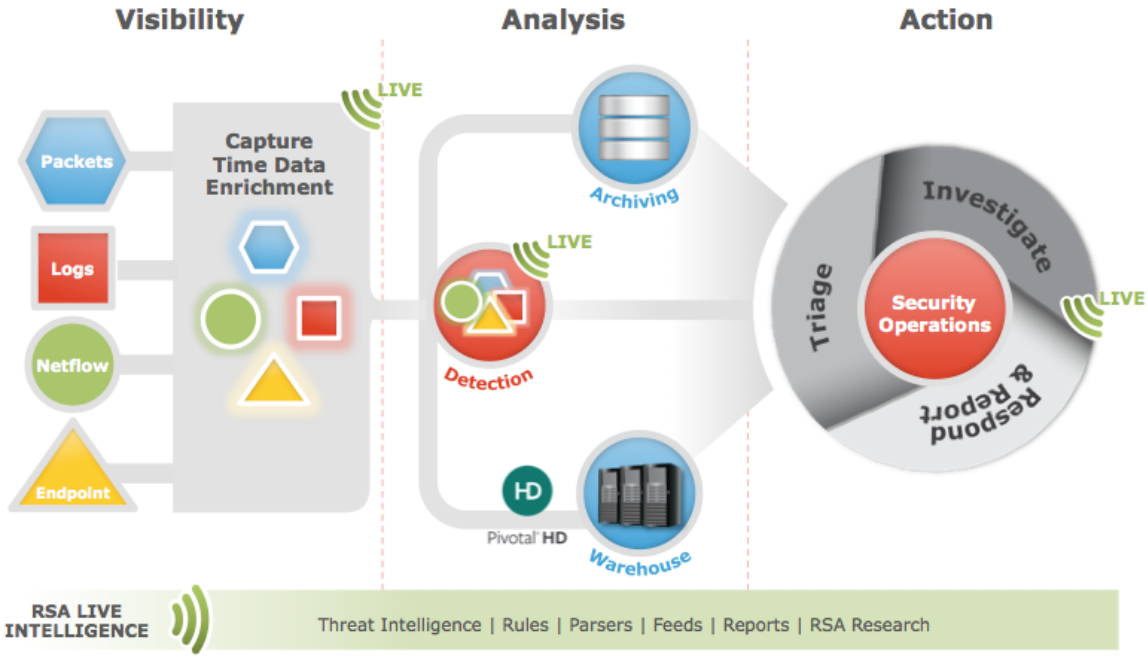
RSA Security Analyticsは、分散型のモジュールで構成される柔軟性の高い導入アーキテクチャを採用しています。このため、組織のニーズに応じてシステムを柔軟に拡張することが可能です。管理者は、Security Analyticsを使用して、パケット データとログ データの2種類のデータをネットワーク インフラストラクチャから収集することができます。このアーキテクチャの特徴を次に示します。

- **分散データ収集**。パケット データは、**Decoder**と呼ばれるホストを使用して収集され、ログ イベントは、**Log Decoder**によって収集されます。Decoderは、レイヤー2～7におけるすべてのネットワーク トラフィック、あるいは数百ものデバイスやイベント ソースのログおよびイベント データを収集、パース、再構築します。**Concentrator**は、ネットワーク トラフィックまたはログ データから抽出したメタデータのインデックスを作成し、エンタープライズ環境全体にわたるクエリーとリアルタイム分析で利用可能にします。また、レポート作成やアラート通知を容易に実行できるようにします。**Broker**は、他のデバイスによって収集されたデータを集計します。Brokerは、構成されたConcentratorのデータを集計します。Concentratorは、Decoderからのデータを集計します。したがって、Brokerはインフラストラクチャ全体の各種のDecoder/Concentratorに保持された複数のリアルタイム データストアを中継する役割を担います。
- **リアルタイム分析**。Security Analytics **ESA(Event Stream Analysis)** ホストは、相関イベントや複雑なイベント処理など、詳細なストリーム解析を高スループットかつ低レイテンシで提供します。ESAでは、Concentratorからの大量の雑多なイベント データを処理することができます。アナリストは、ESAの先進的なイベント処理言語によって、いくつもの異なるイベント ストリームを対象に、フィルタリング、集計、結合、パターン認識、相関を設定することができます。Event Stream Analysisによって、強力なインシデント検出やアラート通知を実装することができます。

  RSA Analytics Warehouse: Hadoopベースの分散コンピューティング システムで構成されます。長期間(数か月、数年など) にわたってセキュリティ データを収集および管理して、分析やレポートを可能にします。Warehouseは、組織におけるデータの分析やアーカイブ、取り出しなどの要件に応じて、3ノード以上のクラスタで構成します。

  Security Analyticsサーバ: Reporting、Investigation、Administration、その他のユーザー インタフェースをホストします。また、Warehouseに保持されたデータからレポートを作成することもできます。
- **キャパシティ**: Security Analyticsのキャパシティ(外部ストレージ) は、直接接続(DAC) またはSAN(ストレージ エリア ネットワーク) を使用したモジュール型のアーキテクチャで構成され、組織における短期間の調査や、長期間の分析およびデータ保存のニーズに対応します。

Security Analyticsの導入は柔軟性に富んでいます。組織におけるパフォーマンスとセキュリティに関する詳細な要件に基づいて、1台から数十台までの物理ホストを使用してアーキテクチャを設計できます。また、Security Analyticsシステムは、仮想化インフラストラクチャ上で動作することも可能です。Security Analytics機能のアーキテクチャを次の図に示します。



システム アーキテクチャは、次のような主要コンポーネントで構成されています: Decoder、Broker、Concentrator、Archiver、ESA、Warehouse Connector、RSA Warehouse。Security Analyticsコンポーネントは、システムとしてまとめて使用することも、個別に使用することもできます。

- SIEM(セキュリティ情報およびイベント管理) 実装では、基本構成として次のコンポーネントが必要です: Log Decoder、Concentrator、Broker、ESA(Event Stream Analysis) 、Security Analyticsサーバ
- フォレンジック実装では、基本構成として次のコンポーネントが必要です: Decoder、Concentrator、Broker、ESA、Malware Analysis。Incident Managementサービスはオプションのコンポーネントです。このコンポーネントは、ESAシステムで稼働し、アラートの優先度を付けるために使用されます。

それぞれの主要コンポーネントについて、次の表で簡単に説明します。

システム コンポーネント	説 明
Decoder/Log Decoder:	• Security Analyticsは、パケット データとログ データの2種 類 のデータを収 集します。 • パケット データ(ネット ワーク パケット) は、組 織 のネット ワークにおける出 口 となるポイントに設 置したネット ワーク タップまたはスパン ポートを介し、Decoderを使 用して収 集されます。 • Log Decoderは、Syslog、ODBC、Windowsイベント 、フラット ファイルの4種 類 のログを収 集 できます。 • Windowsイベント では、Windows 2008のイベント ログを収 集 でき、フラット ファイルではSFTPを介してログを収 集 できます。 • どちらのタイプのDecoderでも、rawデータを取り込 みます。取り込まれたデータは、エンリッチメント や終 了 処 理を経 て、Warehouse やSecurity Analyticsの他 のコンポーネントに集 約されます。 • データ収 集とパースのプロセスは、絶 えず進 化 するオープンなフレームワークで構 成されています。
Concentrator/Broker	• Decoder上 のインデックス作 成 可 能なデータはすべて、Concentratorによってフィルタリングできます。 • Concentratorに保 存されたデータは、メタデータとしてRSA Analytics Warehouseにストリーミングされます。
Archiver	• Archiverは、ログ データのインデックス作 成と圧 縮を行い、それらのデータをアーカイブ ストレージに送 信することによって、長 期 間にわたるログのアーカイブを可 能にするホストです。 • アーカイブ ストレージは、長 期 データ保 存 およびコンプライアンス レポート 作 成 のために利 用 できます。 • Archiverは、Log Decoderからのrawログとログ メタ データを長 期 保 存 のために格 納し、ストレージにDAC(直 接 接 続 機 能) を使 用します。 **注 :** rawパケット やパケット のメタ データは、Archiverに格 納されません。

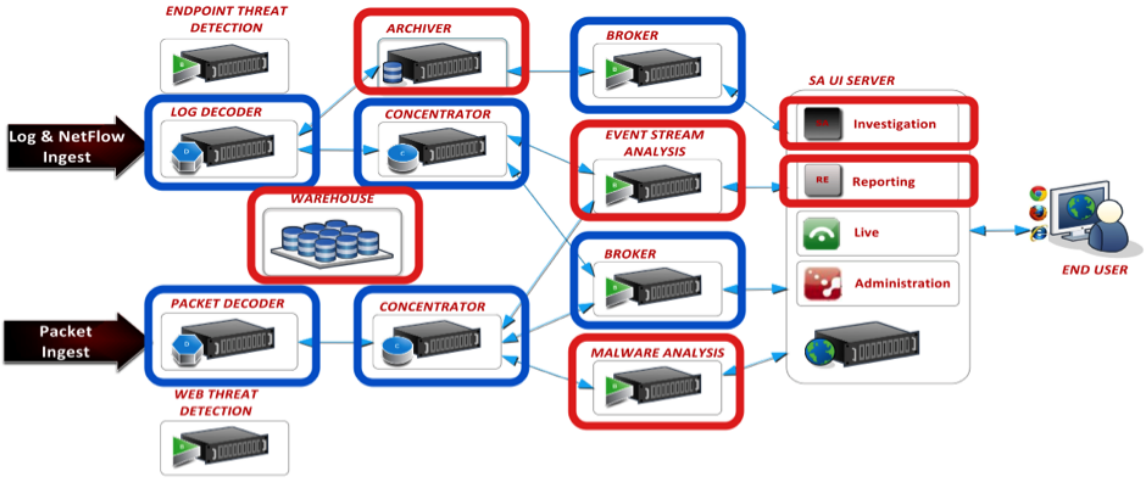
システム コンポーネント	説 明
Event Stream Analysis (ESA)	• ESAホストは、相関イベントや複雑なイベント処理など、ストリーム解析を高スループットかつ低レイテンシで提供します。ESAでは、Concentratorからの大量の雑多なイベント データを処理することができます。 • ESAの先進的なイベント処理言語によって、いくつもの異なるイベント ストリームを対象に、フィルタリング、集計、結合、パターン認識、相関を設定することができます。 • ESAによって、強力なインシデント検出やアラート通知を実現することができます。
Warehouse Connector	• Warehouse Connectorは、メタ データやイベントをDecoderから収集して、Hadoopベースの分散コンピューティング システムにAVRO形式で書き込むことができます。 • Warehouse Connectorは、既存のLog DecoderまたはDecoder上のサービスとして設定することも、仮想環境内の仮想ホストとして実行することもできます。 • Warehouse Connectorには、次のコンポーネントが含まれます。データ ソース、宛先、データ ストリーム。

システム コンポーネント	説明
RSA Analytics Warehouse	• RSA Analytics Warehouseは、セキュリティ情報の分析やレポートの収集、管理を行うためのHadoopベースの分散コンピューティング システムです。また、長期間にわたるデータの格納先としても利用できます。 • RSA Analytics Warehouseがメタ データやイベントをDecoderやLog Decoderから収集して、Hadoopベースの分散コンピューティング システムにAVRO形式で書き込むためには、Warehouse Connectorが必要です。 • Log DecoderとConcentratorで収集および集計したすべてのデータは最終的には、Warehouseに転送されます。 • Warehouseは通常、ストレージ ノードとDAC(Direct Attached Capacity) という2つのユニットで構成されます。 • (メタ データだけでなく) データ全体がRSA Analytics Warehouseに格納され、Security Analyticsから必要に応じて利用することができます。

コア コンポーネントとダウンストリーム コンポーネント

Security Analyticsでは、コア サービスは、データの取得とパース、メタ データの生成、生成されたメタ データとrawデータの集計を行います。コア サービスは、Decoder、Log Decoder、Concentrator、Brokerです。次の図では、青い線で囲まれています。ダウンストリーム システムは、コア サービスに格納されているデータを使用して分析を行います。したがって、ダウンストリーム サービスの動作はSecurity Analytics コアサービスに依存します。ダウンストリーム システムには、Archiver、Warehouse、ESA、Malware Analysis、Investigation、Reportingが含まれます。次の図では、赤い線で囲まれています。

Security Analytics コアサービスは、ダウンストリーム システムなしでも動作し、優れた分析ソリューションを提供できますが、ダウンストリーム コンポーネントによって分析機能を強化できます。ESAは、セッション間およびイベント間だけでなく、ログとパケット データなどの異なるタイプのイベントに対してリアルタイムに相関を分析することができます。Investigationを使用すると、データにドリルダウンして、イベントおよびファイルを調査し、安全な環境でイベントを再構築できます。Malware Analysisサービスでは、ネットワーク セッションおよび関連ファイルに含まれる悪質なアクティビティをリアルタイムかつ自動的に調査します。



Security Analyticsユーザー インタフェース

Security Analyticsが果たす主な役割は次の2つです。

- ブラウザ ベースのグラフィカルなユーザー インタフェースで、Security Analyticsのアーキテクチャ、構成、サービスに対する権限を管理できるようにする。
- Warehouse、Decoder、Concentratorからデータを取得し、解析、アラート通知、レポート作成を行う。
- すべてのSecurity Analyticsモジュールでは、一連のダッシュボード、ビュー、グリッド、ダイアログを使用して、データや構成オプションを共通化された方法で表示します。これにより、ユーザーはシンプルな操作でモジュール間をシームレスに移動できます。ユーザー インタフェースに習熟したユーザーは、特定用途向けのカスタム ダッシュボードを作成することによって、生産性をさらに向上させることができます。たとえば、地域ごとや脅威の種類ごとの情報をカスタム ダッシュボードにまとめて表示できます。

Security Analyticsモジュール

Security Analyticsでは、管理タスク、分析タスク、レポート作成タスクがモジュール単位で構成されており、各モジュールがサービスの機能やタスクの論理的なグループとして編成されています。

- ダッシュボードは、すべてのSecurity Analyticsモジュールのエントリー ポイントであり、他のモジュールの機能へのポータルをユーザーに提供します。
- Administrationモジュールは、ホスト、デバイスとイベント ソース、サービスを管理および監視するためのユーザー インターフェイスです。ホスト、デバイス、イベント ソース、サービスを他の

Security Analyticsモジュールから使用できるようにするには、まずAdministrationモジュールを使用して各コンポーネントを構成する必要があります。

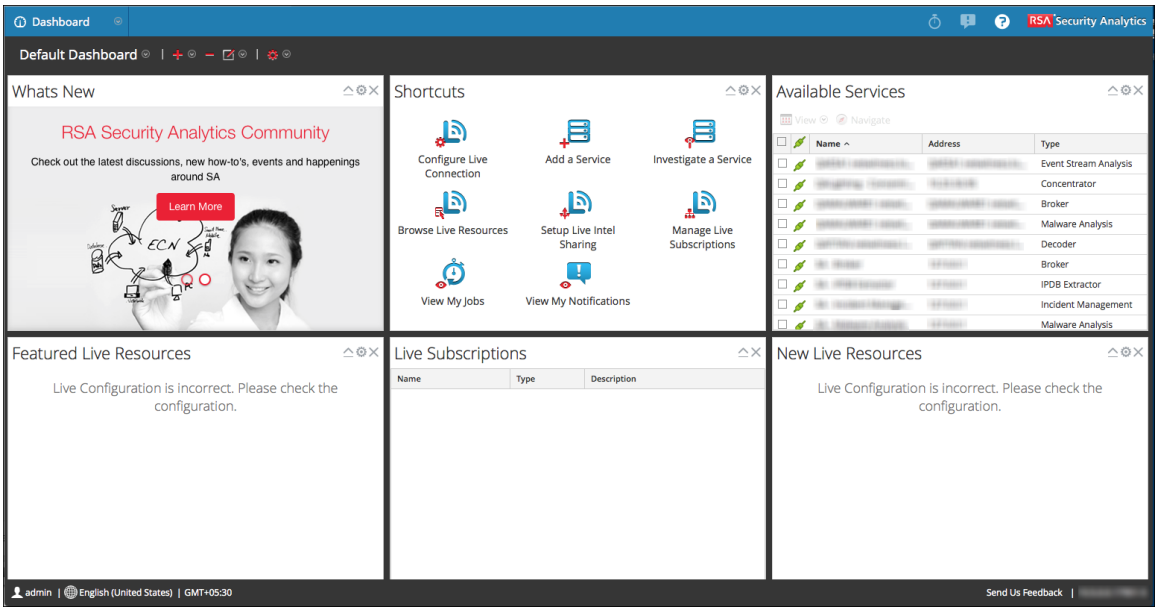
- Investigationモジュールは、Security Analyticsホストによって収集されたパケットを可視化するためのユーザー インタフェースです。Malware Analysisは、自動化されたマルウェア解析のユーザー インタフェースです。
- Liveモジュールは、Liveコンテンツ管理システムを通じてユーザーが利用できるリソースにアクセスし、管理するためのユーザー インタフェースです。
- ReportsモジュールとAlertsモジュールは、レポート作成やアラート通知機能を管理、表示するためユーザー インタフェースです。
- Incidentsモジュールは、Security Analyticsにおけるインシデント管理機能を提供します。インシデント対応プロセスは、インシデント管理機能によって容易にトラッキングすることができます。インシデント管理には、次の機能が用意されています。
  - 一貫性のある方法でインシデントの対応をトラッキングします。
  - 生成されたアラートからセキュリティ インシデントを作成するプロセスを自動化します。
  - チームが根本原因を発見するために役立つビジネス コンテキストと調査ツールを提供します。
  - サード パーティ製ヘルプデスク システムと統合することにより、自動化された方法で改善プロセスをトラッキングします。

ブラウザ ウィンドウに共通する要素

Security Analyticsには、すべてのブラウザ ウィンドウに表示される基本的な要素がいくつかあります。これらの機能は、Security Analyticsのすべてのビューに含まれます。

次のビューを表示するには、次のいずれかの手順を実行します。

- **https://<SA-IP>**にアクセスして、Security Analyticsにログオンします。<SA-IP>はSecurity Analyticsサーバのアドレスです。
- **Security Analytics**メニューで、[**ダッシュボード**]を選択します。



機能

Security Analyticsにアクセスしているすべてのブラウザ ウィンドウには、次の3つの要素が含まれます。

- Security Analyticsメニュー
- Security Analyticsツールバー
- フッター

Security Analyticsツールバー

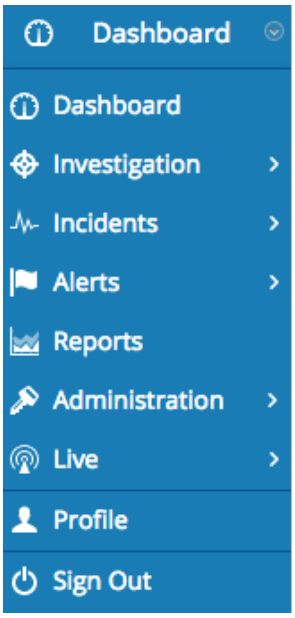
すべてのSecurity Analyticsダッシュボードの上部には、Security Analyticsツールバーがあります。モジュールによって表示されるコンテンツが異なります。ここでは、Security Analyticsツールバーの例を2つ示します。

Security Analyticsツールバーの機能は次のとおりです。

機能	説明
Security Analytics メニュー	各モジュールや、[ヘルプ]、[プロファイル]、[サイン アウト]などにアクセスするオプションが表示されます。一部のモジュールにはサブメニューがあります。
モジュール ビュー オプション	ビューが表示されます。現在表示されているビューのオプションがハイライト表示されます。
Security Analytics メニュー	現在のモジュールがタイトルに表示されます。クリックするとドロップダウン メニューが開き、そこから、モジュールやプロファイルを表示したり、Security Analyticsからサインアウトしたりできます。
ジョブ ボタン 	ジョブ トレイが表示されます。ジョブ トレイには、ユーザーのジョブに関する情報が表示されます。
通知ボタン 	通知トレイが表示されます。通知トレイには、ユーザーに対する通知が表示されます。
[ヘルプ] ボタン 	Security Analyticsのオンライン ヘルプを表示します。

Security Analyticsメニュー

Security Analyticsメニューは Security Analyticsツールバーの左側にあります。



Security Analyticsメニューのオプションは次のとおりです。

メニュー オプション	説明
ダッシュボード	Security Analyticsダッシュボードを表示します。
Investigation	[ナビゲート]ビューが開いた状態でInvestigationモジュールが表示されます。サブメニューには、[ナビゲート]ビュー、[イベント]ビュー、[Malware Analysis]ビューにアクセスするためのオプションがあります。
インシデント	Incident Managementモジュールが表示されます。 サブメニューには、[キュー]ビュー、[アラート]ビュー、[改善]ビュー、[構成]ビューを表示するためのオプションがあります。
アラート	アラート モジュールが表示されます。サブメニューには、[サマリー]、[構成]の各ビューに直接アクセスするためのオプションがあります。
レポート	Reportsモジュールが表示されます。
Administration	Administrationモジュールの[サービス]ビューが表示されます。サブメニューには、Administrationモジュールの[ホスト]、[サービス]、[イベント ソース]、[ヘルスモニタ]、[システム]、[セキュリティ]の各ビューに直接アクセスするためのオプションが表示されます。
Live	Liveモジュールが表示されます。サブメニューには、Liveの[検索]、[構成]、[Feed]の各ビューに直接アクセスするためのオプションがあります。
プロファイル	ユーザー環境設定の構成と通知やジョブの表示を行うための[プロファイル]ビューが表示されます。

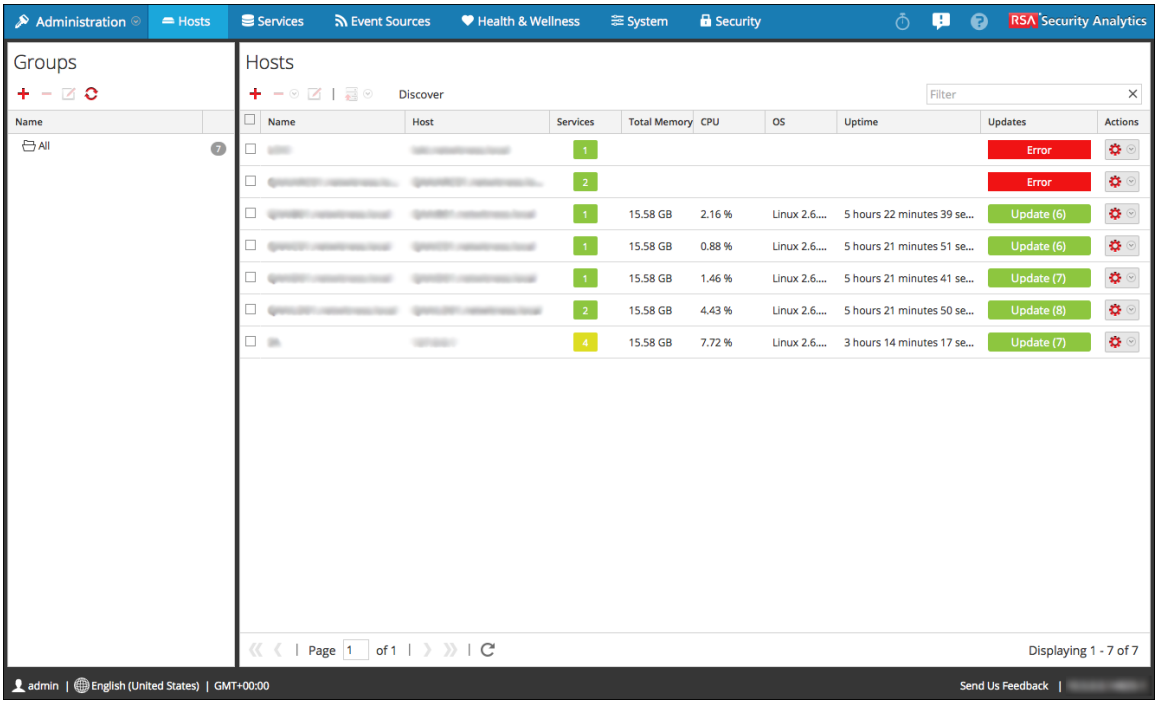
メニュー オプション	説明
サイン アウト	Security Analyticsからサイン アウトします。

ビューに共通する要素

Security Analyticsメニューに表示されるSecurity Analyticsモジュール(Administration、Investigation、Live、Alerts、Reportsなど) はビューと呼ばれ、各ビューはそのモジュール特有の機能を提供します。さらに、Security Analyticsメニューから直接アクセスできる[プロファイル]ビューがあり、ユーザー環境設定のオプションが表示されます。

ビューを表示するには、**Security Analytics**メニューからモジュールを選択します。たとえば、**Security Analyticsメニューで[Administration]**、**[Investigation]**、**[Live]**などを選択します。メニュー上でモジュールにカーソルを合わせると、サブメニューが表示され、ビューを選択することができます。Security Analyticsツールバーからモジュール内の別のビューを選択できます。たとえば、**Administration**には、**[ホスト]**、**[サービス]**、**[イベント ソース]**、**[ヘルスモニタ]**、**[システム]**、**[セキュリティ]**という6個のビューがあります。

この例は、[Administration]の[ホスト]ビューの一部の機能を示しています。



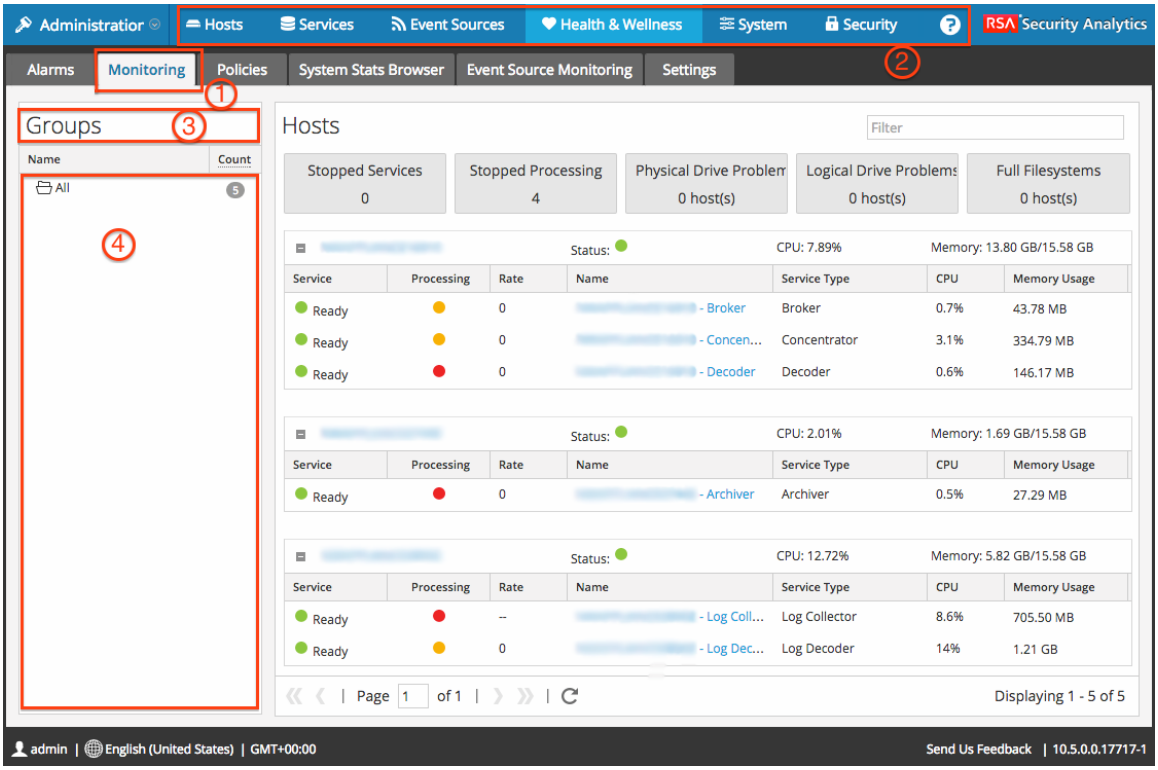
機能

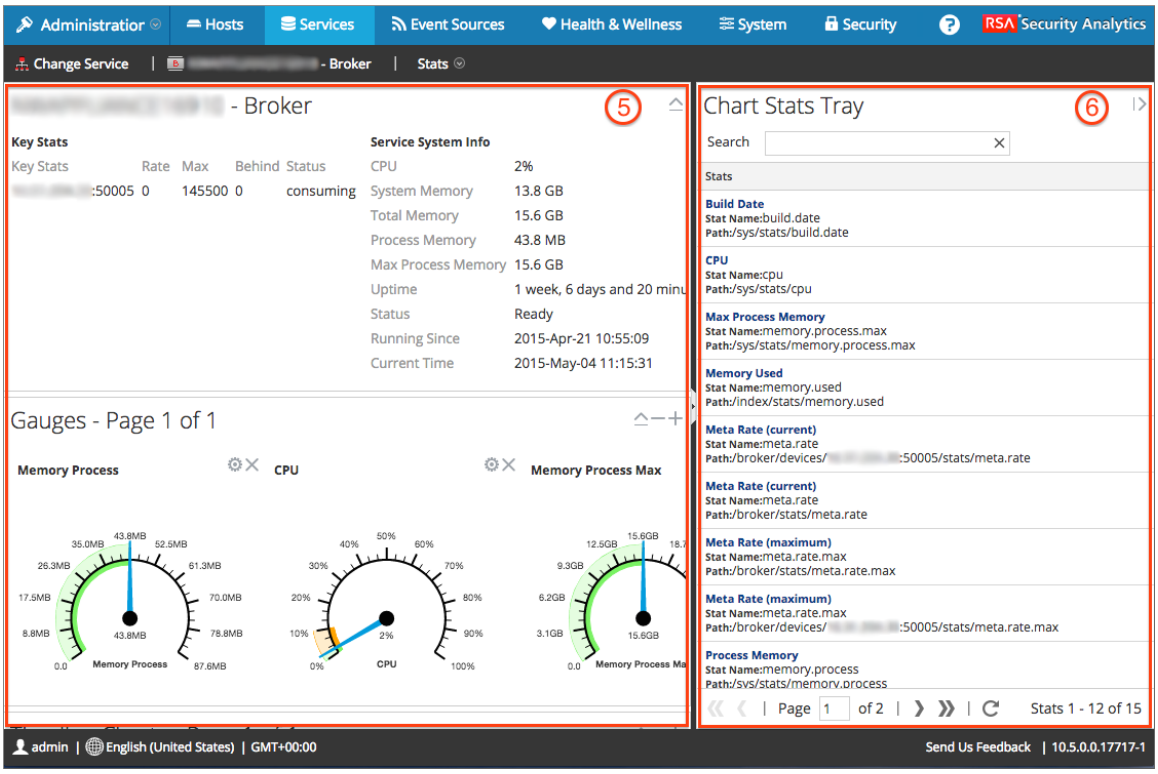
各ビューにはさまざまな機能があります。ビュー内でこれらの機能を組み合わせて使用できます:

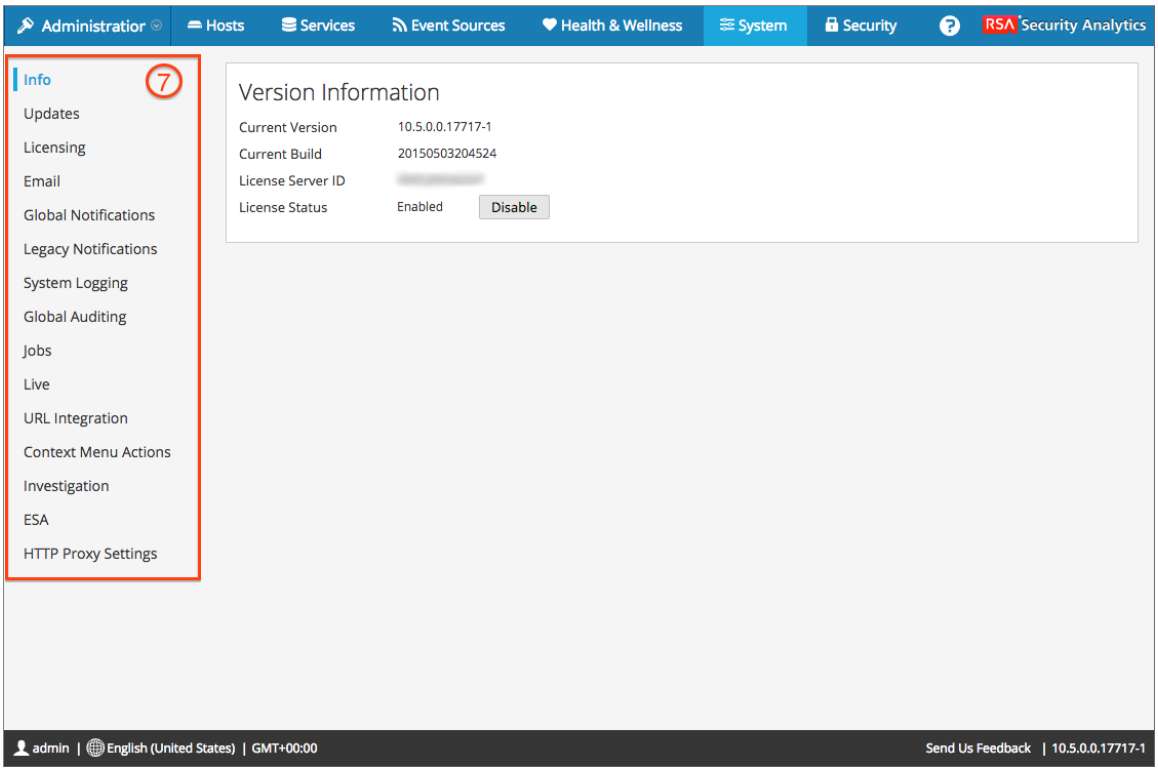
- ツールバー
- セクション
- パネル: オプション パネルとノード ツリーという、2種類の特殊なパネルがあります

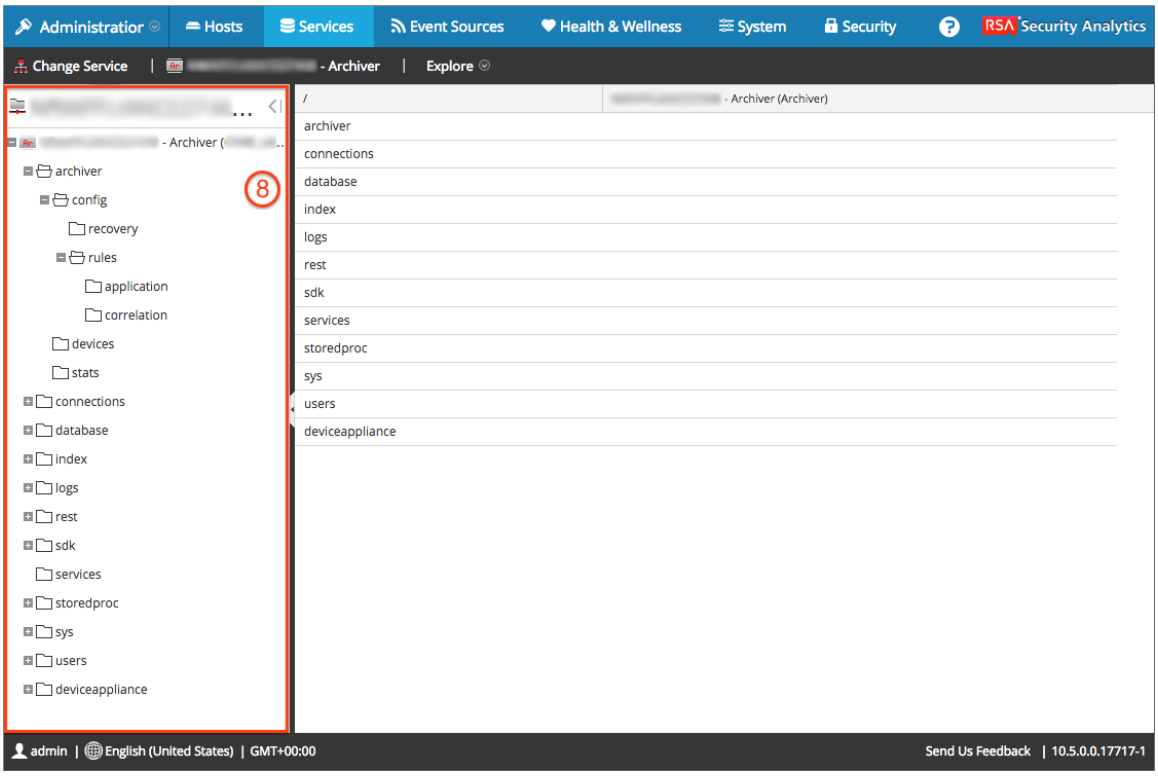
- タブ
- 階層リンク
- グリッドまたは表
- コンテキスト メニュー

ビュー内の一般的なパーツの名前を次の図に示します。




Administration
Hosts
Services
Event Sources
Health & Wellness
System
Security
RSA Security Analytics
Change Service
- Broker
Stats
- Broker
5
Key Stats
Key Stats Rate Max Behind Status
:50005 0 145500 0 consuming
Service System Info
CPU 2%
System Memory 13.8 GB
Total Memory 15.6 GB
Process Memory 43.8 MB
Max Process Memory 15.6 GB
Uptime 1 week, 6 days and 20 minu
Status Ready
Running Since 2015-Apr-21 10:55:09
Current Time 2015-May-04 11:15:31
Gauges - Page 1 of 1
Memory Process
CPU
Memory Process Max
Chart Stats Tray
6
Search
Stats
Build Date
Stat Name:build.date
Path:/sys/stats/build.date
CPU
Stat Name:cpu
Path:/sys/stats/cpu
Max Process Memory
Stat Name:memory.process.max
Path:/sys/stats/memory.process.max
Memory Used
Stat Name:memory.used
Path:/index/stats/memory.used
Meta Rate (current)
Stat Name:meta.rate
Path:/broker/devices/:50005/stats/meta.rate
Meta Rate (current)
Stat Name:meta.rate
Path:/broker/stats/meta.rate
Meta Rate (maximum)
Stat Name:meta.rate.max
Path:/broker/stats/meta.rate.max
Meta Rate (maximum)
Stat Name:meta.rate.max
Path:/broker/devices/:50005/stats/meta.rate.max
Process Memory
Stat Name:memory.process
Path:/sys/stats/memory.process
Page 1 of 2
Stats 1 - 12 of 15
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.5.0.0.17717-1


Administration
Hosts
Services
Event Sources
Health & Wellness
System
Security
RSA Security Analytics
Info
7
Updates
Licensing
Email
Global Notifications
Legacy Notifications
System Logging
Global Auditing
Jobs
Live
URL Integration
Context Menu Actions
Investigation
ESA
HTTP Proxy Settings
Version Information
Current Version 10.5.0.0.17717-1
Current Build 20150503204524
License Server ID
License Status Enabled Disable
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.5.0.0.17717-1



次の表は、前の図に示した各パーツの機能について説明したものです。

番号	機能	説明
1	タブ	パネルの機能を見やすく容易にアクセスできるグループに分けてまとめます。これにより、すべてを表示するためにページを下にスクロールする必要がありません。パネルに多くのオプションがある場合、タブによってパネル内の適切なオプションのグループに容易に移動できます。
2	ツールバー	ツールバーはビュー全体や、セクションごと、パネルごとに表示されることがあります。

番号	機能	説明
3、4	セクション(上から下)	パネル内で、一部のダッシュボードにはセクションがあり、上から下に情報が整理されています。たとえば、[**サービス情報**]ビューの[**サービス**]パネルには2つのセクションがあります。上部が[**サービス**]セクションで、下部が[**セッション情報**]セクションです。パネルの下部にあるセクションを表示するために、下方向へのスクロールが必要になる場合があります。
5、6	パネル(左から右)	ビュー内でパネルが構成されている場合があり、左から右に情報が整理されています。たとえば、[**サービスの統計**]ビューには2つのパネルがあります。左側がメイン パネルで、右側が[**統計チャート トレイ**]パネルです。[**統計チャート トレイ**]は必要な時にのみ使用されるため、折りたたんでメイン パネルの表示を広げることができます。
7	オプション パネル	オプション パネルは、ビュー内で選択できるオプションが一覧表示されるパネルです。オプション パネルにはタイトルがないことがよくあります。ヘッダーなしの選択肢のリストはオプションと呼ばれます。
8	ノード ツリー	ノード ツリーは、展開したり折りたたんだりすることのできるフォルダーを含んだノードのリストです。

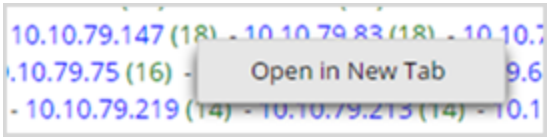
階層リンク

階層リンクには、表示しているビューに到達するまでに選択されたオプションが表示されます。ビューやメニューに戻るには、階層リンクをクリックします。一部のモジュールでは、階層リンクは、追加の機能を持ちます。たとえば、Investigationでは、階層リンクは、現在のドリルダウン ポイントに到達するためのクエリーのシーケンスを表しており、階層リンクから直接クエリーを編集することができます。

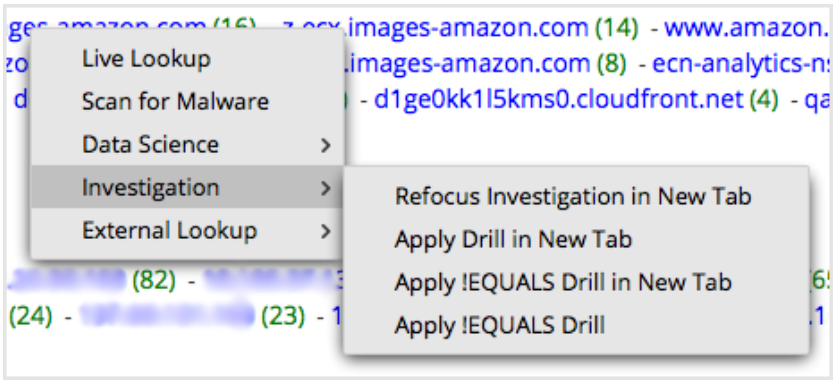
コンテキスト メニュー

コンテキスト メニューでは、選択しているコンテキストに関連するオプションが表示されます。特定のビューで、アイテムを右クリックすると、そのアイテムで使用できるコンテキスト メニューが表示されます。Security Analyticsのドキュメントでは、各モジュールやビューのコンテキスト メニューについて、該当する箇所で説明しています。

[**ナビゲート**]ビューを使用して良く使用するコンテキスト メニューの例を示します。下の図で、メタ値の個数(括弧内の緑色の数値)を右クリックすると、[新しいタブで開く]オプションがコンテキスト メニューに表示されます。



メタ値(青色のテキスト)を右クリックすると、別のコンテキスト メニューが表示されます。このコンテキストでは、[マルウェアのスキャン]、[Liveルックアップ]、[Investigation]モジュールの[新しいタブで再フォーカスして調査]、[新しいタブでドリル ダウン]、[新しいタブで!EQUALSドリル ダウン]、[!EQUALSドリル ダウン]の各オプションが表示されます。



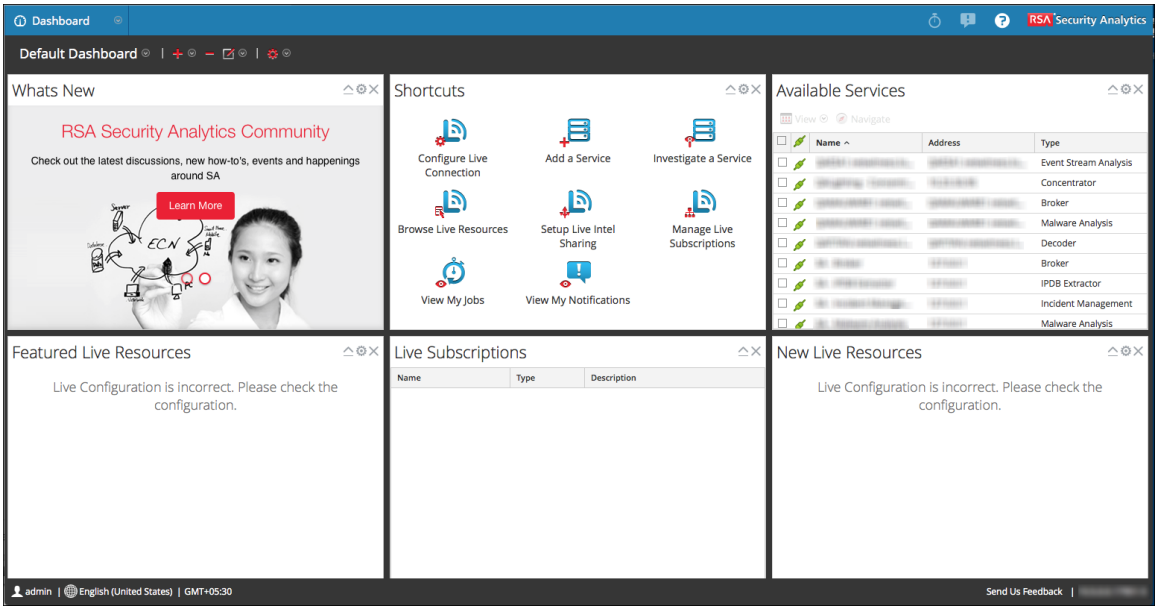
ダッシュボード

ダッシュボードはダッシュレットのグループで構成され、ユーザーにとって重要なさまざまな情報を1か所に表示できます。Security Analyticsでは、ダッシュボードを作成して、Security Analytics環境の全体像を示す概要情報やメトリックを収集したり、日常的な業務に関連性の高い情報のみを表示したりすることができます。

デフォルトでは、Security Analyticsダッシュボードが Security Analyticsへのログイン時に表示されます。このダッシュボードには、画面のカスタマイズの参考になるよう、あらかじめいくつかの便利なダッシュレットが追加されています。すべてのSecurity Analyticsモジュールのダッシュレットは、デフォルトのSecurity Analyticsダッシュボードまたはカスタムの Security Analyticsダッシュボードに追加できます。

Security Analyticsダッシュボードを表示するには、次のいずれかを実行します。

- Security Analyticsにログオンすると、アプリケーションにSecurity Analyticsダッシュボードが表示されます。
- **Security Analytics**メニューで、[**ダッシュボード**]を選択します。



デフォルトのダッシュボード

デフォルトのダッシュボードは、特定のダッシュレットを特定の位置に表示するように構成されています。デフォルトのダッシュボードは、ダッシュボードの構成の例であり、これを基にしてカスタマイズを行うことができます。

- ダッシュレットの操作(編集、追加、移動、最大化、削除)によって、デフォルトのダッシュボードに表示される情報をカスタマイズできます。
- デフォルトのダッシュボードを変更した後でも、デフォルトのレイアウトに復元できます。
- デフォルトのダッシュボードは削除できません

カスタム ダッシュボード

組織内の特定の地域や部門、機能など、特定の用途に使用するカスタム ダッシュボードを作成できます。各カスタム ダッシュボードは、ダッシュボード選択リストに追加されます。

カスタム ダッシュボードを作成すると、次のような操作を行うことができます。

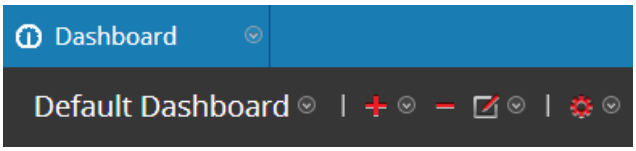
- ダッシュボード選択リストからオプションを選択することによって、ダッシュボードを切り替える。
- カスタム ダッシュボードを削除する。
- ダッシュボードをインポートまたはエクスポートする。

各ダッシュボードには、次のような項目があります。

- ダッシュボード ツールバー
- ダッシュボード タイトルとダッシュボード選択リスト
- ダッシュレット

ダッシュボード ツールバー

現在のダッシュボードのタイトルの隣にあるのがダッシュボード ツールバーです。ダッシュボード ツールバーで、ダッシュボードやダッシュレットに対してさまざまな操作を実行できます。

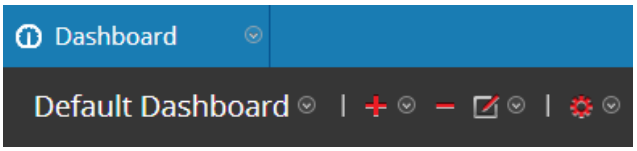


オプション	説明
ダッシュレットの追加	[ダッシュレットの追加]ダイアログを表示します。このダイアログで、現在のダッシュボードにダッシュレットを追加します。
ダッシュボードの削除	カスタム ダッシュボードを削除します。デフォルトのダッシュボードは削除できません。

オプション	説明
ダッシュボード レイアウトの変更	[ダッシュボード レイアウトの変更]ダイアログを表示します。このダイアログでは、5つのオプションのうちのいずれかにダッシュボードのレイアウトを変更できます。
新しいダッシュボードの作成	[ダッシュボードの作成]ダイアログを表示します。このダイアログで、カスタムダッシュボードを定義します。
ダッシュボード名の変更	[ダッシュボード名の変更]を表示します。このダイアログでは、ダッシュボードのタイトルを変更できます。
デフォルトのダッシュボードを復元	デフォルトのダッシュボードを元の表示に復元し、デフォルトのダッシュレットを元の位置に表示します。
ダッシュボードのエクスポート	現在のダッシュボードの構造を含む.cfgファイルを作成します。
ダッシュボードのインポート	以前にエクスポートした.cfgファイルに基づいてダッシュボードを追加します。

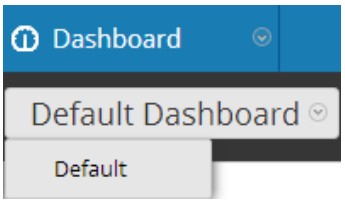
ダッシュボードのタイトル

ダッシュボードのタイトルには、現在のモジュール(ダッシュボードなど) が表示されます。



ダッシュボード選択リスト

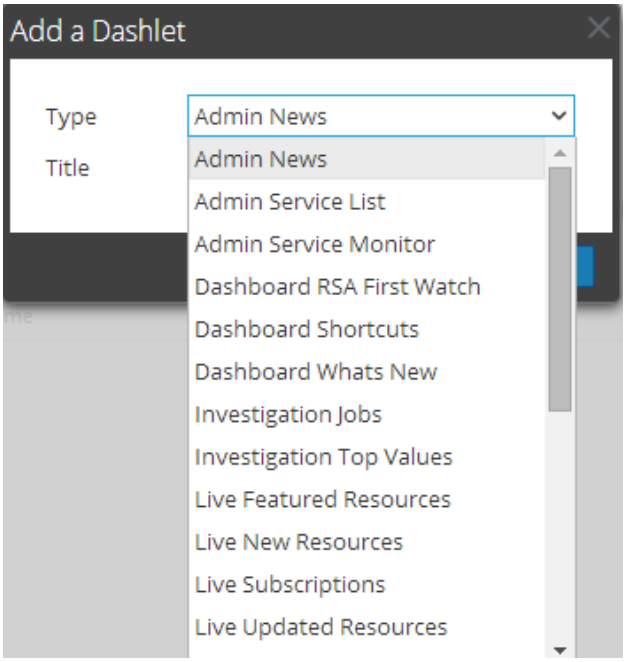
ダッシュボード選択リストでカスタム ダッシュボードにアクセスできます。カスタム ダッシュボードを選択すると、そのタイトルがSecurity Analyticsツールバーの下に表示されます。



ダッシュレット

Security Analyticsでは、ダッシュレットを使用して、システム情報の重要なサブセット、サービス、ジョブ、リソース、サブスクリプション、ルール、インシデント キュー アクティビティ、インシデント アナリスト アクティビティ、その他の情報を表示します。

Security Analyticsモジュールは、[ダッシュレットの追加]ダイアログに表示されるダッシュレットだけを表示できます。メイン ダッシュボードでは、Security Analyticsのすべてのダッシュレットが提供されます。次の図は使用可能なダッシュレットの例です。



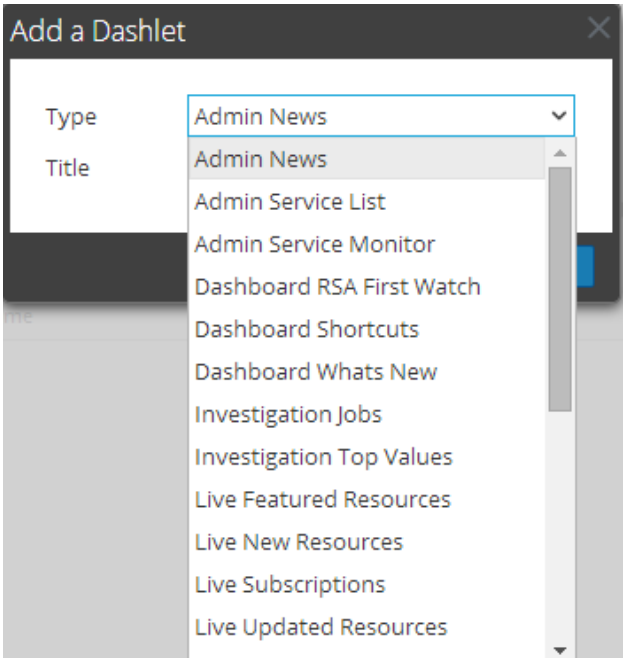
ダッシュレットの操作メニューは各ダッシュレットのタイトル バーにあります。すべてのダッシュレットで共通のコントロールのセットが使用され、特定のダッシュレットで使用するコントロールもタイトル バーに表示されます。

アイコン	名前	説明
	垂直方向に折りたたむ	ダッシュレットを垂直方向に折りたたみ、タイトルのみを表示します。
	垂直方向に展開	ダッシュレットを元のサイズに展開します。
	次のページ	複数のページがあるダッシュレットで、次のページに移動します。

アイコン	名前	説明
	前のページ	複数のページがあるダッシュレットで、前のページに移動します。
	最後のページ	複数のページがあるダッシュレットで、最後のページに移動します。
	最初のページ	複数のページがあるダッシュレットで、最初のページに移動します。
	再ロード	ダッシュレットを再ロードします。
	設定	ダッシュレットの構成可能な設定を表示します。
	最大化	幅(横方向)に収まらない内容を含むダッシュレットで、チャートまたはダッシュレットを最大化してフルスクリーン表示します。
	削除	ダッシュボードからダッシュレットを削除します。

ダッシュレット

すべてのSecurity Analyticsモジュールのダッシュレットは、デフォルトのSecurity Analyticsダッシュボードまたはカスタムのダッシュボードに追加できます。どのダッシュレットにも、次で説明されている共通のコントロールのセットがあります。ダッシュボード次の図は使用可能なダッシュレットの例です。



一部のダッシュレットには、追加の構成パラメーターとコントロールがあります。[Reportsリアルタイム チャート]ダッシュレット、[Malware極めて疑わしいマルウェアの上位リスト]ダッシュレット、[Adminサービス監視]ダッシュレットなどです。これらの追加のコントロールの詳細については、各ダッシュレットに関するトピックを参照してください。

用語

A

用語	説明
Administrationモジュール	Administrationモジュールは、ホスト、デバイス、サービスを管理および監視するためのユーザー インタフェースです。ホスト、デバイス、サービスを他のSecurity Analyticsモジュールから使用できるようにするには、まずAdministrationモジュールを使用して各コンポーネントを構成する必要があります。
Alerts	Security Analytics Alertsモジュールは、自動アラート機能を使用するためのユーザー インタフェースです。
Anonymised data(匿名データ)	「個人データセットから特定の個人を識別可能な要素をすべて削除した場合、そのデータは匿名化されています。匿名化された情報には、相応の努力をすれば個人を再特定できるような要素が残っていてはいけません。適切に匿名化されたデータは個人データではなくなります。」(出典 : EU_DP_LAW_HANDBOOK) この用語は、Security Analyticsデータ プライバシー ソリューションに関連する用語です。
匿名化	Privacy Technology Focus Groupは、匿名化を、クリア テキスト データを非ヒューマンリーダブルな不可逆データに変換するテクノロジーと定義づけています。一方向ハッシュや復号化キーを破棄する暗号化テクノロジーなどが使用されますが、これらに限定されません。この用語は、Security Analyticsデータ プライバシー ソリューションに関連する用語です。
Archiver	RSA Archiverは、ログ データを長期保存するためのアプライアンスです。ログデータのインデックス作成と圧縮を行い、アーカイブ ストレージに送信します。

B

用語	説明

用語	説明
Broker	RSA Brokerは、Security Analyticsネットワークのアプライアンスおよびサービスです。Brokerは、構成済みのConcentratorによって収集されたデータを集計します。Concentratorは、Decoderからのデータを集計します。したがって、Brokerはインフラストラクチャ全体の各種のDecoder/Concentratorに保持された複数のリアルタイム データストアを中継する役割を担います。

C

用語	説明
Capacity (キャパシティ)	Security Analyticsのキャパシティ(外部ストレージ)は、直接接続(DAC)またはSAN(ストレージ エリア ネットワーク)を使用したモジュール型のアーキテクチャで構成され、組織における短期間の調査や、長期間の分析およびデータ保存のニーズに対応します。
コレクション	コレクションは、ログ データを格納するためのログ保存セットです。各コレクションについて、総ストレージ領域に対する使用上限とコレクション内のログを保持する日数を指定できます。コレクションは、Archiverで構成します。
Concentrator	RSA Concentratorは、Security Analyticsネットワークのアプライアンスおよびサービスです。Concentratorは、ネットワークトラフィックまたはログ データから抽出したメタデータのインデックスを作成し、エンタープライズ環境全体にわたるクエリーとリアルタイム分析で利用可能にします。また、レポート作成やアラート通知を容易に実行できるようにします。
コア データベース	パケット、メタ、セッション、インデックス データの組み合わせを指します。
コア サービス	Security Analyticsのコア サービスは、データの取得とパース、メタ データの生成、生成されたメタ データとrawデータの集計を行います。コア サービスには、Decoder、Log Decoder、Concentrator、Brokerがあります。

D

用語	説明
Dashboard (ダッシュボード)	Security Analyticsダッシュボードは、Security Analyticsにログオンしたときに、ブラウザに表示されるユーザー インタフェースです。汎用的な意味で、ダッシュボードと呼ばれる場合もあります。例 : Security Analyticsダッシュボード内にカスタム ダッシュボードを作成することができます。具体的な意味では、「Security Analyticsダッシュボード」は「Unifiedダッシュボード」に代わるものです。
Decoder	RSA Decoderは、Security Analyticsネットワークのアプライアンスおよびサービスです。Security Analyticsネットワークでは、パケット データはDecoderと呼ばれるアプライアンスによって収集され、ログ イベントは、Log Decoderによって収集されます。Decoderは、レイヤー2～7におけるすべてのネットワーク トラフィック、あるいは数百ものデバイスのログおよびイベント データを収集、パース、再構築します。
Downstream system and components (ダウンストリーム システムとコンポーネント)	コア コンポーネントとは逆に、ダウンストリーム システムは、コア サービスに格納されているデータを使用して分析を行います。したがって、ダウンストリーム サービスの動作はSecurity Analyticsコア サービスに依存します。ダウンストリーム システムは、Archiver、Warehouse、ESA、Malware Analysis、Investigation、Reportingです。
Drill Point(ドリルダウン ポイント)	アナリストが[Investigation]ビューでクエリーやフィルタを使用して絞り込んだデータセット。アナリストは、収集されたデータにドリルダウンして、有害なファイルまたはコードが隠れている可能性があるデータを見つけます。

E

用語	説明
Event Stream Analysis (ESA)	RSA ESA(Event Stream Analysis) アプライアンスは、相関イベントや複雑なイベント処理など、詳細なストリーム解析を高スループットかつ低レイテンシで提供します。ESAでは、Concentratorからの大量の雑多なイベント データを処理することができます。アナリストは、ESAの先進的なイベント処理言語によって、いくつもの異なるイベント ストリームを対象に、フィルタリング、集計、結合、パターン認識、相関を設定することができます。Event Stream Analysisによって、強力なインシデント検出やアラート通知を実装することができます。
EPS	秒あたりのイベント数。データを取得するRSAホストの処理能力を測定する単位です。

F

用語	説明
Forensics Implementation (フォレンジック実装)	フォレンジック実装では、Security Analyticsの基本構成に加え、Decoder、Concentrator、Broker、ESA、Malware Analysisのコンポーネントが必要です。Incident Managementサービスはオプションのコンポーネントです。このコンポーネントは、ESAシステムで稼働し、アラートの優先度を付けるために使用されます。

G

用語	説明
Global Audit Logging (グローバル監査ログ)	グローバル監査ログは、Security Analytics監査者への一元的かつリアルタイムな監査ログの提供により、Security Analytics内でのユーザー アクティビティに対する統合的な可視化を実現します。表示される情報には、Security AnalyticsシステムとSecurity Analyticsインフラストラクチャのさまざまなサービスから収集された監査ログが含まれます。

H

用語	説明
Hash (ハッシュ)	機密データを保護するための難読化の方法です。
Host (ホスト)	FQDN(完全修飾ドメイン名)またはIPアドレスで指定される物理機器または仮想マシン。ホストには、すべてのSecurity Analyticsサービス(つまり、Security Analytics Server、Applianceサービス、Archiverサービス、Brokerサービス、Concentratorサービス、Brokerサービス、Decoderサービス(PacketおよびLog)、Hybrid、Malware Analysisサービス、Event Stream Analysisサービス、Log Collectorサービス、Security Analytics Warehouseサービス、Workbenchサービス、Reporting Engineサービス、IPDB Extractorサービス)がインストールされます。

I

用語	説明
Identifiability (識別可能性)	ある情報から個人を特定することができることを意味します。また、直接特定できない場合でも、その情報を元にさらに調査を行えば個人の特定が可能となる場合も該当します。(出典:EU_DP_LAW_HANDBOOK) この用語は、Security Analyticsデータ プライバシー ソリューションの説明で使用されます。
Incident Managementサービス	Incident Managementサービスは、ESAシステムで稼働し、アラートの優先度を付けるために使用されます。
Incidentsモジュール	Incidentsモジュールは、Security Analyticsにおけるインシデント管理機能を提供します。インシデント管理機能を使用すると、インシデント対応プロセスを容易にトラッキングできます。
Index(インデックス)	インデックスは一連のファイルの集合で構成され、メタ値を使用してセッションIDを検索する手段を提供します。

用語	説明
Investigationモジュール	Investigationモジュールは、Security Analyticsアプライアンスによって収集されたパケットとログをビジュアル化および再構築するためのSecurity Analyticsユーザー インタフェースです。

J

用語	説明
Job System (ジョブシステム)	Security Analyticsのジョブ システムで時間のかかるタスクを開始しても、ジョブの実行中にSecurity Analyticsの他の機能は継続して使用することができます。タスクの進行状況を監視できるだけでなく、タスクが完了したこと、また結果が成功か失敗かの通知を受け取ることができます。Security Analyticsのユーザー インタフェースでは、ツールバーからジョブのクイック ビューを開くことができます。

L

用語	説明
Liveモジュール	Liveモジュールは、Liveコンテンツ管理システムを通じてユーザーが利用できるリソースにアクセスし、管理するためのSecurity Analyticsユーザー インタフェースです。
Log Decoder	Log Decoderは、パケットではなくログを収集するタイプのDecoderです。Syslog、ODBC、Windowsイベント、フラット ファイルの4種類のログを収集できます。

M

用語	説明
Malware Analysis	Malware Analysisは専用アプライアンスを使用する場合と、Security Analytics上にサービスを共存させる場合があります。Malware Analysisは自動化されたマルウェア分析に使用され、Investigationモジュールからアクセスできます。

用語	説明
Message Digest(メッセージ ダイジェスト)	一方向ハッシュ関数を使用して、任意の長さのデータを固定長のバイト シーケンスに変換します。データ プライバシー ソリューションで使用されます。
Meta DB(メタ データベース)	メタ データベースには、DecoderまたはLog DecoderによってRAWデータ ストリームから抽出された情報が格納されます。メタ アイテムは、Parser、ルール、Feedが生成します。
Meta ID(メタ ID)	メタ データベース内のメタ アイテムを一意に識別するための数値。
Meta Data (メタ データ) またはMeta Items(メタ アイテム)	Decoderがrawデータを取得してパースし、メタ アイテム(メタ データ) を作成します。
Meta Key(メタ キー)	各メタ アイテムのタイプをクラス分けするための名前。よく使用されるメタ キーとして、ip.src、time、serviceなどがあります。
Meta Value (メタ値)	それぞれのメタ アイテムには、値が格納されています。個々のParser、Feed、ルールによって生成される内容がこの値によって表されます。
従量制ライセンス	従量制ライセンスは、ログ(SIEM) またはネットワーク パケット(ネットワーク モニタリングとネットワーク マルウェア) の1日あたりのスループットに基づいたSecurity Analyticsのライセンス方法です。システムの導入要件とお客様のデータ保存要件を満足するハードウェアを別途購入する必要があります。

N

用語	説明
NetWitnessまたはNextGen デバイス	RSA Broker、Concentrator、Decoder、Log Decoder、Log Collector。NextGenデバイスまたはNetWitnessデバイスという用語が使用されている場合は、コア デバイスと読み替えてください。

O

用語	説明
Out-of-the-box評価版ライセンス	Security Analytics 10.5にはデフォルトで評価版ライセンスが付属しており、全ての機能を90日間使用できます。90日の起点は、Security Analyticsのユーザーインタフェースが構成され、初めて使用されたときです。
Out-of-Compliance(コンプライアンス違反)バナー	ライセンスの有効期限が切れている場合、または使用制限を超過している場合、ログオン時に赤いバナーが表示されます。ライセンスに内部エラーが発生している場合にも、赤いバナーが表示されます。赤いバナーは消すことができません。ライセンスの有効期限が近づいている場合、または使用制限に近づいている場合、システムへのログオン時に黄色いバナーが表示されます。黄色いバナーは[非表示]ボタンをクリックすると、消すことができます。

P

用語	説明
Packet ID(パケットID)	パケット データベース内のパケットやログを一意に識別するための数値。
Packet DB(パケットデータベース)	パケット データベースには、収集されたRAWデータが格納されます。Decoderでは、パケットがネットワークから収集されたままの状態でパケット データベースに格納されます。Log Decoderは、パケット データベースを使用してrawログを格納します。パケット データベースに格納されたRAWデータには、パケットIDでアクセスできます。ただし、このIDは通常、エンド ユーザーからは見えません。
Personal Data(個人データ)	EU法では、個人データは、特定の人または特定可能な人に関連する情報と定義されています。つまり現時点で明白に個人を特定する情報、または追加情報を入手することで明白に特定できる可能性のある情報が含まれます。(出典:EU_DP_LAW_HANDBOOK)

R

用語	説明
RSA Analytics Warehouse	Hadoopベースの分散コンピューティング システムで構成されます。長期間(数か月、数年など) にわたってセキュリティ データを収集および管理して、分析やレポートを可能にします。Warehouseは、組織におけるデータの分析やアーカイブ、取り出しなどの要件に応じて、3ノード以上のクラスタで構成します。メタやイベントをDecoderやLog Decoderから収集して、Hadoopベースの分散コンピューティング システムにAVRO形式で書き込むためには、Warehouse Connectorというサービスが必要です。
Reportsモジュール	Reportsモジュールは、自動化されたレポート作成機能を提供するSecurity Analyticsユーザー インタフェースです。
Roles(ロール)	Security Analyticsでは、ユーザーが実行可能な操作をロールとして定義します。ロールには権限が割り当てられており、各ユーザーにロールを割り当てる必要があります。これにより、ユーザーはロールで許可されている操作を実行できます。

S

用語	説明
Security Analytics Core(旧 NextGen)	Security Analytics Coreスイートには、Decoder、Log Decoder、Concentrator、Broker、Archiver、Workbenchが含まれます。
Security Analytics サーバ	レポート、Investigation、Administrationおよびその他の分析用インタフェースを提供するWebサーバです。また、Warehouseに保持されたデータからレポートを作成することもできます。
Sensitive Data(機微データ)	一部の地域、たとえばEU(欧州連合) では、プライバシーに関わる機微データを処理する情報システムでは情報の保護手段を装備することが規制によって義務づけられています。「いつ、誰が、何を」したかを直接的または間接的に表すデータはすべて、個人データまたは機微データと見なされます。

用語	説明
Service (サービス)	サービスはホスト上で実行され、ログの収集やデータのアーカイブなど、固有の機能を実行します。Security Analyticsサービスには、Archiver、Broker、Concentrator、Decoder、Event Stream Analysis、Incident Management、IPDB Extractor、Log Collector、Log Decoder、Malware Analysis、Reporting Engine、Warehouse Connector、Workbenchがあります。
Service-based(サービス ベース) ライセンス	サービスごとに適用される永続的なSecurity Analyticsライセンスです。有効期限はありません。サービス ベース ライセンスは、ライセンスを必要とするすべてのアプライアンスに適用できます。
Session (セッション)	Packet Decoderでは、単一の論理ネットワーク ストリームをセッションと呼びます。たとえば、TCP/IP接続は1つのセッションです。Log Decoderでは、各ログ イベントが1つのセッションになります。各セッションには、そのセッションを構成するすべてのパケットIDとメタIDへの参照が含まれています。
Session ID (セッション ID)	セッション データベース内のセッションを一意に識別するための数値。
Session DB (セッション データベース)	セッション データベースには、セッションに対してパケットとメタ アイテムを関連づける情報が格納されます。
SIEMの実装	SIEM(Security Information and Event Management) 実装では、Security Analyticsの基本構成として、Log Decoder、Concentrator、Broker、ESA (Event Stream Analysis) 、Security Analyticsサーバ コンポーネントが必要です。

用語	説明
Subscription (サブスクリプション) ライセンス	Security Analyticsのサブスクリプション ライセンスは、特定の期間(12～36か月)に対して提供されます。ライセンスされた後は、サブスクリプション ライセンスをキャンセルまたはダウングレードすることはできません。

T

用語	説明
Transient (一時的) データ	Security Analyticsでは、一時的データはディスクに保存されません。DecoderおよびLog Decoderサービスの[構成]ビューのParser構成セクションまたはカスタム インデックス ファイル内でメタ キーをTransient(一時的)に設定した場合、そのメタ キーはディスクに保存されません。ただし、メモリには保存されるため、上書きされるまで分析に使用することができます。

V

用語	説明
Virtual Host (仮想ホスト)	(正式には仮想アプライアンス) FQDN(完全修飾ドメイン名)またはIPアドレスによって指定された仮想マシン。仮想ホスト上で、Security Analyticsサービス(つまり、Applianceサービス、Archiverサービス、Brokerサービス、Concentratorサービス、Decoderサービス(PacketおよびLog)、Hybrid、Malware Analysisサービス、Event Stream Analysisサービス、Log Collectorサービス、Security Analytics Warehouseサービス、Workbenchサービス、Reporting Engineサービス、IPDB Extractorサービス)を実行できます。Security Analyticsアプライアンスの仮想インスタンスです。

W

用語	説明
Warehouse Connector	Warehouse Connectorは、メタやイベントをDecoderから収集して、Hadoopベースの分散コンピューティング システムにAVRO形式で書き込みます。Warehouse Connectorは、既存のLog DecoderまたはDecoder上のサービスとして設定することも、仮想環境内の仮想アプライアンスとして実行することもできます。

用語	説明
Windows イベント	WindowsイベントはLog Decoderに関係するもので、Windows 2008のイベント ログを収集でき、フラット ファイルではSFTPを介してログを収集できます。

手順

Security Analyticsでは、ユーザーはブラウザを開きログオンする必要があります。Security Analyticsを最大限に活用するには、ジョブや通知の管理方法、ダッシュボードやグリッドの構成方法、言語やタイムゾーンなどのアプリケーション設定のカスタマイズ方法、パスワードの変更方法を把握しておく必要があります。

これらの手順は、Security Analyticsでの使用方法を学ぶすべてのユーザーを対象としています。

Security Analyticsへのアクセス

Security Analyticsへのアクセス方法は、環境によって異なります。ユーザー アカウントには、Security Analyticsの内部ユーザー アカウントと外部ユーザー アカウントがあります。内部ユーザー アカウントはSecurity Analyticsのローカル アカウントで、Security Analyticsにログオンしてロールに基づいた権限を受け取ることができます。外部ユーザー アカウントはSecurity Analyticsの外部で認証を行い、Security Analyticsのロールにマッピングされます。外部ユーザー アカウントを使用している場合に、Security Analyticsにアクセスできない、またはSecurity Analytics内の必要な情報が表示されない場合は、システム管理者にお問い合わせください。管理者が、お使いのアカウントに適切なロールを割り当てることができます。

注：Internet Explorer 10ブラウザ ウィンドウからSecurity Analyticsにログインすると、次のエラーメッセージが表示される場合があります。
`The page can't be displayed.`次の手順に従って、ブラウザのTLS 1.1プロトコルを有効化する必要があります。
[インターネット オプション]＞[詳細設定]＞[設定]＞[セキュリティ]に移動します。TLS 1.1プロトコルの使用が有効化されていることを確認します。[**適用**]をクリックします。ページを再ロードします。

Security Analyticsにログインすると、次のいずれかの状態になります。

- **有効**：Security Analyticsに正常にログオンできます。
- **ロックアウト**：無効な認証情報を使用してログインを何度も試みたため、ログオンできません。この状態は一時的なものです。管理者に問い合わせてください。
- **期限切れ:** Security Analyticsで認証されますが、Security Analyticsにアクセスする前にパスワードを変更する必要があります。

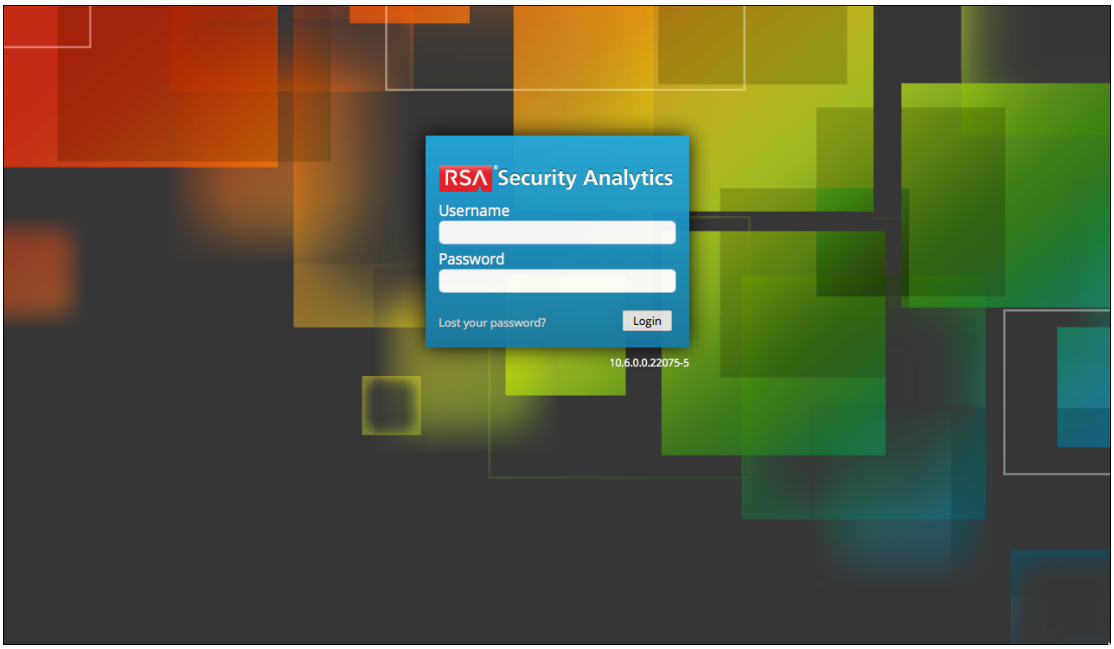
1. 管理者から提供されたSecurity Analyticsアイコンを使用するか、Webブラウザに次のように入力します。

   `https://<hostname or IP address>/login`

   `<hostname or IP address>`にはSecurity Analyticsサーバのホスト名またはIPアドレスを

指定します。

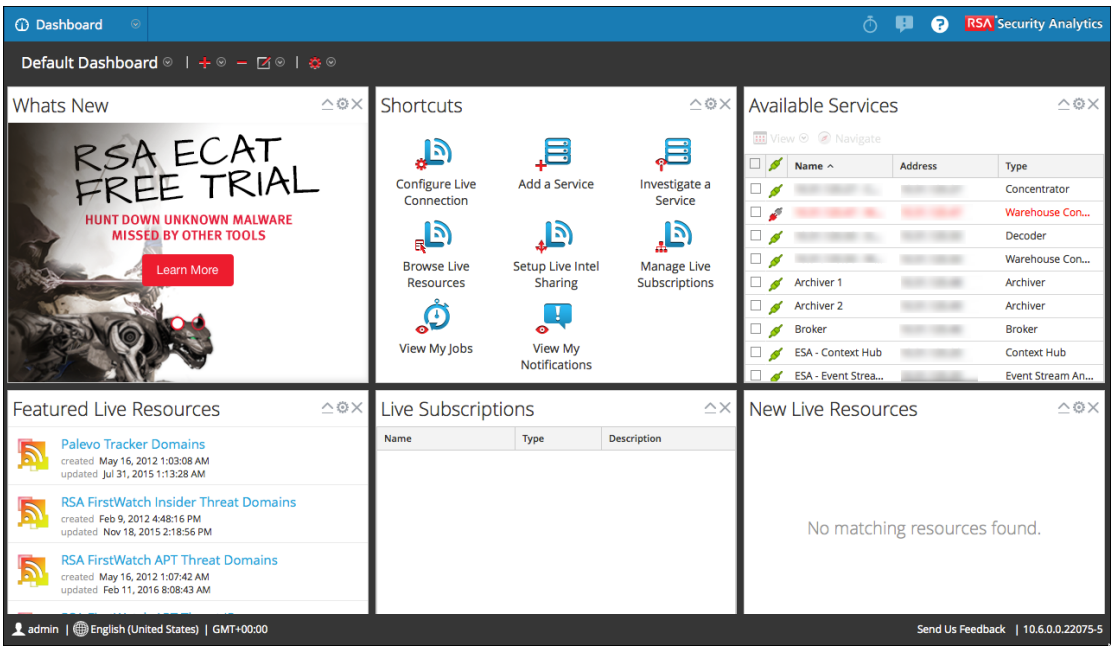
Security Analyticsのログイン画面が表示されます。



2. ユーザー名とパスワードを入力し、[**ログイン**]をクリックします。

正常にログインできたら、ユーザー プロファイルの環境設定に基づいて初期画面が表示されます。

次の図は、Security Analyticsのデフォルト ダッシュボードの例です。

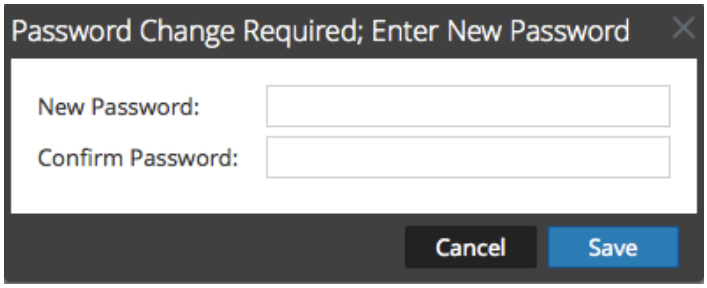


ロックアウトされている場合：

無効なユーザー名またはパスワードを使用してログインを何度も試みた場合は、アカウントがロックされます。アカウントのロックを解除するには、管理者に問い合わせてください。

アカウントの有効期限が切れている場合：

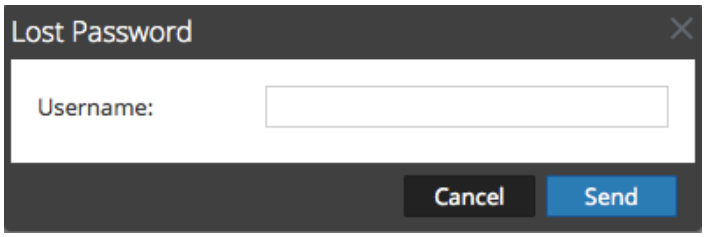
1. ダイアログボックスに新しいパスワードを入力して確認し、[**保存**]をクリックします。



2. [**OK**]をクリックして、パスワードが正常に変更されたことを確認します。
   新しいパスワードは5分以内に入力する必要があります。管理者が設定したセッションとアイドル時間のセキュリティ設定によっては、より短い時間でセッションが終了する場合があります。セッションがタイムアウトになった場合は、古いパスワードでもう一度ログインしてから、パスワードを変更します。

パスワードを忘れた場合：

1. Security Analyticsログイン スクリーンで、[**パスワードを紛失した場合**]リンクをクリックします。
2. [**パスワードの紛失**]ダイアログにユーザー名を入力して、[**送信**]をクリックします。



   指示が記載されたメールを受信します。メールを受信できない場合は、管理者に連絡してアカウントのメールアドレスを追加します。

Security Analyticsに適切にアクセスできない場合：

Security Analyticsに正常にログインできても必要な情報を表示できない場合は、ユーザーアカウントに必要なロールが割り当てられていない可能性があります。管理者に問い合わせてください。

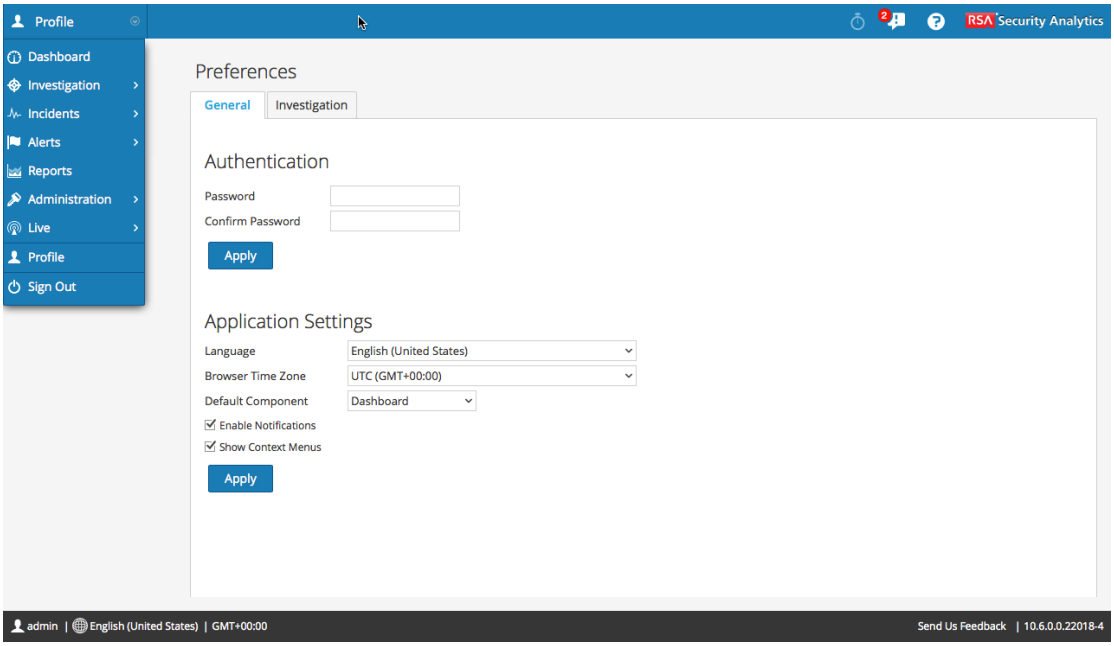
パスワードの変更手順

ユーザーは、Security Analyticsの認証で使うパスワードを[プロファイル]ビュー> [環境設定]パネルから変更できます。ユーザーのパスワードは、adminユーザーの場合を除き、Security Analytics Coreサービスで更新されます。adminユーザーのパスワードはコア サービスに伝播しません。パスワードを変更した後で、ユーザーはログオフしてからログオンし、コア サービスと通信する必要があります。

注:コア サービスの場合、このことは、信頼関係接続を使用しないサービスにのみ当てはまります。コア サービスが信頼関係接続を使用する場合、ユーザーはパスワードを入力しないため、更新は必要ありません。

Security Analyticsパスワードを変更するには:

1. **Security Analytics**メニューで、[**プロファイル**]を選択します。
2. [オプション]パネルで[**環境設定**]を選択します。
   [環境設定]パネルが表示され、[全般]タブが開きます。



3. [**認証**]セクションで、[**パスワード**]フィールドに新しいパスワードを入力します。
4. [**パスワードの確認**]フィールドに、新しいパスワードを再入力します。
5. [**適用**]をクリックします。
   新しいパスワードはすぐに反映され、次にSecurity Analyticsにログオンするときに必要になります。

6. ログオフして新しい認証情報を使用してログオンするには、次の手順を実行します。
   a. **Security Analytics**メニューで[**サイン アウト**]を選択します。
   b. 新しい認証情報を使用してSecurity Analyticsに再びログオンします。

アプリケーション環境設定の構成

このセクションでは、Security Analyticsアプリケーション全般に適用されるユーザー環境設定について説明しています。特にInvestigationに適用される環境設定については、「*Investigationおよび*Malware Analysis*ガイド*」の「**[ナビゲート]ビューおよび[イベント]ビューの構成**」トピックで説明しています。

[環境設定]パネルを使用して、ユーザーの環境設定を表示および管理できます。次の操作を実行できます。

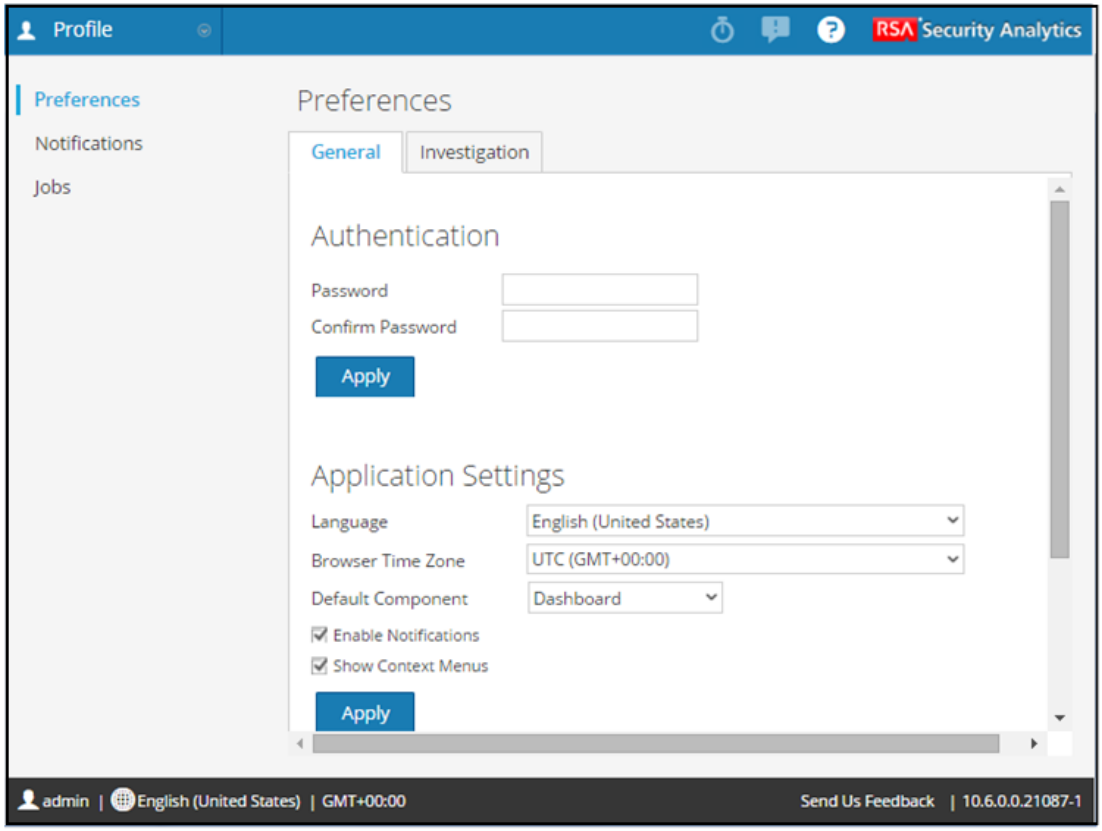
- アプリケーションの表示言語の設定
- ブラウザのタイム ゾーンの設定
- デフォルトのコンポーネントの設定
- 通知の有効化
- コンテキスト メニューの有効化

これらの環境設定は自分のプロファイルに適用されます。

ユーザー環境設定の表示

ユーザー環境設定は次の手順で行います。

1. **Security Analytics**メニューで、[**プロファイル**]を選択します。
2. [オプション]パネルで、[**環境設定**]を選択します。



Security Analyticsの言語、ブラウザのタイムゾーン、デフォルト コンポーネントの設定

表示されているすべてのダッシュボード、ダッシュレット、ビュー、ダイアログの表示言語を変更することができます。Security Analyticsでのローカライズ対象でない言語の場合、デフォルト言語は英語(アメリカ合衆国)になります。表示言語は、Security Analyticsがローカライズされている他の言語に変更できます。これらの設定は[**アプリケーション設定**]セクションで指定できます。

Security Analyticsの表示言語、ブラウザのタイムゾーン、デフォルト コンポーネントの設定を変更するには次の手順を実行します。

1. [**言語**]ドロップダウン リストからローカリゼーションを選択します。
2. [**ブラウザのタイムゾーン**]ドロップダウン リストからタイムゾーンを選択します。
3. [**デフォルトのコンポーネント**]ドロップダウン リストで、Security Analyticsにログオンしたときの最初のビューとなるコンポーネントを選択します。
4. [**適用**]をクリックします。
   選択した設定はすぐに反映されます。

ユーザー アカウントのシステム通知の有効化または無効化

デフォルトでは、新しいユーザー アカウントが作成されると、Security Analyticsシステム通知が有効化されます。各ユーザーは、この設定を変更できます。ユーザー アカウントの通知を有効化または無効化するには次の手順を実行します。

1. [**アプリケーション設定**]セクションで、[**通知の有効化**]チェックボックスをオンまたはオフにします。
2. [**Apply**]をクリックします。
   新しい環境設定はすぐに反映されます。

ユーザー アカウントのコンテキスト メニューの有効化または無効化

デフォルトでは、新しいユーザー アカウントが作成されると、Security Analyticsのコンテキスト メニューが有効化されます。コンテキスト メニューは、ユーザーがビューの特定の個所を右クリックすると表示される追加の機能メニューです。各ユーザーは、この設定を変更できます。ユーザー アカウントのコンテキスト メニューを有効化または無効化するには次の手順を実行します。

1. [**アプリケーション設定**]セクションで、[**コンテキスト メニューの表示**]チェックボックスをオンまたはオフにします。
2. [**Apply**]をクリックします。
   新しい環境設定はすぐに反映されます。

アプリケーションのヘルプの表示

これらの手順は、Security Analyticsの使用中に支援が必要な場合に便利です。Security Analyticsの使用中にヘルプを表示するためのさまざまな方法が用意されています。これには、インライン ヘルプ、ツールチップ、オンライン ヘルプ リンクがあります。

インライン ヘルプの表示

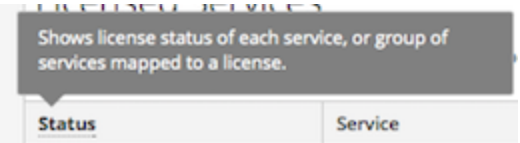
インライン ヘルプでは、Security Analyticsユーザー インターフェイスでユーザーが現在表示しているセクションまたはフィールドで行う操作に関する追加情報が提供されます。インライン ヘルプを表示するには、 の上にマウス ポインターを置きます。インライン ヘルプには、要素の簡単な説明が表示されます。

インライン ヘルプの例 :

ツールチップの表示

ツールチップは、アクション、フィールド、パラメーターに関するテキストまたは追加情報をすばやく表示する方法です。ツールチップは下線付きのテキストに対して表示されます。下線付きのテキストの上にマウス ポインターを置くと、ツールチップが表示され、テキストに関する簡単な説明を確認できます。

ツールチップの例:



オンライン ヘルプの表示

オンライン ヘルプ リンクは、Security AnalyticsからRSAオンライン ドキュメントへの外部リンクです。このサイトにはSecurity Analyticsの完全なドキュメント セットが揃っており、リンクをクリックすると、ユーザー インターフェイスに現在表示されている画面に関連するトピックに直接移動することができます。

オンライン ヘルプから、現在の画面に関連するトピックを表示するには、Security Analyticsツールバーまたはダイアログの  をクリックします。関連するヘルプ トピックが、別のブラウザ ウィンドウに表示されます。トピックには、現在のビューまたはダイアログの特徴や機能が記載されています。そのトピックから関連する手順に素早く移動できます。

次の図に、Security Analyticsツールバーのオンライン ヘルプ アイコンの例を示します。

ダッシュボードの構成

Security Analyticsにさらに詳しくなると、ダッシュボードに迅速かつ簡単に表示したい情報タイプが出てきます。ワークフローをサポートする情報を表示するようにダッシュボードを構成すると、大きなメリットが得られます。

ダッシュボードに関連する操作には、次のような操作があります。

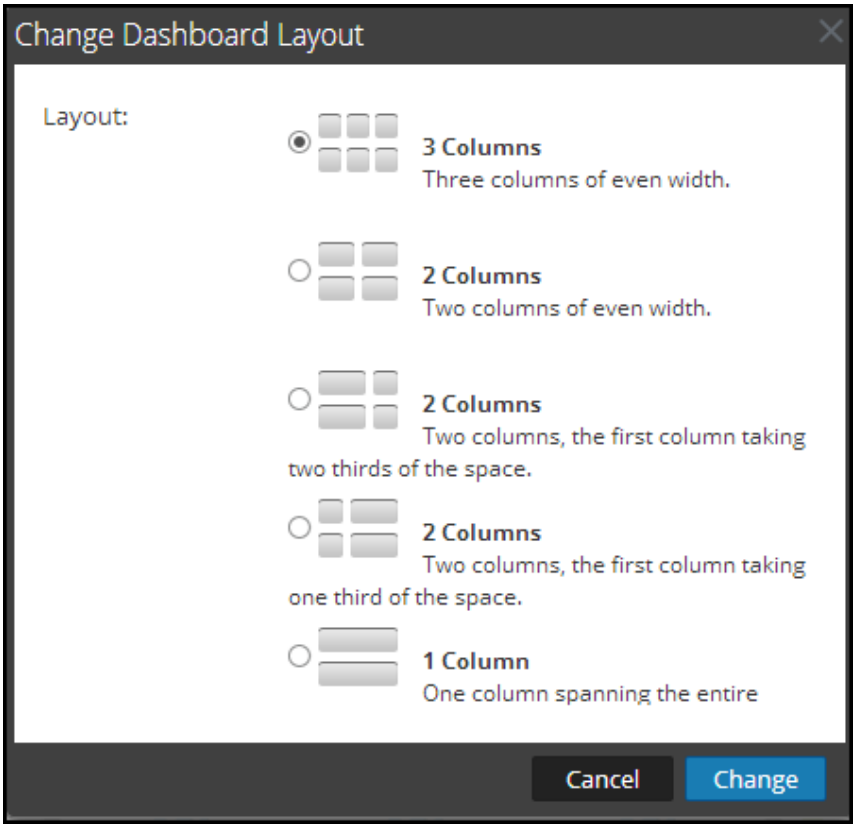
- ダッシュボードの作成と削除
- デフォルトのダッシュボードの復元
- ダッシュボード レイアウトの変更
- ダッシュボードの切り替え
- ダッシュボード内のダッシュレットの追加、削除、移動、編集、最大化
- ダッシュボードのインポートとエクスポート

ダッシュボード レイアウトの調整

Security Analyticsで、**Security Analytics**ダッシュボードまたはカスタム ダッシュボードのレイアウトを変更することができます。

1. レイアウトを変更するダッシュボードに移動します。
2. ダッシュボード ツールバーで、[**編集**]ドロップダウン メニュー( ) をクリックし、[**ダッシュボード レイアウトの変更**]を選択します。

［ダッシュボード レイアウトの変更］ダイアログ ボックスが表示されます。



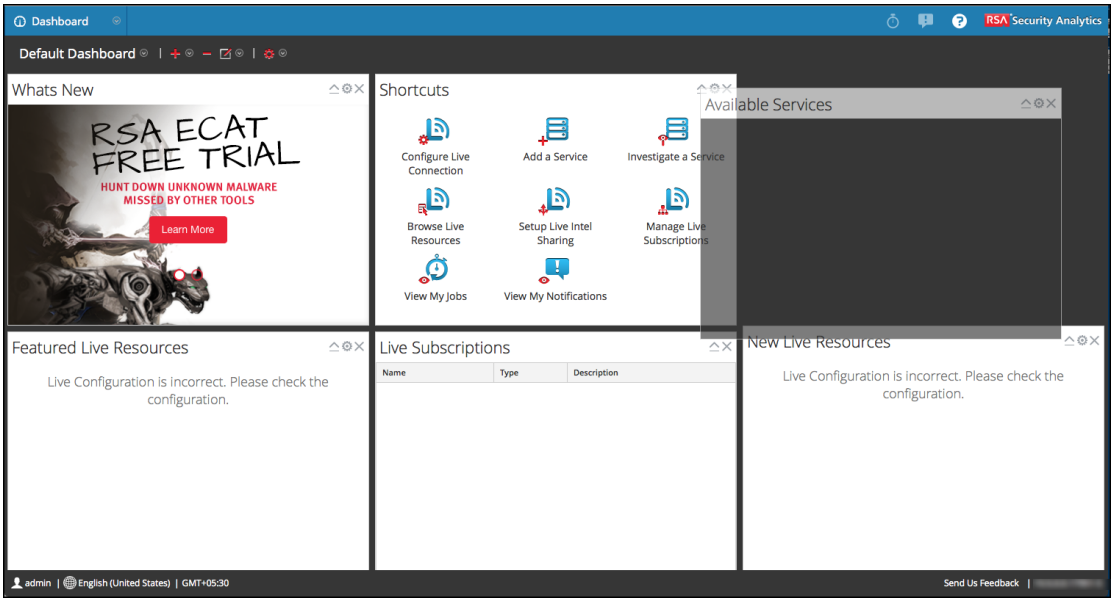
3. ダッシュボードのレイアウトを選択し、［**変更**］をクリックします。
   ダッシュボード レイアウトが、選択したレイアウトに変更されます。

ダッシュレットの別の場所への移動

ダッシュレットは、ダッシュボード上でドラッグ アンド ドロップによって好みの配置に並べ替えることができます。

1. 移動するダッシュレットのヘッダーにカーソルを合わせます。
   ダッシュレット上に方向カーソル ✣ が表示されます。移動するダッシュレットのヘッダにカーソルを合わせます。
2. マウスをクリックし、そのままウィンドウを新しい位置にドラッグします。
   下の画面は、［Available Services］ダッシュレットを、列1の一番下から列3の一番上に移

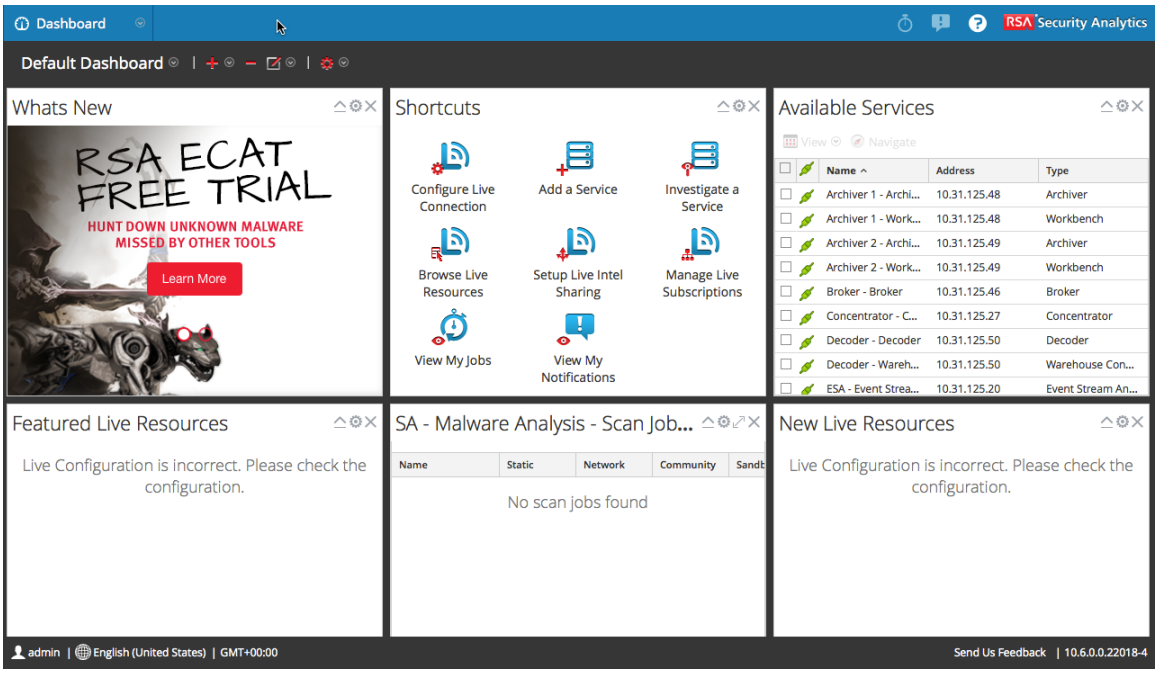
動するイメージです。



3. ダッシュレットを目的の位置に移動したら、マウス ボタンを離してドロップします。
   移動先にもともと配置されていたダッシュレットは下へ移動します。

単体ダッシュレットの最大化

このトピックでは、ダッシュレットを同じダッシュレット タイトルのまま、メインのSecurity Analytics ダッシュボードの領域全体で開く方法について説明します。たとえば、次の図の[スキャン ジョブ]ダッシュレットをSecurity Analyticsダッシュボードの領域全体で表示できます。列またはチャートが多いダッシュレット、たとえば、一部のReportingダッシュレットは、スクロールしなくてもコンテンツ全体が表示できるように最大化すると見やすくなります。

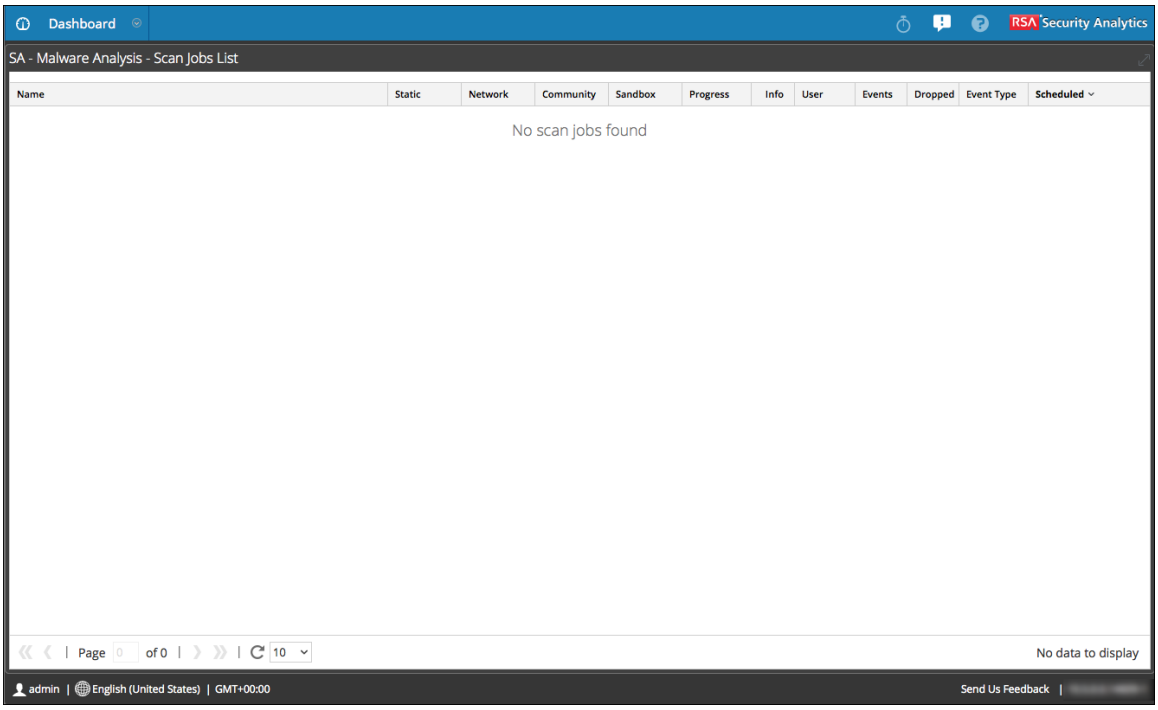


1. ダッシュレットを最大化するには、ダッシュレットのタイトルバーにある最大化コントロールアイコンをクリックします。

   ダッシュレットが全画面表示されます。

2. ダッシュレットを最大化するには、ダッシュレットのタイトルバーにある最大化コントロールアイコンをクリックします。

   ダッシュレットが全画面表示されます。



デフォルトのダッシュボードの復元

Security Analyticsのデフォルトのダッシュボードをカスタマイズした後、[**アクション**]ドロップダウンメニュー( ) の[**デフォルトのダッシュボードを復元**]オプションを使用してダッシュレットを元のレイアウトに復元できます。復元するダッシュボードを表示する必要があります。

1. カスタマイズされたSecurity Analyticsダッシュボードに移動します。
2. ダッシュボード ツールバーで、[**アクション**]ドロップダウンメニュー( ) をクリックし、[**デフォルトのダッシュボードを復元**]を選択します。
   デフォルトのダッシュボードの元のレイアウトが復元されます。

ダッシュレットの追加と管理

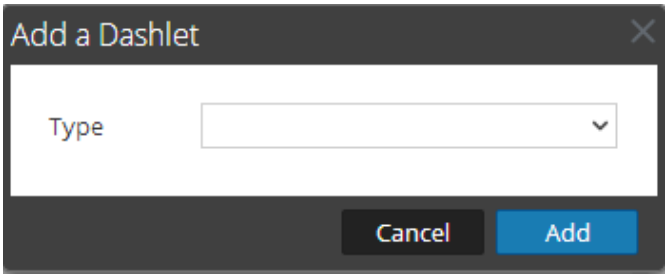
デフォルトのダッシュボードにダッシュレットを追加するか、便利な独自のダッシュレット セットを使用してカスタム ダッシュボードを作成し、ワークフローをより効率的にすることができます。一部のダッシュレットには、外観またはダッシュレットのコンテンツをカスタマイズする構成オプションがあります。

ダッシュレットの追加

Security Analyticsでダッシュボードをカスタマイズする場合には、Security Analyticsダッシュボードまたはカスタム ダッシュボードにダッシュレットを追加できます。Security Analyticsダッシュボードには、その名前のとおり、Security Analyticsのダッシュレットがすべてまとめられています。[ダッシュレットの追加]ダイアログには、新しいダッシュレットの名前や構成可能なパラメータを定義する手段が用意されています。

1. ダッシュレットを追加するダッシュボードに移動します。
2. ダッシュボード ツールバーで、 をクリックし、ドロップダウン メニューから[**ダッシュレットの追加**]を選択します。

   [ダッシュレットの追加]ダイアログが表示されます。

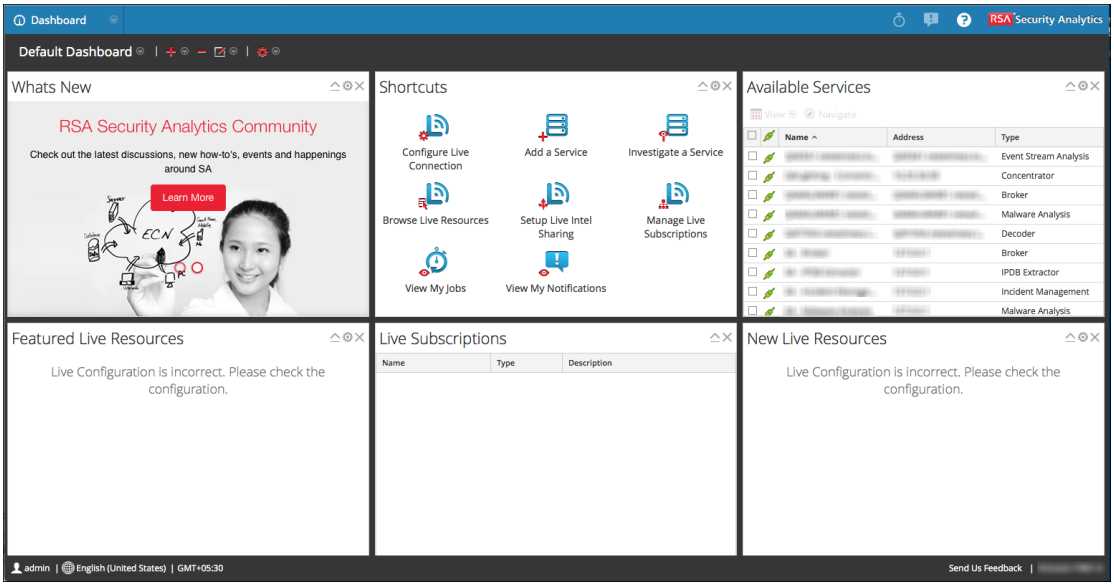


3. [**タイプ**]選択リストをクリックして利用可能なダッシュレットのタイプを表示し、追加するダッシュレットのタイプ([Adminサービス監視]など) を選択します。

[**ダッシュレットの追加**]ダイアログで追加の構成可能なフィールドが表示されます。表示されるフィールドはダッシュレットによって異なります。たとえば、[**Adminサービス監視**]ダッシュレットでは、ダッシュレットのタイトルと監視するサービスのタイプを定義します。すべてのダッシュレットには、タイトルがあります。

4. ダッシュレットのタイトルを入力します。タイトルには、英字、数字、特殊文字、空白を入力できます。たとえば、タイトルを[**サービス監視ダッシュレット**]とします。
5. これ以外にダッシュレットの構成可能なフィールドがある場合は、適切な値を設定します。複数のサービスタイプを選択できます。
6. 必須入力フィールドをすべて構成したら、[**追加**]をクリックします。

ダッシュボードにダッシュレットが追加されます。



ダッシュレットのプロパティの編集

一部のダッシュレットは読み取り専用であり、プロパティを構成できません。その他のダッシュレットは構成可能で、ユーザーはダッシュレットに表示されるデータをカスタマイズできます。編集可能なプロパティを持つダッシュレットには、編集用のプロパティウィンドウを起動する設定アイコン ⚙ があります。

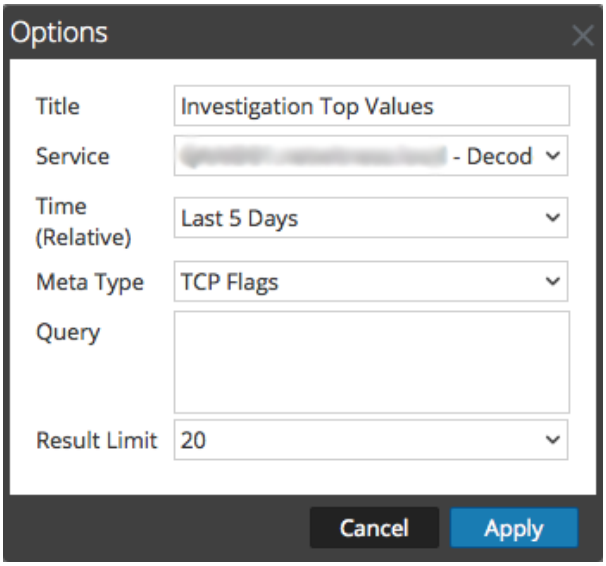
編集可能なプロパティがないダッシュレット([Liveサブスクリプション]ダッシュレットなど) の場合、タイトルバーに設定アイコンは表示されません。

多くのダッシュレットではタイトルを編集できます。構成可能なプロパティを持つダッシュレットの例として、[Adminサービス監視]ダッシュレットでは、次のプロパティを編集できます。

- ダッシュレットの表示タイトル。
- 監視するサービスのタイプ。たとえばDecoderのみを監視したり、DecoderとConcentratorを監視するよう構成できます。

ダッシュレットに表示される情報の種類と量を指定するためのパラメータを持つダッシュレットもあります。例えば、カスタムInvestigationダッシュボードに、3つのダッシュレットを追加します。3つそれぞれに設定アイコンが表示されます。

1. ダッシュレットのオプションを表示および変更するには、ダッシュレットのタイトルバーで設定アイコン をクリックします。
   [**オプション**]ダイアログが表示されます。



2. 表示されているプロパティを変更します。たとえば、[Investigation 上位の値]ダッシュレットでは、結果の件数を20から40に変更できます。
3. [**Apply**]をクリックします。
   変更が適用されます。

ダッシュレットの削除

1. ダッシュレットのタイトルバーにある削除アイコンをクリックします。
   [**ダッシュレットの削除**]ダイアログで、ダッシュレット削除の確認を求められます。
2. 削除する場合は、[**はい**]をクリックします。ダッシュレットがダッシュボードから削除されます。
   削除しない場合は、[**いいえ**]をクリックします。

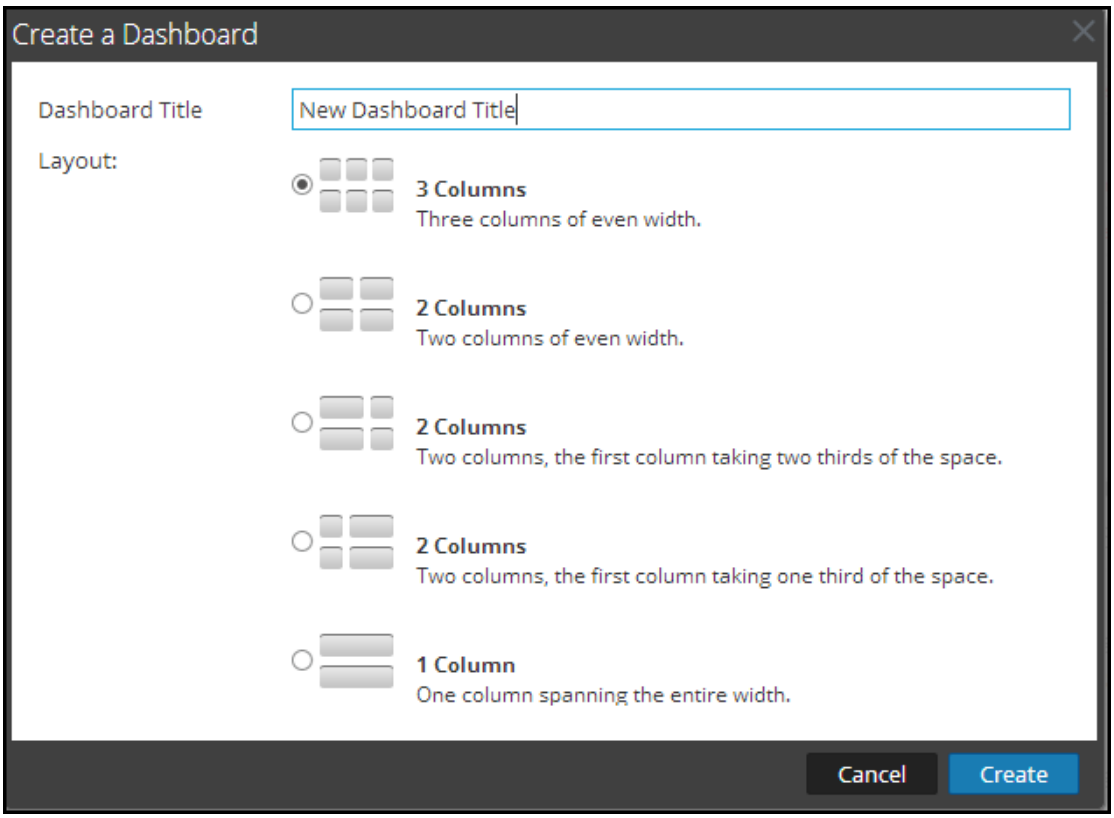
カスタムダッシュボードの使用

ユーザーのサイトや運用管理手法に合わせてカスタムダッシュボードを作成し、Security Analyticsの表示をカスタマイズすることができます。カスタムダッシュボードを作成するのは、次のような理由からです。

- 関連する機能を1つのダッシュボードに統合する。
- すべてのモジュールのダッシュレットをまとめたUnifiedダッシュボードを作成する。
- ネットワークロケーションごとの複数のダッシュレットを統合するダッシュボードを作成する。
- 特定のモジュール機能の一覧画面を作成する。
- 特定のシナリオに特化したダッシュレットを統合する。

カスタム ダッシュボードの作成

1. **Security Analytics**ダッシュボードで、＋ ＞［**新しいダッシュボードの作成**］を選択します。
   ［ダッシュボードの作成］ダイアログが表示されます。



2. 新しいダッシュボードのタイトルを入力します。タイトルには、英字、数字、特殊文字、空白を入力できます。最大長は半角英数255文字です。
3. 新しいダッシュボードのレイアウト オプションを選択します。
   ダッシュボードが作成され、ダッシュボード選択リストに追加されます

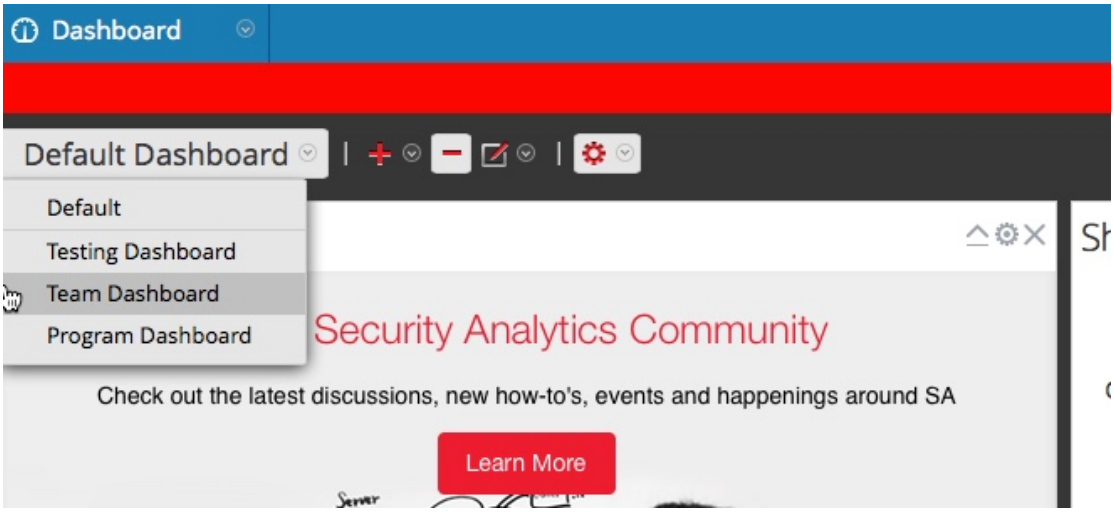
ダッシュボードを作成した後は、次の作業ができるようになります。

- ダッシュボードにダッシュレットを追加します。
- ダッシュボードをエクスポートします。
- ダッシュボードを削除します。
- ダッシュボードの名前を変更します。

ダッシュボードの選択

1. Security Analyticsモジュールのダッシュボードを切り替えるには、**ダッシュボード選択リスト**をクリックします。

   ダッシュボード選択リストが表示されます。



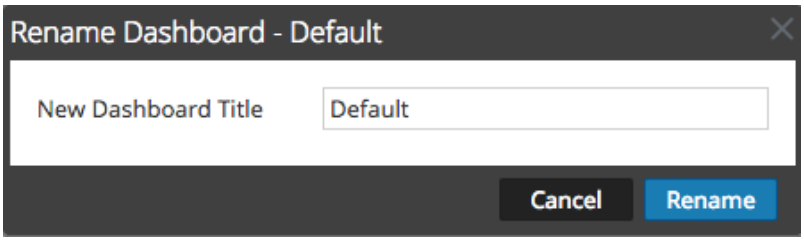
2. 表示するダッシュボードを選択します。

   選択したダッシュボードが表示されます。

カスタム ダッシュボード名の変更

1. ダッシュボード ツールバーで、 > [**ダッシュボード名の変更**]を選択します。

   [ダッシュボード名の変更]ダイアログが表示されます。



2. [**新しいダッシュボードのタイトル**]フィールドに、ダッシュボードの新しいタイトルを入力します。

3. **Rename**をクリックします。

   ダッシュボードが新しいタイトルで更新されます。

カスタム ダッシュボードの削除

Security Analyticsのダッシュボード選択リスト内に不要になったカスタム ダッシュボードが含まれている場合、それらを削除できます。ダッシュボードを削除する場合にはまず、削除するダッシュボードを表示する必要があります。デフォルトのダッシュボードは削除できません。

注:ダッシュボードを後で再利用できるようにする場合は、ダッシュボードを削除する前にダッシュボードをエクスポートします。次のトピックを参照してください。ダッシュボードのインポートとエクスポート.

1. **ダッシュボード選択リスト**で、使用していないダッシュボードを選択します。たとえば、[**Region 3**]を選択します。
   ダッシュボードが表示されます。

2. ダッシュボード ツールバーで、 を選択します。

   ダッシュボードの削除の確認を求めるダイアログが表示されます。

3. ダッシュボードを削除するには、[**はい**]をクリックします。

   ダッシュボードがダッシュボード選択リストから削除されます。

ダッシュボードのインポートとエクスポート

日々、変化する環境や条件に合わせてダッシュボードをカスタマイズすることができますが、結果的に日常的には必要でないダッシュボードが多数作成される場合があります。特別なカスタム ダッシュボードを作成する必要が出てくるたびに、一から定義し直す必要はありません。現在使用していないダッシュボードはエクスポートしておくことができます。以前にエクスポートしたダッシュボードを使用する準備ができている場合には、ダッシュボードをSecurity Analyticsにインポートします。

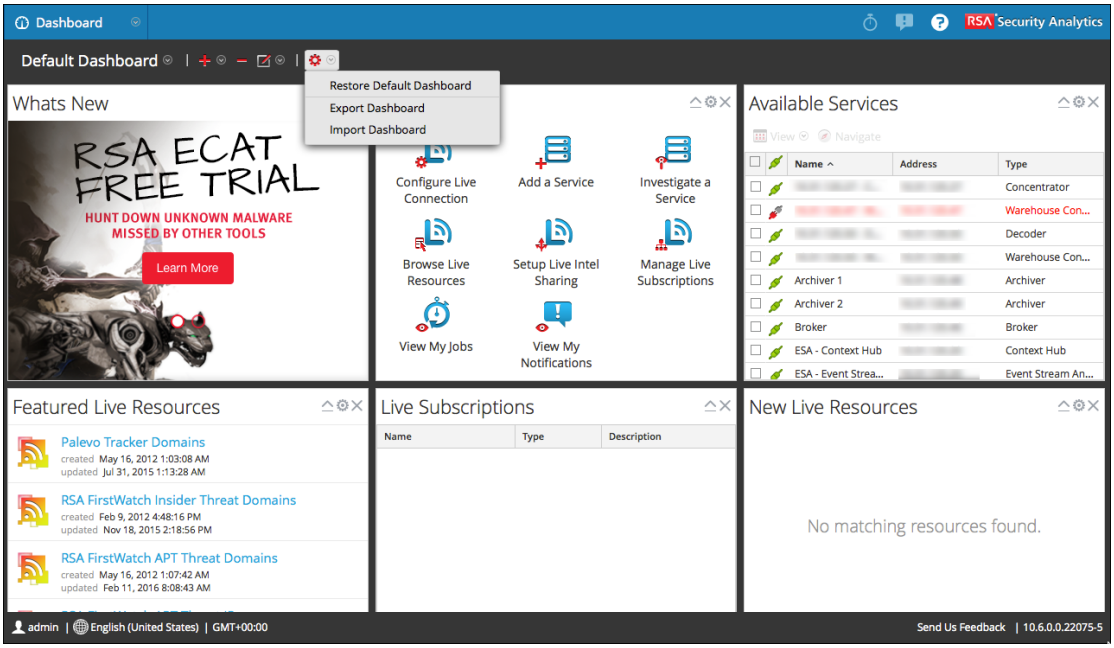
ダッシュボードのエクスポート

エクスポートされたダッシュボードは、同じSecurity Analyticsインスタンス内で使用することを想定しています。同じ権限を持っている、組織内の他のユーザーとカスタム ダッシュボードを共有することもできます。

ダッシュボードをエクスポートするには、ダッシュボードを開いて、ダッシュボード ツールバーの[編集]ドロップダウン メニューから[ダッシュボードのエクスポート]オプションにアクセスする必要があります。

注：レポート リアルタイム チャートを含むダッシュボードをエクスポートする場合には、[レポート リアルタイム チャート]ダッシュレットが使用しているチャートもエクスポートする必要があります。これらのチャートは、デフォルトではエクスポートされません。ダッシュボードをインポートする場合には、[レポート リアルタイム チャート]ダッシュレットが使用しているチャートを手動でインポートしてください。

1. エクスポートするダッシュボードに移動します。現在表示されているダッシュボードの[**ダッシュボード選択リスト**]ドロップダウン メニューに既存のダッシュボードがすべて表示されます。
2. ダッシュボード ツールバーの[**アクション**]ドロップダウン メニュー( ) をクリックし、[**ダッシュボードのエクスポート**]を選択します。

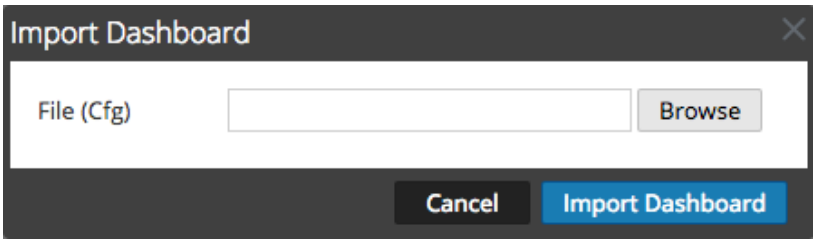


3. ダウンロードしたファイルがコンピュータに損害を及ぼす可能性があるという警告が画面の下部に表示されることがあります。警告を確認し、問題がなければ[**保持**]をクリックします。
4. エクスポートされたファイルを.cfg形式で保存します。

ダッシュボードのインポート

注：レポート リアルタイム チャートを含むダッシュボードおよび関連するチャートは、エクスポート元と同じSecurity Analyticsサーバおよび Reporting Engineのインスタンスにインポートする必要があります。また、Reporting Engine用に構成されたデータ ソースが、エクスポート元のSecurity Analyticsインスタンス上にあるデータ ソースと同じであることを確認する必要があります。ダッシュボードおよび関連するチャートをSecurity Analyticsサーバの別のインスタンスにインポートする場合は、チャート内のデータ ソース名を更新する必要があります。

1. [ダッシュボード]ツールバーで、[**アクション**]ドロップダウン メニュー( ) から[**ダッシュボードのインポート**]を選択します。



2. [**ダッシュボードのインポート**]ダイアログでダッシュボード ファイルを参照します。.cfgファイルのみサポートされます。
3. [**ダッシュボードのインポート**]をクリックします。
   Security Analyticsにダッシュボードが表示されます。

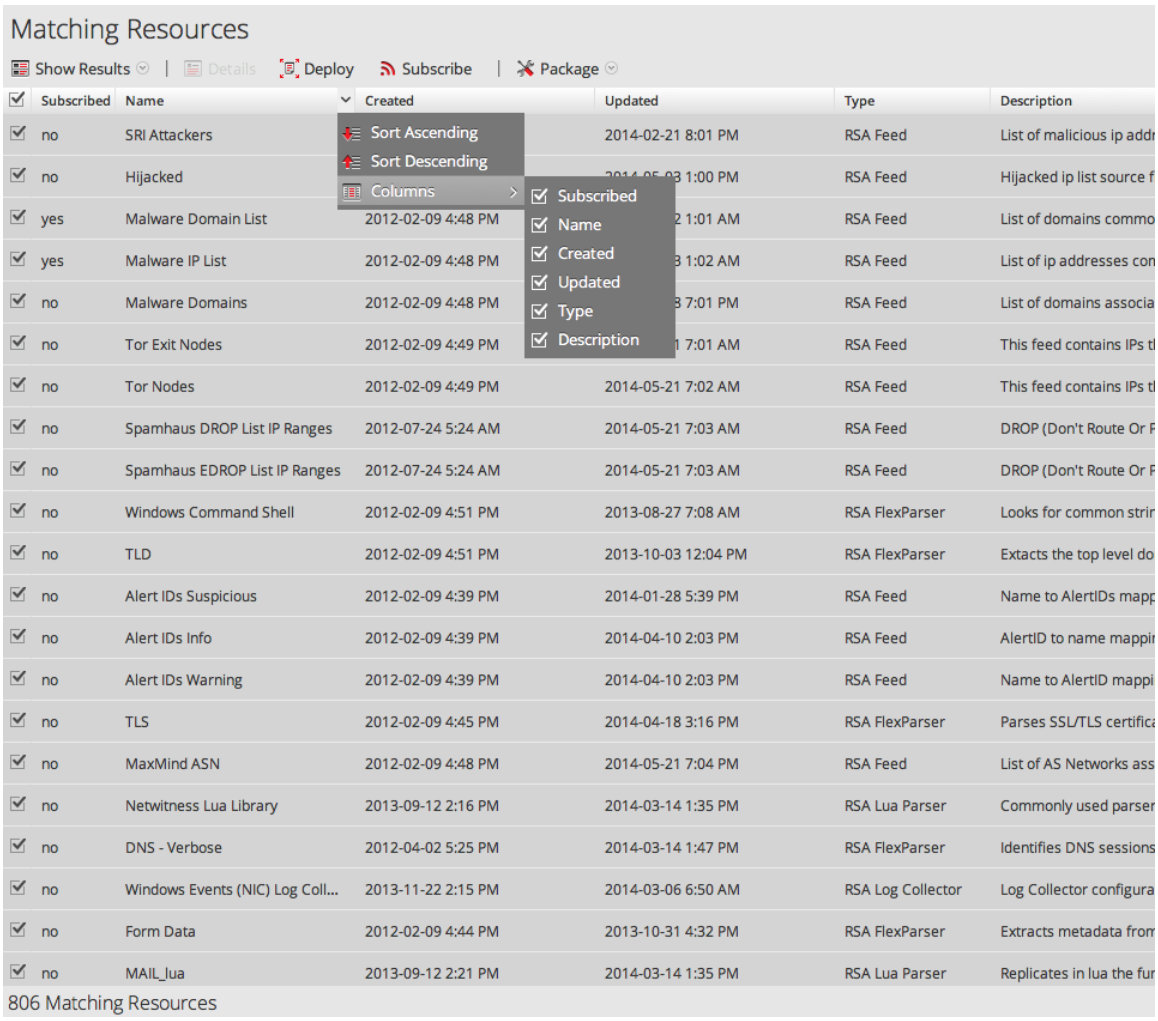
グリッドの構成

Security Analyticsのダッシュボードとダッシュレットに表示される情報の多くは、行と列を使って表示すると見やすくなります。これをグリッドと呼びます。グリッドの表示はカスタマイズすることができます。このページでは、以下の項目について説明します。

- 表示する列を選択する。
- 各列を昇順または降順にソートする。
- 列の幅を変更する。

[Admin サービス監視]ダッシュレットには、ダッシュレット内のグリッドの特定の列を定位置に固定できる独特の機能があります。この機能により、その列の表示を固定した状態で右方向にスクロールすることができます。

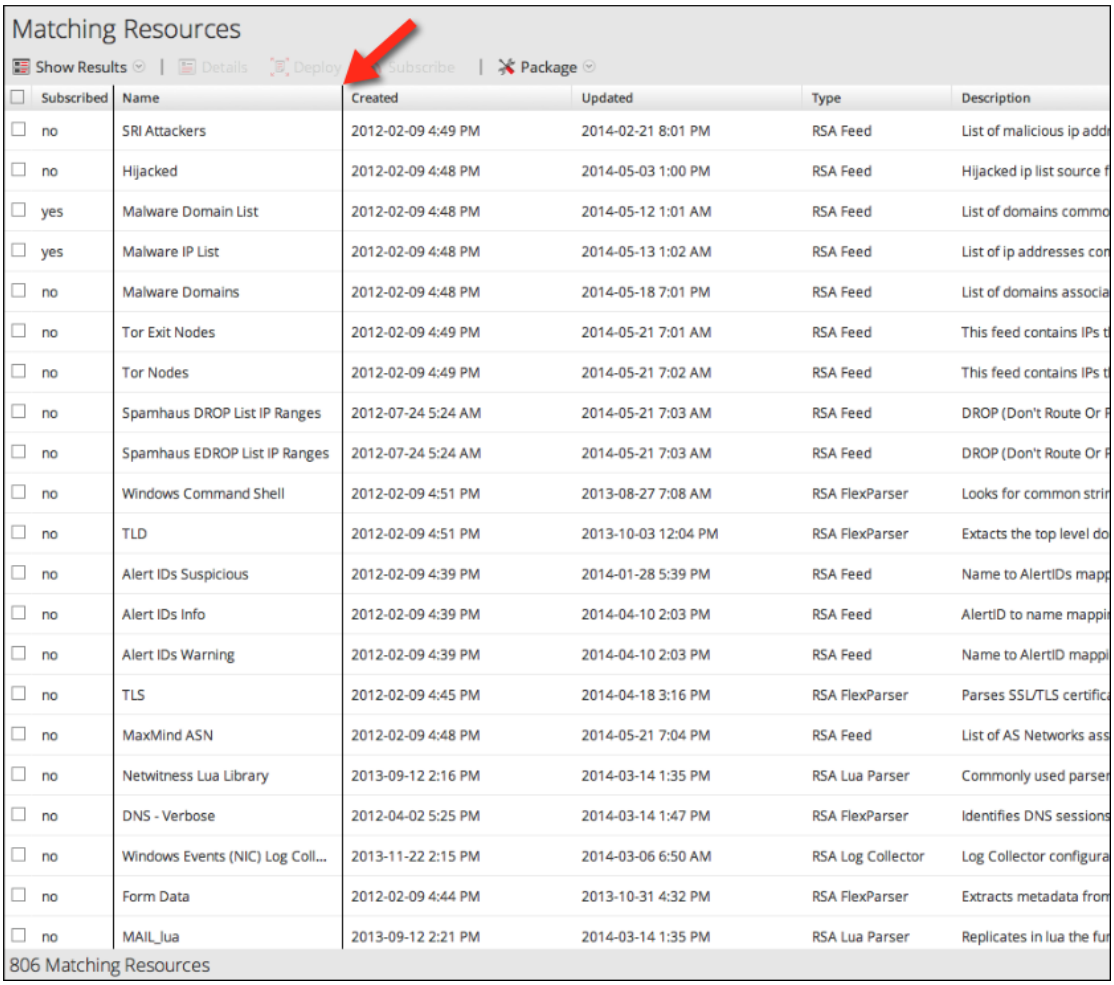
下の画面はグリッドの例(Liveの[検索]ビューの[一致するリソース]グリッド) です。



列幅の変更

列の幅を変更して、デフォルトの幅よりも狭くしたり広くしたりできます。たとえば、列の幅が狭すぎてコンテンツの一部を表示できない場合は、広くすることができます。

1. 列名の右端にカーソルを合わせます。
2. カーソルが、列のサイズ変更用のカーソル(1本の短い縦棒と左右を指す矢印)に変わったら、そのままクリックしてドラッグし、列の幅を変更します。[Name]列のサイズを変更する例を次に示します。

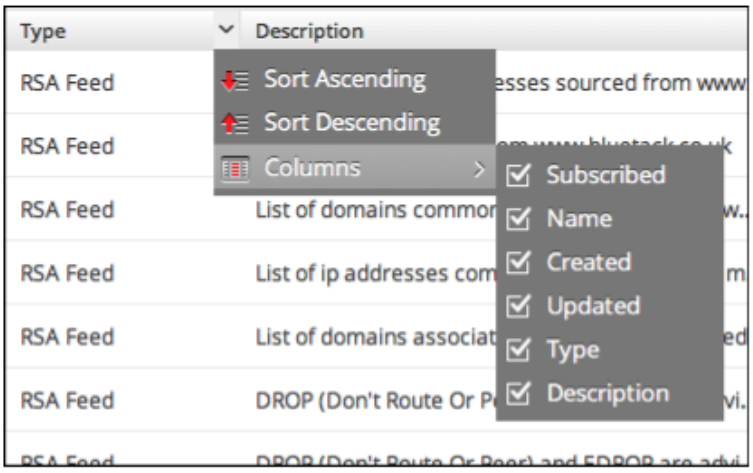


3. 幅が適切なサイズになったら、マウスのボタンを離します。

表示する列の選択

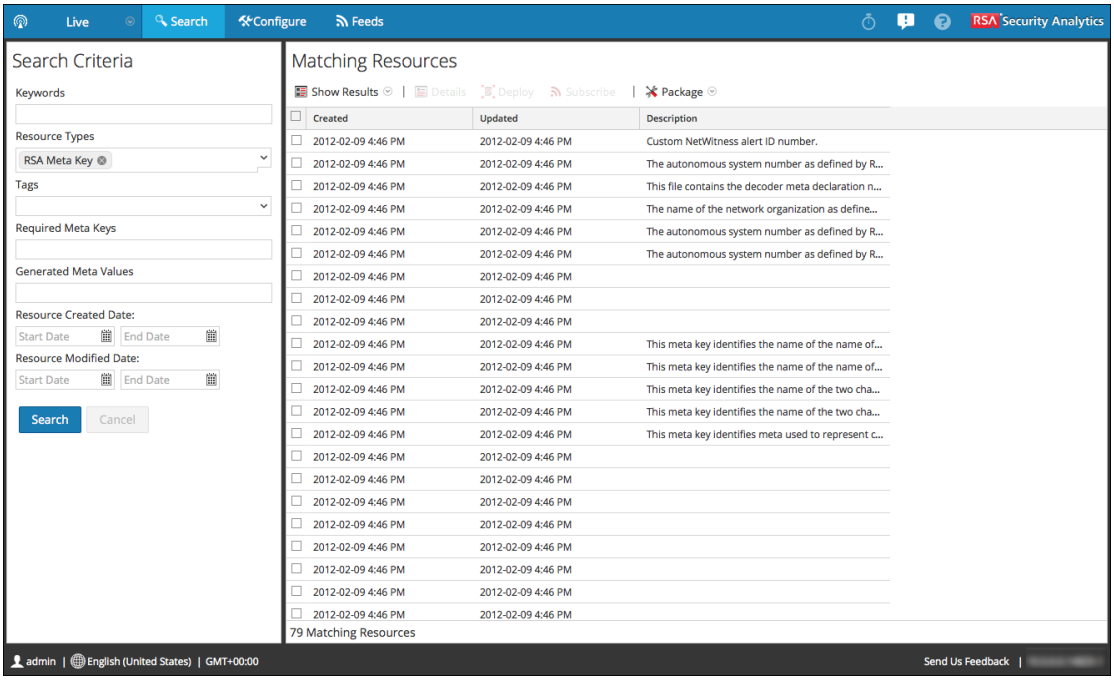
1. 列名の右端にカーソルを合わせます。
2. カーソルが選択リスト アイコン( ) に変わったら、クリックしてリストを表示します。
3. リストから、[**カラム**]を選択します。

使用可能な列の一覧が表示されます。グリッドに現在表示中の列にはチェックマークが付いています。



4. 列名をクリックし、選択と選択解除を切り替えます。

列名を選択解除すると、その列はグリッドから削除されます。列名を選択すると、その列はグリッドに追加されます。これは、複数の列を選択解除した後の[一致するリソース]グリッドの例です。



列の内容のソート

目的に合わせた情報が表示されるよう、グリッドの各列のソート方法を選択することができます。

1. 列名の右端にカーソルを合わせます。
2. カーソルが選択リスト アイコン( ) に変わったら、クリックしてメニューを表示します。

   メニューに使用可能なソート オプションの一覧が表示されます。
3. ソート オプション([昇順]、[降順]など) を選択します。

   選択したオプションに基づいてグリッドがソートされます。

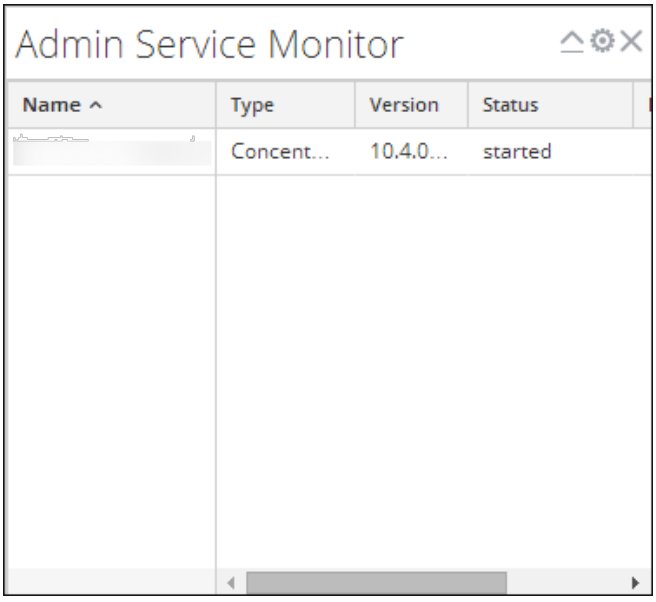
列のロック([Admin サービス監視]ダッシュレットのみ)

[Admin サービス監視]ダッシュレットには、ダッシュレット内のグリッドの特定の列を定位置に固定するオプションがあります。この機能により、その列の表示を固定した状態で右方向にスクロールすることができます。

1. 右にスクロールする際に列の表示を保つには、任意の列のタイトルでドロップダウン メニュー アイコン( ) をクリックします。

   列のコンテキスト メニューが表示されます。
2. [**ロック**]を選択します。

   選択した列はグリッドの左側に移動し、他の列が水平にスクロールしてもそのまま固定されます。この例では、[Name]列が固定され、表示を右にスクロールしてもそのまま表示されます。[Type]列の一部はスクロールに伴って左に移動して表示されなくなりますが、[Name]列はそのままです。



3. 列のロックを解除するには、ドロップダウン メニュー アイコン( ) をクリックし、[**ロック解除**]を選択します。

ジョブの管 理

Security Analyticsでは、アド ホックなタスクやスケジュール設 定されたタスクが完 了 するまでに数 分 かかる場 合 があります。Security Analyticsのジョブ システムで時 間 のかかるタスクを開 始して も、ジョブの実 行 中 にSecurity Analyticsの他 の機 能 は継 続して使 用 することができます。そのよ うな場 合 、タスクの進 行 状 況 を監 視 できるだけでなく、タスクが完 了 したこと、また結 果 が成 功 か失 敗 かの通 知 を受 け取 ることができます。

Security Analyticsのユーザー インタフェースでは、Security Analyticsツールバーからジョブのクイッ クビューを開くことができます。ジョブ トレイはいつでも参 照 が可 能 で、ジョブ ステータスが変 更 さ れると、[ジョブ]アイコンにフラグ( ) が付 けられ、実 行 中 のジョブの数 が示 されます。すべての ジョブが完 了 すると、この数 字 は表 示 されなくなります。

ジョブは次 の2つのビューでも確 認 することができます。

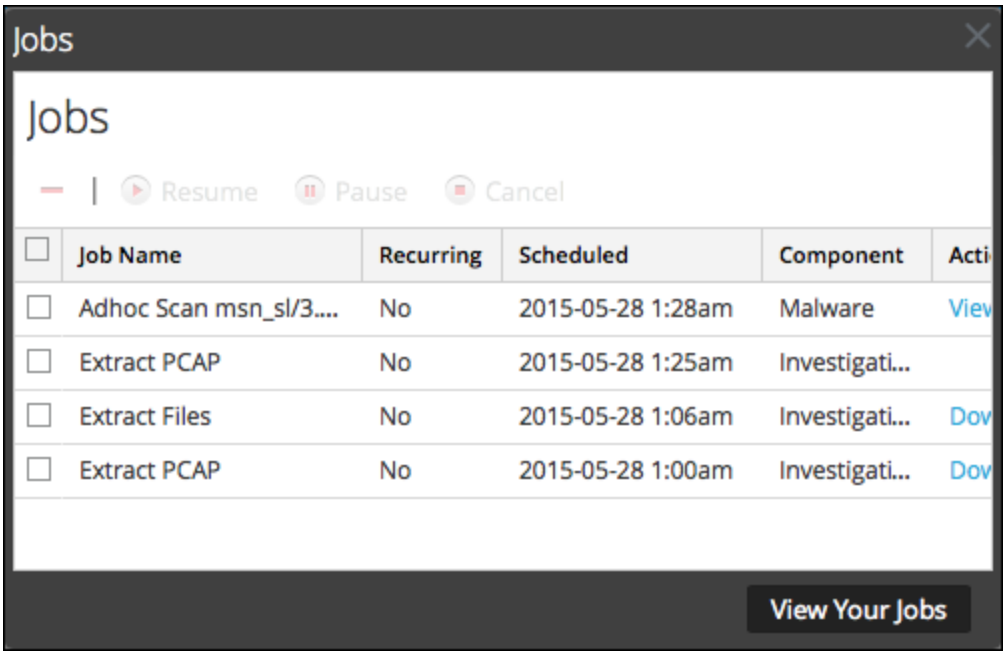
- [プロファイル]ビューでは、ジョブ トレイと同 じ内 容 のジョブ画 面 をフル パネルで表 示 できま す。確 認 することができるのは自 分 が実 行 したジョブだけです。
- [システム]ビューでは、管 理 権 限 を持 つユーザーが、すべてのユーザーのすべてのジョブを1つ のジョブ パネルで表 示 および管 理 できます。

ジョブ パネルの構 造 はすべてのビューで同 じです。

ジョブ トレイの表 示

Security Analyticsツールバーで、[ジョブ]アイコン をクリックします。

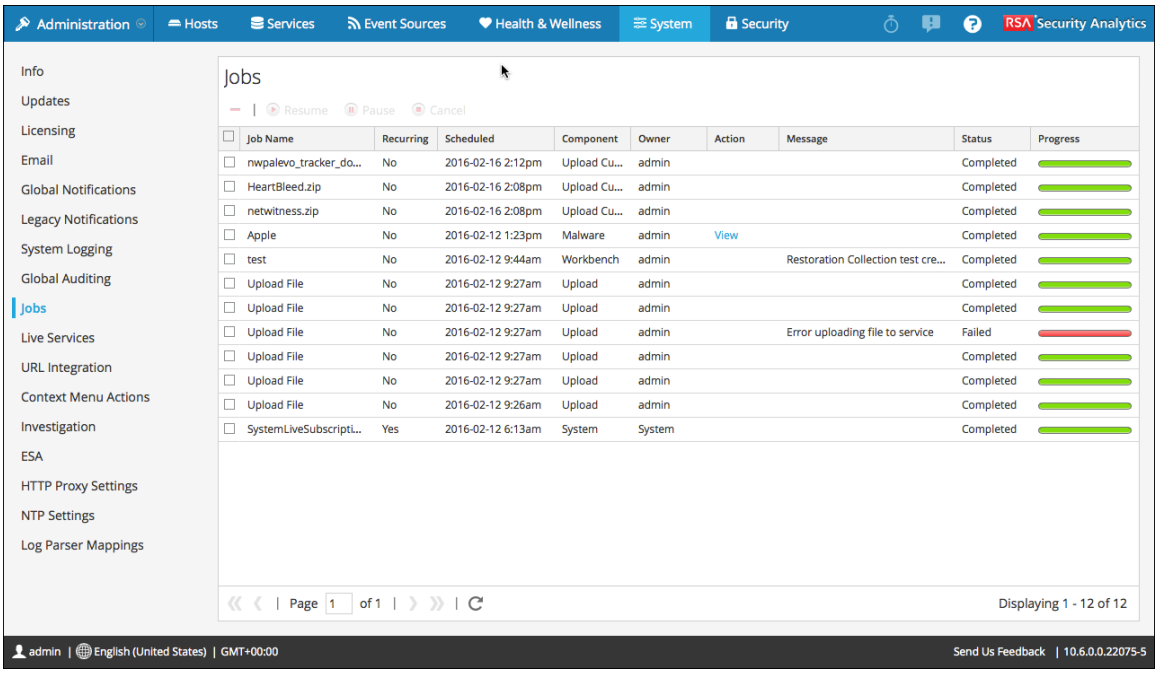
ジョブ トレイが表 示 されます。



ジョブ トレイには、[ジョブ] パネルで使 用 可 能 な列 のサブセットを使 用して、自 分 が管 理 するすべてのジョブ(繰り返しジョブと繰り返しではないジョブ) が一 覧 表 示されます。[ジョブ トレイ]と、[プロファイル]ビュー> [ジョブ] パネルの内 容 は同 一 です。[Administration] の[システム]ビューでは、すべてのユーザーのすべてのSecurity Analyticsジョブの情 報 が[ジョブ] パネルに一 覧 表 示されます。

[プロファイル]ビュー> [ジョブ] パネルでのジョブの表 示

ジョブを拡 大 表 示するには、[**自 分 のジョブを表 示**]をクリックします。
[プロファイル]ビュー> [ジョブ] パネルが表 示されます。



繰り返しジョブの一時停止と再開

[一時停止]と[再開]オプションは、繰り返しジョブにのみ適用されます。実行中の繰り返しジョブを一時停止しても、実行中のジョブには影響しません。(ジョブが一時停止中のままである場合)次の回の実行は、スキップされます。

1. 繰り返しジョブの次回以降の実行を停止するには、[**ジョブ**]パネルで、ジョブを選択し、[**一時停止**]をクリックします。

   このジョブの次回の実行がスキップされ、[再開]をクリックするまでスケジュールは一時停止されます。

2. 一時停止された繰り返しジョブの実行を再開するには、ジョブを選択して、[**再開**]をクリックします。

   このジョブの次回の実行はスケジュール設定どおりに行われ、ジョブのスケジュールが再開されます。

ジョブのキャンセル

実行中または実行のキューに入っているジョブをキャンセルするには、次の手順を実行します。

1. **ジョブトレイ**または[**ジョブ**]パネルで、1つ以上のジョブを選択します。
2. **キャンセル**をクリックします。

   確認ダイアログが表示されます。

3. **はい**をクリックします。

   このジョブはキャンセルされ、**キャンセル済み**ステータスのエントリーがグリッドに残されます。

   繰り返しジョブをキャンセルすると、ジョブのその回の実行がキャンセルされます。スケジュールされているジョブの次の回の実行は、正常に実行されます。

ジョブの削除

注意:ジョブを削除すると、ジョブはすぐにグリッドから削除されます。確認ダイアログは表示されません。繰り返しジョブを削除すると、スケジュールされている以降のジョブの実行もすべて削除されます。

ユーザーは実行前、実行中、実行後に自分のジョブを削除できます。Administratorsロールのユーザーはどのジョブも削除できます。ジョブを削除するには、次の手順を実行します。

1. 1つ以上のジョブを選択します。
2. **削除**をクリックします。
3. ジョブはグリッドから削除されます。

ジョブ結果のダウンロード

[アクション]列が[ダウンロード]ステータスであるジョブの場合、ジョブの結果をダウンロードできます。Investigationモジュールにおいて、セッションのパケット データをPCAPファイルとして抽出したり、セッションからペイロード ファイル(たとえば、Wordドキュメントやイメージ) を抽出したりすると、ジョブの結果としてファイルが作成されます。ローカル システムにファイルをダウンロードするには、[**ダウンロード**]をクリックします。

通知の表示と削除

Security Analyticsのユーザー インタフェースでは、最新のシステム通知を確認することができます。Security Analyticsツールバーから通知のクイック ビューを開くことができます。通知トレイはいつでも参照が可能で、新しい通知を受け取ると、[通知]アイコンにフラグが付けられます。

通知の例としては以下のものがあります。

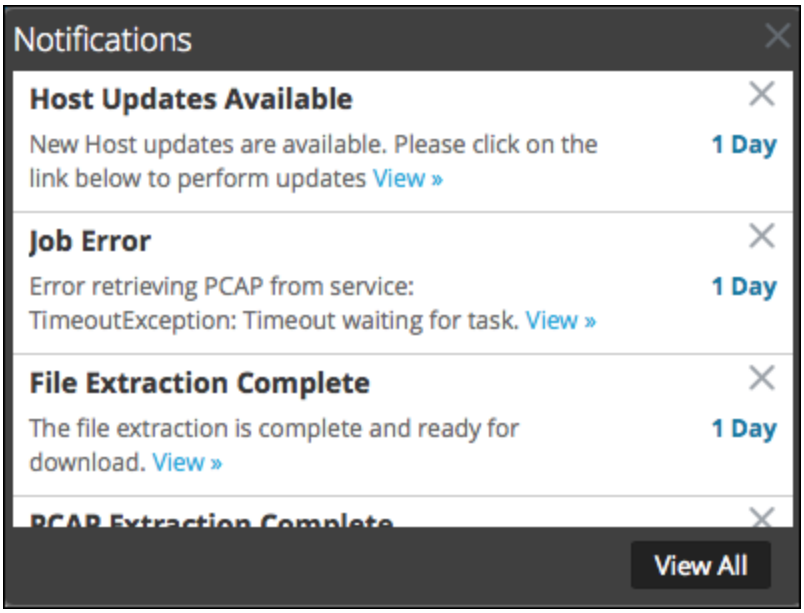
- ホストのアップグレードが完了した。
- DecoderへのParserの適用が完了した。
- 新しいバージョンのソフトウェアが利用可能。

次の2つのビューの[通知]パネルで、すべての通知を確認できます。

- [プロファイル]ビューでは、自分の通知のみを確認できます。
- [システム]ビューでは、管理権限を持つユーザーが、すべてのユーザーのすべての通知を1つのパネルで表示および管理できます。

通知の表示

通知トレイを表示するには、Security Analyticsツールバーの[通知]アイコン() をクリックします。



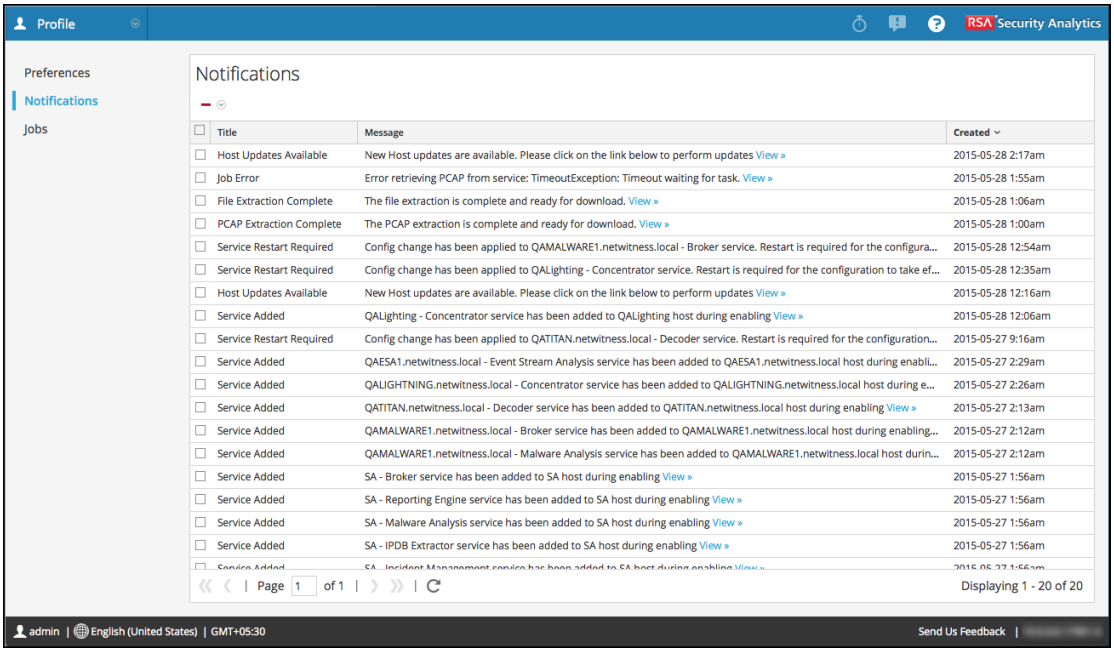
すべての通知の表示

すべての通知を表示するには、次のいずれかの操作を行います。

1. **Security Analytics**メニューで[**プロファイル**]を選択し、[**プロファイル**]ビューのオプション パネルで[**通知**]を選択します。
2. **Security Analytics**メニューで[**Administration**]＞[**システム**]を選択し、[**システム**]ビューのオプション パネルで[**通知**]を選択します。
3. **Security Analytics**ツールバーで をクリックして通知トレイを開き、通知トレイで[**すべて表示**]をクリックします。

   [通知]パネルが表示されます。ここにはすべての通知が表示され、フォーマットは通知トレ

イのフォーマットとは異なります。



通知レコードの削除

通知レコードを削除するには、次を行います。

1. **プロファイル通知**グリッドで、削除する通知を選択します。
2. Delete をクリックします。

   選択した通知がこのグリッドと通知トレイから削除されます。

参考資料

Security Analyticsユーザー インタフェースには次の機能が含まれます。

- [プロファイル]ビュー
- ジョブ トレイ
- 通知トレイ
- ブラウザ ウィンドウ
- ダッシュボード
- コンテキスト メニュー
- グリッド
- ダッシュレット

このセクションではそれぞれの例を示します。ダッシュレットの例は、ダッシュボードをどのようにカスタマイズするかを決定する際に役立ちます。

[ジョブ]パネルとジョブ トレイ

ジョブはさまざまなSecurity Analyticsモジュールによって開始されます。たとえば、Liveモジュールでは、CMSリソースをダウンロードしたり、Administrationモジュールでは、サービスにFeedをアップロードしたりする際にジョブが実行されます。また、Investigationモジュールでは、パケット キャプチャ ファイルのエクスポートやファイルの抽出を実行する場合にもジョブで実行されます。

[Administration]の[システム]ビューの[ジョブ]パネルでは、ADMINグループのユーザーがすべてのSecurity Analyticsジョブを管理できます。他の非管理者ユーザーは、[プロファイル]ビューで自分のジョブを表示できます。

さらに、Security Analyticsのユーザー インターフェイスでは、Security Analyticsツールバーからジョブのクイック ビューを開くことができます。ジョブ ステータスが変更されると、[ジョブ]アイコンにフラグ() が付けられ、実行中のジョブの数が示されます。すべてのジョブが完了すると、この数字は表示されなくなります。

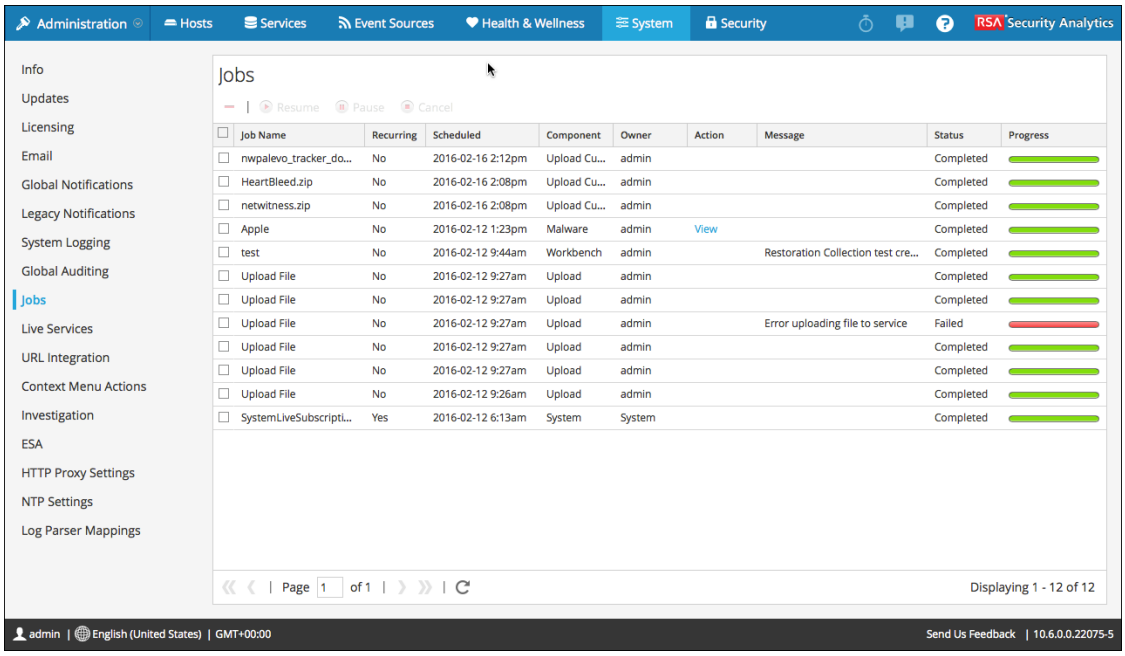
[ジョブ]パネルでは、次のタスクを実行できます。

- ジョブの表示およびソート
- ジョブの一時停止または再開
- ジョブのキャンセル
- ジョブの削除
- ジョブの実行結果のダウンロード

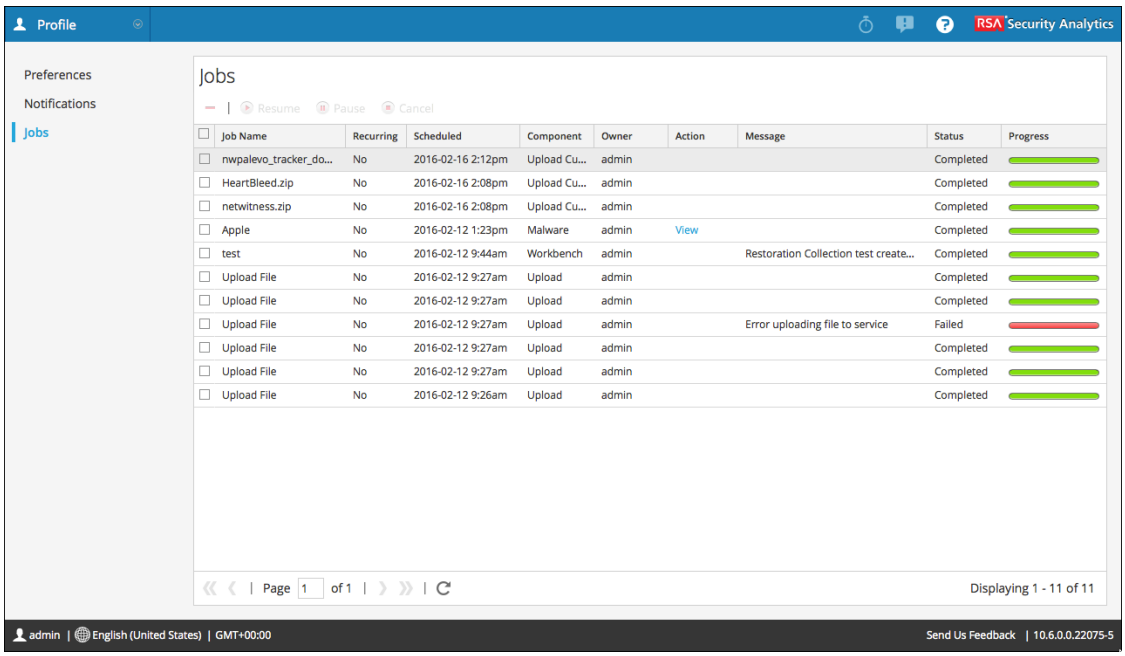
ジョブ パネルの構造はすべてのビューで同じです。[ジョブ]パネルとジョブ トレイに関連する手順については、次のトピックを参照してください: ジョブの管理.

[ジョブ]パネルにアクセスするには、次のいずれかを実行します。

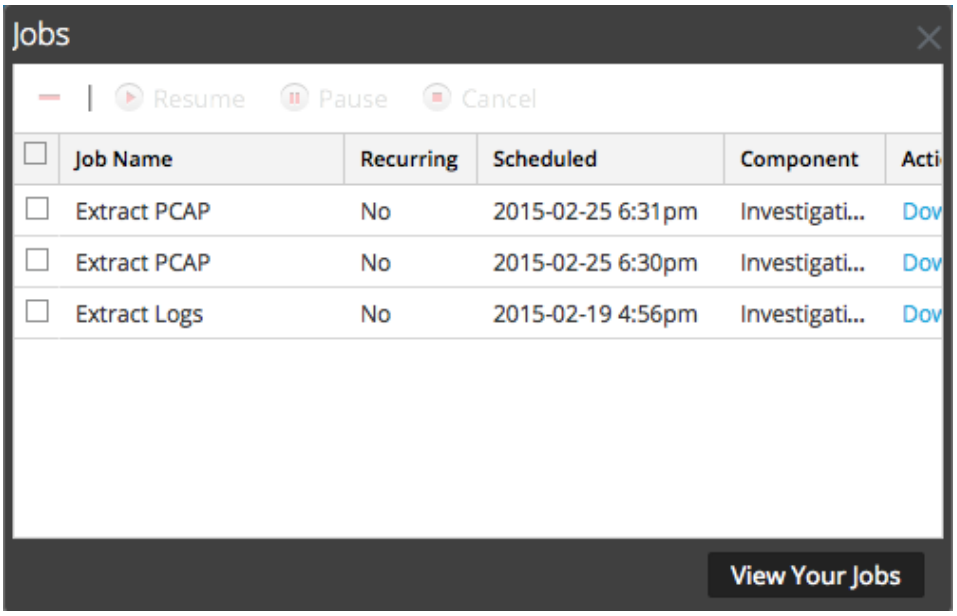
- **Security Analyticsメニュー**で**[Administration]＞[システム]**を選択し、[オプション]パネルで**[ジョブ]**を選択します。



- **Security Analytics**メニューで[**プロファイル**]を選択し、[オプション]パネルで[**ジョブ**]を選択します。



ジョブトレイを表示するには、Security Analyticsツールバーの[**ジョブ**]アイコン  をクリックします。



[ジョブ]パネルでは、ジョブの情報がグリッドに表示されます。列には、ジョブ名、繰り返しオプション、ジョブのコンポーネント、ジョブの所有者、ジョブ結果のダウンロードや表示 ボタン、メッセージ、ステータス、進行状況バーが示されます。

機能

ジョブトレイには、[**ジョブ**]パネルで使用可能な列のサブセットを使用して、自分が管理するすべてのジョブ(繰り返しジョブと繰り返しではないジョブ) が一覧表示されます。[ジョブトレイ]と、[プロファイル]ビュー>[ジョブ]パネルの内容は同一です。[Administration]の[システム]ビューでは、すべてのユーザーのすべてのSecurity Analyticsジョブの情報が[ジョブ]パネルに一覧表示されます。

次の表に、[ジョブ]パネルのツールバー オプションを示します。

機能	説明
	[再開]オプションは、一時停止されていた繰り返しジョブにのみ適用されます。一時停止されていたジョブを再開する場合、ジョブの次の回の実行は、スケジュールどおりに実行されます。
	[一時停止]オプションは、繰り返しジョブにのみ適用されます。実行中の繰り返しジョブを一時停止しても、その回の実行には影響しません。(ジョブが一時停止中のままである場合) 次の回の実行は、スキップされます。

機能	説明
	繰り返しジョブまたは繰り返しではないジョブをキャンセルします。ジョブは、実行中にキャンセルできます。繰り返しジョブをキャンセルすると、ジョブのその回の実行がキャンセルされます。スケジュールされているジョブの次の回の実行は、正常に実行されます。
	[**ジョブ**]パネルから繰り返しジョブまたは繰り返しではないジョブを削除します。ジョブを削除すると、ジョブは[ジョブ]パネルから直ちに削除されます。確認ダイアログは表示されません。繰り返しジョブを削除すると、スケジュールされている以降のジョブの実行もすべて削除されます。

次の表でジョブトレイと[ジョブ]パネルの機能を説明します。

機能	説明
選択ボックス	1つ以上のジョブを選択するには、このボックスをクリックします。
進行状況	ジョブの完了の割合を表示します。
ジョブ名	ジョブの名前を表示します。「**Extract Files**」、「**Upgrade Service**」など。
繰り返し	ジョブが繰り返しジョブであるか、繰り返しではないジョブであるかを示します。[**はい**]=繰り返し、[**いいえ**]=繰り返しではない。
コンポーネント	ジョブを生成したコンポーネントを示します。**Investigation**、**Administration**など。
所有者	ジョブの所有者を示します。ジョブの所有者はデフォルトでは**ジョブトレイ**には表示されません。ジョブトレイには、現在のユーザーのジョブのみが表示されるからです。この列を追加することができます。

機能	説明
ステータス	ジョブのステータスを示します。一般的なステータスの値には、**一時停止**、**実行中**、**キャンセル済み**、**失敗**、**完了**がありますが、その他のステータス値が表示されることもあります。
メッセージ	ジョブに関する補足情報を表示します。「**Extracting files**」、「**No sessions found**」など。
アクション	[Investigation]の[Malware Analysis]ビューでジョブを表示するか、ジョブで出力されたファイルをローカルシステム上のデフォルトの**ダウンロード** ディレクトリにダウンロードします。正常に完了したジョブの場合のみ、[**アクション**]列に[**表示**]リンクが表示されます。ファイルを出力するジョブの場合のみ、[**アクション**]列に[**ダウンロード**]リンクが表示されます。
自分のジョブを表示	**[プロファイル]ビュー> [ジョブ]**パネルにジョブを表示します。
スケジュール	ジョブがスケジュールされた日時を示します。

[通知]パネルと通知トレイ

Security Analyticsでは、特定のアクションや条件について、ユーザーに知らせるためのシステム通知が用意されています。

- ホストのアップグレードが完了した。
- DecoderへのParserの適用が完了した。
- サービスが停止した(特定のタイプの致命的なログ)。
- Visualizationが完了した。
- レポートが完了した。
- 新しいバージョンのソフトウェアが利用可能。

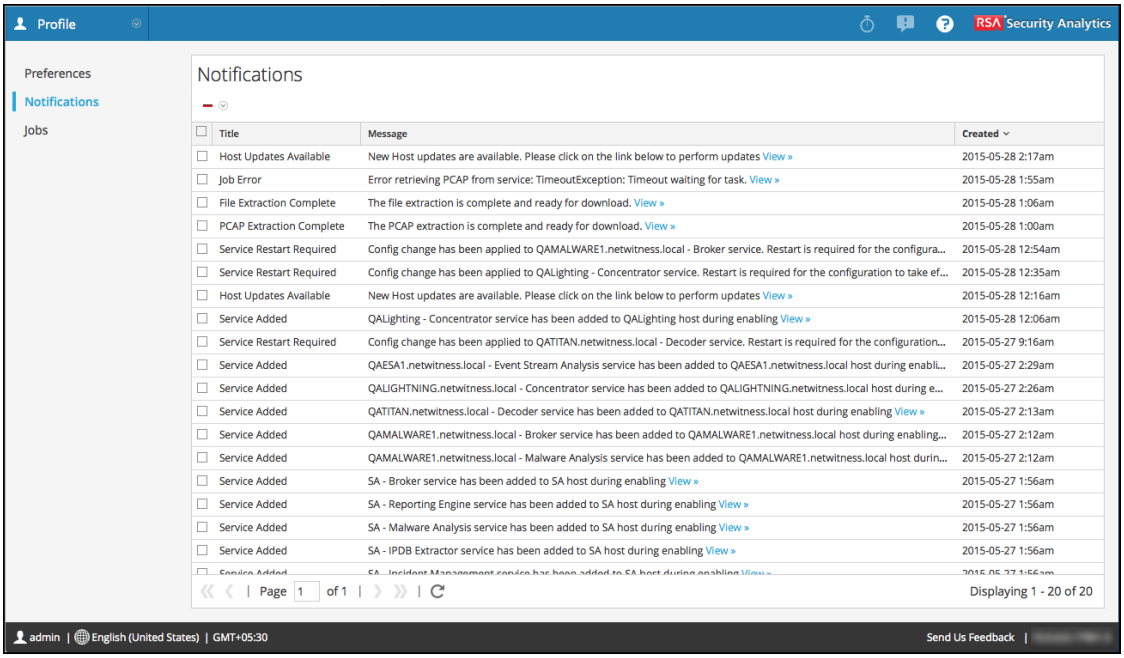
Security Analyticsのユーザー インターフェイスでは、最新のシステム通知を確認することができます。Security Analyticsツールバーから通知のクイック ビューを開くことができます。通知トレイはいつでも参照が可能で、新しい通知を受け取ると、[通知]アイコンにフラグが付けられます。

通知トレイでシステム通知を表示する場合、最近のシステム通知のみが表示されます。[プロファイル]ビューまたは[システム]ビューではグリッド形式ですべての通知を表示できます。通知の表示に関する操作手順については、次のトピックを参照してください。通知の表示と削除.

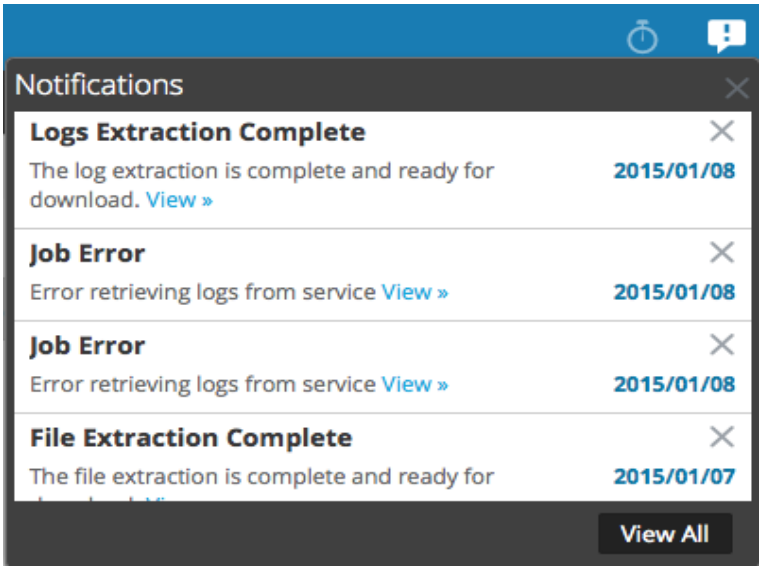
[通知]パネルにアクセスするには、次のいずれかを実行します。

- **Security Analytics**メニューで[**プロファイル**]を選択し、[**プロファイル**]ビューのオプション パネルで[**通知**]を選択します。

- **Security Analytics**メニューで[Administration]＞[システム]を選択し、[システム]ビューのオプション パネルで**[通知]を選択します。**



- **Security Analytics**ツールバーで  をクリックし、通知トレイで[**すべて表示**]をクリックします。



機能

[通知]パネルとトレイには、ツールバーとグリッドがあります。通知トレイは、[通知]パネルに表示される情報のサブセットです。次の表に、[通知]パネルの機能とその説明を示します。

機能	説明
−	ドロップダウン メニューが表示され、[**通知**]グリッドと通知トレイから、選択した通知レコードまたはすべての通知レコードを削除できます。
タイトル	通知のタイトル。「**ファイルの抽出が完了しました**」など。
メッセージ	メッセージ全体。たとえば、**ファイルの抽出が完了し、ダウンロードの準備ができました。**
表示	一部のメッセージには、アクションへのリンクが含まれています。たとえば、ダウンロードするファイルがある場合、このリンクをクリックすると[ジョブ]パネルが開き、このビューでファイルをダウンロードできます。
作成日	通知が作成された日時。 通知トレイでは、通知が作成されてからの日数がこの列に表示されます。
すべて表示	[プロファイル]ビューの通知グリッドを表示します。

[プロファイル]ビュー> [環境設定]パネル

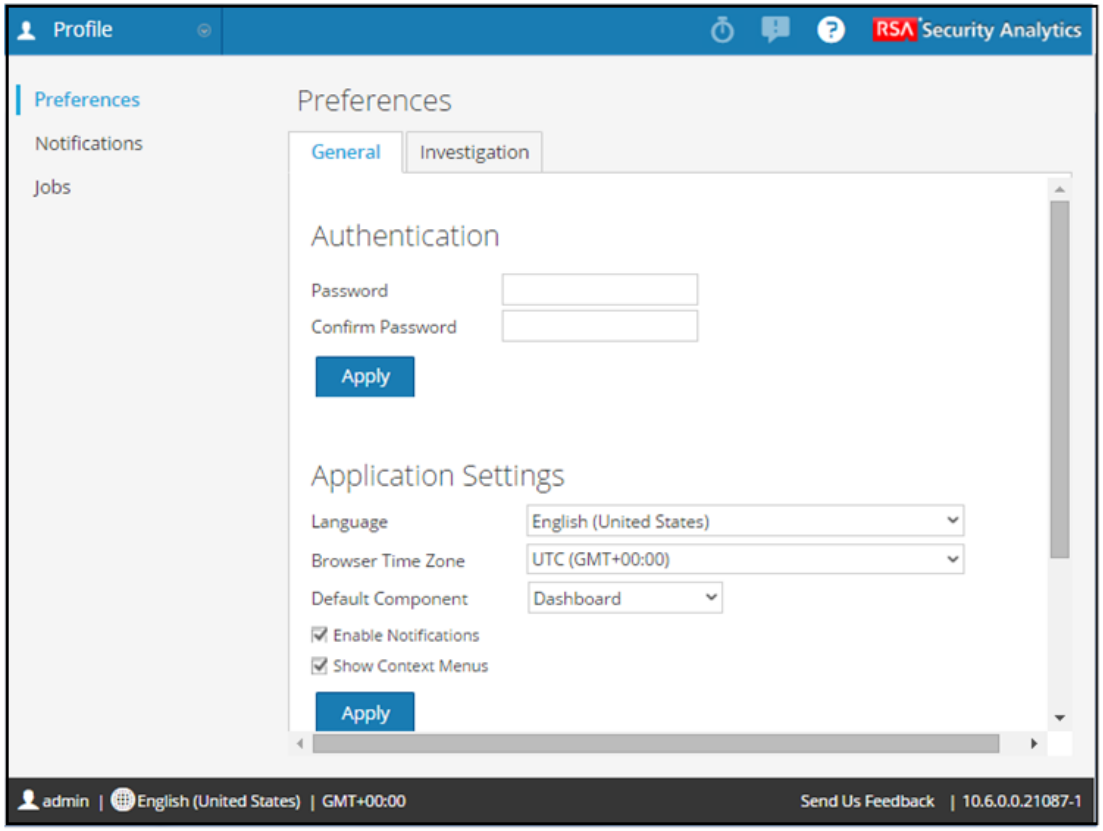
ユーザーは、いくつかのシステム環境設定をユーザーごとに適用することができます。これらの設定は、システム管理者が設定した環境設定より優先されます。これには次のものが含まれます。

- Security Analyticsの全般的な環境設定とSecurity Analyticsアプリケーションの設定
- Investigationに適用され、初期ビューとロード時間に影響する環境設定
- レポートの実行時に適用される環境設定。

このパネルにアクセスするには、次の手順を実行します。

1. **Security Analytics**メニューで、[**プロファイル**]を選択します。
2. [**プロファイル**]ビューの[オプション]パネルで、[**環境設定**]を選択します。

   パネルが表示され、[全般]タブが開きます。



機能

[環境設定]パネル>[全般]タブには、[認証]と[アプリケーション設定]の2つのセクションがあります。

認証

次の表で、[認証]セクションのオプションについて説明します。関連する手順については、次を参照してください。パスワードの変更手順.

機能	説明
Password and Confirm Password	パスワードは8文字以上のレングスにする必要があります。大文字と小文字、数字、特殊文字、スペースを使用できます。
適用	ユーザー インタフェースで使用するタイム ゾーンを変更できます。新しいパスワードはすぐに反映され、次にSecurity Analyticsにログオンするときに必要になります。パスワードの変更は、システム ログオンと、アカウントが追加されているすべてのSecurity Analyticsサービスに適用されます。

アプリケーション設定

次の表で、[アプリケーション設定]セクションのオプションについて説明します。関連する手順については、次のトピックを参照してください: アプリケーション環境設定の構成.

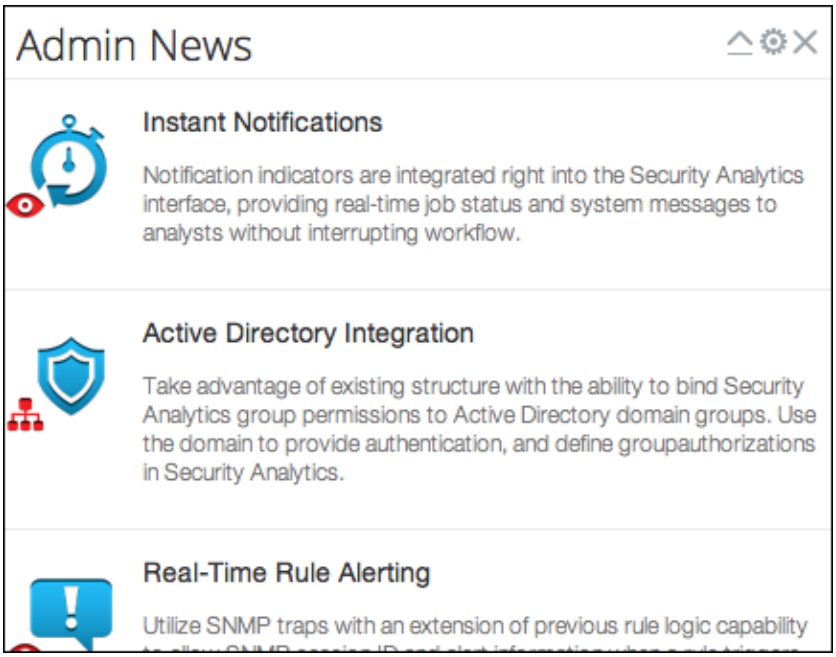
機能	説明
言語	Security Analyticsで使用可能な言語のドロップダウン リストを表示します。
ブラウザのタイム ゾーン	Security Analyticsで使用可能なタイム ゾーンのドロップダウン リストを表示します。

機能	説明
デフォルトのコンポーネント	このフィールドでは、Security Analyticsにログオンしたときの最初のビューとなるコンポーネントをドロップダウン リストから選択できます。
通知の有効化	使用中のユーザー アカウントに対する通知の有効化と無効化を切り替えます。デフォルトでは、新しいユーザー アカウントが作成されると、Security Analyticsシステム通知が有効化されます。
コンテキスト メニューの表示	使用中のユーザー アカウントに対するコンテキスト メニューの有効化と無効化を切り替えます。デフォルトでは、新しいユーザー アカウントが作成されると、Security Analyticsのコンテキスト メニューが有効化されます。コンテキスト メニューは、ユーザーがビューの特定の箇所を右クリックすると表示される追加の機能メニューです。
適用	アプリケーションの設定を更新します。変更内容は直ちに適用されます。

[Admin ニュース]ダッシュレット

このダッシュレットは、Administrationモジュールの製品情報と更新情報を提供します。

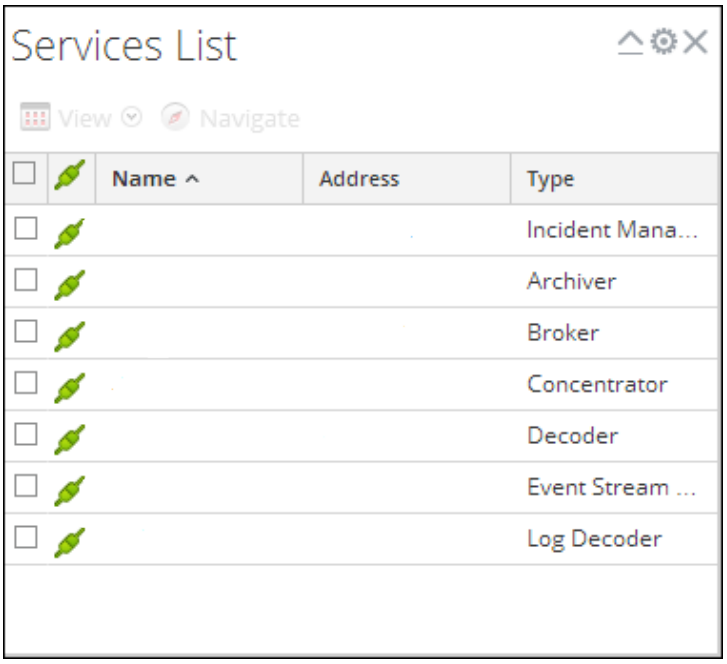
Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで、＋ ＞[**ダッシュレットの追加**]を選択し、[**Adminニュース**]を選択します。



[Admin サービス リスト]ダッシュレット

[Adminサービス リスト]ダッシュレットは、Security Analyticsで利用可能なサービスのリストおよびそれらのサービスの管理タスクへのリンクが表示されます。実際、このダッシュレットは、**[Administration]の[サービス]ビュー**のサブセットです(「*ホストおよびサービス スタート ガイド*」を参照してください)。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞**[ダッシュレットの追加]**を選択して、**[Adminサービス リスト]**を選択します。



機能

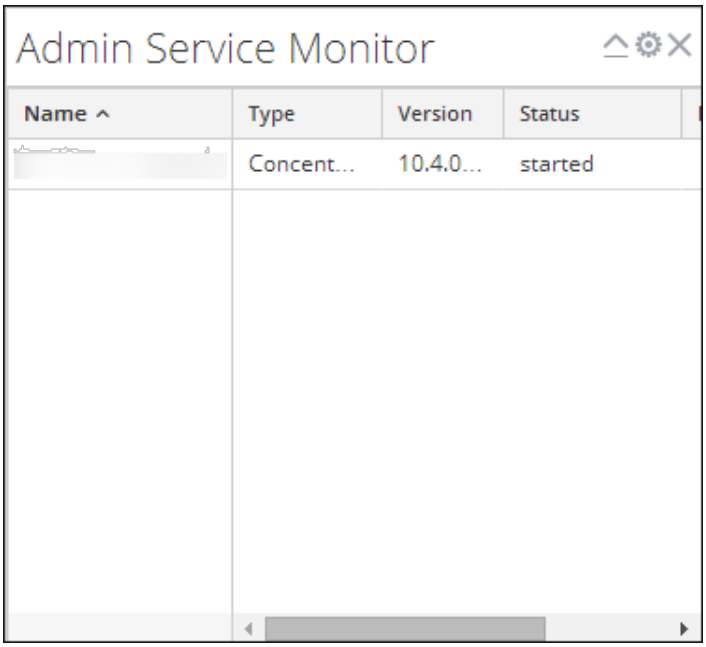
- [表示]メニュー( ) オプションは、Administrationの[サービス]ビューにある[表示]メニューへのクイック リンクです。サービスを選択してここをクリックすると、ビューを選択することができます。
- [ナビゲート]オプションは、Investigationモジュールの[ナビゲート]ビューへのクイック リンクです。
- [サービス]グリッドは、[Administration]の[サービス]ビューのグリッド列のサブセットです。次の表で、ダッシュレットに表示される列の説明を示します。

列	説明
	選択チェックボックス。見出しをクリックすると、リストのすべてのサービスを選択または選択解除できます。
接続ステータス  	接続アイコンは、サービスへの接続が正常(緑)か異常(赤とグレー)かを示します。行全体が赤いテキストになっている場合も接続ステータスが異常であることを示します。
名前	サービスの名前。たとえば、**HQ-Decoder**または**10.26.22.44-Decoder**など。
アドレス	NextGenサービスのIPアドレス。たとえば、**10.26.22.44**など。
タイプ	サービスのタイプ。表示される値は、Broker、Concentrator、Decoder、Log Decoder、Log Collector、Archiver、Workbench、Warehouse Collector、Event Stream Analysis、IPDB Extractor、Reporting Engine、Malware Analysis、Incident Managementです。

[Admin サービス監視]ダッシュレット

[Adminサービス監視]ダッシュレットは、[Administration]＞[ホスト]ビューに表示されるサービスのバージョン情報やステータス情報などのサマリーを表示します。これは、[ホスト]ビューにある列のサブセットです。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞**[ダッシュレットの追加]**をクリックして、**[Adminサービス監視]**を選択します。[ダッシュレットの追加]ダイアログには、新しいダッシュレットのサービス タイプを選択するオプションがあります。



機能

このダッシュレットには、**[ホスト]**ビューにある次の列が含まれます。

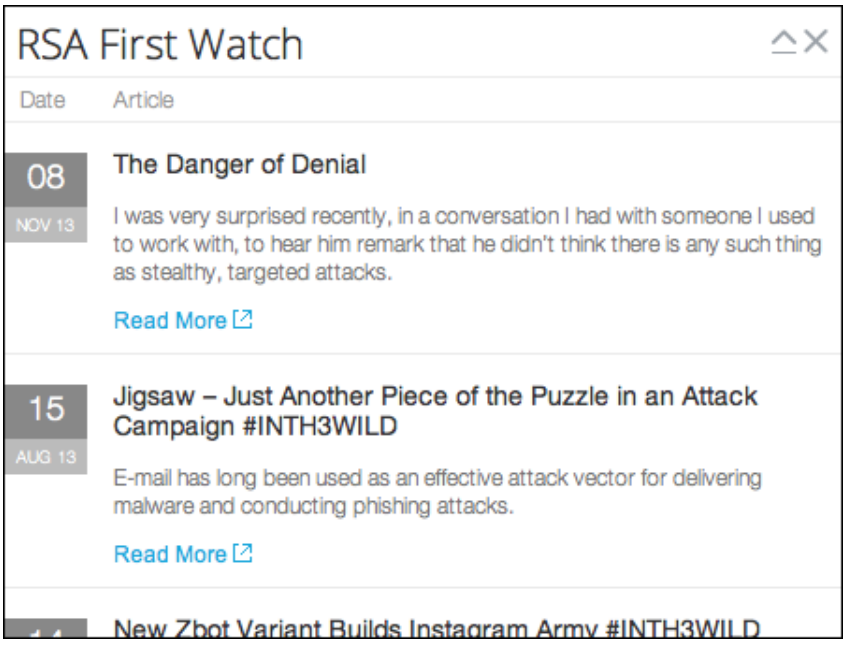
- 名前
- タイプ
- バージョン
- ステータス
- メモリ使用量
- CPU

[ホスト]ビューの詳細については、「*ホストおよびサービス スタート ガイド*」を参照してください。

[ダッシュボードRSA First Watch]ダッシュレット

[ダッシュボードRSA First Watch]ダッシュレットには、RSAのリサーチ/インシデント対応コミュニティからのトピックと脅威インテリジェンスが表示されます。ユーザーは、高度なサイバー脅威への対策や軽減のための情報を得ることができます。RSAのFirst Watch、インシデント対応、CIRC(コンピューター インシデント対応センター)の各チームは、膨大な数のIPとドメインをトラッキングするとともに、主立った脅威の発生源や行為者を追跡しています。

RSAダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボードのツールバーで ＋ ⊙ ＞[**ダッシュレットの追加**]をクリックして、[**ダッシュボードRSA First Watch**]を選択します。



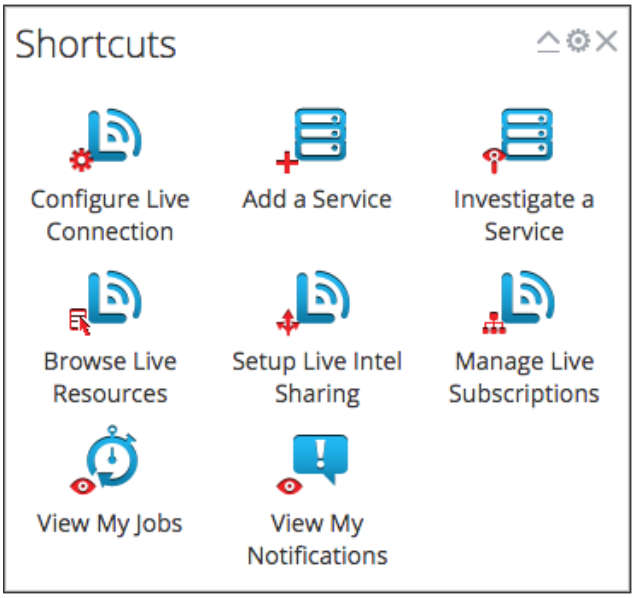
機能

列	説明
日付	記事が投稿された日付。
記事	記事のタイトル、記事のサンプル、詳細情報(記事全体)へのリンク。

[ダッシュボード ショートカット]ダッシュレット

[ダッシュボード ショートカット]ダッシュレットは、Security Analyticsの他の一般的なタスクへのリンクを提供します。システムを初めて使用するユーザーには最適なツールです。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＞[**ダッシュレットの追加**]をクリックして、[**ダッシュボード ショートカット**]を選択します。



機能

このダッシュレットにはSecurity Analyticsの一般的なタスクへのリンクが表示されます。

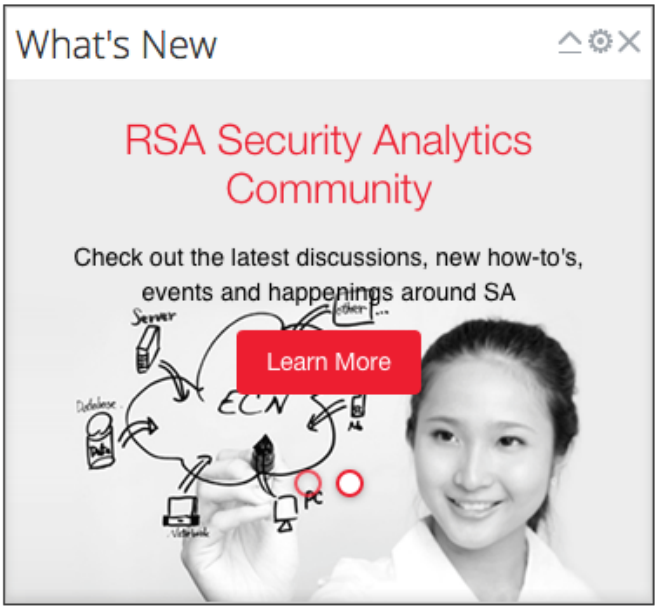
オプション	説明
Live 接続の構成	[Administration]の[システム]ビュー＞[Live構成]パネルにリンクしています。このパネルでは、Liveコンテンツ管理システムへの接続を構成します。
サービスの追加	[サービス]ビューにリンクしています。
サービスの調査	[ナビゲート]ビューの[ナビゲート]タブにリンクしています。このタブでは、利用可能なサービスのリストからサービスを選択してナビゲートできます。
Liveリソースの参照	Liveの[検索]ビューにリンクしています。このビューでは、Liveリソース ライブラリでリソースを検索できます。

オプション	説明
Liveインテリジェンス共有の構成	[Administration]の[システム]ビューにリンクしています。このビューでは、Liveインテリジェンス共有への参加を選択できます。
Liveサブスクリプションの管理	Liveの[構成]ビューにリンクしています。このビューでは、サブスクリプションや導入を表示して編集できます。
ジョブの表示	[ジョブ]パネル([プロファイル]ビュー) にリンクしています。このパネルでは、Security Analyticsのジョブを表示できます。
通知の表示	[通知]パネル([プロファイル]ビュー) にリンクしています。このパネルでは、システム通知を表示できます。

[ダッシュボード What's New]ダッシュレット

[ダッシュボード What's New]ダッシュレットは、すべてのSecurity Analytics製品を対象とした最新の製品情報や発表を表示します。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞ **[ダッシュレットの追加]**をクリックして、**[ダッシュボード What's New]**ダッシュレットを選択します。

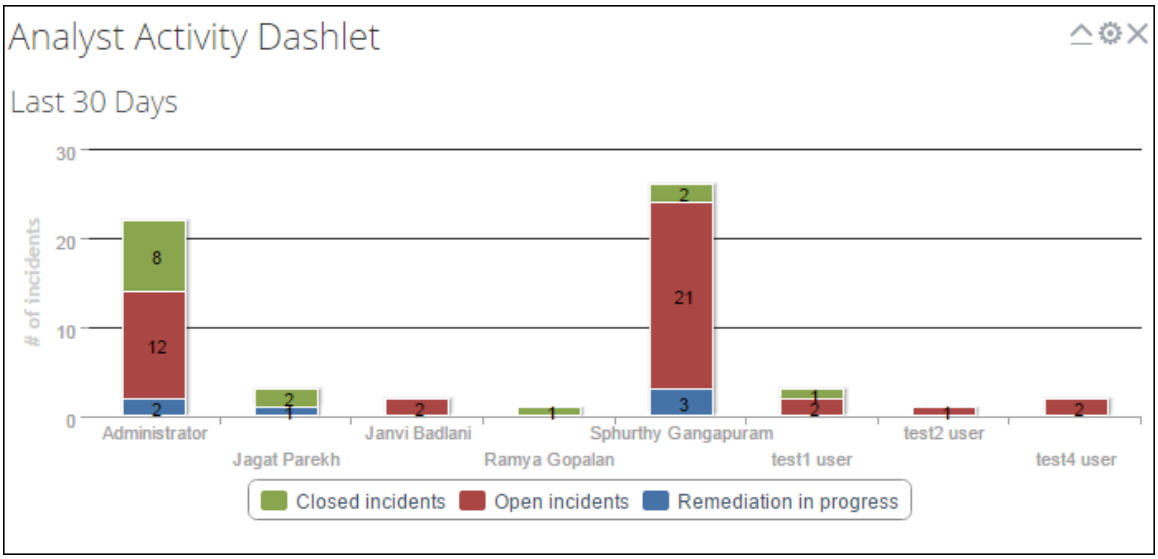


[インシデント アナリストのアクティビティ]ダッシュレット

[インシデント アナリストのアクティビティ]ダッシュレットは、一定期間内のインシデント数とステータスをアナリストごとに表示します。次の3つのカテゴリーを表示します。

- Closed incidents
- Open incidents
- Remediation in progress

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞[**ダッシュレットの追加**]をクリックします。ドロップダウンメニューから[**インシデント アナリストのアクティビティ**]を選択して、アクティビティの期間を設定します。



注：オプションを使用してダッシュレットを折りたたむ場合、棒グラフの再表示に時間がかかります。ブラウザの表示を更新するとグラフを素早く表示できます。

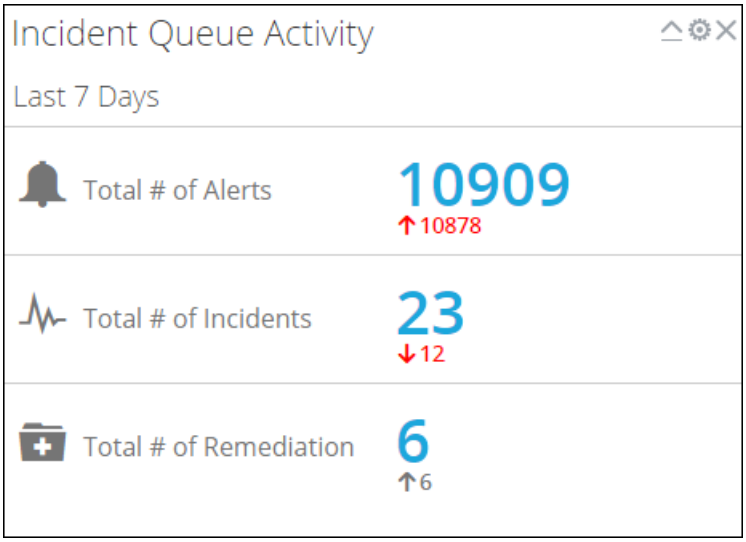
機能	説明
棒グラフ	棒グラフの一部の上にマウスを置くと、インシデントの数とステータスがテキストで表示されます。
インシデントのカテゴリー	下部の凡例には、インシデントのカテゴリーが表示されます。カテゴリーをクリックすると、グラフからカテゴリーが削除されます。カテゴリを再度クリックすると、グラフにカテゴリが再表示されます。

[インシデント キュー アクティビティ]ダッシュレット

[インシデント キューのアクティビティ]ダッシュレットは、選択された期間のアラート、インシデント、改善タスクの総数を表示します。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞[**ダッシュレットの追加**]をクリックして、[**インシデント キューのアクティビティ**]を選択します。[ダッシュレットの追加]ダイアログで、ダッシュレットの名前を入力し、結果を取得する期間を選択します。

次の図は、最近7日間の情報のダッシュレットの例を示します。

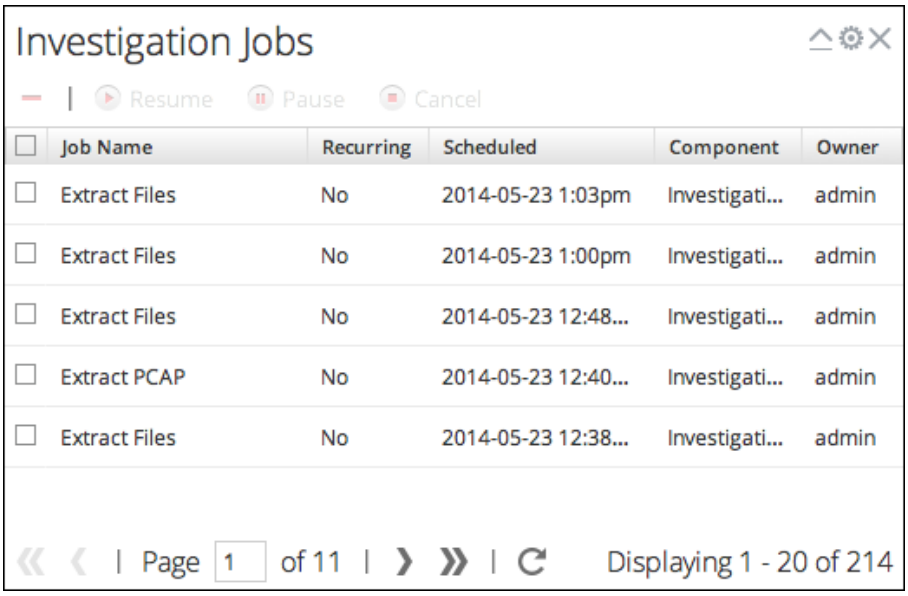


機能	説明
合計	個別の行に、アラート、インシデント、改善の合計が表示されます。 合計をクリックすると、アラート、インシデント、改善タスクのそれぞれのタブが開きます。
増加と減少	合計の下の数字は、増加または減少の量です。増減の幅が33%より大きい場合は、赤で表示されます。増減の幅が33%より小さい場合は、グレーで表示されます。

[Investigation ジョブ]ダッシュレット

[Investigation ジョブ]ダッシュレットは、Investigationモジュールのすべてのジョブのステータスを表示します。このダッシュレットでのツールバー、グリッド、ジョブの操作手順は[ジョブ トレイ]で説明しています。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞[**ダッシュレットの追加**]をクリックし、[**Investigationジョブ**]を選択します。



機能

[Investigationジョブ]ダッシュレットでは、自身が所有するすべてのジョブ(繰り返しおよび繰り返しでない)をリストし、進行状況を監視できます。

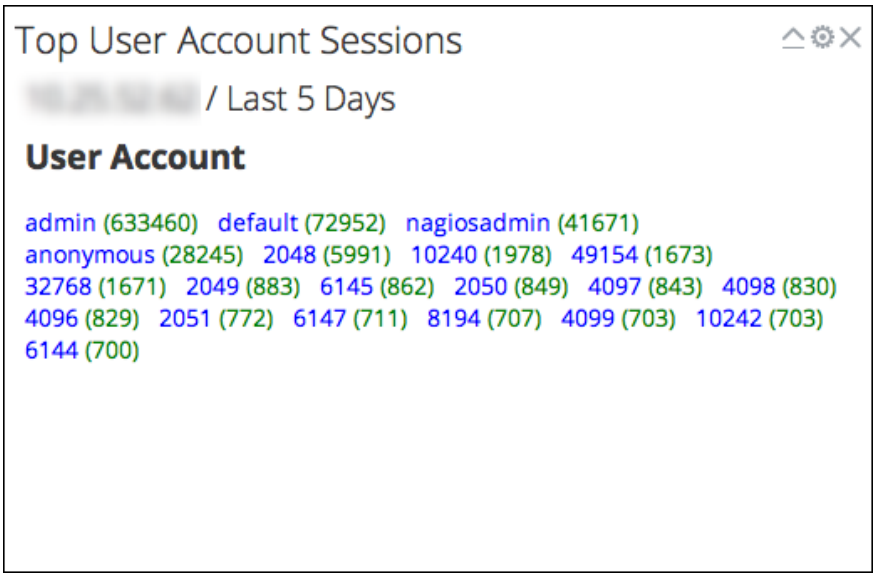
機能	説明
	[再開]オプションは、一時停止されていた繰り返しジョブにのみ適用されます。一時停止されていたジョブを再開する場合、ジョブの次の回の実行は、スケジュールどおりに実行されます。
	[一時停止]オプションは、繰り返しジョブにのみ適用されます。実行中の繰り返しジョブを一時停止しても、その回の実行には影響しません。(ジョブが一時停止中のままである場合)次の回の実行は、スキップされます。

機能	説明
	繰り返しジョブまたは繰り返しではないジョブをキャンセルします。ジョブは、実行中にキャンセルできます。繰り返しジョブをキャンセルすると、ジョブのその回の実行がキャンセルされます。スケジュールされているジョブの次の回の実行は、正常に実行されます。
	[ジョブ]パネルから繰り返しジョブまたは繰り返しではないジョブを削除します。ジョブを削除すると、ジョブは[ジョブ]パネルから直ちに削除されます。確認ダイアログは表示されません。繰り返しジョブを削除すると、スケジュールされている以降のジョブの実行もすべて削除されます。

[Investigation 上位の値] ダッシュレット

[Investigation上位の値]ダッシュレットでは、該当するアプライアンスで、特定の期間と特定のメタ タイプに対して上位の値を調べることができます。メタ データとクエリーのパラメーターは、[ダッシュレットの追加]ダイアログで定義します。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞[**ダッシュレットの追加**]をクリックして、[**Investigation上位の値**]を選択します。



機能

メタ データとクエリーのパラメータは、[**ダッシュレットの追加**]ダイアログで定義します。

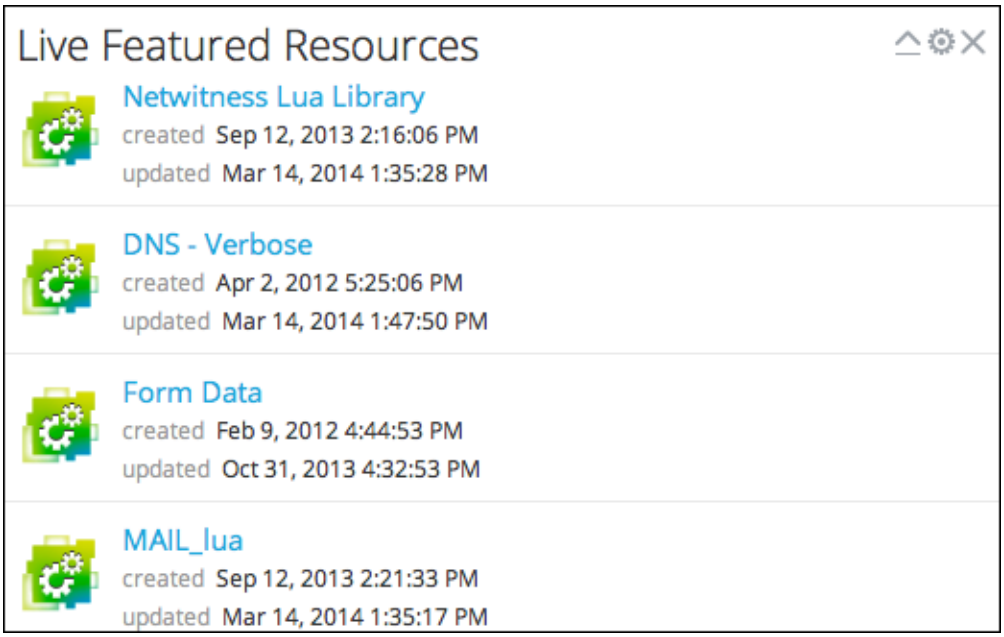
機能	説明
タイトル	ダッシュレットのタイトル。
サービス	ターゲットとなるサービスの名前またはIPアドレス。

機能	説明
時間	直近5分 直近10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
メタ タイプ	ドロップダウン リストからメタ タイプを選択します。
クエリー	クエリーを入力してさらに詳細な結果を表示できます
結果の件数	ドロップダウン リストから表示する結果の数を選択します。

[Live 推奨のリソース]ダッシュレット

[Live推奨のリソース]ダッシュレットは、構成されたCMS(Content Management System) サーバーでfeatured(推奨) としてタグ付けされたLiveリソースのリストを表示します。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞[**ダッシュレットの追加**]をクリックし、[**Live推奨のリソース**]を選択します。



機能

このダッシュレットには、推奨されるLiveリソースのページ ビューが含まれ、各リソースについて次の情報を提供します。

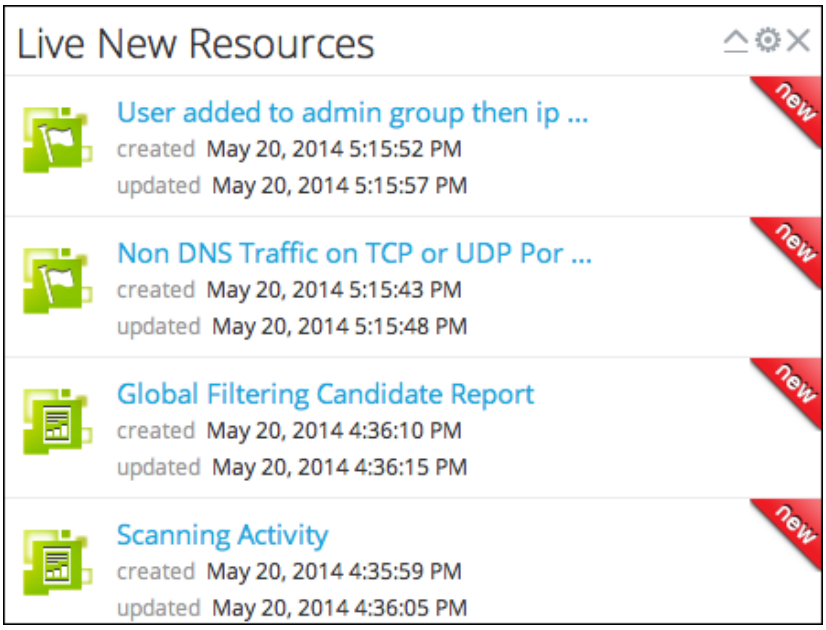
値	説明
(リソース タイプ アイコン)	Liveリソースのタイプが、アイコンで示されます。たとえば、この画面イメージのアイコンは、Parser Feedを示しています。[リソース タイプ]アイコンをクリックすると、新しいブラウザ タブが開き、Liveの[リソース]ビューでリソースの詳細が表示されます。

値	説明
リソース名	リソースの名前。たとえば、「**NetWitness APT Threat IPs**」など。[**リソース名**]をクリックすると、Liveの[リソース]ビューでリソースの詳細が表示されます。ビューは、現在のブラウザタブに表示されます。
作成日	リソースが作成された日。
更新日	リソースが最後に更新された日。

[Live 新しいリソース]ダッシュレット

[Live 新しいリソース]ダッシュレットは、構成されたCMS(Content Management System) サーバー上で「新規」としてタグ付けされたLiveリソースのリストを表示します。リソース名をクリックすると、リソースの詳細ビューにアクセスできます。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞ **[ダッシュレットの追加]**をクリックして、[**Live新しいリソース**]を選択します。



機能

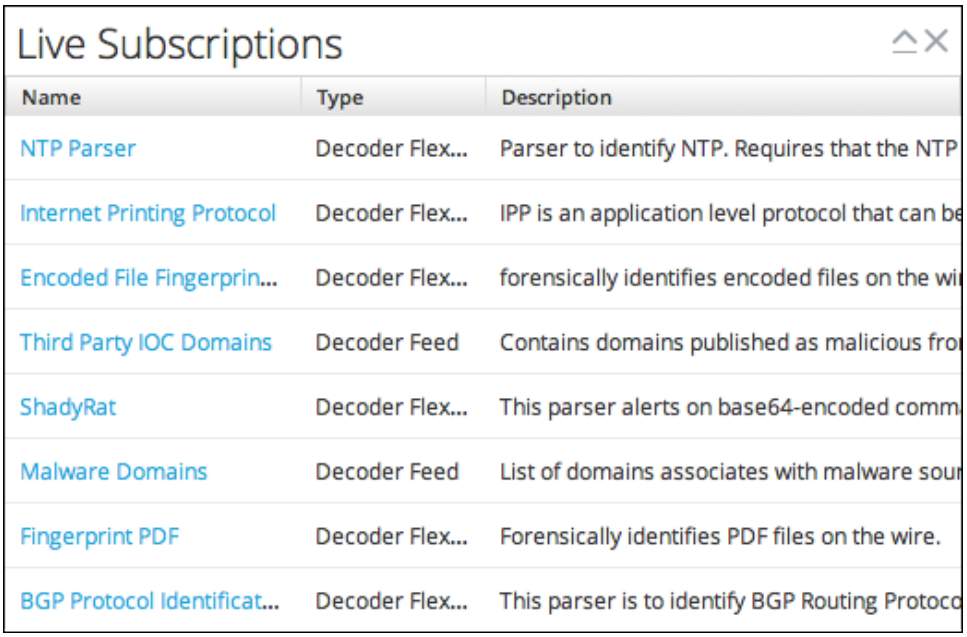
このダッシュレットには、新しいLiveリソースのページ ビューが含まれ、各リソースについて次の情報を提供します。

値	説明
リソースタイプアイコン	 Liveリソースのタイプが、アイコンで示されます。たとえば、左側のアイコンは、Decoder FlexParserを示しています。[リソース タイプ]アイコンをクリックすると、新しいブラウザ タブが開き、Liveの[リソース]ビューでリソースの詳細が表示されます。
リソース名	リソースの名前、たとえば、「**Gh0st Protocol Parser**」など。[リソース名]をクリックすると、Liveの[リソース]ビューでリソースの詳細が表示されます。ビューは、現在のブラウザ タブに表示されます。
作成日	リソースが作成された日。
更新日	リソースが最後に更新された日。

[Liveサブスクリプション]ダッシュレット

[Liveサブスクリプション]ダッシュレットは、このSecurity AnalyticsインスタンスがサブスクライブしているすべてのLiveリソースのリストを提供します。これはシンプルな参照リストです。サブスクリプションを管理する必要がある場合は、Liveの[構成]ビューにある[サブスクリプション]タブを使用します。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞ **[ダッシュレットの追加]**をクリックして、**[Liveサブスクリプション]**を選択します。



機能

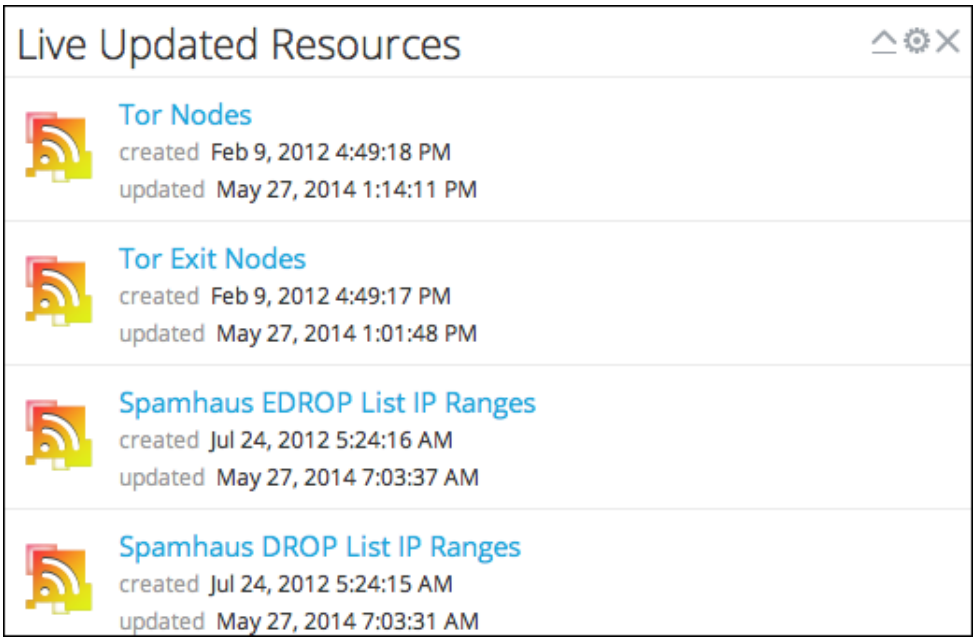
この項目は、Liveの[構成]ビューに表示されるサブスクリプション のグリッドのサブセットです。

値	説明
名前	サブスクリプションの名前を表示します。
タイプ	サブスクリプションのタイプを指定します。
説明	サブスクリプションが提供する情報の種類を説明します。

[Live 更新されたリソース]ダッシュレット

[Live更新されたリソース]ダッシュレットは、構成されたCMS(Content Management System) サーバ上で「更新」としてタグ付けされたLiveリソースのリストを表示します。リソース タイトルをクリックすると、リソースの詳細ビューにアクセスできます。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボードで ＋ ＞[**ダッシュレットの追加**]をクリックして、[**Live更新されたリソース**]を選択します。



機能

このダッシュレットには、更新されたLiveリソースのページ ビューが含まれ、各リソースについて次の情報を提供します。

このダッシュレットには、更新されたLiveリソースのページ ビューが含まれ、各リソースについて次の情報を提供します。

値	説明
 リソースタイプアイコン	Liveリソースのタイプが、アイコンで示されます。たとえば、この画面イメージのアイコンは、Decoder Feedを示しています。[リソース タイプ]アイコンをクリックすると、新しいブラウザ タブが開き、Liveの[リソース]ビューでリソースの詳細が表示されます。
リソース名	リソースの名前、たとえば、「**Spamhaus EDROP List IP Ranges**」など。[リソース名]をクリックすると、Liveの[リソース]ビューでリソースの詳細が表示されます。ビューは、現在のブラウザ タブに表示されます。
作成日	リソースが作成された日。
更新日	リソースが最後に更新された日。

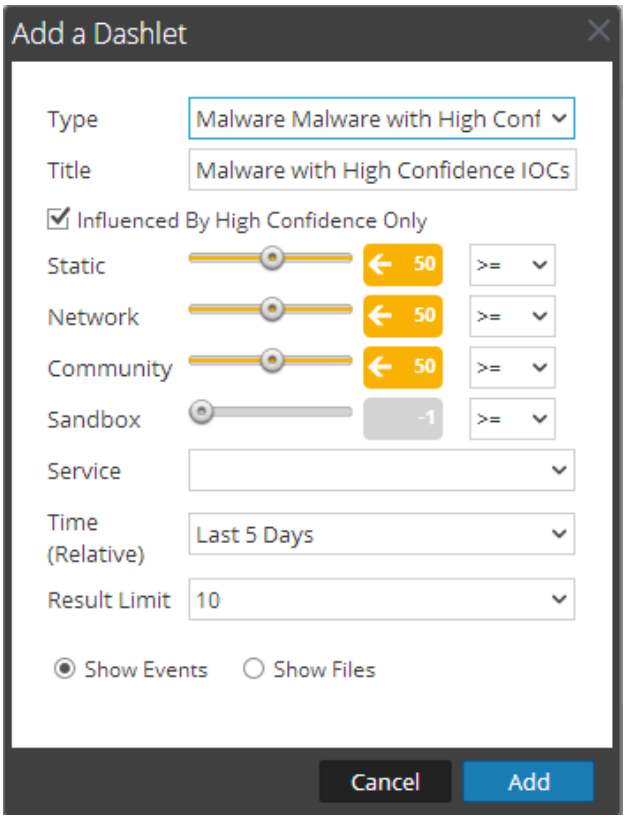
[Malware 高確率IOCとハイスコアのマルウェア]ダッシュレット

[Malware高確率IOCとハイスコアのマルウェア]ダッシュレットは、Malware Analysisがセキュリティ侵害インジケーターで検出したイベントのうち、マルウェアが含まれている可能性が高いものやスコア モジュールでのスコアが高いものを示します。このダッシュレットは、Unifiedダッシュボードおよび[Malware]ビューで使用できます。Malware Analystが最初にSecurity Analyticsにログインするとき、デフォルトでダッシュボードに表示されるのは[What's New]ダッシュレットのみです。アナリストは、追加のMalwareダッシュレットを作成する必要があります。

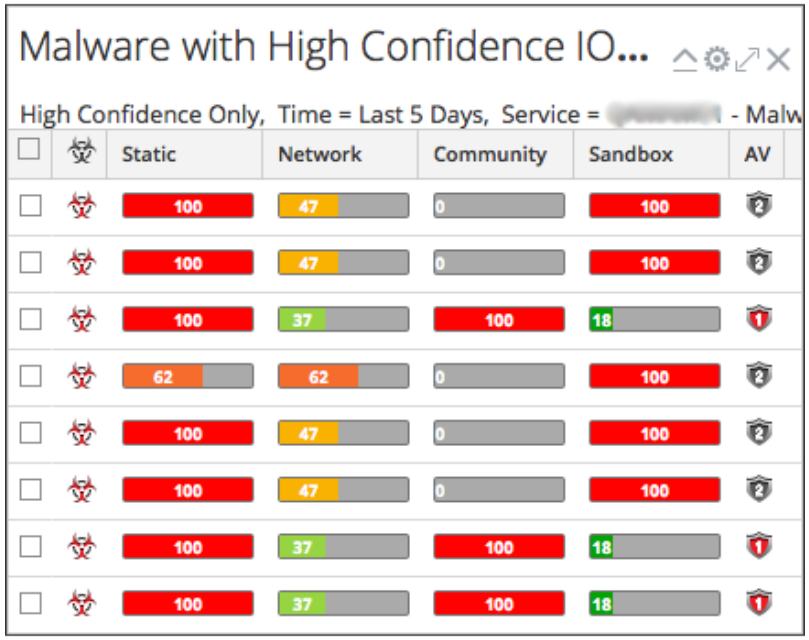
[Malware 高確率IOCとハイスコアのマルウェア]ダッシュレットは構成変更が可能です。ダッシュレットから複数のコピーを作成して結果をフィルタ表示し、イベント リストやファイル リストとして構成することができます。

このダッシュレットを**Security Analyticsダッシュボード**またはカスタム ダッシュボードの一部として表示するには、ダッシュボード ツールバーで ＋ ＞**[ダッシュレットの追加]**を選択し、**[タイプ]**ドロップダウン メニューから**[Malware高確率IOCとハイスコアのマルウェア]**をクリックします。

これは[Malware 高確率IOCとハイスコアのマルウェア]ダッシュレットの設定の例です。



これは[Malware 高確率IOCとハイスコアのマルウェア]ダッシュレットの例です。



機能

次の表に、このダッシュレットの構成可能な値を一覧で示します。

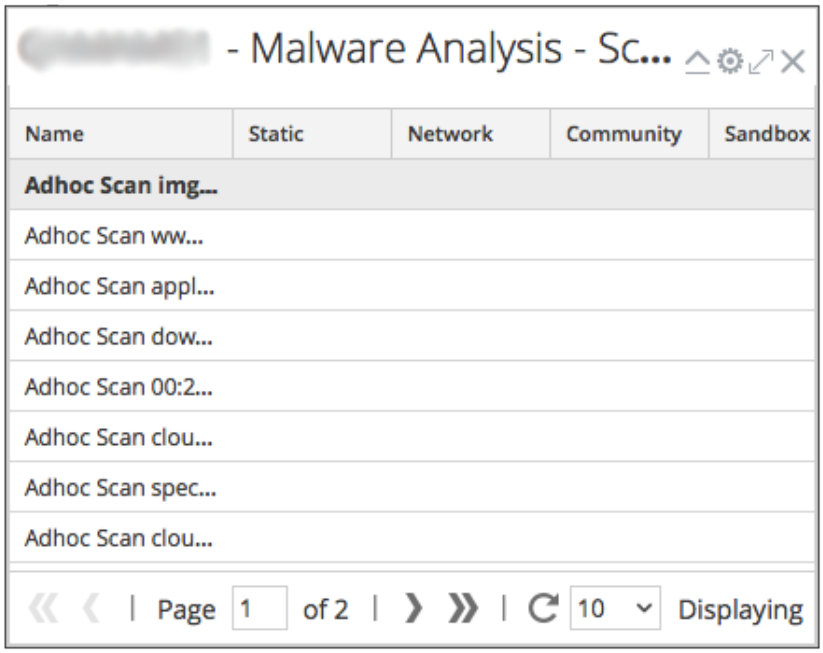
項目	説明
タイトル	ダッシュレットの名前を識別します。各ダッシュレットには一意の名前が必要です。特に、同じダッシュレットのインスタンスが複数ある場合には名前で区別できるようにしておきます。この名前はダッシュレットのタイトル バーに表示されます。
高確率フラグのみ	この項目をオンにすると、高確率フラグが付けられたセキュリティ侵害インジケータを含むイベントおよびファイルのみがダッシュレットに表示されます。
静的、ネットワーク、コミュニティ、サンドボックス	各スコア モジュールのスコアに基づいて結果をフィルタします。値は、=、<=、>=のいずれかに設定できます。
結果の件数	表示する結果の数を設定します。ドロップダウン リストで選択可能な値は、5、10、20、30、40です。
サービス	監視対象のサービスを選択します。

項目	説明
時間	表示される結果の時間範囲を制限します。
イベントの表示またはファイルの表示	結果の形式を、イベント リストまたはファイル リストの形式で指定します。

[Malware Analysis スキャン ジョブ リスト]ダッシュレット

[マルウェア スキャン ジョブリスト]ダッシュレットには、[マルウェア サービスの選択]ダイアログと同じスキャン ジョブ リストが表示されます。このダッシュレットから、完了したスキャンを直接開くことができます。

Security Analyticsダッシュボードに、またはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞[**ダッシュレットの追加**]をクリックし、[**マルウェア スキャン ジョブ リスト**]を選択します。



機能

このスキャン ジョブ リストの列は、[マルウェア サービスの選択]ダイアログのスキャン ジョブ リストと同じです。

ジョブをダブル クリックすると、[Investigation]＞[Malware Analysis]ビューでジョブを表示できます。選択したスキャンの[イベントのサマリー]が開き、デフォルトのダッシュレットが新しいブラウザ タブに表示されます。

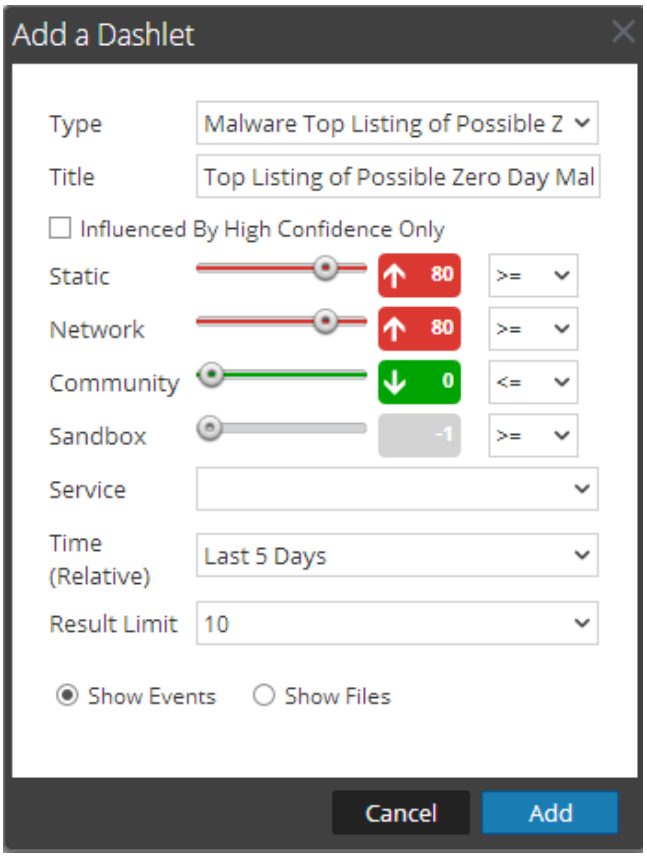
[Malware ゼロデイの可能性が高いマルウェアの上位リスト]ダッシュレット

[ゼロデイの可能性が高いマルウェアの上位リスト]ダッシュレットは、Malware Analysisのイベント リストまたはファイル リストでゼロデイ攻撃の可能性がある上位10イベントを示しています。このダッシュレットは、ダッシュボードおよび[Malware]ビューで使用できます。Malware Analystが最初にSecurity Analyticsにログインするとき、デフォルトでダッシュボードに表示されるのは[What's New]ダッシュレットのみです。アナリストは、追加のMalwareダッシュレットを作成する必要があります。

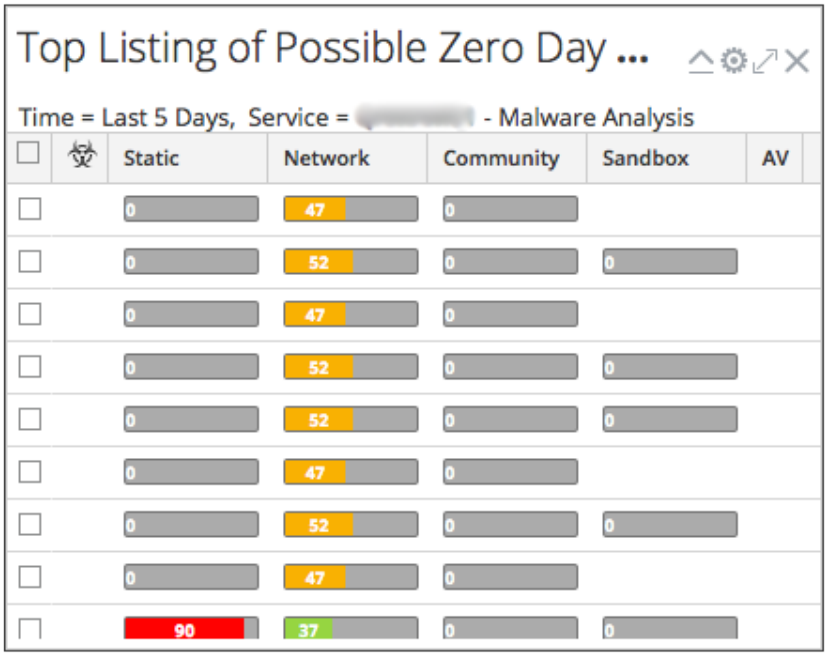
[ゼロデイの可能性が高いマルウェアの上位リスト]ダッシュレットは構成変更が可能です。ダッシュレットから複数のコピーを作成して結果をフィルター表示し、イベント リストやファイル リストとして構成することができます。このダッシュレットからは、イベントをダブル クリックしてSecurity Analytics Investigationを直接起動し、イベントの調査を開始できます。[Investigation] > [Malware]ビューからアクセスする必要はありません。

このダッシュレットを**Security Analytics**ダッシュボードまたはカスタム ダッシュボードの一部として表示するには、ダッシュボード ツールバーで + > **[ダッシュレットの追加]**をクリックして、[**タイプ**]ドロップダウン メニューから[**Malwareゼロデイの可能性が高いマルウェアの上位リスト**]を選択します。

これはイベント リストを表示するように構成されたダッシュレット設定の例です。



これは、ダッシュレットの例です。このダッシュレットの機能は、Malware Analysisのイベント リストまたはファイル リストの機能と同じです。



機能

次の表に、このダッシュレットの構成可能な値を一覧で示します。

項目	説明
タイトル	ダッシュレットの名前を識別します。各ダッシュレットには一意の名前が必要です。特に、同じダッシュレットのインスタンスが複数ある場合には名前で区別できるようにしておきます。この名前はダッシュレットのタイトル バーに表示されます。
高確率フラグのみ	この項目をオンにすると、高確率フラグが付けられたセキュリティ侵害インジケータを含むイベントおよびファイルのみがダッシュレットに表示されます。
静的、ネットワーク、コミュニティ、サンドボックス	各スコア モジュールのスコアに基づいて結果をフィルタします。値は、=、<=、>= のいずれかに設定できます。コミュニティ フィルタの演算子は、デフォルトで、適用されたスライダーの値以下となります。他のフィルタの演算子は、デフォルトで、適用されたスライダーの値以上となります。

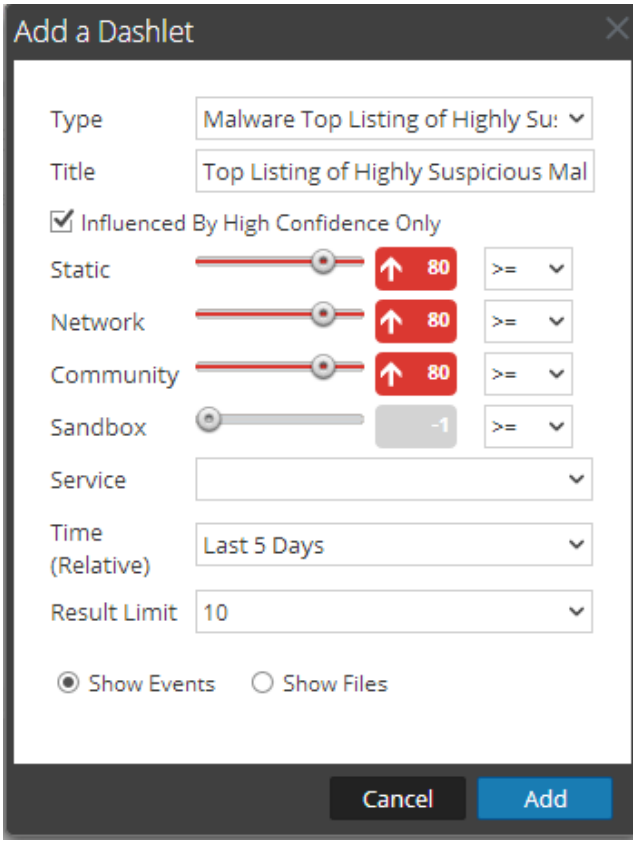
項目	説明
サービス	監視対象のサービスを選択します。
時間	表示される結果の時間範囲を制限します。
結果の件数	表示する結果の数を設定します。ドロップダウン リストで選択可能な値は、5、10、20、30、40です。
イベントの表示またはファイルの表示	結果の形式を、イベント リストまたはファイル リストの形式で指定します。

[Malware 極めて疑わしいマルウェアの上位リスト]ダッシュレット

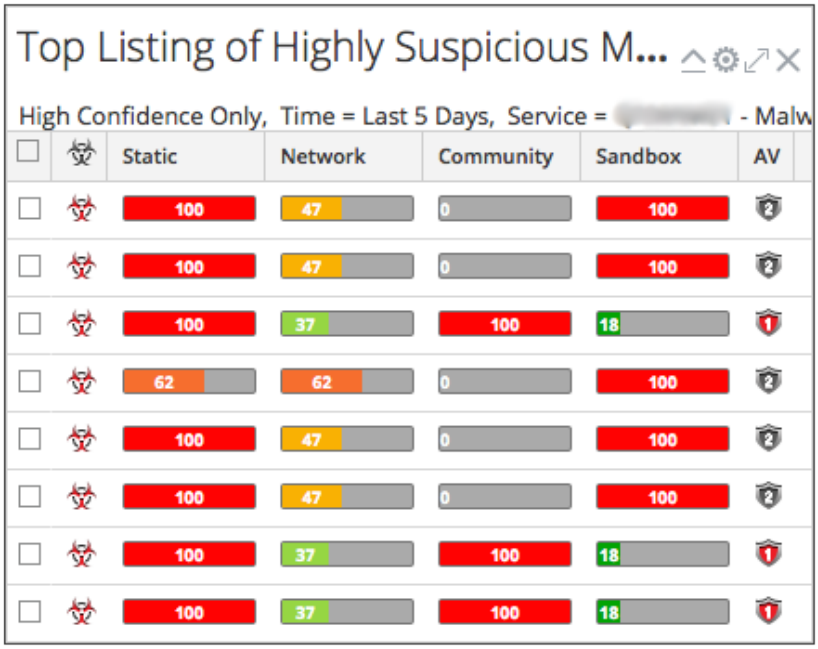
[Malware極めて疑わしいマルウェアの上位リスト]ダッシュレットでは、最も疑わしい上位10のイベントが、Malware Analysisのイベント リストまたはファイル リストに表示されます。このダッシュレットは、ダッシュボードおよび[Malware Analysis]ビューで使用できます。Malware Analystが最初にSecurity Analyticsにログインするとき、デフォルトでダッシュボードに表示されるダッシュレットは[What's New]ダッシュレットのみです。アナリストは、追加のMalware Analysisダッシュレットを作成する必要があります。

[Malware 極めて疑わしいマルウェアの上位リスト]ダッシュレットは構成変更が可能です。ダッシュレットから複数のコピーを作成して結果をフィルタ表示し、イベント リストやファイル リストとして構成することができます。

このダッシュレットを**Security Analyticsダッシュボード**に表示、またはカスタム ダッシュボードの一部として表示するには、ダッシュボード ツールバーで ＋ ＞ **[ダッシュレットの追加]**をクリックし、[**タイプ**]ドロップダウン メニューから[**Malware極めて疑わしいマルウェアの上位リスト**]を選択します。



これは、ダッシュレットの例です。



機能

機能は、**Malware Analysisのイベント リストとファイル リスト**の機能と同じです(詳細については、「*Investigationおよび*Malware Analysis*ガイド*」を参照してください) 。ダッシュレットのアイテムのMalware Analysis Investigationを起動するには、グリッドでイベントまたはファイル名をダブルクリックします。

次の表に、このダッシュレットの構成可能な値を一覧で示します。

項目	説明
タイトル	ダッシュレットの名前を識別します。各ダッシュレットには一意の名前が必要です。特に、同じダッシュレットのインスタンスが複数ある場合には名前で区別できるようにしておきます。この名前はダッシュレットのタイトル バーに表示されます。
高確率フラグのみ	この項目をオンにすると、高確率フラグが付けられたセキュリティ侵害インジケータを含むイベントおよびファイルのみがダッシュレットに表示されます。
静的、ネットワーク、コミュニティ、サンドボックス	各スコア モジュールのスコアに基づいて結果をフィルタします。値は、=、<=、>=のいずれかに設定できます。

項目	説明
サービス	監視対象のサービスを選択します。
時間	表示される結果の時間範囲を制限します。
結果の件数	表示する結果の数を設定します。ドロップダウン リストで選択可能な値は、5、10、20、30、40です。
イベントの表示またはファイルの表示	結果の形式を、イベント リストまたはファイル リストの形式で指定します。

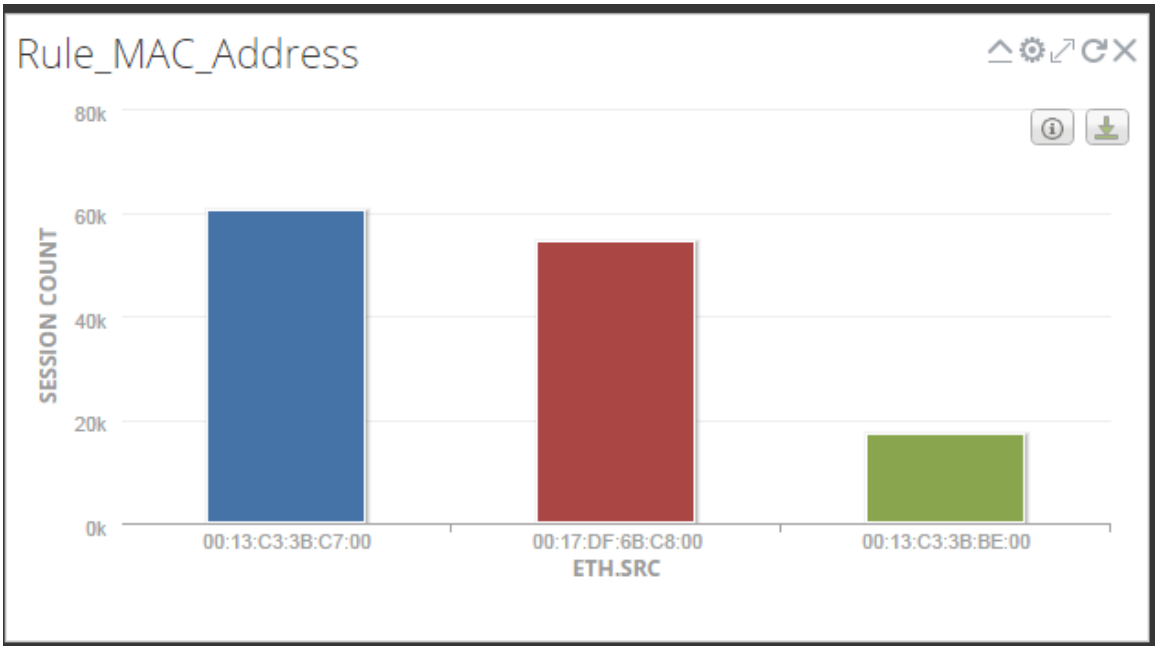
[Reports リアルタイム チャート]ダッシュレット

[Reportsリアルタイム チャート]ダッシュレットは、定義したチャートのリストから1つのチャートを表示します。チャートはリアルタイム データから出力され、設定した更新間隔で更新されます。各チャートは、選択したチャート タイプや時間の設定で定義されます。

[時系列チャート]オプションと[合計チャート]オプションのいずれかを選択できます。チャートは、現在のデータをグラフに表示し、過去の特定の時点のみのデータは表示しません。

チャートは、チャートの定義で定義された時間間隔に基づくデータによって生成されます。データは最大で過去20回の時間間隔から表示できます。たとえば、チャートの定義で更新間隔として5分を選択し、時間数として60分を選択した場合、チャートは現在から過去60分までのデータを表示します。ダッシュレット内のチャートは、定義した更新間隔で更新されます。

Security Analyticsダッシュボードまたはカスタム ダッシュボードの一部としてこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ > **[ダッシュレットの追加]**をクリックして、**[タイプ]**ドロップダウン メニューから**[Reportsリアルタイム チャート]**を選択します。



機能

以下の表でチャート オプションを説明します。

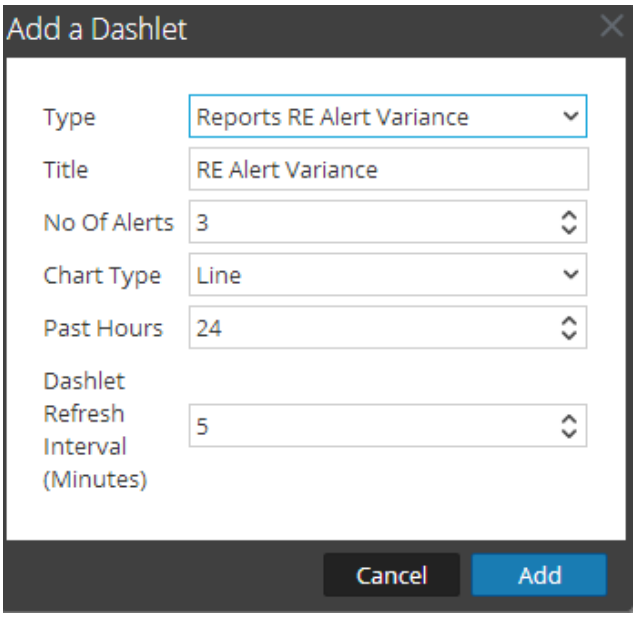
項目	説明
チャート	定義済みのチャートから、表示するチャートを選択します。ダッシュレットにつき1つのチャートのみ選択できます。

項目	説明
タイトル	[Reportsリアルタイム チャート]ダッシュレットの名前を入力します。この名前はダッシュレットのタイトル バーに表示されます。
系列	**時系列チャート**:チャートには、選択した時間帯の値の変化が表示されます。
	合計チャート:チャートには、選択した時間帯の各集計値の合計が表示されます。
チャート タイプ	ダッシュレットに含めるチャート タイプを選択します。ドロップダウンに表示される値は、面、列、折れ線などです。
時間	過去の時間間隔を選択します。
ダッシュレット更新間隔(分)	ダッシュレットのデータを更新する時間間隔(分)を設定します。時間間隔の値は1～180分です。

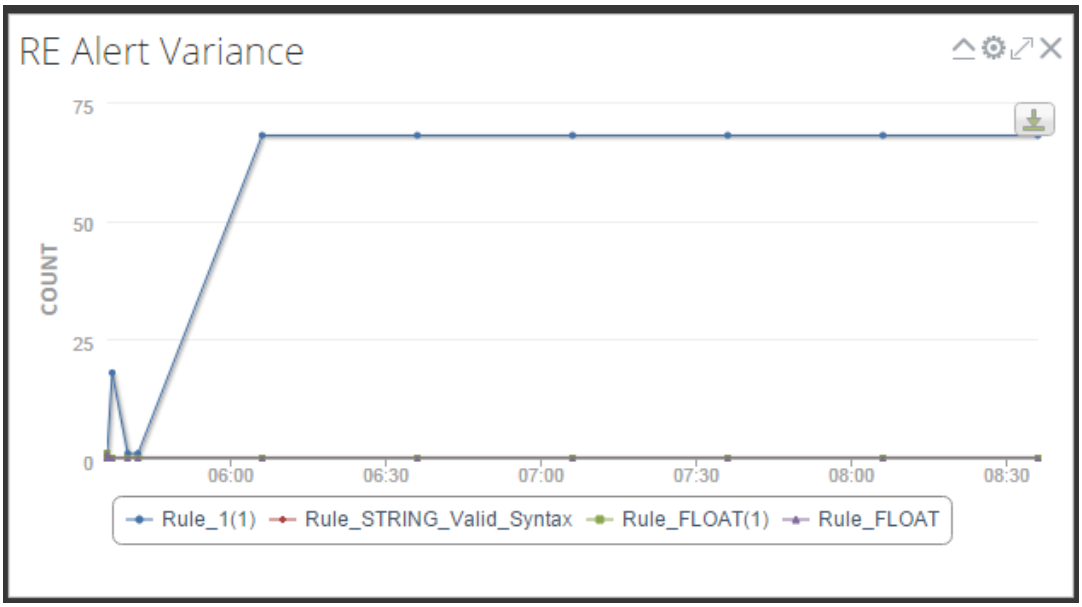
Reports アラート推移ダッシュレット

[Reportsアラート推移]ダッシュレットは、4種類の時系列チャートでアラートの上位項目を表示し、構成変更が可能なダッシュレットです。チャートに含める結果を構成できます(指定した時間範囲内で上位2アラートから上位15アラートまで)。

Security Analyticsダッシュボードまたはカスタムダッシュボードにこのダッシュレットを表示するには、ダッシュボードのツールバーで >**[ダッシュレットの追加]**を選択して、[**タイプ**]ドロップダウンメニューから[**Reportsアラート推移**]を選択します。



次の図に例を示します。



機能

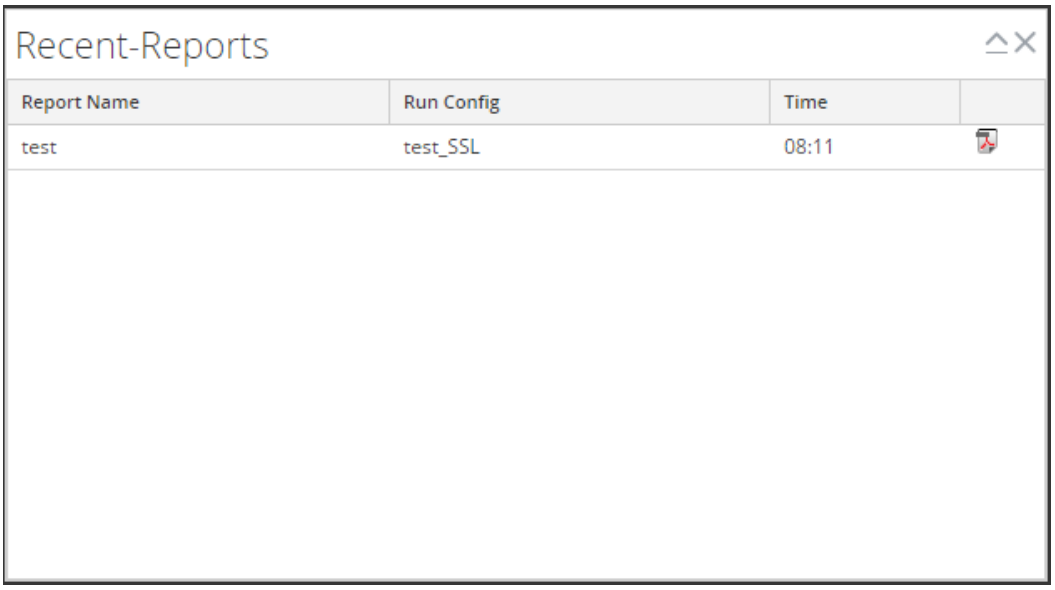
このダッシュレットは、対象となるReporting Engineが最も頻繁にトリガーするアラートを可視化することができます。各チャート タイプでは、アラートの数、過去何時間分のアラートを取得するか、チャートの更新間隔などを定義します。

項目	説明
タイプ	ダッシュレットに含めるチャート タイプを選択します。 • 横棒(X軸 = カウントおよびY軸 = アラート名) • 縦棒(X軸 = カウントおよびY軸 = アラート名) • 折れ線(X軸 = カウントおよびY軸 = アラート名)
タイトル	ダッシュレットの名前を指定します。この名前はダッシュレットのタイトルバーに表示されます。
アラート数	アラートの数を選択します。値の範囲は2～15です。
時間	アラートを取得する対象となる時間数を選択します。
ダッシュレット更新間隔(分)	ダッシュレットのデータを更新する時間間隔(分)を設定します。この間隔は1～180分です。

[Reports 直近のレポート]ダッシュレット

[Reports直近のレポート]ダッシュレットには、Security Analyticsで最近実行されたレポートのリストが表示されます。表示される最近のレポートは過去24時間のものです。

Security Analyticsダッシュボードまたはカスタム ダッシュボードの一部としてこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞[**ダッシュレットの追加**]をクリックして、[**タイプ**]ドロップダウン メニューから[**Reports直近のレポート**]を選択します。



機能

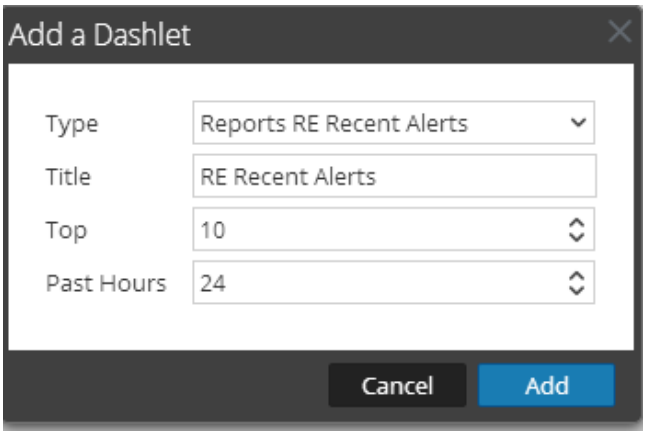
デフォルトのダッシュレットに表示される各列について、次の表で説明します。

列	説明
レポート名	最近実行されたレポートの名前。
スケジュール名	最近実行されたレポートのスケジュール名です。
時間	レポートがスケジュールされた時刻です。
エクスポート	ファイルをエクスポートするには、エクスポート アイコン( ) をクリックします。

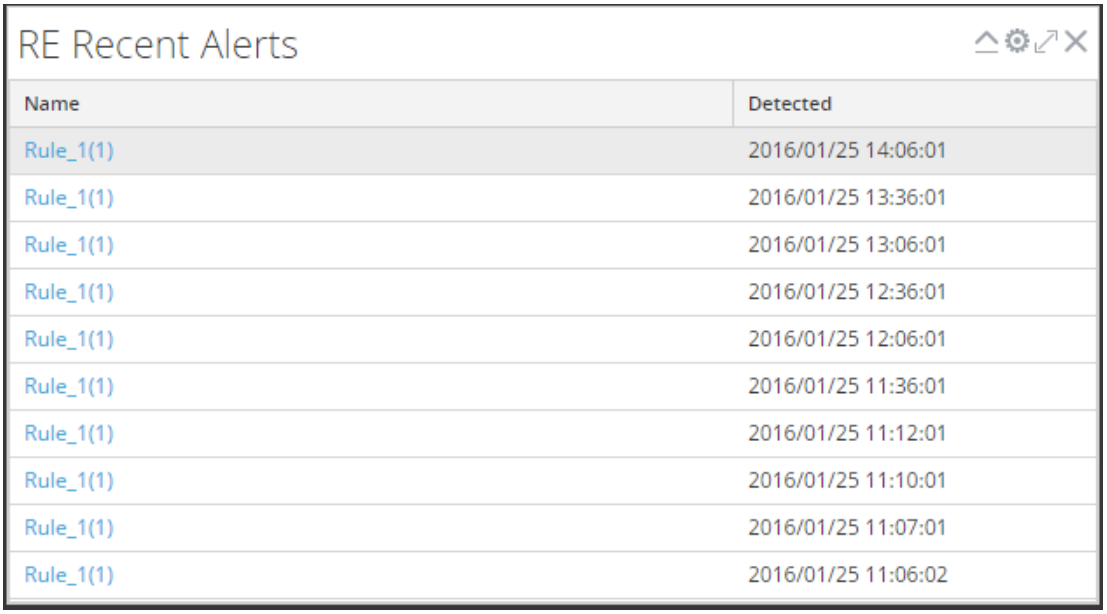
[Reports 直近のREアラート]ダッシュレット

[Reports 直近のREアラート]ダッシュレットは、ダッシュボード上に最近のアラートを表示します。このダッシュレットでは、表示する最新アラートの数を構成でき、アラートを取得する時間範囲を指定することもできます。

Security Analyticsダッシュボードまたはカスタム ダッシュボードにこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ > **[ダッシュレットの追加]**を選択して、**[タイプ]**ドロップダウン メニューから**[Reports直近のREアラート]**を選択します。



次の図に例を示します。



機能

次の表は、[Reports直近のREアラート]ダッシュレットの列について説明しています。

列	説明
名前	定義されているアラートの名前。
検出	アラートが発生した日付と時刻。検出日時は、Security Analyticsがこのアラートを発生させる状況を検出した時点の時刻です。

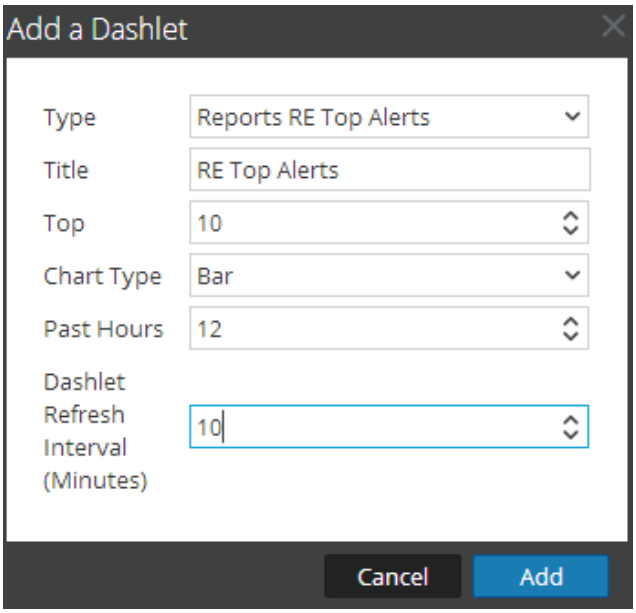
[Reports RE上位アラート]ダッシュレット

[ReportsRE上位アラート]ダッシュレットは構成変更が可能なダッシュレットで、4種類のチャートで上位アラートを示します。チャートに含める結果を構成できます(指定した時間範囲内で上位2アラートから上位15アラートまで)。

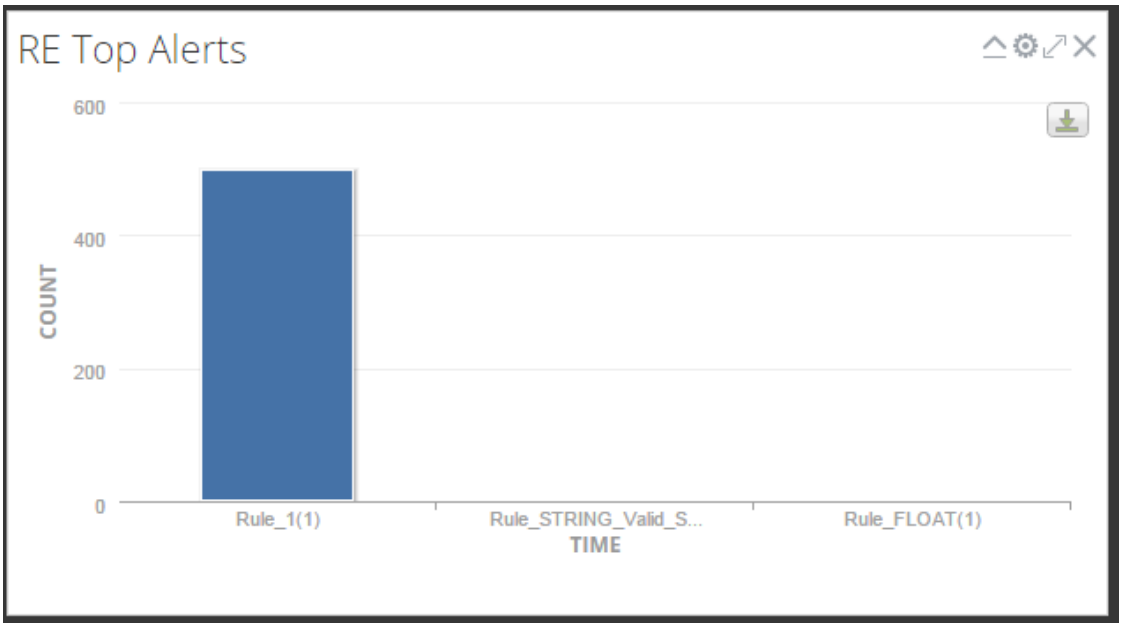
このチャートでは、指定した時間と更新間隔内に発生した上位(Top)のアラートについて、トリガーされたイベント数を表示します。チャートの最初のデータポイントは、定義された時間でアラートがトリガーしたイベント数(アラート カウント)を表示します。それ以降のデータポイントは、最初のデータポイントのアラート カウントと定義された更新間隔のアラート カウントを加えることによって示されます。

たとえば、定義した時間範囲でアラートによってトリガーされたイベント数(アラート カウント)が10の場合、チャートの最初のデータポイントには10と表示されます。それ以降のデータポインは最初の値10に加えて、定義されたダッシュレットの更新間隔内のアラートによってトリガーされたイベント数(アラート カウント)となります。

Security Analyticsダッシュボードまたはカスタム ダッシュボードの一部としてこのダッシュレットを表示するには、ダッシュボード ツールバーで ＋ ＞[**ダッシュレットの追加**]をクリックして、[**タイプ**]ドロップダウン メニューから[**Reports RE上位アラート**]を選択します。



次の図に例を示します。



機能

このダッシュレットは、対象となるReporting Engineが最も頻繁にトリガーするアラートを可視化することができます。各チャート タイプでは、上位アラートの数、アラートを取得する時間、ダッシュレットでのチャートの更新間隔を定義します。

項目	説明
チャート タイプ	ダッシュレットに含めるチャート タイプを選択します。 • 横棒(X軸 = カウントおよびY軸 = アラート名) • 縦棒(X軸 = カウントおよびY軸 = アラート名) • 円 • 折れ線(X軸 = カウントおよびY軸 = アラート名) • 表(X軸 = カウントおよびY軸 = アラート名)
タイトル	[Reportsリアルタイム チャート]ダッシュレットの名前を入力します。この名前はダッシュレットのタイトル バーに表示されます。
上位	上位アラートの数を選択します。値の範囲は2～15です。
時間	アラートを取得する対象となる時間数を選択します。

項目	説明
ダッシュレット更新間隔(分)	ダッシュレットのデータを更新する時間間隔(分)を設定します。この間隔は1～180分です。