NetWitness® Plattform

Version 12.5

Versionshinweise

NETWITNESS
Platform

Contact Information

NetWitness Community unter https://community.netwitness.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie Produktdokumentationen, Communitydiskussionen und Case Management bereitgestellt werden.

Marken

RSA und andere Marken sind Marken von RSA Security LLC oder deren Tochtergesellschaften („RSA“). Eine Liste der RSA-Marken finden Sie unter https://www.rsa.com/de-de/company/rsa-trademarks. Alle anderen Marken sind Marken ihrer jeweiligen Inhaber.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von RSA Security LLC oder deren Tochtergesellschaften und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Angabe des unten stehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden. Diese Software kann ohne Vorankündigung geändert werden und ist nicht als Verpflichtung von RSA zu verstehen.

Es wird empfohlen, keine Repositorys von Drittanbietern bereitzustellen oder Änderungen am zugrunde liegenden NetWitness-Betriebssystem vorzunehmen, die nicht Teil der unterstützten NetWitness-Version sind. Jede derartige Änderung außerhalb des von NetWitness genehmigten Images kann zu einem Service- oder Funktionskonflikt führen und ein Re-Imaging des NetWitness-Systems erfordern, um NetWitness wieder in einen optimierten Funktionszustand zu versetzen. Falls ein Repository eines Drittanbieters bereitgestellt oder eine andere nicht unterstützte Änderung vom Kunden ohne Genehmigung von NetWitness vorgenommen wird, übernimmt der Kunde die volle Verantwortung für jegliche Systemfehlfunktion, bis das Problem durch Troubleshooting oder ein Re-Imaging des Services behoben werden kann.

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf NetWitness Community verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren müssen beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

Für die Nutzung, das Kopieren und die Verteilung der in dieser Veröffentlichung beschriebenen Software von RSA Security LLC oder deren Tochtergesellschaften („RSA“) ist eine entsprechende Softwarelizenz erforderlich.

RSA ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN WERDEN OHNE GEWÄHR ZUR VERFÜGUNG GESTELLT. RSA MACHT KEINE ZUSICHERUNGEN UND ÜBERNIMMT KEINE HAFTUNG JEDWEDER ART IM HINBLICK AUF DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN UND SCHLIESST INSBESONDERE JEDWEDE IMPLIZITE HAFTUNG FÜR DIE HANDELSÜBLICHKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AUS.

Sonstiges

Dieses Produkt, diese Software, die zugehörigen Dokumentationen sowie die Inhalte unterliegen den allgemeinen Geschäftsbedingungen von NetWitness, die zum Zeitpunkt der Veröffentlichung dieser Dokumentation gültig sind und unter https://www.netwitness.com/standard-form-agreements/ zu finden sind.

September 2024

Inhalt

Neuheiten in Version 12.5.0.0

In den Versionshinweisen zu NetWitness 12.5.0.0 werden neue Funktionen, Verbesserungen, Sicherheitsupdates, Upgrade-Pfade, behobene und bekannte Probleme, nicht mehr unterstützte Funktionen, Build-Nummern und Selbsthilferessourcen erläutert.

Verbesserungen

Die folgenden Abschnitte enthalten eine vollständige Liste und Beschreibung der Verbesserungen bestimmter Merkmale:

- Dashboard
- Untersuchen
- Reagieren
- Insight
- Analyse des Nutzer- und Entitätsverhaltens (UEBA)
- SASE-Merkmale
- Endpoint
- Policy-basiertes zentralisiertes Contentmanagement (CCM)
- Concentrator-, Decoder-, Log Collector- und Archiver-Services
- Protokollintegrationen
- Context Hub
- Live-Cloudservice

Informationen zum Auffinden der Dokumente, auf die in diesem Abschnitt verwiesen wird, finden Sie unter https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246.

Der Abschnitt Produktdokumentation enthält Links zur Dokumentation zu dieser Version.

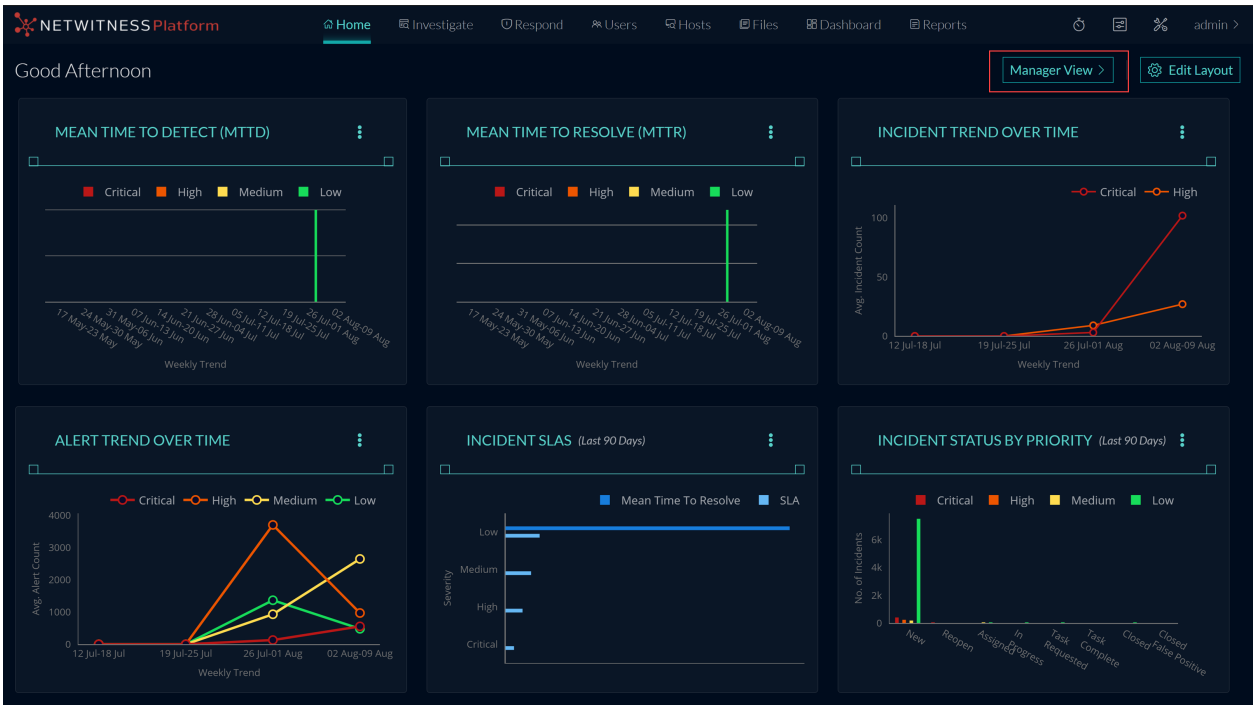
Dashboard

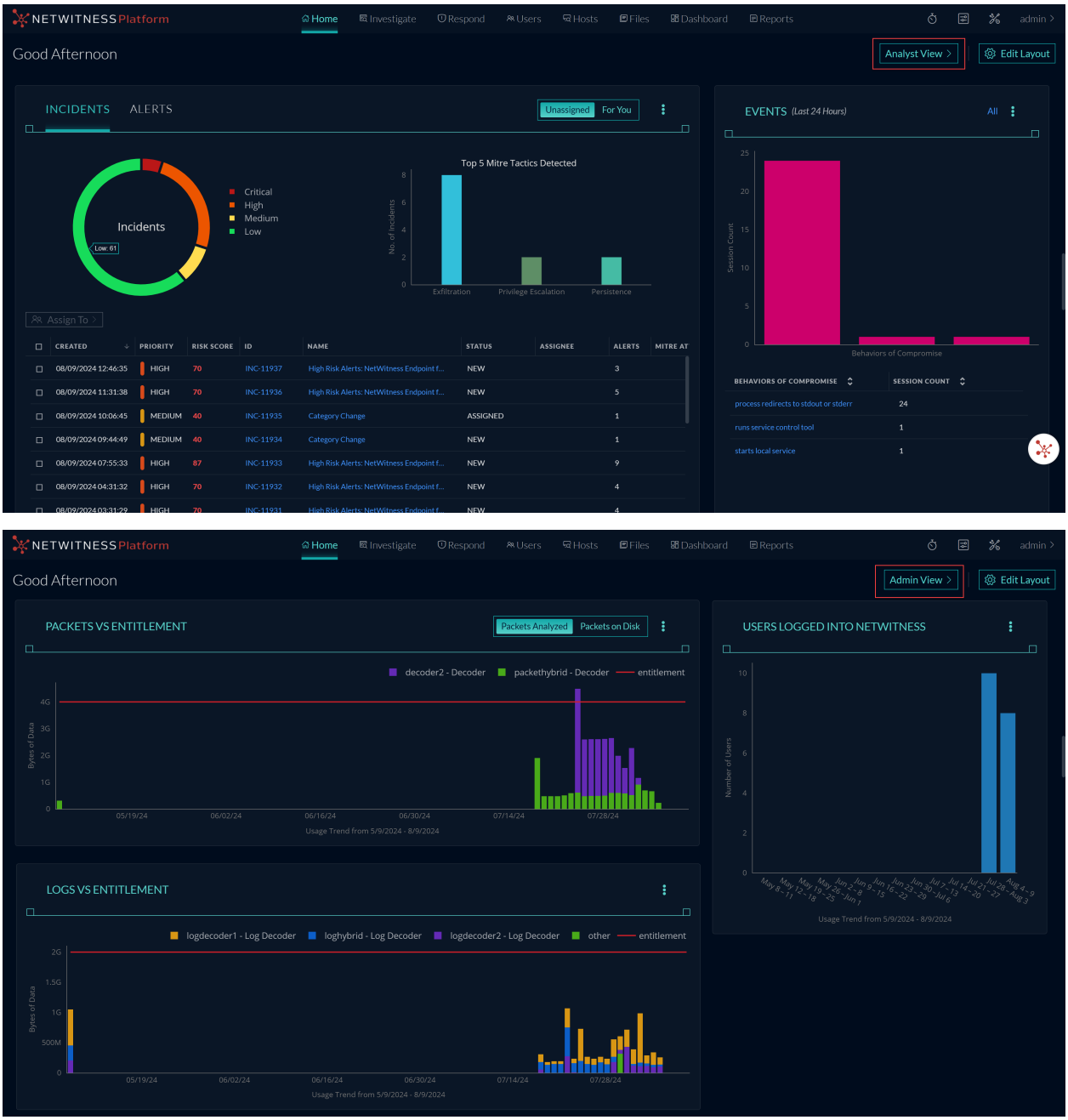
Der folgende Abschnitt beschreibt die neuen Verbesserungen an der Dashboard-Komponente:

Neue Homepages

NetWitness führt ein neues Menü auf der **Startseite** ein, das aus den Ansichten **Admin**, **Analyst** und **Manager** besteht. Jede Homepage besteht aus mehreren Widgets. Administratoren, Analysten und SOC-Manager können auf die entsprechenden Widgets zugreifen, die bestimmte Daten in grafischer Form anzeigen. Die Daten können mit Endpunkten, Nutzern, Ressourcen, Inhalten, Vorfällen, Alarmen, MITRE ATT&CK, Aufbewahrung und vielem mehr verknüpft werden.


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



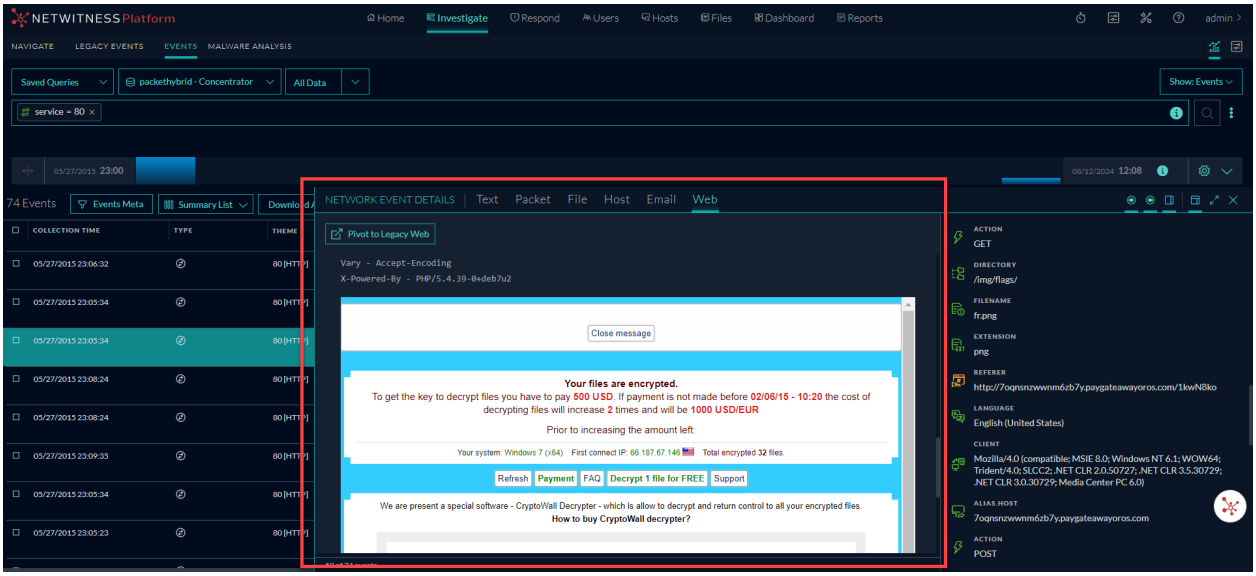
Weitere Informationen finden Sie im Thema **Manage Home Widgets** im NetWitness-Einführungshandbuch für 12.5.

Untersuchen

Im folgenden Abschnitt werden die neuen Erweiterungen für die Investigate-Komponente beschrieben:

Web-Rekonstruktion aus der Ereignisansicht

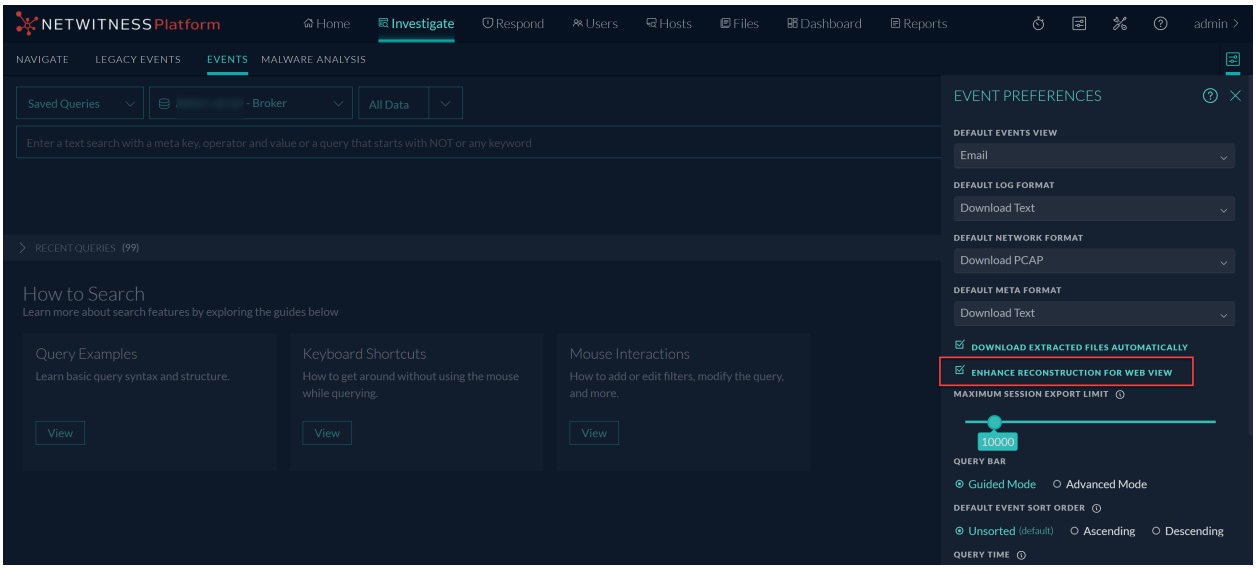
Analysten können die Webansicht des Zielereignisses sicher aus der Ansicht **Ereignisse > Webrekonstruktion** rekonstruieren, wenn ein Nutzer Webseiten besucht hat, die mit einem bestimmten Ereignis in Zusammenhang stehen. NetWitness kann die gleiche Webseite rekonstruieren, indem es die in Paketen verfügbaren Daten verwendet, die Webseite anzeigt und sie so genau wie möglich mit den Bildern und CSS-Stilen in Beziehung setzt. Dieser Web-Rekonstruktionsprozess ermöglicht Analysten, wertvolle Einblicke in die durchgeführten Webaktivitäten zu gewinnen und so eine effektive Analyse und Untersuchung durchzuführen.



Weitere Informationen finden Sie im Abschnitt **Web-Rekonstruktion** des Themas **Ereignisdetails in der Ereignisansicht untersuchen** im NetWitness Investigate-Benutzerhandbuch für 12.5.

Verbesserte Rekonstruktion von Ereignissen in der Web-Ansicht

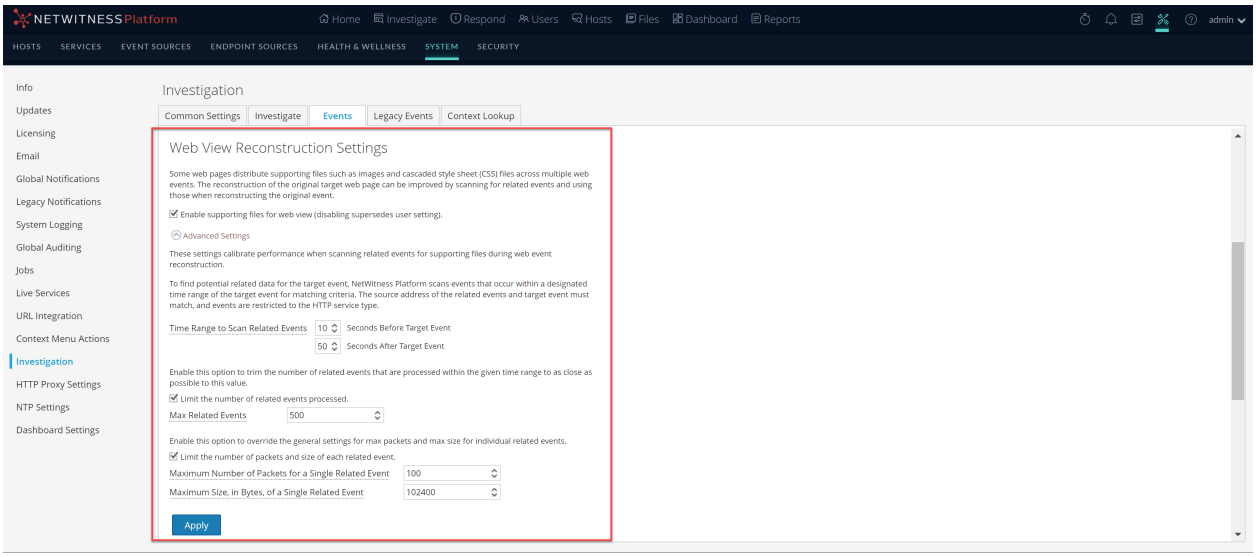
Die neue Benutzereinstellung **Rekonstruktion für Web-Ansicht verbessern** wurde in der Ansicht **Untersuchen** > **Ereignisse** im Bereich **Ereigniseinstellungen** ergänzt. Diese Einstellung ist standardmäßig für alle Benutzer aktiviert. Diese Option verbessert die Rekonstruktion von Websites, die ein Ereignis rekonstruieren, indem sie CSS, Bilder und Links verwendet, um die Ansicht effektiv zu formatieren. Auf diese Weise können Analysten den Kontext und die Details der Ereignisse, die sie rekonstruieren, besser verstehen. Diese Verbesserung ermöglicht es Analysten, fundiertere und genauere Analysen durchzuführen und entsprechende Maßnahmen zu ergreifen.



Weitere Informationen finden Sie im *Benutzerhandbuch zu NetWitness Investigate* unter **Festlegen von Benutzereinstellungen für die Ereignisansicht**.

Einführung der Einstellungen für die Rekonstruktion der Webansicht aus der Systemansicht

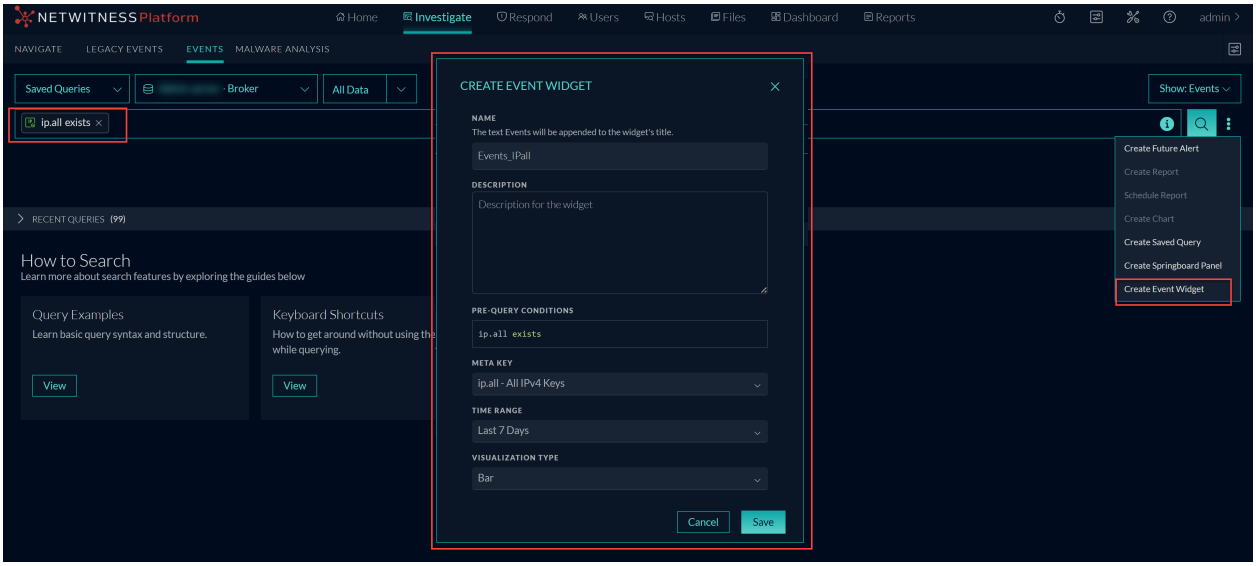
NetWitness führt die neuen **Einstellungen für die Rekonstruktion der Webansicht** in der Ansicht **(Admin)** > **System** > **Investigation** ein. Mit dieser Einstellung auf der Registerkarte **Ereignisse** können Administratoren die Rekonstruktion von Webansichten verbessern, indem sie verwandte Ereignisse mit denselben unterstützenden Dateien scannen und rekonstruieren. Bei der Rekonstruktion einer Web-Ansicht, die mehrere Ereignisse umfasst, kann das System die Rekonstruktion des Zielereignisses verbessern, indem es verwandte Ereignisse einbezieht, die relevante Bilder und CSS-Dateien enthalten. Nur Ereignisse vom Servicetyp HTTP mit derselben Quelladresse wie das Zielereignis und einem Zeitstempel innerhalb eines spezifizierten Zeitbereichs vor und nach dem Zielereignis werden gescannt. Administratoren können außerdem die maximale Anzahl zusammengehöriger Ereignisse zum Scannen konfigurieren, was für mehr Flexibilität und Präzision bei der Rekonstruktion der Web-Ansicht sorgt. Die Option „Erweiterte Einstellungen“ zeigt alle konfigurierbaren Einstellungen in diesem Abschnitt an.



Weitere Informationen finden Sie im Abschnitt **Einstellungen für Rekonstruktion der Webansicht** des Themas **Investigation-Konfigurationsbereich** im Systemkonfigurationsleitfaden.

Benutzerdefiniertes Ereignis-Widget aus Abfrage erstellen

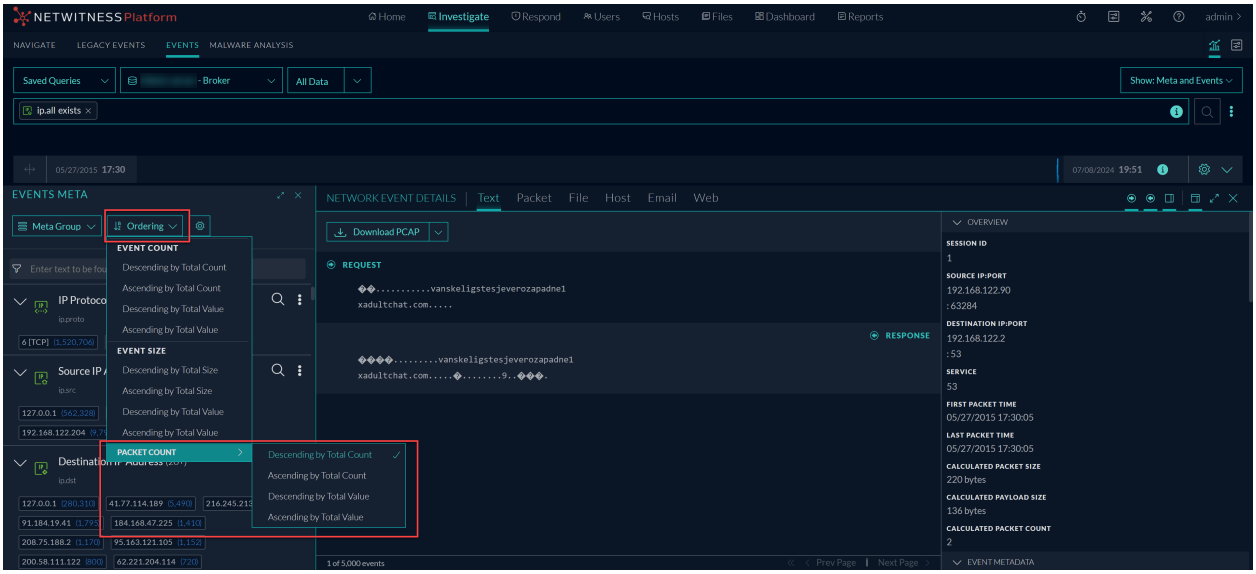
Während der Untersuchung können Administratoren und Analysten jetzt ein Ereignis-Widget aus der Ansicht **Untersuchen** > **Ereignisse** erstellen. Benutzer können der Abfragesuchleiste eine beliebige Anzahl Filter hinzufügen und diese Suchvorgänge zur verbesserten Erkennung und Überwachung in Ereignis-Widgets umwandeln. Damit schnell darauf zugegriffen werden kann, wird das neu erstellte Widget in der Homepage-Bibliothek gespeichert. Die Nutzer können dann das Ereignis-Widget zur Dashboard-Layoutansicht (**Admin**, **Analyst** oder **Manager**) auf der Startseite hinzufügen und seine Konfiguration ihren Anforderungen entsprechend anpassen. Diese Funktion verbessert die Überwachung und Analyse von Ereignissen und ermöglicht es Benutzern, relevante und wichtige Ereignisse in Echtzeit zu verfolgen und zu beobachten.



Weitere Informationen finden Sie im Thema zum **Erstellen von Ereignis-Widgets aus der Ereignisansicht** im NetWitness Investigate – Benutzerhandbuch für 12.5.

Metaschlüsselergebnisse nach der Paketanzahl sortieren

Analysten können jetzt die Ergebnisse jedes Metaschlüssels nach der Anzahl der Pakete in der Sitzung auf der Seite **Investigate** > **Ereignisse** sortieren. Sie können die Ergebnisse nach Wert oder Gesamtsumme und in aufsteigender oder absteigender Reihenfolge sortieren. Durch Sortieren der Metaschlüsselergebnisse nach Paketanzahl können Sie leicht die am häufigsten oder am wenigsten häufigen Metawerte finden, die in der Benutzerumgebung aufgetreten sind und für weitere Untersuchungen oder Analysen verwendet werden können.



Weitere Informationen finden Sie im Abschnitt **Set the Ordering Method for Meta Values** im Thema **Drill into Metadata in the Events View** im NetWitness Investigate – Benutzerhandbuch für 12.5.

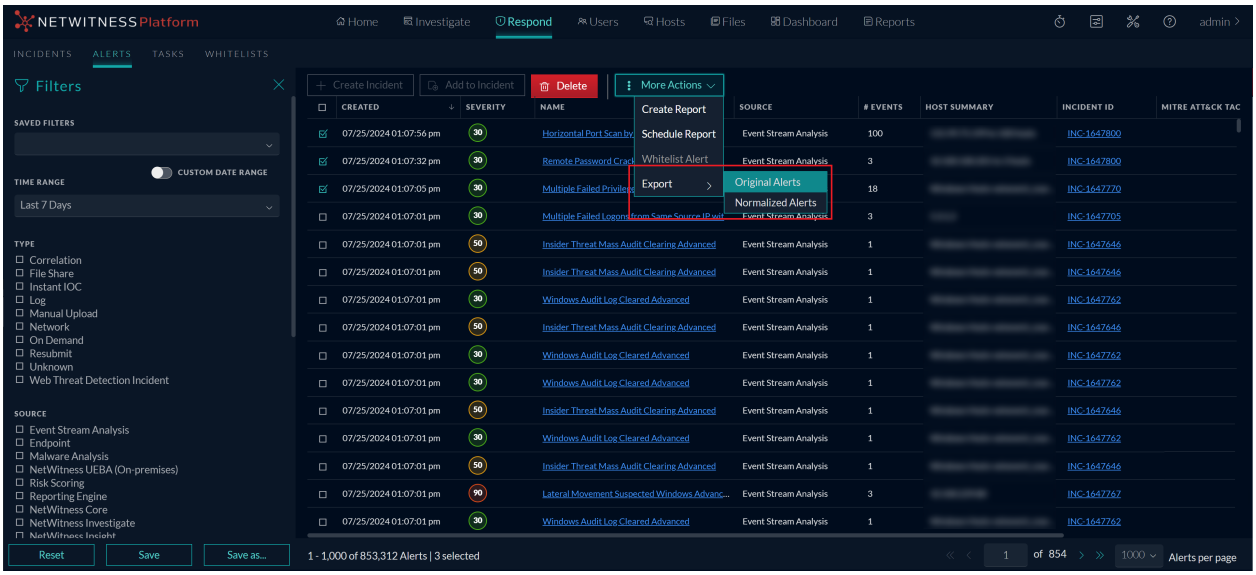
Reagieren

Der folgende Abschnitt beschreibt die neuen Verbesserungen an der Respond-Komponente:

Verbesserung der Warnmeldungsansicht

Mit der Option **Export** unter **Reagieren** > **Warnmeldungen** > Warnmeldung auswählen > **Mehr Aktionen** können Sie die ursprünglichen und normalisierten Warnmeldungen zusammen mit den Ereignissen im JSON-Format exportieren und herunterladen. Mit der NetWitness Platform können Sie bis zu **1000** Warnmeldungen gleichzeitig exportieren, um sie offline zu untersuchen.

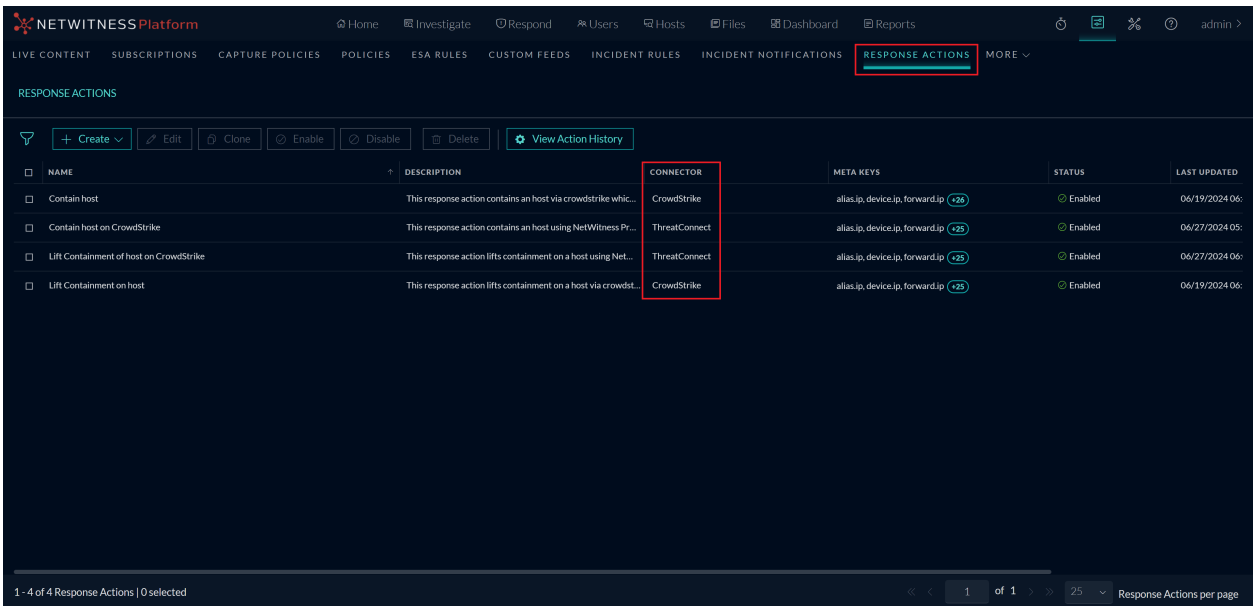
Weitere Informationen finden Sie unter **Export Alerts Data** im *NetWitness Respond-Benutzerhandbuch für 12.5*.



OOTB-Antwortaktionen

Einführung von Out-of-the-Box(OOTB)-Aktionen als Teil des Dienstes für Antwortaktionen. Die OOTB-Aktionen „Contain Host“ und „Lift Containment on Host“ sind für CrowdStrike und CrowdStrike, das über NetWitness Orchestrator integriert ist, aktiviert. Diese Erweiterung ermöglicht es Analysten, Reaktionsmaßnahmen nach der Überprüfung eines Vorfalls manuell oder automatisch als Teil eines ausgelösten Vorfalls durchzuführen. Die Reaktionsmaßnahmen mit CrowdStrike sind direkt oder über NetWitness Orchestrator verfügbar.

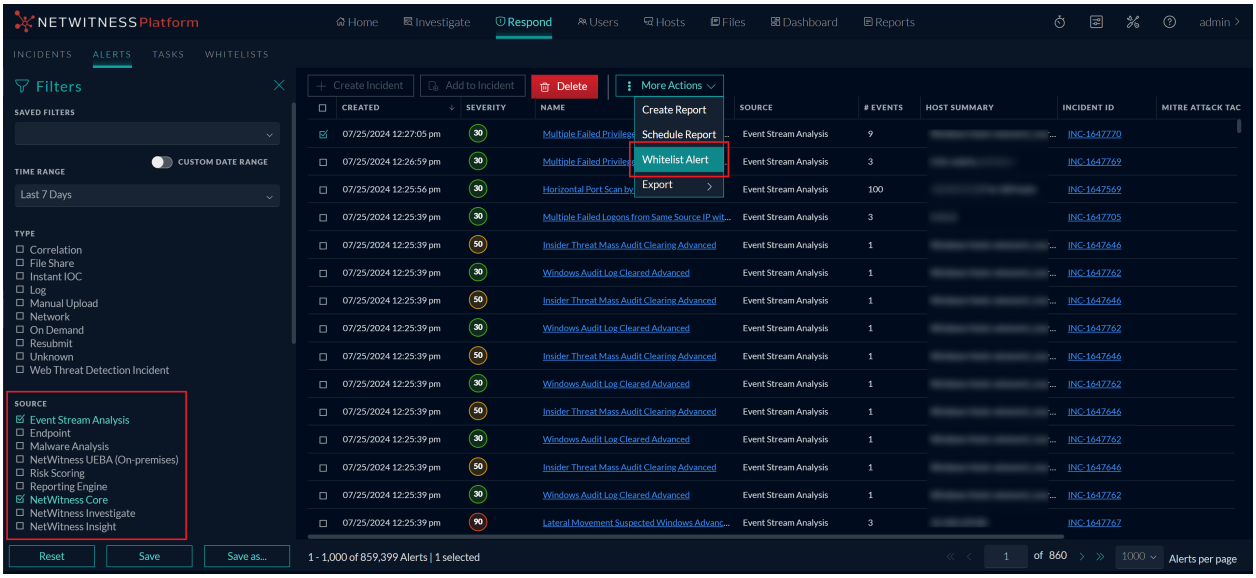
Weitere Informationen finden Sie unter **Antwortaktionen** im *Aktionskonfigurationsleitfaden für NetWitness Respond 12.5*.



Whitelist-Erweiterung

Die Whitelist-Funktion wurde um Warnmeldungen für die Dienste Event Stream Analysis und NetWitness Core erweitert. Sie können jetzt unerwünschte und wiederkehrende nicht verdächtige Warnungen hinsichtlich dieser Dienste auf die Whitelist setzen. Dadurch können Sie bestimmte Entitäten auswählen und Whitelist-Bedingungen festlegen, um unerwünschte Warnungen zu diesen Entitäten zu verhindern.

Weitere Informationen finden Sie unter im *NetWitness Respond-Benutzerhandbuch zu 12.5* **Whitelists List View**///.

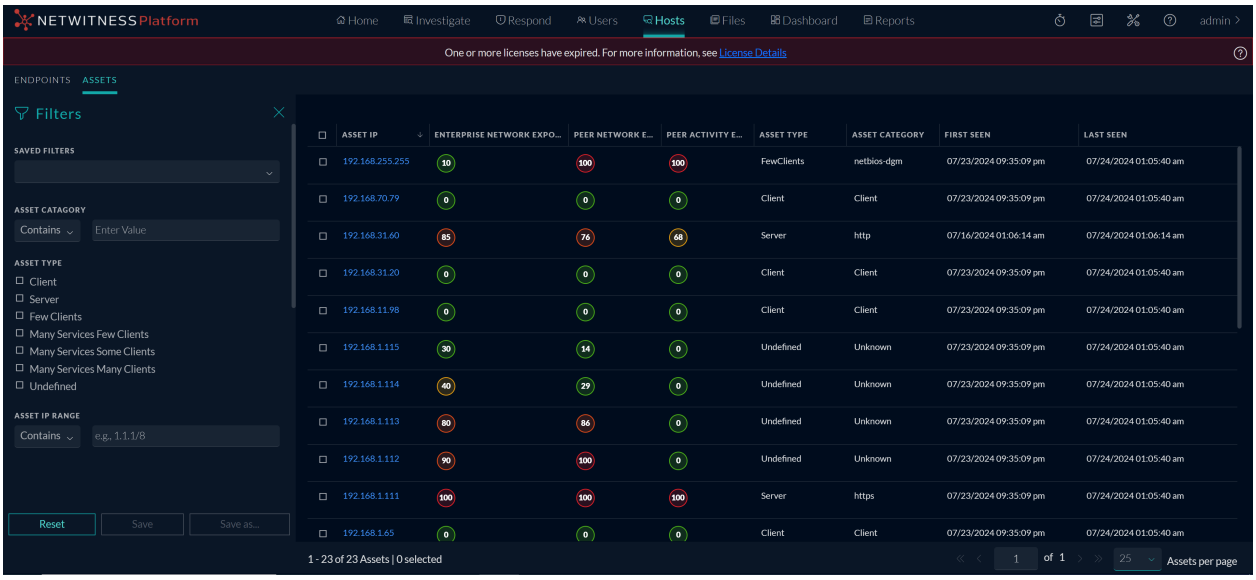


Insight

Der folgende Abschnitt beschreibt die neuen Verbesserungen an der Insight-Komponente:

Neue Asset-Ansicht zur Erkennung und Untersuchung von Netzwerk-Assets

In NetWitness gibt es im Menü **Hosts > Assets** jetzt eine neue Assets-Ansicht. Diese Ansicht bietet einen zentralen Ort, an dem alle Netzwerkressourcen in Ihrer Umgebung erkannt werden, zusammen mit den zugehörigen Details, wie z. B. die Ressourcen-IP, der Ressourcen-Typ, die Ressourcenkategorie, die Gefährdung gegenüber Unternehmensnetzwerken, die Peer-Netzwerkgefährdung, die Gefährdung gegenüber Peer-Aktivitäten, die erste und die letzte Anzeige. Mithilfe von Filtern können Sie die Assets nach verschiedenen Kriterien eingrenzen. Mithilfe dieser Ansicht können Analysten Assets mit ungewöhnlichem Verhalten oder unbekannte Assets problemlos identifizieren und priorisieren. So können sie sofort Maßnahmen ergreifen, um potenzielle Sicherheitsrisiken zu minimieren.



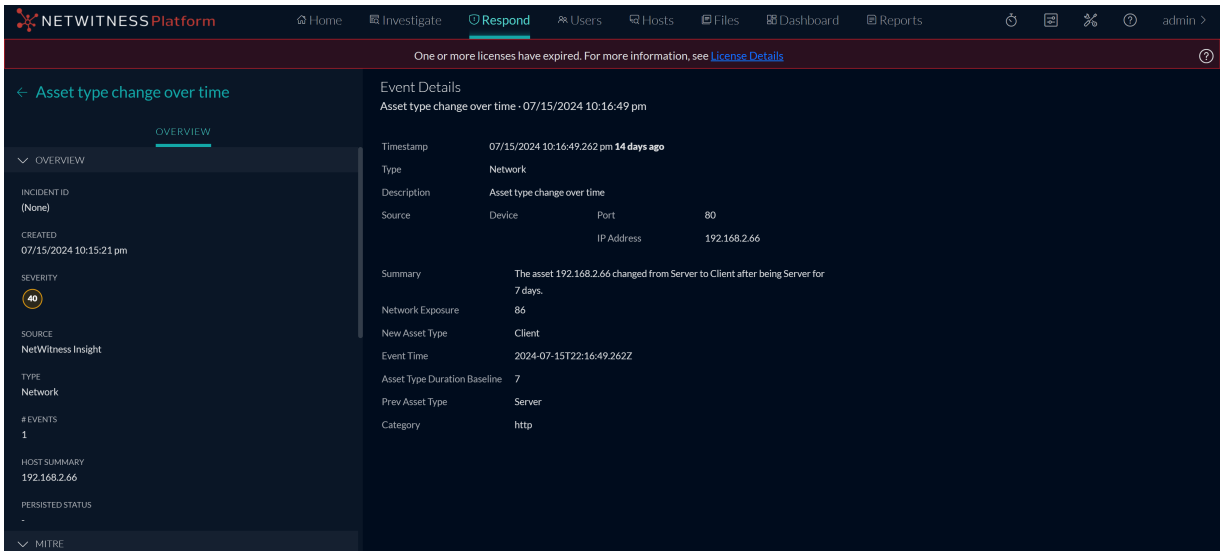
Neue Insight-Warnungen für Netzwerkressourcen

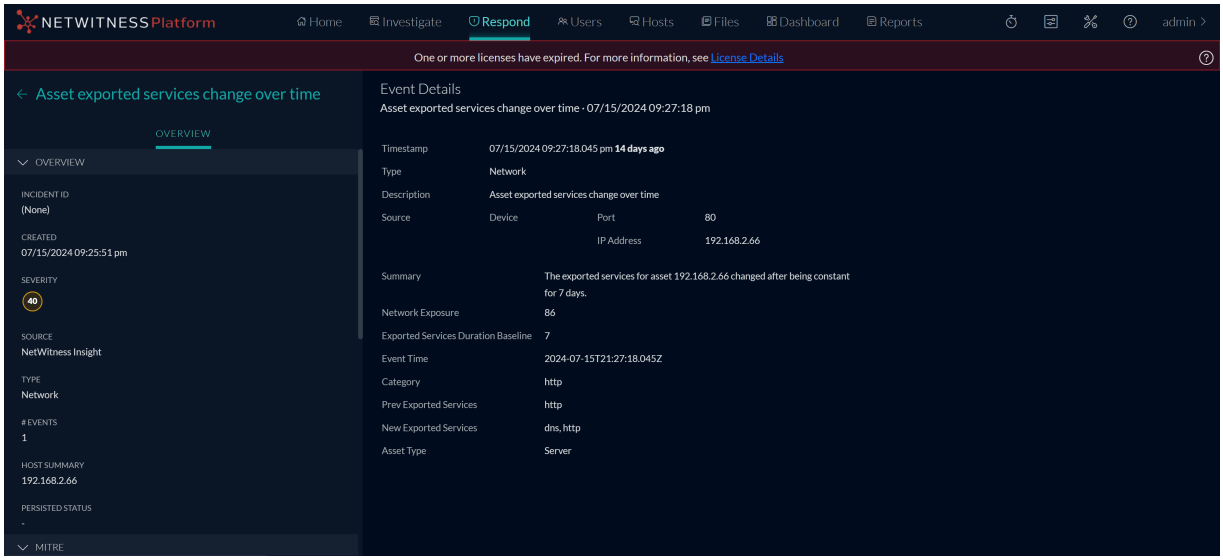
NetWitness führt zwei neue Insight-Warnungen ein, die Ihnen dabei helfen, Änderungen an Ihren Netzwerkressourcen zu überwachen und darauf zu reagieren. Diese Warnungen sind in der Ansicht **Respond** > **Warnmeldungen** verfügbar und basieren auf dem Ressourcentyp und den exportierten Diensten jeder Ressource.

- **Änderung des Ressourcentyps im Laufe der Zeit**: Diese Warnung wird generiert, wenn sich der Typ eines Assets ändert (z. B. von Client zu Server), nachdem derselbe Typ sieben Tage in Folge beobachtet wurde.

- **Änderung der exportierten Ressourcendienste im Laufe der Zeit**: Diese Warnung wird generiert, wenn sich die Anzahl der von einer Ressource exportierten Dienste ändert, nachdem die gleiche Anzahl von Diensten an 7 aufeinander folgenden Tagen beobachtet wurde, selbst wenn die Ressourcenkategorie unverändert bleibt.

  Diese Warnungen helfen Analysten, potenzielle Anomalien oder Bedrohungen in ihrer Umgebung zu identifizieren und zu untersuchen.





Weitere Informationen finden Sie im Abschnitt **NetWitness Insight** im *NetWitness-Dokumentationsportal*.

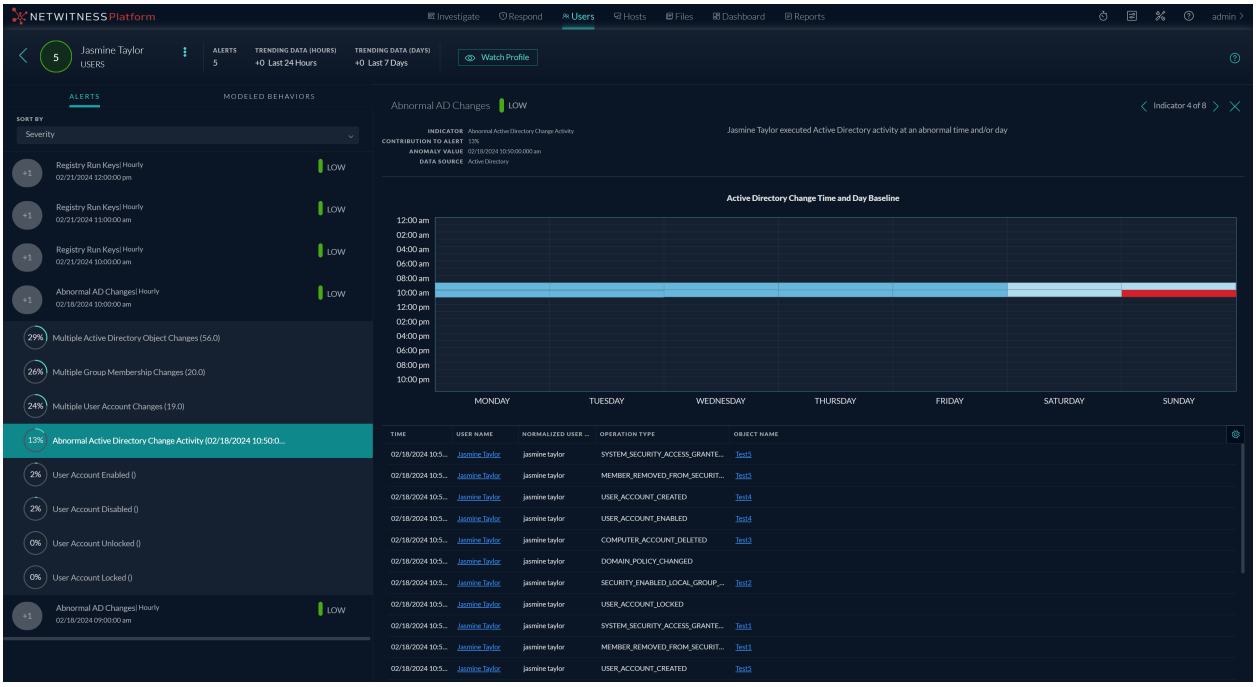
Analyse des Nutzer- und Entitätsverhaltens (UEBA)

Im folgenden Abschnitt werden die neue Erweiterungen der UEBA-Komponente beschrieben:

UEBA-Anomalieerkennung anhand des Wochentags

NetWitness UEBA erweitert seine Funktionen zur Anomalieerkennung durch die Einführung der Wochentag-Funktion. Diese Funktion ermöglicht die Erkennung nicht standardmäßiger Zugriffsmuster, die auf ein kompromittiertes Konto oder eine Insider-Bedrohung hinweisen können. Weicht die Aktivität eines überwachten Benutzers oder einer Netzwerkeinheit an einem bestimmten Wochentag vom üblichen Ausgangswert ab, kennzeichnet UEBA dies als Anomalie, generiert eine Warnung bezüglich nicht standardmäßigen Zugriffs oder nicht standardmäßiger Aktivität und benachrichtigt die Analysten, damit weitere Untersuchungen und Überprüfungen stattfinden können. Weitere Informationen zu den überwachten Aktivitäten, die bei nicht standardmäßigem Zugriff und nicht standardmäßiger Aktivität verfolgt werden, finden Sie im *Benutzerhandbuch zu NetWitness UEBA* unter **Alert Types**.

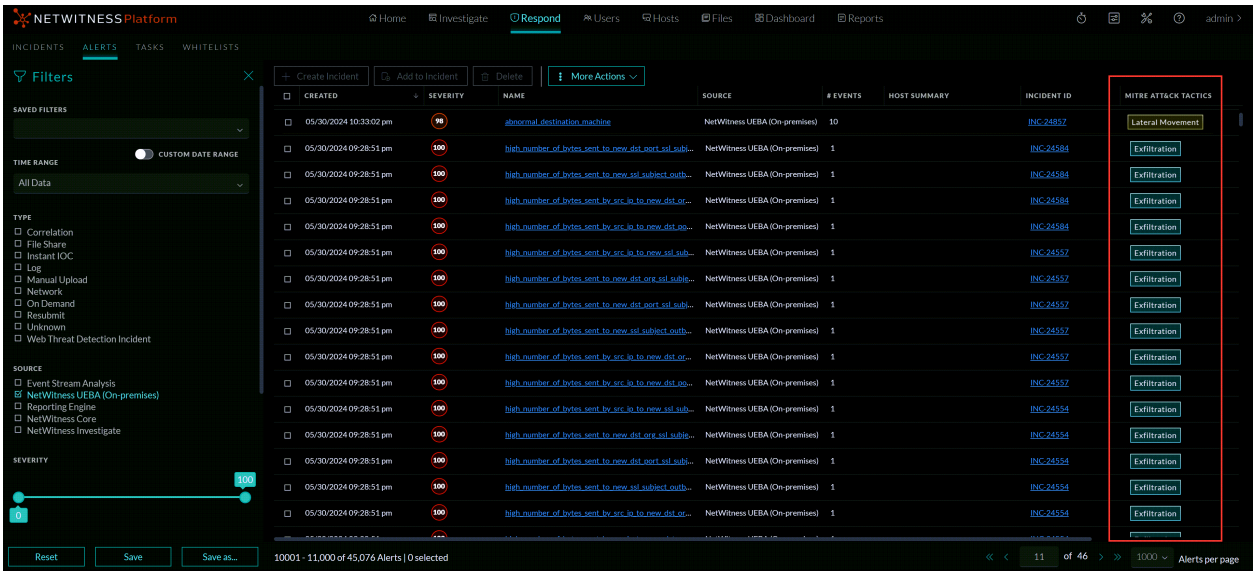
Beispielsweise hat der Benutzer an einem ungewöhnlichen Tag auf das Active Directory zugegriffen. Der Benutzer arbeitet normalerweise von Montag bis Freitag, hat sich jedoch an einem Sonntag angemeldet und Änderungen im Active Directory vorgenommen. Dieses Verhalten wurde von NetWitness UEBA als Anomalie erkannt, basierend auf der Wochentagserweiterung, die darauf hinweist, dass dies ein ungewöhnlicher Tag für diesen Nutzer ist, um Änderungen in AD vorzunehmen. Es wird eine Warnung zur Untersuchung durch die Analysten generiert.



MITRE ATT&CK Mapping für UEBA

NetWitness integriert jetzt die MITRE ATT&CK-Framework-Zuordnung für UEBA-Warnmeldungen und -Vorfälle. Diese Zuordnung hilft Analysten dabei, die möglichen Taktiken, Techniken und Teilprozesse des Angreifers, zu erkennen, die hinter den erkannten Aktivitäten stehen, indem diese mit bekannten Verhaltensweisen korreliert werden. Bei der Untersuchung von UEBA-Warnungen und -Vorfällen wird den Analysten in der Ansicht **Respond** eine Liste der zugeordneten Taktiken und Techniken sowie ein spezieller Bereich **ATT&CK Explorer** mit weiterem Kontext und zugehörigen Informationen angezeigt. Dadurch ist es nicht mehr erforderlich, für ATT&CK-Informationen die MITRE-Website aufzurufen. Diese Verbesserung liefert wertvolle Einblicke in die Schwere und Art der Bedrohung und ermöglicht schnellere und fundiertere Reaktionsentscheidungen.

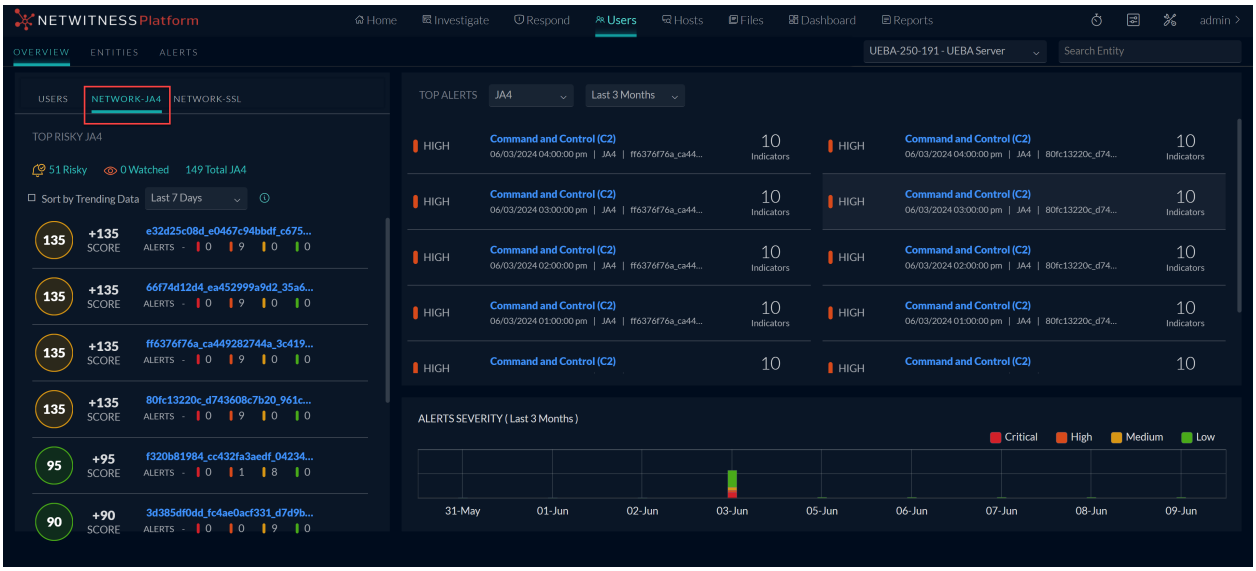
Beispielsweise geht aus einer UEBA-Warnung hervor, dass von einem Benutzerkonto aus ein verdächtiger Remote-Zugriff erfolgt ist. Dieses Verhalten steht im Einklang mit der MITRE ATT&CK-Taktik der **Lateral Movement** und der Technik unter Verwendung von **Remote Services**. Es weist Analysten darauf hin, einen möglichen Versuch zur Datenbeschaffung zu untersuchen und die erforderlichen Maßnahmen zu ergreifen.



Weitere Informationen zur Verwendung des MITRE ATT&CK-Frameworks für UEBA finden Sie im Thema **Use MITRE ATT&CK® Framework** im NetWitness Respond-Benutzerhandbuch zu 12.5.

JA4-Unterstützung in UEBA zur verbesserten Client-Identifizierung und Bedrohungserkennung hinzugefügt

NetWitness hat Unterstützung für den JA4-Fingerabdruck hinzugefügt und ist der Standard für UEBA ab Version 12.5 oder höher. Diese Änderung wird implementiert, da JA4 als die zuverlässigste und verbesserte Methode zur Client-Identifizierung gilt. JA4 nutzt TLS-Client-Hello-Pakete, um anwendungsspezifische Verkehrsmuster zu erkennen und für jede Anwendung eindeutige Fingerabdrücke zu erstellen. Dadurch wird bei modernen Browsern die Gesamtzahl eindeutiger Fingerabdrücke verringert. Folglich hat ein einzelner Client nur einen JA4-Fingerabdruck statt mehrerer, was die Verfolgung und Überwachung erleichtert. Diese Verbesserung von UEBA mit JA4 trägt dazu bei, die Fingerabdrücke von Schadanwendungen zu ermitteln und ermöglicht Analysten, in verschlüsseltem Datenverkehr versteckte Bedrohungen proaktiv zu erkennen und einzudämmen.

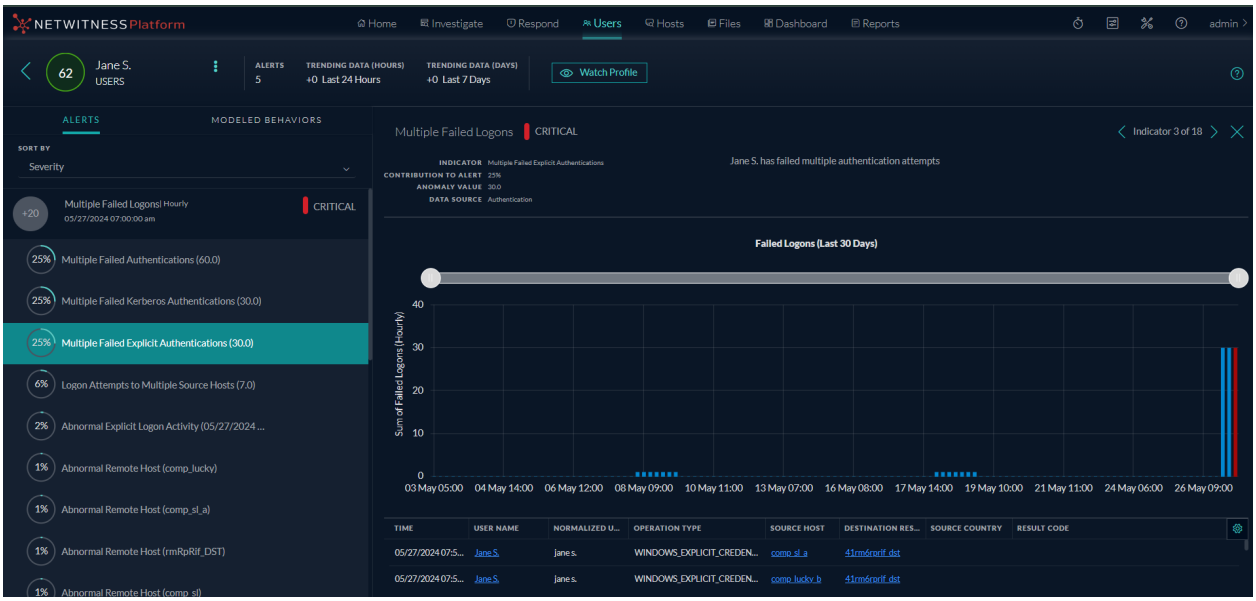


Weitere Informationen zur JA4-Unterstützung finden Sie im NetWitness UEBA-Benutzerhandbuch zu 12.5.

Verbesserter UEBA zur Erkennung von Kerberos und expliziter Anmeldeaktivität

Die Erkennungsfunktionen von NetWitness UEBA für Anmeldeaktivitäten wurden durch die Einführung von zwei neuen Indikatoren und modellierten Verhaltensweisen speziell für **Kerberos** und **explizite** Anmeldungen verbessert. Diese Verbesserung ermöglicht eine präzisere Unterscheidung zwischen verschiedenen Anmeldeereignissen in Ihrer Umgebung und reduziert Fehlalarme und Inkonsistenzen im Zusammenhang mit Kerberos- und expliziten Anmeldeaktivitäten erheblich. Durch die Trennung dieser Anmeldetypen können Analysten abnormales Anmeldeverhalten effektiver erkennen und die Umgebung vor möglichen Bedrohungen schützen. Diese neuen Indikatoren erlauben tiefere Einblicke in Anmeldeaktivitäten und helfen Analysten dabei, verdächtiges oder kriminelles Verhalten effektiv zu überwachen und zu untersuchen.

So kann beispielsweise die Warnung **Mehrere fehlgeschlagene Anmeldungen** ausgelöst werden, wenn eine anomale Aktivität für mehrere fehlgeschlagene Authentifizierungsversuche sowohl bei **Kerberos**- als auch bei **expliziten Anmeldeaktivitäten** festgestellt wird.



Weitere Informationen finden Sie im NetWitness UEBA-Benutzerhandbuch zu 12.5 unter dem Punkt **NetWitness UEBA-Anwendungsfälle** im Abschnitt **Anmeldeaktivitätsindikatoren**.

SASE-Merkmale

Im folgenden Abschnitt wird die neue Erweiterung für SASE beschrieben:

NetWitness SASE-Integration mit Netskope (privater Vorschaumodus)

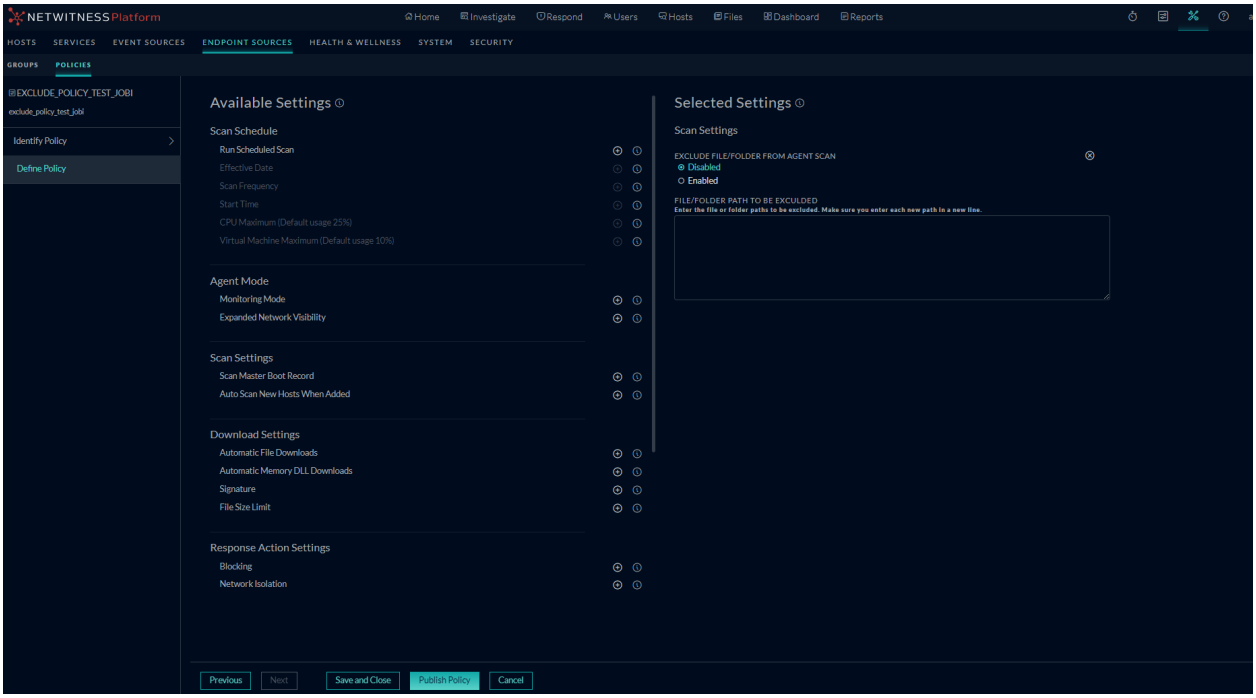
Die neue NetWitness-Integration mit Netskope SASE sorgt für vollständige Transparenz in Bezug auf Netzwerke und Protokolle. Mit dieser benutzerdefinierten technischen Integration erhalten NetWitness-Nutzer und -Nutzerinnen Einblick in das Verhalten und die Kommunikation zwischen Geräten und Services in Remote-Netzwerken und verteilten Netzwerken in On-Premise-, Hybrid- und Cloud-Bereitstellungen. Die NetWitness-Netskope SASE-Integration ermöglicht es Kunden, die SASE-Flexibilität und die damit verbundenen Sicherheitsvorteile zu nutzen und gleichzeitig vollständige Transparenz für Bedrohungserkennung und -abwehr zu erhalten. In der Version 12.5 befindet sich die NetWitness SASE-Integration mit Netskope im privaten Vorschaumodus.

Endpoint

Im folgenden Abschnitt werden die neuen Verbesserungen an der Endpoint-Komponente beschrieben.

Ausschluss bestimmter Dateien und Ordner von vollständigen Systemscans durch den Agenten

Sie können die NetWitness Platform so konfigurieren, dass bestimmte Dateien und Ordner von den vollständigen System-Scans des NetWitness Endpoint Agent ausgeschlossen werden. Wenn Sie Dateien oder Ordner ausschließen, ignoriert der NetWitness Endpoint Agent diese beim Scannen auf Sicherheitsrisiken. Wenn Sie große Dateien und Ordner ausschließen, stellen Sie möglicherweise fest, dass die Scanzeit des Endpoint Agent verkürzt wird. Wenn Sie eine Datei oder einen Ordner von den Scans des NetWitness Endpoint Agent ausschließen, verringert sich das Schutzlevel der Hosts in Ihrem Netzwerk. Diese Option sollte nur verwendet werden, wenn ein konkreter Bedarf besteht und Sie sicher sind, dass die Elemente nicht infiziert sind. Sie können nur Dateien und Ordner von einem vollständigen Systemscan ausschließen.



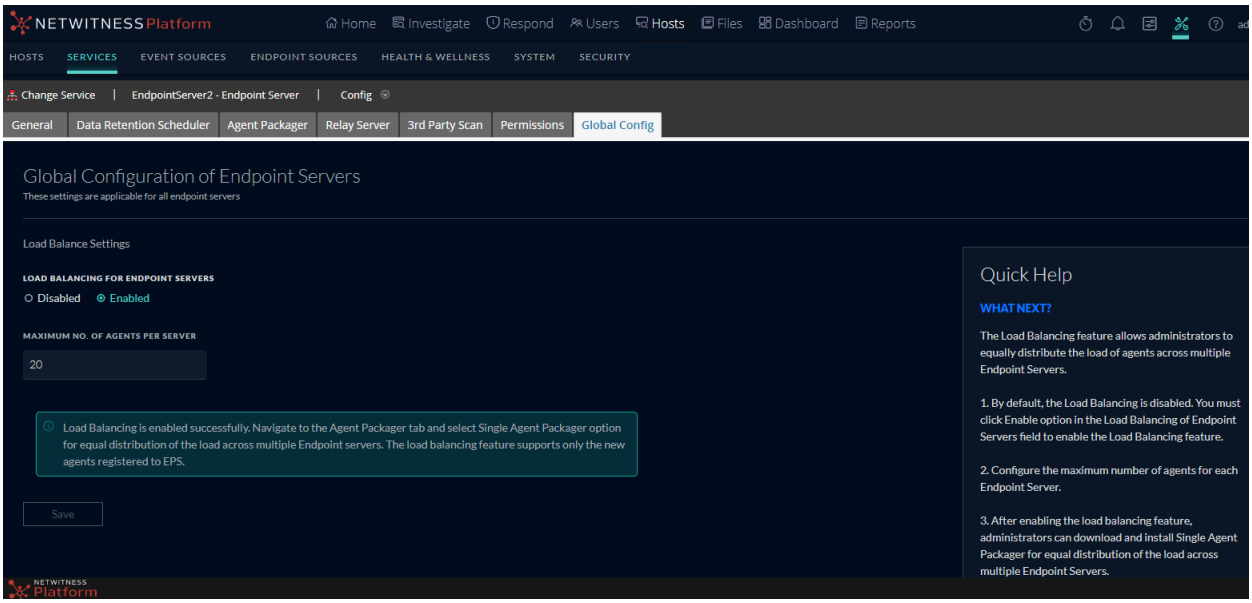
Weitere Informationen darüber, wie Sie Dateien und Ordner vom vollständigen Systemscan von NetWitness Agent ausschließen können, finden Sie im Konfigurationsleitfaden für NetWitness Endpoint.

Leistungsoptimierung: Lastausgleichsfunktionen in Endpoint-Servern

Mit der neu eingeführten Lastenausgleichsfunktion können Administratoren die Last der Agents gleichmäßig auf die Endpunktserver in der Umgebung verteilen.

Wenn Unternehmen größer werden, steigt die Notwendigkeit, neue Agents für Bereitstellungen hinzuzufügen, und die Verteilung von Agents auf Endpoint-Server wird schwierig. Administratoren müssen für jeden Endpunktserver einen anderen Packager herunterladen und die Last mit Hilfe von Policys entsprechend den Bedingungen verteilen. Dank der Lastausgleichsfunktion müssen Kunden nur einen Agent-Packager herunterladen und ihn an alle Endpunkt-Agenten übertragen. Je nach der festgelegten Last und den Parametern werden die Agents gleichmäßig auf die Endpoint-Server verteilt.

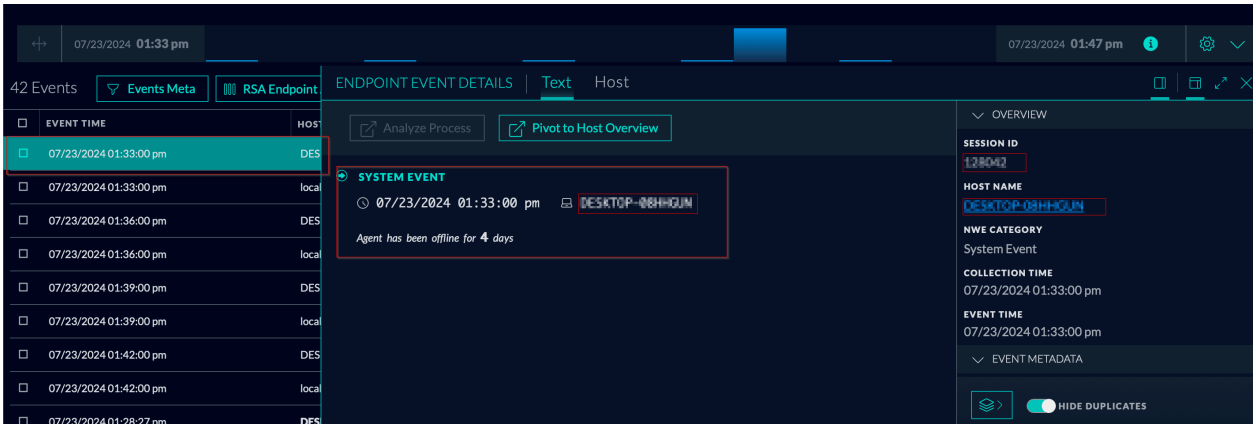
Durch die Implementierung eines Lastenausgleichs können Unternehmen eine effiziente Skalierung ihrer Bereitstellung sicherstellen. Dadurch wird das Risiko einer Überlastung einzelner Endpunktserver verringert und eine optimale Leistung im gesamten Netzwerk aufrechterhalten. Um die Lastausgleichsfunktion nutzen zu können, müssen Sie den Lastausgleich aktivieren.



Weitere Informationen zum Lastenausgleich finden Sie im *NetWitness Endpoint-Benutzerhandbuch* unter den Punkten „Informationen zum Lastenausgleich“ und „Lastenausgleich aktivieren“.

Möglichkeit zur Überwachung der Details zum letzten Aktivitätsstatus von Endpunkt-Agents

Mithilfe der NetWitness Platform können Administratoren und Analysten regelmäßig Berichte mit detaillierten Angaben zur Anzahl der Endpunkt-Agenten erstellen, die sich über eine bestimmte Anzahl von Tagen nicht gemeldet haben. Auf diese Weise werden Compliance und Governance im Unternehmen sichergestellt. Wenn man weiß, wann der Endpunkt-Agent zuletzt aktiv war, erhält man Einblicke in die Gesamtleistung der Endgeräte. Die Überwachung des „Zuletzt gesehen“-Status der Endpunkt-Agenten ist von entscheidender Bedeutung für die Gewährleistung von Sicherheit, Compliance, Betriebseffizienz und effektiver Ressourcenverwaltung innerhalb einer Organisation.



Weitere Informationen finden Sie im NetWitness Endpoint-Benutzerhandbuch unter „Monitor Endpoint Agents' Last-seen Details“.

Unterstützte Betriebssystemverbesserungen

Administratoren haben die Möglichkeit, Endpunkt-Agents unter den folgenden Versionen des Windows-Betriebssystems bereitzustellen:

- **Windows 11 (bis Version 23H2)**

Weitere Informationen finden Sie im *NetWitness Endpoint Agent-Installationshandbuch* unter **Introduction to Endpoint Agent Installation**.

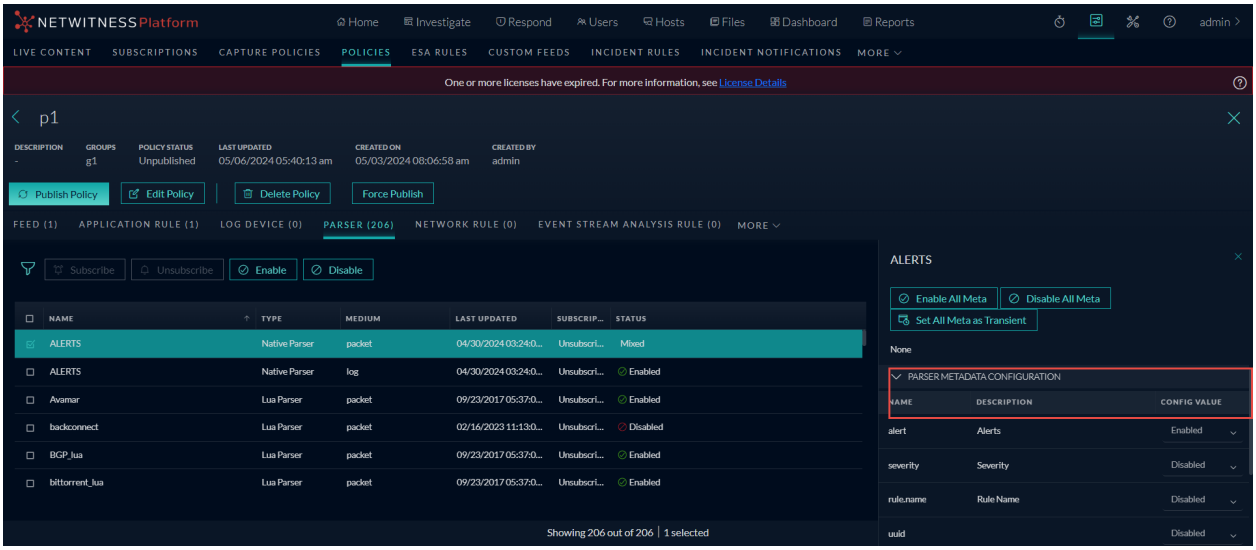
Policy-basiertes zentralisiertes Contentmanagement (CCM)

Die folgenden Verbesserungen wurden beim CCM in der Version 12.5.0.0 vorgenommen:

Unterstützung für native Parser

Parser-Metadatenkonfiguration anzeigen

Die Ansicht **Policy-Details** > **Parser** wurde erweitert, um die **Parser-Metadaten-Konfiguration** auf der rechten Seite anzuzeigen, die alle Metadaten für den ausgewählten Parser enthält.



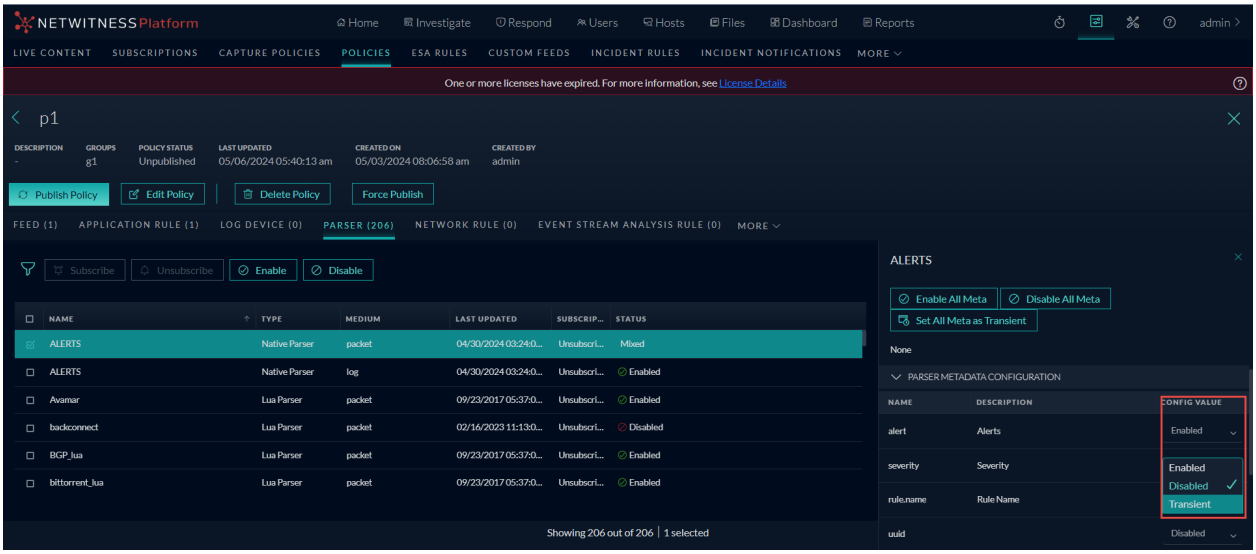
Weitere Informationen finden Sie im Thema **Anzeigen einer Richtlinie** im *Leitfaden zum Policy-basierten zentralisierten Contentmanagement*.

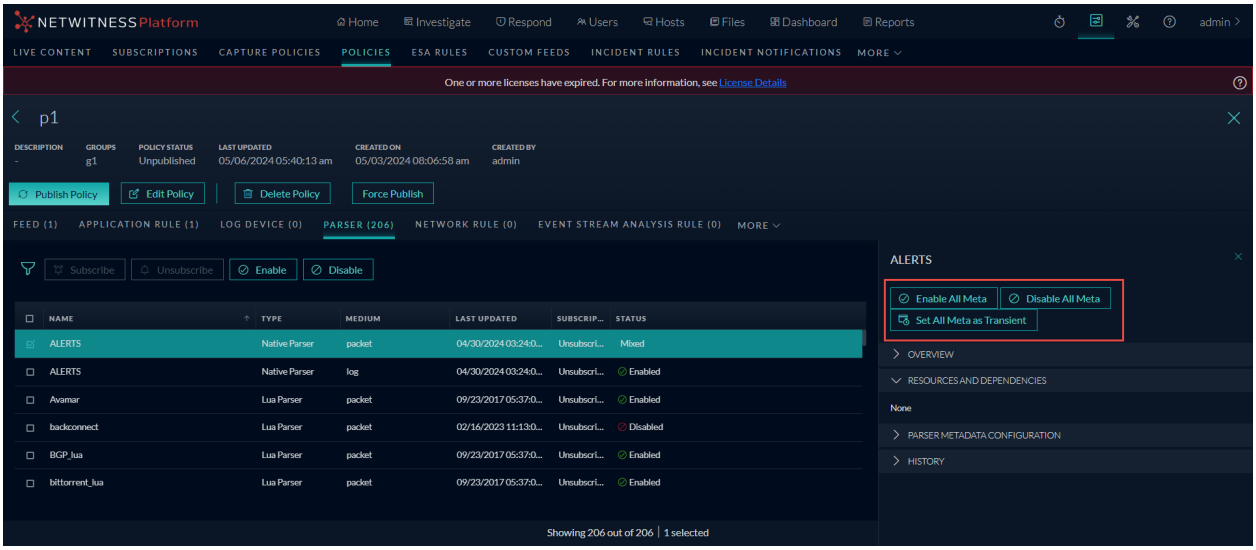
Parser-Metadaten aktivieren oder deaktivieren

Die Ansicht **Policy-Details** > **Parser** wurde erweitert, um bestimmte Parser-Metadaten zu aktivieren oder zu deaktivieren, sodass Sie entscheiden können, ob Sie native Parser verwenden möchten oder nicht. Sie können Folgendes tun:

- Alle Metadaten aktivieren
- Alle Metadaten deaktivieren

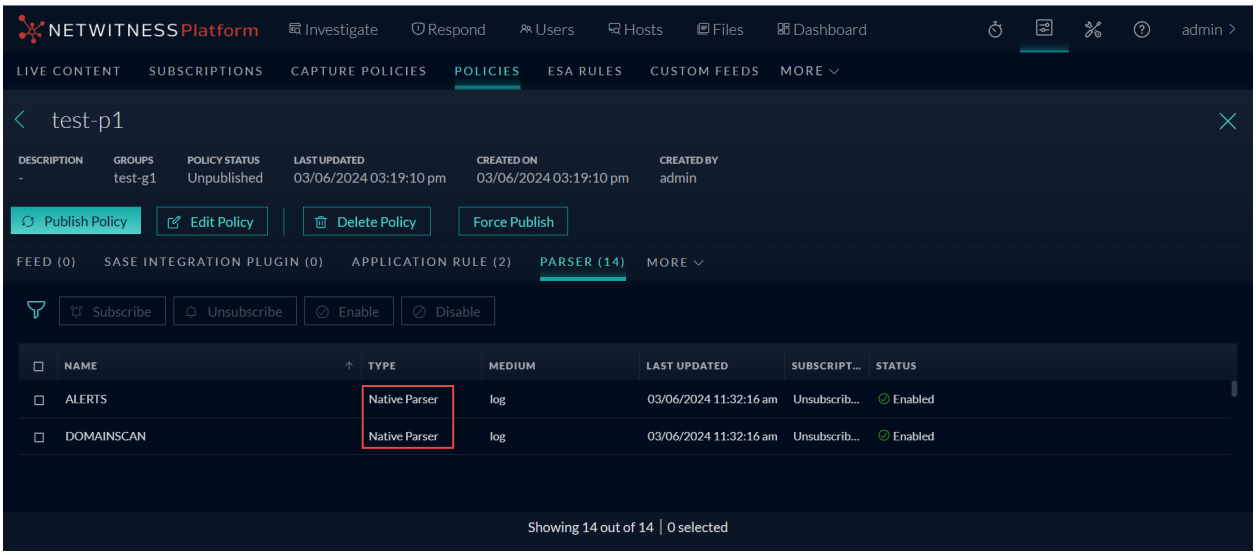
- Alle Metadaten als vorübergehend festlegen
- Individuelle Metadaten aktivieren
- Einzelne Metadaten deaktivieren
- Individuelle Metadaten als vorübergehend festlegen





Anzeigen nativer Parser, die für Dienste aktiviert und an Richtlinien angehängt sind

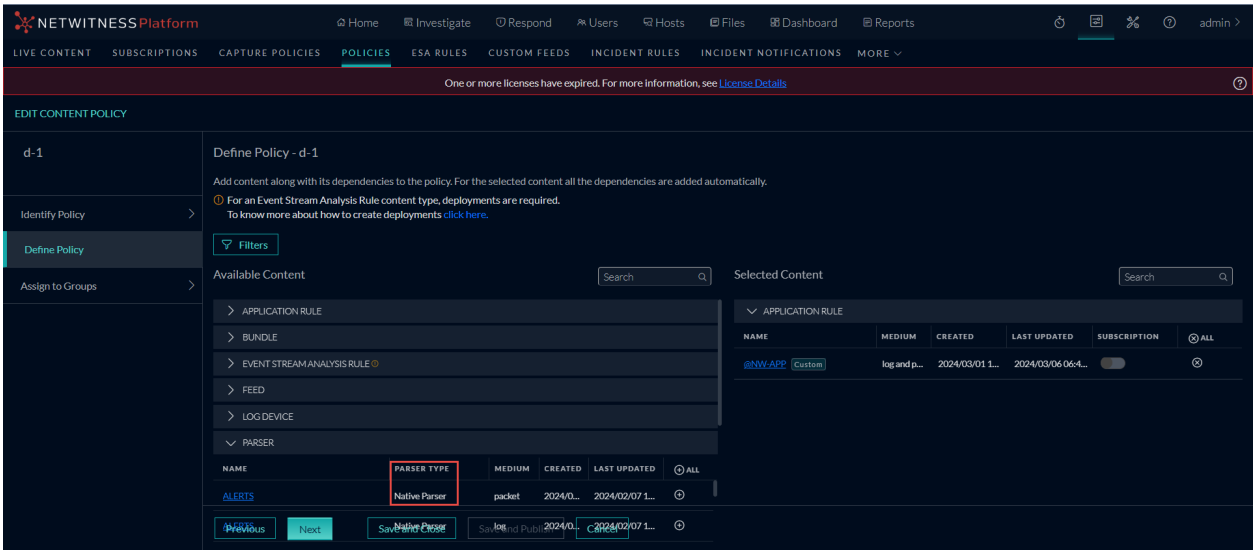
Sie können die für Dienste aktivierten und einer Richtlinie zugeordneten nativen Parser problemlos anzeigen, da sie automatisch auf der Seite **Richtliniendetails** angezeigt werden.



Weitere Informationen finden Sie im Thema **Anzeigen einer Richtlinie** im *Leitfaden zum Policy-basierten zentralisierten Contentmanagement*.

Beim Erstellen einer Richtlinie zwischen nativen Parsern und LUA-Parsern unterscheiden

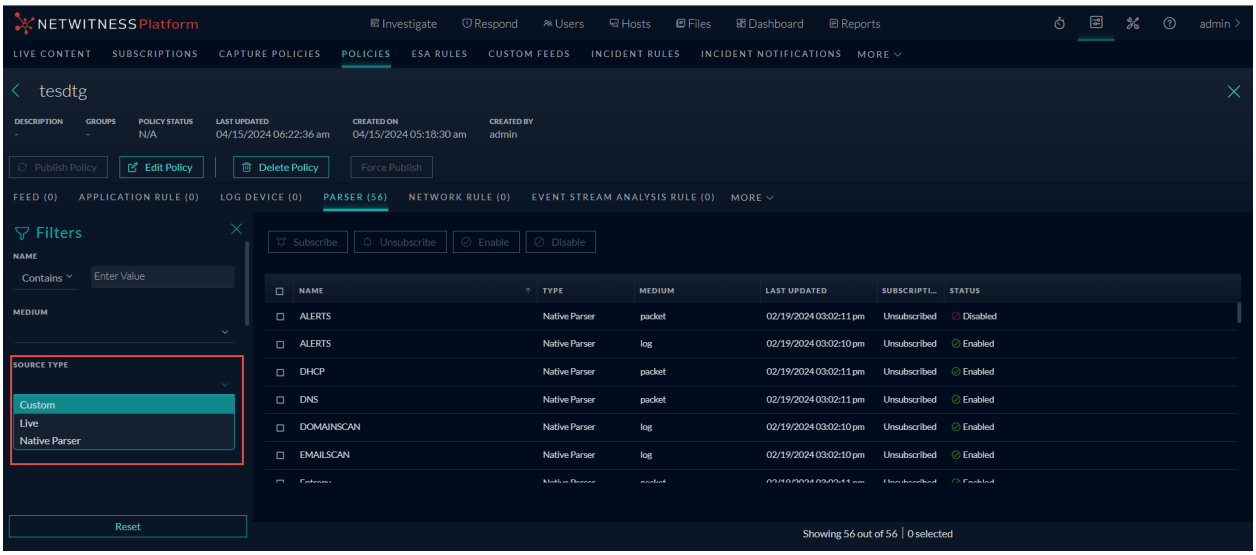
Auf der Seite **Policy erstellen** oder **Policy bearbeiten** wird eine unterscheidbare Kennung für den nativen Parser erstellt, damit Sie beim Erstellen einer Policy zwischen dem nativen Parser und dem LUA-Parser unterscheiden können.



Weitere Informationen finden Sie im Thema **Create and Publish Policies** im *Leitfaden zum Policy-basierten zentralisierten Contentmanagement*.

Native Parser filtern

Sie können die nativen Parser auf den Seiten **Policy erstellen**, **Policy bearbeiten** und **Policy-Details** filtern, sodass Sie die für die Policy erforderlichen nativen Parser einfach auswählen oder anzeigen können. Dadurch wird der Prozess optimiert und Sie können beim Erstellen oder Ändern von Richtlinien problemlos native Parser hinzufügen oder entfernen.



Weitere Informationen finden Sie im Thema **Create and Publish Policies** im *Leitfaden zum Policy-basierten zentralisierten Contentmanagement*.

Concentrator-, Decoder-, Log Collector- und Archiver-Services

Die folgenden Verbesserungen wurden für Concentrator-, Decoder-, Log Collector- und Archiver-Services in der Version 12.5.0.0 vorgenommen:

Einführung in JA4 TLS Fingerprinting

JA4 identifiziert anwendungsspezifische Verkehrsmuster durch Analyse der TLS-Handshake-Verhandlungen (Client Hello) und verbessert so die UEBA-Bedrohungserkennungsfunktionen.

Weitere Informationen finden Sie im *Decoder-Konfigurationshandbuch* unter **Support für die JA4-Entität für UEBA**.

Logstash-Ereignisquellen

Einführung der Unterstützung für das NetWitness JDBC Logstash Input-Plugin zum Sammeln von Protokollen aus MSSQL-, IBMDB2- und Oracle-Datenbanken.

Weitere Informationen finden Sie im Thema **Configure Logstash Event Sources in NetWitness** im *Leitfaden für die Protokollsammlung*.

Erweiterte Metadaten

Eine optionale Konfiguration zum Erhöhen der Länge der Werte, die in der Metadatenbank gespeichert werden können, um eine höhere Genauigkeit bei bestimmten Anwendungsfällen zu erreichen, die Übereinstimmungen mit langen Zeichenfolgen erfordern.

Extended Meta bietet eine Möglichkeit, bestimmte Metaschlüssel selektiv zu konfigurieren, um Werte größer als 256 Bytes zu unterstützen. Mit dieser Funktion können Metawerte, die zuvor auf die 256-Byte-Grenze gekürzt wurden, jetzt auf eine Länge von bis zu 4.096 Byte erweitert werden.

Weitere Informationen finden Sie in den Richtlinien für erweiterte Metadaten, die im *NetWitness Extended Meta User Guide for 12.5* erwähnt werden.

Anwendungsregelverfolgung

Zählt, wie oft eine Anwendungsregel erfüllt wird, und bietet die Möglichkeit, den Zähler zur Fehlerbehebung zurückzusetzen.

Weitere Informationen finden Sie im *API-Handbuch für 12.5*.

Protokollintegrationen

NetWitness Platform unterstützt die Integration der folgenden Ereignisquellen zum Sammeln und Analysieren von Protokollen. Sofern nicht anders angegeben, werden diese Services in NetWitness Platform 12.2.0.0 oder höher unterstützt.

- Amazon AWS CloudWatch
- Okta Workforce Identity Cloud

Weitere Informationen zur Integration der Parser-Services finden Sie im NetWitness Platform – Integrationshandbuch.

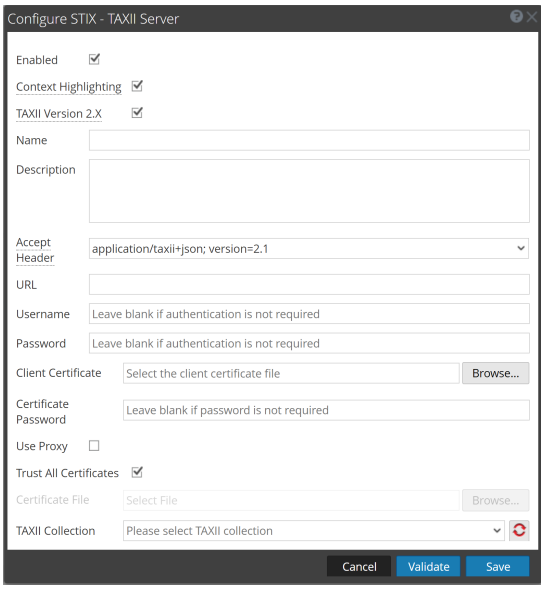
Context Hub

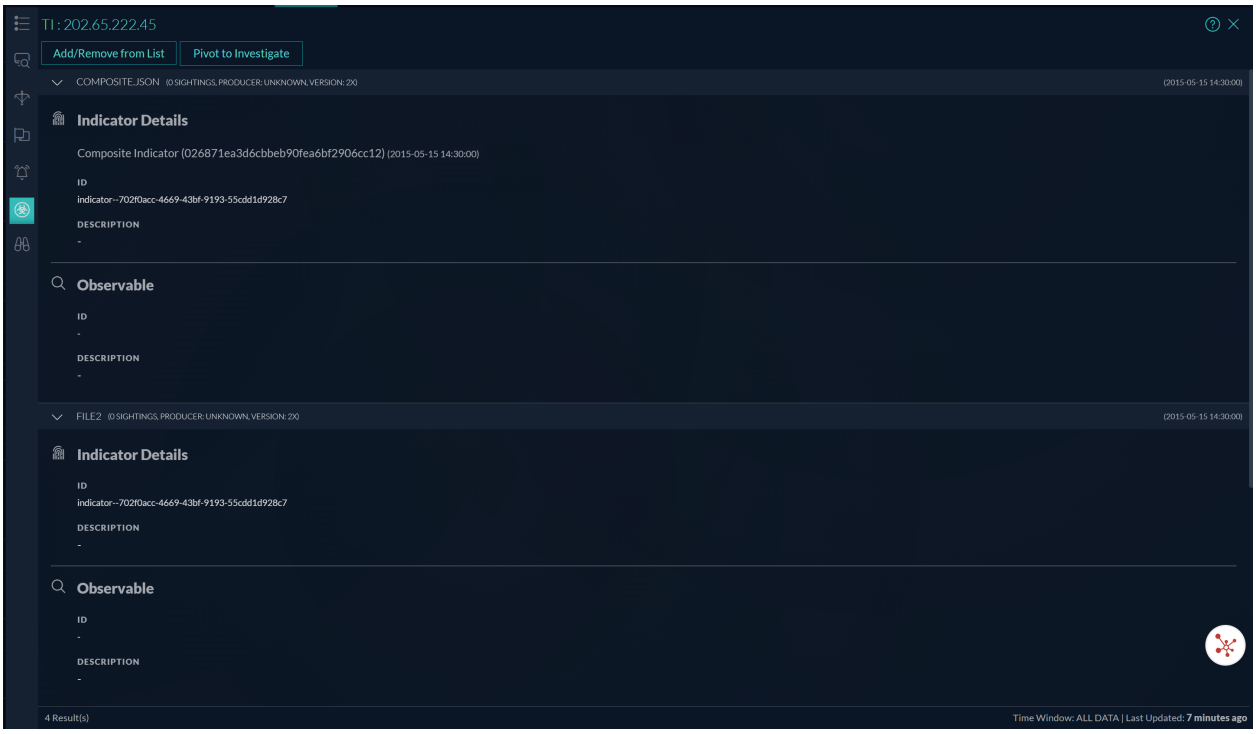
Der folgende Abschnitt beschreibt die neuen Verbesserungen an der Context Hub-Komponente:

Verbesserte Threat Intelligence mit STIX 2.x-Integration

NetWitness hat seine Funktionen zur Bedrohungserkennung und Sicherheitsüberwachung durch die Integration der Unterstützung für STIX 2.x-Feeds, einschließlich der Versionen 2.0 und 2.1, verbessert. Administratoren können File-, REST- und TAXII-Server jetzt mit STIX 2.x (JSON-Format) als Datenquellenindikatoren für Context Hub konfigurieren. Diese Erweiterung ermöglicht Ihnen die Erstellung benutzerdefinierter Feeds mit STIX 2.x-Datenquellen. Die NetWitness-Plattform analysiert Daten im Hintergrund, um wertvolle Bedrohungsinformationen zu extrahieren und bösartige Muster zu erkennen. Sie bietet durch die Kontextsuche auf den Seiten **Untersuchen** und **Reagieren** einen erweiterten Kontext und hilft Analysten dabei, Untersuchungen effektiver durchzuführen.

Diese Verbesserung vereinfacht die Nutzung strukturierter Bedrohungsinformationen, indem viele bisherige Einschränkungen beseitigt werden und eine aussagekräftigere und effektivere Meldung von Sichtungen ermöglicht wird. Diese Integration beinhaltet die Konvertierung strukturierter Bedrohungsinformationen vom STIX-Format in ein Format, das das SIEM-System leicht verstehen und verwenden kann. Dadurch wird seine Wirksamkeit beim Schutz vor Bedrohungen verbessert.





Weitere Informationen finden Sie im Context Hub-Konfigurationsleitfaden unter **Konfigurieren von STIX als Datenquelle**.

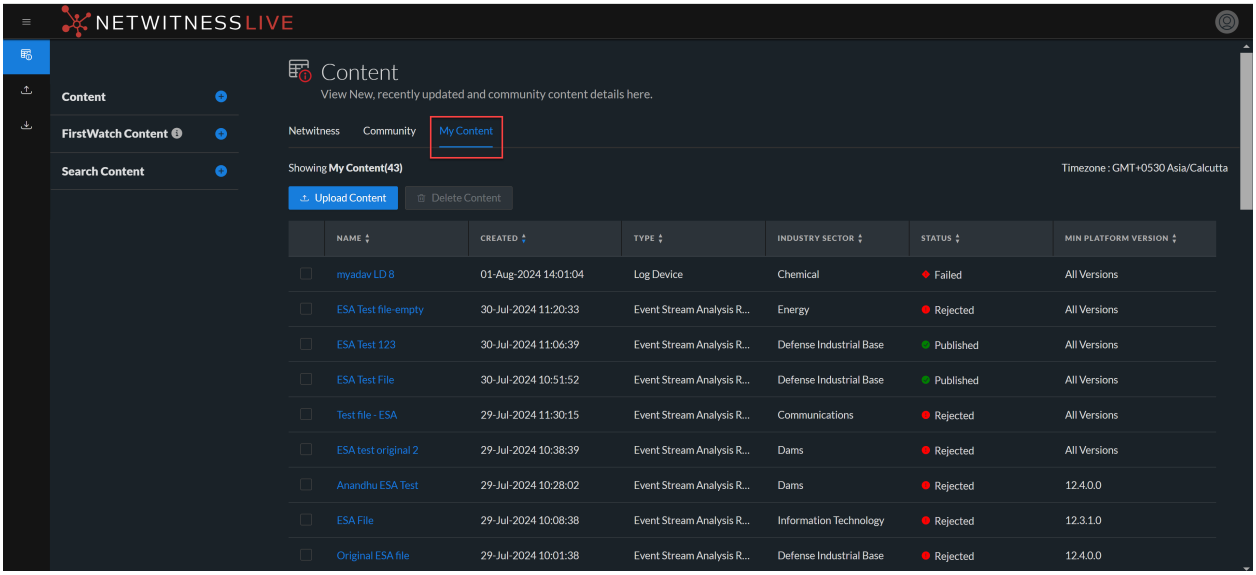
Live-Cloudservice

Im folgenden Abschnitt werden die neuen Verbesserungen an der Live-Cloudservice-Komponente beschrieben:

Benutzerdefinierte Community-Inhalte auf NetWitness Live handhaben

NetWitness führt die neue Funktion „Mein Inhalt“ ein, mit der Benutzer benutzerdefinierte Inhalte nahtlos direkt über die NetWitness Live-Benutzeroberfläche verwalten können. Hierzu gehört das Hochladen, Löschen und Herunterladen von benutzererstellten Inhalten wie Protokollgeräten, Regeln für die Ereignisstromanalyse, Parsern, Feeds usw. Diese Funktion bietet Benutzern eine effizientere Möglichkeit, nützliche und relevante benutzerdefinierte Inhalte unter anderen Benutzern auszutauschen, wodurch der Zeit- und Arbeitsaufwand für die Veröffentlichung von Inhalten durch Inhaltsveröffentlichungsteams reduziert wird. Benutzer können aus einer Reihe von Inhaltsoptionen wählen, die ihren Anforderungen und Anwendungsfällen entsprechen.

Hinweis: Die Funktion „Mein Inhalt“ von NetWitness Live unterstützt in dieser Version nur Log Device- und ESA-Inhalte.



Weitere Informationen finden Sie im Thema **Benutzerdefinierte Inhalte verwalten** im NetWitness Live Services Management Guide.

Sicherheitsupdates

Behebt die neuesten Sicherheitslücken, die für verschiedene von der NetWitness Platform verwendete Bibliotheken gemeldet wurden, darunter eine kritische (CVE-2016-1000027), 35 schwerwiegende, 103 moderate und 16 geringfügige Sicherheitslücken.

Weitere Informationen zu Sicherheitskorrekturen finden Sie unter https://community.netwitness.com/t5/netwitness-platform-advisories/ct-p/netwitness-advisories#security.

Upgradepfade

Die folgenden Upgradepfade werden für NetWitness 12.5.0.0 unterstützt:

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

Weitere Informationen zum Upgrade auf 12.5.0.0 finden Sie unter Upgrade-Leitfaden für NetWitness 12.5.0.0

WICHTIG: NetWitness rät Nutzern, ihre Softwareversionen zu überprüfen und weist darauf hin, dass die Versionen bis 12.2 am 31. März 2024 das Ende der Nutzungsdauer erreicht haben. Weitere Informationen finden Sie unter https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875. NetWitness empfiehlt, ein Upgrade auf Version 12.5 durchzuführen, um die neuesten Funktionen und Sicherheitsupdates nutzen zu können.

WICHTIG: Wenn Sie ein Upgrade von den Versionen 11.7.x (Service Packs) oder 11.7.x.x (Patches) auf die Version 12.5.0.0 durchführen möchten, müssen Sie zunächst ein Upgrade auf die Version 12.2.0.0 oder 12.3.0.0 durchführen, bevor Sie auf 12.5 aktualisieren.

WICHTIG: Der Warehouse Connector verwendet eine Lockbox, um Anmeldeinformationen für Datenintegrationsquellen und -ziele sicher zu speichern. Nutzer, die von früheren Versionen auf die Version 12.5 aktualisieren, können die konfigurierten Streams jedoch nicht starten, ohne ihre vorhandenen Anmeldeinformationen in die neue Lockbox zu migrieren. Daher müssen Nutzer manuell einen neuen Lockbox-Schlüssel erstellen und dann, sofern zutreffend, das Kennwort für ihre im Warehouse Connector konfigurierten Quellen und Ziele aktualisieren. Ausführliche Anweisungen zum Erstellen des neuen Lockbox-Schlüssels finden Sie im Abschnitt **Warehouse Connector** unter den **Aufgaben nach dem Upgrade** im Upgrade-Leitfaden für NetWitness 12.5.0.0.

Lebenszyklus der Produktversion von NetWitness Platform

Eine Liste der Versionen, die das Ende des Primärsupports (EOPS) erreichen, finden Sie unter Produktversionslebenszyklus von NetWitness Platform.

Neuerungen in früheren Versionen

Der Abschnitt enthält neue Funktionen und Verbesserungen für alle unterstützten Vorgängerversionen.

Weitere Informationen finden Sie unter https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-12-x/ta-p/695650.

In Version 12.5.0.0 behobene Probleme

In diesem Abschnitt werden in der Version 12.5.0.0 behobene Probleme aufgeführt.

Weitere Informationen zu behobenen Problemen finden Sie in der Spalte „Behobene Version“ in der Liste bekannter Probleme in NetWitness® Platform (https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872) im NetWitness Community Portal.

Endpunkt-Fixes

Rückverfolgungsnummer	Beschreibung
SACE-21629	Der Polling-Mechanismus auf dem Endpoint-Server hat bei der Überprüfung der Nachrichtenwarteschlange des Relay-Servers aufgrund eines übermäßigen Timeout-Limits nicht wie erwartet geendet.

Fehlerbehebungen für die Startseite

Rückverfolgungsnummer	Beschreibung
ASOC-148336	Die Nutzer können jetzt in den Benutzereinstellungen „Startseite“ als Standard-Landingpage auswählen, ohne dass ein leerer Bildschirm angezeigt wird.

Problembehebungen in der Plattform

Rückverfolgungsnummer	Beschreibung
ASOC-146908	Während des Upgrades kann der Host nicht in den el8-Kernel booten, nachdem die Betriebssystemmigration abgeschlossen ist.

Decoder-Korrekturen

Rückverfolgungsnummer	Beschreibung
ASOC-147188	Bei der Ausführung des optionalen Prune-Befehls als Teil der DPDK-Migration werden in den Protokollen fortlaufend Fehlermeldungen zu einigen Schnittstellen angezeigt.
ASOC-144467	Beim Neuladen des Hosted-Plug-ins wird die Plug-in-Instanz gelöscht, anstatt sie aus dem Decoder/der Hosted-Struktur neu zu laden.
ASOC-154781	Das Decoder-Upgrade auf 12.4.x füllt die Partition /var/netwitness/decoder schließlich mit Parsestatdb-Daten.

Bekannte Probleme in Version 12.5.0.0

Probleme, die in dieser Version weiterhin ungelöst sind, sind in der Liste der bekannten Probleme der NetWitness® Platform im NetWitness-Community-Portal dokumentiert:
https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872

Build-Nummern für 12.5.0.0-Komponenten

Die folgende Tabelle enthält die Build-Nummern für die verschiedenen Komponenten von NetWitness Platform 12.5.0.0.

Komponente	Versionsnummer
NetWitness Admin-Server	rsa-nw-admin-server-12.5.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm
NetWitness Inhalte zu erweiterten Analysen	rsa-nw-advanced-analytics-content-12.5.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm
NetWitness Erweiterter Analyseserver	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-Plugin	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 Bootstrap	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-Service	rsa-nw-cloud-connector-server-12.5.0.0-240116135943.5.4220688.el8.alma.noarch.rpm
NetWitness Cloud-Link-Server	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 Beschreibung der Komponente	rsa-nw-Komponentendeskriptor-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 Konfigurationsmanagement	rsa-nw-config-management-12.5.0.0-2402050947.5.b7e9f64.el8.noarch.rpm
NetWitness Konfigurationsserver	rsa-nw-config-server-12.5.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm
NetWitness Konsole	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 Korrelationsserver (ESA)	rsa-nw-correlation-server-12.5.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm
NetWitness Dashboard-Inhalt	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-Analyseinhalte	rsa-nw-decoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Decoder-Content	rsa-nw-decodercontent-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Bereitstellung-Upgrade	rsa-nw-deployment-upgrade-12.5.0.0-2402150604.5.dbd95e3.el8.noarch.rpm
NetWitness Endpoint-Agents	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 Endpunkt-Decoder-Analyseinhalte	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 Integrationsserver	rsa-nw-integration-server-12.5.0.0-240117101347.5.0ed5cc33.el8.alma.noarch.rpm
NetWitness Investigate 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-Inhalte	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 Tools	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-Analyseinhalte	rsa-nw-logdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Log Decoder-Basisinhalte	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-Exportdienstprogramm	rsa-nw-metaexport-utility-12.5.0.0-110124.5.el8.x86_64.rpm
NetWitness Server für Messwerte	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 Orchestrierungs-CLI	rsa-nw-orchestration-cli-12.5.0.0-2401091103.5.7317baa.el8.noarch.rpm
NetWitness Orchestrierungsserver	rsa-nw-orchestration-server-12.5.0.0-240119064852.5.a87bb81f.el8.alma.noarch.rpm
NetWitness Platzhalter	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-Konfigurationsserver	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-Ausgabe	rsa-nw-presidio-output-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio-Benutzeroberfläche	rsa-nw-presidio-ui-12.5.0.0-2402270745.5.0844250.el8.noarch.rpm

NetWitness Protobufs	rsa-protobufs-rt-12.5.0.0-928.5.6254aabd8.el8.x86_64.rpm
NetWitness Wiederherstellungstools	rsa-nw-recovery-tool-12.5.0.0-2401230435.5.f34a9fd.el8.noarch.rpm
NetWitness Relay-Server	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-Antwortserver	rsa-nw-respond-server-12.5.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm
NetWitness Antwortaktionsserver	rsa-nw-response-actions-server-12.5.0.0-240116034125.5.0af5d71.el8.alma.noarch.rpm
NetWitness Root-CA-Update	rsa-nw-root-ca-update-12.5.0.0-2401221231.5.96cd15b.el8.noarch.rpm
NetWitness SA-Tools	rsa-sa-tools-12.5.0.0-2401251338.5.89600eb.el8.noarch.rpm
NetWitness Sicherheits-CLI	rsa-nw-security-cli-12.5.0.0-2401091103.5.18ab320.el8.noarch.rpm
NetWitness Sicherheitsserver	rsa-nw-security-server-12.5.0.0-240123034132.5.11d93f41.el8.alma.noarch.rpm
NetWitness Shell	rsa-nw-shell-12.5.0.0-240108140410.5.0b0d73f5.el8.alma.noarch.rpm
NetWitness SOS-Berichts-Plugins	rsa-nw-sosreport-plugins-12.5.0.0-2401162235.5.af21a76.el8.noarch.rpm
NetWitness SMS-Laufzeit 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 Quellserver	rsa-nw-source-server-12.5.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm
NetWitness Quellserverinhalt	rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm
NetWitness Benutzeroberfläche	rsa-nw-ui-12.5.0.0-240131063757.5.d1b137ecbc.el8.alma.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-12.4.5.0-12866.5.1aefe557c.el8.x86_64.rpm

Hilfe zu NetWitness Platform

Produktdokumentation

Die folgende Dokumentation ist im Lieferumfang der Version enthalten.

Dokumentation	Standort-URL
NetWitness Platform – Masterinhaltsverzeichnis	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.5.0.0 Produktdokumentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
Leitfaden zum Upgrade auf NetWitness Platform 12.5.0.0	https://community.netwitness.com/t5/rsa-netwitness-platform-staged/upgrade-guide-for-12-4/ta-p/709308
NetWitness Analytics in der Cloud	Weitere Informationen zu neuen Funktionen und Verbesserungen in Versionen von NetWitness Analytics in der Cloud finden Sie im folgenden Abschnitt „Neuheiten“: Informationen zu UEBA Cloud finden Sie unter https://docs.netwitness.com/netwitnessueba/release_information/whats_new/. Informationen zu Insight finden Sie unter https://docs.netwitness.com/netwitnessinsight/release-information/insight_whatsnew/.

Ressourcen zur Selbsthilfe

Es gibt mehrere Optionen, die Ihnen bei der Installation und Verwendung von NetWitness bei Bedarf Hilfestellung bieten:

- Weitere Informationen zu allen Aspekten von NetWitness finden Sie hier: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Benutzen Sie die Felder **Search** und **Create a Post** im NetWitness Community-Portal, um hier spezifische Informationen zu finden: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- Weitere Informationen finden Sie in der NetWitness Wissensdatenbank: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- Weitere Informationen finden Sie im Abschnitt „Troubleshooting” in den Leitfäden.

- Siehe auch NetWitness® Platform-Blogbeiträge.
- Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an den NetWitness Support.

NetWitness Support kontaktieren

Wenn Sie den NetWitness-Support kontaktieren, sollten Sie sich an Ihrem Computer befinden. Bereiten Sie sich darauf vor, die folgenden Informationen zu geben:

- Die Versionsnummer des verwendeten NetWitness Platform-Produkts oder der Appliance.
- Typ der verwendeten Hardware

Verwenden Sie die folgenden Kontaktinformationen, wenn Sie Fragen haben oder Unterstützung benötigen.

NetWitness Community Portal	https://community.netwitness.com Klicken Sie im Hauptmenü auf **Support > Portal für Support-Fälle > Meine Fälle anzeigen**.
Internationale Kontakte (So kontaktieren Sie den NetWitness-Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
NW-Update	https://update.netwitness.com/
LiveUI	https://live.netwitness.com

NetWitness Educational Services

Melden Sie sich an, um Zugang zu NetWitness-Kursen und zusätzlichen Ressourcen zu NetWitness Educational Services und Schulungen zu erhalten.

NetWitness Education Portal	https://netwitness.sabacloud.com/Saba/Web_spf/NA10P2PRD088/guestapp/home;spf-url=guest%2Fguestlearningcatalog
NetWitness Educational Services-Kurskatalog	https://community.netwitness.com/t5/netwitness-education-courses/tkb-p/netwitness-training
NetWitness Educational Services-Schulungsplan	https://community.netwitness.com/t5/netwitness-education-blog/netwitness-instructor-led-training-schedule/ba-p/655826
Kontakt zum NetWitness Educational Services-Support	education.support@netwitness.com

Feedback zur Produktdokumentation

Sie können eine E-Mail an feedbacknwdocs@netwitness.com senden, um Feedback zu den Dokumentation der NetWitness Platform zu geben.