



# RSA NetWitness UEBA Benutzerhandbuch

für Version 11.2



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

## **Kontaktinformationen**

RSA Link unter <https://community.rsa.com> enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

## **Marken**

Eine Liste der RSA-Marken finden Sie unter [germany.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://germany.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **Lizenzvereinbarung**

Diese Software und die zugehörige Dokumentation sind Eigentum von Dell und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden 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 sollte nicht als Verpflichtung seitens Dell ausgelegt werden.

## **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 RSA Link 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 sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

## **Verteilung**

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

February 2019

# Inhalt

---

<b>Einführung</b> .....	<b>5</b>
Funktionsweise von NetWitness UEBA .....	5
Abrufen von Protokolldaten .....	6
Erstellen von Baselines .....	7
Erkennen von Anomalien .....	7
Generieren von Warmmeldungen .....	8
Nutzer mit riskantem Verhalten priorisieren .....	8
Unterstützte Protokollquellen .....	9
Empfohlene Workflows .....	9
Erkennungsworkflow .....	9
Forensischer Workflow .....	11
Zugriff auf NetWitness UEBA .....	13
<b>NetWitness UEBA-Indikatoren</b> .....	<b>14</b>
Windows-Dateiserver .....	14
Active Directory .....	14
Anmeldeaktivität .....	15
<b>NetWitness UEBA-Anwendungsfälle für Windows-Protokolle</b> .....	<b>17</b>
<b>Untersuchen von Nutzern mit hohem Risiko</b> .....	<b>22</b>
Identifizieren von Nutzern mit hohem Risiko .....	24
Anzeigen der fünf Nutzer mit dem höchsten Risiko .....	24
Anzeigen aller Nutzer mit hohem Risiko .....	25
Anzeigen von Nutzern bestimmter Gruppen .....	26
Anzeigen von Nutzern basierend auf forensischer Untersuchung .....	28
Starten von Untersuchungen für Nutzer mit hohem Risiko .....	28
Ergreifen von Maßnahmen für Nutzer mit hohem Risiko .....	30
Geben Sie an, ob eine Warmmeldung kein Risiko ist. ....	31
Speichern von Verhaltensmustern .....	31
Hinzufügen aller Nutzer in der Überwachungsliste .....	32
Anzeigen eines Nutzerprofils .....	33
Exportieren von Nutzern mit hohem Risiko .....	34
<b>Untersuchen von Top-Warmmeldungen</b> .....	<b>36</b>
Starten einer Ermittlung kritischer Warmmeldungen .....	38
Filtern von Warmmeldungen .....	41
Untersuchen von Indikatoren .....	42
Top-Warmmeldungen verwalten .....	45

---

<b>Anzeigen von NetWitness UEBA-Metriken zu Integrität und Zustand</b> .....	<b>48</b>
<b>Referenz</b> .....	<b>51</b>
Registerkarte „Übersicht“ .....	51
Workflow .....	51
Was möchten Sie tun? .....	51
Verwandte Themen .....	52
Überblick .....	52
Registerkarte „Nutzer“ .....	55
Workflow .....	55
Was möchten Sie tun? .....	55
Verwandte Themen .....	56
Überblick .....	57
Registerkarte „Warnmeldungen“ .....	60
Workflow .....	60
Was möchten Sie tun? .....	60
Verwandte Themen .....	60
Überblick .....	61
Ansicht „Nutzerprofil“ .....	64
Workflow .....	64
Was möchten Sie tun? .....	64
Verwandte Themen .....	65
<b>Anhang: NetWitness UEBA – Windows-Überwachungrichtlinien</b> .....	<b>68</b>

## Einführung

RSA NetWitness UEBA (Analyse des Nutzer- und Entitätsverhaltens) ist eine fortschrittliche Analyselösung zur Entdeckung, Untersuchung und Überwachung von riskanten Verhaltensweisen für alle Nutzer und Entitäten in Ihrer Netzwerkumgebung. NetWitness UEBA wird für folgende Zwecke verwendet:

- Erkennen von böswilligen Nutzern
- Erkennen von hochriskanten Verhaltensweisen
- Erkennen von Angriffen
- Untersuchen von aufkommenden Sicherheitsbedrohungen

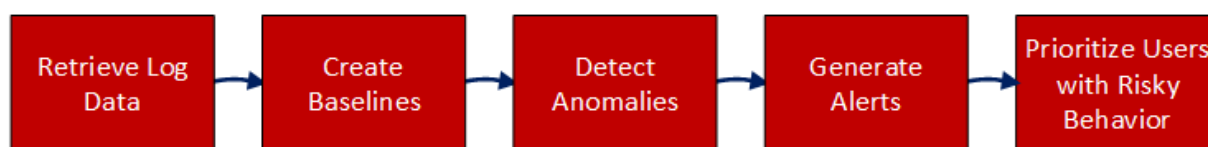
**Hinweis:** Standardmäßig werden nur Windows-Protokolle unterstützt. Sie können zusätzliche Protokollquellen hinzufügen, mit denen bestehende Modelle aufgefüllt werden. Weitere Informationen finden Sie unter [Unterstützte Protokollquellen](#).

NetWitness UEBA nutzt vorhandene Daten in NetWitness Platform-Protokollen und stellt SOC-Managern im Unternehmen und Analysten Erkenntnisse und Ermittlungsmöglichkeiten zur Verfügung, mit denen Cyberbedrohungen verringert werden können.

Dieser Leitfaden ist für Analysten und SOC-Manager konzipiert und bietet Informationen und Anweisungen für die Nutzung aller NetWitness UEBA-Funktionen. Es werden die wichtigsten Ermittlungsmethoden, die wichtigsten Systemfunktionen, gängige Anwendungsfälle und Schritt-für-Schritt-Anleitungen für empfohlene Workflow-Strategien beschrieben.

## Funktionsweise von NetWitness UEBA

Basierend auf Analysen erkennt NetWitness UEBA Anomalien in Protokolldaten und leitet daraus Verhaltensergebnisse ab. Dieser Prozess besteht aus fünf grundlegenden Schritten, die im folgenden Diagramm veranschaulicht werden:



Die folgende Tabelle enthält eine kurze Beschreibung dieser Schritte.

Schritt	Beschreibung	Weitere Informationen
1. Protokolldaten abrufen	NetWitness UEBA ruft Protokolldaten aus der NetWitness Platform-Datenbank (NWDB) ab und erstellt auf der Grundlage dieser Daten Analyseergebnisse.	Siehe <a href="#">Abrufen von Protokolldaten</a>

Schritt	Beschreibung	Weitere Informationen
2. Baselines erstellen	Baselines werden aus einer detaillierten Analyse des normalen Nutzerverhaltens abgeleitet und dienen als Grundlage für den Vergleich mit dem Nutzerverhalten im Laufe der Zeit.	Siehe <a href="#">Erstellen von Baselines</a>
3. Anomalien erkennen	Eine Anomalie ist eine Abweichung vom normalen Baselineverhalten eines Nutzers. NetWitness UEBA führt eine statistische Analyse durch, in der jede neue Aktivität mit der Baseline verglichen wird. Nutzeraktivitäten, die von den erwarteten Baselinewerten abweichen, werden entsprechend bewertet, sodass der Schweregrad der Abweichung reflektiert wird.	Siehe <a href="#">Erkennen von Anomalien</a>
4. Warnmeldungen generieren	Alle in Schritt 3 gefundenen Anomalien werden in Stundenstapeln zusammengefasst. Jeder Stapel wird auf der Grundlage der Einzigartigkeit seiner Indikatoren bewertet. Wenn die Indikatorzusammensetzung im Vergleich zu den historischen Stundenstapeln eines Nutzers einzigartig ist, ist es wahrscheinlich, dass dieser Stapel in eine Warnmeldung umgewandelt wird.	Siehe <a href="#">Generieren von Warnmeldungen</a>
5. Nutzer mit riskantem Verhalten priorisieren	NetWitness UEBA priorisiert das potenzielle Risiko eines Nutzers durch die Verwendung einer zusätzlichen vereinfachten Bewertungsformel. Jeder Warnmeldung wird ein Schweregrad zugewiesen, durch den die Bewertung eines Nutzers um eine vorgegebene Punktzahl erhöht wird. Nutzer mit hohen Punktzahlen verfügen entweder über mehrere Warnmeldungen oder über Warnmeldungen mit hohem Schweregrad.	Siehe <a href="#">Nutzer mit riskantem Verhalten priorisieren</a>

## Abrufen von Protokolldaten

Der NetWitness UEBA-Server verbindet sich zum Abrufen von Protokolldaten aus den Concentrators mit dem Broker- oder Concentrator-Service. Sie können den Broker-Service nutzen, der auf dem NetWitness-Admin-Server verfügbar ist, wenn Sie in der Bereitstellung nicht über einen exklusiven Broker verfügen. Während der NetWitness UEBA-Installation gibt der Administrator die IP-Adresse des Broker-Service an.

Weitere Informationen finden Sie im Thema „(Optional) Aufgabe 2 – Installieren von NetWitness UEBA“ im *NetWitness Platform 11.2 Installationsleitfaden für physische Hosts*.

## Erstellen von Baselines

NetWitness UEBA analysiert mehrere Aspekte der Aktionen eines Nutzers innerhalb eines Datenflusses auf der Grundlage von maschinellem Lernen und baut nach und nach eine mehrdimensionale Baseline für das typische Verhalten jeden Nutzers auf. Zum Beispiel kann die Baseline Informationen über die Stunden enthalten, in denen sich ein Nutzer typischerweise einloggt.

Verhaltensbaselines werden auch auf globaler Ebene erstellt. Damit werden allgemeine Aktivitäten beschrieben, die im gesamten Netzwerk beobachtet werden. Wenn eine Arbeitsstunde für einen Nutzer ungewöhnlich war, aber für die Organisation nicht ungewöhnlich ist, verringern die falsch-positiven Reduktionsalgorithmen die Auswirkungen auf die Punktzahl für die Warnmeldung.

Modelle werden häufig aktualisiert und verbessern sich im Laufe der Zeit ständig.

**Hinweis:** Damit NetWitness UEBA eine angemessene Baseline für alle Nutzer in Ihrem Netzwerk erstellen kann, sind historische Protokolldaten über 28 Tage erforderlich. RSA empfiehlt jedoch, NetWitness UEBA so zu konfigurieren, dass Sie zwei Monate vor dem Bereitstellungsdatum `<today-60days>` mit der Erstellung der Baseline für Ihre Daten beginnen. Die ersten 28 Tage werden für das Modelltraining genutzt und nicht genutzt. Die restlichen 32 Tage werden genutzt, um das Modell zu verbessern und zu aktualisieren. Außerdem werden diese Tage für den Anfangswert gewertet.

**Hinweis:** Für Version 11.2 gibt es nur eine begrenzte Unterstützung für Umgebungen mit mehreren Domains. Die unterschiedlichen Werte für Nutzernamen, die unter verschiedenen Domains registriert werden, werden normalisiert und dann zu einer modellierten Entität zusammengefasst. Infolgedessen werden verschiedene Nutzer, die den gleichen Nutzernamen in verschiedenen Domains teilen, fälschlicherweise einer einzigen normalisierten Entität zugeschrieben.

## Erkennen von Anomalien

Sobald eine Verhaltensbaseline für alle Nutzer in der Umgebung erstellt wurde, wird jedes eingehende Ereignis mit der Baseline verglichen. Auf dieser Grundlage wird eine Punktzahl vergeben, die anzeigt, ob das neue Verhalten ungewöhnlich ist und insbesondere ob es eine starke Abweichung von der Baseline darstellt. Wenn z. B. die normalen Arbeitszeiten eines Nutzers von 9:00 Uhr bis 17:00 Uhr sind, stellt eine neue Aktivität um 6:00 Uhr oder 7:00 Uhr keine starke Abweichung dar und wird wahrscheinlich nicht als Anomalie gewertet. Eine Authentifizierung um Mitternacht ist jedoch eine starke Abweichung und wird als Anomalie gewertet.

Erkannte Anomalien werden in Indikatoren für eine Infizierung umgewandelt, die in der Benutzeroberfläche als Indikatoren bezeichnet werden. Mithilfe dieser Indikatoren definiert NetWitness UEBA validierte ungewöhnliche Aktivitäten, wie zum Beispiel verdächtige Nutzeranmeldungen, Brute-Force-Passwortangriffe, ungewöhnliche Nutzeränderungen und ungewöhnliche Dateizugriffe. Indikatoren stellen entweder in einem einzigen Ereignis gefundene Anomalien oder mehrere Ereignisse dar, die im Laufe der Zeit zusammengefasst wurden.

## Generieren von Warnmeldungen

Alle gefundenen Anomalien sind in Benutzernamen- und Stundenstapeln gruppiert. Jeder Stapel wird auf der Grundlage der Einzigartigkeit seiner Indikatoren bewertet. Wenn eine Zusammensetzung im Vergleich zu den historischen Daten eines Nutzers einzigartig ist, ist es wahrscheinlich, dass dieser Stapel in eine Warnmeldung und die Anomalien in Indikatoren umgewandelt werden. Ein Stapel mit hoch bewerteten Anomalien wird zu einer Warnmeldung mit validierten Indikatoren für die Infizierung.

Selbst wenn eine ungewöhnliche Aktivität Hunderte Male am Tag in einem großen Unternehmensumfeld auftritt, spiegelt sie allein nicht unbedingt eine Kontoinfizierung wider. Allerdings könnte ein ungewöhnliches Verhalten, das zusammen mit vielen anderen ungewöhnlichen Verhaltensweisen auftritt, darauf hindeuten, dass das Konto infiziert ist. Treten diese drei Verhaltensweisen gemeinsam auf, könnte dies darauf hindeuten, dass zusätzliche Analysen erforderlich sind.

- Authentifizierung eines ungewöhnlichen Computers
- Mehrere in kurzer Zeit identifizierte Authentifizierungsversuche
- Mehrere Dateien wurden von diesem Nutzer aus der Firmendatei gelöscht

**Hinweis:** Die NetWitness UEBA-Benutzeroberfläche kann zunächst leer sein, da Warnmeldungen erst nach der Einrichtung der Baselines erzeugt werden. Wenn es bei aktiviertem NetWitness UEBA keine historischen Prüfdaten gibt, beginnt das System mit der Generierung der Baselines ab dem Zeitpunkt der Bereitstellung. Danach dauert es 28 volle Tage, bevor das System beginnt, neue Warnmeldungen zu generieren. Wenn historische Prüfdaten bei aktiviertem NetWitness UEBA verarbeitet werden, werden Warnmeldungen erst nach der Verarbeitung der historischen Daten angezeigt – in der Regel innerhalb von zwei bis vier Tagen.

## Nutzer mit riskantem Verhalten priorisieren

Die Nutzerwerte sind ein primäres Werkzeug für die Priorisierung von Incidents. Die Nutzerbewertung basiert auf einer einfachen additiven Berechnung der Warnmeldungen des Nutzers. Warnmeldungen und Analystenfeedback sind die einzigen Faktoren in der Berechnung der Nutzerbewertung, wobei der Einfluss auf die Punktzahl durch ihren Schweregrad bestimmt wird.

Für Nutzer- und Warnmeldungsbewertungen wird ein einheitlicher Farbcode verwendet:

Schweregrad	Farbe	Bewertung
Kritisch	Rot	+20
Hoch	Orange	+15
Mittel	Gelb	+10
Niedrig	Grün	+1



## Unterstützte Protokollquellen

NetWitness UEBA unterstützt nativ folgende Windows-Protokollquellen:

- Windows Active Directory
- Windows-Anmelde- und -Authentifizierungsaktivität
- Windows-Dateiserver

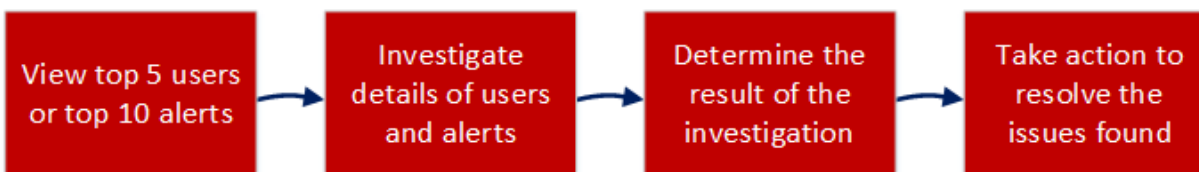
## Empfohlene Workflows

Es gibt zwei Workflows, mit denen Sie NetWitness UEBA am effektivsten nutzen können: Erkennungsworkflow und forensischer Workflow.

### Erkennungsworkflow

Mit dem Erkennungsworkflow können Sie sich einen Überblick über den Zustand Ihrer Umgebung verschaffen und sich dann darauf konzentrieren, die wichtigsten Nutzer mit hohem Risiko und Warnmeldungen zu untersuchen, die auf der Registerkarte „Übersicht“ angezeigt werden.

Im folgenden Flussdiagramm sind die möglichen Schritte dargestellt, mit denen Sie verdächtiges Verhalten in Ihrer Umgebung erkennen.



In der folgenden Tabelle werden die einzelnen Workflows beschrieben.

Schritt	Beschreibung	Anweisungen
Anzeigen der wichtigsten fünf Nutzer oder der wichtigsten 10 Warnmeldungen	Auf der Registerkarte „Übersicht“ sind die Nutzer mit den riskantesten Verhaltensweisen und den kritischsten Warnmeldungen zu erkennen.	<a href="#">Untersuchen von Nutzern mit hohem Risiko</a> und <a href="#">Untersuchen von Top-Warnmeldungen</a>
Untersuchen von Details zu Nutzern und Warnmeldungen	Schauen Sie sich die detaillierten Informationen über risikoreiches Nutzerverhalten und kritische Warnmeldungen an. So können Sie die Ursache und Lösung dieser Aktionen ermitteln.	<a href="#">Untersuchen von Nutzern mit hohem Risiko</a> und <a href="#">Untersuchen von Indikatoren</a>

Schritt	Beschreibung	Anweisungen
Bestimmen des Ermittlungsergebnisses	Identifizieren Sie anhand der in der Benutzeroberfläche aus den vorherigen Schritten bereitgestellten zusammenfassenden Informationen Bereiche, auf die Sie sich zur Lösung der gefundenen Probleme konzentrieren müssen.	<a href="#">Identifizieren von Nutzern mit hohem Risiko</a> und <a href="#">Untersuchen von Indikatoren</a>
Ergreifen von Maßnahmen zur Lösung der gefundenen Probleme	Konzentrieren Sie sich auf Benutzerverhalten und -ereignisse und nutzen Sie die Ergebnisse zur Verbesserung und genaueren Definition zukünftiger Ermittlungen.	<a href="#">Ergreifen von Maßnahmen für Nutzer mit hohem Risiko</a>

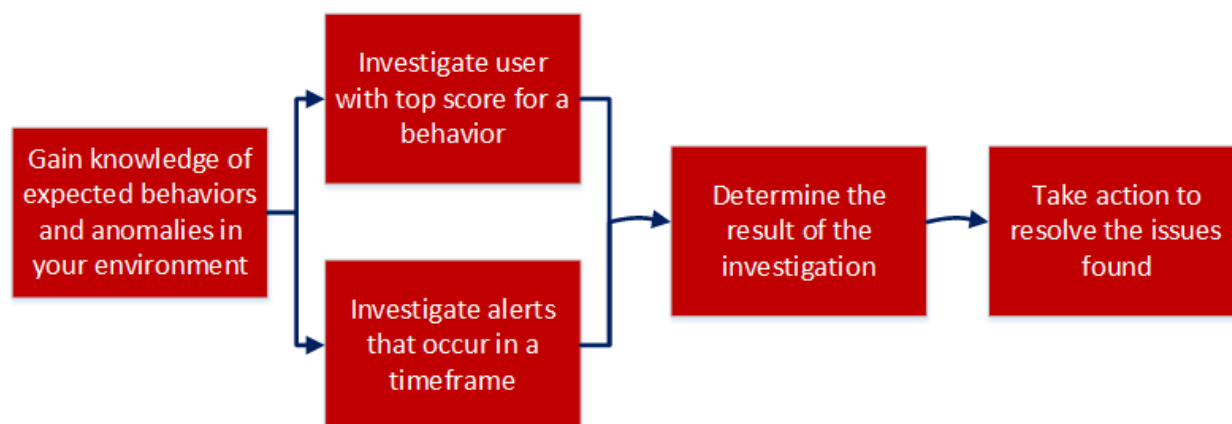
## Forensischer Workflow

Der forensische Workflow wird empfohlen, wenn Sie ein Verständnis für die typischen Benutzerverhaltensweisen und Anomalien in Ihrer Umgebung gewonnen haben. Mit diesem Workflow können Sie sich auf bestimmte, auf einem Benutzerverhalten basierende forensische Informationen oder auf einen bestimmten Zeitrahmen konzentrieren, in dem verdächtige Ereignisse aufgetreten sind.

Anhand von forensischen Informationen können die Analysten die vom Angreifer sehr wahrscheinlich angewendeten Handlungen und Verhaltensweisen bestimmen und folgende Fragen beantworten:

- Welche grundlegenden Techniken und Verhaltensweisen sind über alle Angriffe hinweg verbreitet?
- Welche Beweise hinterlassen diese Techniken?
- Was tun Angreifer?
- Was sind normale Verhaltensweisen für meine Konten und Entitäten?
- Welche meiner Maschinen sind besonders empfindlich und wo befinden sie sich?

Im folgenden Flussdiagramm ist dargestellt, wie Sie forensische Informationen untersuchen, die auf einem bestimmten Benutzerverhalten oder auf einem bestimmten Zeitrahmen basieren, in dem verdächtige Ereignisse aufgetreten sind.



In der folgenden Tabelle werden die einzelnen Workflows beschrieben.

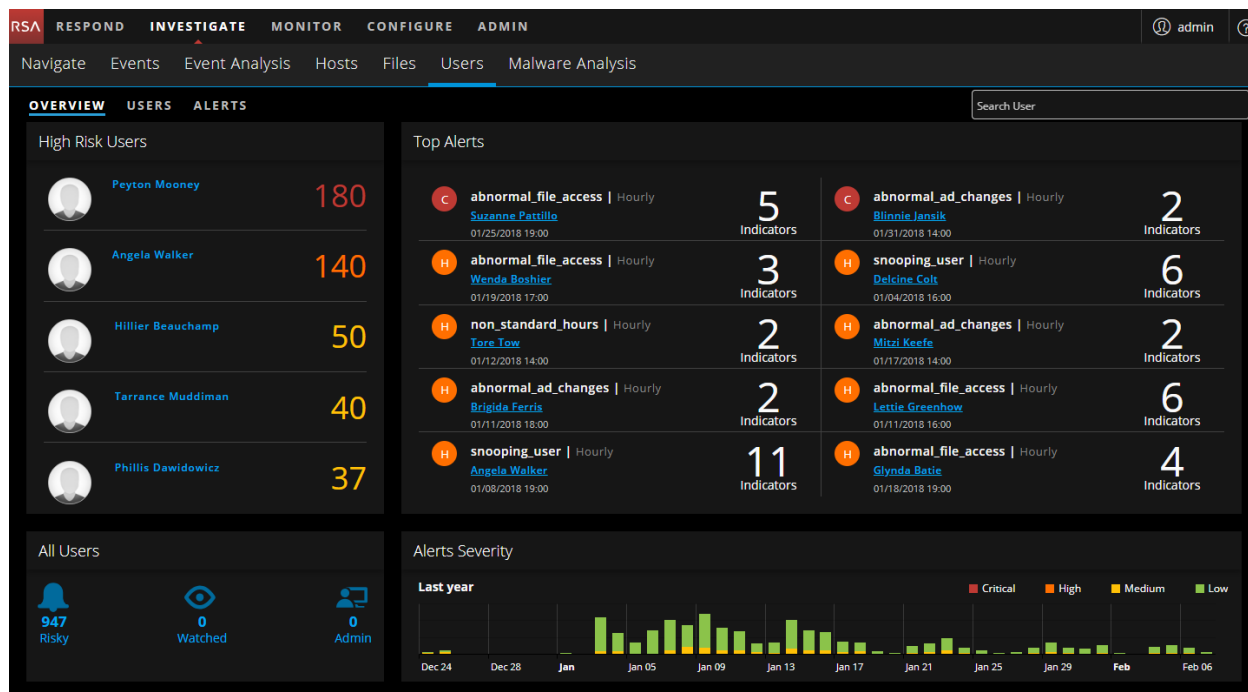
Schritt	Beschreibung	Anweisungen
Wissen über die zu erwartenden Verhaltensweisen und Anomalien in Ihrer Umgebung gewinnen	Legen Sie eine Baseline für normale Verhaltensweisen, erwartete Anomalien und unerwartete Anomalien fest, sodass Sie sich auf Anomalien konzentrieren können, die für Ihre Umgebung von Bedeutung sind.	<a href="#">Abrufen von Protokolldaten</a> abrufen, <a href="#">Erkennen von Anomalien</a> und <a href="#">Generieren von Warnmeldungen</a> .
Nutzer mit der höchsten Punktzahl auf ein bestimmtes Verhalten untersuchen	Wählen Sie einen Nutzer mit einer hohen Punktzahl für ein bestimmtes Verhalten aus und sammeln Sie detaillierte Informationen.	<a href="#">Untersuchen von Nutzern mit hohem Risiko</a> und <a href="#">Untersuchen von Indikatoren</a>

Schritt	Beschreibung	Anweisungen
Warnmeldungen untersuchen, die in einem bestimmten Zeitrahmen auftreten	Legen Sie einen bestimmten Zeitrahmen fest und wählen Sie diesen auf der Registerkarte „Warnmeldungen“ aus, um detaillierte Informationen über Warnmeldungen anzuzeigen, die während dieses Zeitraums aufgetreten sind.	<a href="#">Untersuchen von Indikatoren</a>
Bestimmen des Ermittlungsergebnisses	Konzentrieren Sie sich auf der Grundlage Ihres Wissens über das erwartete Nutzerverhalten auf die während des angegebenen Zeitraums angezeigten Indikatoren und bestimmen Sie, ob die entdeckten Anomalien behoben werden müssen.	<a href="#">Untersuchen von Indikatoren</a> und <a href="#">Identifizieren von Nutzern mit hohem Risiko</a>
Ergreifen von Maßnahmen zur Lösung der gefundenen Probleme	Konzentrieren Sie sich auf Nutzerverhalten und -ereignisse und nutzen Sie die Ergebnisse zur Verbesserung und genaueren Definition zukünftiger Ermittlungen.	<a href="#">Ergreifen von Maßnahmen für Nutzer mit hohem Risiko</a>

## Zugriff auf NetWitness UEBA

**Hinweis:** Für den Zugriff auf den NetWitness UEBA-Service und die Registerkarte „Benutzer“ müssen Sie entweder der UEBA\_Analyst-Rolle oder der Administratorrolle zugeordnet werden. Weitere Informationen über die Zuordnung dieser Rollen finden Sie im Thema „So funktioniert Role-Based Access Control“ im *Handbuch Systemsicherheit und Benutzerverwaltung*. Darüber hinaus müssen Sie die richtige NetWitness UEBA-Lizenzierung konfiguriert haben. Informationen über die NetWitness UEBA-Lizenzierung finden Sie unter „Analyse des Nutzer- und Entitätsverhaltens“ im *Leitfaden zum Lizenzierungsmanagement*.

Für den Zugriff auf NetWitness UEBA melden Sie sich bei NetWitness Platform an und gehen Sie zu **Untersuchen > Benutzer**. Die Ansicht „Benutzer“ mit allen NetWitness UEBA-Funktionen wird angezeigt.



## NetWitness UEBA-Indikatoren

In den folgenden Tabellen werden Indikatoren aufgelistet, die bei Erkennung potenziell bösartiger Aktivitäten angezeigt werden.

### Windows-Dateiserver

Indikator	Warnmeldungstyp	Beschreibung
Ungewöhnliche Dateizugriffszeit	Nicht-Standard-Stunden	Ein Benutzer hat zu einem ungewöhnlichen Zeitpunkt auf eine Datei zugegriffen.
Ungewöhnliche Änderung der Dateizugriffsberechtigung	Änderungen zahlreicher Berechtigungen	Ein Benutzer hat mehrere Freigabeberechtigungen geändert.
Ungewöhnliches Dateizugriffsereignis	Ungewöhnlicher Dateizugriff	Ein Benutzer hat auf ungewöhnliche Weise auf eine Datei zugegriffen.
Mehrere Änderungen der Dateizugriffsberechtigung	Änderungen zahlreicher Berechtigungen	Ein Benutzer hat mehrere Dateifreigabeberechtigungen geändert.
Mehrere Dateizugriffsereignisse	Snooping-Benutzer	Ein Benutzer hat mehrere Dateifreigabeberechtigungen geändert.
Mehrere gescheiterte Dateizugriffsereignisse	Snooping-Benutzer	Ein Benutzer hat mehrfach keinen Zugriff auf eine Datei erhalten.
Mehrere Datei-Öffnen-Ereignisse	Snooping-Benutzer	Ein Benutzer hat mehrere Dateien geöffnet.
Mehrfache Ordner-Öffnen-Ereignisse	Snooping-Benutzer	Ein Benutzer hat mehrere Ordner geöffnet.
Mehrere Datei-Löschen-Ereignisse	Ungewöhnlicher Dateizugriff	Ein Benutzer hat mehrere Dateien gelöscht.

### Active Directory

Indikator	Warnmeldungstyp	Beschreibung
Ungewöhnliche Active Directory-Änderungszeit	Nicht-Standard-Stunden	Ein Benutzer hat Active Directory zu einem ungewöhnlichen Zeitpunkt geändert.

Indikator	Warnmeldungstyp	Beschreibung
Ungewöhnliche Änderung von Active Directory	Ungewöhnliche AD-Änderungen	Es wurde eine ungewöhnlich Änderung an einem Active Directory-Attribut vorgenommen.
Mehrere Änderungen der Gruppenmitgliedschaft	Mehrfachänderungen der Gruppen	Ein Benutzer hat mehrere Änderungen an Gruppen vorgenommen.
Mehrere Änderungen an der Kontoverwaltung	Ungewöhnliche AD-Änderungen	Ein Benutzer hat mehrere Active Directory-Änderungen vorgenommen.
Mehrfache Änderungen an der Kontoverwaltung durch Benutzer	Ungewöhnliche AD-Änderungen	Ein Benutzer hat mehrere vertrauliche Active Directory-Änderungen vorgenommen.
Mehrere fehlgeschlagene Änderungen in der Kontoverwaltung	Ungewöhnliche AD-Änderungen	Einem Nutzer sind mehrere Änderungen im Active Directory fehlgeschlagen.
Geändertes Administratorpasswort	Änderung des Administratorpassworts	Das Passwort eines Administrators wurde geändert.
Aktivieren eines Nutzerkontos	Sensible Änderungen des Nutzerstatus	Das Konto eines Nutzers wurde aktiviert.
Nutzerkonto wurde deaktiviert	Sensible Änderungen des Nutzerstatus	Das Konto eines Nutzers wurde deaktiviert.
Nutzerkonto wurde entsperrt	Sensible Änderungen des Nutzerstatus	Das Konto eines Nutzers wurde freigeschaltet.
Art des Nutzerkontos geändert	Sensible Änderungen des Nutzerstatus	Ein Nutzertyp wurde geändert.
Nutzerkonto wurde gesperrt	Sensible Änderungen des Nutzerstatus	Das Konto eines Nutzers wurde gesperrt.
Nutzerpasswort wurde geändert	Sensible Änderungen des Nutzerstatus	Das Passwort eines Nutzers wurde geändert.

## Anmeldeaktivität

Indikator	Warnmeldungstyp	Beschreibung
Ungewöhnliche Anmeldezeit	Nicht-Standard-Stunden	Ein Nutzer hat sich zu einem ungewöhnlichen Zeitpunkt angemeldet.
Ungewöhnlicher Computer	Nutzeranmeldung auf ungewöhnlichem Host	Ein Nutzer hat versucht, auf einen ungewöhnlichen Computer zuzugreifen.

Indikator	Warnmeldungstyp	Beschreibung
Mehrere erfolgreiche Authentifizierungen	Mehrere Anmeldungen durch den Nutzer	Ein Nutzer hat sich mehrfach angemeldet.
Mehrfach fehlgeschlagene Authentifizierungen	Mehrere fehlgeschlagene Anmeldungen	Einem Nutzer sind mehrere Authentifizierungsversuche fehlgeschlagen.
Anmeldung auf mehreren Computern	Nutzer auf mehreren Hosts angemeldet	Ein Nutzer hat versucht, sich von mehreren Computern aus anzumelden.



## NetWitness UEBA-Anwendungsfälle für Windows-Protokolle

NetWitness UEBA konzentriert sich auf die Bereitstellung von fortschrittlichen Erkennungsmöglichkeiten, mit denen Unternehmen vor Bedrohungen durch Insider geschützt werden. Diese könnten entweder vertrauenswürdige Nutzer des Netzwerks oder alternativ ein böswilliger externer Angreifer sein, der die erworbenen Berechtigungen für eine erweiterte Kontoübernahme nutzt.

Identitätsdiebstahl beginnt in der Regel mit dem Diebstahl von Berechtigungen. Diese werden für den unbefugten Zugriff auf Ressourcen genutzt, um die Kontrolle über das Netz zu erlangen. Angreifer können auch infizierte Nicht-Admin-Nutzer ausnutzen, um Zugriff auf Ressourcen zu erhalten, für die sie administrative Rechte haben, und diese Rechte dann eskalieren.

Ein Angreifer, der gestohlene Berechtigungen verwendet, kann während des Zugriffs auf Ressourcen verdächtige Netzwerkereignisse auslösen. Das Erkennen unerlaubter Berechtigungen ist möglich. Allerdings müssen Sie dazu die Angreiferaktivität von der hohen Menge rechtmäßiger Ereignisse trennen. Mithilfe von NetWitness UEBA können Sie möglicherweise bösartige Aktivitäten von den sonst ungewöhnlichen, aber nicht riskanten Nutzeraktionen trennen.

Die folgenden Anwendungsfälle definieren bestimmte Risikotypen und die entsprechenden Systemfunktionen, mit deren Hilfe sie erkannt werden. Sie können die Anwendungsfälle, die durch ihren Warnmeldungstyp und ihre Beschreibung dargestellt werden, überprüfen und so ein erstes Verständnis für das damit verbundene riskante Verhalten jedes einzelnen gewinnen. Mit NetWitness UEBA können Sie dann für die Indikatoren für möglicherweise riskante Nutzeraktivitäten einen Drill-down durchführen und erhalten so weitere Informationen. Weitere Informationen zu von NetWitness UEBA unterstützten Indikatoren finden Sie unter [NetWitness UEBA-Indikatoren](#).

Warnmeldungstyp	Beschreibung
Mehrfachänderungen der Gruppen	An Gruppen wurde eine ungewöhnliche Anzahl von Änderungen vorgenommen. Untersuchen Sie, welche Elemente geändert wurden, und entscheiden Sie, ob die Änderungen legitim waren oder möglicherweise das Ergebnis eines riskanten oder bösartigen Verhaltens sind. Dieser Aktivität wird in der Regel der Indikator <b>Mehrere Änderungen der Gruppenmitgliedschaft</b> zugeordnet.
Erweiterte Rechte erteilt	An einen Benutzer wurden erweiterte Kontorechte delegiert. Angreifer nutzen oft reguläre Nutzerkonten, die ihnen erweiterte Rechte gewähren, um das Netzwerk anzugreifen. Untersuchen Sie den Nutzer, der die erweiterten Rechte hat, und entscheiden Sie, ob diese Änderungen legitim waren oder möglicherweise das Ergebnis eines riskanten oder bösartigen Verhaltens sind. Dieser Aktivität wird in der Regel der Indikator <b>Verschachteltes Mitglied zu wichtiger Enterprise-Gruppe hinzugefügt</b> und der Indikator <b>Mitglied zu wichtiger Enterprise-Gruppe hinzugefügt</b> zugeordnet.

Warnmeldungstyp	Beschreibung
Mehrere fehlgeschlagene Anmeldungen	Bei der herkömmlichen Passwortentschlüsselung versucht der Angreifer, ein Passwort durch Vermutungen oder durch den Einsatz anderer Methoden mit geringem technischem Aufwand abzurufen und damit einen ersten Zugriff zu erhalten. Der Angreifer riskiert, erwischt oder ausgesperrt zu werden, weil er explizit versucht, sich zu authentifizieren. Aber mit einigen Vorkenntnissen über den Passwortverlauf des Opfers, kann er sich erfolgreich authentifizieren. Suchen Sie nach zusätzlichen ungewöhnlichen Hinweisen darauf, dass nicht der Kontoinhaber versucht, auf dieses Konto zuzugreifen. Dieser Aktivität wird in der Regel der Indikator <b>Mehrere fehlgeschlagene Authentifizierungen</b> zugeordnet.
Nutzeranmeldungen auf mehreren AD-Websites	Domain-Controller speichern Hashes für Berechtigungspasswörter für alle Konten auf der Domain, sodass sie hochwertige Ziele für Angreifer sind. Nicht stringent aktualisierte und gesicherte Domain-Controller sind anfällig für Angriffe und Infizierung, die die Domain gefährden könnten. Nutzerrechte auf mehreren Domains könnten darauf hindeuten, dass eine übergeordnete Domain infiziert wurde. Bestimmen Sie, ob der Zugriff des Nutzers auf und von mehreren Websites legitim ist oder ein Hinweis auf eine mögliche Infizierung ist. Dieser Aktivität wird in der Regel der Indikator <b>Anmeldungen auf mehreren Domains</b> zugeordnet.
Nutzeranmeldung auf ungewöhnlichem Host	Häufig müssen Angreifer Berechtigungen erneut erwerben und andere sensible Aktivitäten ausführen, wie zum Beispiel die Verwendung von Remotezugriff. Die Rückverfolgung der Zugriffskette kann zur Entdeckung anderer Computer führen, die möglicherweise in riskante Aktivitäten verwickelt sind. Wenn die Anwesenheit eines Angreifers auf einen einzigen infizierten Host oder auf viele infizierten Hosts beschränkt ist, kann dieser Aktivität der Indikator <b>Ungewöhnlicher Computer</b> zugeordnet werden.
Datenexfiltration	Die Datenexfiltration ist das unerlaubte Kopieren, Übertragen oder Abrufen von Daten von einem Computer oder Server. Datenexfiltration ist eine böswärtige Aktivität, die in der Regel durch verschiedene Techniken von Cyberkriminellen über das Internet oder ein anderes Netzwerk durchgeführt wird. Dieser Aktivität können die Indikatoren <b>Übermäßige Anzahl an Datei-Umbenennen-Ereignissen</b> , <b>Übermäßige Anzahl an Dateien, die aus dem Dateisystem verschoben wurden</b> und <b>Übermäßige Anzahl an Dateien, die auf das Dateisystem verschoben wurden</b> zugeordnet werden.
Massenhafte Dateiumbenennung	Ransomware ist eine Art Malware, mit der Desktop- und Systemdateien verschlüsselt und unzugänglich gemacht werden. Mit Ransomware, wie beispielsweise „Locky“, werden Dateien im Rahmen ihrer anfänglichen Ausführung verschlüsselt und umbenannt. Mithilfe des Indikators „Massenhafte Dateiumbenennung“ können Sie feststellen, ob das Dateisystem mit Ransomware infiziert wurde. Dieser Aktivität kann der Indikator <b>Mehrere Datei-Umbenennen-Ereignisse</b> zugeordnet werden.

Warnmeldungstyp	Beschreibung
Snooping-Nutzer	Snooping ist unbefugter Zugriff auf die Daten einer anderen Person oder eines Unternehmens. Snooping kann so einfach sein wie die gelegentliche Überwachung einer E-Mail auf dem Computer einer anderen Person oder das Beobachten der Eingabe einer Person auf einem Computer. Bei ausgefeilterem Snooping wird Aktivität mithilfe von Softwareprogrammen auf einem Computer oder Netzwerkgerät remote überwacht. Dieser Aktivität können die Indikatoren <b>Mehrere Dateizugriffereignisse</b> , <b>Mehrere fehlgeschlagene Dateizugriffereignisse</b> , <b>Mehrere Datei-Öffnen-Ereignisse</b> oder <b>Mehrere Ordner-Öffnen-Ereignisse</b> zugeordnet werden.
Mehrere Anmeldungen durch den Nutzer	Alle Authentifizierungsaktivitäten, ob böswillig oder nicht, erscheinen als normale Anmeldungen. Daher sollten Administratoren unerwartet autorisierte Aktivitäten überwachen. Der Schlüssel besteht darin, dass Angreifer diese gestohlenen Zugangsdaten für unbefugten Zugriff nutzen. Dies kann eine Möglichkeit zur Erkennung bieten. Wenn ein Konto für ungewöhnliche Aktivitäten verwendet wird, zum Beispiel bei einer Authentifizierung mit ungewöhnlicher Häufigkeit, kann das Konto infiziert sein. Dieser Aktivität kann in der Regel der Indikator <b>Mehrere fehlgeschlagene Authentifizierungen</b> zugeordnet werden.
Benutzer auf mehreren Hosts angemeldet	Angreifer müssen in der Regel in regelmäßigen Abständen erneut Berechtigungen erwerben. Das liegt daran, dass ihr Schlüsselbund gestohlener Berechtigungen im Laufe der Zeit aufgrund von Passwortänderungen und Resets natürlich kleiner wird. Angreifer halten daher häufig in der infizierten Organisation einen Fuß in der Tür, indem sie Hintertüren installieren und sich die Berechtigungen von vielen Computern in der Umgebung sichern. Dieser Aktivität kann der Indikator <b>Anmeldung auf mehreren Computern</b> zugeordnet werden.
Änderung des Administratorpassworts	Freigegebene Langzeitgeheimnisse, wie zum Beispiel privilegierte Kontopasswörter, werden häufig verwendet, um von Druckservern bis hin zu Domain-Controllern auf alles zuzugreifen. Wenn Sie Angreifer, die diese Konten zu nutzen versuchen, fernhalten möchten, achten Sie genau auf Passwortänderungen durch Administratoren und stellen Sie sicher, dass sie von vertrauenswürdigen Parteien gemacht wurden. Außerdem sollte kein weiteres ungewöhnliches Verhalten im Zusammenhang mit diesen Passwörtern auftreten. Dieser Aktivität kann der Indikator <b>Änderung des Administratorpassworts</b> zugeordnet werden.

Warnmeldungstyp	Beschreibung
Änderungen zahlreicher Berechtigungen	<p>Bei einigen Diebstahltechniken für Berechtigungen, zum Beispiel Pass-the-Hash, wird ein iterativer, zweistufiger Prozess verwendet. Zuerst erhält ein Angreifer eine erweiterte Lese- und Schreibberechtigung für privilegierte Bereiche von flüchtigen Speicher- und Dateisystemen, die in der Regel nur für Prozesse auf Systemebene auf mindestens einem Computer zugänglich sind. Im zweiten Schritt versucht der Angreifer, den Zugriff auf andere Computer im Netz zu erhöhen. Prüfen Sie, ob auf den Dateisystemen ungewöhnliche Berechtigungsänderungen stattgefunden haben. So können Sie sicherstellen, dass sie nicht von einem Angreifer infiziert wurden. Dieser Aktivität können die Indikatoren <b>Mehrere Änderungen an Dateizugriffsberechtigungen, Mehrfach fehlgeschlagene Änderungen an Dateizugriffsberechtigungen und Ungewöhnliche Änderung der Dateizugriffsberechtigung</b> zugeordnet werden.</p>
Ungewöhnliche AD-Änderungen	<p>Wenn ein Angreifer einen hochgradig privilegierten Zugriff auf eine Active Directory-Domain oder einen Domain-Controller erhält, kann er mit diesem Zugriff auf die Gesamtstruktur zugreifen, sie kontrollieren oder sogar zerstören. Wenn ein einzelner Domain-Controller infiziert ist und ein Angreifer die AD-Datenbank ändert, replizieren sich diese Modifikationen auf jedem anderen Domain-Controller in der Domain und abhängig von der Partition, in der die Änderungen vorgenommen werden, auch in der Gesamtstruktur. Untersuchen Sie ungewöhnliche von Administratoren und Nicht-Administratoren in AD durchgeführte Änderungen und stellen Sie fest, ob sie die Domain möglicherweise wirklich infizieren. Dieser Aktivität können die Indikatoren <b>Ungewöhnliche Active Directory-Änderung, Mehrere Änderungen an der Kontoverwaltung, Mehrere Änderungen an der Kontoverwaltung durch Benutzer und Mehrere fehlgeschlagene Änderungen in der Kontoverwaltung</b> zugeordnet werden.</p>
Sensible Änderungen des Nutzerstatus	<p>Ein Domain- oder Enterprise-Administratorkonto kann standardmäßig alle Ressourcen in der Domain kontrollieren, unabhängig davon, ob es eine böswillige oder gutartige Absicht dahintersteckt. Im Rahmen dieser Kontrolle können Konten erstellt und geändert, Daten gelesen, geschrieben oder gelöscht, Anwendungen installiert oder geändert und Betriebssysteme gelöscht werden. Einige dieser Aktivitäten werden organisch als Teil des natürlichen Lebenszyklus des Kontos ausgelöst. Untersuchen Sie diese sicherheitsrelevanten Nutzerkontoänderungen und stellen Sie fest, ob diese infiziert wurden. Dieser Aktivität können die Indikatoren <b>Aktivieren eines Benutzerkontos, Benutzerkonto wurde deaktiviert, Benutzerkonto wurde entsperrt, Art des Benutzerkontos geändert, Benutzerkonto wurde gesperrt, Option „Benutzerpasswort läuft niemals ab“ wurde geändert, Benutzerpasswort wurde durch andere Person als Besitzer geändert und Änderung des Passworts</b> zugeordnet werden.</p>

Warnmeldungstyp	Beschreibung
Ungewöhnlicher Dateizugriff	<p>Überwachen Sie den ungewöhnlichen Dateizugriff, um unsachgemäßen Zugriff auf vertrauliche Dateien und Diebstahl sensibler Daten zu verhindern. Durch die selektive Überwachung von Ansichten, Änderungen und Löschungen von Dateien können Sie möglicherweise unberechtigte Änderungen an sensiblen Dateien erkennen, die durch einen Angriff oder einen Änderungsmanagementfehler verursacht wurden. Dieser Aktivität können die Indikatoren <b>Ungewöhnliches Dateizugriffereignis</b> und <b>Mehrere Datei-Löschen-Ereignisse</b> zugeordnet werden.</p>
Nicht-Standard-Stunden	<p>Alle Authentifizierungsaktivitäten, ob böswillig oder nicht, erscheinen als normale Anmeldungen. Daher sollten Administratoren unerwartet autorisierte Aktivitäten überwachen. Der Schlüssel besteht darin, dass Angreifer diese gestohlenen Zugangsdaten für unbefugten Zugriff nutzen. Dies kann eine Möglichkeit zur Erkennung bieten. Wenn ein Konto für ungewöhnliche Aktivitäten verwendet wird, zum Beispiel für Authentifizierungen mit ungewöhnlicher Häufigkeit, kann das Konto infiziert sein. Durch die Angabe einer ungewöhnlichen Aktivitätszeit können Sie feststellen, ob das Konto von einem externen Akteur übernommen wurde. Dieser Aktivität können die Indikatoren <b>Ungewöhnliche Dateizugriffszeit</b>, <b>Ungewöhnliche Änderungszeit des Active Directory</b> und <b>Ungewöhnliche Anmeldezeit</b> zugeordnet werden.</p>

## Untersuchen von Nutzern mit hohem Risiko

Auf der Grundlage der Bewertung und des Schweregrads der Warnmeldungen wird eine Nutzerbewertung erstellt. Mit Hilfe der Nutzerbewertung können Sie Nutzer identifizieren, die sofortige Aufmerksamkeit benötigen, eine tiefere Untersuchung durchführen und erforderliche Maßnahmen ergreifen. Sie können Nutzer mit hohem Risiko entweder auf der Registerkarte **Übersicht** oder auf der Registerkarte **Benutzer** identifizieren.

Die folgende Abbildung ist ein Beispiel für die fünf Nutzer mit dem höchsten Risiko, die im Bereich **Übersicht** angezeigt werden.



Die folgende Abbildung ist ein Beispiel für alle Nutzer mit hohem Risiko in der Umgebung, die auf der Registerkarte **Benutzer** angezeigt werden.

The screenshot shows the RSA NetWitness UEBA interface. At the top, there are navigation tabs: RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below these are sub-tabs: Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The main interface is divided into sections: OVERVIEW, USERS, and ALERTS. A search bar is located at the top right. On the left, there are filters for Risky Users (947), Watchlist Users (0), and Admin Users (0). The main area shows a summary of 947 users with a risk score of 180 and 20 alerts. Below this, a list of users is displayed with their names, risk scores, and alert counts.

User Name	Risk Score	Alerts
Peyton Mooney	180	20 Alerts
Angela Walker	140	13 Alerts
Hillier Beauchamp	50	5 Alerts

Im Folgenden finden Sie ein übergeordnetes Verfahren zur Untersuchung von Nutzern mit hohem Risiko in Ihrer Umgebung.

1. Identifizieren Sie die Nutzern mit hohem Risiko. Sie können die Nutzern mit hohem Risiko auf folgende Weise identifizieren:
  - Auf der Registerkarte **Übersicht** sind die fünf Nutzer mit dem höchsten Risiko in Ihrer Umgebung aufgeführt. Identifizieren Sie unter den aufgelisteten Nutzern die Nutzer mit kritischem Schweregrad oder einer Nutzerbewertung von mehr als 100 Punkten.
  - Auf der Registerkarte **Benutzer** werden alle risikoreichen Nutzer in Ihrer Umgebung sortiert nach Risikobewertung angezeigt. Identifizieren Sie, wie viele Nutzer mit einem Schweregrad von „Kritisch“, „Hoch“ und „Mittel“ markiert sind, oder identifizieren Sie das bösartige Nutzerverhalten von Nutzern auf der Grundlage der forensischen Untersuchung und erstellen Sie Nutzerlisten mithilfe von Verhaltensfiltern. Zusätzlich können Sie zum Identifizieren einer Zielgruppe risikoreicher Nutzer auch verschiedene Filtertypen (Risikoreich, Administrator oder Überwachungsliste) verwenden.

**Hinweis:** Die Untersuchung sollte sich vor allem auf die Schweregrade „Kritisch“, „Hoch“ und „Mittel“ konzentrieren. Nutzer mit geringen Punktzahlen sind in der Regel keiner Untersuchung wert.

Bewegen Sie den Mauszeiger über die Anzahl der Warnmeldungen, die risikoreichen Nutzern zugeordnet sind. So können Sie schnell erkennen, wie sie aussehen und ob es sich um eine gute Mischung handelt.

**Hinweis:** Die Anzahl der Warnmeldungen korreliert nicht immer mit den höchsten Punktzahlen, da einige Warnmeldungen nur wenige Punkte zur Gesamtpunktzahl eines Nutzers beitragen, aber je mehr Warnmeldungen vorhanden sind, desto einfacher ist es, eine Zeitleiste der Aktivität anzuzeigen, die zu der hohen Punktzahl geführt hat.

Weitere Informationen finden Sie unter [Identifizieren von Nutzern mit hohem Risiko](#).

2. In der Ansicht **Benutzerprofil** untersuchen Sie die Warnmeldungen und Indikatoren eines Nutzers.
  - a. Überprüfen Sie die Liste der mit dem Nutzer verbundenen Warnmeldungen sowie die nach Schweregrad sortierten Bewertungen der einzelnen Warnmeldungen.
  - b. Wenn Sie den Verlauf einer Bedrohung ermitteln möchten, erweitern Sie die Namen der Warnmeldungen. Der stärkste Indikator bestimmt den Namen der Warnmeldung, der auch andeutet, warum diese Stunde markiert ist.
  - c. Mithilfe der Zeitleiste des Warnmeldungsflusses können Sie die ungewöhnlichen Aktivitäten erkennen.
  - d. Überprüfen Sie die Details aller Indikatoren einer Warnmeldung. Dazu gehört auch die Zeitleiste, in der die Anomalie aufgetreten ist. Außerdem können Sie den Incident mithilfe externer Ressourcen wie SIEM, Netzwerkforensik oder durch direkten Kontakt zum Nutzer oder Geschäftsführer usw. untersuchen.

Weitere Informationen finden Sie unter [Starten von Untersuchungen für Nutzer mit hohem Risiko](#) .

3. Nach Abschluss der Untersuchung können Sie Ihre Beobachtung wie folgt aufzeichnen:
  - a. Geben Sie an, ob eine Warnmeldung kein Risiko ist
  - b. Speichern Sie das Verhaltensprofil für den in Ihrer Umgebung gefundenen Anwendungsfall
  - c. Zum Verfolgen der Nutzeraktivität können Sie Nutzer in die Überwachungsliste aufnehmen und das Nutzerprofil verfolgen

Weitere Informationen finden Sie unter [Ergreifen von Maßnahmen für Nutzer mit hohem Risiko](#).

## Identifizieren von Nutzern mit hohem Risiko

Sie können risikoreiche Nutzer in Ihrer Umgebung auf folgende Weise identifizieren:

- Anzeigen der fünf Nutzer mit dem höchsten Risiko
- Anzeigen aller Nutzer mit hohem Risiko
- Anzeigen von Nutzern bestimmter Gruppen
- Anzeigen von Nutzern basierend auf forensischer Untersuchung

## Anzeigen der fünf Nutzer mit dem höchsten Risiko

Auf der Registerkarte **Übersicht** können Sie die Liste der fünf Nutzer mit dem höchsten Risiko in Ihrer Umgebung zusammen mit der Nutzerbewertung anzeigen.



### So zeigen Sie die fünf Nutzer mit dem höchsten Risiko an:

Melden Sie sich bei **NetWitness Platform** an und gehen Sie zu **Untersuchen > Benutzer**. Auf der Registerkarte „Übersicht“ werden die Nutzer mit dem höchsten Risiko im Bereich „Benutzer mit hohem Risiko“ angezeigt.



### Anzeigen aller Nutzer mit hohem Risiko

Auf der Registerkarte **Benutzer** können Sie eine Liste aller risikoreichen Nutzer in Ihrer Umgebung zusammen mit der Nutzerbewertung und der Gesamtzahl der den Nutzern zugeordneten Warnmeldungen anzeigen.

### So zeigen Sie alle Nutzer mit hohem Risiko an:

1. Melden Sie sich bei **NetWitness Platform** an und gehen Sie zu **Untersuchen > Benutzer**. Die Registerkarte „Übersicht“ wird angezeigt.

- Klicken Sie auf die Registerkarte **Benutzer**.  
Die Liste aller risikoreichen Nutzer wird angezeigt.

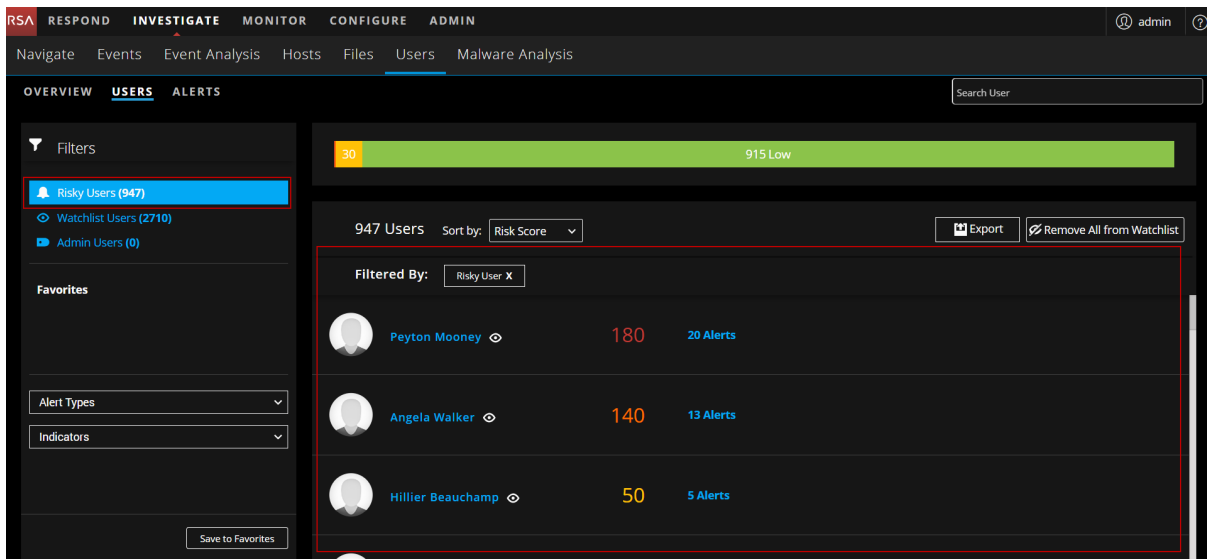
The screenshot shows the RSA NetWitness UEBA interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'Users' section is active, showing a search bar and a 'Search User' input. The main content area displays a list of users filtered by 'Risky User X'. The top bar shows '30' and '915 Low'. The main content area shows a list of users with their risk scores and alert counts. The users listed are Peyton Mooney (180, 20 Alerts), Angela Walker (140, 13 Alerts), and Hillier Beauchamp (50, 5 Alerts). The interface also includes a sidebar with filters and a 'Save to Favorites' button.

## Anzeigen von Nutzern bestimmter Gruppen

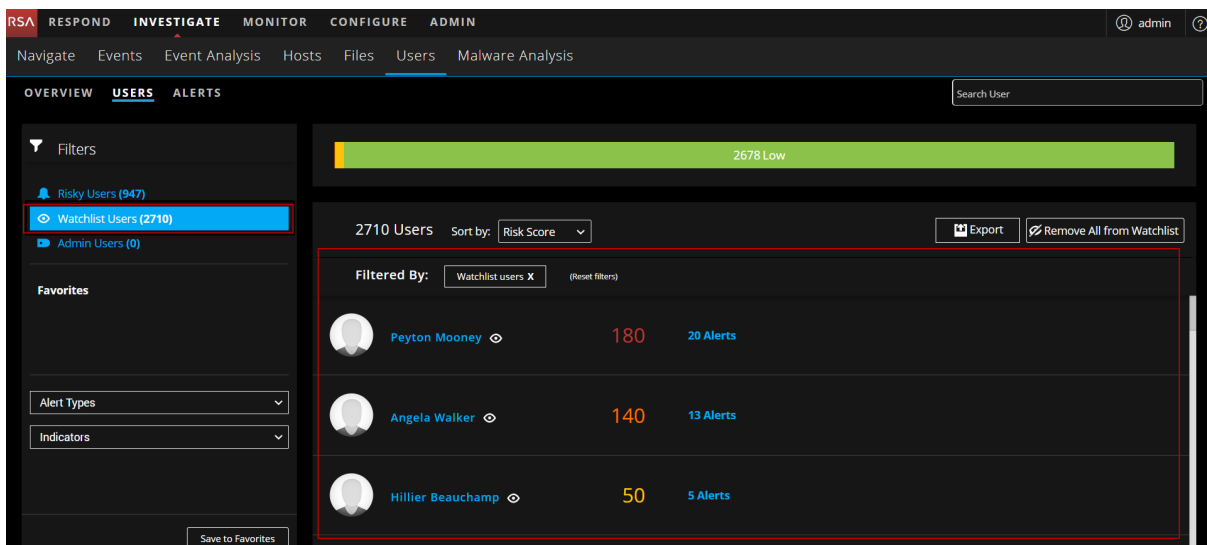
Auf der Registerkarte **Benutzer** können Sie mithilfe verschiedener Filter Zielgruppen von Nutzern mit hohem Risiko identifizieren.

### So zeigen Sie Nutzer bestimmter Gruppen an:

- Melden Sie sich bei **NetWitness Platform** an und gehen Sie zu **Untersuchen > Benutzer**. Die Registerkarte „Übersicht“ wird angezeigt.
- Klicken Sie auf die Registerkarte **Benutzer**.
- Führen Sie im Bereich **Filter** einen der folgenden Schritte aus:
  - Benutzer mit hohem Risiko:** Zum Anzeigen aller Nutzer mit hohem Risiko in Ihrer Umgebung wählen Sie **Benutzer mit hohem Risiko** aus. Standardmäßig werden risikoreiche Nutzer zusammen mit ihrer Nutzerbewertung angezeigt.



- **Benutzerüberwachungsliste:** Zum Anzeigen der Lister der Nutzer, die Sie der Überwachungsliste hinzugefügt haben und für die Sie bestimmte Änderungen überwachen möchten, wählen Sie **Benutzerüberwachungsliste** aus.



- **Administratornutzer:** Zum Anzeigen aller in den Ereignissen als Administrator markierter Nutzer wählen Sie **Administratornutzer** aus.

**Hinweis:** Sie können Nutzer einer oder mehrerer Gruppen durch Auswahl eines oder mehrerer Filter anzeigen. Wenn Sie zum Beispiel die Liste der Administratornutzer mit hohem Risiko anzeigen möchten, wählen Sie die Filter **Administratornutzer** und **Benutzer mit hohem Risiko** aus.

## Anzeigen von Nutzern basierend auf forensischer Untersuchung

Auf der Registerkarte **Benutzer** können Sie Warnmeldungstypen und Indikatoren als Filter für die Anzeige von Nutzern mit hohem Risiko basierend auf forensischer Untersuchung verwenden. Weitere Informationen zur forensischen Untersuchung finden Sie unter *Forensischer Workflow* im Thema [Einführung](#).

### So zeigen Sie Nutzer basierend auf einer bestimmten forensischen Untersuchungen an:

1. Melden Sie sich bei **NetWitness Platform** an und gehen Sie zu **Untersuchen > Benutzer**. Die Registerkarte „Übersicht“ wird angezeigt.
2. Klicken Sie auf die Registerkarte **Benutzer**.
3. Zum Erstellen eines Verhaltensfilters mithilfe von Warnmeldungstypen wählen Sie in der Drop-down-Liste **Warnmeldungstypen** einen oder mehrere Warnmeldungen aus.
4. Zum Erstellen eines Verhaltensfilters mithilfe von Indikatoren wählen Sie in der Drop-down-Liste **Indikatoren** einen oder mehrere Indikatoren aus.

**Hinweis:** Sie können eine Kombination aus einem oder mehreren Warnmeldungstypen und Indikatoren auswählen und so einen auf Ihren Anforderungen basierenden Verhaltensfilter erstellen. Zum Überwachen von ungewöhnlichem Zugriff auf vertrauliche Dateien und des Diebstahls sensibler Daten können Sie einen Verhaltensfilter mit den Warnmeldungstypen **Ungewöhnlicher Dateizugriff** und den Indikatoren **Ungewöhnliche Dateioperation** erstellen.

The screenshot shows the RSA NetWitness Platform interface. The top navigation bar includes 'RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN' and a user profile 'admin'. Below the navigation bar, there are tabs for 'OVERVIEW', 'USERS', and 'ALERTS'. The 'USERS' tab is active, showing a search bar and a 'Filters' sidebar. The sidebar contains 'Filters' (Risky Users (947), Watchlist Users (2710), Admin Users (0)), 'Favorites', and a section for 'Alert Types: abnormal\_file\_access' and 'Indicator Types: abnormal\_file\_action\_operation\_t...'. The main content area shows '56 Users' sorted by 'Risk Score'. A table lists three users: Darsey Moohan (26 users, 3 Alerts), Manya Padefield (16 users, 7 Alerts), and Pincas Lambart (15 users, 1 Alerts). A 'Save to Favorites' button is visible at the bottom of the sidebar.

Speichern Sie diese Verhaltensfilter als Favoriten für zukünftige Untersuchungen.

## Starten von Untersuchungen für Nutzer mit hohem Risiko

Nach der Identifizierung der Nutzer mit hohem Risiko können Sie mit der Untersuchung selbiger beginnen.

## So untersuchen Sie Nutzer mit hohem Risiko:

1. Melden Sie sich bei **NetWitness Platform** an und gehen Sie zu **Untersuchen > Benutzer**. Führen Sie eine der folgenden Aktionen aus:
  - a. Wählen Sie auf der Registerkarte **Übersicht** im Bereich **Benutzer mit hohem Risiko** einen zu untersuchenden Nutzer aus und klicken Sie entweder auf den Nutzernamen oder auf die Nutzerbewertung.
  - b. Klicken Sie auf der Registerkarte **Benutzer** auf den Namen des zu untersuchenden Nutzers. Die Ansicht „Benutzerprofil“ wird angezeigt.
2. Um die Warnmeldungen des Nutzers zu untersuchen, klicken Sie auf den Namen der Warnmeldung im Bereich **Benutzerrisikobewertung**. Die folgenden Informationen werden angezeigt:
  - Die Namen der Warnmeldungen
  - Der Zeitrahmen der Warnmeldung (stündlich oder täglich)
  - Das Schweregrad-Symbol
  - Der Beitrag zur Nutzerpunktzahl (z. B. +20)
  - Die Datenquellen für die Warnmeldung (z. B. Anmeldung)

Der mittlere Bereich ist der Bereich „Warnmeldungsfluss“. In diesem Bereich wird eine Zeitleiste von mit der Bildung der Warnmeldung zusammenhängenden Ereignisse bereitgestellt. Mithilfe der Zeitleiste der Ereignisse können Sie feststellen, ob die Warnmeldung ein tatsächliches Risiko darstellt oder nicht.

The screenshot shows the RSA NetWitness UEBA interface. At the top, there are navigation tabs: RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, there are sub-tabs: Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The main content area is titled 'OVERVIEW USERS ALERTS' and features a search bar for 'Search User'. The user profile for 'Peyton Mooney' is displayed, including a 'Stop Watching' button. The 'User Risk Score' is prominently shown as 180. Below the score, there is a list of alerts, with the top one being 'mass\_changes\_to\_groups' (Hourly) with a contribution of +20 points. The 'Alert Flow' section shows a timeline of events on 07/23/2018, with a 'mass\_changes\_to\_groups' alert highlighted.

3. Um die Indikatoren im Zusammenhang mit der Warnmeldung eines Nutzers zu untersuchen, wählen Sie im Bereich **Benutzerrisikobewertung** eine Warnmeldung und dann einen Indikator aus. Die folgenden Informationen werden angezeigt:
  - Der Indikatorname und eine Beschreibung des Indikatorstyps
  - Beitrag zur Warnmeldung
  - Die Anomaliewerte

- Die Datenquelle der Ereignisse, die im Indikator gefunden werden  
Die Anzeige im mittleren Bereich ändert sich abhängig vom ausgewählten Indikator.

The screenshot displays the RSA NetWitness UEBA interface. At the top, there are navigation tabs: RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, there are sub-tabs: Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The main content area is divided into several sections:

- User Profile:** Shows a profile picture and the name "Peyton Mooney".
- User Risk Score:** A large red number "180" is displayed, with a "Sort By Severity" dropdown menu below it.
- Alerts:** A list of alerts is shown, including "mass\_changes\_to\_groups | Hourly" (01-30-2018 | 12:00 AM) and "Multiple User Account Changes (30)".
- Indicator Details:** A detailed view of the "mass\_changes\_to\_groups | Hourly" indicator is shown. It includes:
  - Indicator: Multiple User Account Changes (Hourly)
  - Contribution to Alert: 43%
  - Anomaly Value: 30
  - Datasource: Active Directory
- Sensitive Active Directory Changes (Last 30 Days):** A bar chart showing the frequency of sensitive AD changes over time, with a red bar indicating a recent spike.
- Event Log Table:** A table showing the details of the event:
 

TIME DETECTED	USERNAME	USER ID	OPERATION TYPE	OPERATION TYPE CATEGORY	OBJECT NAME	RESULT
01/30/2018 00:43:12	Mooney, Peyton	pimooney	User Password Changed	SECURITY_SENSITIVE_OPERATION, USER_CHANGE_OPERATION	Duwall, Lisa	Success

## Ergreifen von Maßnahmen für Nutzer mit hohem Risiko

Nach der Ermittlung können Sie Maßnahmen gegen die risikoreichen Nutzer ergreifen und damit weitere Schäden durch böswillige Angreifer in Ihrer Organisation reduzieren oder verhindern. Sie können eine der folgenden Maßnahmen ergreifen:

- Geben Sie an, ob eine Warnmeldung kein Risiko ist
- Speichern Sie das Verhaltensprofil für den in Ihrer Umgebung gefundenen Anwendungsfall
- Zum Verfolgen der Nutzeraktivität können Sie Nutzer in die Überwachungsliste aufnehmen und das Nutzerprofil überwachen

## Geben Sie an, ob eine Warnmeldung kein Risiko ist.

### So geben Sie an, ob eine Warnmeldung kein Risiko ist:

1. Melden Sie sich bei **NetWitness Platform** an und gehen Sie zu **Ermittlung > Benutzer**.
2. Auf den folgenden Registerkarten ergreifen Sie Maßnahmen für die Nutzer:
  - a. Wählen Sie auf der Registerkarte **Übersicht** im Bereich **Benutzer mit hohem Risiko** einen Nutzer aus und klicken Sie entweder auf den Nutzernamen oder auf die Nutzerbewertung.
  - b. Klicken Sie auf der Registerkarte **Benutzer** auf den Benutzernamen. Die Ansicht „Benutzerprofil“ wird angezeigt.
3. Wenn die Warnmeldung kein Risiko darstellt, klicken Sie auf **Kein Risiko**.

The screenshot shows the RSA NetWitness UEBA interface. At the top, there are navigation tabs: RESPOND, INVESTIGATE, MONITOR, CONFIGURE, ADMIN. Below that, there are sub-tabs: OVERVIEW, USERS, ALERTS. The main content area shows the user profile for Peyton Mooney. On the left, there is a 'User Risk Score' section with a score of 180. Below that, there is an 'Alerts' section with a list of alerts. One alert, 'mass\_changes\_to\_groups', is highlighted with a red box and labeled 'Not a Risk'. The alert details show a contribution to the user score of 20 points from Active Directory. The 'Alert Flow' section shows a timeline of events from 07/23/2018 | 01:20 PM.

Wenn eine Warnmeldung als **Kein Risiko** markiert wird, reduziert sich die Benutzerbewertung automatisch.

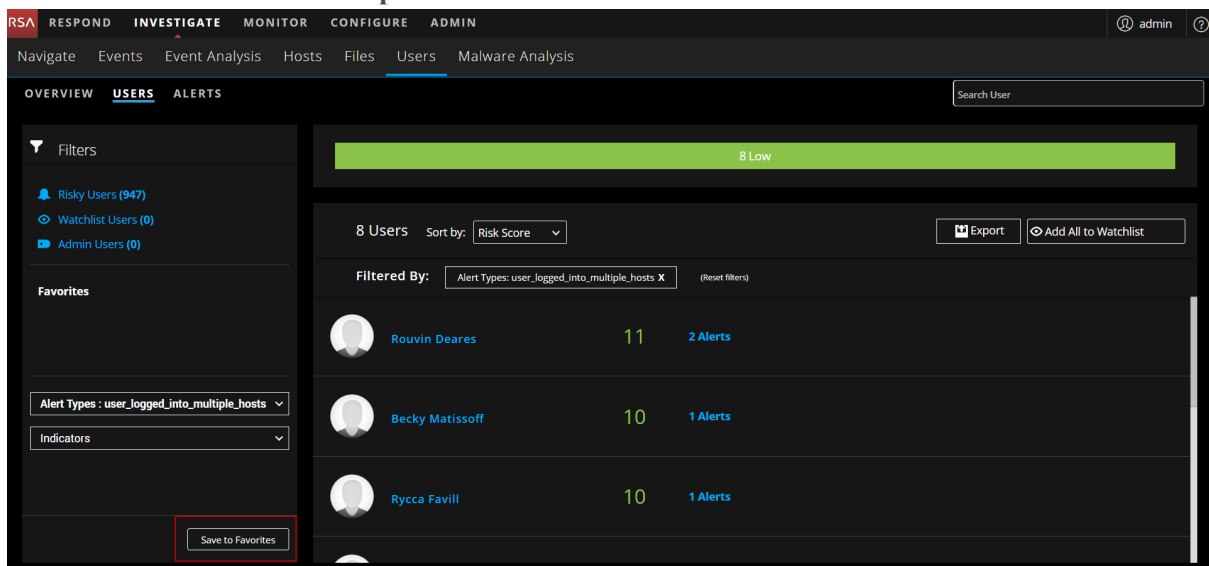
## Speichern von Verhaltensmustern

Die Kombination der Warnmeldungstypen und Indikatoren, die Sie bei der forensischen Untersuchung auswählen, ist ein Verhaltensprofil. Sie können das Verhaltensprofil speichern, damit Sie diesen Anwendungsfall in Zukunft überwachen können.

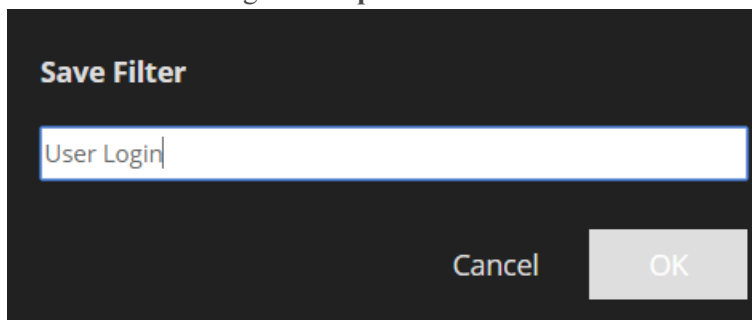
Wenn z. B. Angreifer einen Brute-Force-Angriff auf die Nutzerkonten Ihrer Organisation vornehmen, können Filter für den Warnmeldungstyp „Brute-Force“ auswählen. Dieser Filter kann als Favorit gespeichert werden. So können Sie zukünftige Brute-Force-Versuche proaktiv überwachen. Klicken Sie dazu auf den Favoriten. So können Sie erkennen, ob neue Nutzer Opfer dieses Angriffstyps geworden sind.

### So speichern Sie ein Verhaltensprofil:

1. Melden Sie sich bei **NetWitness Platform** an und gehen Sie zu **Ermittlung > Benutzer**. Die Registerkarte „Übersicht“ wird angezeigt.
2. Klicken Sie auf die Registerkarte **Benutzer**.
3. Wählen Sie im Bereich **Favoriten** im Drop-down-Menü **Warnmeldungstyp** die Warnmeldung und im Drop-down-Menü **Indikatoren** die Indikatoren aus.
4. Klicken Sie auf **In Favoriten speichern**.



5. Geben Sie im Dialog **Filter speichern** den Namen des Filters ein und klicken Sie auf **Ok**.



Das Verhaltensprofil wird gespeichert und im Bereich „Favoriten“ angezeigt. Zum Überwachen der Nutzer können Sie in den Favoriten auf das Profil klicken.

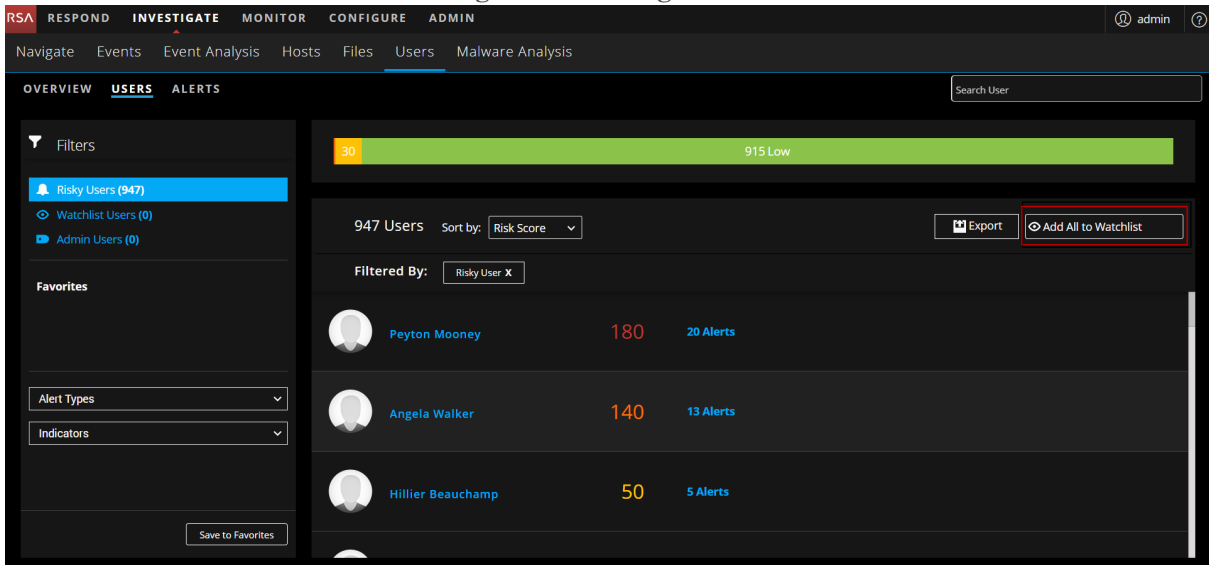
### Hinzufügen aller Nutzer in der Überwachungsliste

Wenn Sie Nutzer und deren jüngste Aktivität nachverfolgen möchten, um eine sofortige Untersuchung zu beginnen, können Sie die Nutzer der Überwachungsliste hinzufügen. So können Sie jederzeit überprüfen, ob die Risikobewertung gestiegen ist.



## So fügen Sie der Überwachungsliste alle Nutzer hinzu:

1. Melden Sie sich bei **NetWitness Platform** an und gehen Sie zu **Ermittlung > Benutzer**. Die Registerkarte „Übersicht“ wird angezeigt.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie mithilfe von Filtern Nutzer bestimmter Kategorien aus.
4. Klicken Sie auf **Alle zur Überwachungsliste hinzufügen**.



Die Liste der Nutzer wird in die Überwachungsliste aufgenommen.

## Anzeigen eines Nutzerprofils

Das Nutzerüberwachungsprofil ist eine Liste der Nutzer, die Sie auf potenzielle Bedrohungen überwachen möchten. Im Nutzerüberwachungsprofil wird ein Nutzer markiert, damit im Dashboard ein schneller Verweis auf den Nutzer erstellt wird. Dabei handelt es sich im Wesentlichen um ein Lesezeichen, mit Sie verdächtige Nutzer überwachen können.

## So überwachen Sie ein Nutzerprofil:

1. Melden Sie sich bei **NetWitness Platform** an und gehen Sie zu **Ermittlung > Benutzer**. Führen Sie eine der folgenden Aktionen aus:
  - a. Wählen Sie auf der Registerkarte **Übersicht** im Bereich **Benutzer mit hohem Risiko** einen Nutzer aus und klicken Sie entweder auf den Nutzernamen oder auf die Nutzerbewertung.
  - b. Klicken Sie auf der Registerkarte **Benutzer** auf einen Benutzernamen. Die Ansicht „Benutzerprofil“ wird angezeigt.
2. Klicken Sie in oben rechts im Nutzerprofil auf **Überwachungsprofil**.

The screenshot displays the user profile for Angela Walker. The interface includes a navigation bar with tabs for OVERVIEW, USERS, and ALERTS. A search bar is located in the top right. The main content area shows the user's risk score (140) and a list of alerts, including 'mass\_changes\_to\_groups | Hourly' with a severity of 'High'. The 'Alert Flow' section shows a timeline of events. A red box highlights the 'Watch Profile' button in the top right corner of the user profile card.

Der Nutzer wird in die Überwachungsliste aufgenommen.

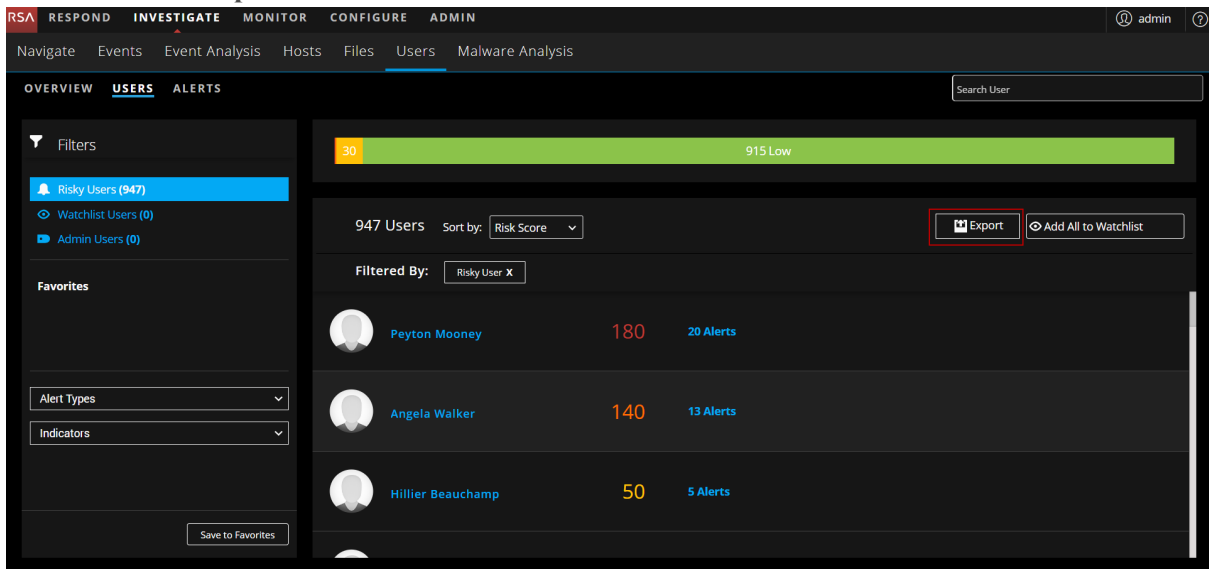
## Exportieren von Nutzern mit hohem Risiko

Sie können eine Liste aller Nutzer und deren Bewertung in eine CSV-Datei exportieren. Anhand dieser Informationen können sie mit anderen Datenanalysewerkzeugen wie Tableau, Powerbi, Zeppelin verglichen werden.

### So exportieren Sie Nutzer mit hohem Risiko:

1. Navigieren Sie zu **UNTERSUCHEN > Benutzer**. Die Registerkarte „Übersicht“ wird angezeigt.
2. Wählen Sie die Registerkarte **Benutzer** aus.

### 3. Klicken Sie auf **Exportieren**.

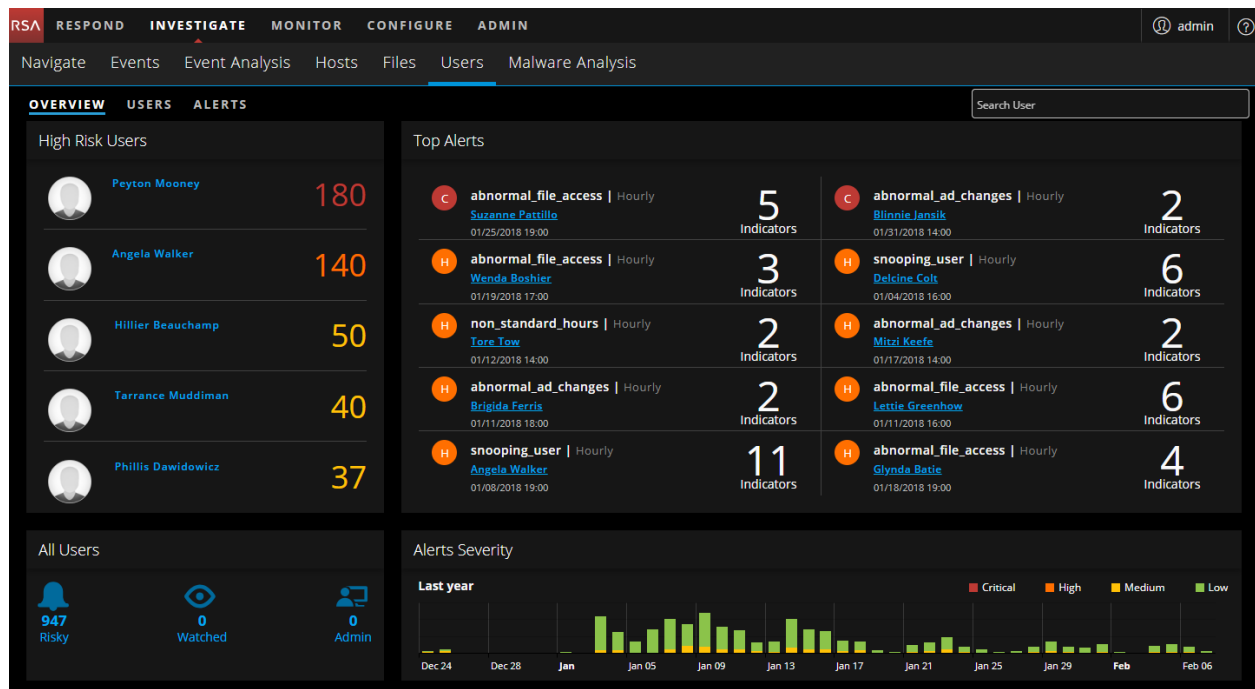


Die Liste aller Nutzer und die zugehörige Nutzerbewertung werden in eine CSV-Datei heruntergeladen.

## Untersuchen von Top-Warmmeldungen

Anomalien, die bei eingehenden Ereignissen gefunden werden, werden mit der Baseline verglichen und in stündlichen Warmmeldungen zusammengefasst. Relativ starke Abweichungen von der Baseline in Kombination mit einer einzigartigen Zusammensetzung von Anomalien erhalten eher eine höhere Warmmeldungsbewertung.

Sie können schnell die wichtigsten Warmmeldungen in Ihrer Umgebung sehen und diese entweder auf der Registerkarte „ÜBERSICHT“ oder auf der Registerkarte „WARNMELDUNGEN“ untersuchen. In der folgenden Abbildung ist ein Beispiel für die Top-Warmmeldungen auf der Registerkarte „ÜBERSICHT“ dargestellt. Die Warmmeldungen werden in der Reihenfolge des Schweregrads und der Anzahl der Nutzer aufgelistet, die die Warmmeldungen generieren.



Zum Untersuchen einer Warmmeldung auf dieser Seite klicken Sie im Abschnitt **Top-Warmmeldungen** auf eine Warmmeldung, sodass die entsprechenden Details angezeigt werden.

In der folgenden Abbildung sind Details über das Ereignis, das die Warnmeldung verursacht hat, und den Zeitrahmen seines Auftretens dargestellt.

The screenshot shows the 'USERS' section for 'Peyton Mooney'. On the left, the 'User Risk Score' is 180. The main area displays an alert for 'mass\_changes\_to\_groups' with a severity of 'Critical' (C). The alert details include:

- Indicator: mass\_changes\_to\_groups | Hourly
- Contribution to Alert: 43%
- Anomaly Value: 30
- Datasource: Active Directory

A bar chart shows 'Sensitive Active Directory Changes (Last 30 Days)' with a peak on Jan 29. Below the chart is a table of detected events:

TIME DETECTED	USERNAME	USER ID	OPERATION TYPE	OPERATION TYPE CATEGORY	OBJECT NAME	RESULT
01/30/2018 00:43:12	Mooney, Peyton	pimooney	User Password Changed	SECURITY_SENSITIVE_OPERATION, USER_CHANGE_OPERATION	Duwall, Lisa	Success
01/30/2018 00:43:12	Mooney, Peyton	pimooney	User Account Enabled	SECURITY_SENSITIVE_OPERATION, USER_CHANGE_OPERATION	Duwall, Lisa	Success
01/30/2018 00:43:12	Mooney, Peyton	pimooney	User Password Changed By Non Owner	SECURITY_SENSITIVE_OPERATION, USER_CHANGE_OPERATION	Duwall, Lisa	Success

Auf der Registerkarte „ÜBERSICHT“ können Sie im Bereich „Schweregrade für Systemwarnungen“ zum Überprüfen der wichtigsten Warnmeldungen auf der Registerkarte „WARNMELDUNGEN“ auf eine Leiste im Diagramm klicken (siehe folgende Abbildung).

The screenshot shows the 'ALERTS' section. At the top, there is a summary of alert counts by severity: 5 Critical (C), 0 High (H), 0 Medium (M), and 0 Low (L). Below this is a table of alerts for the date range 'Jul 17, 2018':

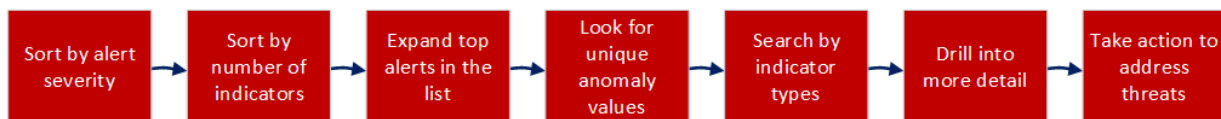
ALERT NAME	ENTITY NAME	START TIME	# INDICATORS	STATUS	FEEDBACK
Snooping User   Hourly	CHunsto	07/17/2018 23:00	2	Unreviewed	No feedback
Brute Force Authentication   Hourly	LBargh	07/17/2018 22:00	3	Unreviewed	No feedback
Multiple Logons by User   Hourly	NHeasem	07/17/2018 21:00	2	Unreviewed	No feedback
Non-Standard Hours   Hourly	AKeelin	07/17/2018 21:00	1	Unreviewed	No feedback
Snooping User   Hourly	GStitso	07/17/2018 20:00	2	Unreviewed	No feedback

At the bottom of the alert list, there is a pagination control showing '10 Items per page' and '1 - 5 of 5 Items'.

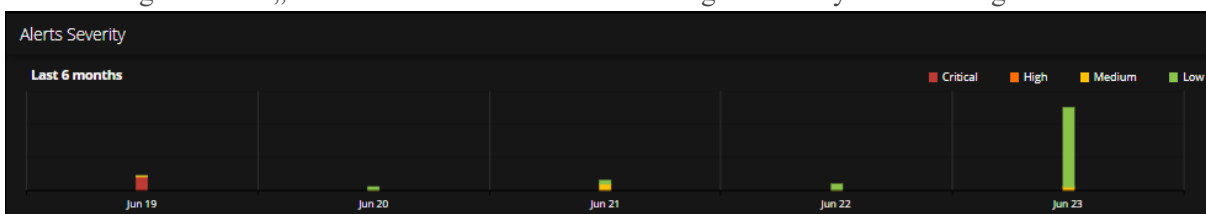
Die Untersuchung von Warnmeldungen ist besonders nützlich, wenn Sie sich auf einen Zeitrahmen konzentrieren wollen, in dem Ihr System vermutlich infiziert wurde. Sie können forensische Informationen anhand eines Zeitrahmens einsehen und detaillierte Informationen über Ereignisse sammeln, die sich während dieser Zeit auf der Registerkarte „Warnmeldungen“ ereignet haben.

## Starten einer Ermittlung kritischer Warnmeldungen

Sie können Ihre Ermittlung kritischer Warnmeldungen auf folgende Weise beginnen:

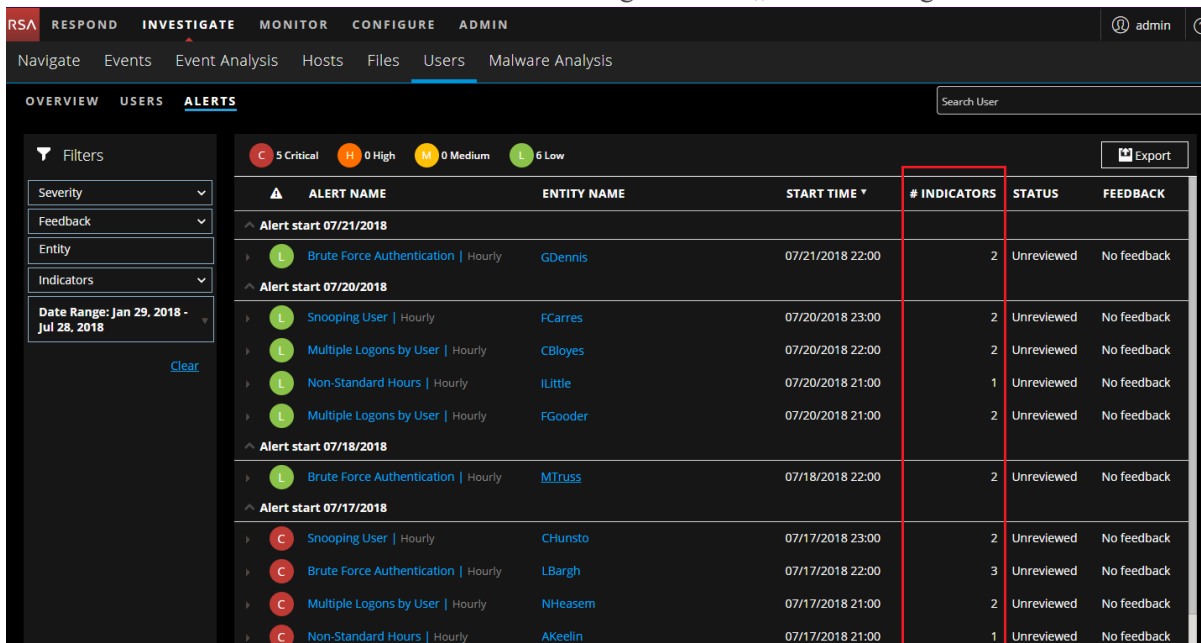


1. Auf der Registerkarte „Übersicht“ sehen Sie den Schweregrade für Systemwarnungen.



Gibt es eine gleichmäßige Verteilung der Warnmeldungen oder ist an einigen Tagen ein spürbarer Anstieg zu verzeichnen? Eine Spitze könnte auf etwas Verdächtiges wie Malware hinweisen. Notieren Sie sich diese Tage, damit Sie die Warnmeldungen überprüfen können (die Leiste aus dem Diagramm enthält einen direkten Link zu den Warnmeldungen für einen bestimmten Tag).

2. Sortieren Sie die Anzahl der Indikatoren auf der Registerkarte „Warnmeldungen“:



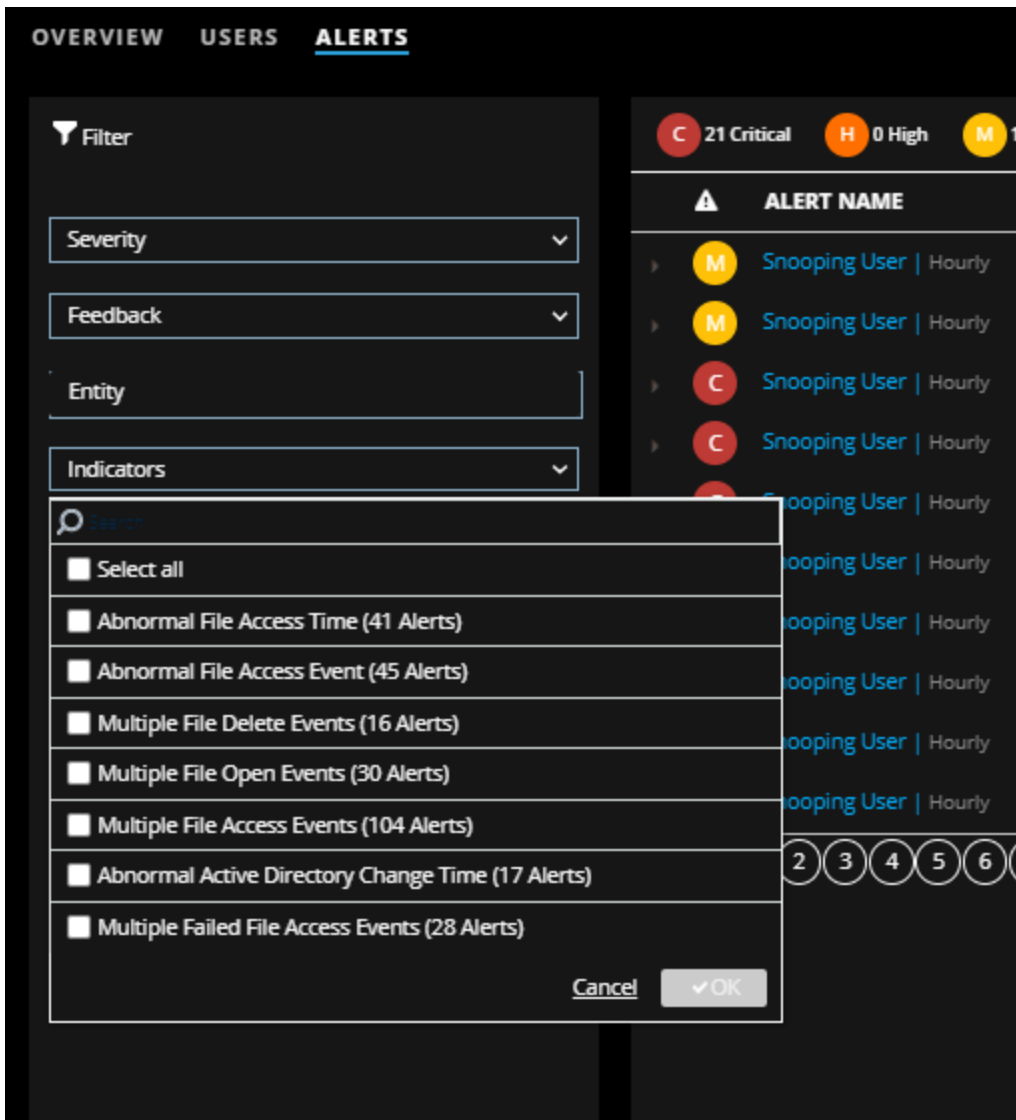
Stellen Sie sicher, dass die in den meisten Indikatoren aggregierten Warnmeldungen oben in der Liste angezeigt werden. Ähnlich wie bei der Identifizierung der Nutzer mit der höchsten Anzahl von Warnmeldungen kann mithilfe vieler Indikatoren ein aussagekräftigeres Bild erstellt werden und Sie erhalten eine solidere Zeitleiste zur Nachverfolgung.

3. Erweitern Sie die wichtigsten Warnmeldungen in der Liste:

- Suchen Sie nach Warnmeldungen mit unterschiedlichen Datenquellen. Diese zeigen ein breiteres Verhaltensmuster.
- Suchen Sie nach einer Vielzahl verschiedener Indikatoren.
- Suchen Sie nach Indikatoren mit hohen numerischen Werten, insbesondere nach hohen Werten, die nicht auf durch einen Menschen manuell ausführbare Aktivitäten hindeuten (z. B. wenn ein Nutzer auf 8.000 Dateien zugegriffen hat).

4. Suchen Sie nach einzigartigen Windows-Ereignistypen, die Nutzer normalerweise nicht ändern, da diese verdächtige administrative Aktivitäten anzeigen können.

## 5. Suche nach Indikatoren:



In der Liste wird die Anzahl der ausgegebenen Warnmeldungen aufgeführt, die jeden Indikator enthalten.

- Suchen Sie nach den häufigsten Indikatoren. Filtern Sie nach einem bestimmten Indikator und suchen Sie nach Nutzern mit der höchsten Anzahl dieses Indikators.
- In der Regel können Sie zeitbasierte Warnmeldungen (z. B. ungewöhnliche Anmeldezeit) ignorieren, da diese sehr häufig sind. Sie bieten jedoch einen guten Kontext, wenn sie mit interessanteren Indikatoren kombiniert werden.

## 6. Zeigen Sie Details an:

- Erstellen Sie mithilfe von Warnmeldungsname ein Bedrohungsnarrativ. Der einflussreichste Indikator legt in der Regel den Namen der Warnmeldung fest. Nutzen Sie diese Tatsache als Erläuterung für den Grund der Markierung dieses Nutzers.



- Skizzieren Sie die gefundenen Aktivitäten mithilfe der Zeitleiste und suchen Sie nach möglichen Ursachen für die beobachteten Verhaltensweisen.
  - Prüfen Sie weiterhin jeden Indikator und zeigen Sie, wie Supportinformationen in Form von Grafiken oder Ereignissen die Analysen bei der Überprüfung eines Incidents unterstützen können. Schlagen Sie mögliche nächste Untersuchungsphasen mit externen Ressourcen vor (z. B. SIEM, Netzwerkforensik und direkter Kontakt zum Nutzer oder Geschäftsführer).
  - Bitten Sie um Feedback und Kommentare und schließen Sie damit die Untersuchung ab.
7. Ergreifen Sie Maßnahmen, mit denen Sie die durch Ihre Ermittlung der Warnmeldungen ermittelten Bedrohungen beheben. Weitere Informationen finden Sie unter [Ergreifen von Maßnahmen für Nutzer mit hohem Risiko](#).

In den folgenden Themen werden verschiedene Möglichkeiten für die Untersuchung von Warnmeldungen beschrieben.

- [Filtern von Warnmeldungen](#)
- [Untersuchen von Indikatoren](#)
- [Top-Warnmeldungen verwalten](#)
- [Anzeigen von NetWitness UEBA-Metriken zu Integrität und Zustand](#)

## Filtern von Warnmeldungen

Sie können die auf der Registerkarte „Warnmeldungen“ angezeigten Warnmeldungen nach Schweregrad, Feedback, Entität, Indikatoren und Datumsbereich filtern.

1. Melden Sie sich bei NetWitness Platform an und gehen Sie zu **UNTERSUCHEN > Benutzer > WARNMELDUNGEN**. Die Registerkarte „Warnmeldungen“ wird angezeigt.

ALERT NAME	ENTITY NAME	START TIME	# INDICATORS	STATUS	FEEDBACK
<b>Alert start 07/21/2018</b>					
Brute Force Authentication   Hourly	GDennis	07/21/2018 22:00	2	Unreviewed	No feedback
<b>Alert start 07/20/2018</b>					
Snooping User   Hourly	FCarres	07/20/2018 23:00	2	Unreviewed	No feedback
Multiple Logons by User   Hourly	CBloyes	07/20/2018 22:00	2	Unreviewed	No feedback
Non-Standard Hours   Hourly	ILittle	07/20/2018 21:00	1	Unreviewed	No feedback
Multiple Logons by User   Hourly	FGooder	07/20/2018 21:00	2	Unreviewed	No feedback
<b>Alert start 07/18/2018</b>					
Brute Force Authentication   Hourly	MTruss	07/18/2018 22:00	2	Unreviewed	No feedback
<b>Alert start 07/17/2018</b>					
Snooping User   Hourly	CHunsto	07/17/2018 23:00	2	Unreviewed	No feedback
Brute Force Authentication   Hourly	LBargh	07/17/2018 22:00	3	Unreviewed	No feedback
Multiple Logons by User   Hourly	NHeasem	07/17/2018 21:00	2	Unreviewed	No feedback
Non-Standard Hours   Hourly	AKeelin	07/17/2018 21:00	1	Unreviewed	No feedback

2. Wenn Sie nach Schweregrad filtern möchten, klicken Sie im Bereich **Warnmeldungsfilter** auf **Schweregrad**, wählen Sie eine oder mehrere Optionen aus und klicken Sie dann auf **OK**. Die Optionen sind „Alle auswählen“, „Kritisch“, „Hoch“, „Mittel“ und „Niedrig“.
3. Zum Filtern nach Feedback klicken Sie unter **Feedback** auf den Pfeil nach unten, wählen Sie eine oder mehrere Optionen aus und klicken Sie dann auf **OK**. Die Optionen sind „Alle auswählen“, „Kein Feedback“ und „Kein Risiko“.
4. Zum Filtern nach Entität geben Sie einen Benutzernamen oder den Namen einer Entität in das Feld **Entität** ein.

ALERT NAME	ENTITY NAME	START TIME	# INDICATORS	STATUS	FEEDBACK
<b>Alert start 07/21/2018</b>					
Brute Force Authentication   Hourly	GDennis	07/21/2018 22:00	2	Unreviewed	No feedback
<b>Alert start 07/20/2018</b>					
Snooping User   Hourly	FCarres	07/20/2018 23:00	2	Unreviewed	No feedback
Multiple Logons by User   Hourly	CBloyes	07/20/2018 22:00	2	Unreviewed	No feedback
Non-Standard Hours   Hourly	ILittle	07/20/2018 21:00	1	Unreviewed	No feedback
Multiple Logons by User   Hourly	FGooder	07/20/2018 21:00	2	Unreviewed	No feedback
<b>Alert start 07/18/2018</b>					
Brute Force Authentication   Hourly	MTruss	07/18/2018 22:00	2	Unreviewed	No feedback
<b>Alert start 07/17/2018</b>					
Snooping User   Hourly	CHunsto	07/17/2018 23:00	2	Unreviewed	No feedback
Brute Force Authentication   Hourly	LBargh	07/17/2018 22:00	3	Unreviewed	No feedback
Multiple Logons by User   Hourly	NHeasem	07/17/2018 21:00	2	Unreviewed	No feedback
Non-Standard Hours   Hourly	AKeelin	07/17/2018 21:00	1	Unreviewed	No feedback

5. Zum Filtern nach Datumsbereich klicken Sie für den **Datumsbereich** auf den Pfeil nach unten, wählen Sie eine Option aus und klicken Sie dann auf **OK**. Die Optionen sind „Letzte Woche“, „Letzter Monat“ und „Bereich auswählen“.

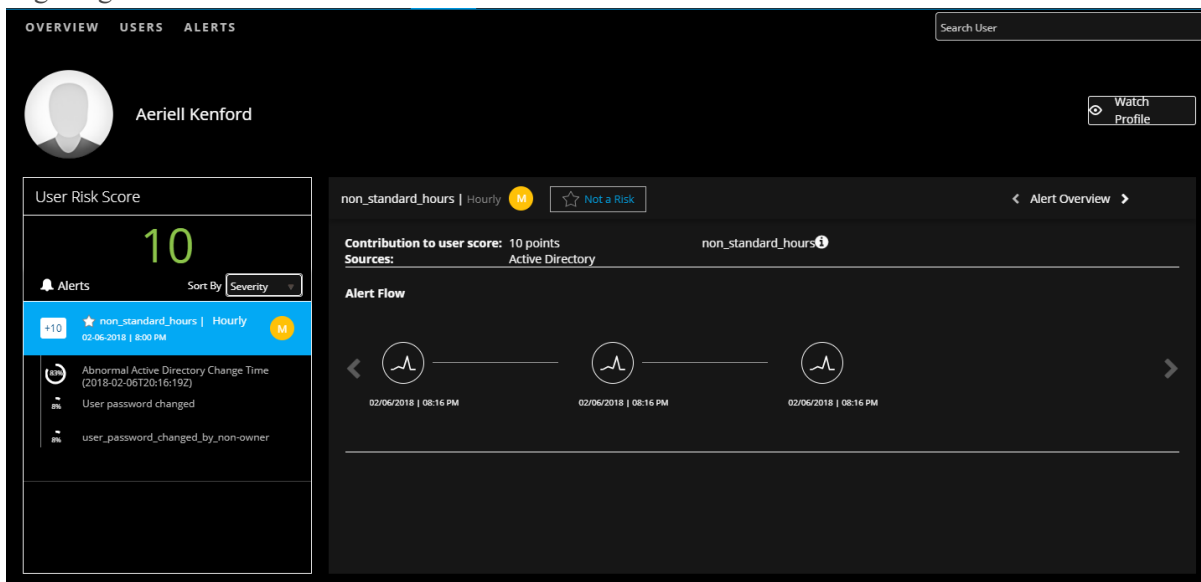
Die Warnmeldungen werden je nach dem von Ihnen gewählten Filter im rechten Bereich angezeigt. Zum Löschen eines Filters klicken Sie im linken Bereich auf **Löschen**.

## Untersuchen von Indikatoren

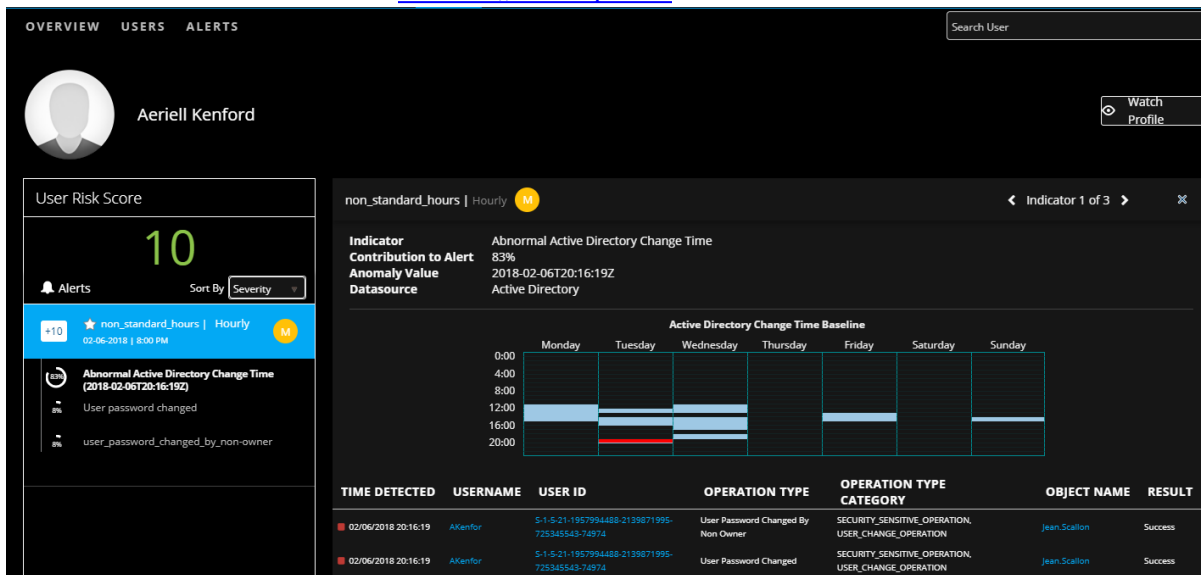
Auf der Registerkarte „WARNMELDUNGEN“ können Sie alle Indikatoren zu einer Warnmeldung anzeigen. Zu jedem Indikator wird zudem ein Anomaliewert in Klammern angezeigt. Sie sehen den Indikatornamen und eine Beschreibung des Indikatortyps, die Anomaliewerte und die Datenquelle der Ereignisse im Indikator. Sie können auch ein Diagramm mit Details zu einem bestimmten Indikator anzeigen. Sie können einen Indikator untersuchen, mit dem Sie über einen Zeitraum nach verwandten Aktivitäten suchen. Wechseln Sie dazu in die Ansicht **UNTERSUCHEN > Ereignisse**. In der Ansicht „Benutzer“ werden Werte, für die in eine andere Ansicht gewechselt werden kann, in Hellblau hervorgehoben. Zum Öffnen der Ansicht „Ereignis“ können Sie auf einen Wert klicken. In der Ansicht „Ereignis“ wird der ausgewählte Wert in allen Metaschlüsseln festgelegt und der Zeitbereich wird auf einen Tag eingestellt. Sie können den Zeitbereich ändern.

### So zeigen Sie alle Bedrohungsindikatoren mit Warnmeldungen an:

1. Melden Sie sich bei NetWitness Platform an und gehen Sie zu **UNTERSUCHEN > Benutzer > WARNMELDUNGEN**.
2. Klicken Sie unter **NAME DER WARNMELDUNG** auf einen Warnmeldungsnamen. Die Indikatoren werden zusammen mit dem Anomaliewert, der Datenquelle und der Startzeit angezeigt.



3. Klicken Sie unter **Warnmeldungsfluss** auf das Diagrammsymbol. Es wird ein Diagramm mit Details zu einem bestimmten Indikator angezeigt, einschließlich der Zeitleiste, in der die Anomalie aufgetreten ist, und dem mit dem Indikator verbundenen Benutzer. In der folgenden Abbildung ist ein Beispiel für ein Diagramm dargestellt. Die Art der Grafik kann abhängig von der Art der von NetWitness UEBA durchgeführten Analyse variieren. Weitere Informationen erhalten Sie unter [Ansicht „Nutzerprofil“](#).

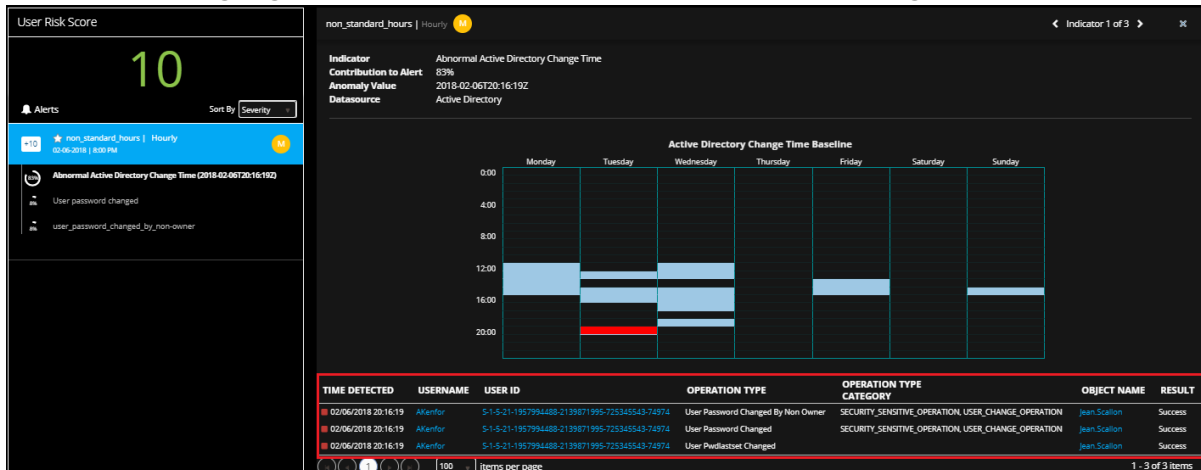


**So wechseln Sie in die Ansicht „Ereignisse“:**

1. Navigieren Sie zu **UNTERSUCHEN > Benutzer** und wählen Sie eine Warnmeldung oder einen Benutzer aus.
2. Wählen Sie unter **Benutzerrisikobewertung** einen Namen der Warnmeldung aus.  
Unter der Warnmeldung werden Indikatoren angezeigt.

The screenshot displays the 'User Risk Score' interface. At the top, the title 'User Risk Score' is shown. Below it, a large green number '10' represents the risk score. To the left of the score is a bell icon labeled 'Alerts', and to the right is a 'Sort By' dropdown menu set to 'Severity'. A blue horizontal bar contains a '+10' indicator, a star icon, the text 'non\_standard\_hours | Hourly', and a yellow circle with the letter 'M'. Below this bar, a red-bordered box highlights a specific alert: 'Abnormal Active Directory Change Time (2018-02-06T20:16:19Z)'. This alert is associated with a 83% risk score and includes two indicators, each with an 8% weight: 'User password changed' and 'user\_password\_changed\_by\_non-owner'.

- Wählen Sie einen interessanten Indikator aus.  
Zum Umschalten geeignete Werte werden unten im Bereich hellblau hervorgehoben.



- Klicken Sie auf ein in blau hervorgehobenes Indikatorelement.  
In der geöffneten Ansicht „Ereignisse“ werden Details zum Indikatorelement angezeigt.  
Das Datum in der Ansicht „Ereignisse“ ist der Tag, an dem die Warnmeldung aufgetreten ist. Der Text im Suchfeld ist der von Ihnen ausgewählte Wert. Die angezeigten Ereignisse sind Ereignisse, die mit dem gewählten Wert zusammenhängen.

Informationen über die Untersuchung interessanter Elemente in der Ansicht „Ereignisse“ finden Sie unter „Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“ im *NetWitness Investigate – Benutzerhandbuch*.

Weitere Informationen zu Bedrohungsindikatoren finden Sie im Abschnitt „Bedrohungsindikatoren“ in der [Einführung](#).

## Top-Warmmeldungen verwalten

Sie können eine Liste aller Warmmeldungen in eine Datei im CSV-Format exportieren. Anhand dieser Informationen kann ein Analyst die Daten aus anderen Quellen in anderen Datenanalysewerkzeugen wie Tableau, Powerbi, Zepplin vergleichen.

### So exportieren Sie die Daten aus Warmmeldungen in eine CSV-Datei:

- Melden Sie sich bei NetWitness Plattform an und gehen Sie zu **UNTERSUCHEN > Benutzer > WARNMELDUNGEN**.  
Die Registerkarte „Warmmeldungen“ wird angezeigt.

RSA **RESPOND** **INVESTIGATE** MONITOR CONFIGURE ADMIN admin

Navigate Events Event Analysis Hosts Files Users Malware Analysis

OVERVIEW USERS **ALERTS**  Export

**Filters**  
 Severity  
 Feedback  
 Entity  
 Indicators  
 Date Range: Jan 29, 2018 - Jul 28, 2018 Clear

5 Critical 0 High 0 Medium 6 Low

ALERT NAME	ENTITY NAME	START TIME	# INDICATORS	STATUS	FEEDBACK
<b>Alert start 07/21/2018</b>					
<span>L</span> Brute Force Authentication   Hourly	GDennis	07/21/2018 22:00	2	Unreviewed	No feedback
<b>Alert start 07/20/2018</b>					
<span>L</span> Snooping User   Hourly	FCarres	07/20/2018 23:00	2	Unreviewed	No feedback
<span>L</span> Multiple Logons by User   Hourly	CBloyes	07/20/2018 22:00	2	Unreviewed	No feedback
<span>L</span> Non-Standard Hours   Hourly	ILittle	07/20/2018 21:00	1	Unreviewed	No feedback
<span>L</span> Multiple Logons by User   Hourly	FGooder	07/20/2018 21:00	2	Unreviewed	No feedback
<b>Alert start 07/18/2018</b>					
<span>L</span> Brute Force Authentication   Hourly	MTruss	07/18/2018 22:00	2	Unreviewed	No feedback
<b>Alert start 07/17/2018</b>					
<span>C</span> Snooping User   Hourly	CHunsto	07/17/2018 23:00	2	Unreviewed	No feedback
<span>C</span> Brute Force Authentication   Hourly	LBargh	07/17/2018 22:00	3	Unreviewed	No feedback
<span>C</span> Multiple Logons by User   Hourly	NHeasem	07/17/2018 21:00	2	Unreviewed	No feedback
<span>C</span> Non-Standard Hours   Hourly	AKeelin	07/17/2018 21:00	1	Unreviewed	No feedback

2. Klicken Sie oben rechts auf **Exportieren**.

Alle Warnmeldungsdaten werden in eine CSV-Datei heruntergeladen. Hier ein Beispiel für in das CSV-Format exportierte Warnmeldungsdaten:

	A	B	C	D	E	F	G
1	Alert Name	Entity Name	Start Time	# of Indicators	Status	Feedback	Severity
2	Brute Force Au	presidio_4769_u	Jul 21 2018 22:0	2	Reviewed	No Feedback	Low
3	Snooping User	4769_user122	Jul 20 2018 23:0	2	Reviewed	No Feedback	Low
4	Multiple Logon	presidio_4769_u	Jul 20 2018 22:0	2	Reviewed	No Feedback	Low
5	Non-Standard	4769_user122	Jul 20 2018 21:0	1	Reviewed	No Feedback	Low
6	Multiple Logon	PRESIDIO_USER:	Jul 20 2018 21:0	2	Reviewed	No Feedback	Low
7	Brute Force Au	presidio_4769_u	Jul 18 2018 22:0	2	Reviewed	No Feedback	Low
8	Snooping User	4769_user122	Jul 17 2018 23:0	2	Reviewed	No Feedback	Critical
9	Brute Force Au	presidio_4769_u	Jul 17 2018 22:0	3	Reviewed	No Feedback	Critical
10	Multiple Logon	PRESIDIO_USER:	Jul 17 2018 21:0	2	Reviewed	No Feedback	Critical
11	Non-Standard	4769_user122	Jul 17 2018 21:0	1	Reviewed	No Feedback	Critical
12							

## Anzeigen von NetWitness UEBA-Metriken zu Integrität und Zustand

RSA NetWitness UEBA sendet Metriken an die Registerkarte „Systemstatistikbrowser“ in **ADMIN > Integrität und Zustand**. Neben grundlegenden Informationen zur Systemnutzung werden auch für NetWitness UEBA-Benutzer spezifische Metriken, Warnmeldungen und Ereignisse bereitgestellt.

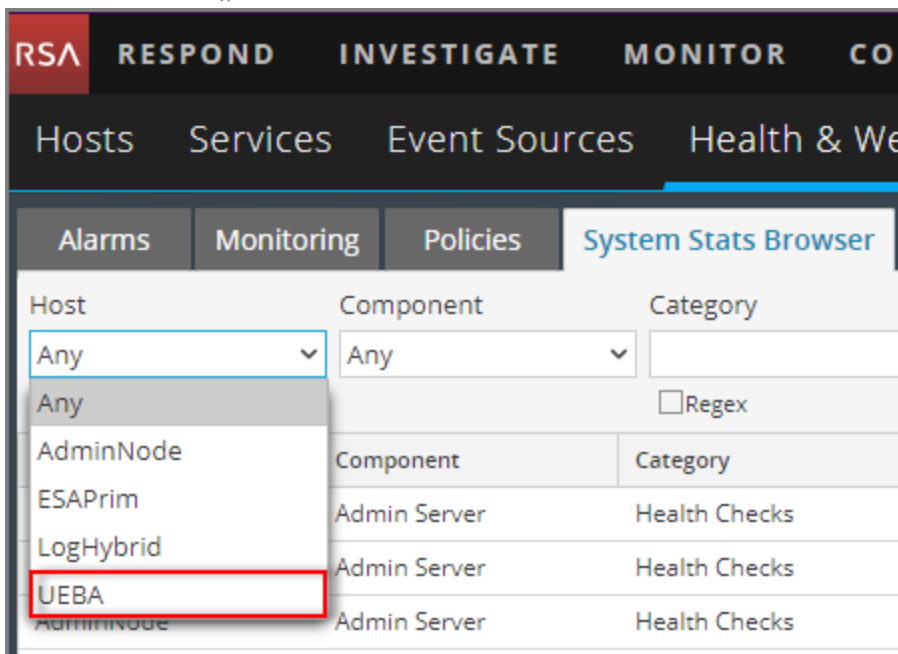
Analysten können diese Metriken auf folgende Weise verwenden:

- Bestätigen, dass die derzeit beschaffte Lizenz ihren Lizenzverträgen entspricht, sowie der Nutzungsdauer pro Tag
- Bestimmen, ob das System erwartungsgemäß funktioniert
- Aktives Beobachten neuer Ereignisse
- Überwachen der Erstellung neuer Indikatoren und Warnmeldungen

Wenn diese kritischen Metriken mit dem Wert „0“ gemeldet werden, könnte dies auf eine Systemstörung hinweisen.

### So zeigen Sie NetWitness UEBA-Metriken im Systemstatistikbrowser unter „Integrität und Zustand“ an:

1. Melden Sie sich bei NetWitness Platform an und gehen Sie zu **ADMIN > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte „Systemstatistikbrowser“.  
Die Registerkarte „Systemstatistikbrowser“ wird angezeigt.
3. Wählen Sie unter „Host“ **UEBA** aus und klicken Sie dann auf **Anwenden**.





Die Ergebnisse für NetWitness UEBA werden angezeigt.

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
UEBA	Host	FileSystem	Error Status		0	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/run/user/0	12.59 GB size 0 bytes used 12.59 GB available	2018-07-30 03:48:22 A...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/	29.99 GB size 9.32 GB used 20.67 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/dev	62.95 GB size 0 bytes used 62.95 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/home	9.99 GB size 32.19 MB used 9.96 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/var/netwitness	140.24 GB size 2.76 GB used 137.48 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/var/log	9.99 GB size 3.82 GB used 6.17 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/sysfs/cgroup	62.96 GB size 0 bytes used 62.96 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/run	62.96 GB size 4.12 GB used 58.84 GB available	2018-07-30 07:10:22 P...	

- Zum Anzeigen der Details für eine Statistik klicken Sie auf **Statistikdetails**.

Die Details zur Statistik werden angezeigt.

Stat Details	
Host	a14e8169-55d4-4bf9-b068-dd1abc8fa57e
Hostname	UEBA
Component ID	presidioairflow
Component	Presidio Airflow
Name	Daily Active Users Count
Subitem	
Path	
Plugin	presidioairflow_usage
Plugin Instance	
Type	gauge
Type Instance	active_users_count_last_day
Description	Number of active users in the previous 24 hour UTC time period
Category	Usage
Last Updated Time	2018-07-28 05:05:22 PM
Value	0
Raw Value	0.0
Graph Data Key	a14e8169-55d4-4bf9-b068-dd1abc8fa57e/presidioairflow_usage/gauge-active_users_count_last_day
Stat Key	a14e8169-55d4-4bf9-b068-dd1abc8fa57e/presidioairflow_usage/gauge-active_users_count_last_day

Die Felder **Name** und **Beschreibung** bieten eine Zusammenfassung der angezeigten Metriken.

Weitere Informationen über die Integrität und den Zustand und die Registerkarte „Systemstatistikbrowser“ finden Sie im *Leitfaden Systemwartung*. Navigieren Sie zu [Masterinhaltsverzeichnis](#), worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

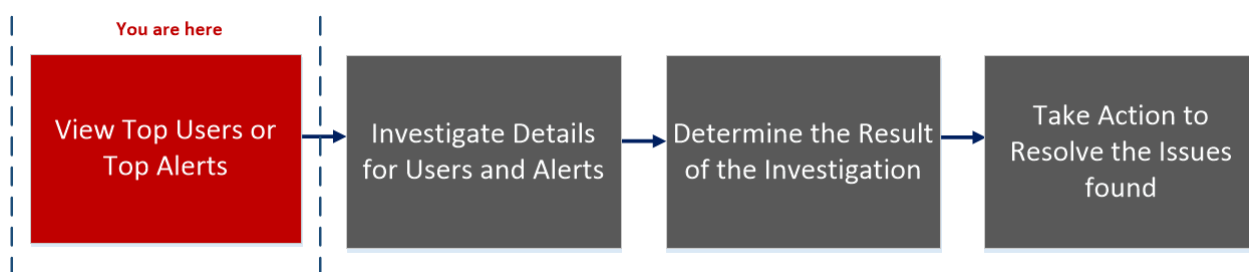
## Referenz

Dieser Abschnitt enthält Informationen über die Benutzeroberfläche von RSA NetWitness UEBA.

### Registerkarte „Übersicht“

Die Registerkarte **Übersicht** gibt einen ersten Einblick in die aktuellen und wichtigsten Nutzeraktivitäten in der Umgebung. Jeder Bereich zeigt entweder priorisierte Incidents für die Untersuchung oder konsolidierte Kennzahlen, die auf potenzielle Risiken für das Unternehmen hindeuten.

#### Workflow



#### Was möchten Sie tun?

Nutzerrolle	Ziel	Dokumentation
UEBA-Analyst	Anzeigen der fünf Nutzer mit dem höchsten Risiko.*	<a href="#">Identifizieren von Nutzern mit hohem Risiko</a>
UEBA-Analyst	Anzeigen von als riskant eingestuften Nutzern, von auf der Überwachungsliste stehenden Nutzern sowie von Administratoren.*	<a href="#">Identifizieren von Nutzern mit hohem Risiko</a>
UEBA-Analyst	Anzeigen von Nutzern basierend auf Typ der Warnmeldung und Indikator.	<a href="#">Identifizieren von Nutzern mit hohem Risiko</a>
UEBA-Analyst	Untersuchen von Warnmeldungen in meiner Umgebung.	<a href="#">Untersuchen von Top-Warnmeldungen</a>
UEBA-Analyst	Starten einer Untersuchung kritischer Warnmeldungen.	<a href="#">Untersuchen von Top-Warnmeldungen</a>
UEBA-Analyst	Sortieren von Warnmeldungen, um meine Untersuchung zu fokussieren.	<a href="#">Filtern von Warnmeldungen</a>

Nutzerrolle	Ziel	Dokumentation
UEBA-Analyst	Untersuchen von Bedrohungsindikatoren	<a href="#">Untersuchen von Indikatoren</a>
UEBA-Analyst	Exportieren von Warnmeldungsdaten	<a href="#">Top-Warmmeldungen verwalten</a>

\*Sie können diese Aufgaben hier durchführen.

## Verwandte Themen

- [Starten von Untersuchungen für Nutzer mit hohem Risiko](#)
- [Untersuchen von Top-Warmmeldungen](#)
- [Filtern von Warnmeldungen](#)
- [Top-Warmmeldungen verwalten](#)

## Überblick

Die folgende Abbildung zeigt die Registerkarte „Übersicht“.



Um auf diese Ansicht zuzugreifen, navigieren Sie zu **Ermittlung > Nutzer**.

Die Registerkarte „Übersicht“ enthält folgende Bereiche:

- 1 Bereich mit Nutzern mit hohem Risiko
- 2 Bereich mit Top-Warmmeldungen
- 3 Bereich mit allen Nutzern
- 4 Bereich mit Schweregrad der Warnmeldungen

### Bereich mit Nutzern mit hohem Risiko

Im diesem Bereich sind die fünf Nutzer mit dem höchsten Risiko zusammen mit ihrer Punktzahl aufgelistet.

Die folgende Tabelle beschreibt die Elemente dieses Bereichs.

Name	Beschreibung
Nutzername	Der Name des Nutzers.
Punktzahl	Die Punktzahl des Nutzers, wobei die Farbe den Schweregrad der Punktzahl angibt. Rot kennzeichnet einen Incident als „Kritisch“, Orange steht für Incidents mit der Risikobewertung „Hoch“, Gelb für Incidents mit der Risikobewertung „Mittel“ und Grün für Incidents mit der Risikobewertung „Niedrig“.

### Bereich mit Top-Warmmeldungen

In diesem Bereich werden eine Liste der Top-Warmmeldungen für den zugehörigen Nutzer, der Schweregrad, das Erstellungsdatum der Warmmeldung sowie die Anzahl der Indikatoren angezeigt. Die Liste umfasst die zehn wichtigsten Warmmeldungen der letzten 7 Tage.

Die folgende Tabelle beschreibt die wichtigsten Elemente dieses Bereichs.

Name	Beschreibung
Schweregrad-Symbol	Das Symbol für den Schweregrad der Warmmeldung. Die Optionen sind „Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“.
Name der Warmmeldung	Der Name der Warmmeldung.
Erstellungsdatum der Warmmeldung	Das Datum, an dem eine Warmmeldung erzeugt wurde.
Anzahl der Indikatoren	Die Anzahl der Indikatoren, die der Warmmeldung zugeordnet sind.

### Bereich mit allen Nutzern

In diesem Bereich werden die Nutzer in den einzelnen vordefinierten Gruppen von NetWitness UEBA angezeigt.


Die folgende Tabelle beschreibt die Elemente dieses Bereichs.

Gruppe	Beschreibung
Risikoreich	Alle Nutzer mit einem Risikowert größer als 0.
Unter Beobachtung	Alle Nutzer, die derzeit mit „Unter Beobachtung“ gekennzeichnet sind.
Administrator	Alle Nutzer, die zuvor als Administrator markiert wurden.

## Bereich mit Schweregrad der Warnmeldungen

In diesem Bereich wird die Anzahl der im vergangenen Jahr erzeugten Warnmeldungen nach Schweregrad graphisch dargestellt.

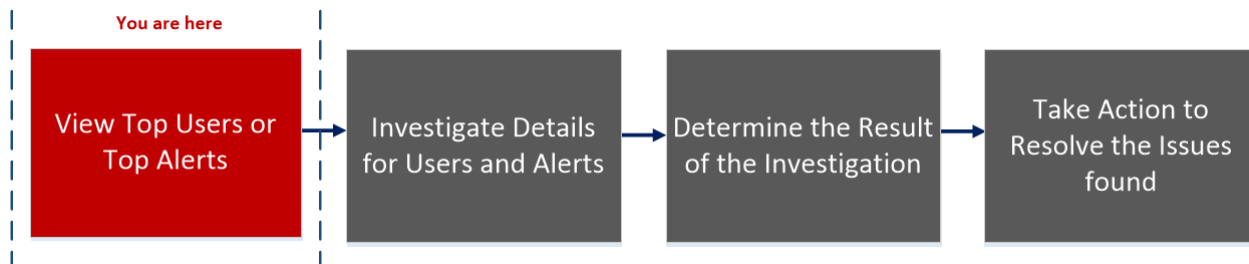
Die folgende Tabelle beschreibt die Elemente dieses Bereichs.

Name	Beschreibung
Letztes Jahr	Die Anzahl der im vergangenen Jahr erzeugten Warnmeldungen.
Schweregrad	<p>Für den Schweregrad wird folgender Farbcode verwendet: Rot kennzeichnet eine Warnmeldung als „Kritisch“, Orange steht für Warnmeldungen mit der Risikobewertung „Hoch“, Gelb für Warnmeldungen mit der Risikobewertung „Mittel“ und Grün für Warnmeldungen mit der Risikobewertung „Niedrig“.</p> <p>Beispiel:</p> 

## Registerkarte „Nutzer“

Die Registerkarte **Nutzer** ist eine proaktive Konsole zur Bedrohungserkennung. Sie können Verhaltensfilter verwenden, um vom Anwendungsfall abhängige Ziellisten zu erstellen und die Umgebung kontinuierlich auf bestimmte riskante Verhaltensmuster zu überwachen.

### Workflow



### Was möchten Sie tun?

Nutzerrolle	Ziel	Dokumentation
UEBA-Analyst	Anzeigen aller Nutzer mit hohem Risiko.*	<a href="#">Identifizieren von Nutzern mit hohem Risiko</a>
UEBA-Analyst	Anzeigen von Nutzern basierend auf Typ der Warnmeldung und Indikator.*	<a href="#">Identifizieren von Nutzern mit hohem Risiko</a>
UEBA-Analyst	Starten von Untersuchungen für Nutzer mit hohem Risiko.	<a href="#">Starten von Untersuchungen für Nutzer mit hohem Risiko</a>
UEBA-Analyst	Ergreifen von Maßnahmen für Nutzer mit hohem Risiko.*	<a href="#">Ergreifen von Maßnahmen für Nutzer mit hohem Risiko</a>
UEBA-Analyst	Exportieren von Nutzern mit hohem Risiko.*	<a href="#">Exportieren von Nutzern mit hohem Risiko</a>
UEBA-Analyst	Starten einer Untersuchung kritischer Warnmeldungen.	<a href="#">Untersuchen von Top-Warnmeldungen</a>
UEBA-Analyst	Untersuchen von Bedrohungsindikatoren	<a href="#">Untersuchen von Indikatoren</a>

\*Sie können diese Aufgaben hier durchführen.

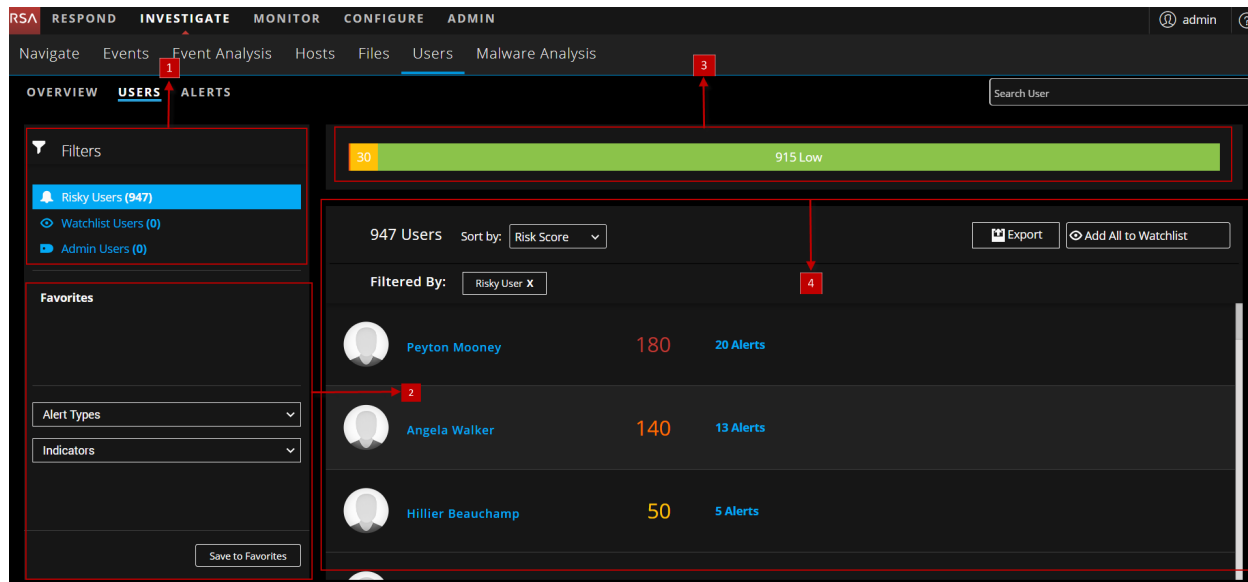
## Verwandte Themen

- [Starten von Untersuchungen für Nutzer mit hohem Risiko](#)
- [Untersuchen von Top-Warmmeldungen](#)
- [Filtern von Warmmeldungen](#)
- [Untersuchen von Indikatoren](#)
- [Exportieren von Nutzern mit hohem Risiko](#)



## Überblick

Die folgende Abbildung zeigt die Registerkarte „Nutzer“.



So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **Ermittlung** > **Nutzer**.  
Die Registerkarte „Übersicht“ wird angezeigt.
2. Klicken Sie auf **Nutzer**.

Die Registerkarte „Nutzer“ enthält folgende Bereiche:

- 1** Bereich „Filter“
- 2** Bereich „Favoriten“
- 3** Bereich „Risikoindikator“
- 4** Bereich „Nutzerliste“

### Bereich „Filter“

Im Bereich „Filter“ sind drei vordefinierte Filter aufgelistet, hinter denen jeweils in Klammern die zugehörige Anzahl der Nutzer angegeben ist.

In der folgenden Tabelle werden die Filtertypen beschrieben.

Filtertyp	Beschreibung
Nutzer mit hohem Risiko	Alle Nutzer mit einem Risikowert größer als 0.
Nutzerüberwachungsliste	Alle Nutzer, die derzeit mit „Unter Beobachtung“ gekennzeichnet sind.
Administratornutzer	Alle Nutzer, die zuvor als Administrator markiert wurden.

### Bereich „Favoriten“

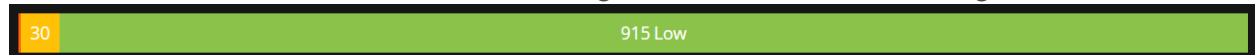
Der Bereich „Favoriten“ zeigt die Liste der Verhaltensprofile an, die als Favoriten gespeichert sind.

In der folgenden Tabelle werden die Filtertypen für die Verhaltensprofile beschrieben.

Filter	Beschreibung
Warnmeldungstypen	Beliebige der vorhandenen Warnmeldungstypen, die die unterstützten Anwendungsfälle beschreiben (z. B. Brute-Force-Angriff, Snooping durch Nutzer, Abnormale AD-Änderung, Datenexfiltration).
Indikatoren	Beliebige der vorhandenen Verhaltensmerkmale von NetWitness UEBA modelliert. Dieser Filter kann auch verwendet werden, um nur Warnmeldungen aus einer bestimmten Datenquelle oder Anwendung anzuzeigen.

### Bereich „Risikoindikator“

Der Risikoindikator liefert eine auf dem Schweregrad basierende Aufschlüsselung der Zielnutzer.



Die folgende Tabelle beschreibt die Elemente des Bereichs „Indikatoren“.

Farbe	Schweregrad
Rot	Kritisch
Orange	Hoch
Gelb	Mittel
Grün	Niedrig

## Nutzerlistenbereich

Der Bereich „Nutzerliste“ zeigt eine Liste aller Nutzer in Ihrer Umgebung zusammen mit der Nutzerpunktzahl und der Anzahl der dem Nutzer zugeordneten Warnmeldungen an.

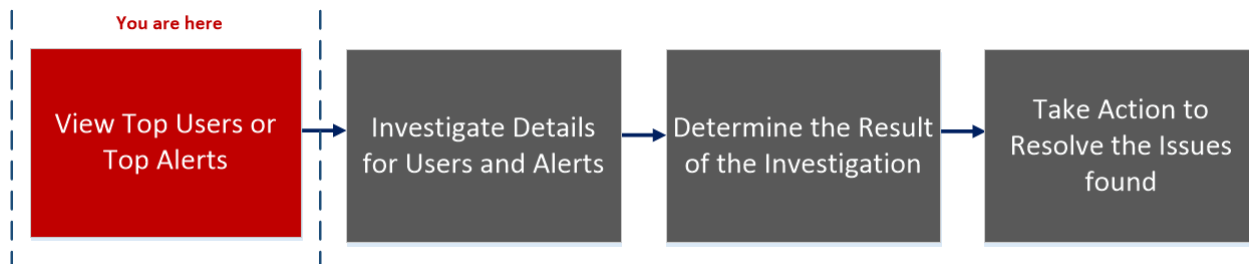
Die folgende Tabelle beschreibt die Elemente des Bereichs „Nutzerliste“.

Nutzerdaten	Beschreibung
Nutzername	Der Name des Nutzers.
Bewertung	Die Punktzahl des Nutzers.
Anzahl der Warnmeldungen	Die Gesamtzahl der für den Nutzer erzeugten Warnmeldungen.
Sortieren nach	Über das Drop-down-Menü „Sortieren nach“ können Sie die Sortiermethode für die Liste auswählen. Es sind folgende Optionen verfügbar: Risikowert, Name, Warnmeldungen
Exportieren	Exportieren Sie eine Liste aller Nutzer und deren Bewertung in eine CSV-Datei.
Alle zur Beobachtungsliste hinzufügen	Fügt alle Nutzer in der gefilterten Ansicht zur Beobachtungsliste hinzu.
Suchbenutzer	Sucht nach einem Nutzernamen, den Sie eingegeben haben, und wählt ihn aus der Liste aus, die zu Ihrem Eintrag angezeigt wird.

## Registerkarte „Warnmeldungen“

Auf der Registerkarte „Warnmeldungen“ werden Details zu allen Warnmeldungen in Ihrer Umgebung angezeigt. Sie können forensische Informationen zu verdächtigen Aktivitäten in Ihrer Umgebung anzeigen, die auf einem bestimmten Zeitrahmen basieren.

### Workflow



### Was möchten Sie tun?

Nutzerrolle	Ziel	Dokumentation
UEBA-Analyst	Untersuchen von Warnmeldungen in meiner Umgebung.*	<a href="#">Untersuchen von Top-Warnmeldungen</a>
UEBA-Analyst	Sortieren von Warnmeldungen, um meine Untersuchung zu fokussieren.*	<a href="#">Filtern von Warnmeldungen</a>
UEBA-Analyst	Untersuchen von Incidents anhand von Bedrohungsindikatoren.*	<a href="#">Untersuchen von Indikatoren</a>
UEBA-Analyst	Teilen von Warnmeldungsdaten im Tabellenformat.	<a href="#">Top-Warnmeldungen verwalten</a>
UEBA-Analyst	Schnelles Anzeigen einer Zusammenfassung von Nutzerwarnmeldungen.	<a href="#">Anzeigen von Zusammenfassungen von Nutzerwarnmeldungen</a>

\*Sie können diese Aufgaben hier durchführen.

### Verwandte Themen

- [Untersuchen von Top-Warnmeldungen](#)
- [Filtern von Warnmeldungen](#)
- [Untersuchen von Indikatoren](#)
- [Top-Warnmeldungen verwalten](#)

## Überblick

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **Ermittlung > Nutzer**.  
Die Registerkarte „Übersicht“ wird angezeigt.
2. Klicken Sie auf **Warnmeldungen**.

Die Registerkarte „Warnmeldungen“ enthält folgende Bereiche:

- 1 Bereich „Filter“
- 2 Bereich „Alerts“

### Bereich „Filter“

Verwenden Sie den Bereich „Filter“, um Ihre Untersuchung von Warnmeldungen zu verfeinern. Die Filter werden automatisch angewendet, wenn Sie Ihre Auswahl treffen. Sie können alle derzeit eingestellten Filter löschen, indem Sie auf **Löschen** klicken.

In der folgenden Tabelle werden die Filtertypen beschrieben.

Filtername	Beschreibung	Optionen
Schweregrad	Filtert die Liste der Warnmeldungen so, dass Warnmeldungen für einen oder mehrere Schweregrade angezeigt werden.	Kritisch, Hoch, Mittel oder Niedrig.
Feedback	Filtert die Liste der Warnmeldungen so, dass Warnmeldungen für einen oder mehrere Feedbacktypen angezeigt werden.	Wählen Sie „Alle“, „Kein Feedback“ oder „Kein Risiko“ aus.

Filtername	Beschreibung	Optionen
Entität	Filtert die Liste der Warnmeldungen so, dass nur Warnmeldungen für einen bestimmten Nutzernamen angezeigt werden.	NA.
Indikatoren	Filtert die Liste der Warnmeldungen so, dass Warnmeldungen für einen oder mehrere Indikatoren angezeigt werden.	Beispiele für Indikatoren sind: <ul style="list-style-type: none"> <li>• Active Directory – ungewöhnliche lange Anmeldezeit</li> <li>• Authentifizierung – Anmeldung an mehreren Computern</li> <li>• Mehrere Dateizugriffsfehler</li> </ul>
Datumsbereich	Filtert die Liste der Warnmeldungen so, dass Warnmeldungen angezeigt werden, die in einem bestimmten Zeitraum erstellt wurden.	Letzte Woche, letzter Monat oder ein benutzerdefinierter Zeitraum

### Bereich „Warnmeldungen“

Der Bereich „Warnmeldungen“ zeigt für jede Warnmeldung die folgenden Informationen an:

- Schweregrad-Symbol: Ein Symbol neben der Warnmeldung, das den Schweregrad der Warnmeldung anzeigt
- Name der Warnmeldung: Der Name der Warnmeldung und ihr Zeitrahmen
- Entitätsname: Der Name der Entität (Nutzerkonto), von der die Warnmeldung erzeugt wurde
- Startzeit: Datum und Uhrzeit der ersten Erkennung dieser Warnmeldung
- Indikatorenanzahl: Die Anzahl der einzigartigen Verhaltensanomalien (Indikatoren), die der Warnmeldung zugeordnet sind
- Status: Zeigt an, ob die Warnmeldung mit „Unüberprüft“ oder „Kein Risiko“ markiert wurde
- Feedback: Zeigt an, ob ein Feedbackwert für die Warnmeldung zugewiesen wurde

Am Anfang jeder Warnmeldungszeile befindet sich ein Symbol, mit dem die Warnmeldung erweitert werden kann, um zusätzliche Details anzuzeigen. Nach dem Erweitern werden folgende Felder angezeigt:

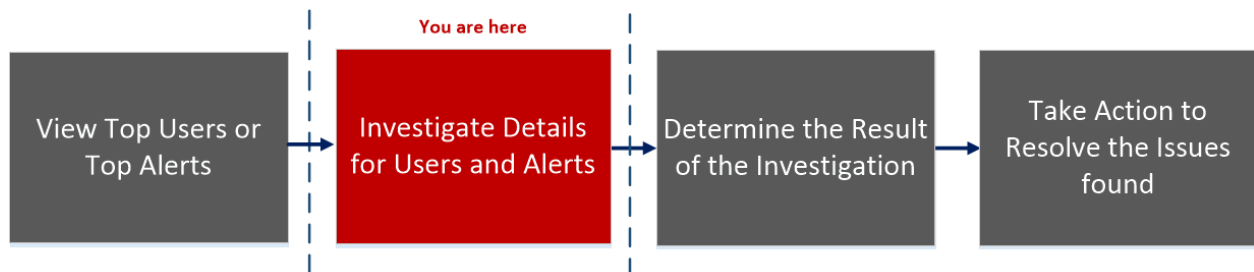
- Indikatorname: Der Name jedes einzelnen Indikators, der der Warnung zugeordnet ist
- Anomaliewert: Der Wert des Indikators, der den Betrag oder Wert der Abweichung darstellt, wenn er sich vom normalen Verhalten des Nutzers unterscheidet
- Datenquelle: Die Art der Daten, in denen der Indikator gefunden wurde
- Startzeit: Datum und Uhrzeit, an denen dieser Indikator zum ersten Mal erkannt wurde
- Ereignisanzahl: Die Anzahl der Ereignisse im Indikator

Die Daten, die derzeit im zentralen Bereich angezeigt werden, können in eine CSV-Datei exportiert werden, indem Sie oben rechts im Bereich auf „Export“ klicken.

## Ansicht „Nutzerprofil“

Die Ansicht **Nutzerprofil** bietet detaillierte Informationen zu allen Warnmeldungen eines Nutzers inklusive der zugehörigen Indikatoren.

### Workflow



### Was möchten Sie tun?

Nutzerrolle	Ziel	Dokumentation
UEBA-Analyst	Anzeigen aller Nutzer mit hohem Risiko*	<a href="#">Identifizieren von Nutzern mit hohem Risiko</a>
UEBA-Analyst	Starten von Untersuchungen für Nutzer mit hohem Risiko*	<a href="#">Starten von Untersuchungen für Nutzer mit hohem Risiko</a>
UEBA-Analyst	Ergreifen von Maßnahmen für Nutzer mit hohem Risiko.	<a href="#">Ergreifen von Maßnahmen für Nutzer mit hohem Risiko</a>
UEBA-Analyst	Exportieren von Nutzern mit hohem Risiko.	<a href="#">Exportieren von Nutzern mit hohem Risiko</a>
UEBA-Analyst	Starten einer Untersuchung kritischer Warnmeldungen*	<a href="#">Untersuchen von Top-Warnmeldungen</a>
UEBA-Analyst	Untersuchen von Bedrohungsindikatoren	<a href="#">Untersuchen von Indikatoren</a>

\*Sie können diese Aufgaben hier durchführen.



## Verwandte Themen

- [Starten von Untersuchungen für Nutzer mit hohem Risiko](#)
- [Untersuchen von Top-Warmmeldungen](#)
- [Filtern von Warmmeldungen](#)
- [Untersuchen von Indikatoren](#)
- [Exportieren von Nutzern mit hohem Risiko](#)

## Überblick

Die folgende Abbildung zeigt die Ansicht „Nutzerprofil“.

The screenshot shows the user profile for Angela Walker. The User Risk Score is 140. The Alerts section lists several events, including 'Multiple Group Membership Changes (167)'. The Alert Flow section shows a sequence of alerts for 'mass\_changes\_to\_groups'.

The screenshot shows a detailed view of an indicator for Angela Walker. The indicator is 'Multiple Group Membership Changes (Hourly)' with a 30% contribution to the alert. Below the indicator is a bar chart showing group changes over the last 30 days. A table below the chart lists detected events.

TIME DETECTED	USERNAME	USER ID	OPERATION TYPE	OPERATION TYPE CATEGORY	OBJECT NAME	RESULT
01/17/2018 23:42:57	AWalker	S-1-S-21-1957994488-2139871995-725345543-371587	Member Added To Group	GROUP_MEMBERSHIP, GROUP_MEMBERSHIP_ADD	FOD-CRM-PHPUsers-No-Blanks&No-History-Search	Success

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **Ermittlung** > **Nutzer**. Führen Sie eine der folgenden Aktionen aus:
  - a. Wählen Sie auf der Registerkarte **Übersicht** im Bereich **Nutzer mit hohem Risiko** einen Nutzer aus und klicken Sie entweder auf den Nutzernamen oder auf die Nutzerbewertung.
  - b. Klicken Sie auf der Registerkarte **Nutzer** auf den Nutzernamen.
  - c. Wählen Sie auf der Registerkarte **Warnmeldungen** den Namen einer Warnmeldung oder einer Entität aus.

Der Bereich „Nutzerprofil“ hat folgende Bereiche:

- 1** Bereich „Nutzerrisikobewertung“
- 2** Bereich „Warnmeldungsfluss“
- 3** Bereich „Indikatoren“

## Bereich „Nutzerrisikobewertung“

Der Bereich „Nutzerrisikobewertung“:

Name	Beschreibung
Punktzahl	Die entsprechend dem Schweregrad markierte Punktzahl des Nutzers.
Warnmeldungen	Die folgenden Informationen werden angezeigt: <ul style="list-style-type: none"> <li>• Die Namen der Warnmeldungen</li> <li>• Das Schweregrad-Symbol</li> <li>• Das Startdatum und die Startuhrzeit der Warnmeldung</li> <li>• Der Zeitrahmen der Warnmeldung (stündlich oder täglich)</li> <li>• Der Risikowert der Warnmeldung (+20)</li> <li>• Eine Liste der Namen der Indikatoren und die Häufigkeit, mit der die Indikatorereignisse aufgetreten sind.</li> </ul>
Sortieren nach	Die Warnmeldungen werden nach Schweregrad und Datum sortiert. Standardmäßig werden sie nach Schweregrad sortiert.

## Bereich „Warnmeldungsfluss“

Im Bereich „Warnmeldungsfluss“ werden die folgenden Informationen angezeigt:

Name	Beschreibung
Name der Warnmeldung	Der Name der Warnmeldung.

Name	Beschreibung
Zeitraumen	Der Zeitrahmen der Warnmeldung (stündlich oder täglich).
Schweregrad	Der Schweregrad der Warnmeldung.
Beitrag zur Nutzerpunktzahl	Der Beitrag zur Nutzerpunktzahl (z. B. +20).
Quellen	Die Datenquellen für die Warnmeldung (z. B. Active Directory).
Graphische Darstellung der Zeitleiste	Die Zeitleiste der Ereignisse, die mit dem Entstehen der Warnmeldung zusammenhängen.

## Bereich „Indikatoren“

Klicken Sie auf ein Diagrammsymbol im Bereich „Warnmeldungsfluss“, um den Bereich „Indikatoren“ zu öffnen. Die folgende Tabelle beschreibt die Elemente des Bereichs „Indikatoren“.

Name	Beschreibung
Indikator	Der Name des Indikators mit dem Zeitrahmen des Indikators in Klammern. Beispiel: Mehrere Änderungen an der Gruppenmitgliedschaft (stündlich)
Beitrag zur Warnmeldung	Der zum Entstehen der Warnmeldung geleistete Beitrag in Prozent.
Anomaliewert	Der Anomaliewert.
Datenquelle	Die Datenquelle, von der die Warnmeldung ausgelöst wird.
Zeit der Erkennung	Das Datum und die Uhrzeit für das Auslösen des Indikators.
Nutzername	Der Name des Nutzers, für den ein Indikator ausgelöst wird.
Nutzer-ID	Der ID des Nutzers, für den ein Indikator ausgelöst wird.
Betriebstyp	Die vom Nutzer ausgeführte Aktion. Beispiel: Hinzufügen eines Mitglieds zur Gruppe
Kategorie des Vorgangstyps	Die Kategorie des Vorgangstyps. Beispiel: GROUP_MEMBERSHIP
Ergebnis	Der Status der vom Nutzer ausgeführten Aktion.

## Anhang: NetWitness UEBA – Windows-Überwachungsrichtlinien

RSA empfiehlt, die hier beschriebenen Windows-Überwachungsrichtlinien umzusetzen. So ziehen Sie den größten Nutzen aus RSA NetWitness UEBA.

Informationen zu den grundlegenden Überwachungsrichtlinien finden Sie im Abschnitt „Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, und Windows Server 2008 Überwachungseinstellungen“ des folgenden Microsoft-Artikels: [Empfehlungen zu Überwachungsrichtlinien](#).

Die Richtlinien unter „Nachdrücklichere Empfehlung“ sind ebenso erforderlich wie die folgenden Richtlinien, damit alle erforderlichen Authentifizierungs- und Active Directory-Ereignisse sicher überwacht werden:

- Überwachung detaillierter Dateifreigabe
- Überwachung der Dateifreigabe
- Überwachung des Dateisystems

RSA empfiehlt, die Überwachung sowohl für Erfolge als auch für Misserfolge zu aktivieren.

Folgende Windows-Ereignisse müssen überwacht werden:

### Für die Authentifizierungsmodelle:

4624 4625 4769

### Für die AD-Modelle:

4670 4717 4720 4722 4723 4724 4725 4726

4727 4728 4729 4730 4731 4732 4733 4734

4735 4737 4738 4739 4740 4741 4742 4743

4754 4755 4756 4757 4758 4764 4767 4794

5136 5376 5377

### Für Dateizugriffsmodelle:

4660 4663 4670 5145

