NetWitness® Platform

バージョン12.5

リリース ノート

NETWITNESS
Platform

連絡先

NetWitnessコミュニティ(https://community.netwitness.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およびその他の商標は、RSA Security LLCまたはその関連会社(「RSA」) の商標または登録商標です。RSAの商標のリストについては、https://www.rsa.com/en-us/company/rsa-trademarksを参照してください。その他の商標は、それぞれの所有者の商標または登録商標です。

使用許諾契約

本ソフトウェアと関連ドキュメントは、RSA Security LLCまたはその関連会社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、民事および刑事上の責任が課せられる可能性があります。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。

サードパーティのリポジトリを展開したり、サポートされているNetWitnessバージョンに含まれない基盤となるNetWitnessオペレーティング システムに変更を加えたりしないことをお勧めします。NetWitnessが承認したイメージ以外でのこのような変更は、サービスまたは機能の競合を引き起こす可能性があり、NetWitnessを最適化された機能状態に戻すにはNetWitnessシステムの再イメージ化が必要になる場合があります。サードパーティのリポジトリが展開された場合、またはNetWitnessの承認なしに顧客がサポートされていない変更を行った場合、トラブルシューティングの取り組みまたはサービスの再イメージ化によって問題が解決されるまで、システムの誤動作については顧客が全責任を負います。

サード パーティ ライセンス

本製品には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、NetWitnessコミュニティ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、本製品のユーザーは、これらの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。

ディストリビューション

本文書に記載される、RSA Security LLCまたはその関連会社(「RSA」) のいかなるソフトウェアの使用、複製、配布にも、適切なソフトウェア ライセンスが必要です。

RSA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。この情報は予告なく変更されることがあります。

この資料に記載される情報は、「現状有姿」の条件で提供されています。RSAは、この資料に記載される情報に関する、どのような内容についても表明保証条項を設けず、特に、商品性や特定の目的への適応性に対する黙示的保証はいたしません。

その他

この製品、このソフトウェア、関連ドキュメント、およびそのコンテンツは、このドキュメントの発行日時点で有効なNetWitnessの標準利用規約に従うものとし、これらの利用規約は https://www.netwitness.com/standard-form-agreements/ で確認できます。

2024年9月

目次

12.5.0.0リリースの新機能

NetWitness 12.5.0.0リリース ノートには、新機能、拡張機能、セキュリティ更新、アップグレード パス、修正された問題、既知の問題、サポート終了機能、ビルド番号、およびセルフヘルプ リソースが記載されています。

機能拡張

次のセクションでは、機能分野ごとに拡張内容を詳細に説明します。

- ダッシュボード
- Investigate
- Respond
- Insight
- User and Entity Behavior Analytics
- SASE機能
- Endpoint
- ポリシーベースのコンテンツ一元管理(CCM)
- Concentrator、Decoder、Log Collector、Archiverサービス
- ログ統合
- コンテキスト ハブ
- ライブクラウド サービス

このセクションで言及されているドキュメントを見つけるには、https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246を参照してください。

「製品ドキュメント」セクションには、このリリースのドキュメントへのリンクが記載されています。

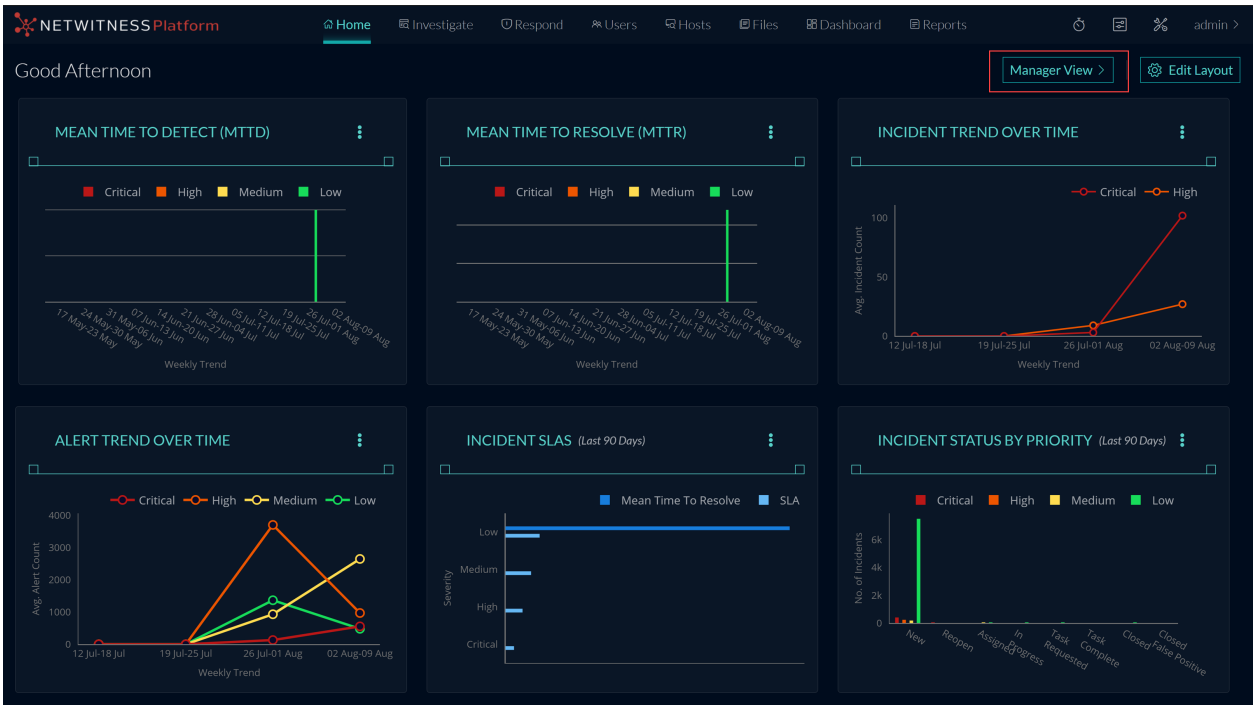
ダッシュボード

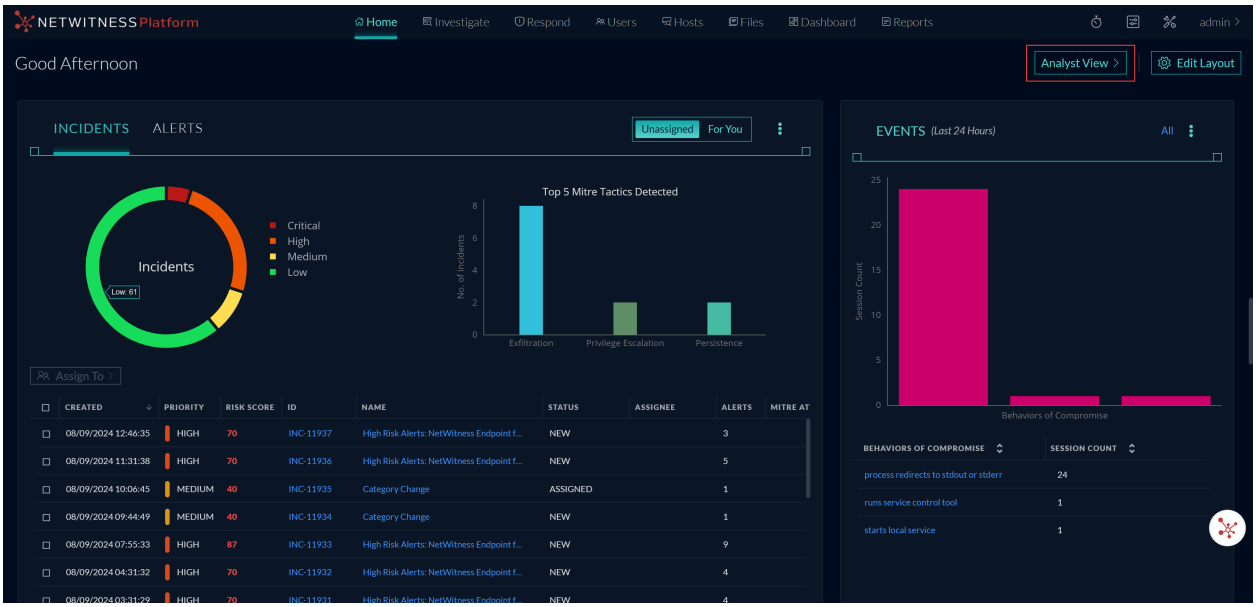
次のセクションでは、ダッシュボード コンポーネントの新しい機能強化について説明します。

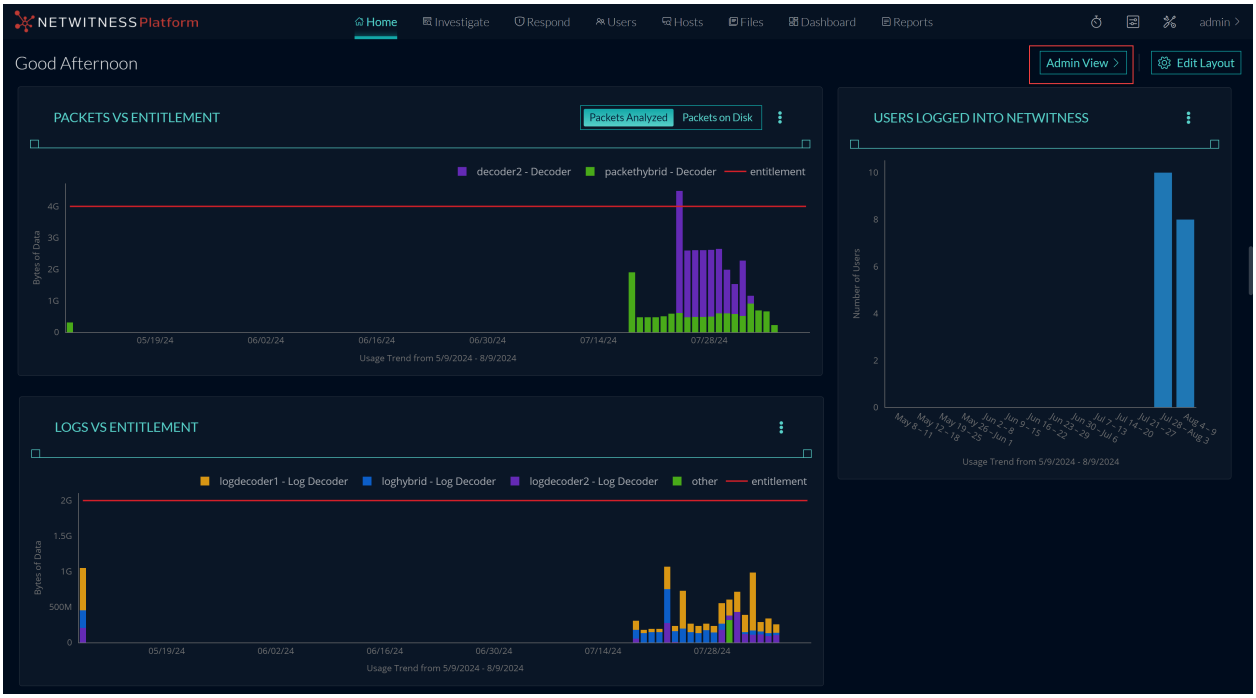
新しいホームページ

NetWitnessには新しい**ホーム** ページ メニューが導入されました。ホーム ページは [**管理者**]、 [**アナリスト**]、 [**マネージャー**]の各ビューで構成されています。各ホームページは複数のウィジェットで構成されています。管理者、アナリスト、SOCマネージャーは、特定のデータをグラフィック形式で表示するそれぞれのウィジェットにアクセスできます。データは、エンドポイント、ユーザー、資産、コンテンツ、インシデント、アラート、MITRE ATT&CK、保存期間など、さまざまなものに関連付けることができます。


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
Good Afternoon
Manager View
Edit Layout
INCIDENTS
9
NEW INCIDENTS
8
CLOSED INCIDENTS
0
ALERTS
40
MEAN TIME TO RESOLVE
0 Sec
MITRE ATT&CK® OVERVIEW
MEDIUM
CONTENT TYPE
EXPAND ALL SUB TECHNIQUES
Deployed
Partially Deployed
Not Deployed
Unavailable
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
5 of 10 techniques
2 of 8 techniques
7 of 10 techniques
7 of 14 techniques
15 of 20 techniques
13 of 14 techniques
25 of 43 techniques
7 of 17 techniques
16 of 32 techniques
3 of 9 techniques
9 of 17 techniques
7 of 17 techniques
6 of 9 techniq


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
Good Afternoon
Manager View
Edit Layout
MEAN TIME TO DETECT (MTTD)
Critical
High
Medium
Low
Weekly Trend
MEAN TIME TO RESOLVE (MTTR)
Critical
High
Medium
Low
Weekly Trend
INCIDENT TREND OVER TIME
Critical
High
Avg. Incident Count
100
50
0
12 Jul-18 Jul
19 Jul-25 Jul
26 Jul-01 Aug
02 Aug-09 Aug
Weekly Trend
ALERT TREND OVER TIME
Critical
High
Medium
Low
Avg. Alert Count
4000
3000
2000
1000
0
12 Jul-18 Jul
19 Jul-25 Jul
26 Jul-01 Aug
02 Aug-09 Aug
Weekly Trend
INCIDENT SLAS (Last 90 Days)
Mean Time To Resolve
SLA
Severity
Low
Medium
High
Critical
INCIDENT STATUS BY PRIORITY (Last 90 Days)
Critical
High
Medium
Low
No. of Incidents
6k
4k
2k
0
New
Reopen
Assigned
In Progress
Task Requested
Task Complete
Closed
Closed False Positive





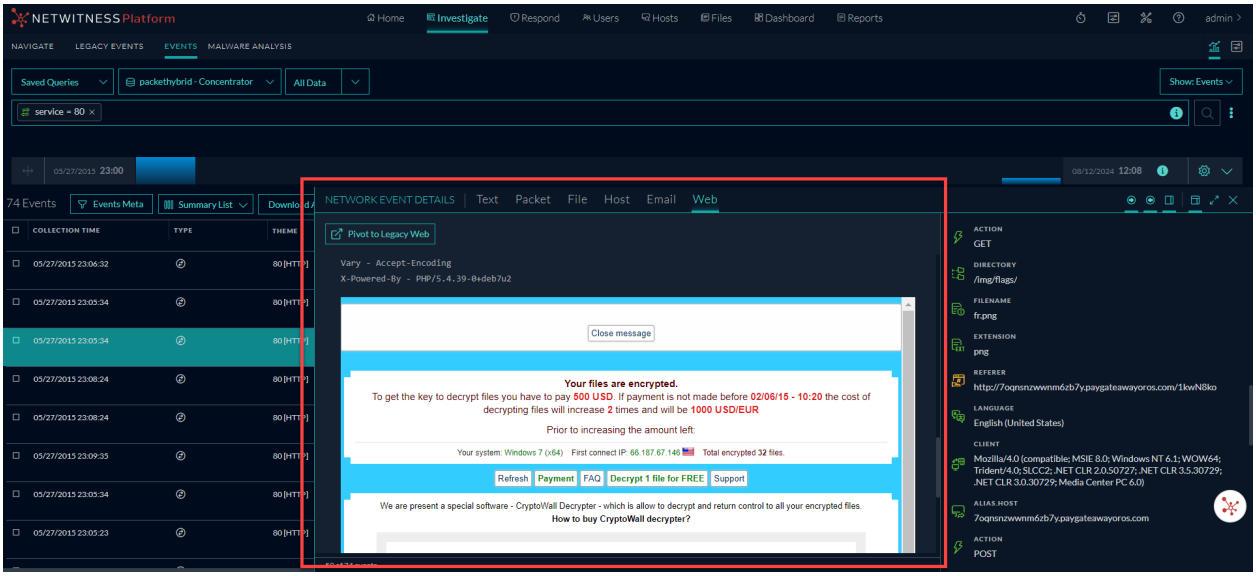
詳細については、『NetWitness 12.5入門ガイド』の「**Manage Home Widgets**」トピックを参照してください。

Investigate

次のセクションでは、Investigateコンポーネントの新しい拡張機能について説明します。

イベントビューからのWeb再構築

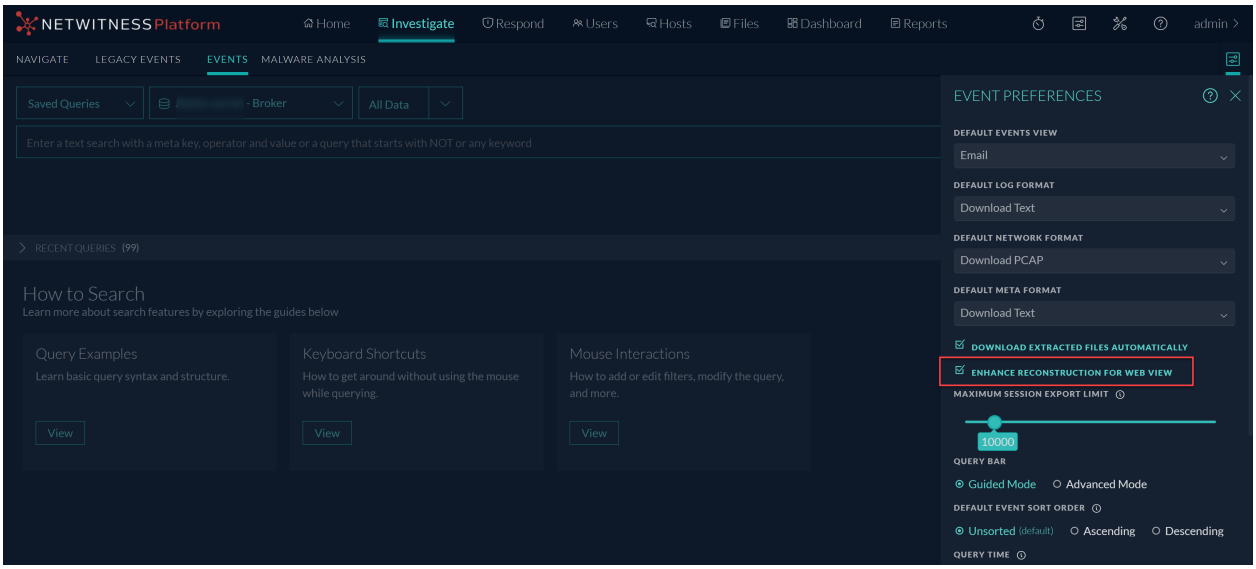
ユーザーが特定のイベントに関連するWebページにアクセスした場合、アナリストは［**イベント**］＞［**Web再構築**］ビューから対象イベントのWebビューを安全に再構築できます。NetWitnessは、パケット内で利用可能なデータを使用してWebページを表示し、それをイメージやCSSスタイルにできるだけ正確に関連付けることで、同じWebページを再構築できます。このWeb再構築プロセスにより、アナリストは実行されたWebアクティビティに関する貴重な洞察を得ることができ、効果的な分析と調査が容易になります。



詳細については、『NetWitness Investigate 12.5ユーザー ガイド.』の「**［イベント］ビューでのイベント詳細の調査**」トピックで「**Web再構築**」セクションを参照してください。

Webビューでのイベントの再構築の改善

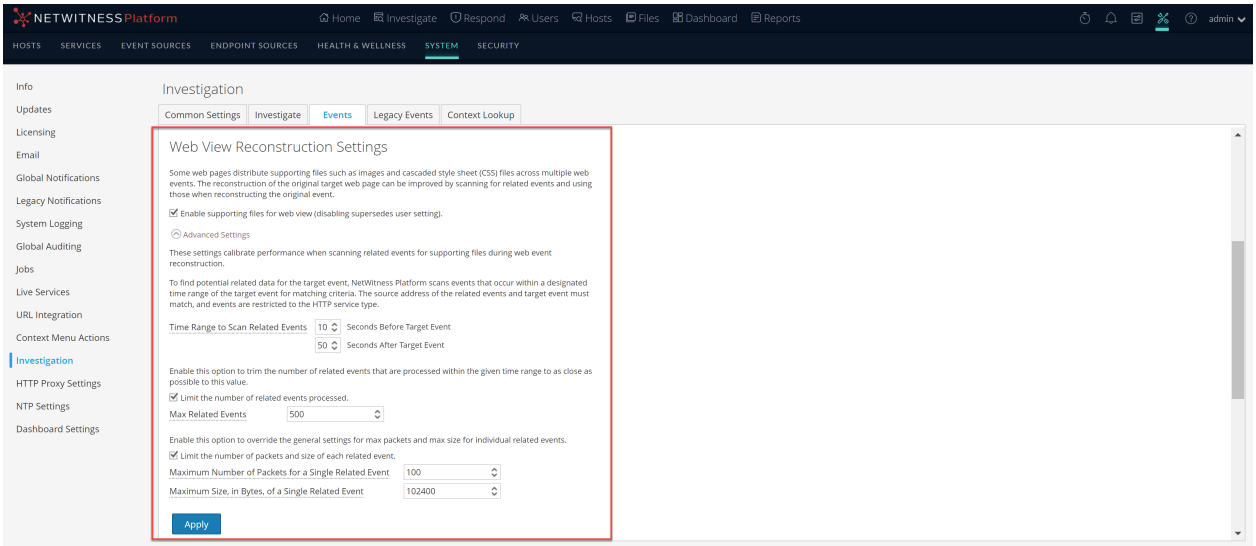
新しいユーザー設定である［**Webビューの再構築の強化**］が、［**Investigate**］＞［**イベント**］ビューの［**イベント設定**］パネルに追加されました。この設定は、すべてのユーザーに対してデフォルトで有効になっています。このオプションは、CSS、画像、リンクを使用してビューを効果的にフォーマットすることにより、イベントを再構築するWebサイトの再構築を改善し、アナリストが再構築するイベントのコンテキストと詳細をよりよく理解できるようにします。この機能強化により、アナリストはより情報に基づいた正確な分析を実施し、適切なアクションを実行できるようになります。



詳細については、『*NetWitness Investigateユーザー ガイド*』のトピック「**［イベント］ビューのユーザー環境設定の設定**」を参照してください。

システムビューからのWebビュー再構築設定の導入

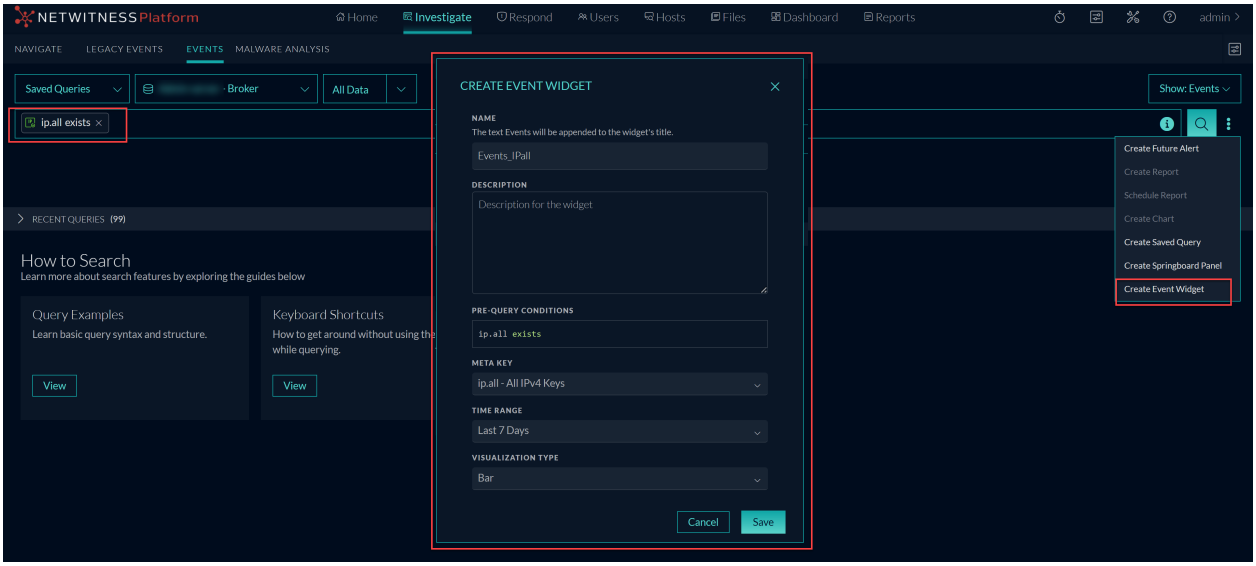
NetWitnessでは、［**管理**］>［**システム**］>［**調査**］ビューの新しい［**Webビューの再構築設定**］が導入されています。**[イベント]** タブのこの設定により、管理者は同じサポート ファイルを使用して関連イベントをスキャンおよび再構築することで、Webビューの再構築を強化できます。複数のイベントにまたがるWebビューを再構築する場合、システムは関連する画像やCSSファイルを含む関連イベントを含めることで、ターゲット イベントの再構築を改善できます。ソース アドレスがターゲット イベントと同じで、ターゲット イベントの前後の指定された時間内のタイム スタンプを持つHTTPサービス タイプのイベントのみがスキャンされます。管理者はスキャンする関連イベントの最大数を設定することもでき、これによりWebビューの再構築における柔軟性と精度が向上します。 ［詳細設定］オプションにより、このセクションで構成可能なすべての設定が表示されます。



詳細については、『システム構成ガイド』の「**調査構成］パネル**」トピックで「**Webビューの再構築の設定**」セクションを参照してください。

クエリからカスタムイベント ウィジェットを作 成する

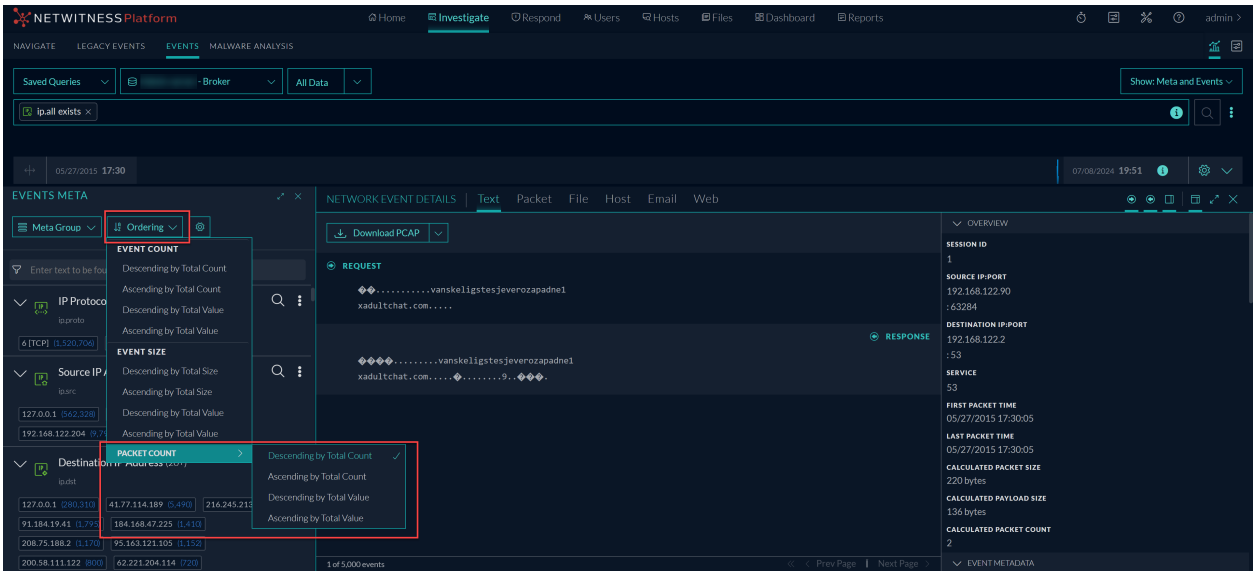
調 査 中 に、管 理 者 とアナリストは、**「調 査 」**>**「イベント」**ビューからイベント ウィジェットを作 成 できるようになりました。ユーザーはクエリ検 索 バーに任 意 の数 のフィルターを追 加 し、これらの検 索 をイベント ウィジェットに変 換 して、検 出 と監 視 を強 化 できます。新 しく作 成 されたウィジェットは、ホームページ ライブラリの下 に簡 単 にアクセスできるように保 存 されます。ユーザーは、ホームページのダッシュボード レイアウト ビュー (**管 理 者** 、**アナリスト** 、または **マネージャー**) にイベント ウィジェットを追 加 し、ニーズに合わせて構 成 をカスタマイズできます。この機 能 により、イベントの監 視 と分 析 が強 化 され、ユーザーは関 連 性 のある重 要 なイベントをリアルタイムで追 跡 および監 視 できるようになります。



詳 細 については、『NetWitness Investigate 12.5ユーザー ガイド』のトピック「 **調 査**]**ビューからイベント ウィジェットを作 成 する**」を参 照 してください。

メタキーの結 果 をパケット数 で並 べ替 える

アナリストは、**調 査** > **イベント** ページで、各 メタキーの結 果 をセッション内 のパケット数 で並 べ替 えることができるようになりました。結 果 を値 または合 計 の昇 順 または降 順 に並 べ替 えることができます。メタキーの結 果 をパケット数 で並 べ替 えると、ユーザー環 境 で発 生 した最 も頻 度 の高 いメタ値 や最 も頻 度 の低 いメタ値 を簡 単 に見 つけることができ、さらに調 査 や分 析 に使 用 できます。



詳細については、『NetWitness Investigate 12.5ユーザー ガイド』の「**[イベント]ビューでのメタデータのドリルダウン**」トピックで「**メタ値の並べ替え方法を設定する**」セクションを参照してください。

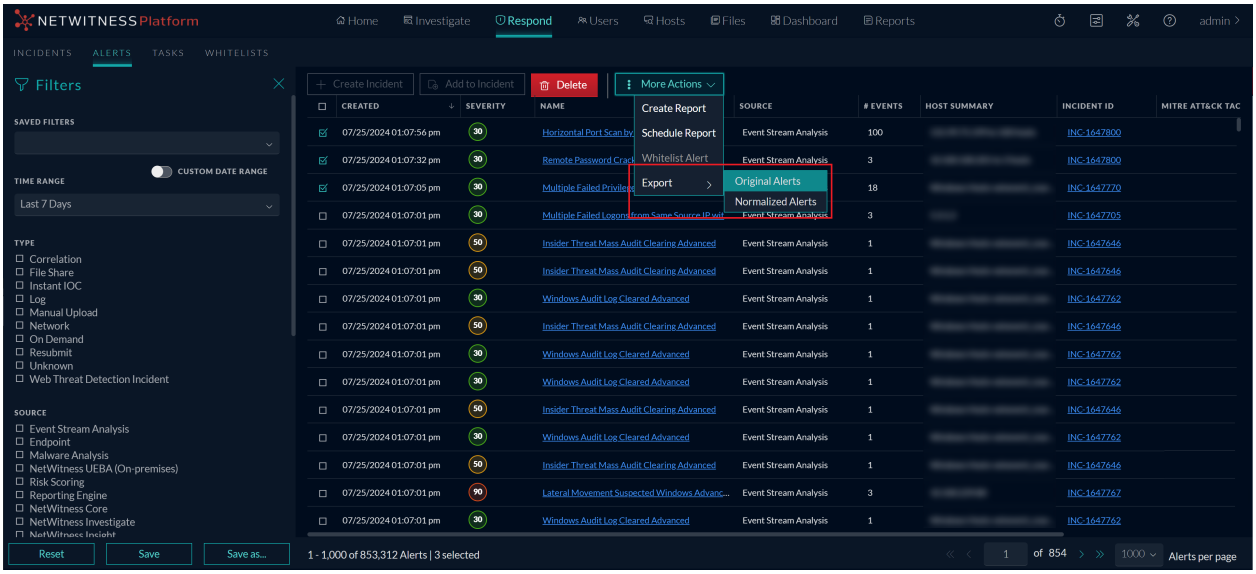
Respond

次のセクションでは、Respondコンポーネントの新しい機能強化について説明します。

アラートビューの強化

[Respond] > **[アラート]** > アラートの選択 > **[その他のアクション]**の**[エクスポート]**オプションを使用すると、元のアラートと正規化されたアラートをJSON形式のイベントとともにエクスポートしてダウンロードできます。NetWitness Platformでは、オフライン調査のために一度に最大 **1000** のアラートをエクスポートできます。

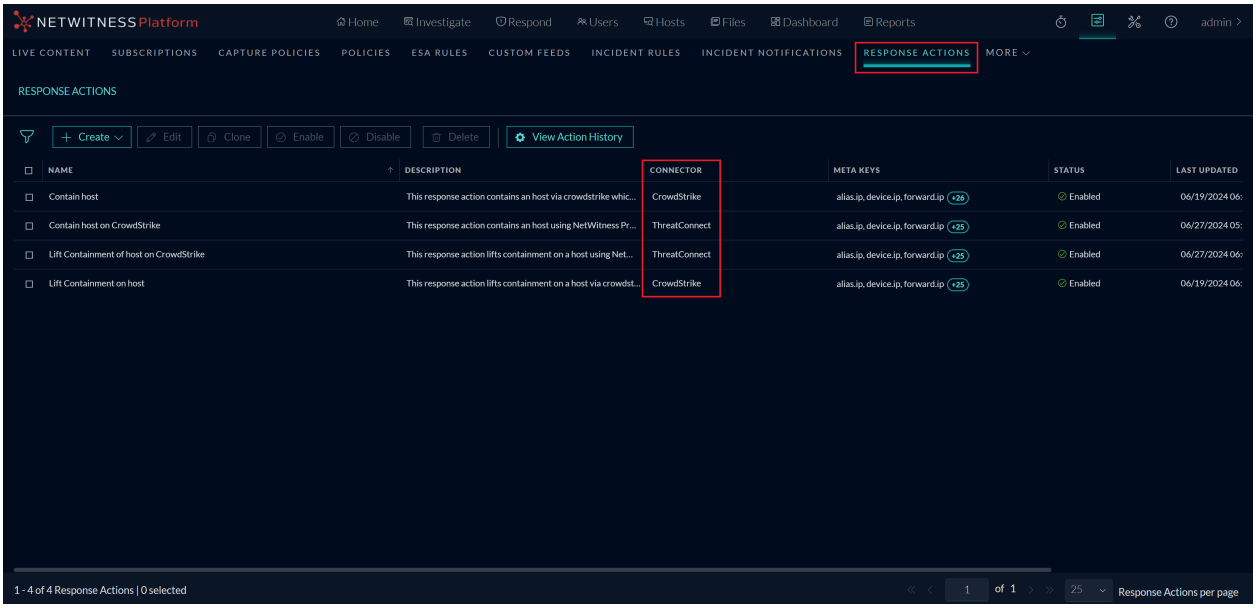
詳細については、『NetWitness Respond 12.5ユーザー ガイド』の「**アラート データのエクスポート**」を参照してください。



OOTB応答アクション

対応アクション サービスの一部として、すぐに使用できる(OOTB)アクションが導入されました。CrowdStrikeおよびNetWitness Orchestratorを通じて統合されたCrowdStrikeでは、OOTBアクション「ホストの封じ込め」と「ホストの封じ込め解除」が有効になっています。この機能強化により、アナリストはインシデントを確認した後、手動で対応アクションを実行したり、トリガーされたインシデントの一部として自動的に対応アクションを実行したりできるようになります。CrowdStrikeによるレスポンス アクションは、直接またはNetWitness Orchestratorを通じて利用できます。

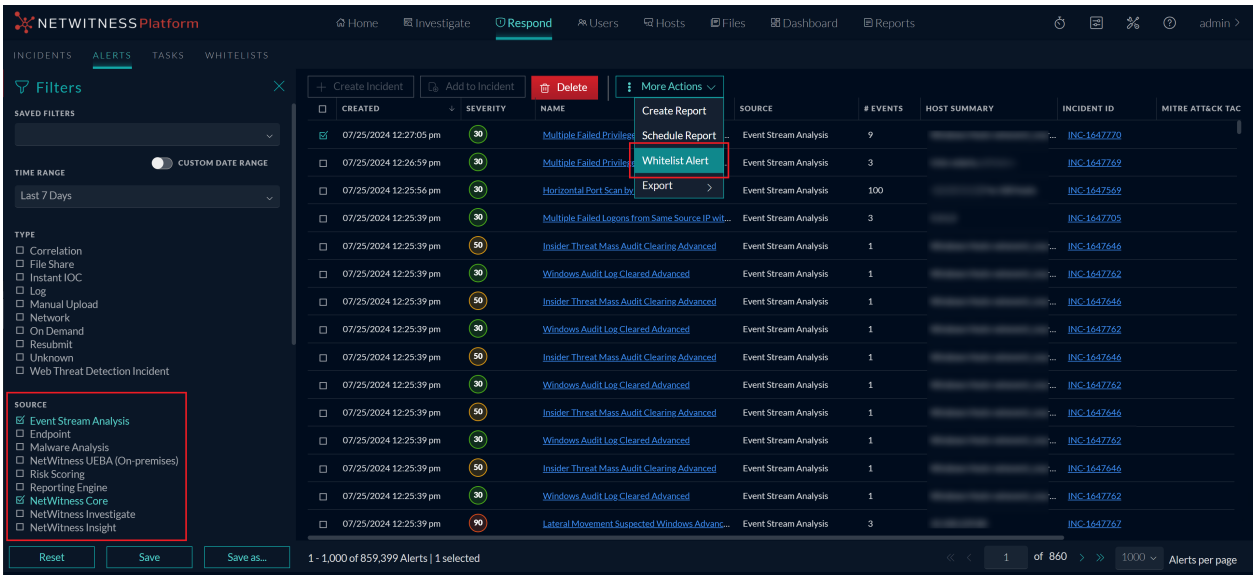
詳細については、『NetWitness 12.5対応アクション構成ガイド』の「**対応アクション**」を参照してください。



ホワイトリストの強化

ホワイトリスト機能が強化され、イベント ストリーム分析およびNetWitness Coreサービスのアラートが含まれるようになりました。これらのサービスに対して、不要で繰り返し発生する、疑わしくないアラートをホワイトリストに登録できるようになりました。これにより、特定のエンティティを選択し、ホワイトリスト条件を設定して、それらのエンティティに対する不要なアラートを防ぐことができます。

詳細については、『NetWitness Respond 12.5ユーザー ガイド』の「**ホワイトリスト リスト ビュー**」を参照してください。

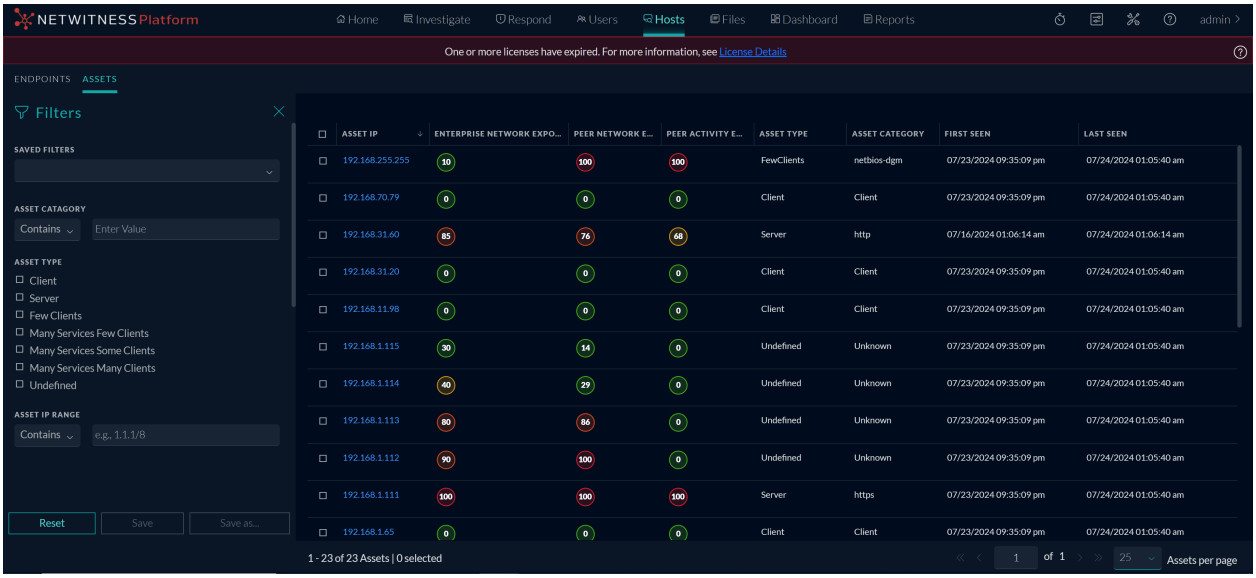


Insight

次のセクションでは、Insightコンポーネントの新しい機能強化について説明します。

ネットワーク資産の検出と調査のための新しい資産ビュー

NetWitnessでは、［**ホスト**］>［**資産**］メニュー内に新しい資産ビューが導入されています。このビューでは、環境内で検出されたすべてのネットワーク資産が、資産IP、資産タイプ、資産カテゴリー、エンタープライズ ネットワークへの公開、ピア ネットワークへの公開、ピア アクティビティの露出度、初回検出、最終検出などの関連する詳細情報とともに一元的に表示されます。フィルターを使用して、さまざまな基準で資産を絞り込むことができます。このビューにより、アナリストは異常な動作をしている資産や見慣れない資産を簡単に識別して優先順位を付けることができ、潜在的なセキュリティ リスクを緩和するためのアクションを速やかに実行できるようになります。

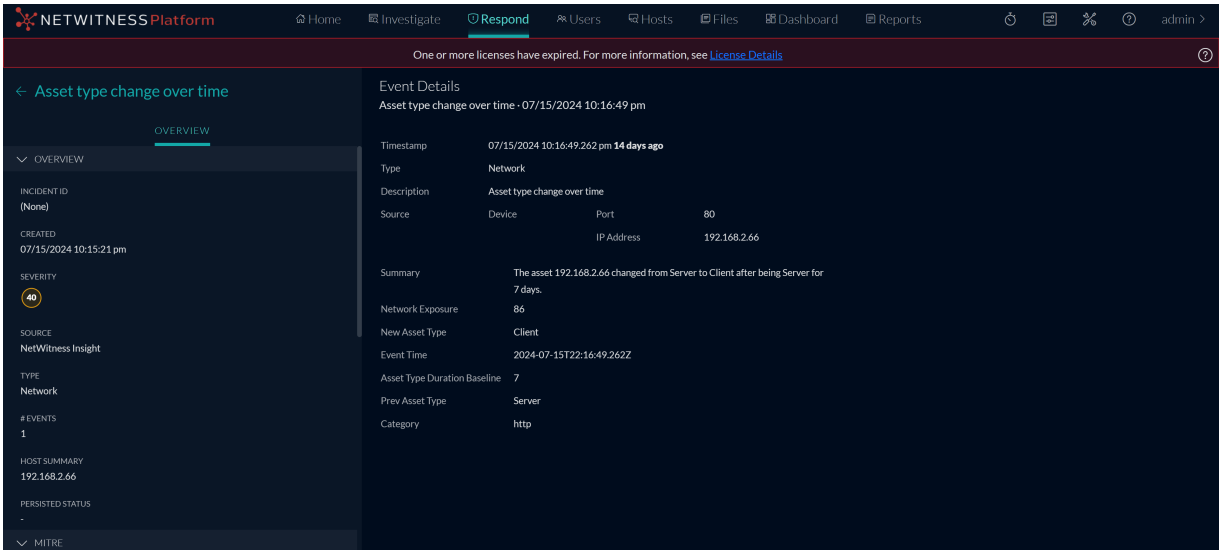


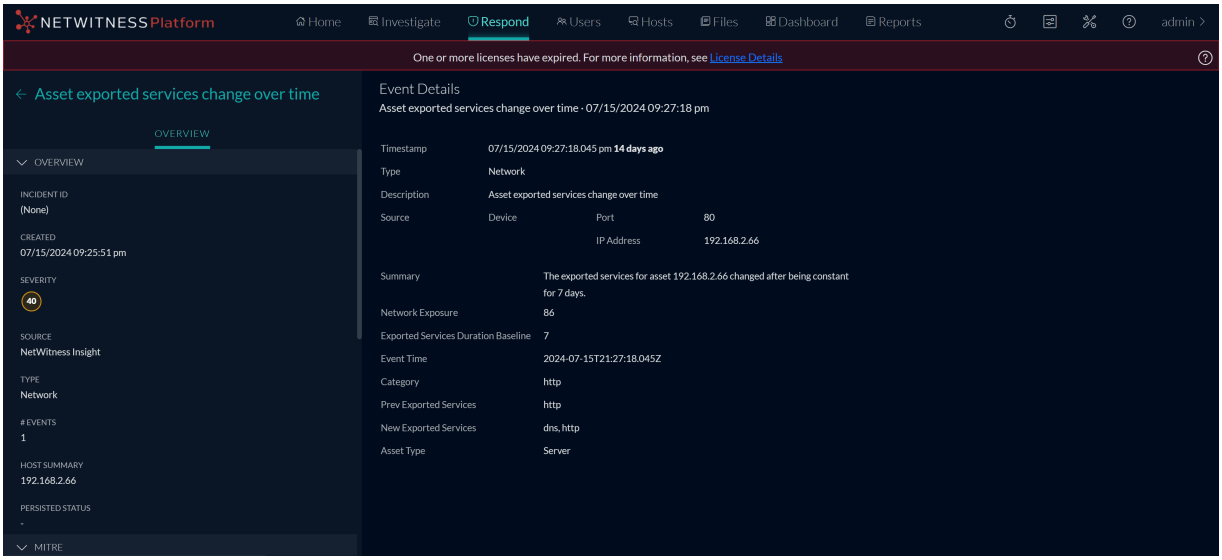
ネットワーク資産に関する新しいインサイトアラート

NetWitnessでは、ネットワーク資産の変化を監視して対応できるように、2つの新しいInsightアラートが導入されています。これらのアラートは、**「対応」**>**「アラート」**ビューで利用でき、資産タイプと各資産のエクスポートされたサービスに基づいています。

- **資産タイプの時間経過による変化**:このアラートは、同じタイプが7日間連続して観察された後で、資産のタイプが変更(クライアントからサーバーへの変更など)されたときに生成されます。
- **アセットエクスポートサービスは時間の経過とともに変化します**:このアラートは、資産カテゴリーが変更されていない場合でも、7日間連続して同じ数のサービスが観測された後で、資産によってエクスポートされたサービスの数が変化すると生成されます。

  これらのアラートは、アナリストが環境内の潜在的な異常や脅威を特定して調査するのに役立ちます。





詳細については、『*NetWitnessドキュメント ポータル*』の「**NetWitness Insightセクション**を参照してください。

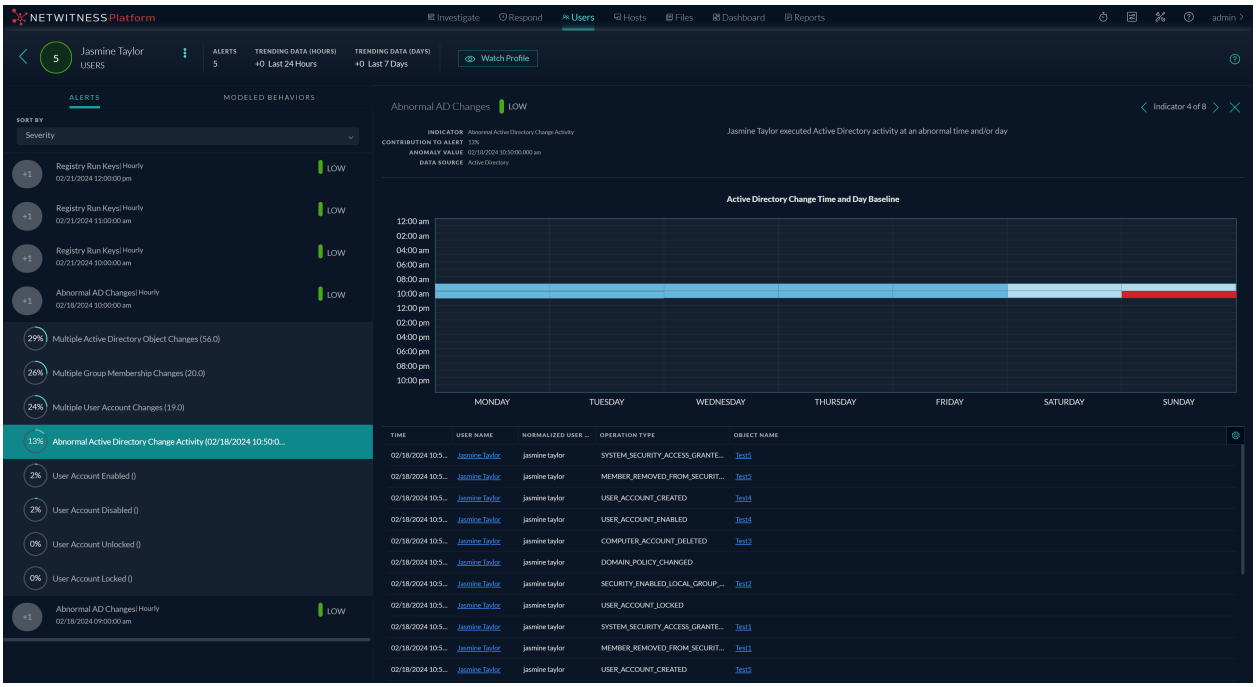
User and Entity Behavior Analytics

次のセクションでは、UEBAコンポーネントの新しい拡張機能について説明します。

曜日を使用したUEBA異常検出

NetWitness UEBAでは、曜日機能を導入することで異常検出機能が強化されています。この機能により、侵害されたアカウントや内部脅威を示唆する非標準のアクセス パターンを検出できるようになります。監視対象のユーザーまたはネットワーク エンティティのアクティビティが特定の曜日に通常のベースラインと異なる場合、UEBAはそれを異常としてフラグ付けし、非標準アクセスまたは非標準アクティビティのアラートを生成し、アナリストに通知してさらに調査と検証を行います。非標準アクセスおよび非標準アクティビティについて追跡される監視対象アクティビティの詳細については、『NetWitness UEBAユーザー ガイド』のトピック「**アラート タイプ**」を参照してください。

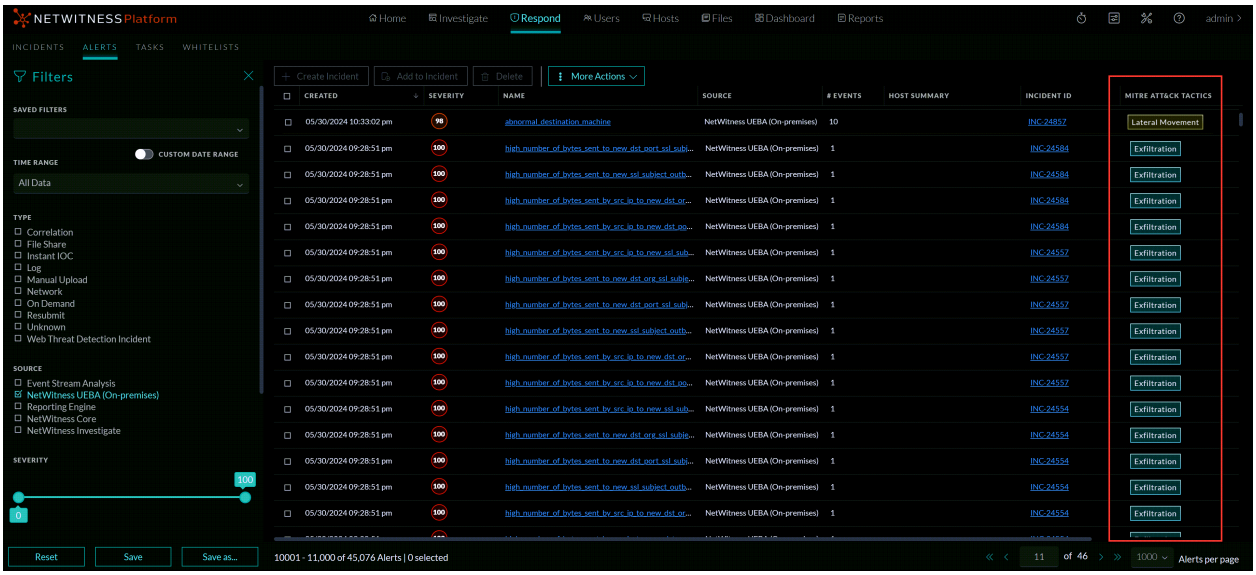
たとえば、ユーザーが通常と異なる曜日にActive Directoryにアクセスしたとします。ユーザーは通常、月曜日から金曜日まで働いていますが、日曜日にログインしてActive Directoryを変更しました。この動作は曜日ベースの強化機能に基づき、NetWitness UEBAによって異常として検出されました。この曜日にこのユーザーがADに変更を加えるのは通常ではないため、アナリストが調査を行うためのアラートが生成されます。



UEBA向けMITRE ATT&CKマッピング

NetWitnessでは、UEBAアラートおよびインシデント用のMITRE ATT&CKフレームワーク マッピングが統合されるようになりました。このマッピングにより、アナリストは、検出されたアクティビティを既知の動作と関連付けることで、攻撃者の潜在的な戦術、手法、サブテクニックを理解することができます。UEBAのアラートやインシデントを調査する際、アナリストは［**対応**］ビューでマッピングされた戦術や手法のリストを確認でき、さらに詳細なコンテキストや関連情報を提供する専用の［**ATT&CK Explorer**］パネルも利用できます。これにより、ATT&CK情報を調べるためにMITREのWebサイトにアクセスする必要がなくなります。この機能強化により、脅威の重大度と性質に関する貴重な洞察が得られ、より迅速かつ情報に基づいた対応決定が可能になります。

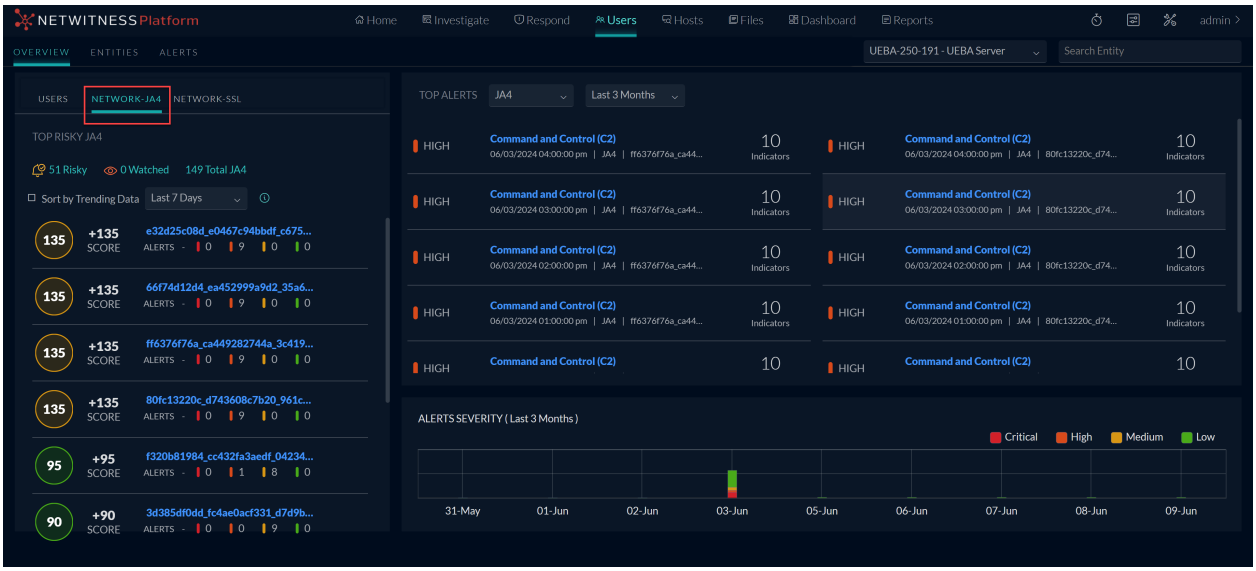
たとえば、UEBAアラートは、ユーザー アカウントからの疑わしいリモート アクセス動作を識別します。この動作は、MITRE ATT&CKの戦術である **ラテラルムーブメント** と **リモート サービス**を使用した手法と一致しており、アナリストにデータ取得の試みの可能性を調査し、必要な措置を講じるよう警告します。



UEBAでのMitre ATT&CKフレームワークの使用に関する詳細については、『NetWitness 12.5対応ガイド』のトピック「**MITRE ATT&CK®フレームワークの使用**」を参照してください。

クライアント識別と脅威検出を向上させるため、UEBAにJA4サポートを追加

NetWitnessではJA4フィンガープリントのサポートが追加され、バージョン12.5以降ではUEBAのデフォルトになりました。この変更は、JA4が最も信頼性が高く、改善されたクライアント端末識別方法として認識されているため実施されました。JA4はTLSクライアントHelloパケットを活用して、アプリケーション固有のトラフィック パターンを識別し、各アプリケーションに固有のフィンガープリントを作成します。これにより、最新のブラウザの固有のフィンガープリントの総数が削減されます。その結果、単一のクライアントには複数のJA4フィンガープリントではなく1つのJA4フィンガープリントのみが存在することになり、追跡と監視が容易になります。JA4を使用したUEBAのこの改良により、悪意のあるアプリケーションのフィンガープリントを特定できるようになり、暗号化されたトラフィック内に隠れた脅威をアナリストが事前に特定して緩和することが可能になります。

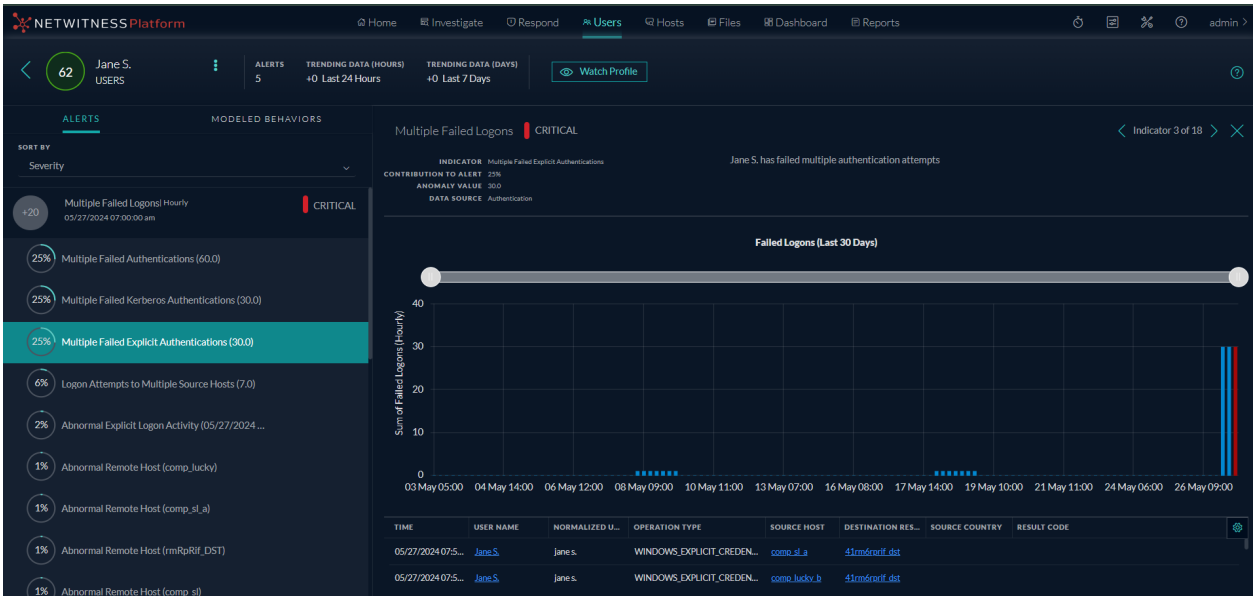


JA4サポートの詳細については、NetWitness UEBAユーザー ガイド 12.5 を参照してください。

Kerberosおよび明示的なログオン アクティビティを検出するための強化されたUEBA

NetWitness UEBAは、**Kerberos** および **明示的** ログオン専用の2つの新しいインジケーターとモデル化された動作を導入することで、ログオン アクティビティの検出機能を強化しました。この機能強化により、環境内のさまざまなログオン イベントをより正確に区別できるようになり、Kerberosおよび明示的なログオン アクティビティに関連する誤検知や不整合が大幅に削減されます。これらのログオン タイプを分離することで、アナリストは異常なログオン動作をより効果的に識別し、潜在的な脅威から環境を保護することができます。これらの新しい指標によりログオン活動についての詳細なインサイトが得られ、アナリストは疑わしい動作や悪意のある動作を効果的に監視、調査できるようになります。

たとえば、**複数のログオン失敗** アラートは、**Kerberosと明示的なログオン**の両方のアクティビティで認証試行が複数回失敗し、異常なアクティビティが特定された場合にトリガーされる可能性があります。



詳細については、『NetWitness UEBA 12.5ユーザー ガイド』のトピック「**NetWitness UEBAのユース ケース**」で「**ログオン アクティビティ指標**」セクションを参照してください。

SASE機能

次のセクションでは、SASEの新しい拡張機能について説明します。

NetWitness SASEとNetskopeの統合 (プライベート プレビュー モード)

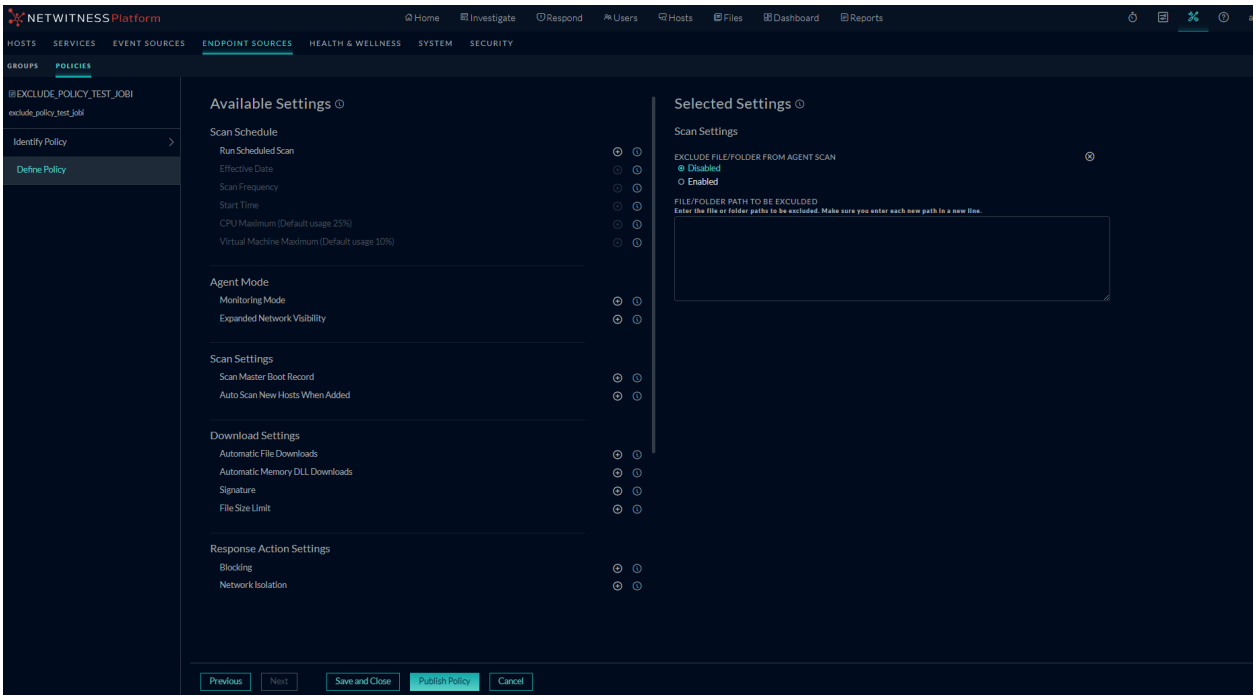
NetWitnessとNetskope SASEの統合を導入し、完全なネットワークとログの可視性を提供します。この技術面のカスタム統合により、NetWitnessユーザーは、オンプレミス、ハイブリッド、クラウド導入環境にわたるリモートおよび分散ネットワーク内のデバイスとサービスの動作や、それらの間の通信についてインサイトを得ることができます。NetWitnessとNetskope SASEの統合により、お客様はSASEの柔軟性と固有のセキュリティ上の利点を活用しながら、脅威の検出と対応の完全な可視性を維持できます。12.5リリースでは、NetWitness SASEとNetskopeの統合はプライベート プレビュー モードです。

Endpoint

次のセクションでは、エンドポイントコンポーネントの新しい機能強化について説明します。

エージェント フル システム スキャンから特定のファイルとフォルダの除外

NetWitness Endpoint Agentのシステム全体のスキャンから特定のファイルとフォルダを除外するようにNetWitness Platformを構成できます。ファイルまたはフォルダを除外すると、NetWitness Endpoint Agentはセキュリティ リスクをスキャンするときにそれらを無視します。サイズの大きいファイルやフォルダを除外すると、Endpointエージェントのスキャン時間が短縮されることがあります。NetWitness Endpointエージェント スキャンからファイルまたはフォルダを除外すると、ネットワーク上のホストの保護レベルが低下します。この機能は、特別なニーズがあり、アイテムが感染していないと確信できる場合にのみ使用してください。完全システム スキャンからのみファイルとフォルダを除外できます。



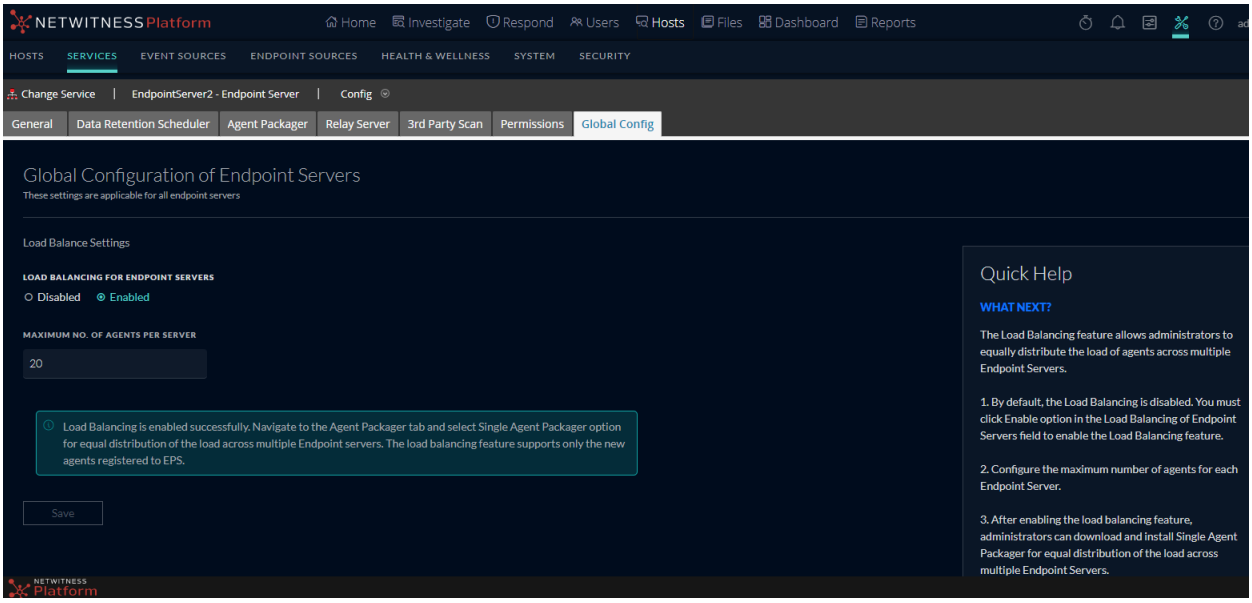
NetWitnessエージェントのフル システム スキャンからファイルとフォルダを除外する方法の詳細については、『NetWitness Endpoint構成ガイド』を参照してください。

パフォーマンスの最適化:エンドポイント サーバーの負荷分散機能

新しく導入された負荷分散機能により、管理者は環境内のエンドポイント サーバー全体にエージェントの負荷を均等に分散できます。

組織が大きくなると、展開用に新しいエージェントを追加する必要性が高まり、エンドポイント サーバー間でエージェントを配布することが困難になります。管理者は、エンドポイント サーバーごとに異なるパッケージャーをダウンロードし、ポリシーを使用して条件に基づいて負荷を分散する必要があります。負荷分散機能を使用すると、顧客はエージェント パッケージャーを1つダウンロードし、それをすべてのエンドポイント エージェントにプッシュするだけで済みます。定義された負荷とパラメーターに基づいて、エージェントはエンドポイント サーバーに均等に分散されます。

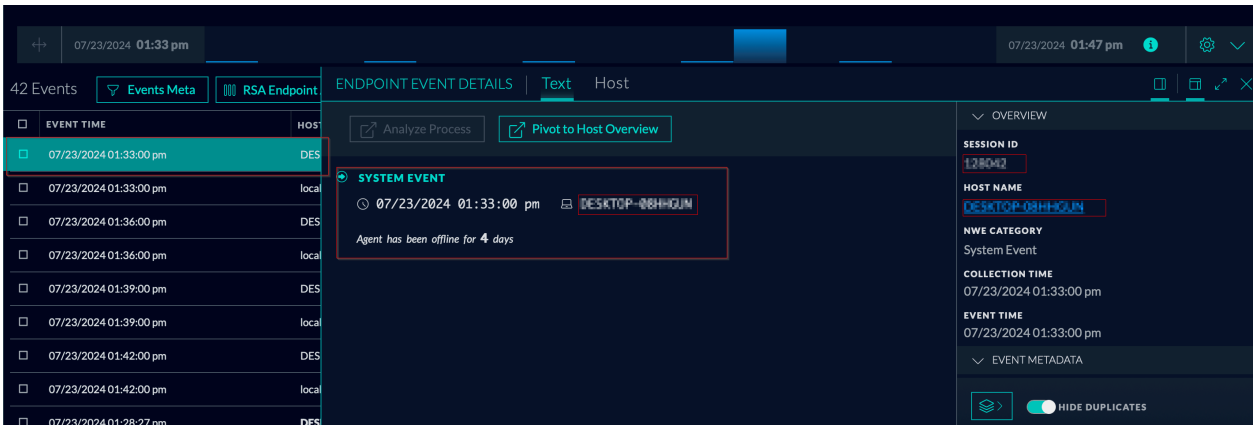
負荷分散を実装することで、組織は展開を効率的に拡張し、単一のエンドポイント サーバーに過負荷がかかるリスクを軽減し、ネットワーク全体で最適なパフォーマンスを維持できます。負荷分散機能を使用するには、負荷分散を有効にする必要があります。



ロード バランシングの詳細については、『*NetWitness Endpointユーザー ガイド*』のトピック「ロード バランシングについて」および「ロード バランシングを有効にする」を参照してください。

エンドポイント エージェントの最終確認状況を監視する機能

NetWitness Platformを使用すると、管理者とアナリストは、指定された日数にわたってレポートしていないエンドポイント エージェントの数の詳細を示すレポートを定期的に作成し、組織内のコンプライアンスとガバナンスを確保できます。エンドポイント エージェントが最後にアクティブになった時期を把握することで、エンドポイント デバイスの全体的なパフォーマンスに関する洞察が得られます。エンドポイント エージェントの最終確認状況を監視することは、組織内のセキュリティ、コンプライアンス、運用効率、および効果的なリソース管理を確保する上で不可欠です。



詳細については、『NetWitness Endpointユーザー ガイド』のトピック「エンドポイント エージェントの最終確認状況を監視する」を参照してください。

オペレーティング システムのサポートを拡大

管理者は、次のバージョンのWindowsオペレーティング システムにエンドポイント エージェントを展開するオプションがあります。

- **Windows 11 (バージョン23H2まで)**

詳細については、『NetWitness Endpointエージェント インストール ガイド』のトピック「**Endpointエージェントのインストールの概要**」を参照してください。

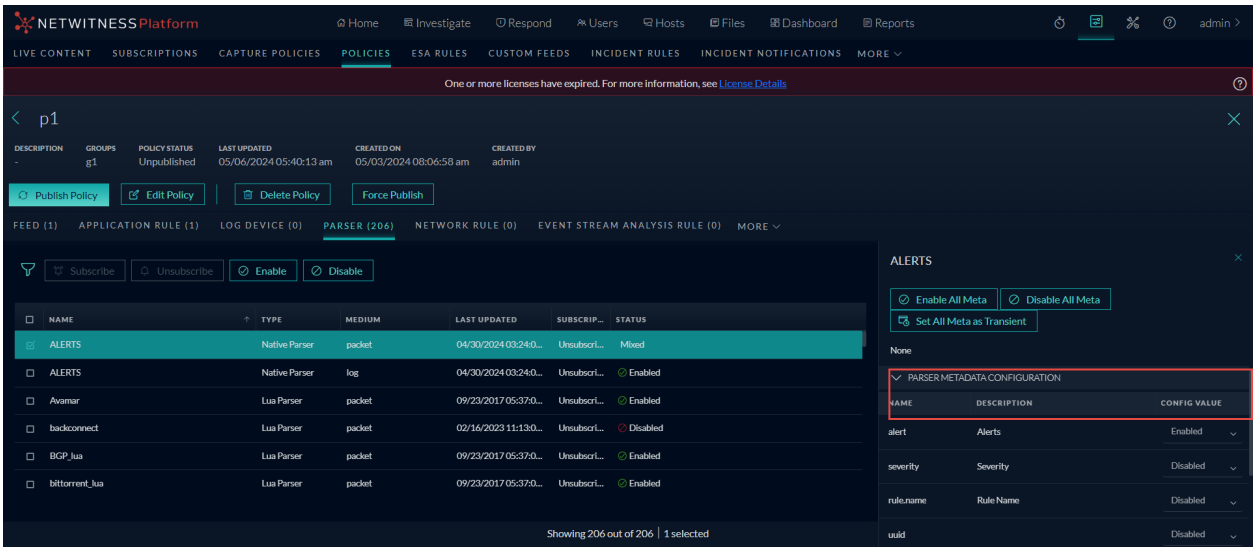
ポリシーベースのコンテンツ一元管理(CCM)

12.5.0.0バージョンでは、CCMに対して次の機能強化が行われます。

ネイティブパーサーのサポート

パーサーメタデータ構成の表示

ポリシーの詳細 > **パーサー**ビューが拡張され、右側のパネルに**パーサー メタデータ構成** が表示され、選択したパーサーのすべてのメタが表示されるようになりました。

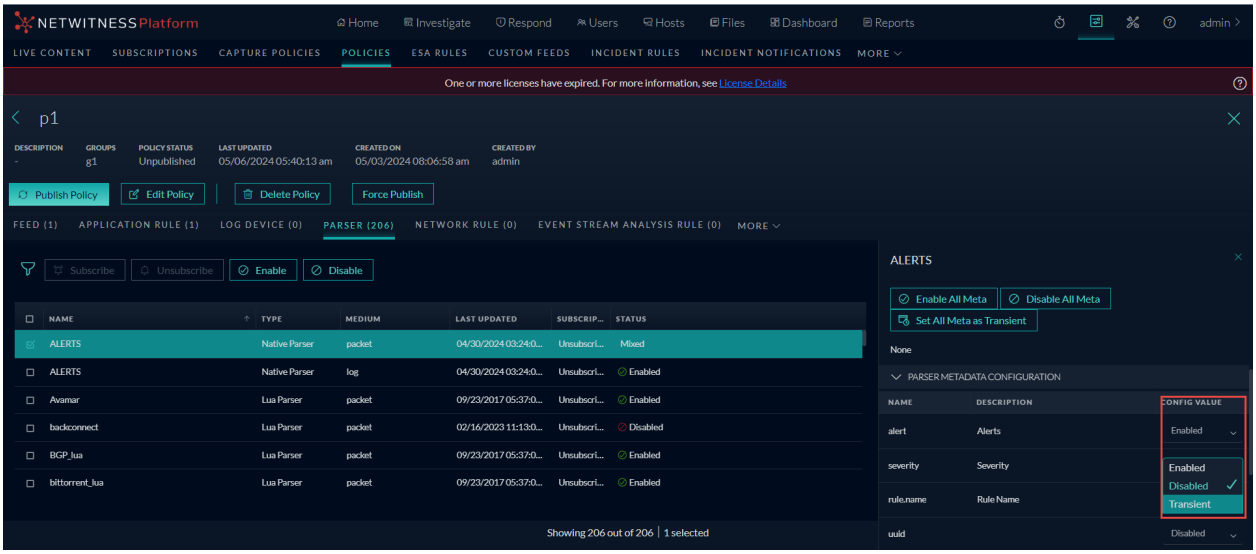


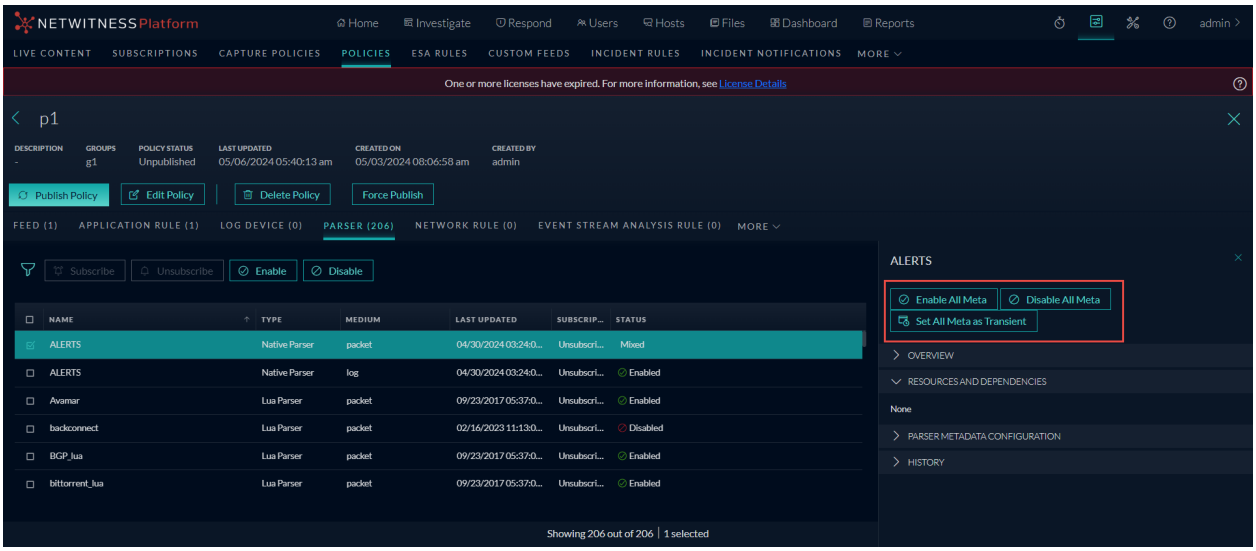
詳細については、『ポリシーベースのコンテンツー元管理ガイド』のトピック「**ポリシーの表示**」を参照してください。

パーサーメタの有効化または無効化

［**ポリシーの詳細**］> ［**パーサー**］ビューが強化され、特定のパーサー メタを有効または無効にできるようになり、ネイティブ パーサーを使用するかどうかを選択できるようになりました。次の操作を実行できます。

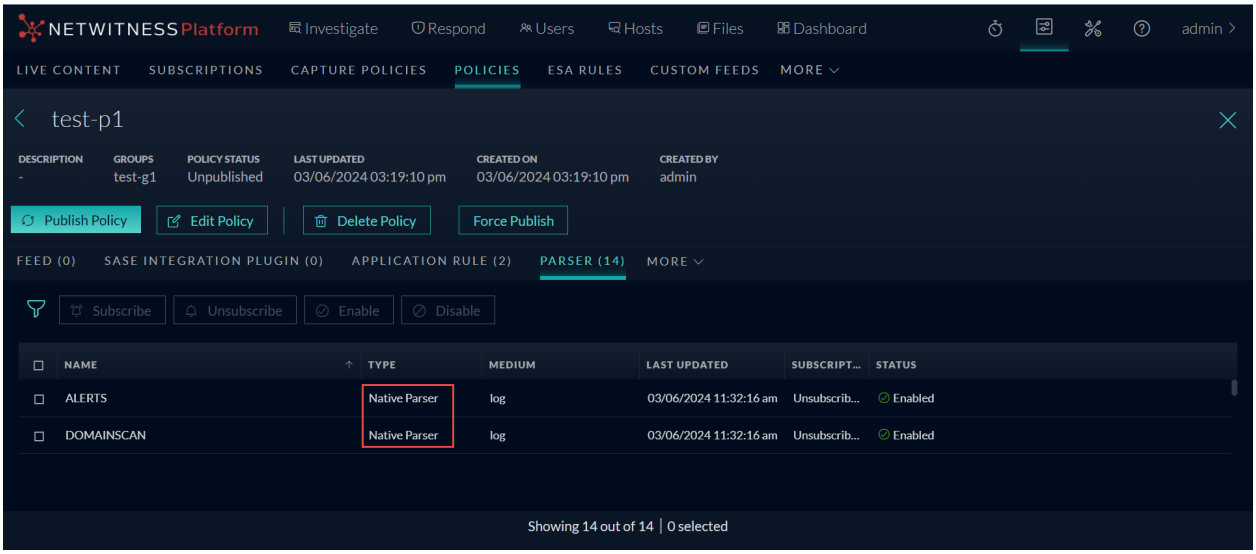
- すべてのメタを有効にする
- すべてのメタを無効にする
- すべてのメタを一時的にする
- 個別のメタを有効にする
- 個別のメタを無効にする
- 個々のメタを一時的にする





サービスに対して有効になっており、ポリシーに添付されているネイティブ パーサーを表示する

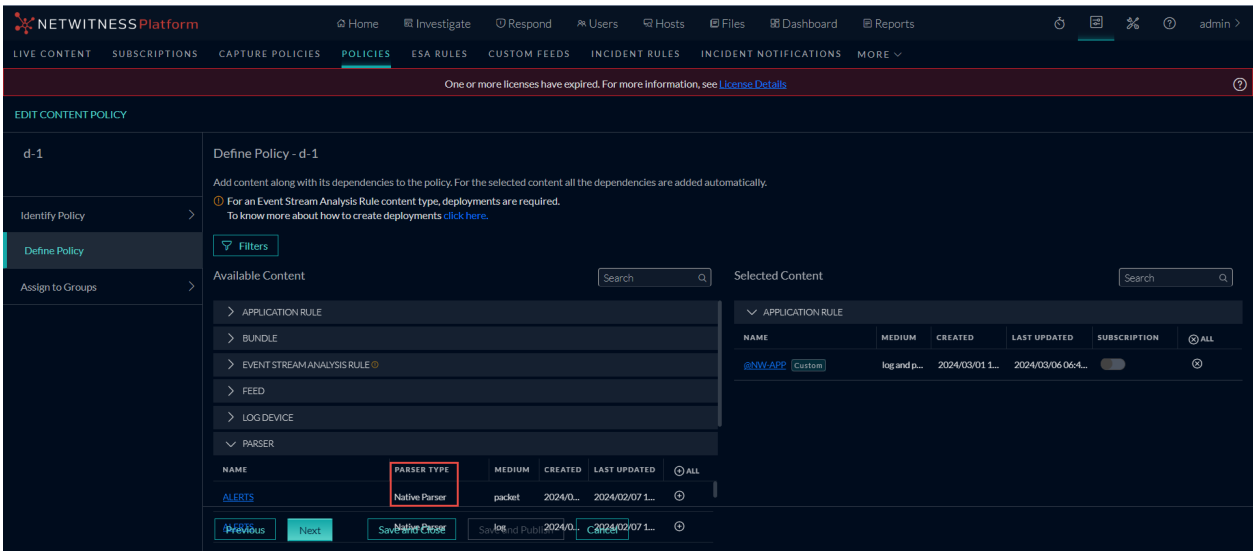
サービスに対して有効になっていてポリシーに添付されているネイティブ パーサーは、［**ポリシーの詳細**］ページに自動的に表示されるため、簡単に確認できます。



詳細については、『ポリシーベースのコンテンツー元管理ガイド』のトピック「**ポリシーの表示**」を参照してください。

ポリシーを作成する際にネイティブ パーサーとLUAパーサーを区別する

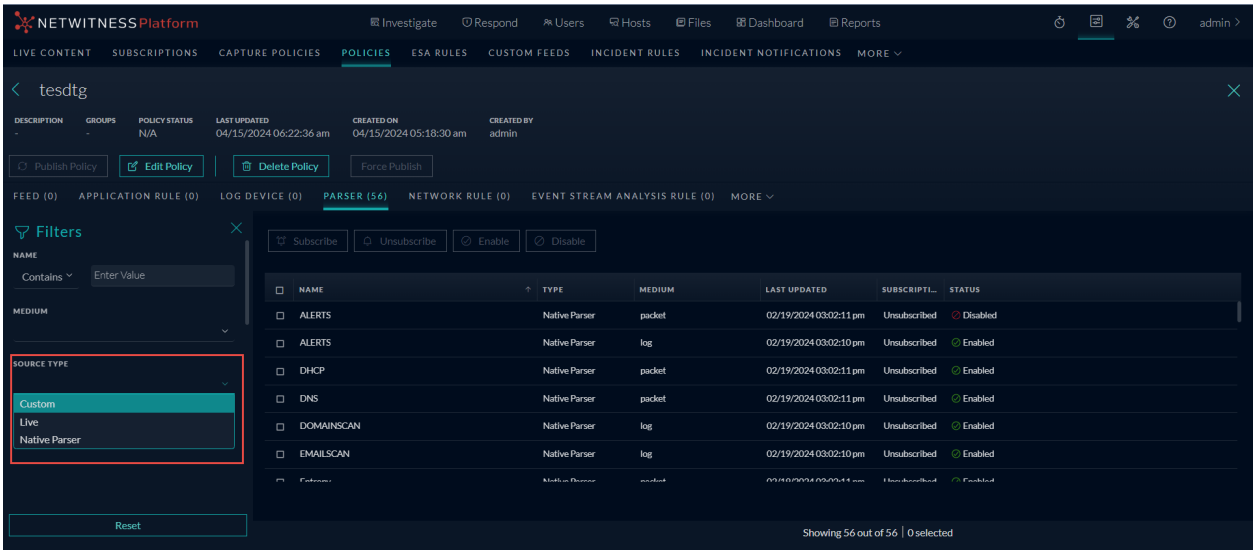
ポリシーを作成する際にネイティブ パーサーとLUAパーサーを区別できるように、［**ポリシーの作成**］または［**ポリシーの編集**］ページでネイティブ パーサーの識別子が作成されます。



詳細については、『ポリシーベースのコンテンツー元管理ガイド』のトピック「**ポリシーの作成と公開**」を参照してください。

ネイティブパーサーをフィルタリングする

［**ポリシーの作成**］、［**ポリシーの編集**］、および［**ポリシーの詳細**］ページでネイティブ パーサーをフィルター処理して、ポリシーに必要なネイティブ パーサーを簡単に選択または表示できます。これによりプロセスが効率化され、ポリシーの作成中や変更中にネイティブ パーサーを簡単に追加または削除できるようになります。



詳細については、『ポリシーベースのコンテンツー元管理ガイド』のトピック「**ポリシーの作成と公開**」を参照してください。

Concentrator、Decoder、Log Collector、Archiverサービス

12.5.0.0バージョンでは、Concentrator、Decoder、Log Collector、Archiverサービスに対して次の機能強化が加えられています。

JA4 TLSフィンガープリンティングの導入

JA4は、TLSハンドシェイク ネゴシエーション(Client Hello)を分析することでアプリケーション固有のトラフィック パターンを識別し、UEBAの脅威検出機能を強化します。

詳細については、『Decoder構成ガイド』のトピック「**UEBAのJA4エンティティのサポート**」を参照してください。

Logstashイベント ソース

MSSQL、IBMDB2、およびOracleデータベースからログを収集するためのNetWitness JDBC Logstash入力プラグイン サポートが導入されました。

詳細については、『ログ収集ガイド』のトピック「**NetWitnessでLogstashイベント ソースを構成する**」を参照してください。

拡張メタ

メタ データベースに保存できる値の長さを増やすことで、長い文字列の一致を必要とする特定のユース ケースの精度を高めるためのオプションの構成。

拡張メタは、256バイトを超える値をサポートするために特定のメタ キーを選択的に構成する方法を提供します。この機能により、以前は256バイトの制限によって切り捨てられていたメタ値の長さを最大4,096バイトまで拡張できるようになりました。

詳細については、『NetWitness 12.5拡張メタ ユーザー ガイド』に記載されている拡張メタのガイドラインを参照してください。

アプリケーション ルールの追跡

アプリケーション ルールが一致する頻度をカウントし、トラブルシューティングの目的でカウンターをリセットすることもできます。

詳細については、『12.5 APIガイド』を参照してください。

ログ統合

NetWitness Platformは、ログの収集と解析のために次のイベント ソースの統合をサポートしています。特に指定のない限り、これらのサービスはNetWitness Platform 12.2.0.0以降でサポートされます。

- Amazon AWS CloudWatch
- Okta Workforce Identity Cloud

パーサ サービスの統合の詳細については、『NetWitness Platform統合ガイド』を参照してください。

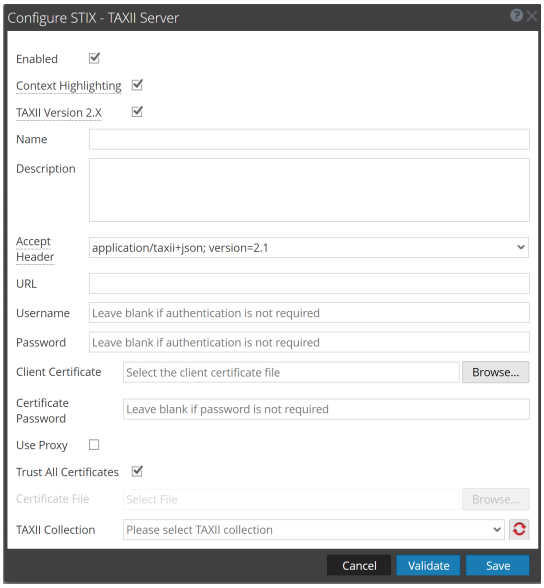
コンテキスト ハブ

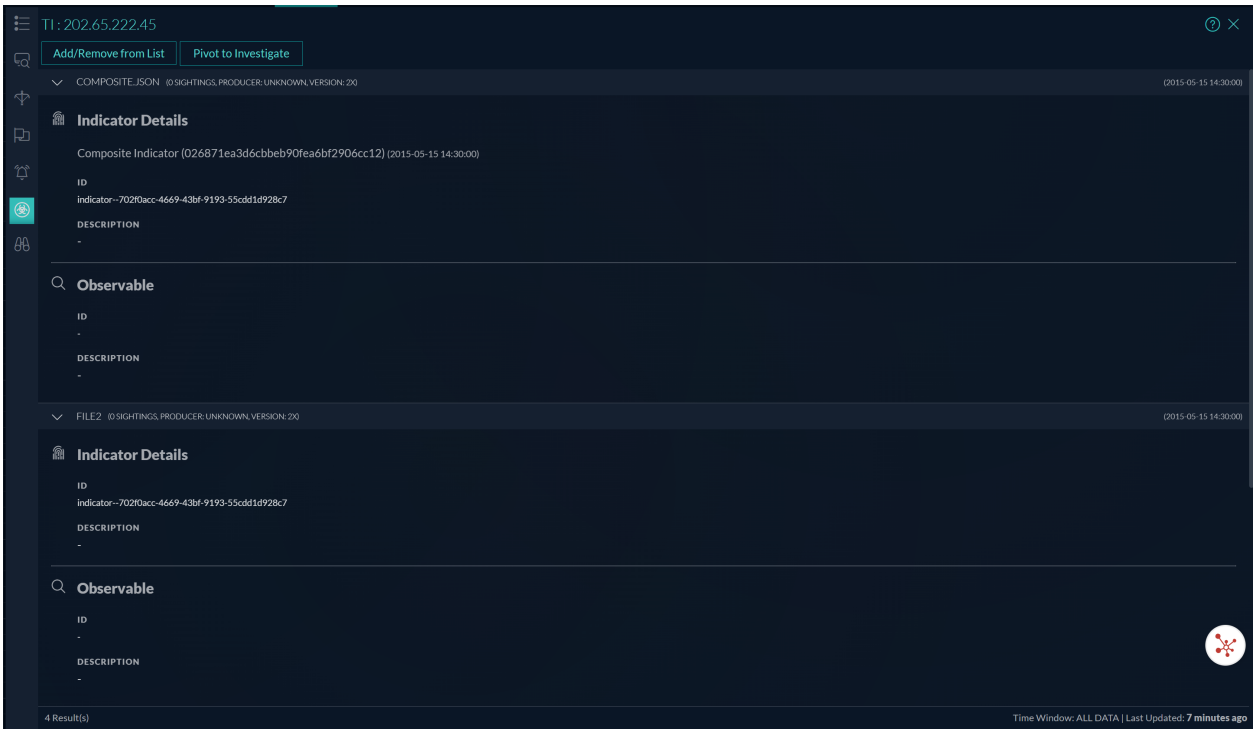
次のセクションでは、Context Hubコンポーネントの新しい機能強化について説明します。

STIX 2.x統合による脅威インテリジェンスの向上

NetWitnessは、バージョン2.0および2.1を含むSTIX 2.xフィードのサポートを統合することで、脅威検出およびセキュリティ監視機能を強化しました。管理者は、STIX 2.x (JSON形式) を使用して、ファイル、REST、およびTAXIIサーバーをContext Hubのデータ ソース インジケーターとして構成できるようになりました。この機能強化により、STIX 2.xデータ ソースを使用してカスタム フィードを作成できるようになります。NetWitnessプラットフォームは、バックグラウンドでデータを分析し、価値の高い脅威インテリジェンスを抽出して悪意のあるパターンを特定し、 **調査**]ページと **対応**]ページのコンテキスト ルックアップを通じて豊富なコンテキストを提供し、アナリストがより効果的に調査を実施できるようにします。

この強化により、多くの制約が解消され、より記述的で効果的な脅威インテリジェンスの活用と目撃情報の報告が可能になります。この統合では、STIX形式の構造化された脅威インテリジェンスをSIEMシステムが理解しやすく活用できる形式に変換し、脅威対策の効果を高めます。





詳細については、『Context Hub構成ガイド』のトピック「**STIXをデータ ソースとして構成する**」を参照してください。

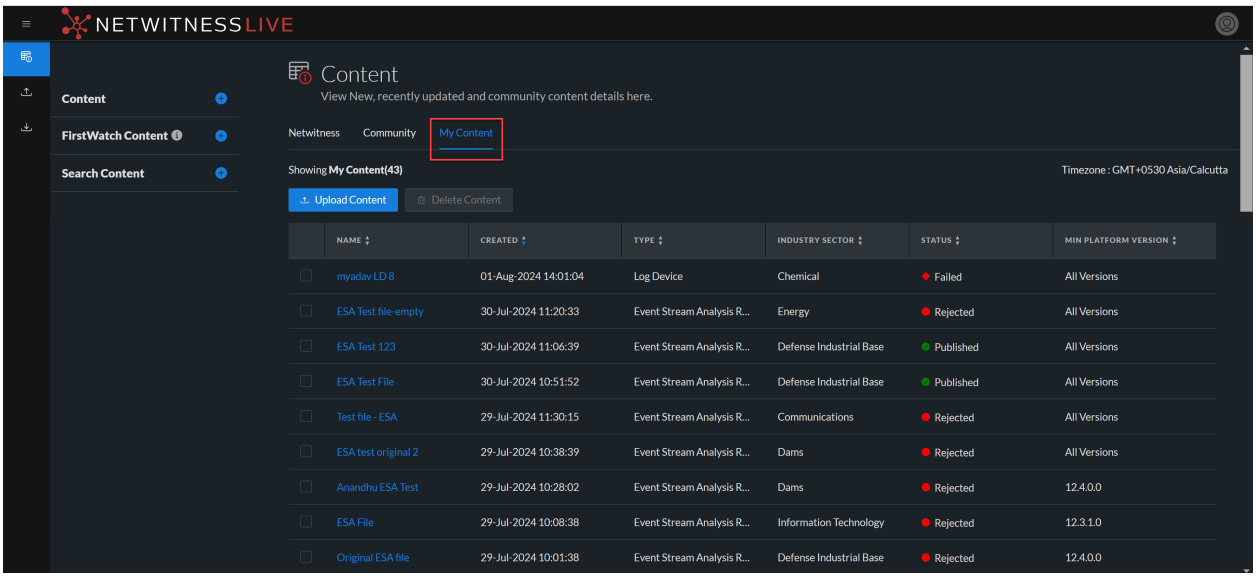
ライブクラウド サービス

次のセクションでは、Live Cloud Serviceコンポーネントの新しい機能強化について説明します。

NetWitness Liveでカスタム コミュニティ コンテンツを管理する

NetWitnessでは新しいMy Content機能が導入され、ユーザーはNetWitness Live UIからカスタム コンテンツをシームレスに直接管理できるようになりました。これには、ログ デバイス、イベント ストリーム分析ルール、パーサー、フィードなどのユーザーが作成したコンテンツのアップロード、削除、ダウンロードが含まれます。この機能により、ユーザー間で有用かつ関連性の高いカスタム コンテンツをより効率的に共有できるため、コンテンツ公開チームを通じた公開に要する時間と労力が削減されます。ユーザーは、ニーズやユースケースに合ったさまざまなコンテンツ オプションから選択できます。

注 : NetWitness Live My Content機能は、このリリースではログ デバイスとESAコンテンツのみをサポートします。



詳細については、『NetWitness Liveサービス管理ガイド』のトピック「**カスタム コンテンツの管理**」を参照してください。

セキュリティアップデート

NetWitness Platformが使用するさまざまなライブラリに対して報告された最新のセキュリティ脆弱性 (重大な脆弱性1件 (CVE-2016-1000027)、重大な脆弱性35件、中程度の脆弱性103件、および軽微な脆弱性16件) に対処します。

セキュリティ修正の詳細については、https://community.netwitness.com/t5/netwitness-platform-advisories/ct-p/netwitness-advisories#securityを参照してください。

アップグレード パス

NetWitness 12.5.0.0では、次のアップグレード パスがサポートされます。

- NetWitness 12.4.2.0から12.5.0.0
- NetWitness 12.4.1.0から12.5.0.0
- NetWitness 12.4.0.0から12.5.0.0
- NetWitness 12.3.1.0から12.5.0.0
- NetWitness 12.3.0.0から12.5.0.0
- NetWitness 12.2.0.1から12.5.0.0
- NetWitness 12.2.0.0から12.5.0.0

12.5.0.0へのアップグレードの詳細については、NetWitness 12.5.0.0のアップグレード ガイドを参照してください。

重要 : NetWitnessは、バージョン12.2までが2024年3月31日をもってサポート終了 (EOL) に達したことを指摘し、ユーザーにソフトウェア バージョンを確認するようアドバイスしています。詳細については、https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875を参照してください。最新の機能とセキュリティ更新を活用するには、NetWitnessではバージョン12.5にアップグレードすることをお勧めします。

重要 :11.7.xまたは11.7.x.xバージョンから12.5.0.0バージョンにアップグレードする場合は、12.5にアップグレードする前に、まず12.2.0.0または12.3.0.0バージョンにアップグレードする必要があります。

重要 : Warehouseコネクタは、ロックボックスを使用して、データ統合のソースと宛先の資格情報を安全に保存します。ただし、以前のバージョンから12.5バージョンにアップグレードするユーザーは、既存の資格情報を新しいロックボックスに移行しないと、構成されたストリームを開始できません。そのため、ユーザーは手動で新しいロックボックス キーを作成し、該当する場合はWarehouse Connectorで構成されているソース宛先のパスワードを更新する必要があります。新しいロックボックス キーを作成する詳細な手順については、『NetWitness 12.5.0.0のアップグレード ガイド』の「**アップグレード後のタスク**」で『**Warehouse Connector**』セクションを参照してください。

NetWitness Platformの製品バージョン ライフ サイクル

プライマリー サポート終了 (EOPS) が到来するバージョンについては、「NetWitness Platformの製品バージョン ライフ サイクル」のリストを参照してください。

以前のリリースの新機能

このセクションでは、サポートされる以前のすべてのリリースの新機能と機能拡張について説明します。

詳細については、https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-12-x/ta-p/695650を参照してください。

12.5.0.0リリースで修正された問題

このセクションでは、12.5.0.0バージョンで修正された問題を一覧表示します。

修正された問題の詳細については、NetWitnessコミュニティー ポータルのNetWitness® Platform既知の問題リスト(https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872) で 修正されたバージョン]列を参照してください。

エンドポイントの修正

追跡番号	説明
SACE-21629	タイムアウト制限が高すぎるため、リレー サーバーのメッセージ キューをチェックするときに、Endpointサーバーのポーリング メカニズムが期待どおりにタイムアウトしませんでした。

ホームページの修正

追跡番号	説明
ASOC-148336	ユーザーは、ユーザー設定オプションで「ホーム ページ」をデフォルトのランディング ページとして選択できるようになり、空白の画面が表示されることはありません。

プラットフォームの修正

追跡番号	説明
ASOC-146908	アップグレード中、OS移行が完了した後に、ホストがel8カーネルで起動しない問題が発生しました。

デコーダーの修正

追跡番号	説明
ASOC-147188	DPDK移行の一環としてオプションのPruneコマンドを実行すると、一部のインターフェイスに関連する継続的なエラー メッセージがログに表示されます。

追跡番号	説明
ASOC-144467	Hostedプラグインを再読み込みすると、デコーダー/ホステッド ツリーから再読み込みされるのではなく、プラグイン インスタンスが削除されてしまいます。
ASOC-154781	デコーダーを12.4.xにアップグレードすると、最終的に /var/netwitness/decoderパーティションがparsestatdbデータでいっぱいになります。

12.5.0.0リリースの既知の問題

本リリースで解決されていない問題は、NetWitnessコミュニティー ポータルの「NetWitness® Platformの既知の問題リスト」に記載されています。https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872

12.5.0.0コンポーネントのビルド番号

次の表は、NetWitness 12.5.0.0の各コンポーネントのビルド番号の一覧です。

コンポーネント	バージョン番号
NetWitness管理サーバー	rsa-nw-admin-server-12.5.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm
NetWitness Advanced Analyticsコンテンツ	rsa-nw-advanced-analytics-content-12.5.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm
NetWitness Advanced Analytics サーバー	rsa-nw-advanced-analytics-server-12.5.0.0-231212110325.5.9b3b362.el8.alma.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Auditプラグイン	rsa-audit-plugins-12.5.0.0-4892.5.9d0750b41.el8.noarch.rpm
NetWitness Audit RT	rsa-audit-rt-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitnessブートストラップ	rsa-nw-bootstrap-12.5.0.0-2401240926.5.a3d68ef.el8.noarch.rpm
NetWitness Broker	rsa-nw-broker-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-12.5.0.0-2787.5.721a8daa7.el7.x86_64.rpm
NetWitness Cloud	rsa-nw-cloud-12.5.0.0-12867.5.957818c84.el8.x86_64.rpm
NetWitness Cloud Connectorサーバー	rsa-nw-cloud-connector-server-12.5.0.0-240116135943.5.4220688.el8.alma.noarch.rpm
NetWitness Cloud Linkサーバー	rsa-nw-cloud-link-server-12.5.0.0-240117032857.5.d4a8422.el8.alma.noarch.rpm
NetWitness Collectd	rsa-collectd-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Component Descriptor	rsa-nw-component-descriptor-12.5.0.0-2402280945.5.4c3391a.el8.noarch.rpm
NetWitness Concentrator	rsa-nw-concentrator-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-12.5.0.0-2402050947.5.b7e9f64.el8.noarch.rpm
NetWitness Concentrator	rsa-nw-config-server-12.5.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm
NetWitness Console	rsa-nw-console-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm

NetWitness Content Server	rsa-nw-content-server-12.5.0.0-240109040529.5.314fc043.el8.alma.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-12.5.0.0-240122010054.5.d98d0ac61.el8.alma.noarch.rpm
NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-12.5.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm
NetWitness Dashboardコンテンツ	rsa-nw-dashboard-content-20231220155210-5.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Decoder Analyticsコンテンツ	rsa-nw-decoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Decoderコンテンツ	rsa-nw-decodercontent-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-12.5.0.0-2402150604.5.dbd95e3.el8.noarch.rpm
NetWitness Endpointエージェント	rsa-nw-endpoint-agents-12.5.0.0-2402061657.5.db93b9a.el8.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-12.5.0.0-240103053136.5.8430874.el8.alma.noarch.rpm
NetWitness Endpoint Decoder Analyticsコンテンツ	rsa-nw-endpointdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-12.5.0.0-240125030031.5.12c246114.el8.alma.noarch.rpm
NetWitness ESPER Enterprise	rsa-nw-esper-enterprise-12.5.0.0-2311071130.5.04c15de.el8.alma.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-12.5.0.0-240117101347.5.0ed5cc33.el8.alma.noarch.rpm
NetWitnessInvestigate Server	rsa-nw-investigate-server-12.5.0.0-240109023320.5.2a0d2764.el8.alma.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-12.5.0.0-240122162503.5.40628dd.el8.almalinux.noarch.rpm
NetWitness License Server	rsa-nw-license-server-12.5.0.0-240111044400.5.a6108af.el8.alma.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Collectorコンテンツ	rsa-nw-logcollectorcontent-20240105141144-5.x86_64.rpm
NetWitness Log Collector Perl	rsa-nw-logcollector-perl-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm

NetWitness Log Collectorツール	rsa-nw-logcollector-tools-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Log Decoder Analyticsコンテンツ	rsa-nw-logdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Log Decoder Baseコンテンツ	rsa-nw-logdecoder-base-content-20240124060008-5.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-12.5.0.0-240207115909.5.1511622.el8.almalinux.x86_64.rpm
NetWitness Meta Export Utility	rsa-nw-metaexport-utility-12.5.0.0-110124.5.el8.x86_64.rpm
NetWitness Metrics Server	rsa-nw-metrics-server-12.5.0.0-240109050254.5.c078db1.el8.alma.noarch.rpm
NetWitness Node Infra Server	rsa-nw-node-infra-server-12.5.0.0-240116091133.5.70861f6.el8.alma.noarch.rpm
NetWitness Orchestration Cli	rsa-nw-orchestration-cli-12.5.0.0-2401091103.5.7317baa.el8.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-server-12.5.0.0-240119064852.5.a87bb81f.el8.alma.noarch.rpm
NetWitness Placeholder	rsa-nw-placeholder-12.5.0.0-2310040926.5.cebd204.el8.noarch.rpm
NetWitness Presidio Airflow	rsa-nw-presidio-airflow-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Config Server	rsa-nw-presidio-configserver-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Core	rsa-nw-presidio-core-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Elastic Search Init	rsa-nw-presidio-elasticsearch-init-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Ext NetWitness	rsa-nw-presidio-ext-netwitness-12.5.0.0-2401151152.5.18bd06b.el8.noarch.rpm
NetWitness Presidio Manager	rsa-nw-presidio-manager-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Output	rsa-nw-presidio-output-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio UI	rsa-nw-presidio-ui-12.5.0.0-2402270745.5.0844250.el8.noarch.rpm

NetWitness Protobuf	rsa-protobufs-rt-12.5.0.0-928.5.6254aabd8.el8.x86_64.rpm
NetWitnessリカバリ ツール	rsa-nw-recovery-tool-12.5.0.0-2401230435.5.f34a9fd.el8.noarch.rpm
NetWitnessリレー サーバー	rsa-nw-relay-server-12.5.0.0-240112083607.5.6d41796.el8.alma.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-12.5.0.0-5996.5.b76234be4.el8.x86_64.rpm
NetWitness Respond Server	rsa-nw-respond-server-12.5.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm
NetWitness Response Actionsサーバー	rsa-nw-response-actions-server-12.5.0.0-240116034125.5.0af5d71.el8.alma.noarch.rpm
NetWitness ルート CA の更新	rsa-nw-root-ca-update-12.5.0.0-2401221231.5.96cd15b.el8.noarch.rpm
NetWitness SAツール	rsa-sa-tools-12.5.0.0-2401251338.5.89600eb.el8.noarch.rpm
NetWitnessセキュリティCli	rsa-nw-security-cli-12.5.0.0-2401091103.5.18ab320.el8.noarch.rpm
NetWitness Security Server	rsa-nw-security-server-12.5.0.0-240123034132.5.11d93f41.el8.alma.noarch.rpm
NetWitnessシェル	rsa-nw-shell-12.5.0.0-240108140410.5.0b0d73f5.el8.alma.noarch.rpm
NetWitnessSOSレポート プラグイン	rsa-nw-sosreport-plugins-12.5.0.0-2401162235.5.af21a76.el8.noarch.rpm
NetWitness SMS Runtime RT	rsa-sms-runtime-rt-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Source Server	rsa-nw-source-server-12.5.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm
NetWitnessソース サーバー コンテンツ	rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm
NetWitness ユーザーインターフェース	rsa-nw-ui-12.5.0.0-240131063757.5.d1b137ecbc.el8.alma.noarch.rpm
NetWitness ワークベンチ	rsa-nw-workbench-12.4.5.0-12866.5.1aefe557c.el8.x86_64.rpm

NetWitness Platformのヘルプ情報

製品ドキュメント

このリリースでは、次のドキュメントが提供されます。

マニュアル	参照場所
NetWitness Platformマスター目次	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.5.0.0 Product Documentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.5.0.0 アップグレード ガイド	https://community.netwitness.com/t5/rsa-netwitness-platform-staged/upgrade-guide-for-12-4/ta-p/709308
NetWitness Analytics on Cloud	NetWitness Analytics on Cloudリリースの新機能と拡張機能の詳細については、次の「新機能」セクションを確認してください。 UEBAクラウドについては、https://docs.netwitness.com/netwitnessueba/release_information/whats_new/をご覧ください。 Insightについては、https://docs.netwitness.com/netwitnessinsight/release-information/insight_whatsnew/をご覧ください。

セルフ ヘルプ リソース

NetWitnessのインストールおよび使用について支援が必要な場合は、次の情報をご利用ください。

- NetWitnessに関するすべてのドキュメントは、次の場所から参照できます。https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- 特定の情報を見つけるには、NetWitnessコミュニティー ポータルの［Search］および［Create a Post］フィールドを使用します(https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions) 。
- NetWitnessのナレッジベース :https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- ガイドの「トラブルシューティング」セクションを参照します。

- NetWitness® Platformのブログ投稿も参照してください。
- さらに支援が必要な場合は、カスタマー サポートにお問い合わせください。

カスタマー サポートへのお問い合わせ

カスタマー サポートに連絡する場合は、コンピューターを操作できる状態である必要があります。以下の情報を提供できるように準備しておいてください。

- お使いのNetWitness Platform製品またはアプリケーションのバージョン番号
- お使いのハードウェアのタイプ

質問や支援が必要な場合は、以下の連絡先までお問い合わせください。

NetWitnessコミュニティ ポータル	https://community.netwitness.com メイン メニューで [**Support**] > [**Case Portal**] > [**View My Cases**] をクリックします。
各国のお問い合わせ窓口	https://community.netwitness.com/t5/support/ct-p/support
コミュニティ	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
NW更新	https://update.netwitness.com/
LiveUI	https://live.netwitness.com

NetWitness教育サービス

登録すると、NetWitnessのコースや、NetWitness教育サービスおよびトレーニングに関する追加リソースにアクセスできるようになります。

NetWitness教育ポータル	https://netwitness.sabacloud.com/Saba/Web_spf/NA10P2PRD088/guestapp/home;spf-url=guest%2Fguestlearningcatalog
NetWitness教育サービス コース カタログ	https://community.netwitness.com/t5/netwitness-education-courses/tkb-p/netwitness-training
NetWitness教育サービス トレーニング スケジュール	https://community.netwitness.com/t5/netwitness-education-blog/netwitness-instructor-led-training-schedule/ba-p/655826
NetWitness教育サービス サポート連絡先	education.support@netwitness.com

製品ドキュメントへのフィードバック

NetWitness Platformのドキュメントに関するフィードバックは、feedbacknwdocs@netwitness.comまでメールで送信してください。